КАРДАШЕВСЬКИЙ Ю. Р.,
доктор філософії у галузі права,
керівник відділу внутрішнього контролю
(Національне агентство з питань запобігання корупції)

УДК 343.9
DOI https://doi.org/10.32842/2078-3736/2025.4.2.29

СУЧАСНІ ВИКЛИКИ КІБЕРЗЛОЧИННОСТІ В БАНКІВСЬКОМУ СЕКТОРІ

Стаття присвячена дослідженню проблеми кіберзлочинності в банківському секторі України в умовах стрімкого розвитку цифрових технологій та змін у сфері кібербезпеки. Зазначено, що кіберзлочинність у фінансовому секторі становить серйозну загрозу для стабільності національної економіки та безпеки. Злочинці використовують різні методи для порушення роботи банківських систем, серед яких особливо поширеними є фішинг, DDoS-атаки, програми-вимагачі та крадіжки персональних даних. Ці атаки спрямовані не лише на фінансове збагачення, але й на отримання доступу до конфіденційної інформації, що може призвести до значних фінансових втрат та втрати довіри до фінансової системи країни.

Однією з основних проблем є вразливості банківських інформаційних систем, які часто виникають через використання застарілих технологій, недостатню увагу до оновлення програмного забезпечення та недостатню підготовку персоналу. Така ситуація відкриває можливості для несанкціонованого доступу до даних, загрожує безпеці клієнтів та створює умови для незаконних фінансових операцій. Окрім технічних факторів, важливою є проблема соціальної інженерії. Злочинці активно маніпулюють співробітниками банків для отримання доступу до конфіденційної інформації, використовуючи методи фішингу через електронну пошту або соціальні мережі.

У статті також підкреслюється, що боротьба з кіберзлочинністю в банківському секторі вимагає постійного моніторингу нових загроз та адаптації заходів безпеки. Це передбачає впровадження сучасних методологій, таких як ризик-орієнтований підхід та методика IOCTA Європолу, які дозволяють ефективно оцінювати ризики та мінімізувати їх вплив на фінансову систему. У статті також проаналізовано кримінальні правопорушення, передбачені Кримінальним кодексом України, зокрема крадіжки, незаконні операції з платіжними картками, відмивання грошей та порушення банківської таємниці. Найбільш поширеними є правопорушення, визначені у статті 200 Кримінального кодексу України, пов'язані з незаконними діями з платіжними картками, та у статті *209, яка охоплює відмивання грошей, отриманих злочинним шляхом.*

Ключові слова: *кіберзлочинність, банківська картка, банківський рахунок, крадіжка даних платіжних карток, відмивання грошей.*

Kardashevskyy Yu. R. Current challenges of cybercrime in the banking sector

The article is dedicated to examining the problem of cybercrime in the banking sector of Ukraine in the context of rapid digital technology development and changes in the field of cybersecurity. It is noted that cybercrime in the financial sector poses a serious threat to the stability of the national economy and security. Criminals use

various methods to disrupt the operation of banking systems, with phishing, DDoS attacks, ransomware, and theft of personal data being particularly widespread. These attacks aim not only at financial enrichment but also at gaining access to confidential information, which can lead to significant financial losses and a loss of trust in the country's financial system.

One of the main problems is the vulnerabilities in banking information systems, which often arise due to the use of outdated technologies, insufficient attention to software updates, and inadequate staff training. This situation opens opportunities for unauthorized access to data, threatening the security of clients and creating conditions for illegal financial transactions. In addition to technical factors, the problem of social engineering is also important. Criminals actively manipulate bank employees to gain access to confidential information, using phishing methods via email or social media.

The article also emphasizes that combating cybercrime in the banking sector requires constant monitoring of emerging threats and the adaptation of security measures. This involves implementing modern methodologies, such as a risk-oriented approach and Europol's IOCTA methods, which allow for effective risk assessment and minimizing their impact on the financial system. The article also analyzes criminal offenses outlined in the Criminal Code of Ukraine, specifically theft, illegal activities with payment cards, money laundering, and violation of banking secrecy. The most common offenses are those defined in Article 200 of the Criminal Code of Ukraine, related to illegal actions with payment cards, and Article 209, which covers money laundering.

