Кримінальне право та кримінологія; кримінально-виконавче право

УДК 343
DOI 10.33244/2617-4154.2(19).2025.145-153

В. О. Борисенко,
здобувач вищої освіти третього рівня (PhD),
Державний податковий університет
e-mail: soksana@ukr.net
ORCID ID 0009-0009-0747-7606

КЛАСИФІКАЦІЯ ТА ТИПОЛОГІЯ КІБЕРЗЛОЧИНІВ У БАНКІВСЬКІЙ СФЕРІ

Розвиток цифрових технологій суттєво змінив банківську сферу, відкривши нові можливості не тільки для банківських операцій, але й для кіберзлочинів. стрімкий процес інформатизації в Україні несе в собі потенційну можливість використання комп'ютерних технологій з вигодою для злочинця.

Метою статті є дослідження наукових підходів до класифікації та типології кіберзлочинів у банківській сфері.

Під час дослідження були застосовані загально- та спеціально-наукові методи дослідження. Структурно-функціональний метод дав змогу виділити кіберзлочини як особливу категорію злочинності й дослідити наявні класифікації та типології кіберзлочинів, а для формування висновків і пропозицій застосовувалися методи аналізу, синтезу, індукції, дедукції, аналогії.

У статті розглянуто підходи науковців до визначення кіберзлочинів і розглянуто їхні існуючі класифікації та типології.

Запропоновано власне бачення на визначення кіберзлочинів, яке сформульовано з урахуванням поглядів науковців. Також акцентується увага на доцільності класифікації кіберзлочинів за рядом критеріїв: залежно від об'єкта посягання; за способами та методами вчинення; за методами втручання в процес передачі даних; залежно від значення інформаційної системи в механізмі реалізації кримінально протиправної діяльності.

Зроблено висновок, що, враховуючи стрімкий розвиток технологій, нових форм та методів вчинення злочинів у кіберпросторі, поширення злочинів у банківській сфері, кіберзлочини є одним з найбільш небезпечних видів кримінальних правопорушень, які становлять загрозу міжнародній та національній безпеці в кіберпросторі й потребують подальшого дослідження.

Ключові слова: *кіберзлочини, кіберзлочинність, шахрайство, фішинг, вішинг, фітинг, скіммінг.*

Постановка проблеми та її актуальність. Забезпечення інформаційної безпеки в Україні є однією з функцій сучасної держави. Розвиток мережі «Інтернет», інформаційних технологій спричинив виникнення нового виду злочинів – кіберзлочинів, а стрімкий процес інформатизації (діджиталізації) в Україні несе в собі потенційну можливість використання комп'ютерних технологій з вигодою для злочинця.

Набувають поширення кіберзлочини, пов'язані з використанням мережі «Інтернет», серед яких і використання віртуальних крамниць, фірм з надання платних послуг щодо вилучення з рахунків і кредитних карток їх власників «електронних» коштів; різних казино, інтернет-аукціони; вимагання під погрозою знищення чи змін інформаційних баз даних; незаконна діяльність у сфері програмного забезпечення, тощо.

Актуальність обраної теми обумовлена тим, що розвиток цифрових технологій суттєво змінив банківську сферу, відкривши нові можливості для банківських операцій, і водночас відкрив поле для виникнення кіберзлочинів.

З упровадженням банківськими установами інновацій, які забезпечують зручність, швидкість обслуговування клієнтам, зростають і ризики вчинення кіберзлочинів, що загрожує не лише фінансовим установам, але й мільйонам їхніх клієнтів. Поширення набувають, зокрема, атаки на банківські системи, які стають дедалі витонченішими і вимагають від установ впровадження більш досконалих механізмів захисту.

Вищенаведене зумовлює потребу в поглибленому вивченні різновидів кіберзлочинів з метою подальшої розробки ефективних засобів боротьби з ними.

Окремі аспекти кіберзлочинів досліджували у своїх працях В. В. Коваленко, О. А. Криклій, О. В. Кузьменко, А. І. Марущак, О. І. Мотлях, Я. В. Неділько, О. С. Омельян, Л. П. Паламарчук, Д. В. Пашнєв, М. В. Салтевський, О. В. Сіренко, В. Г. Тімашов, Н. В. Трусов, В. А. Журавель, Хахановський та інші.

