

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ  
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ  
ВНУТРІШНІХ СПРАВ

**МАЛЮТІН ЕДУАРД ВІКТОРОВИЧ**



УДК 343.98: 343.131

**ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ  
КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ  
ІЗ ВИКОРИСТАННЯМ Е-БАНКІНГУ**

Спеціальність 12.00.09 – кримінальний процес та криміналістика;  
судова експертиза; оперативно-розшукова діяльність

Автореферат  
дисертації на здобуття наукового ступеня  
кандидата юридичних наук

Дніпро – 2024

Дисертацією є рукопис.

Робота виконана у Науково-дослідному інституті публічного права.

**Науковий керівник –**

доктор юридичних наук, професор

**Чаплинський Костянтин Олександрович,**

Дніпровський державний університет внутрішніх справ,

завідувач кафедри криміналістики та домедичної підготовки.

**Офіційні опоненти:**

доктор юридичних наук, професор,

Заслужений юрист України

**Тарасенко Олег Сергійович,**

Національна академія внутрішніх справ,

професор кафедри оперативно-розшукової діяльності;

доктор юридичних наук, професор

**Степанюк Руслан Леонтійович,**

Харківський національний університет внутрішніх справ,

професор кафедри оперативно-розшукової діяльності

та розкриття злочинів факультету № 2.

Захист відбудеться 21 вересня 2024 року о 09-00 годині на засіданні спеціалізованої вченої ради Д 08.727.02 Дніпровського державного університету внутрішніх справ за адресою: 49005, м. Дніпро, просп. Науки, 26.

З дисертацією можна ознайомитись у загальній бібліотеці Дніпровського державного університету внутрішніх справ (м. Дніпро, просп. Науки, 26).

Автореферат розіслано 15 серпня 2024 року.

**Учений секретар  
спеціалізованої вченої ради**



**В.С. Березняк**

## ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність теми.** Процес інтеграції України до європейського співтовариства та безперервні зміни у цифровій галузі, що відбуваються в соціумі, впливають на всі сфери суспільного життя. Під час повномасштабного вторгнення російської федерації на територію України суттєво збільшилася кількість кримінальних правопорушень у кіберпросторі. Це переважно протиправні діяння у сфері е-комерції, використання банківських електронних платежів, е-бізнесу та ін. Зважаючи на збільшення чисельності внутрішньо переміщених осіб, релокацію бізнесу зі східних і південних областей країни у її центральні та західні регіони, а також за кордон, спостерігається зростання кількості кримінальних правопорушень, пов'язаних із використанням е-банкінгу, що вчинюються майже в усіх суспільних сферах – від побутової до загальнодержавної. Дедалі спостерігається суттєве збільшення кількості зламів і пошкоджень різноманітних платіжних систем та втручань у їхню ефективну діяльність. До протиправної діяльності залучаються хакери, фахівці у сфері комп'ютерних технологій та програмування, представники кримінальних угруповань, які діють в економічному секторі, адже така діяльність приносить значні злочинні прибутки.

Так, відповідно до офіційної статистичної звітності Офісу Генерального прокурора у 2019 р. до ЄРДР було внесено 2467 фактів шахрайства, учиненого шляхом незаконних операцій із використанням електронно-обчислювальної техніки, а особам вручено повідомлення про підозру лише у 706 випадках. Щодо інших статей КК України, котрі корелюються із застосуванням е-банкінгу, у цей період була майже подібна ситуація, зокрема: за ст. 200 КК України – 711 фактів зареєстровано, з них 674 повідомлення про підозру; за ст. 222 КК України – 76 фактів зареєстровано, з них 59 повідомлень про підозру; за ст. 231 КК України – 8 фактів зареєстровано, повідомлення про підозру відсутні; за ст. 232 КК України – 5 фактів зареєстровано, повідомлення про підозру відсутні; за ст. 361 КК України – 1183 факти зареєстровано, з них 706 повідомлень про підозру; за ст. 361-1 КК України – 191 факт зареєстровано, з них 152 повідомлення про підозру; за ст. 361-2 КК України – 57 фактів зареєстровано, з них 24 повідомлення про підозру; за ст. 362 КК України – 762 факти зареєстровано, з них 598 повідомлень про підозру; за ст. 363<sup>1</sup> КК України – 4 факти зареєстровано, повідомлення про підозру відсутні. У період 2020–2023 рр. значних коливань у статистичних показниках не спостерігалось. У I півріччі 2024 р.: за ст. 200 КК України – 469 фактів зареєстровано, з них 422 повідомлення про підозру; за ст. 222 КК України – 39 фактів зареєстровано, з них 21 повідомлення про підозру; за ст. 231 КК України та ст. 232 КК України відповідно 0 та 1 факт зареєстровано, повідомлення про підозру відсутні; за ст. 361 КК України – 1214 фактів зареєстровано, з них 793 повідомлення про підозру; за ст. 361-1 КК України – 24 факти зареєстровано, з них 3 повідомлення про підозру; за ст. 361-2 КК України – 116 фактів зареєстровано, з них 69 повідомлень про підозру; за

ст. 362 КК України – 1001 факт зареєстровано, з них 822 повідомлення про підозру; за ст. 363-1 КК України – взагалі відсутня реєстрація фактів. З огляду на наведені показники злочинна діяльність у сфері використання е-банкінгу залишається на достатньо високому рівні, а кількість притягнутих до відповідальності осіб дедалі зменшується.

Зважаючи на швидкоплинність інформаційних процесів, неврегульованість низки проблем стосовно функціонування е-банкінгу, низький рівень контролю з боку відповідних державних контролюючих органів, а також суттєве збільшення злочинних посягань у цій сфері, виникає необхідність розробки сучасної дієвої методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

Крім того, на потребу створення окремої комплексної методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, вказали 92 % опитаних респондентів. З-поміж причин низької якості розслідування зазначених діянь вони вказали такі: неналежне процесуальне керівництво досудовим розслідуванням – 56 %, низький фаховий рівень працівників підрозділів правоохоронних органів, які задіяні у кримінальних провадженнях досліджуваної категорії – 62 %, невчасне проведення слідчих (розшукових) дій, НСРД та інших заходів – 32 %, низький рівень координації взаємодії слідчого з працівниками оперативних підрозділів і кіберполіції – 67 %, небажання потерпілих і свідків співпрацювати з уповноваженими особами – 39 %.

Теоретичне підґрунтя дисертації стосовно різних аспектів розслідування кримінальних правопорушень становлять фундаментальні роботи науковців, а саме: Ю. Аленіна, В. Бахіна, В. Весельського, А. Волобуєва, І. Гори, В. Дарагана, В. Дрозд, М. Єфімова, В. Журавля, А. Іщенка, В. Коновалової, В. Кузьмічова, В. Лукашевича, Є. Лук'янчикова, І. Пирога, М. Погорецького, М. Салтевського, Р. Степанюка, О. Тарасенка, О. Татарова, О. Тіщенко, П. Цимбала, К. Чаплинського, С. Чернявського, Ю. Черноус, В. Шепітька, М. Щербаковського та ін.

Окремі проблеми розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, досліджували такі вчені, як: Г. Бідняк, С. Буяджи, С. Головкін, А. Жилін, В. Коба, І. Коваленко, Н. Козак, Т. Коршикова, С. Кузьменко, О. Курман, О. Мотлях, О. Мусієнко, Т. Охрімчук, Н. Павлова, В. Пазиніч, Д. Птушкін, Д. Ричка, О. Самойленко, С. Самойлов, В. Хахановський, С. Чернявський, С. Чучко та ін.

