МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

СИСОЛЯТІН ВАЛЕРІЙ ВІКТОРОВИЧ

УДК 343.98: 343.131

РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ІНТЕРНЕТ-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,
Дніпропетровський державний університет внутрішніх справ,
завідувач кафедри криміналістики та домедичної підготовки.

Офіційні опоненти:

доктор юридичних наук, професор,
заслужений юрист України
Дрозд Валентина Георгіївна,
Департамент забезпечення діяльності Голови Національної поліції України,
головний спеціаліст консультативно-контрольного відділу;

доктор юридичних наук, професор
Степанюк Руслан Леонтійович,
Харківський національний університет внутрішніх справ,
професор кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1.

Захист відбудеться 28 січня 2024 року об 09-00 годині на засіданні спеціалізованої вченої ради Д 08.727.02 Дніпропетровського державного університету внутрішніх справ за адресою: 49005, м. Дніпро, просп. Гагаріна, 26.

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

Автореферат розіслано 26 грудня 2023 року.

Учений секретар
спеціалізованої вченої ради **В.С. Березняк**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Світ невпинно розвивається, здійснюються нові наукові відкриття, дедалі запроваджуються процеси діджиталізації суспільства, створюються сучасні цифрові технології. Такі новації ефективно використовуються в економічній сфері, секторі державного управління, суспільстві та приватному житті. Формуються новітні поняття – криптовалюта, інтернет-банкінг, е-бізнес, «Qiwi-гаманець», MoneyGram, Perfect Money, е-комерція, blockchain) та ін. Цифрові процеси значно змінюють архітектоніку фінансових, комерційних та сервісних операцій, що позитивно впливає на розвиток суспільства. Останнім часом більшість провідних компаній перейшли на діджиталізований формат співпраці, що дозволяє швидко здійснювати комерційні операції, укладати угоди та перераховувати гроші. Безумовно такими новаціями не могли не скористуватися представники кримінальних угрупувань (хакери, фішери), які дедалі частіше роблять спроби швидко заволодіти коштами як пересічних громадян, так і підприємств, установ та організацій різних форм власності. Виходячи з цього, на сьогодні перед правоохоронними органами, насамперед, підрозділами Національної поліції, постають нагальні питання створення діючих алгоритмів встановлення вказаних осіб, попередження їхніх неправомірних посягань та ефективного розслідування протиправних діянь.

За даними узагальнення правоохоронної практики встановлено, що серед вказаних кримінальних правопорушень є великий масив тих, які пов’язані з використанням інтернет-банкінгу.

Так, відповідно до відомостей Офісу Генерального прокурора України до ЄРДР за 2018 рік було внесено 3366 фактів шахрайств, учинених з використанням високих інформаційних технологій, а обвинувальний акт було вручено лише у 847 випадках. У тому ж році за іншими статтями КК України, які пов’язані з використанням інтернет-банкінгу, була майже подібна ситуація або навіть гірша: ст. 200 КК – 609 випадків обліковано, 505 обвинувальних актів; ст. 222 КК – 58 випадків обліковано, 27 обвинувальних актів; ст. 231 КК – 272 випадків обліковано, 103 обвинувальних акта; ст. 232 КК – 11 випадків обліковано, а обвинувальні акти взагалі відсутні; ст. 361 КК – 1023 випадків обліковано, 479 обвинувальних актів; ст. 361^1 КК – 134 випадки обліковано, 79 обвинувальних актів; ст. 361^2 КК – 52 випадки обліковано, 23 обвинувальних актів; ст. 362 КК – 1070 випадків обліковано, 740 обвинувальних актів; ст. 363^1 КК – 10 випадків обліковано, 8 обвинувальних актів. Протягом наступних років статистика майже не змінювалася. Для підтвердження, приведемо статистичні дані за перші 5 місяців 2023 року: ст. 200 КК – 185 випадків обліковано, 103 обвинувальних акта; ст. 222 КК – 8 випадків обліковано та лише 1 обвинувальний акт; ст. 231 КК та ст. 232 КК відповідно 1 та 4 випадки обліковано, а обвинувальні акти взагалі відсутні; ст. 361 КК – 810 випадків обліковано, 356 обвинувальних актів; ст. 361^1 КК – 21 випадків обліковано, 3 обвинувальних акта; ст. 361^2 КК – 45 випадків обліковано, 7 обвинувальних актів; ст. 362 КК – 853 випадків обліковано, 406 обвинувальних актів; ст. 363^1 КК – 3 випадки обліковано, а обвинувальні акти взагалі відсутні. Наведені показники вказують на те, що кількість кримінальних правопорушень

визначеної категорії з року в рік дедалі збільшується, а кількість правопорушників, за якими складено обвинувальний акт, – залишається на досить незначному рівні. Окрім того, більшість протиправних дій мають високий рівень латентності, внаслідок чого значна кількість фактів залишаються невикритими.

Низька якість розслідування кримінальних проваджень та незначна кількість викритих й притягнутих до відповідальності злочинців зумовлена низкою чинників: відсутність чіткої взаємодії й належної координації окремих підрозділів Національної поліції (зокрема, співробітників кіберполіції та слідчих) – 71 %, невчасне здійснення СРД, НСРД та інших процесуальних заходів – 61 %, поверхневе використання техніко-криміналістичних засобів під час проведення окремих процесуальних дій та ігнорування залучення відповідних спеціалістів – 79 %, відсутність міжнародної практики розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу – 82 %, порушення послідовності дій під час збирання доказів на початковому етапі кримінального провадження – 62 %, невизначеність заходів щодо профілактики злочинних проявів – 91 % та ін.

Теоретичне підґрунтя дисертаційного дослідження становлять ґрунтовні праці вчених з різних напрямків юридичної науки (криміналістики, кримінального процесу, кримінології, кримінального права, оперативно-розшукової діяльності), які здійснили вагомий внесок у методику розслідування окремих видів кримінальних правопорушень, а саме: Ю. П. Аленін, І. В. Басиста, В. П. Бахін, В. Д. Берназ, В. К. Весельський, А. Ф. Волобуєв, В. Г. Дрозд, М. М. Єфімов, В. А. Журавель, А. В. Іщенко, Н. І. Клименко, В. О. Коновалова, В. С. Кузьмічов, В. В. Лисенко, В. Г. Лукашевич, Є. Д. Лук’янчиков, В. Л. Ортинський, І. В. Пиріг, М. В. Салтевський, Р. Л. Степанюк, В. Є. Тарасенко, В. В. Тіщенко, П. В. Цимбал, К. О. Чаплинський, С. С. Чернявський, Ю. М. Чорноус, В. Ю. Шепітько та ін.