Виклад основного матеріалу. На сьогодні не існує єдиного підходу до визначення кіберзлочину. Так, М. Погорецький вважає, що кіберзлочинами потрібно вважати ті, що вчиняються за допомогою або через комп'ютерні системи чи пов'язані саме з комп'ютерними системами, тобто із сукупністю пристроїв, із яких один чи більше, відповідно до певної програми, виконують автоматичну обробку даних [11, с. 89–96].

На думку В. М. Болгова, кіберзлочини – це сукупність передбачених чинним законодавством кримінально караних суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію [2].

О. В. Сіренко визначає кіберзлочин як «кримінальне правопорушення, що вчиняється за допомогою або через комп'ютерні системи, посягає на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології,

права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію і за яке передбачено кримінальну відповідальність» [13, с. 48].

М. О. Думчиков пропонує під злочинами в сфері комп'ютерної інформації розуміти умисні суспільно небезпечні, протиправні, винні діяння, що посягають та заподіюють шкоду суспільним відносинам, які регламентують порядок зберігання, розповсюдження, використання інформації та їх захист [5].

Якщо ж звернутись до нормативно-правової бази, то поняття «кіберзлочин» було відсутнє в українському законодавстві до моменту ухвалення Закону України «Про основні засади забезпечення кібербезпеки України» 2017 р., в якому п. 9 ст. 1 визначено, що кіберзлочин (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена Законом України «Про основні засади забезпечення кібербезпеки України» та/або яке визнано злочином міжнародними договорами України (п. 8 ст. 1 Закону) [12].

Отже, узагальнюючи вищевикладене, кіберзлочини це – умисні суспільно небезпечні, протиправні, винні діяння, що вчиняються за допомогою або через комп'ютерні системи та заподіюють шкоду суспільним відносинам, які регламентують порядок зберігання, розповсюдження, використання інформації та їх захист і за які передбачена відповідальність законом України про кримінальну відповідальність та/або які визнані злочинами міжнародними договорами України.

Кіберзлочини, як зазначають науковці, «на відміну від традиційних, мають низку характерних особливостей, серед яких слід зазначити такі: – місце вчинення кіберзлочину, на відміну від традиційних, може знаходитись в різних юрисдикціях – правопорушник активізує кібератаку, наприклад, з Інтернет-кафе однієї країни, бот-мережа знаходиться в іншій, а атакована інформаційна система – у третій; – переважна кількість доказів кіберзлочинів існують в електронній формі (так звані «електронні» або «цифрові» докази). Вони, на відміну від традиційних, можуть швидко знищуватися чи модифікуватися. Для їх отримання, зберігання та аналізу необхідне спеціалізоване обладнання; – внаслідок специфічної природи кіберпростору постраждалий не завжди обізнаний про вчинення кіберзлочину тощо» [3, с. 119].

Що саме належить до кіберзлочинів, питання дискусійне. Умовно науковці розділились на основні дві групи: «перша група науковців відносить до кіберзлочинів дії, у яких комп'ютер є об'єктом або засобом посягання. Друга група визначає кіберзлочини як злочини, об'єктом посягання в яких є інформація, що обробляється в електронно-обчислювальній машині (комп'ютері) або в комп'ютерній системі, а засобом вчинення є електронно-обчислювальна машина (комп'ютер), тобто протизаконні дії у сфері автоматичної обробки інформації» [1, с. 7].

Загалом до кіберзлочинів відносять злочини, що вчиняються з використанням електронно-обчислювальних машин (комп'ютерів) та комп'ютерних мереж. Зокрема, це: **фішинг, шахрайство з платіжними картками, атаки на банкомати тощо.**

Важливим є питання класифікації та типології кіберзлочинів загалом і в банківській сфері зокрема, і тут потрібно звернутись до Конвенції Ради Європи про кіберзлочинність [9], яка містить найбільш поширену класифікацію кіберзлочинів.

