ISSN 2072-8670 (Print) **НАУКА І ПРАВООХОРОНА**
NAUKA I PRAVOOKHORONA

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) **Issue 3-4(65-66) 2024**

УДК 343.97:336.7

Користін Олександр Євгенійович,
доктор юридичних наук, професор,
заслужений діяч науки і техніки України,
головний науковий співробітник ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0001-9056-5475
Кардашевський Юрій Романович,
доктор філософії в галузі права, керівник відділу внутрішнього
контролю НАЗК, м. Київ, Україна,
ORCID ID 0009-0009-8940-6384

КІБЕРЗЛОЧИННІСТЬ У БАНКІВСЬКІЙ СФЕРІ

У статті досліджено проблему кіберзлочинності в банківській сфері України, акцентуючи увагу на загрозах для фінансової безпеки та стабільності. В умовах стрімкого розвитку цифрових технологій кіберзлочинці використовують різноманітні методи, такі як фішинг, DDoS-атаки, віруси-шифрувальники та крадіжка персональних даних, що призводять до значних фінансових і репутаційних втрат. Розглянуто проблему вразливостей у банківських інформаційних системах, зокрема через застарілі технології та недоліки у кваліфікації персоналу. Окрему увагу зосереджено на методах соціальної інженерії. Визначено, що кіберзлочинність у банківському секторі вимагає постійного оновлення заходів безпеки. Використовуючи методологію Європолу IOCTA, проаналізовано кримінальні правопорушення в Україні, зокрема крадіжки, незаконні дії з платіжними картками та відмивання коштів і наголошено на важливості розвитку стратегічного менеджменту для протидії цим загрозам.

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

Постановка проблеми. Розвиток цифрових технологій формує новітні виклики глобальному світу та національним економікам, суттєво впливає на формування базових засад кібербезпеки. Сьогодні 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. В умовах формування сучасних технологічних викликів, що сприяють поширенню новітніх загроз, зокрема й у кіберпросторі, у суспільстві значно зросли вимоги щодо підвищення ефективності та результативності діяльності органів правопорядку. Саме тому трендом правоохоронної діяльності є упровадження стратегічного менеджменту на основі розвитку методологій інформаційно-аналітичного забезпечення та осмислення реальних тенденцій у кримінальному середовищі.

DOI (Article): https://doi.org/10.36486/np.2024.3(65).13

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

Останнім часом в дослідженнях багатьох відомих вітчизняних дослідників: Баранова О.А. [2], Бєлякова К.І. [3; 4], Бірюкова Д.С., Бутузова В.М. [5; 6], Веселової Л.Ю. [7], Гавловського В.Д. [8; 9; 10], Гуцалюка М.В. [11; 12], Довганя О.Д. [13], Дубова Д.В., Казмірчук С. [14], Кормича Б.А., Корченка О.Г. [14], Лісовської Ю.П., Марущака А.І. [15], Пилипчука В.Г., Тихомирова О.О., Хахановського В.Г. [16], Цимбалюка В.С., Швеця М.Я., Шеломенцева В.П. [17; 18] та інших значна увага приділяється різним проблемам, пов'язаним з розробкою напрямів щодо кібербезпеки, а також протидії кіберзлочинності. Вивчали окреслене питання у своїх роботах і зарубіжні науковці та фахівці [19–22]. Розуміння реального стану та впровадження адекватної державної політики в цій сфері потребує компетентного розвідувального аналітичного процесу, усвідомлення сучасних трендів і реального пізнання ключових кіберзагроз [7; 23; 24].

Зважаючи на стрімкий технологічний розвиток інформаційного простору та цифрового контенту, окремі напрями кіберзлочинів, зокрема й у банківській сфері, набувають особливого розвитку та поширення і є загрозою не лише для нинішнього світу, а й майбутніх процесів і суспільних відносин.

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

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 у сфері кіберпростору посідає одне з пріоритетних місць у системі національної безпеки. Сучасний світ з огляду на такі зміни намагається брати до уваги загальні тенденції та впроваджувати механізми протидії кіберзлочинності [25].

Нині зловмисники використовують різноманітні методи для порушення роботи банківської системи, що включають і технічні, і психологічні методи впливу на користувачів. Серед найбільших загроз є зростання кількості кібератак, таких як фішинг, DDoS-атаки, віруси-шифрувальники та крадіжка персональних даних, які мають на меті не лише безпосереднє фінансове збагачення, а й доступ до конфіденційної інформації, що може завдати значної шкоди клієнтам банків.

Важливою проблемою є й вразливості в банківських інформаційних системах. Багато фінансових установ через технічну неосвіченість персоналу або недостатню увагу до оновлення програмного забезпечення використовують застарілі системи, які не відповідають сучасним стандартам безпеки, що дає змогу зловмисникам застосовувати різні методи для несанкціонованого доступу до даних.