Проблемні питання кримінально-процесуального, криміналістичного та оперативно-розшукового забезпечення розслідування кіберзлочинів, кримінальних правопорушень у сфері використання банківських електронних платежів або учинених через мережу Інтернет висвітлювалися у наукових працях: А. І. Анапольської, О. В. Герасимова, Б. М. Головкіна, І. А. Гукової, О. І. Деньковича, О. В. Доброво ї, О. Ю. Довженка, А. Е. Жиліна, Т. В. Коршикової, В. Б. Коби, І. О. Коваленка, О. В. Курмана, В. В. Луцика, О. І. Мотляха, В. Р. Мойсика, О. Л. Мусієнко, Т. В. Охрімчук, Н. В. Павлової, В. І. Пазиніч, Д. А. Птушкіна, А. В. Рейнгольда, А. В. Реуцького, Д. О. Рички, О. А. Самойленко, С. В. Самойлова, Т. Л. Тропіної, В. Г. Хахановського, Д. М. Цехана, К. О. Чередник, С. С. Чернявського, С. В. Чучка та ін.

Серед сучасних наукових розробок можна виділити дисертацію О. Ю. Довженка «Основи методики розслідування кіберзлочинів» (м. Харків, 2020 р.), в якій автор визначив стан наукової розробки проблем розслідування кіберзлочинів, встановив основні підходи до класифікації кіберзлочинів і запропонував на їх основі інтегрований підхід; надав криміналістичну характеристику кіберзлочинів як особливого типу злочинів, розглянув особливості допиту потерпілих, свідків, підозрюваних і обвинувачуваних у справах про кіберзлочини, виявив особливості отримування доказів та проведення експертиз у

справах про кіберзлочини. У свою чергу, С. В. Чучко у дисертації «Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет» (м. Дніпро, 2021 р.) охарактеризував особливості правового регулювання правовідносин у віртуальному просторі, що впливають на рівень вчинення шахрайства у мережі Інтернет, здійснив науковий аналіз обстановки вчинення шахрайства при купівлі-продажу товарів через мережу Інтернет та особливості їх слідової картини, сформулював систему типових слідчих ситуацій початкового етапу розслідування та висвітлив особливості використання спеціальних знань під час розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет. А вже колектив авторів у складі Б. М. Головкіна, О. І. Деньковича, В. В. Луцика і Д. М. Цехана у навчальному посібнику «Кіберзлочинність та електронні докази» (м. Львів, 2022 р.) визначив види кіберзлочинів, поняття кіберзлочинності та її місце у загальній структурі злочинності, окреслив особливості методики розслідування кіберзлочинів, охарактеризував електронні докази у кримінальному провадженні. А. Е. Жилін у дисертації «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів» (м. Дніпро, 2023 р.) розкрив стан наукових досліджень питань протидії шахрайствам у сфері використання банківських електронних платежів, охарактеризував основні елементи криміналістичної характеристики досліджуваного виду шахрайства, розглянув взаємодію слідчих та оперативних підрозділів Національної поліції, сформулював заходи профілактичної діяльності працівників правоохоронних органів щодо виявлення й усунення причин та умов шахрайства у сфері використання банківських електронних платежів, виокремив тактичні операції стосовно збирання початкових відомостей про обставини події та виявлення ознак шахрайства, визначив перелік заходів під час проведення тактичної операції «Електронно-обчислювальна техніка».

Проте, не зважаючи на теоретичну значущість наведених праць, більшість вчених обмежилися дослідженням лише проблемних аспектів розслідування кіберзлочинів або окремих видів шахрайств чи інших суміжних протиправних діянь. На сьогодні відсутнє комплексне дослідження міжвидової методики розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу, особливо в умовах запровадженого воєнного стану. Наведені обставини у своїй сукупності визначили актуальність окресленої проблематики, її теоретичне й практичне значення, а також зумовили вибір напряму дисертаційної роботи.

Зв’язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до положень Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації (розпорядження Кабінету Міністрів України від 17.11.2021 № 1467-р), Стратегії національної безпеки України (Указ Президента України від 14.09.2020 № 392/2020), Стратегії воєнної безпеки України (Указ Президента України від 25.03.2021 № 121/2021), Стратегії кібербезпеки України (Указ Президента України від 14.05.2021 № 447/2021), Національної економічної стратегії на період до 2030 року (постанова Кабінету Міністрів України від 03.03.2021 № 179), Стратегії

боротьби з організованою злочинністю (розпорядження Кабінету Міністрів України від 16.09.2020 № 1126-р), Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року (розпорядження Кабінету Міністрів України від 30.03.2023 № 272-р), Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки (Указ Президента України від 11.05.2023 № 273/2023), 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 задачі дослідження. *Мета* дисертаційного дослідження виявляється у розв'язанні конкретного наукового завдання з розробки теоретичних засад методики розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

Відповідно до обраної мети в дисертації поставлено та вирішуються такі основні взаємопов'язані *задачі*:

– узагальнити наукові погляди стосовно кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та запропонувати їхню криміналістичну класифікацію;

– визначити сучасні наукові підходи до розуміння криміналістичної характеристики як складової методики розслідування протиправних діянь досліджуваної категорії;

– охарактеризувати окремі елементи криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу;

– здійснити криміналістичний аналіз первісної інформації та сформулювати коло обставин, що підлягають встановленню у кримінальному провадженні;

– конкретизувати типові слідчі ситуації, що виникають на початковому етапі розслідування, а також відповідні кожній з них алгоритми дій працівників правоохоронних органів;

– визначити особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу;

– охарактеризувати подальший етап розслідування у кримінальних провадженнях досліджуваної категорії;

– виокремити особливості використання спеціальних знань під час розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

Об'єктом дослідження є кримінальні процесуальні відносини, що виникають у діяльності правоохоронних органів під час розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