З-поміж останніх наукових праць, що стосувалися досліджуваної проблематики, варто виокремити наступні. Так, О. Довженко у дисертації «Основи методики розслідування кіберзлочинів» (м. Харків, 2020 р.) розкрив стан наукової розробки проблем розслідування кіберзлочинів, визначив перелік обставин, що підлягають встановленню у кримінальному провадженні, охарактеризував типові слідчі ситуації, що виникають на початковому етапі розслідування, розглянув особливості допиту потерпілих, свідків і підозрюваних. У свою чергу, А. Рейнгольд у дисертації «Основи методики

розслідування шахрайства в інтернет-комерції» (м. Дніпро, 2023 р.) визначив стан наукового дослідження питань розслідування шахрайства в інтернет-комерції, окреслив специфіку початкового етапу розслідування шахрайства, розглянув основні елементи організації й планування розслідування шахрайства та визначив коло обставин, що підлягають встановленню. А вже В. Сисолятин у роботі «Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу» (м. Дніпро, 2024 р.) узагальнив наукові погляди стосовно кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та запропонував їх криміналістичну класифікацію; окреслив окремі елементи криміналістичної характеристики протиправних діянь; здійснив криміналістичний аналіз первісної інформації та сформулював коло обставин, що підлягають встановленню у кримінальному провадженні; конкретизував типові слідчі ситуації, що виникають на початковому і подальшому етапах розслідування; з'ясував особливості використання спеціальних знань.

Відзначаючи теоретичну цінність наведених робіт, слід зауважити, що вчені розробляли лише окремі проблемні питання розслідування кримінальних правопорушень визначеної категорії. Недослідженими залишаються питання застосування тактичних операцій щодо збирання первинних даних про обставини злочинної події та виявлення ознак протиправних діянь, координації й взаємодії слідчих та працівників оперативних підрозділів Національної поліції у кримінальному провадженні, не опрацьовувалися питання профілактичної діяльності уповноважених осіб стосовно усунення причин та умов учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, та ін.

Наведені обставини у своїй сукупності визначили актуальність окресленої проблематики, її теоретичне і практичне значення, а також зумовили вибір напряму дисертаційної роботи.

**Зв'язок роботи з науковими програмами, планами, темами, грантами.** Дисертацію виконано відповідно до положень Стратегії національної безпеки України (Указ Президента України від 14.09.2020 № 392/2020), Стратегії кібербезпеки України (Указ Президента України від 14.05.2021 № 447/2021), Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та плану заходів щодо її реалізації (розпорядження Кабінету Міністрів України від 17.11.2021 № 1467-р), Стратегії кібербезпеки України (Указ Президента України від 14.05.2021 № 447/2021), Стратегії боротьби з організованою злочинністю (розпорядження Кабінету Міністрів України від 16.09.2020 № 1126-р), Національної економічної стратегії на період до 2030 року (постанова Кабінету Міністрів України від 03.03.2021 № 179), Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року (розпорядження Кабінету Міністрів України від 30.03.2023 № 272-р), Порядку електронної інформаційної взаємодії Офісу Генерального прокурора та Міністерства внутрішніх справ України (спільний наказ Офісу Генерального прокурора та МВС України від 22.11.2021 № 371/846), тематики наукових

досліджень і науково-технічних (експериментальних) розробок Міністерства освіти і науки на 2022–2026 роки (наказ МОН України від 03.02.2022 № 109), тематики наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки (наказ МВС України від 11.06.2020 № 454), Основних напрямів наукових досліджень Науково-дослідного інституту публічного права на 2020–2024 рр.

**Мета і завдання дослідження.** *Мета* дисертаційного дослідження полягає у вирішенні конкретного наукового завдання з розробки теоретичних положень та криміналістичних рекомендацій щодо формування методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

Комплексність мети, її багатоплановість обумовили необхідність вирішення окремих завдань:

- визначити сутність та систему криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу;
- охарактеризувати обстановку та систематизувати типові способи й сліди вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу;
- з'ясувати криміналістично вагомі ознаки особи злочинця, визначити та охарактеризувати віктимогенні групи потерпілих;
- конкретизувати особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу;
- розкрити особливості взаємодії слідчих та працівників оперативних підрозділів Національної поліції України у кримінальному провадженні;
- виокремити заходи профілактичної діяльності працівників правоохоронних органів щодо виявлення й усунення причин та умов учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу;
- розкрити тактичні операції щодо збирання первинних даних про обставини злочинної події та виявлення ознак протиправних діянь;
- сформулювати перелік заходів для реалізації тактичної операції «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання».

*Об'єктом дослідження* є кримінальні процесуальні відносини, що формуються під час функціонування правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

Предмет дослідження – *основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу.*

**Методи дослідження.** Відповідно до поставленої мети крізь призму об'єкта і предмета дослідження застосовано низку загальнонаукових і спеціальних методів наукового пізнання. *Функціональний метод* використано для формулювання перспективних напрямів застосування тактичних операцій, а також з'ясування особливостей проведення окремих слідчих (розшукових) дій, НСРД та інших процесуальних дій під час їх реалізації (підрозділи 3.1–3.2). *Системно-структурний метод* було застосовано для формулювання сутності та

системи криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу, а також для систематизації типових способів їх учинення та слідової картини (матеріальних, ідеальних, віртуальних слідів) (розділ 1). Використано *документальний метод* для виявлення тактичних помилок і прорахунків в організаційно-тактичному забезпеченні проведення окремих слідчих (розшукових) дій та НСРД (підрозділи 3.1–3.2). *Соціологічний та статистичний методи* були застосовані для аналізу судово-слідчої практики, узагальнення статистичних даних, матеріалів кримінальних проваджень і опитування респондентів (розділи 1–3). За допомогою *методу синтезу* зроблено загальні висновки за тематикою дисертаційного дослідження (розділи 1–3).

*Емпіричну основу дослідження* складають структурована інформація Єдиного звіту про вчинені кримінальні правопорушення Офісу Генерального прокурора України за 2018–2024 рр., а також результати аналізу кримінальних проваджень за 2017–2024 рр. Зокрема, було опрацьовано матеріали 215 кримінальних проваджень із проблематики дослідження у Вінницькій, Дніпропетровській, Донецькій, Закарпатській, Запорізькій, Івано-Франківській, Київській, Львівській, Миколаївській, Одеській, Полтавській, Сумській, Тернопільській, Харківській, Херсонській, Черкаській та Чернівецькій областях та в м. Київ. Також було проанкетовано 250 слідчих, 286 працівників оперативних підрозділів, 52 представники кіберполіції, 96 працівників органів прокуратури, 67 працівників експертних установ МВС України. Крім того, під час проведення дослідження було застосовано власний досвід роботи у підрозділах Національної поліції України.

**Наукова новизна одержаних результатів** полягає в тому, що дисертаційна робота є першим у вітчизняній науці комплексним монографічним дослідженням теоретичних і практичних основ методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, в якому сформульовано низку наукових положень, висновків і практичних рекомендацій, спрямованих на підвищення ефективності діяльності органів досудового розслідування Національної поліції України, що вирізняються науковою новизною та мають важливе теоретичне і практичне значення, зокрема:

*вперше:*

– запропоновано систему окремої методики розслідування, в яку включено складові з огляду на організаційно-тактичні особливості здійснення кримінальних проваджень, розпочатих за фактом учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, зокрема, додано такі, як: криміналістична характеристика кримінальних правопорушень; розгляд первинної інформації, а також особливості занесення відповідних даних в Єдиний реєстр досудових розслідувань; обставини, котрі варто з'ясувати під час розслідування; типові слідчі ситуації розслідування; початковий етап розслідування (проведення слідчих (розшукових) дій, НСРД та розшукових заходів); подальший етап розслідування (проведення слідчих (розшукових) дій,

НСРД та інших процесуальних заходів); використання спеціальних знань у кримінальному провадженні; тактичні операції; взаємодія підрозділів правоохоронних органів; встановлення причин та умов, що сприяли учиненню протиправного діяння;

– сформовано перелік профілактичних заходів, що можуть проводитись уповноваженими особами правоохоронних органів (слідства, дізнання, кіберполіції) стосовно усунення причин і умов учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, а саме: повідомлення громадян за допомогою засобів масової інформації про юридичну відповідальність (адміністративну, цивільну, кримінальну) за протиправні дії; реалізація профілактичного впливу на громадян шляхом використання окремих процесуальних дій із метою здійснення профілактики; встановлення осіб, схильних до антисуспільної поведінки у сфері використання електронно-обчислювальної техніки, а також їх подальше занесення до обліку в підрозділах кіберполіції; участь працівників кіберполіції у тематичних передачах, круглих столах або ток-шоу; вивчення матеріалів кримінальних проваджень для з'ясування та усунення умов і причин, що сприяли вчиненню протиправних діянь; організація дискусій у ЗМІ (електронних та друкованих) із обговоренням кіберзлочинності та її впливу на суспільство; інформування громадян у соціальних мережах, ЗМІ, месенджерах щодо фактів учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (фішингу, кардингу, спамінгу);