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, безпосереднє втручання в робочі процеси банківських працівників.

З огляду на такі 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 у банківській сфері належать 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.

За даними опитування працівників кіберполіції НПУ найбільш поширеними в зазначеному переліку є кримінальні правопорушення, передбачені ст. 200 КК України (66 %). Водночас крадіжка (185 КК України) та відмивання коштів (209 КК України), на думку експертів кіберполіції, також значно поширені.

Загальне співвідношення кримінальних правопорушень цієї групи за наслідками їх вчинення переважно зберігається. Найзначнішими наслідками характеризуються кримінальні правопорушення, передбачені ст. 200 КК України. Серед інших виокремлюють кримінальні правопорушення, передбачені ст. 209 КК України, які характеризуються в усьому спектрі сум матеріальними збитками, у тому числі й щодо сум у певних випадках понад 500 млн грн та 1 млрд грн (табл. 1).

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				

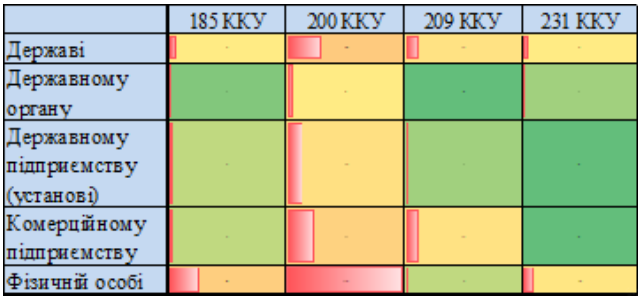
Крім того, за даними експертного опитування при розгляді наслідків вчинення кримінальних правопорушень цієї групи серед суб'єктів переважно найбільших збитків зазнають фізичні особи та держава. Водночас значні збитки несуть державні та

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

комерційні підприємства від протиправної діяльності, передбаченої ст. 200 КК України (табл. 2).

Таблиця 2

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



Мотивація злочинців передусім пов'язана з їх матеріальним збагаченням, що характеризується вибіркою 55–59 % у межах генеральної сукупності (табл. 3). Вибіркою в межах 10–17 % зазначена 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 КК України – 7 %, 200 КК України – 16 %, 209 КК України – 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

DOI (Article): https://doi.org/10.36486/np.2024.3(65).13

За наявними ознаками кваліфікації злочинів, передбачених ст. 200 КК України, понад 35 % вчиняється у складі ОЗУ і майже третина – за ст. 209 КК України. Загроза діяльності ОЗУ безпосередньо на території України становить: за ст. 185 КК України – 5,88 %, за ст. 200 КК України – 7,72 %, за ст. 209 КК України – 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. Автори вказали на основні проблеми, такі як зростання кібератак (фішинг, DDoS-атаки, віруси-шифрувальники) і вразливості банківських систем через застаріле програмне забезпечення й недоліки у кваліфікації персоналу. Особливу увагу зосереджено на соціальній інженерії та маніпуляціях з боку злочинців для отримання доступу до конфіденційної інформації.

У дослідженні наголошено й на важливості постійного моніторингу та адаптації заходів безпеки в умовах технологічного розвитку. Використовуючи методологію Європолу IOCTA та ризик-орієнтований підхід, ми проаналізували 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 цих правопорушень. З огляду на викладені обставини ми акцентуємо увагу на необхідності посиленої роботи правоохоронних органів та вдосконаленні 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: СофтПрес, 2005. 316 с.

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

4. *Zolotar O.O., Zaitsev M.M., Topolnitskyi V.V., Bieliakov K.I. & Koropatnik I.M*. Prospects and current status of defence information security in Ukraine. *Linguistics and Culture Review.* 2021. 5(S3), 513–524. DOI: https://doi.org/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. *Користін О.Є., Веселова Л.Ю.* Ризикорієнтованість кібербезпеки. *Наука і правоохоронна.* 2021. № 3. С. 16–23.

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

9. *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.

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

10. *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.

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

12. *Гуцалюк М.В., Хахановський В.Г.* Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* 2020. 31(1). С. 13–19. DOI: https://doi.org/10.37025/1992-4437/2019-31-1-13.

13. *Довгань О.Д., Доронін І.М.* Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. Київ: АртЕк, 2017. 107 с.

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

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

16. *Хахановський В.Г., Гавловський В.Д.* Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. *Інформація і право.* 2020. № 2(33). С. 99–110.

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

19. *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.* Challenges in network science: applications to infrastructures, climate, social systems, and economics. *European Physical Journal: Special Topics.* 2012. P. 214, 273–293.