Предмет дослідження – розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

Методи дослідження. В дисертації використано багатоманітні методи наукового пізнання у розрізі визначених мети, завдань, об'єкта й предмета дослідження. Базисом їх застосовування є діалектичний метод, який визначає вагомість взаємодії складових будь-якої системи та їх взаємозв'язок для її ефективної діяльності. Зокрема, *порівняльно-правовий метод* використовувався при опрацюванні кримінально-процесуальних і кримінальних норм, системи процесуальних дій, а також деяких нормативно-правових актів (розділи 1–3). Застосовування *методу формальної логіки* надало змогу детально з'ясувати сутність криміналістичної характеристики кримінального правопорушення та виокремити її основні складові (підрозділи 1.1-1.2). Використання *історико-правового методу* зумовлено необхідністю опрацювання ґенези наукових поглядів щодо кримінальних правопорушень досліджуваної категорії (підрозділ 1.1). *Системно-структурний метод* дозволив здійснити криміналістичну класифікацію правопорушень, пов'язаних із використанням інтернет-банкінгу, а також класифікацію типових способів їх підготовки, безпосереднього учинення й приховування; виділення віктимогенних груп потерпілих (розділ 1). *Метод моделювання* застосовувався під час формулювання загальних висновків та конкретних пропозицій стосовно вдосконалення КК та КПК України (розділи 1–3). *Документальний, соціологічний* та *статистичний методи* використано під час узагальнення результатів опитування респондентів та аналізу матеріалів кримінальних проваджень (розділи 1–3), а також при з'ясуванні недоліків в організаційно-тактичному забезпеченні проведення окремих процесуальних дій під час розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу (розділи 2–3). *Типологічний метод* – використано для створення «портрету» ймовірного правопорушника та виокремлення віктимогенних груп потерпілих (підрозділ 1.3). На основі *синтезу* сформульовано загальні висновки за темою дослідження (розділи 1–3).

Емпіричну основу дослідження становлять згруповані відомості Єдиного звіту про вчинені кримінальні правопорушення Офісу Генерального прокурора України та Департаменту інформаційно-аналітичної підтримки Національної поліції за період 2018-2023 рр., а також результати узагальнення оперативної, слідчої та судової практики протягом 2015-2023 рр. Зокрема, опрацьовано матеріали 247 кримінальних проваджень за напрямом дослідження (Волинська, Дніпропетровська, Донецька, Закарпатська, Запорізька, Івано-Франківська, Київська, Кіровоградська, Львівська, Миколаївська, Одеська, Сумська, Ужгородська, Харківська та Чернівецька області, м. Київ), а також проаналізовано зведені результати опитувань 151 працівника прокуратури, 316 слідчих, 376 працівників оперативних підрозділів та 84 працівників експертних установ МВС України. Під час дослідження використано власний досвід роботи в правоохоронних органах України.

Наукова новизна одержаних результатів полягає у тому, що дисертаційна робота є першим у вітчизняній науці комплексним монографічним дослідженням основ методики розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, в якому сформульовано низку наукових положень 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 криміналістичну класифікацію визначеної категорії протиправних діянь, зокрема: а) кримінальні правопорушення, пов'язані із використанням інтернет-банкінгу, у сфері власності; б) кримінальні правопорушення, пов'язані із використанням інтернет-банкінгу, у сфері господарської діяльності; в) кримінальні правопорушення, пов'язані із використанням інтернет-банкінгу, у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку;

– сформовано структуру окремої міжвидової методики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, в якій виокремлено наступні елементи: 1) криміналістична класифікація протиправних діянь; 2) криміналістична характеристика; 3) аналіз початкової інформації щодо вчиненого діяння; 4) обставини, що підлягають встановленню; 5) типові слідчі ситуації та відповідний їм алгоритм дій уповноважених осіб; 6) профілактична діяльність уповноважених осіб зі встановлення причин й умов, що сприяли учиненню кримінальних правопорушень; 7) взаємодія підрозділів правоохоронних органів та інших структур у кримінальному провадженні; 8) початковий етап розслідування; 9) подальший етап розслідування; 10) особливості використання спеціальних знань;

– запропоновано систему запобіжних заходів, котрі необхідно здійснювати уповноваженим особам правоохоронних органів при розслідуванні досліджуваної категорії протиправних діянь, зокрема: 1) застосовування протоколів безпеки, зокрема, використання криптографічних функцій, а також системи аутентифікації користувачів шляхом перевірки правильності внесених даних і запобігання заміни особи; 2) застосовування технологій фіксації транзакцій, для прикладу, блокчейн, що допускають фіксувати всю інформацію; 3) повідомлення громадян через ЗМІ, соціальні мережі та месенджери (Viber, Telegram, WhatsApp) про факти скоєння кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу (фішинг, кардинг); 4) встановлення осіб, які мають нахили до антисуспільної поведінки в інформаційній сфері та постановка їх на відповідні обліки у підрозділах правоохоронних органів (зокрема, кіберполіції);

– надано перелік тактичних завдань, які повинні вирішуватись працівниками правоохоронних органів у кримінальних провадженнях досліджуваної категорії, а також розроблено комплекси дій для їх вирішення в рамках реалізації початкового та подальшого етапів розслідування;

удосконалено:

– теоретичні концепції стосовно інформативного наповнення криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу;

– систему способів безпосереднього вчинення досліджуваної категорії кримінальних правопорушень, як-от: 1) шахрайські дії під час використання

інтернет-банкінгу (фішинг, кардінг); 2) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; 3) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; 4) розповсюдження шкідливих програмних чи технічних засобів або їхній збут з використанням мережі Інтернет; 5) несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах; 6) умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп'ютерів, та ін.;

– сукупність відомостей відносно обстановки вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, з урахуванням нормативно-правових, просторово-часових, соціальних, психологічних та економічних чинників;

– перелік можливих місць учинення кримінальних правопорушень: місця розташування електронно-обчислювальної техніки, з якої вчинювалися протиправні дії (стаціонарне комп'ютерне обладнання, ноутбук, планшет, телефон) – 61 %; місця знаходження банкоматів, установ, підприємств та організацій фінансової сфери – 21 %; місце знаходження потерпілого, який виявив факт учинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу – 12 %;

– криміналістичні ознаки й властивості осіб, які є потерпілими від кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, завдяки виокремленню відповідних віктимогенних груп;

– пропозиції з приводу аналізу початкової інформації та на їх основі прийняття обґрунтованого висновку щодо початку досудового розслідування;

– систему обставин, що підлягають встановленню у кримінальному провадженні;