– розроблено систему заходів для реалізації тактичної операції «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання», як-от: допити потерпілих; встановлення та допити свідків; огляд електронно-обчислювальної техніки; зняття інформації з електронних інформаційних систем або її частини; встановлення місцезнаходження радіоелектронного засобу; встановлення особи злочинця та оголошення її у розшук; встановлення місцезнаходження злочинця; затримання злочинця; направлення вимог щодо надання правоохоронними органами, органами державної влади та органами місцевого самоврядування інформації, що має значення для кримінального провадження за фактами вчинення протиправних діянь, пов'язаних із використанням е-банкінгу; обшуки за місцем проживання та в інших місцях перебування злочинця; допит підозрюваного для встановлення ймовірних співучасників кримінального правопорушення; проведення затримання співучасників (членів ОЗГ, які задіяні до злочинної діяльності); обмін інформацією між відповідними підрозділами правоохоронних органів іноземних держав та міждержавних органів (Інтерполу, Європолу) стосовно реагування на кіберзлочини; призначення та проведення судових експертиз;

*удосконалено:*

– теоретичні концепції класифікації типових способів підготовки, безпосереднього вчинення та приховування протиправних діянь, учинених із використанням е-банкінгу;

– характеристику слідової картини кримінальних правопорушень шляхом



надання відомостей стосовно матеріальної (ЕОТ, папілярні візерунки), особистісної (показання потерпілих, свідків, підозрюваних) та віртуальної (пам'ять ЕОТ, кеш-пам'ять серверів інтернет-провайдерів, пам'ять смартфонів, кеш-пам'ять електронного реєстру термінала чи банкомата) інформації;

– систему тактичних завдань, що мають місце у діяльності працівників правоохоронних органів у кримінальних провадженнях досліджуваної категорії, а також комплекс заходів для їх вирішення в межах проведення низки тактичних операцій;

– перелік питань, котрі необхідно з'ясувати під час допиту підозрюваного, як-от: у який спосіб було вчинено протиправні дії (безконтактно – за допомогою мережі Wi-Fi загального користування, домашньої мережі Wi-Fi, контактно – за допомогою заволодіння ЕОТ зі встановленими паролями); які способи використовувалися для входження у застосунок для е-банкінгу (застосування спам-ботів; застосування реквізитів картки, отриманої у користувача або із сайтів фіктивних онлайн-магазинів; застосування вірусних програм); протягом якого терміну були скоєні кримінальні правопорушення та які супутні протиправні діяння було вчинено; чи були вчинені протиправні дії ОГ чи ЗО; якщо так, то які функції кожного з їх учасників та яка система розподілу грошових коштів між ними; які засоби застосовувалися під час вчинення протиправних дій (технічні – ЕОТ, модеми, смартфони, маршрутизатори; програмні – web-браузери, VPN); якою була загальна сума грошових коштів (валюта, криптовалюта) на момент закінчення вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу;

– систему тактичних операцій щодо збирання первинних даних про обставини події та виявлення ознак досліджуваних протиправних діянь, а саме: «Встановлення характеру події кримінального правопорушення», «З'ясування місця та часу вчинення протиправного діяння», «Встановлення способу вчинення протиправного діяння (фішинг, застосування шпигунських програм, спам-ботів)», «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання», «З'ясування особи потерпілого та її віктимної поведінки, а також перевірка їхніх зв'язків»;

*дістали подальшого розвитку:*

– теоретичні домінанти з приводу загальних кримінально-процесуальних та криміналістичних категорій (як-от: методика розслідування, криміналістична характеристика, обставини, що підлягають доказуванню, типові слідчі ситуації, взаємодія, профілактична діяльність, тактичні операції);

– структура криміналістичної характеристики досліджуваних протиправних діянь, у якій виокремлено такі елементи, як: спосіб та обстановка кримінального правопорушення, слідова картина, особа злочинця, особа потерпілого;

– система відомостей стосовно обстановки вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, крізь призму просторових, часових та соціальних чинників;

– пропозиції стосовно внесення норми в чинний КПК України, в якій буде

вказано обов'язок працівників правоохоронних органів (слідчих, дізнавачів, детективів, прокурорів) забезпечувати усунення причин та умов, що сприяли вчиненню протиправних діянь;

– організаційно-тактичні особливості взаємодії підрозділів Національної поліції України (кіберполіції, слідства), а також форми взаємодії, зокрема: здійснення доручень уповноваженої особи під час проведення слідчих (розшукових) дій, НСРД та інших заходів, обмін інформацією, надання уповноваженій особі відомостей, зібраних у процесі оперативно-розшукової діяльності, для вирішення питання стосовно внесення інформації до ЄРДР, спільне планування розшукових заходів, здійснення оперативним підрозділом доручень уповноваженої особи стосовно перевірки відомостей, що мають значення для встановлення наявності чи відсутності підстав для внесення відомостей до ЄРДР за оперативними матеріалами;

– формулювання профілактики протиправних діянь як спеціального різновиду правоохоронної діяльності, що складається із сукупності конкретних дій та заходів, котрі реалізують працівники правоохоронних органів (слідчі, дізнавачі, детективи, прокурори), що має на меті усунення причин та умов скоєння окремих категорій кримінальних правопорушень.

**Практичне значення одержаних результатів** полягає в тому, що викладені й аргументовані в дисертації теоретичні положення, висновки та практичні рекомендації впроваджені та використовуються у:

– *законотворчій діяльності* – для удосконалення законодавства у сфері попередження кримінальних правопорушень, пов'язаних із використанням е-банкінгу, викладено низку рекомендацій стосовно внесення змін і доповнень до діючого Кримінального процесуального кодексу України;

– *науковій діяльності* – для удосконалення методики розслідування окремих видів кримінальних правопорушень проти власності (акти впровадження Національної академії внутрішніх справ від 26.02.2024, Харківського національного університету внутрішніх справ від 29.02.2024, Дніпропетровського державного університету внутрішніх справ від 11.03.2024);

– *освітньому процесі* – при викладанні навчальних дисциплін «Організація розслідування кримінальних правопорушень», «Криміналістика», «Кримінальний процес», «Оперативно-розшукова діяльність», «Криміналістичні засоби та методи розслідування кримінальних правопорушень». а також при підготовці підручників і навчальних посібників (акти впровадження Національної академії внутрішніх справ від 27.02.2024, Інституту права та суспільних відносин Відкритого міжнародного Університету розвитку людини «Україна» від 13.03.2024);

– *правозастосовній діяльності* – для вдосконалення діяльності органів досудового розслідування, оперативних та експертних підрозділів Національної поліції України (акти впровадження Управління стратегічних розслідувань в Дніпропетровській області ДСР Національної поліції України від 21.09.2023).

**Апробація результатів дисертації.** Основні теоретичні положення й висновки дисертації оприлюднено на міжнародних науково-практичних

конференціях: «Виклики сучасності та наукові підходи до їх вирішення» (м. Київ, 2020 р.), «Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення» (м. Київ, 2021 р.), «Взаємодія публічного та приватного права: сучасні проблеми та виклики» (м. Київ, 2022 р.), «Інноваційні підходи до реформування сучасного законодавства» (м. Київ, 2023 р.).

**Публікації.** Основні положення та результати дисертації відображено у десяти наукових публікаціях, з яких п'ять статей – у виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук, одна – у закордонному юридичному виданні, чотири – у збірниках тез наукових доповідей, оприлюднених на міжнародних науково-практичних конференціях.