20. *Jansen W.* Directions in security metrics research. The National Institute of Standards and Technology (NISTIR), 7564. 2009. URL: http://csrc. nist.gov/publications/nistir/ir7564/nistir-7564_ metrics-research.pdf (дата звернення: 15.10.2024).

21. *Bartol N., Bates B., Goertzel K. & Winograd T.* Measuring cyber security and information assurance: a state of the art report. 2009. URL: https://www.thecsiac.com/sites/default/files/ cybersecurity.pdf (дата звернення: 15.10.2024).

22. *Bodeau D. & Graubart R.* Cyber resiliency engineering framework. MTR110237. 2011. URL: http://www.mitre.org/sites/default/files/pdf/ 11_4436.pdf3 (дата звернення: 15.10.2024).

23. *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).

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

25. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 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 (дата звернення: 15.10.2024).

REFERENCES

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

2. *Baranov, O.A.* (2005). Informatsiine pravo Ukrainy: stan, problemy, perspektyvy. "Information law of Ukraine: status, problems, prospects". Kyiv: Publishing House "SoftPres". 316 p. [in Ukrainian].

3. *Bieliakov, K.I.* (2006). Informatsiia v pravi: teoriia i praktyka. "Information in law: theory and practice": monograph. Kyiv: "KVITs" Publishing. 116 p. [in Ukrainian].

DOI (Article): https://doi.org/10.36486/np.2024.3(65).13

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: https://doi.org/10.37028/Lingcure.V5ns3.1545 [in English].

5. *Butuzov, V.M.* (2010). Protydiia kompiuternii zlochynnosti v Ukraini (systemno-strukturnyi analiz). "Counteraction to computer crime in Ukraine (systemic and structural analysis)": monograph. Kyiv: KYT. 408 p. [in Ukrainian].

6. *Butuzov, V.M., Titunina, K.V.* (2007). Suchasni zahrozy: kompiuternyi teroryzm. "Modern threats: computer terrorism. Fight against organized crime and corruption". *Borotba z Orhanizovanoiu Zlochynnistiu i Koruptsiieiu, 17,* 316-324 [in Ukrainian].

7. *Korystin, O.Ye., Veselova, L.Yu.* (2021). Ryzykoriientovanist kiberbezpeky. "Risk-oriented cybersecurity". *Nauka i Pravookhorona, 3,* 16-23 [in Ukrainian].

8. *Havlovskyi, V.D.* (2019). Zakhyst informatsii shliakhom posylennia efektyvnosti protydii kiberatakam. "Information protection by increasing the effectiveness of countering cyberattacks". *Informatsiia i Pravo, 2(30),* 105-110 [in Ukrainian].

9. *Havlovskyi, V.D., Titunina, K.V.* (2008). Deiaki suchasni problemy protydii kompiuterni zlochynnosti ta kompiuternomu teroryzmu. "Some modern problems of countering computer crime and computer terrorism". *Naukovo-praktychnyi Zhurnal Mizhvidomchoho Naukovo-doslidnoho Tsentru z Pytan Orhanizovanoi Zlochynnosti ta Koruptsii, 19,* 247-251 [in Ukrainian].

10. *Taran, O.V., Havlovskyi, V.D.* (2021). Orhanizovana kiberzlochynnist v Ukraini: problemy formuvannia ofitsiinoi statystyky ta yii analizu. "Organized cybercrime in Ukraine: problems of forming official statistics and its analysis". *Informatsiia i Pravo, 4(39),* 193-201 [in Ukrainian].

11. *Hutsaliuk, M.V.* (2019). Suchasni tendentsii orhanizovanoi kiberzlochynnosti. "Modern trends in organized cybercrime". *Informatsiia i Pravo, 1(28),* 118-128 [in Ukrainian].

12. *Hutsaliuk, M.V., Khakhanovskyi, V.H.* (2020). Osoblyvosti vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh. "Peculiarities of using electronic (digital) evidence in criminal proceedings". *Kryminalistychnyi Visnyk, 31(1),* 13–19. DOI: https://doi.org/10.37025/1992-4437/2019-31-1-13 [in Ukrainian].

13. *Dovhan, O.D., Doronin, I.M.* (2017). Eskalatsiia kiberzahroz natsionalnym interesam Ukrainy ta pravovi aspekty kiberzakhystu. "Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber protection": monograph. Kyiv: Puplishing House "ArtEk". 107 p. [in Ukrainian].

14. *Korchenko, O., Kazmirchuk, S. and Akhmetov, B.* (2017). Prykladni systemy otsiniuvannia ryzykiv informatsiinoi bezpeky. "Applied systems for assessing information security risks": monograph. Kyiv: TsP Komprynt. 435 p. [in Ukrainian].