– сукупність криміналістичних версій, які можна висувати на початковому етапі розслідування: 1) кримінальне правопорушення, пов'язане з використанням інтернет-банкінгу, вчинене з метою отримання матеріальної вигоди «хакером»; 2) протиправне діяння вчинене з метою отримання матеріальної вигоди співробітником певної установи, яка володіє навичками роботи з комп'ютерною технікою; 3) протиправне діяння вчинено з метою заволодіння інформацією з обмеженим доступом особою (особами), що має вільний доступ до визначеної комп'ютерної техніки; 4) протиправне діяння вчинено з метою заволодіння інформацією з обмеженим доступом особою (особами), що не має вільного доступу до визначеної комп'ютерної техніки; 5) протиправне діяння вчинено з метою порушення алгоритму обробки даних, знищення або пошкодження комп'ютерних програм і баз даних, а так само їхніх носіїв;

– принципи інформаційного забезпечення проведення слідчих (розшукових) дій початкового та подальшого етапів розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, в розрізі інформаційного забезпечення допиту підозрюваних, свідків та потерпілих;

дістали подальшого розвитку:

– наукові положення щодо напрямів теоретичних досліджень з проблем розслідування кримінальних правопорушень, пов'язаних із використанням е-банкінгу, враховуючи умови запровадженого воєнного стану;

– система відомостей стосовно віртуальних (електронних, комп'ютерних) слідів, що визначають слідову картину протиправного діяння та їх взаємозалежність діям правопорушника з підготовки, вчинення й приховування кримінального правопорушення та обстановкою, у якій вони утворилися;

– сукупність криміналістичних ознак та властивостей особи правопорушника, на основі яких утворено його ймовірний «портрет» злочинця;

– положення відносно планування та організації розслідування досліджуваної категорії протиправних діянь;

– система типових слідчих ситуацій під час розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу;

– організація і тактика проведення слідчих (розшукових) дій для вилучення інформації з матеріальних та особистісних джерел з урахуванням завдань, що потребують вирішення під час їх підготовки та проведення, а також проведення окремих негласних слідчих (розшукових) дій, серед яких варто виділити наступні: спостереження за об'єктом, прослуховування телефонних переговорів, зняття інформації з транспортних та електронних систем;

– пропозиції відносно застосовування спеціальних знань у формі залучення спеціалістів відповідного профілю при їх безпосередній участі у процесуальних діях, зокрема: огляду комп'ютерної техніки – спеціаліст в галузі комп'ютерних технологій для ефективного виявлення та вилучення слідів правопорушення; допиту потерпілого – спеціаліста-фоноскопіста для роботи з голосовими даними (запис розмови потерпілого та правопорушника), які є в матеріалах кримінального провадження, а також подальшого призначення та проведення відповідних експертиз; обшуку – спеціаліст в галузі комп'ютерних технологій для ефективного вилучення електронно-обчислювальної техніки та носіїв інформації шляхом якісного подолання систем захисту, роботи з пристроями електроживлення, а також правильного зняття цифрових даних.

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

– *науковій діяльності* – під час реалізації наукових досліджень, спрямованих на розробку й удосконалення основ методики розслідування окремих видів кримінальних правопорушень у сфері власності й господарської діяльності, а також у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (акти впровадження Харківського національного університету внутрішніх справ від 06.04.2023 р., Національної академії внутрішніх справ від 23.05.2023 р.);

– *освітньому процесі* – при викладанні навчальних дисциплін «Організація розслідування кримінальних правопорушень», «Криміналістика», «Кримінальний процес», «Тактичні особливості проведення слідчих (розшукових) дій», «Оперативно-розшукова діяльність», а також підготовці підручників, навчальних посібників, проведення практичних занять з кримінального процесу та

криміналістики (акти впровадження ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» від 25.05.2023 р.);

– *законотворчій діяльності* – для покращення нормативно-правового забезпечення профілактики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, зокрема, в результаті наукового дослідження викладено низку пропозицій стосовно внесення змін і доповнень до діючих Кримінального процесуального кодексу України та Кримінального кодексу України;

– *правозастосовній діяльності* – для вдосконалення діяльності органів прокуратури, досудового розслідування, оперативних та експертних підрозділів Національної поліції (акти впровадження Дніпропетровського НДЕКЦ МВС від 19.05.2023 р.).

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.), «Перспективні напрямки розвитку юридичної науки у 21-му сторіччі» (м. Київ, 2022 р.), «Пріоритетні напрями розвитку юридичної науки в умовах сьогодення » (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 вісім підрозділів, висновків), списку використаних джерел і додатків. Загальний обсяг дисертації становить 230 сторінок, з яких 158 сторінок основного тексту. Список використаних джерел налічує 191 найменування та займає 22 сторінки, 4 додатки викладено на 27 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **Вступі** аргументовано актуальність теми дослідження, розкрито рівень опрацювання проблематики, її зв'язок роботи з науковими програмами, планами та темами, визначено мету і завдання, сформульовано об'єкт та предмет дослідження, розглянуто методи серед яких також розкрито емпіричну основу роботи, з'ясовано наукову новизну, викладено практичне значення отриманих результатів, розкрито дані про апробацію окремих положень дисертації, крім того, наведено наявні публікації і структуру дисертаційного дослідження.

Розділ 1 «Теоретичні засади побудови криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу» складається з трьох підрозділів, в яких розглядається стан наукової розробки окресленої проблематики та характеристика ознак окремих складових криміналістичної характеристики.

У *підрозділі 1.1 «Ґенеза наукових підходів стосовно кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та їх криміналістична класифікація»* здійснено детальний аналіз протиправних діянь у сфері використання банківських електронних платежів та запропоновано їхню обґрунтовану класифікацію.

Акцентовано увагу на «цифровізації» суспільства. Доведено, що на сьогодні термін «цифровізація» вживають у значно широкому розумінні, у тому числі і як «цифрову революцію» в економіці, суспільстві та приватному житті.

Наголошено, що поняття «кіберзлочинів» утворилося у 1980-х роках після запуску в 1971 році комп'ютерного вірусу за назвою «Creeper» (дистанційна програма), який після потрапляння в комп'ютерну мережу залишав вислів: «Я – Повзун. Спіймай мене якщо зможеш». Зосереджено увагу на тому, що на протязі значного періоду протиправні діяння, що вчинялися за допомогою електронно-обчислювальної техніки, взагалі не характеризувались як кримінальне правопорушення.