**Структура та обсяг дисертації.** Дисертація складається з основної частини (вступу, трьох розділів, що містять дев'ять підрозділів, висновків), списку використаних джерел і додатків. Загальний обсяг дисертації становить 239 сторінок, з яких 159 сторінок – основного тексту. Список використаних джерел налічує 221 найменування і займає 25 сторінок, 4 додатки викладено на 33-х сторінках.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

У **Вступі** аргументовано актуальність теми дослідження, розкрито рівень вивчення проблематики, зв'язок роботи з науковими програмами, планами та темами, визначено мету і завдання, сформульовано об'єкт і предмет дослідження, охарактеризовано методи й емпіричну основу роботи, окреслено наукову новизну та практичне значення отриманих результатів, наведено дані про наявні публікації та апробацію окремих положень дисертації, визначено структуру й обсяг роботи.

**Розділ 1 «Теоретичні засади криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу»** складається з чотирьох підрозділів, що характеризують стан наукової розробки визначеної проблематики, поняття, сутність та структуру криміналістичної характеристики протиправного діяння, а також її складові елементи.

У *підрозділі 1.1 «Сутність та система криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу»* на основі наукових розробок учених (як-от: В.Б. Коба, І.О. Коваленко, Р.Л. Степанюк, С.С. Чернявський) здійснено криміналістичний аналіз протиправних діянь у сфері використання банківських електронних платежів.

Криміналістична характеристика є складовою методики розслідування кримінальних правопорушень та має важливе значення для ефективного проведення слідчих (розшукових) дій, НСРД та інших процесуальних заходів.

На основі аналізу праць науковців (як-от: А.Ф. Волобуєв, А.В. Іщенко, О.В. Пчеліна, М.В. Салтевський, В.В. Тіщенко, В.Ю. Шепітько) запропоновано систему окремої методики розслідування. Зокрема, з огляду на організаційно-тактичні особливості реалізації кримінальних проваджень, розпочатих за

фактом учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, до неї включено такі складові: тактичні операції, взаємодію підрозділів правоохоронних органів, встановлення причин та умов, що сприяли вчиненню протиправного діяння.

Охарактеризовано наукові підходи стосовно сутності окремих наукових категорій, що характеризують правовідносини у сфері використання банківських електронних платежів, зокрема: «електронна торгівля», «е-банкінг», «цифрова торгівля», «е-бізнес», «е-комерція» тощо, які відрізняються і мають різний зміст та наповнення.

Криміналістичну характеристику сформульовано як систему взаємопов'язаних відомостей про криміналістично значущі ознаки кримінального правопорушення, що поєднані відповідними кореляційними зв'язками та допомагають у розслідуванні завдяки побудові версій у результаті проведення окремих процесуальних дій та розшукових заходів.

Вирізнено складові криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як-от: спосіб і обстановка учинення кримінального правопорушення, слідова картина, особа злочинця, особа потерпілого. Доведено, що наведені елементи повинні бути максимально оптимізовані й спрямовані на вирішення практичних завдань кримінального провадження.

У підрозділі 1.2 «Спосіб учинення кримінального правопорушення як основний елемент криміналістичної характеристики» акцентується увага на тому, що з розвитком електронно-обчислювальної техніки та мережі Інтернет видозмінюються протиправні дії у сфері е-банкінгу, а правопорушники дедалі модернізують і ускладнюють способи їх підготовки, вчинення та приховування.

На основі вивчення матеріалів кримінальних проваджень та праць учених-криміналістів (як-от: О.В. Курман, Н.В. Павлова, О.А. Самойленко, С.В. Самойлов) з'ясовано, що повноструктурний склад способу вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, мав місце у 100 % діянь, адже майже в усіх випадках наявними є елементи підготовки та приховування кримінально караного діяння.

Систематизовано підготовчі дії, як-от: 1) знаходження необхідної електронно-обчислювальної техніки (ноутбук, комп'ютер, планшет) з відповідним програмним забезпеченням; 2) виготовлення шпигунських технічних або програмних засобів для протиправного використання під час здійснення операцій е-банкінгу; 3) збут чи розповсюдження без необхідного дозволу у мережі Інтернет відомостей, що мають значення під час здійснення операцій е-банкінгу; 4) створення необхідної обстановки для реалізації протиправних дій та ін.

Охарактеризовано типові способи вчинення кримінальних правопорушень.

Зосереджено увагу на способах приховування протиправних діянь, таких як: знищення технічних пристроїв (устаткування), що застосовувалися для скоєння протиправних дій – 72 %; надання завідомо неправдивих показань або

неправдивого алібі під час здійснення процесуальних дій – 45 %; відмова від надання показів – 58 %; маскування шпигунського програмного або технічного забезпечення під їхні законні аналоги – 46 %; застосування зміни ідентифікатора місця знаходження обладнання, за допомогою якого скоєні протиправні дії при застосуванні е-банкінгу – 78 %.

Наголошено на чинниках, що впливають на вибір способів протиправних дій, пов'язаних із використанням е-банкінгу, як-от: умови запровадженого воєнного стану; загальна обстановка, що склалася у державі; ситуація у конкретному регіоні (області), особистісні якості потерпілої сторони, наявність певних злочинних умінь і навичок у правопорушника та ін.

У підрозділі 1.3 «Обстановка та слідова картина кримінальних правопорушень, пов'язаних із використанням е-банкінгу» на основі узагальнення наукових розробок учених (О.Ю. Довженка, О.І. Мотляха, В.В. Сисолятіна, С.В. Чучка) охарактеризовано об'єктивні умови, в яких вчинюються кримінальні правопорушення, пов'язані з використанням е-банкінгу. З'ясовано, що обстановка є найбільш дискусійною складовою криміналістичної характеристики кримінальних правопорушень, оскільки, по-перше, майже весь процес протиправної діяльності відбувається у віртуальному просторі; по-друге, вчинення протиправних дій може відбуватися як у різних регіонах держави, так і за її межами. Доведено, що 74 % кримінальних правопорушень, пов'язаних із використанням е-банкінгу, не мають конкретно визначеного місця події.

Сформульовано авторське визначення обстановки вчинення протиправних діянь як комплексу об'єктивних і суб'єктивних чинників матеріального світу, а також просторово-часових ознак місця та часу, що впливають на підготовку, вчинення та приховування протиправного діяння.

Визначено та охарактеризовано місця учинення злочинних дій, пов'язаних із використанням е-банкінгу: місця розміщення ЕОТ, що була застосована для вчинення протиправних дій (смартфон, комп'ютер, ноутбук, планшет) – 74 %; місця розташування банкоматів, банків, а також інших підприємств фінансової сфери – 16 %; місце розташування потерпілої особи, на яку були спрямовані протиправні дії – 9 %.

Розглянуто слідову картину та виокремлено кореляційні зв'язки між способами та слідами кримінальних правопорушень, пов'язаних із використанням е-банкінгу, а також іншими елементами криміналістичної характеристики.

Більшість протиправних дій відображаються у віртуальних, цифрових або комп'ютерних слідах. Вказані електронні сліди здебільшого вилучаються з таких місць: профілів соціальних мереж та онлайн-магазинів, кеш-пам'яті акаунтів і веббраузерів, флеш-носіїв, месенджерів («Телеграм», «Фейсбук», «Інстаграм», «Твіттер») для криптовалютних листувань, пам'яті та кеш-пам'яті ЕОТ, бази інтернет-провайдерів. У випадках безпосередньої зустрічі зі злочинцем чи спілкування з ним у форматі відеоконференції потерпілий може вказати відомості про його зовнішність.

Виокремлено вузлові ділянки, де можуть бути зосереджені сліди злочинного діяння.

У підрозділі 1.4 «Характеристика особи правопорушника та потерпілого» встановлено криміналістично значущі типологічні ознаки особи злочинця, а також особливості віктимогенної поведінки особи потерпілого.

З'ясовано перелік ознак і властивостей, що характеризують особу злочинця, як-от: фізичні, соціально-демографічні, інтелектуальні та моральні. Встановлено та узагальнено криміналістично значущі типологічні ознаки особи злочинця. Визначено, що досліджувані протиправні діяння переважно скоюють чоловіки (81 %). Стосовно вікових особливостей встановлено, що у 9 % випадків кримінальні правопорушення здійснюються особами віком від 16 до 20 років, у 34 % випадків – 20–30 років, у 31 % випадків – 30–40 років, у 20 % випадків – 40–50 років, у 6 % випадків – 50 років і старше. Загалом, більшість злочинців мають базову вищу (38 %) і повну вищу (42 %) освіту. Базову загальну середню освіту мають 3 % злочинців, повну загальну середню освіту – 5 %, професійно-технічну освіту – 12 %. Якщо злочинна діяльність здійснюється у складі ОЗГ, то повну загальну середню освіту мають переважно особи, які виконували другорядні ролі.