Key words: *cybercrime, bank card, bank account, payment card data theft, money laundering.*

Постановка проблеми. Розвиток цифрових технологій формує новітні виклики глобальному світу та національним економікам, суттєво впливає на формування базових засад кібербезпеки. Сучасні національні інтереси пріоритетно зосереджуються на формуванні кіберстійкості країни, ключовими напрямами якої є захист критичної інфраструктури, зниження рівня кіберзлочинності, підвищення обізнаності та дотримання інтересів національної безпеки [1].

Протидія кіберзлочинності сьогодні є невід'ємною частиною протиборства в кіберпросторі. Водночас, в умовах формування сучасних технологічних викликів, що сприяють поширенню новітніх загроз, зокрема і в кіберпросторі, у суспільстві значно зросли вимоги щодо підвищення ефективності та результативності діяльності органів правопорядку. Саме тому трендом правоохоронної діяльності сьогодні є упровадження стратегічного менеджменту на основі розвитку сучасних методологій інформаційно-аналітичного забезпечення та осмислення реальних тенденцій в кримінальному середовищі.

В останні роки, у дослідженнях багатьох відомих вітчизняних дослідників, значна увага приділяється різним проблемам, пов'язаним з розробкою напрямів щодо кібербезпеки, зокрема протидії кіберзлочинності: Баранова О.А. [2], Бєлякова К.І. [3; 4], Бірюкова Д.С., Бутузова В.М. [5; 6], Веселової Л.Ю. [10], Гавловського В.Д. [13; 14], Гуцалюка М.В. [15; 16], Довганя О.Д. [7], Дубова Д.В., Казмірчук С. [8], Кормича Б.А., Корченка О.Г. [8], Лісовської Ю.П., Марущака А.І. [9], Пилипчука В.Г., Тихомирова О.О., Хахановського В.Г. [19], Цимбалюка В.С., Швеця М.Я., Шеломенцева В.П. [17; 20] та інших. Значну увагу цим питанням приділяли у своїх роботах відомі науковці та фахівці в зарубіжних виданнях [21–24]. Разом з тим, розуміння реального стану та упровадження адекватної державної політики у цій сфері потребує компетентного розвідувального аналітичного процесу, усвідомлення сучасних трендів й реального пізнання ключових кіберзагроз [10-12].

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 кіберзлочинності в банківській сфері.

Метою статті є дослідження проблематики кіберзлочинності в банківській сфері та специфіка їх прояву в Україні, враховуючи окремі характеристики та ознаки вчинення цього злочину.

Виклад основного матеріалу. Небезпечні високотехнологічні загрози глобального характеру, що мають високий потенційний вплив та руйнівні наслідки для життєдіяльності будь-якого суспільства, є невід'ємним наслідком розвитку новітніх технологій. І охорона суспільних відносин, інтересів людини, суспільства та держави в сфері кіберпростору займає одне з пріоритетних місць в системі національної безпеки. Сучасний світ, враховуючи такі зміни намагається враховувати загальні тенденції та впроваджувати механізми протидії кіберзлочинності [25].

Зокрема, і кіберзлочинність у банківській сфері є серйозною загрозою для фінансової безпеки та стабільності. Зловмисники використовують різноманітні методи для порушення роботи банківських систем, що включає як технічні, так і психологічні методи впливу на користувачів. Однією з найбільших проблем є зростання кількості кібератак, таких як фішинг, DDoS-атаки, віруси-шифрувальники та крадіжка персональних даних. Ці атаки мають на меті не лише безпосереднє фінансове збагачення, а й доступ до конфіденційної інформації, що може завдати значної шкоди клієнтам банків.

Ще однією важливою проблемою є вразливості в банківських інформаційних системах. Багато фінансових установ використовують застарілі системи, що не відповідають сучасним стандартам безпеки, що дозволяє зловмисникам використовувати різні методи для несанкціонованого доступу до даних. Це може бути як технічна неосвіченість персоналу, так і недостатня увага до оновлення програмного забезпечення.

Крім того, соціальна інженерія залишається серйозною загрозою. Атаки на працівників банку через маніпуляції або обман, коли зловмисники намагаються отримати доступ до конфіденційної інформації, також є частим явищем. Це може включати фішинг через електронну пошту або соціальні мережі, а також методи, що передбачають безпосереднє втручання в робочі процеси банківських працівників.

Враховуючи ці фактори, кіберзлочинність у банківському секторі вимагає постійного моніторингу та адаптації заходів безпеки для боротьби з новими загрозами, що з'являються з розвитком технологій.