На початку 2000-х років законодавці у більшості країн Європейського Союзу дійшли висновків про необхідність виокремлення конкретних протиправних діянь, які можуть вчинюватися з використанням комп'ютерних систем (технологій). Вказані положення було закріплено у низці міжнародних нормативно-правових актів, серед яких необхідно виокремити Конвенцію про кіберзлочинність та Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Аналіз Кримінального кодексу України та ряду інших нормативно-правових актів дозволив зробити висновок, що заходи, визначені як Конвенцією, так і Додатковим протоколом до неї, майже повністю імплементовані у правове поле нашої держави.

Встановлено, що низці кримінальних правопорушень, які передбачені КК України та віднесені до різних його розділів, притаманна загальна характеристика – вчинення з використанням інтернет-банкінгу. На підставі цього, запропоновано криміналістичну класифікацію визначеної категорії протиправних діянь.

Охарактеризовано наукові підходи щодо сутності окремих наукових категорій, що характеризують правовідносини у сфері використання банківських електронних платежів, зокрема: «е-банкінг», «електронний бізнес», «цифрова торгівля» та ін.

Здійснено узагальнення нормативно-правових актів, що визначають організаційно-правові засади діяльності у сфері інтернет-банкінгу в Україні.

Визначено коло суб'єктів, які задіяні у сфері використання банківських електронних платежів та охарактеризовано характер їхньої взаємодії.

Підрозділ 1.2 «Криміналістична характеристика як складова методики розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу» присвячений дослідженню визначеної наукової категорії з окресленням її структури.

Сформовано структуру окремої міжвидової методики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, в якій виокремлено наступні елементи: 1) криміналістична класифікація протиправних

діянь; 2) криміналістична характеристика; 3) аналіз початкової інформації щодо вчиненого діяння; 4) обставини, що підлягають встановленню; 5) типові слідчі ситуації та відповідний їм алгоритм дій уповноважених осіб; 6) профілактична діяльність уповноважених осіб зі встановлення причин й умов, що сприяли учиненню кримінальних правопорушень; 7) взаємодія підрозділів правоохоронних органів та інших структур у кримінальному провадженні; 8) початковий етап розслідування; 9) подальший етап розслідування; 10) особливості використання спеціальних знань.

Надано авторське визначення криміналістичної характеристики правопорушень, пов'язаних з використанням Інтернет-банкінгу, як сукупності даних, отриманих із судово-слідчої практики, про криміналістично значимі ознаки певної категорії протиправних діянь, яка зводиться до кореляційних зв'язків між ними та забезпечує побудову і перевірку криміналістичних версій для вирішення основних завдань кримінального провадження, а також надає додаткову інформацію, необхідну для ефективного проведення слідчих (розшукових) дій та НСРД.

На основі вивчення матеріалів кримінальних проваджень визначено перелік основних елементів криміналістичної характеристики правопорушень, пов'язаних із використанням інтернет-банкінгу.

У *підрозділі 1.3 «Характеристика окремих елементів криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу»* на підставі узагальнення наукових досліджень учених (А. І. Анапольська, Б. М. Головкін, О. І. Денькович, О. Ю. Довженко, А. Е. Жилін, Т. В. Коршикова, І. О. Коваленко, О. В. Курман, В. В. Луцик, О. Л. Мусієнко, Н. В. Павлова, А. В. Рейнгольд, О. А. Самойленко, С. В. Самойлов, Д. М. Цехан, С. В. Чучко) проаналізовано найбільш вагомі складові досліджуваної наукової категорії.

Обґрунтовано, що у переважній більшості випадків (99 %) мають місце повноструктурний склад способу вчинення протиправних дій. Аргументовано, що спосіб є центральним елементом криміналістичної характеристики.

В умовах діджиталізації суспільства злочинна діяльність видозмінює свої форми та методи, злочинці дедалі використовують складні й нетипові способи учинення та приховання злочинних дій.

На основі вивчення матеріалів кримінальних проваджень охарактеризовано основні підготовчі дії до вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу: 1) підбір та підготовка необхідної електронно-обчислювальної техніки (комп'ютерів, ноутбуків, планшетів); 2) створення шкідливих програмних чи технічних засобів з метою протиправного використання, розповсюдження або збуту; 3) несанкціоновані збут або розповсюдження через мережу Інтернет інформації з обмеженим доступом, яка зберігається в комп'ютерах; 4) створення повідомлень електрозв'язку для подальшого їх масового розповсюдження, здійснене без попередньої згоди адресатів; 5) створення сприятливих умов для здійснення злочинних дій та ін.

Встановлено найбільш типові способи учинення та приховування досліджуваної категорії протиправних діянь.

Значну увагу приділено обстановці учинення кримінальних правопорушень як системи об'єктивних чинників й умов матеріальної обстановки, а також просторово-часових характеристик місця та часу. Охарактеризовано місця учинення досліджуваної категорії кримінальних правопорушень.

Визначено слідову картину протиправних діянь. Встановлено, що переважний масив слідової інформації залишається у мережі Інтернет (безпосередньо в проведених інтернет-операціях, в кеш-пам'яті або хмарних сховищах). З'ясовано, що у більшості випадків потерпілий не має візуального контакту з правопорушником.

Охарактеризовано криміналістично значущі типологічні ознаки особи злочинця та особливості віктимогенної поведінки потерпілих.

Надано перелік ознак і властивостей, що характеризують особу злочинця, зокрема: інтелектуальні, психологічні, соціально-демографічні, моральні та фізичні.

Встановлено, що досліджувані протиправні діяння вчинюють переважно чоловіки (91 %). Стосовно критерію віку особи, яка їх вчинила, з'ясовано, що це були особи у віці 16-20 років – 8 %, 20-30 років – 42 %, 30-40 – 26 %, 40-50 років – 19 %, 50 років і старше – 5 %.

Відносно рівня освіти правопорушників встановлено наступні дані: базову середню освіту має 1 % правопорушників, середню – 2 %, середню спеціальну – 4 %, базову вищу – 15 %, вищу – 79 %. Підсумовуючи зазначене, було створено ймовірний «портрет» особи правопорушника.

Охарактеризовано особу потерпілого. Вирізнено віктимогенні групи осіб щодо яких було вчинено кримінальні правопорушення визначеної категорії: а) працівники фінансових установ, підприємств та організацій різних форм власності; б) їхні клієнти; в) родичі клієнтів.