У переважній більшості випадків злочинці не є місцевими жителями (81 %).

Наведені відомості дозволяють слідчому скласти найбільш вірогідний «портрет» особи злочинця, що дозволяє: а) вчасно висувати слідчі версії щодо злочинної події; б) окреслити чи звузити коло підозрюваних осіб; в) організувати затримання злочинців «за гарячими слідами»; г) вилучити знаряддя злочину (смартфони, комп'ютери, ноутбуки, планшети, флеш-носії); д) спрогнозувати тактику поведінки злочинця під час проведення СРД та інших процесуальних заходів; е) вирішити низку інших завдань кримінального провадження.

Сформовано типовий «портрет» особи злочинця, який відіграє важливу розшукову роль під час реалізації НСРД та пошукових заходів.

Встановлено, що властивою характеристикою злочинця є особливий вид ознак – інтелектуальні. Адже вказані особи (зокрема спеціалісти з комп'ютерного програмування, фахівці з використання ЕОТ, хакери, фішери, фрікери, спамери, кіберсквотери) повинні володіти достатнім рівнем інтелекту для реалізації своїх професійних функцій.

Надано характеристику особі потерпілого. Вирізнено віктимогенні групи осіб, стосовно яких було вчинено протиправні діяння, зокрема: а) фізичні особи, які здійснювали купівлю-продаж товарів і послуг на онлайн-платформах та інтернет-аукціонах із використанням е-банкінгу; б) працівники фінансових установ, підприємств та організацій різних форм власності; в) їхні клієнти; г) родичі клієнтів; д) юридичні особи – при здійсненні матеріально-технічного постачання та інших заходів у випадках використання інтернет-банкінгу.

Зосереджено увагу на кореляційних зв'язках особи злочинця з потерпілим.

**Розділ 2 «Організація розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу»** налічує три підрозділи, що характеризують особливості початкового етапу розслідування правопорушення, типові слідчі ситуації, а також форми взаємодії окремих підрозділів поліції і напрями реалізації профілактичних заходів у досліджуваній категорії кримінальних проваджень.

У підрозділі 2.1 *«Особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу»* розглянуто приводи та підстави для відкриття кримінального провадження, виокремлено джерела, які надають змогу отримати офіційні відомості, що підтверджують або спростовують інформацію про факт учинення протиправних дій у кіберпросторі.

Визначено, що початковий етап розслідування характеризується такими етапами, як: отримання повідомлення про вчинене правопорушення, аналіз початкової інформації та внесення відомостей до ЄРДР у разі її підтвердження.

Наведений алгоритм дій зумовлює стислі строки реалізації первинних заходів для встановлення особи злочинця, збирання доказової бази та формування кола обставин, що підлягають встановленню. Важливого значення набуває невідкладність проведення огляду місця події.

Наголошено на труднощах, котрі виникають на початковому етапі розслідування, що зумовлено відсутністю злочинця на місці події.

На основі аналізу матеріалів кримінальних проваджень з'ясовано, що підставою для внесення даних до Єдиного реєстру досудових розслідувань за фактом учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, стали початкові дані, що надійшли до правоохоронних органів із таких джерел: а) заяви, листи й повідомлення, що надійшли від потерпілих – 79 %; б) заяви, листи й повідомлення від громадян, які отримали інформацію про вчинене кримінальне правопорушення або були свідками його скоєння – 8 %; в) повідомлення працівників установ, підприємств та організацій – 3 %; г) матеріали досудового розслідування, виділені з інших кримінальних проваджень – 4%; д) матеріали, одержані в ході проведення НСРД та розшукових заходів – 7 %.

Надано рекомендації щодо оцінки первинної інформації, яка надходить до правоохоронних органів.

Вирізняють типові слідчі ситуації, що формуються на початковому етапі розслідування протиправного діяння, а також визначено відповідні тактичні завдання, які необхідно вирішити у кожній з них.

Вирізняють тактичні помилки, що їх припускаються слідчі, які розпочали розслідування: прорахунки у діагностуванні злочинної події та визначенні напрямів розслідування – 84 %, порушення процесуального порядку проведення СРД – 62 %, проведення невідкладних слідчих (розшукових) дій без участі спеціаліста – 57 %, ігнорування встановлення низки важливих обставин – 37 %, «поверхневий» характер невідкладних слідчих (розшукових) дій (огляд, обшук) – 29 % та ін.

У підрозділі 2.2 «Взаємодія слідчих та працівників оперативних підрозділів Національної поліції України у кримінальному провадженні» на основі наукових розробок дослідників (як-от: М.А. Погорецький, К.О. Чаплинський, Ю.М. Черноус, О.О. Юхно) з'ясовано, що правильно спланована й організована взаємодія різних підрозділів Національної поліції України забезпечить отримання достатньої доказової інформації для найбільш ефективного проведення процесуальних дій та розшукових заходів.

Взаємодію сформульовано як спільну й взаємообумовлену діяльність окремих підрозділів Національної поліції України, котру визначено нормативно-правовою базою та погоджено за місцем, часом і єдиною метою функціонування окремих підрозділів, що виявляється в оптимальному проведенні спільних організаційно-тактичних заходів для запобігання та розслідування протиправних посягань.

Така діяльність здійснюється під єдиним керівництвом, що зводиться до проведення усіх слідчих (розшукових) дій, НСРД та розшукових заходів у чіткій співпраці та координації з метою найбільш швидкого й ефективного досягнення та вирішення завдань конкретного кримінального провадження.

З'ясовано особливості взаємодії уповноважених осіб (слідчих, дізнавачів, прокурорів, детективів) із іншими працівниками правоохоронних органів, а також різних установ, підприємств та організацій, громадськістю тощо.

Особливу увагу приділено найбільш розповсюдженим формам взаємодії підрозділів Національної поліції України, особливо з підрозділами Департаменту кіберполіції, – організаційній та процесуальній.

Наголошено на важливості використання обміну інформацією як однієї з найбільш ефективних форм взаємодії, особливо в умовах запровадженого воєнного стану.

Така інформація може стосуватися наступних обставин: а) ознак злочинного діяння, пов'язаного з використанням е-банкінгу (яке вчинене або знаходиться на етапі підготовки); б) структури ОГ та ЗО, що здійснюють тривалу злочинну діяльність в економічній сфері; в) характерних ознак злочинців (хакерів, спамерів, фішерів, фрікерів, кіберсквотерів, лідерів ОЗГ та їхніх членів), які здійснюють протиправну діяльність).

У підрозділі 2.3 «Профілактична діяльність уповноважених осіб у кримінальних провадженнях за фактами вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу» наголошено, що ефективна протидія злочинним проявам у сфері використання банківських електронних платежів вимагає від правоохоронних органів не тільки збирання доказової інформації, але й забезпечення певної профілактичної функції.

Доведено, що одним із основних напрямів організації розслідування кримінальних правопорушень є вжиття ефективних заходів щодо запобігання їм.

Окреслено основні напрями профілактичної діяльності працівників правоохоронних органів щодо виявлення й усунення причин та умов учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, а також відповідні заходи, що спрямовані на своєчасне їх попередження та усунення.



Профілактику протиправних діянь визначено як спеціальний різновид правоохоронної діяльності, що складається з конкретної сукупності певних дій та заходів, котрі реалізують працівники правоохоронних органів (слідчі, дізнавачі, детективи, прокурори), та має метою усунення причин і умов скоєння окремих категорій кримінальних правопорушень.

Вирізняють причини та умови, що впливають на вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як-от: 1) недосконалість діючих нормативно-правових актів; 2) наявність нормативно-правових колізій стосовно оптимальної реалізації е-банкінгу; 3) прогалини, що наявні у кримінальному законодавстві; 4) суперечливість судової практики стосовно кримінальних правопорушень, учинених у кіберпросторі; 5) транснаціональний характер протиправних дій; 6) хакерські атаки на сайти, де здійснюються операції е-банкінгу; 7) допомога протиправним діям із боку працівників банків, інтернет-провайдерів, операторів мобільного зв'язку.