Використовуючи методологію Європолу IOCTA та застосовуючи ризик-орієнтований підхід, на стратегічному рівні проаналізовано особливості кіберзлочинності в банківській сфері в Україні.

За вітчизняним кримінальним законодавством до переліку кримінальних правопорушень в банківській сфері відносяться такі:

Стаття 185. *Крадіжка*

Стаття 200. *Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення*

Стаття 209. *Легалізація (відмивання) майна, одержаного злочинним шляхом*

Стаття 231. *Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю*

Найбільш поширеними, за даними опитування працівників кіберполіції НПУ [25], у зазначеному переліку є кримінальні правопорушення, передбачені статтею 200 ККУ (66%) (*рис. 1)*. Водночас крадіжка (185 ККУ) та відмивання коштів (209 ККУ) на думку експертів кіберполіції також мають значне поширення.

Загальне співвідношення кримінальних правопорушень цієї групи за наслідками їх вчинення переважно зберігається. Найзначнішими наслідками характеризується к/п за ст. 200 ККУ. Водночас, серед інших виділяються к/п передбачені ст. 209 ККУ, які характеризуються в усьому спектрі сум матеріальними збитками, у тому числі і щодо сум в окремих випадках більше 500 млн. грн. та 1 млрд. грн. (*табл. 1*).

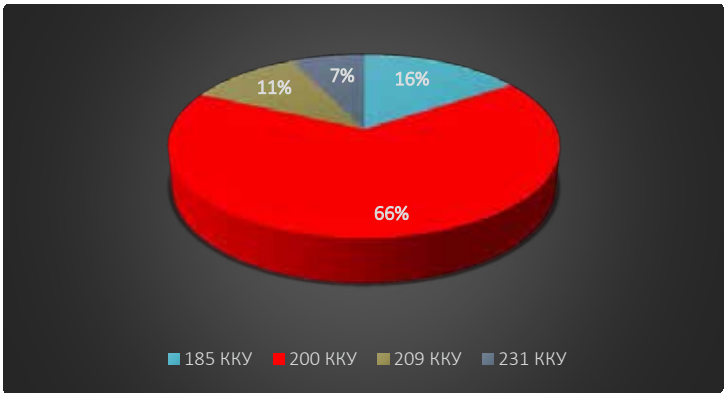

Рис. 1. Питома вага кіберзлочинів, що вчиняються в банківській сфері

Таблиця 1

Співвідношення злочинів за наслідками їх вчинення та сумою збитків

	185 ККУ	200 ККУ	209 ККУ	231 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, за даними експертного опитування, при розгляді наслідків вчинення к/п цієї групи, серед суб'єктів переважно найбільших збитків зазнають фізичні особи та держава. Водночас, значні збитки несуть державні та комерційні підприємства від протиправної діяльності, передбаченої ст. 200 ККУ (*табл. 2*).

Таблиця 2

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

	185 ККУ	200 ККУ	209 ККУ	231 ККУ
Державі				
Державному органу				
Державному підприємству (установі)				
Комерційному підприємству				
Фізичній особі				

Мотивація злочинців, перш за все, повязана з їх матеріальним збагаченням, що характеризується вибіркою 55-59% в межах генеральної сукупності (*Табл.3*). Водночас, вибіркою в межах 10-17% 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: 185 ККУ – 7%; 200 ККУ – 16%; 209 ККУ – 14%.

Таблиця 3

Мотивація злочинців

Мотивація злочинців	185 ККУ %	200 ККУ %	209 ККУ %
матеріальне збагачення	55	55	59
складова гібридної війни	17	11	10
співпраця з агресором	7	16	14
хуліганські дії	8	13	14
соціальний протест	3	2	3
невідомо	10	3	0

Експертним середовищем акцентовано увагу на вчиненні певної частини злочинів у банківській сфері організованими злочинними угрупованнями (*Табл. 4*).

Таблиця 4

Питома вага вчинених злочинів ОЗУ

Стаття ККУ	185 ККУ	200 ККУ	209 ККУ
ОЗУ, %	14,70	35,79	29,79
ОЗУ укр, %	5,88	7,72	17,02

За наявними ознаками кваліфікації злочинів, передбачених ст. 200 ККУ більше 35 відсотків вчиняється у складі ОЗУ і майже третина – за ст. 209 ККУ. Водночас, експерти зазначають щодо загрози діяльності ОЗУ безпосередньо на території України: за ст. 185 ККУ – 5,88%; за ст. 200 ККУ – 7,72%; за ст. 209 ККУ – 17,02%.