Відповідно до згаданої Конвенції, кіберзлочини поділяють на чотири групи (пізніше Додатковим протоколом було виділено ще п'яту групу) [4]. До першої групи належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ (ст. 2), нелегальне перехоплення (ст. 3), втручання в дані (ст. 4), втручання в систему (ст. 5), зловживання пристроями (ст. 6). До другої групи входять правопорушення, пов'язані з комп'ютерами: підробка та шахрайство, пов'язані з комп'ютерами (статті 7, 8). До третьої групи належать правопорушення, пов'язані зі змістом: правопорушення, пов'язані з дитячою порнографією (ст. 9). До четвертої групи увійшли правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10) [9], до п'ятої групи належать правопорушення, які стосуються дій расистського та ксенофобного характеру, вчинені через комп'ютерні системи [4].

Погоджуємось з думкою науковців, що «залежно від об'єкта посягання кіберзлочини (комп'ютерні злочини) можна класифікувати за такими видами:

1) злочини, вчинені у кіберпросторі та/або з його використанням, відповідальність за які передбачена різними розділами Кримінального кодексу України (далі – КК України). Такі злочини посягають на різні об'єкти кримінально-правової охорони: основи національної безпеки, громадську безпеку, відносини у сфері охорони права на об'єкти інтелектуальної власності, власність, господарські відносини, права та свободи тощо. Ознакою віднесення цих злочинів до кіберзлочинів є те, що вони вчиняються з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки;

2) злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж, що передбачені Розділом XVI КК України. Ознакою віднесення цих злочинів до комп'ютерних є те, що вони посягають на відносини, які виникають у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [10].

Традиційною темою кіберзлочинності є банківська картка, і основними видами кіберзлочинів у цій сфері є: 1) скіммінг – вид кіберзлочинності, скоєний пристроєм для зчитування інформації з пластикових карток [6].

Розрізняють: – фізичний скіммінг (зловмисники копіюють усю інформацію з магнітної смуги картки (ім'я власника, номер картки, термін закінчення терміну її дії, CVV- та CVC-код), дізнатися про ПІН-код можна за допомогою мінікамери або накладок на клавіатуру, встановлених на банкоматах);

– програмний скіммінг (полягає у встановленні зловмисниками на банкомат певного шкідливого програмного забезпечення, яке буде здійснювати копіювання магнітної стрічки картки, ссв коду та дати дії картки, та подальше надіслання таких даних на сервери зловмисників) [5];

2) шахрайство в системах віддаленого банку – це різновид кіберзлочинності, в результаті якого злочинці можуть відстежувати будь-які банківські операції [14, с. 103].

Фахівці банківської системи та правоохоронних органів відокремлюють такі основні види шахрайства: шахрайство з використанням банкомату; інтернет-шахрайство; шахрайство в термінальній мережі; шахрайство в системах дистанційного обслуговування (ДБО); соціальна інженерія [16].

Також, як зазначають науковці, кіберзлочини класифікують за методами втручання в процес передачі даних: переривання (блокування процесу передачі); перехоплення (незаконний доступ до переданих даних); модифікація (незаконна зміна даних); виробництво (організація фальсифікованого сеансу спілкування) [15].

Залежно від значення інформаційної системи в механізмі реалізації кримінально протиправної діяльності можна виділити: кіберзлочини у власному розумінні, тобто ті, які неможливо вчинити без використання інформаційних (комп'ютерних) систем. Це прояви кримінально протиправної поведінки, які спрямовані проти інформаційних (комп'ютерних) систем або проти об'єктів чи предметів, які існують, зберігаються, передаються, обробляються у них (комп'ютерні програми, інформація тощо); пов'язані з інформаційними (комп'ютерними) системами кримінальні правопорушення, тобто ті прояви кримінально протиправної поведінки, які вчиняються з використанням цих систем, але водночас можуть вчинятися й без них. Ці прояви кримінально протиправної поведінки можуть полягати, зокрема, у тому, що саме кримінально протиправне діяння вчиняється в кіберпросторі з використанням інформаційних технологій або ж інформаційні технології чи кіберпростір використовуються злочинцем на інших етапах реалізації кримінально протиправної діяльності, як наприклад знаряддя чи засіб вчинення діяння [7, с. 32–33].