Запропоновано заходи профілактики, що можуть здійснюватися уповноваженими особами у кримінальних провадженнях для попередження кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

Наведено деякі факти стосовно аналізу технічних та програмних можливостей ЕОТ, а також специфіки діяльності мережі Інтернет. Зокрема встановлено, що вказане може свідчити як про злочинні дії, так і про попередження їхніх проявів. Опрацьовано модель прояву властивостей кіберзагроз у транзакціях користувачів е-банкінгу.

Підтримується позиція щодо внесення в чинний Кримінальний процесуальний кодекс України норми, в якій буде зазначено про обов'язок працівників правоохоронних органів (слідчих, дізнавачів, детективів, прокурорів) забезпечувати усунення причин та умов, що сприяли вчиненню протиправних діянь. Оскільки вказаний обов'язок забезпечить постійну реалізацію відповідних профілактичних заходів.

**Розділ 3 «Комплекси тактичних операцій при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу»** складається з двох підрозділів, у яких охарактеризовано можливості оптимізації процесу реалізації кримінальних проваджень і висвітлено питання організації та проведення тактичних операцій під час розслідування досліджуваних кримінальних правопорушень.

У підрозділі 3.1 *«Тактичні операції щодо збирання первинної інформації про обставини події та виявлення ознак кримінального правопорушення»* на основі аналізу праць низки науковців (як-от: А.Е. Жилін, С.С. Кузьменко, О.Л. Мусієнко, Н.В. Павлова, А.В. Рейнгольд) запропоновано підхід до розгляду методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, крізь призму проведення комплексів тактичних операцій.

Тактична операція являє собою комплекс процесуальних дій та заходів, котрі спрямовані на розв'язання певного тактичного завдання, що відіграє важливу роль під час розслідування кримінальних правопорушень.

Виокремлено завдання, що їх потрібно вирішувати для здійснення

тактичних операцій стосовно збирання первинної інформації про обставини події та виявлення ознак кримінального правопорушення, як-от: обставини, що передували вчиненню протиправних дій; способи вчинення протиправних дій (фішинг, застосування шпигунських програм, спам-ботів); електронно-обчислювальна техніка, що використовувалася для здійснення протиправних дій; час і тривалість злочинних дій; учасники, їхня кількість і роль кожного в учиненні протиправних дій; загальна кількість потерпілих та їх характеристика.

Надано перелік тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

Запропоновано низку питань, котрі необхідно з'ясувати під час допиту підозрюваного, як-от: у який спосіб було вчинено протиправні дії; які способи використовувалися для входження у застосунок для е-банкінгу; протягом якого часу були скоєні кримінальні правопорушення та які супутні протиправні діяння було вчинено; чи були вчинені протиправні дії у складі ОГ чи ЗО; якщо так, то які функції кожного з їх учасників та яка система розподілу грошових коштів між ними; які засоби застосовувалися під час учинення протиправних дій; якою була загальна сума грошових коштів на момент закінчення вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, та ін.

Вказано на найбільш ефективні тактичні прийоми допиту підозрюваного. Наголошено на їх обов'язковому використанні під час вирішення конфліктних ситуацій допиту.

У підрозділі 3.2 *«Тактичні операції, спрямовані на встановлення та викриття осіб, які належать до події кримінального правопорушення, їх розшук та затримання»* охарактеризовано особливості реалізації комплексу слідчих (розшукових) дій, НСРД, процесуальних і розшукових заходів та інших дій, направлених на реалізацію визначеної тактичної операції.

Наголошено, що тактичні операції спрямовані на встановлення й затримання злочинців, збирання доказів, що доводять їхню причетність до протиправних дій та свідчать про характер злочинної діяльності, а також на з'ясування причетності до цього інших осіб.

Значну увагу приділено тактиці допиту потерпілих і свідків, який є першочерговою СРД у комплексі заходів для оптимальної реалізації визначеної тактичної операції.

З'ясовано основні завдання допиту, зокрема: а) одержання відомостей для виявлення акаунта злочинця; б) встановлення особливостей зв'язку потерпілого з правопорушником (особисте спілкування, соціальні мережі, телефонна розмова чи листування); в) з'ясування контактної інформації про злочинця (номер телефону, е-гаманця, карткового рахунку, інстаграм-сторінки чи його електронної адреси тощо).

Під час допиту потерпілого доцільно пред'являти таку доказову інформацію: а) скріншоти листування зі злочинцем; б) скріншоти сторінок або облікового запису шахрая у месенджері; в) скріншоти документів, що підтверджують сплату грошових коштів.

Визначено особливості тактики огляду. Виокремлено вузлові ділянки, на яких розташовані сліди протиправних дій, як-от: 1) місце розташування ЕОТ, що була застосована під час учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу; 2) розташування терміналів, відділення банку, банкоматів тощо; 3) локації програмно-технічних засобів, на які було спрямовано протиправні дії.

Наголошено на тактиці огляду віртуальної інформації, що знаходиться у відкритому доступі у мережі Інтернет чи перебуває на матеріальних носіях даних або відповідних сервісах зберігання вказаних даних. Зокрема, при огляді ЕОТ (комп'ютера, смартфона, планшета) об'єктом є як сама техніка, так і носії даних (кеш-пам'ять, програми, системні дані, cookies браузерів тощо).

Акцентовано увагу на обов'язковій реалізації НСРД – зняття інформації з електронних інформаційних систем або її частини та встановлення місцезнаходження радіоелектронного засобу. Проведення зазначених заходів зумовить оптимальне отримання орієнтуючої інформації для подальшого здійснення необхідних процесуальних дій.

Визначено, що тимчасовий доступ до речей і документів для подальшого вилучення майна та огляд речей (ЕОТ, планшетів, смартфонів) дозволить вирішувати такі завдання: 1) з'ясування списку задіяної ЕОТ у кримінальних правопорушеннях, пов'язаних із використанням е-банкінгу; 2) визначення необхідного програмного забезпечення для неї; 3) розгляд платіжних процесів для знаходження латентних замаскованих платежів; 4) вирішення питання доступу до акаунтів (особистих, банківських), що були створені для здійснення е-банкінгу.

Окреслено особливості призначення і проведення судових експертиз при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу (як-от: судова комп'ютерно-технічна експертиза, програмно-комп'ютерна та інформаційно-комп'ютерна експертизи).

## **ВИСНОВКИ**

У дисертації надано теоретичне узагальнення і сучасне опрацювання наукового завдання, що виявляється у розробленні теоретико-прикладних основ методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, та визначення науково обґрунтованих практичних рекомендацій та пропозицій стосовно розвитку цих основ та покращення з огляду на практику зарубіжних країн. У результаті дослідження вироблено низку теоретичних положень, висновків та практичних рекомендацій, першорядними з яких виокремити такі:

1. Здійснено криміналістичний аналіз проведення електронних операцій у сфері використання банківських електронних платежів. Охарактеризовано фактори, що впливають на вчинення протиправних дій. Динаміка звернень до правоохоронних органів за фактами вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, дедалі зростає та набуває все більш прихованого та організованого характеру. Дієві заходи із запобігання злочинним проявам не відповідають сучасним загрозам.

Визначено сучасні наукові підходи до розуміння сутності та системи криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

Запропоновано систему окремої методики розслідування, до якої включено складові з огляду на організаційно-тактичні особливості реалізації кримінальних проваджень, розпочатих за фактом учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як-от: криміналістична характеристика; розгляд первинної інформації, а також особливості занесення відповідних даних до Єдиного реєстру досудових розслідувань; обставини, котрі варто з'ясувати під час розслідування; типові слідчі ситуації та інші.

Окреслено структуру криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу, елементами якої є: спосіб та обстановка учинення кримінального правопорушення, слідова картина, особа злочинця, особа потерпілого.

Доведено, що наведені складові мають сталі кореляційні зв'язки та важливе значення для початкового етапу розслідування з огляду на можливість висунення слідчих версій та проведення невідкладних слідчих (розшукових) дій та НСРД.