Висвітлено кореляційні зв'язки між елементами криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

Розділ 2 «Організаційні основи розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу» складається з двох підрозділів, у яких охарактеризовано особливості отримання початкової інформації про вчинене діяння, сформовано коло обставин, що підлягають встановленню, а також виокремлено типові слідчі ситуації, що виникають на початковому етапі розслідування.

У *підрозділі 2.1 «Криміналістичний аналіз первісної інформації та організація розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу»* охарактеризовано правові підстави початку кримінального провадження та визначено обставини, які підлягають встановленню.

З'ясовано, що первинна інформація, яка була підставою для внесення відомостей до Єдиного реєстру досудових розслідувань за фактом учинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, надавалася до підрозділів правоохоронних органів наступним чином: а) заяви, листи та повідомлення від громадян, які є потерпілими від досліджуваних протиправних діянь – 77 %; б) заяви, листи й повідомлення від громадян, які

отримали інформацію про вчинене протиправне діяння або стали його свідками – 9 %; в) повідомлення працівників установ, підприємств та організацій – 3 %; г) матеріали досудового розслідування, виділені з інших кримінальних проваджень – 6 %; д) матеріали, отримані під час проведення НСРД та розшукових заходів – 5 %.

На підставі узагальнення матеріалів кримінальних проваджень визначено джерела, які дають змогу отримати офіційні відомості, що підтверджують або спростовують інформацію про факт учинення протиправних дій в кіберпросторі.

З'ясовано коло обставин, що підлягають встановленню, зокрема: 1) обставини, що характеризують вчинення кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу: а) відомості про час, місце та спосіб учинення протиправних дій, як-от, застосовування шкідливих програм чи вірусів, заведених до комп'ютерного забезпечення потерпілого та дублювання за допомогою них акаунту на власний ґаджет (смартфон, планшет, ноутбук, комп'ютер); б) відомості про віртуальні сліди кримінального правопорушення; в) встановлення місця одержання безпідставного доступу до мережі Інтернет; г) засоби, які застосовувалися під час скоєння протиправного діяння (технічні – різні ґаджети, зокрема, смартфони, ноутбуки, модеми; програмні – шпигунські програми, браузери, шкідливі віруси); 2) обставини, які розкривають особу правопорушника з різних сторін (професійної, злочинної. розумової); 3) обставини, які розкривають особу потерпілого з різних сторін (професійної, злочинної. розумової); 4) причинно-наслідкові взаємозв'язки: факт чіткого зв'язку між діями правопорушників та їх наслідками; 5) обставини, які обтяжують чи пом'якшують покарання, або у цілому виключають кримінальну відповідальність за скоєння протиправних діянь, пов'язаних із використанням інтернет-банкінгу.

Запропоновано систему запобіжних заходів, котрі необхідно здійснювати уповноваженим особам правоохоронних органів при розслідуванні досліджуваної категорії протиправних діянь.

У *підрозділі 2.2 «Типові слідчі ситуації, що виникають під час розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу»* здійснено аналіз наукових розробок учених стосовно поняття, сутності та видів слідчих ситуацій. Сформульовано типові слідчі ситуації розслідування кримінальних правопорушень та визначено алгоритми дій правоохоронних органів відповідно до кожної з них.

Зокрема, *у першій ситуації* (наявна особистісна доказова інформація та правопорушник відомий) уповноважена особа повинна провести комплекс заходів, за допомогою яких необхідно з'ясувати можливі обставин провадження для доказування вини правопорушника, зокрема: огляд засобів електронно-обчислювальної техніки правопорушника під час проведення обшуку (смартфонів, планшетів, ноутбуків, персональних комп'ютерів); допит підозрюваного з приводу обставин обману громадян та законності його діяльності; допит потерпілого щодо обставин зняття коштів через інтернет-банкінг; затребування відомостей від інтернет-провайдерів та операторів телекомунікаційного зв'язку; з'ясування умов створення фіктивного сайту, створення програм віддаленого доступу, «троянів», «ботів»; пред'явлення

підозрюваного для впізнання потерпілому за голосом (у разі спілкування в телефонному режимі) та в натурі (у разі комунікації у режимі відео-конференції); призначення комп'ютерно-технічної та інших видів експертиз.

Друга ситуація є найбільш розповсюдженою у досліджуваній категорії кримінальних проваджень – наявна особистісна доказова інформація, але правопорушник невідомий. Для її вирішення всі зусилля уповноважених осіб повинні бути направлені на встановлення особи, яка вчинила кримінальне правопорушення, пов'язане з використанням інтернет-банкінгу, а також її місцезнаходження. Для реалізації вказаного потрібно проводити комплекс розшукових заходів, спрямованих на встановлення IP-адреси та осіб, які мали доступ до електронно-обчислювальної техніки.

У *третій ситуації* (наявна матеріальна та особистісна доказова інформація, правопорушник відомий, але його дії замасковані під вид законних фінансових операцій) уповноважені особи повинні спрямувати усі зусилля на опрацювання змісту файлів й аналізу змісту web-браузерів, а також дослідження змісту електронної пошти, журналу вхідних і вихідних дзвінків на усіх доступних ґаджетах потерпілого.

Четверта ситуація (наявна заява від потерпілого та відсутня достатня доказова інформація) вирішується завдяки проведенню максимальної кількості СРД, НСРД та інших розшукових заходів для з'ясування як обставин учиненого протиправного діяння, так і встановлення особи правопорушника.

Сформульовано відповідні тактичні завдання, що необхідно вирішувати у кримінальних провадженнях досліджуваної категорії.

Розділ 3 «Тактика проведення процесуальних дій при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу» складається з трьох підрозділів, в яких охарактеризовано особливості початкового та подальшого етапів розслідування протиправних діянь досліджуваної категорії.

У *підрозділі 3.1 «Початковий етап розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу»* визначено особливості початкового етапу розслідування та охарактеризовано специфіку організаційних заходів та процесуальних дій.

На основі аналізу наукових праць вчених (А. І. Кунтій, Б. Є. Лук'янчиков, Є. Д. Лук'янчиков, С. Ю. Петряєв) сформульовано криміналістичні версії, які можна висувати на початковому етапі розслідування.

На основі вивчення матеріалів кримінальних проваджень виокремлено найбільш поширені процесуальні дії початкового етапу розслідування досліджуваної категорії протиправних діянь, а саме: огляд місця події (98 %), огляд електронної інформації (94 %), обшук (91 %), призначення та проведення експертиз (100 %), тимчасовий доступ до речей і документів (79 %), огляд документів (53 %), допит потерпілих та свідків (100 %).