Що стосується типології кіберзлочинів у банківській сфері, то науковці виділяють такі типи: фішинг як вид інтернет-шахрайства, за допомогою якого злочинцям вдається отримати дані клієнтів банку: викрадення паролів, номерів, даних кредитних карток, банківських рахунків та іншої конфіденційної інформації; вішинг – вид шахрайства за допомогою мобільного телефону. Шахраї телефонують на певний номер, і абонент повідомляє конфіденційні дані на банківських рахунках; фітинг – дублікат сайту як дзеркало реального сайту. Під час онлайн-покупки за допомогою банківської картки клієнт вводить свої дані, і в цей час зловмисники знімають з неї кошти [14, с. 104].

В. О. Тімашов, О. А. Корольова, Д. Г. Юрченко такі типи кіберзлочинів, як: несанкціонований доступ, зловмисна вірусна модифікація, перехоплення інформації та комбіноване невикористання [15].

З огляду на вищевикладене, доцільно виділити такі види кіберзлочинів у банківській сфері:

1) залежно від об'єкта посягання: кримінальні правопорушення у кіберпросторі з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки; кримінальні правопорушення, що посягають на відносини, які виникають у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

2) за способами та методами вчинення: скіммінг (фізичний, програмний) – вид кіберзлочинності, скоєний пристроєм для зчитування інформації з пластикових карток; шахрайство в системах віддаленого банку: а) шахрайство з використанням банкомату; б) інтернет-шахрайство; в) шахрайство в термінальній мережі; г) шахрайство в системах дистанційного обслуговування;

3) за методами втручання в процес передачі даних: переривання (блокування процесу передачі); перехоплення (незаконний доступ до переданих даних); модифікація (незаконна зміна даних); виробництво (організація фальсифікованого сеансу спілкування);

4) залежно від значення інформаційної системи у механізмі реалізації кримінально протиправної діяльності: ті, які неможливо вчинити без використання інформаційних (комп'ютерних) систем; які вчиняються з використанням інформаційних (комп'ютерних) систем, але можуть вчинятися і без них.

До типів кіберзлочинів у банківській сфері потрібно віднести:

1) за формою вчинення: фішинг; вішинг; фітинг;

2) за методом вчинення: технічні злочини, які охоплюють використання шкідливого програмного забезпечення, вірусів, троянських програм або бот-мереж для проникнення в банківські системи; **соціальна інженерія –** злочинці маніпулюють людьми для отримання доступу до важливої інформації (через телефонні дзвінки, підроблені повідомлення або особистий контакт, вдаючи службовців банку або інших довірених осіб);

3) за ступенем організованості кіберзлочинців: **організовані злочини** – кіберзлочинці, об'єднуючись здійснюють масштабні кібератаки на банківські установи; **індивідуальні злочини** – окремі особи використовуючи власні навички здійснюють кібератаки на банки.

Висновки. Враховуючи стрімкий розвиток технологій, нових форм та методів вчинення злочинів у кіберпросторі, поширення злочинів у банківській сфері, можна зробити висновок, що кіберзлочини є одним з найбільш небезпечних видів кримінальних правопорушень, які становлять загрозу міжнародній та національній безпеці в кіберпросторі. Розгляд наукових праць продемонстрував багатогранність питання класифікації та типології кіберзлочинів у банківській сфері та потреба в подальшому дослідженні зазначеної проблематики. І хоча в Україні створено умови для боротьби з кіберзлочинністю, визначено основні цілі, напрями та принципи державної політики, все ще існують питання стосовно кіберзлочинів у банківській сфері, які потребують якомога швидкого вирішення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Амелін О. Визначення кіберзлочинів у національному законодавстві. *Науковий часопис Національної академії прокуратури України*. 2016. № 3. С. 1–10.

2. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : наук.-практ. посіб. / В. М. Болгов, Н. М. Гадіон, О. З. Гладун та ін. К. : Національна академія прокуратури України, 2015. 202 с.