2. Охарактеризовано обстановку та систематизовано типові способи й сліди вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

З'ясовано, що способи злочинної діяльності мають широкі межі та виявляються у системі взаємопов'язаних дій із підготовки, безпосереднього вчинення й приховування протиправних дій, що пов'язані між собою єдиними мотивом і метою. Систематизовано підготовчі дії, а також зосереджено увагу на способах приховування досліджуваної категорії протиправних діянь.

Виявлено й охарактеризовано типові способи вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, зокрема: 1) протиправні дії при застосовуванні е-банкінгу; 2) протиправні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; 3) протиправні дії з відомостями, що знаходяться у пам'яті електронно-обчислювальної техніки; 4) поширення шпигунських програмних чи технічних засобів, а також їх збут із застосовуванням мережі Інтернет.

Обстановка вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, характеризується умовами часу та місця, що здебільшого не мають чітких територіальних і часових меж. Визначено найбільш розповсюджені місця вчинення злочинних дій. До обстановки віднесено такі складові: 1) час, протягом якого здійснювалися злочинні дії; 2) час, коли настали наслідки від протиправних дій; 3) місце реалізації злочинних дій (віртуальне середовище, в якому вчиняються дії, і місця, де знаходяться точки доступу, – IP-адреси).

Слідова картина кримінальних правопорушень, пов'язаних із використанням е-банкінгу, охоплює 3 групи слідів: 1) матеріальні сліди, що містяться на різноманітних матеріальних носіях інформації (квитанції, банківські картки, сім-картки, паперові копії даних з ЕОТ, відбитки папілярних

ліній на ЕОТ, клавіатурі банкомата); 2) ідеальні сліди, що становлять відомості у пам'яті потерпілих, підозрюваних та осіб, які були свідками незаконних операцій із використанням е-банкінгу; 3) віртуальні сліди (пам'ять ЕОТ, кеш-пам'ять серверів інтернет-провайдерів, пам'ять смартфонів, кеш-пам'ять електронного реєстру терміналу чи банкомата тощо).

3. З'ясовано криміналістично вагомні ознаки особи злочинця, визначено та охарактеризовано віктимогенні групи потерпілих.

Сформовано ймовірний «портрет» особи злочинця. З'ясовано, що особам, які вчиняють кримінальні правопорушення, пов'язані з використанням е-банкінгу, притаманні високий рівень інтелекту, винахідливість та комунікабельність. Властивою характеристикою особи злочинця (хакери, фішери, фрікери, спамери, кіберсквотери, спеціалісти з програмного забезпечення та використання ЕОТ) є особливий вид ознак – інтелектуальні. Ці особи мають спеціальні знання й навички у сфері електронного бізнесу, е-комерції, інтернет-торгівлі, здійснення банківських операцій, використання цифрових технологій, комп'ютерного програмування та ін. Здебільшого це чоловіки віком 20–40 років, які мають базову або повну вищу освіту.

Виокремлено віктимогенні групи потерпілих.

4. Конкретизовано особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. Встановлено, що початкові відомості, котрі стали приводом для внесення інформації до ЄРДР за фактом учинення кримінальних правопорушень, які надійшли до правоохоронних органів, визначають напрямки розслідування.

Вирізняють типові слідчі ситуації, що формуються на початковому етапі розслідування кримінальних правопорушень: 1) вчинено кримінальне правопорушення, пов'язане з використанням е-банкінгу, наявна достатня кількість доказової інформації, встановлено особу злочинця – 7 %; 2) вчинено кримінальне правопорушення, наявна достатня кількість доказової інформації, особу злочинця не встановлено – 62 %; 3) вчинено кримінальне правопорушення, наявна достатня кількість доказової інформації, встановлено особу злочинця, але злочинні дії замасковані під легальну фінансову діяльність – 8 %; 4) вчинено кримінальне правопорушення, наявна заява потерпілої особи, відсутня будь-яка доказова інформація – 23 %.

5. Визначено особливості взаємодії слідчих та працівників оперативних підрозділів Національної поліції України у кримінальному провадженні.

Встановлено найбільш розповсюджені форми взаємодії, зокрема: здійснення доручень уповноваженої особи під час проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів (91 %); обмін інформацією (83 %); надання уповноваженій особі відомостей, що зібрані у процесі оперативно-розшукової діяльності, для вирішення питання стосовно внесення відомостей до ЄРДР (65 %); групове планування розшукових заходів (31 %); здійснення оперативним підрозділом доручень уповноваженої особи стосовно перевірки відомостей, що мають значення для встановлення наявності чи відсутності підстав для внесення відомостей до ЄРДР за оперативними

матеріалами (29 %).

У кримінальному провадженні вагомого значення набуває використання обміну інформацією як однієї з найбільш ефективних форм взаємодії, особливо в умовах запровадженого воєнного стану.

Така інформація може стосуватися наступних обставин: а) ознак злочинного діяння, пов'язаного з використанням е-банкінгу; б) структури ОГ та ЗО, що здійснюють тривалу злочинну діяльність в економічній сфері; в) характерних ознак злочинців, які здійснюють протиправну діяльність.

6. Виокремлено заходи профілактичної діяльності працівників правоохоронних органів (слідства, дізнання, кіберполіції) щодо виявлення й усунення причин та умов учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, а саме: 1) повідомлення громадян за допомогою засобів масової інформації про юридичну відповідальність за вчинені протиправні дії; 2) встановлення осіб, схильних до антисуспільної поведінки у сфері використання ЕОТ, а також їх подальше занесення до обліку в підрозділах кіберполіції; 3) участь працівників кіберполіції у тематичних передачах, круглих столах, ток-шоу, де висвітлюються питання запобігання протиправним діям у кіберпросторі; 4) вивчення матеріалів кримінальних проваджень для з'ясування та усунення умов і причин, що сприяли вчиненню протиправних діянь; 5) інформування громадян у соціальних мережах, ЗМІ, месенджерах щодо фактів учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (як-от: фішинг, кардинг, спамінг).

Вирізнено причини та умови, що впливають на вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

Встановлено, що однією з головних причин неефективності заходів із запобігання кримінальним правопорушенням, пов'язаним із використанням е-банкінгу, залишається низький рівень обізнаності слідчих та працівників оперативних підрозділів Національної поліції України щодо типових злочинних схем під час здійснення незаконних банківських операцій та напрямів збирання електронних доказів, встановлення правопорушників за цифровою слідовою картиною, особливостей документування злочинних дій у кіберпросторі тощо.

7. Розкрито тактичні операції щодо збирання первинних даних про обставини злочинної події та виявлення ознак досліджуваних протиправних діянь, а саме з-поміж них визначено такі, як: «Встановлення характеру події кримінального правопорушення», «З'ясування місця та часу вчинення протиправного діяння», «Встановлення способу вчинення протиправного діяння (фішинг, застосування шпигунських програм, спам-ботів)», «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання», «З'ясування особи потерпілого та її віктимної поведінки, а також перевірка їх зв'язків» та ін.

Виокремлено завдання, котрі потрібно вирішувати для ефективного проведення відповідних тактичних операцій.

На основі узагальнення судово-слідчої практики запропоновано перелік слідчих (розшукових) дій, НСРД та інших процесуальних заходів, необхідних для ефективного здійснення тактичних операцій у кримінальному провадженні.

Виявлено тактичні помилки, яких припускаються уповноважені особи під час реалізації таких операцій.

8. Сформовано перелік заходів для реалізації тактичної операції «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання», як-от: 1) допити потерпілих; 2) встановлення очевидців злочинної події та допити свідків; 3) огляд електронно-обчислювальної техніки; 4) зняття інформації з електронних інформаційних систем або її частини; 5) встановлення місцезнаходження радіоелектронного засобу; 6) встановлення особи злочинця та оголошення її у розшук; 7) встановлення місцезнаходження злочинця; 8) затримання злочинця; 9) направлення вимог щодо надання правоохоронними органами, органами державної влади та органами місцевого самоврядування інформації, котра має значення для кримінального провадження за фактами вчинення протиправних діянь, пов'язаних із використанням е-банкінгу; 10) обшуки за місцем проживання та в інших місцях перебування злочинця; 11) допит підозрюваного для встановлення ймовірних співучасників кримінального правопорушення (лідера та активних учасників ОЗГ); 12) проведення затримання співучасників, залучених до злочинної діяльності; 13) обмін інформацією між відповідними підрозділами правоохоронних органів іноземних держав та міждержавних органів (Інтерполу, Європолу) стосовно реагування на кіберзлочини; 14) призначення та проведення судових експертиз.