15. *Marushchak, A.I.* (2009). Informatsiini resursy derzhavy: zmist ta problema zakhystu. "State information resources: content and protection problem". *Pravova Informatyka, 1(21),* 65-71 [in Ukrainian].

16. *Khakhanovskyi, V.H., Havlovskyi, V.D.* (2020). Tlumachennia ta klasyfikatsiia kryminalnykh pravoporushen yak kiberzlochyniv. "Interpretation and classification of criminal offenses as cybercrimes". *Informatsiia i Pravo, 2(33),* 99-110 [in Ukrainian].

17. *Pohoretskyi, M.A., Shelomentsev, V.P.* (2009). Kompiuterna systema yak znariaddia vchynennia zlochynu. "Computer system as a tool for committing a crime". *The Journal of V.N.Karazin Kharkiv National University. Series "Law", 872(6),* 117-121 [in Ukrainian].

18. *Shelomentsev, V.P.* (2009). Orhanizovana kiberzlochynnist: do vyznachennia poniattia. "Organized cybercrime: to define the concept. Fight against organized crime and corruption (theory and practice)". *Borotba z Orhanizovanoiu Zlochynnistiu i Koruptsiieiu (Teoriia i Praktyka), 21,* 314-322 [in Ukrainian].

19. *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

DOI (Issue): https://doi.org/10.36486/np.2024.3(65) Issue 3-4(65-66) 2024

network science: applications to infrastructures, climate, social systems, and economics. *European Physical Journal: Special Topics, 214,* 273-293 [in English].

20. *Jansen, W.* (2009). Directions in security metrics research. The National Institute of Standards and Technology (NISTIR), 7564. URL: http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_ metrics-research.pdf (Date of Application: 15.10.2024) [in English].

21. *Bartol, N., Bates, B., Goertzel, K. & Winograd, T.* (2009). Measuring cyber security and information assurance: a state of the art report. URL: https://www.thecsiac.com/sites/default/files/ cybersecurity.pdf (Date of Application: 15.10.2024) [in English].

22. *Bodeau, D. & Graubart, R.* (2011). Cyber resiliency engineering framework. MTR110237. URL: http://www.mitre.org/sites/default/files/pdf/11_4436.pdf3 (Date of Application: 15.10.2024) [in English].

23. *Korystin O.Ye., Korystin O.O.* (2022). Zahrozy u sferi kiberbezpeky v Ukraini. "Threats in the field of cyber security in Ukraine". *Nauka i Pravookhoronna, 1 (55),* 119-126. DOI: https://doi.org/10.36486/np.2022.1(55) [in Ukrainian].

24. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021. Publications Office of the European Union. Luxembourg. 2021 [in English].

25. Dyrektyva Yevropeiskoho Parlamentu i Rady (YeEs) 2016/1148. "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union". URL: https://zakon.rada.gov.ua/ laws/show/984_01316/find?text=%F0%E8%E7%E8%EA (Date of Application: 15.10.2024) [in Ukrainian].

UDC 343.97:336.7

Korystin Oleksandr,
Doctor of Juridical Sciences, Professor,
Honored Worker of Science and Technology of Ukraine, Chief Researcher,
State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0001-9056-5475
Kardashevskyi Yurii,
PhD in Law, Head of Internal Control Department, National
Agency for the Prevention of Corruption, Kyiv, Ukraine,
ORCID ID 0009-0009-8940-6384

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 are not solely driven by the pursuit of financial gain; they are also aimed at acquiring access to confidential information. This can result in substantial financial losses and erode public confidence in the country›s financial system.

DOI (Article): https://doi.org/10.36486/np.2024.3(65).13

One of the key issues we are dealing with is the fact that banking information systems are often vulnerable. This is typically due to outdated technology, failure to keep up with 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 issue of social engineering is also of significance. 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. This research focuses on criminal offences outlined in the Criminal Code of Ukraine, specifically theft, illegal activities involving payment cards, money laundering, and violation of banking secrecy. The most prevalent violations pertain to those delineated in Article 200 of the Criminal Code of Ukraine, which pertains to illicit activities involving payment cards, and Article 209, which addresses money laundering.

According to expert surveys, criminals are primarily motivated by financial gain; however, some crimes have a hybrid warfare component, particularly in the context of cooperation with the russian aggressor. The authors› primary focus is on the activities of organized criminal groups that are actively committing criminal offenses in the banking sector, thereby further complicating the fight against cybercrime. The article highlights the importance of strategic management development in law enforcement for effectively countering these threats, as well as the need to improve state policy in the field of cybersecurity, particularly in developing new methods to protect financial institutions and citizens from cybercriminals.

Keywords: cybercrime, bank card, bank account, payment card data theft, money laundering.

Отримано 24.10.2024