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

4. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003. URL : http://zakon.rada.gov.ua/ laws/show/994_687

5. Думчиков М. О. Кримінальні правопорушення в сфері комп'ютерної інформації: ретроспективний аналіз. *Науковий вісник Міжнародного гуманітарного університету*. Сер.: Юриспруденція. 2022. № 57. С. 86–90.

6. Карткові шахраї обікрали українців за рік на 360 млн. URL : https://news.finance.ua/ua/news/-/465343/kartkovi-shahrayi-obikralyukrayintsiv-za-rik-na-360mln?utm_source=telegram&utm_medium=social&utm_campaign=co_vsk&utm_content=kartk-shahrai_160220

7. Кіберзлочинність та електронні докази : навч. посібник / Головкін Б. М., Денькович О. І., Луцик В. В., Цехан Д. М. ; за ред. канд. юрид. наук, доц. О. Денькович, д-р права, проф. Габріеле Шмельцер [Електрон. вид.]. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL : https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf

8. Конвенція про кіберзлочинність від 23.11.2001. URL : https://zakon.rada.gov.ua/laws/show/994_575/

9. Конвенція про кіберзлочинність від 21.11.2001. URL : http://zakon.rada.gov.ua/laws/show/994_575

10. Кундеус В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. Нові виклики в епоху постмодерну*. Харків, 2020. С. 44–45. URL : https://dspace.univd.edu.ua/server/api/core/bitstreams/6e42bc23-7a3f-41b5-b4cf-9a5a737e8184/content

11. Погорецький М. Кіберзлочини: до визначення поняття. *Вісник прокуратури*. 2012. № 8. С. 89–96.

12. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19

13. Сіренко О. В. Поняття кіберзлочинів та особливості методики їх розслідування. *Кібербезпека в Україні: правові та організаційні питання* : матеріали Всеукр. наук.-практ. конф., м. Одеса. Одеса : ОДУВС, 2017. С. 48–49.

14. Сучасне банківництво: теорія і практика : навч. посібник. Ужгород, 2018. 364 с.

15. Тімашов В. О., Корольова О. А., Юрченко Д. Г. Правові засади забезпечення кібербезпеки у банківській сфері. *Юридичний науковий електронний журнал*. 2021. № 3. С. 226–230. URL : http://lsej.org.ua/3_2021/60.pdf

16. Шахрайство із платіжними картками та способи боротьби з ними / НБУ. URL : https://vk24.ua/news/shakhraystvo-iz-platizhnimi-kartkami-ta-sposobi-borotbi-z-nimi-nbu

REFERENCES

1. Amelin O. Vyznachennia kiberzlochyniv u natsionalnomu zakonodavstvi. *Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy.* 2016. № 3. S. 1–10.

2. Bolhov V. Orhanizatsiino-pravove zabezpechennia protydii kryminalnym pravoporushenniam, shcho vchyniaiutsia z vykorystanniam informatsiinykh tekhnolohii : nauk.-prakt. posib. / V. M. Bolhov, N. M. Hadion, O. Z. Hladun ta in. K. : Natsionalna akademiia prokuratury Ukrainy, 2015. 202 s.

3. Hutsaliuk M. V. Suchasni tendentsii orhanizovanoi kiberzlochynnosti. *Informatsiia i pravo.* 2019. № 1 (28). S. 118–128.

4. Dodatkovyi protokol do Konventsii pro kiberzlochynnist, yakyi stosuietsia kryminalizatsii dii rasystskoho ta ksenofobnoho kharakteru, vchynenykh cherez kompiuterni systemy vid 28.01.2003. URL : http://zakon.rada.gov.ua/ laws/show/994_687

5. Dumchykov M. O. Kryminalni pravoporushennia v sferi kompiuternoi informatsii: retrospektyvnyi analiz. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu.* Ser.: Yurysprudentsiia. 2022. № 57. S. 86–90.