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

*Наукові праці, в яких опубліковано основні наукові результати дисертації:*

1. Малютін Е. В. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 1. Т. 2. С. 143–147.

2. Малютін Е. В. Наукові диспути щодо тактичної операції «встановлення особи злочинця та його співучасників, їх розшук та затримання» під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридична наука*. 2020. № 2. Т. 2. С. 122–128.

3. Малютін Е. В. Проблемні питання реалізації профілактичних заходів працівниками правоохоронних органів під час розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Юридичний науковий електронний журнал*. 2021. № 9. С. 425–428. URL : [http://www.lsej.org.ua/9\\_2021/9\\_2021.pdf](http://www.lsej.org.ua/9_2021/9_2021.pdf).

4. Малютін Е. В. Наукова полеміка відносно сутності та форм взаємодії різних підрозділів правоохоронних органів при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Держава та регіони. Серія : Право*. 2022. № 2. С. 232–236.

5. Малютін Е. В. Теоретико-прикладні аспекти формування тактичних операцій стосовно збирання первинних даних щодо обставин події та виявлення ознак кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

*Knowledge, Education, Law, Management*. 2023. № 3. С. 178–183.

6. Малютін Е. В. Спосіб учинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу (криміналістичний аналіз). *Науковий вісник публічного та приватного права*. 2024. Вип. 2. С. 77–82.

*Наукові праці, які засвідчують апробацію матеріалів дисертації:*

7. Малютін Е. В. Обстановка вчинення кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як елемент криміналістичної характеристики. *Виклики сучасності та наукові підходи до їх вирішення: матеріали Міжнародної науково-практичної конференції* (м. Київ, 12–13 серпня 2020 р.). Київ: Науково-дослідний інститут публічного права, 2020. С. 132–134.

8. Малютін Е. В. Особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення: матеріали Міжнародної науково-практичної конференції* (м. Київ, 22–23 вересня 2021 р.). Київ: Науково-дослідний інститут публічного права, 2021. С. 171–173.

9. Малютін Е. В. Окремі аспекти використання спеціальних знань при розслідуванні кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Взаємодія публічного та приватного права: сучасні проблеми та виклики: матеріали Міжнародної науково-практичної конференції* (м. Київ, 21–22 лютого 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 139–141.

10. Малютін Е. В. Наукові підходи до побудови криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Інноваційні підходи до реформування сучасного законодавства: матеріали Міжнародної науково-практичної конференції* (м. Київ, 20–21 квітня 2023 р.). Київ: Науково-дослідний інститут публічного права, 2023. С. 144–146.

## АНОТАЦІЯ

**Малютін Е. В. Основи методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. – На правах рукопису.**

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. – Дніпровський державний університет внутрішніх справ, Дніпро, 2024.

У дисертації досліджено теоретико-прикладні засади методики розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу. Здійснено криміналістичний аналіз проведення електронних операцій у сфері використання банківських електронних платежів. Охарактеризовано фактори, що впливають на вчинення протиправних дій. Визначено сучасні



наукові підходи до розуміння сутності та системи криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу. Виокремлено елементи криміналістичної характеристики, як-от: спосіб та обстановка вчинення кримінального правопорушення, слідова картина, особа злочинця, особа потерпілого.

Охарактеризовано способи, обстановку та слідову картину протиправної діяльності. Способи злочинної діяльності мають широкі межі та виявляються у системі взаємопов'язаних дій із підготовки, безпосереднього вчинення та приховування протиправних дій, що пов'язані між собою єдиними мотивом і метою. Систематизовано способи підготовки та приховування протиправних дій.

Сформовано ймовірний «портрет» особи злочинця та виділено віктимогенні групи потерпілих.

Конкретизовано особливості аналізу первісної інформації, кваліфікації протиправних дій та визначення основних напрямів організації розслідування. Вирізняє типові слідчі ситуації, що формуються на початковому етапі розслідування. Визначено напрями взаємодії слідчих із працівниками кіберполіції, банківських установ, операторами мобільного зв'язку та суб'єктами, які забезпечують передачу і зберігання інформації з використанням інформаційно-комунікаційних систем.

Запропоновано заходи профілактики, що можуть здійснюватися уповноваженими особами у кримінальних провадженнях для попередження кримінальних правопорушень, пов'язаних із використанням е-банкінгу.

Розкрито тактичні операції щодо збирання первинних даних про обставини злочинної події та виявлення ознак досліджуваних протиправних діянь, а саме з-поміж них визначено такі, як: «Встановлення характеру події кримінального правопорушення», «З'ясування місця та часу вчинення протиправного діяння», «Встановлення способу вчинення протиправного діяння (фішинг, застосування шпигунських програм, спам-ботів)», «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання», «З'ясування особи потерпілого та її віктимної поведінки, а також перевірка їх зв'язків» та ін.

Сформовано перелік заходів для реалізації тактичної операції «Встановлення особи злочинця та його співучасників, а також їх розшук і затримання».

**Ключові слова:** е-банкінг, банківські операції, е-бізнес, електронний переказ, транзакція, кіберзлочини, комерція, інтернет-банкінг, досудове розслідування, методика, криміналістична характеристика, кримінальне правопорушення, слідчі (розшукові) дії, експертиза, спеціальні знання.

## SUMMARY

**Maliutin E. V. Basics of the methodology of investigation of criminal offenses related to the use of e-banking. – The manuscript.**

The thesis is for candidate's degree of law in the field 12.00.09 – Criminal

Procedure and Forensic Sciences; Judicial Examination; Operational-Search Activity. – Dnipro State University of Internal Affairs of the Ministry of Internal Affairs of Ukraine, Dnipro, 2024.

The thesis examines the theoretical and applied principles of the methodology of investigation of criminal offenses related to the use of e-banking. A forensic analysis of the implementation of electronic transactions in the field of the use of bank electronic payments was carried out. The factors influencing the commission of illegal actions are characterized. Modern scientific approaches to understanding the essence and system of forensic characterization of criminal offenses related to the use of e-banking are defined. The elements of the forensic characteristics are singled out: the method and circumstances of the commission of the criminal offense, the trail picture, the identity of the criminal, the identity of the victim.

The methods, situation and trace pattern of illegal activity are characterized. The methods of criminal activity have broad boundaries and are manifested in a system of interrelated actions of preparation, direct commission and concealment of illegal actions, which are connected by a single motive and goal. Methods of preparation and concealment of illegal actions have been systematized.

A probable «portrait» of the criminal was formed and victimogenic groups of victims were identified.

The specifics of the analysis of primary information, the qualification of illegal actions and the determination of the main directions of the organization of the investigation are specified. Typical investigative situations formed at the initial stage of the investigation are distinguished. The areas of interaction of investigators with employees of the cyber police, banking institutions, mobile operators and entities that ensure the transmission and storage of information using information and communication systems have been determined.

Preventive measures that can be implemented by authorized persons in criminal proceedings to prevent criminal offenses related to the use of e-banking are proposed.

Tactical operations related to the collection of primary data on the circumstances of the criminal event and the detection of signs of the investigated illegal acts are disclosed, among them the following are defined: «Establishing the nature of the event of the criminal offense», «Finding out the place and time of the commission of the illegal act», «Establishing the method of commission illegal act (phishing, use of spyware, spambots)», «Identification of the criminal and his accomplices, as well as their search and arrest», «Clarification of the identity of the victim and his victim behavior, as well as verification of their connections» etc.

A list of measures for the implementation of the tactical operation «Identification of the criminal and his accomplices, as well as their search and arrest» has been formed.

**Keywords:** *e-banking, banking operations, e-business, electronic transfer, transaction, cybercrimes, commerce, internet banking, pre-trial investigation, methodology, forensic characteristics, criminal offense, investigative (search) actions, expertise, special knowledge.*