Висновки. Кіберзлочини в банківській сфері, пов'язані з незаконними діями з банківськими картками та доступом до банківських рахунків, крадіжкою даних платіжних карток та відмиванням коштів. Відповідні злочини не лише спричиняють значні матеріальні втрати (до 1 млрд грн), але й часто мають організований характер.

Кіберзлочинність у банківській сфері становить серйозну загрозу для національної безпеки та економіки, зокрема через використання новітніх технологій і методів впливу на фінансові установи. Стаття вказує на основні проблеми, такі як зростання кібератак (фішинг, DDoS-атаки, віруси-шифрувальники) та вразливості банківських систем через застаріле програмне забезпечення та недоліки у кваліфікації персоналу. Особливу увагу приділено соціальній інженерії та маніпуляціям з боку злочинців для отримання доступу до конфіденційної інформації.

Дослідження також підкреслює важливість постійного моніторингу та адаптації заходів безпеки в умовах технологічного розвитку. Використовуючи методологію Європолу IOCTA та ризик-орієнтований підхід, стаття аналізує поширеність кіберзлочинів, таких як крадіжка, незаконні дії з платіжними картками та відмивання коштів. Більшість злочинів мотивовані матеріальним збагаченням, а також відзначається роль організованих злочинних угруповань у скоєнні таких правопорушень. Враховуючи ці обставини, стаття акцентує на необхідності посиленої роботи правоохоронних органів та вдосконалення політики у сфері кібербезпеки.

Список використаних джерел:

1. Roger Hurwitz. Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace. *Georgetown Journal of International Affairs*: Georgetown University. 2014.

2. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи. Київ : Видавничий дім «СофтПрес», 2005. 316 с.

3. Бєляков К.І. Інформація в праві: теорія і практика: монографія. Київ: Видавництво «КВІЦ», 2006. 116 с.

4. Zolotar, O. O., Zaitsev, M. M., Topolnitskyi, 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

5. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ : КИТ, 2010. 408 с.

6. Бутузов В.М., Тітуніна К.В. Сучасні загрози: комп'ютерний тероризм. *Боротьба з організованою злочинністю і корупцією*. 2007. № 17. С. 316–324.

7. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія. Київ : Видавничий дім «АртЕк», 2017. 107 с.

8. Корченко О., Казмірчук С., Ахметов Б. Прикладні системи оцінювання ризиків інформаційної безпеки : монографія, Київ : ЦП Компринт, 2017. 435 с.

9. Марущак А.І. Інформаційні ресурси держави: зміст та проблема захисту. *Правова інформатика*. 2009. № 1(21). С. 65–71.

10. Користін О.Є., Веселова Л.Ю. Ризикорієнтованість кібербезпеки. *Наука і правоохоронна*. 2021. № 3. С. 16–23.

11. Користін О.Є., Користін О.О. Загрози у сфері кібербезпеки в Україні. *Наука і правоохоронна*. 2022. № 1 (55). С. 119–126. DOI: https: //doi.org/10.36486/np.2022.1(55)

12. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021. Publications Office of the European Union. Luxembourg. 2021.

13. Гавловський В.Д. Захист інформації шляхом посилення ефективності протидії кібератакам. *Інформація і право.* 2019. № 2(30). С. 105–110.

14. 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.

15. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності. Інформація і право. 2019. № 1(28). С. 118–128.

16. 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.

17. 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.

18. 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.

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. Організована кіберзлочинність: до визначення поняття. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2009. Вип. 21. С. 314–322.

21. 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.

22. 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

23. 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

24. Bodeau, D. & Graubart, R. (2011). Cyber resiliency engineering framework. MTR110237. Retrieved from http://www.mitre.org/sites/default/files/pdf/ 11_4436.pdf3

25. Директива Європейського Парламенту І Ради (ЄС) 2016/1148 від 6 липн. 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA

26. 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 першого надходження рукопису до видання: 25.07.2025
Дата прийнятого до друку рукопису після рецензування: 22.08.2025
Дата публікації: 26.09.2025