6. Kartkovi shakhrai obikraly ukraintsiv za rik na 360 mln. URL : https://news.finance.ua/ua/news/-/465343/kartkovi-shahrayi-obikralyukrayintsiv-za-rik-na-360mln?utm_source=telegram&utm_medium=social&utm_campaign=co_vsk&utm_content=kartk-shahrai_160220

7. Kiberzlochynnist ta elektronni dokazy : navch. posibnyk / Holovkin B. M., Denkovych O. I., Lutsyk V. V., Tsekhan D. M. ; za red. kand. yuryd. nauk, dots. O. Denkovych, d-r prava, prof. Habriele Shmeltser [Elektron. vyd.]. Lviv : LNU im. Ivana Franka, 2022. 298 s. URL : https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf

8. Konventsiia pro kiberzlochynnist vid 23.11.2001. URL : https://zakon.rada.gov.ua/laws/show/994_575/

9. Konventsiia pro kiberzlochynnist vid 21.11.2001. URL : http://zakon.rada.gov.ua/laws/show/994_575

10. Kundeus V. H. Poniattia ta vydy kiberzlochyniv. *Derzhava i zlochynnist. Novi vyklyky v epokhu postmodernu.* Kharkiv, 2020. S. 44–45. URL : https://dspace.univd.edu.ua/server/api/core/bitstreams/6e42bc23-7a3f-41b5-b4cf-9a5a737e8184/content

11. Pohoretskyi M. Kiberzlochyny: do vyznachennia poniattia. *Visnyk prokuratury.* 2012. № 8. S. 89–96.

12. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy vid 05.10.2017 № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19

13. Sirenko O. V. Poniattia kiberzlochyniv ta osoblyvosti metodyky yikh rozsliduvannia. *Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia* : materialy Vseukr. nauk.-prakt. konf., m. Odesa. Odesa : ODUVS, 2017. S. 48–49.

14. Suchasne bankivnytstvo: teoriia i praktyka : navch. posibnyk. Uzhhorod, 2018. 364 s.

15. Timashov V. O., Korolova O. A., Yurchenko D. H. Pravovi zasady zabezpechennia kiberbezpeky u bankivskii sferi. *Yurydychnyi naukovyi elektronnyi zhurnal.* 2021. № 3. S. 226–230. URL : http://lsej.org.ua/3_2021/60.pdf

16. Shakhraistvo iz platizhnymy kartkamy ta sposoby borotby z nymy / NBU. URL : https://vk24.ua/news/shakhraystvo-iz-platizhnimi-kartkami-ta-sposobi-borotbi-z-nimi-nbu

V. O. Borysenko. CLASSIFICATION AND TYPOLOGY OF CYBERCRIMES IN THE BANKING SECTOR

The development of digital technologies has significantly changed the banking sector, opening up new opportunities not only for banking operations, but also for cybercrimes. The rapid process of informatization in Ukraine carries with it the potential for the use of computer technologies with the benefit of the criminal.

The purpose of the article is to study scientific approaches to the classification and typology of cybercrimes in the banking sector.

During the study, general and special scientific research methods were applied. The structural-functional method allowed us to identify cybercrimes as a special category of crime and to study the existing classifications and typologies of cybercrimes, and the methods of analysis, synthesis, induction, deduction, and analogy were used to form conclusions and proposals.

The article examines the approaches of scientists to the definition of cybercrimes and their varieties. Existing classifications of cybercrimes are considered.

The author proposes his own vision of the definition of cybercrimes, which is formulated taking into account the points of view of scientists. Also, attention is focused on the feasibility of classifying cybercrimes according to a number of criteria: depending on the object of the attack; by means and methods of commission; by methods of interference in the data transmission process; depending on the importance of the information system in the mechanism of implementation of criminally unlawful activities.

It is concluded that taking into account the rapid development of technologies, new forms and methods of committing crimes in cyberspace, the spread of crimes in the banking sector, cybercrimes are one of the most dangerous types of criminal offenses that pose a threat to international and national security in cyberspace and require further research.

Keywords: *cybercrimes, cybercrime, fraud, phishing, vishing, fitting, skimming.*

Стаття надійшла до редколегії 12 березня 2025 року