Встановлено місця, які найчастіше підлягають огляду на початковому етапі розслідування, зокрема: робоче місце потерпілого, робоче місце підозрюваного, банкомати, місця доступу до загальної мережі Wi-Fi та ін.

З'ясовано, що на початковому етапі розслідування необхідно максимально

забезпечити збереження інформації, яка перебуває на флеш-накопичувачах, жорстких дисках (носіях), кеш-пам'яті відповідного пристрою, в хмарних сховищах та ін. Для цього обов'язково потрібно застосовувати проведення одночасних обшуків за різними адресами ймовірного знаходження правопорушників.

Встановлено особливості вилучення заблокованих та розблокованих переносних ґаджетів (смартфон, smart-годинник, портативний відео-реєстратор, GPS-навігатор).

Означено перелік об'єктів, що повинні вилучатись під час обшуку в досліджуваній категорії кримінальних проваджень.

Для визначення місць перебування вказаних осіб необхідно організувати та провести низку НСРД, серед яких виділено спостереження за об'єктом та прослуховування телефонних переговорів.

Підкреслено важливість детального огляду смартфонів, сітьового та серверного обладнання, комп'ютерної техніки, а також її комплектуючих (процесорів, модулів пам'яті, жорстких дисків).

Встановлено, що до проведення допиту потерпілих необхідно оглянути наявну в них електронно-обчислювальну техніку (смартфони, ноутбуки, планшети), за допомогою якої відбувалася переписка чи розмова з правопорушником. Зосереджено увагу на допиті потерпілого й свідка. Визначено основні завдання допиту, а також сформовано перелік об'єктів, що варто демонструвати під час допиту потерпілого або свідка.

У *підрозділі 3.2 «Подальший етап розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу»* з'ясовано, що на подальшому етапі розслідування переважно проводяться такі слідчі (розшукові) дії: допит підозрюваних (100 %), одночасний допит раніше допитаних осіб (82 %), призначення та проведення експертиз (100 %), пред'явлення для впізнання за голосом (3 %) та в натурі (1 %).

Наголошено на обов'язковому проведенні пред'явлення підозрюваного для впізнання у випадках можливості встановлення потерпілим його тотожності за голосом (у випадках телефонної розмови) або в натурі (у випадках розмови за допомогою відео-конференції).

Особливу увагу приділено тактиці допиту підозрюваного. З'ясовано, що під час допиту підозрюваних необхідно встановлювати наступні факти: електронно-обчислювальна техніка, яка була застосована для вчинення протиправних діянь; програмне забезпечення, яке використовувалось для вчинення кримінального правопорушення (програми віддаленого доступу, «трояни», «боти»); логіни та паролі акаунтів, які використовувались для спілкування з потерпілими; реквізити банківських карт та рахунків, на які переказувались кошти.

Визначено безконфліктні й конфліктні ситуації допиту. Охарактеризовано тактичні прийоми, що найчастіше застосовуються під час допиту підозрюваного: створення уявлення про інформованість уповноваженої особи – 89 %, швидкий темп допиту – 56 %, використання фактора раптовості – 57 %, створення напруги – 69 %, пред'явлення речових доказів – 33 %, застосування відеозапису – 45 %. Серед них особливе місце займає пред'явлення речових доказів.

Висвітлено особливості залучення до проведення допиту різних спеціалістів, серед яких виділено фахівців у економічній кібернетиці, цифрових технологіях, компетентною у галузі комерційної чи банківської діяльності.

З'ясовано, що для усунення розбіжностей у показаннях потерпілих, свідків та підозрюваних у 23 % випадках здійснювався одночасний допит двох або більше раніше допитаних осіб. Одночасний допит раніше допитаних осіб проводився: між підозрюваним та потерпілим – у 91 % випадків, між підозрюваним та свідками – 2 %, між підозрюваними особами – 7 %.

Встановлено, що у 63 % випадках під час проведення одночасного допиту між потерпілим і підозрюваним останній повністю або частково засвідчив свідчення, які раніше заперечував.

Виокремлено тактичні помилки, яких припускаються слідчі при проведенні процесуальних дій.

У *підрозділі 3.3 «Особливості використання спеціальних знань у кримінальному провадженні»* розглянуто поняття, форми, види й суб'єкти використання спеціальних знань та участь спеціаліста під час проведення слідчих (розшукових) дій.

Визначено, що спеціаліст у більшості випадків залучався до проведення наступних процесуальних дій: огляд місця події (100 %), огляд електронної інформації (100 %), обшук (98 %), тимчасовий доступ до речей та документів (51 %), допит (41 %), зняття інформації з транспортних телекомунікаційних мереж та електронних систем (100 %).

Охарактеризовано процесуальні та непроцесуальні форми використання спеціальних знань у кримінальному провадженні. На підставі аналізу судово-слідчої практики визначено перелік судових експертиз, що можуть призначатися при розслідуванні кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу: а) судова експертиза комп'ютерної техніки і програмних продуктів (експертиза технічних комп'ютерних засобів, експертиза даних, експертиза програмного забезпечення); б) експертиза телекомунікаційних систем і засобів; в) судово-бухгалтерська експертиза.

З'ясовано особливості підготовки і проведення судових експертиз. Виокремлено об'єкти, що направляються на експертизу: власні ґаджети потерпілого (смартфон, планшет, ноутбук, комп'ютер, модеми, маршрутизатори), власні ґаджети підозрюваного (смартфон, планшет, ноутбук, комп'ютер, модеми, маршрутизатори), флеш-накопичувачі, жорсткі диски та ін.

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, що виявляється в розробленні теоретичних і практичних засад методики розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, а також формулювання науково обґрунтованих пропозицій і практичних рекомендацій щодо їх розвитку й удосконалення з урахуванням досвіду зарубіжних країн. В результаті дослідження сформовано низку теоретичних положень, висновків і практичних рекомендацій, основними з яких є такі:

1. Здійснено криміналістичний аналіз функціонування сфери використання

банківських електронних платежів (е-банкінгу). Виокремлено основні фактори, що зумовлюють учинення протиправних дій. Здійснено аналіз наукових поглядів учених стосовно кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. З'ясовано, що низка вітчизняних і зарубіжних дослідників (Д. Деннінг, О. Довженко, Г. Загіка, В. Клей, О. Порфімович, Ф. Уільямс, О. Чернавський, Л. Шеллі) досліджували питання визначення сутності кіберзлочинності, а також можливі способи протидії та напрями запобігання вказаному негативному явищу. Проте кількість звернень за фактами протиправних дій дедалі зростає, злочинна діяльність набуває все більш латентного та організованого характеру. Заходи щодо протидії злочинним проявам з урахуванням запровадженого воєнного стану не відповідають сучасним загрозам і потребують удосконалення.

Запропоновано криміналістичну класифікацію визначеної категорії протиправних діянь, зокрема: 1) кримінальні правопорушення, пов'язані із використанням інтернет-банкінгу, у сфері власності; 2) кримінальні правопорушення, пов'язані із використанням інтернет-банкінгу, у сфері господарської діяльності; 3) кримінальні правопорушення, пов'язані із використанням інтернет-банкінгу, у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

2. Визначено сучасні наукові підходи до розуміння криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та основних її елементів, на підставі чого окреслено кореляційні зв'язки між ними. Система криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, складається з таких елементів: спосіб і обстановка вчинення правопорушення, слідова картина, особа злочинця та особа потерпілого.

Запропоновано авторське визначення. Доведено, що правильно сформована структура криміналістичної характеристики дозволить виокремити найбільш чіткі кореляційні зв'язки, які допоможуть як в побудові криміналістичних версій, так і ефективному проведенні окремих слідчих (розшукових) дій та НСРД.

3. Охарактеризовано окремі елементи криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

Способи досліджуваної категорії протиправних діянь мають глибокі грані, які виявляються у сукупності взаємопов'язаних дій з підготовки, безпосереднього вчинення та їх приховування. Дані стосовно вказаних способів є найбільш інформативним джерелом у кримінальному провадженні.

Охарактеризовано типові способи вчинення досліджуваної категорії кримінальних правопорушень: 1) шахрайські дії під час використання інтернет-банкінгу (фішинг, кардінг); 2) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; 3) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення; 4) розповсюдження шкідливих програмних чи технічних

засобів або їх збут з використанням мережі Інтернет; 5) несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах; 6) умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп'ютерів, та ін. Визначено способи підготовки та приховування протиправних діянь. З'ясовано злочинні схеми, що застосовуються під час запровадженого воєнного стану.

Визначено обстановку протиправних дій, яка характеризується обставинами місця та часу, що в більшості випадків є невизначеними, адже обіймають велику кількість об'єктів, що можуть бути місцем події.

Охарактеризовано місця учинення досліджуваної категорії кримінальних правопорушень: місця розташування електронно-обчислювальної техніки, з якої вчинились протиправні дії (стаціонарне комп'ютерне обладнання, ноутбук, планшет, телефон) – 61 %; місця знаходження банкоматів, установ, підприємств та організацій фінансової сфери – 21 %; місце знаходження потерпілого, який виявив факт вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу – 12 %.

Встановлено слідову картину кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. Визначено, що досліджувані категорії протиправних діянь характерні електронні сліди (віртуальні, цифрові, комп'ютерні). Зазначені сліди переважно знаходяться в наступних місцях: акаунти, пам'ять електронно-обчислювальної техніки, профілі соціальних мереж, сайти для криптовалютних переписок, бази даних операторів зв'язку та інтернет-провайдерів, флеш-носії.

Узагальнено криміналістично вагомі ознаки особи злочинця, на підставі чого сформовано ймовірний «портрет» правопорушника. Вирізнено віктимогенні групи осіб щодо яких було вчинено кримінальні правопорушення визначеної категорії.

4. Визначено особливості криміналістичного аналізу первісної інформації та охарактеризовано основні напрями організації розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

Окреслено коло обставин, що підлягають встановленню: 1) обставини, що характеризують вчинення кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу: а) відомості про час, місце та спосіб учинення протиправних дій, як-от, застосовування шкідливих програм чи вірусів, заведених до комп'ютерного забезпечення потерпілого та дублювання за допомогою них акаунту на власний ґаджет (смартфон, планшет, ноутбук, комп'ютер); б) відомості про віртуальні сліди кримінального правопорушення; в) встановлення місця одержання безпідставного доступу до мережі Інтернет; г) засоби, які застосовувалися під час скоєння протиправного діяння (технічні – різні ґаджети, зокрема, смартфони, ноутбуки, модеми; програмні – шпигунські програми, браузери, шкідливі віруси); 2) обставини, які розкривають особу правопорушника з різних сторін (професійної, злочинної. розумової); 3) обставини, які розкривають особу потерпілого з різних сторін (професійної, злочинної. розумової); 4) причинно-наслідкові взаємозв'язки: факт чіткого зв'язку між діями правопорушників та їх наслідками; 5) обставини, які обтяжують чи пом'якшують

покарання, або у цілому виключають кримінальну відповідальність за скоєння протиправних діянь, пов'язаних із використанням інтернет-банкінгу.

5. Конкретизовано слідчі ситуації, що виникають на початковому етапі розслідування, а також відповідні кожній з них алгоритми дій працівників правоохоронних органів. Серед типових слідчих ситуацій виокремлено наступні: 1) скоєно кримінальне правопорушення, пов'язане з використанням інтернет-банкінгу, має місце достатня доказова база, особу правопорушника встановлено – 6 %; 2) скоєно протиправне діяння, має місце достатня доказова база, особу правопорушника не встановлено – 64 %; 3) скоєно протиправне діяння, має місце достатня доказова база, особу правопорушника встановлено, та протиправні дії приховані під легальну фінансову діяльність – 9 %; 4) скоєно протиправне діяння, має місце заява потерпілого, відсутня будь-яка доказова база – 21 %.

Для вирішення вказаних слідчих ситуацій запропоновано вирішення наступних тактичних завдань: 1) з'ясування механізму кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу; 2) визначення точок доступу, з яких реалізувалися протиправні дії; 3) перевірка цифрових слідів, які залишені під час проведення електронних операцій; 4) встановлення осіб, які реалізували незаконне втручання в роботу інтернет-банкінгу; 5) перевірка мобільних контактів правопорушника та його особистих зв'язків; 6) перевірка банківських і поштових переказів правопорушника; 7) з'ясування всіх епізодів протиправної діяльності; 8) вжиття заходів стосовно попередження протидії розслідуванню.

6. Визначено особливості початкового етапу розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. Сформульовано криміналістичні версії, які можна висувати на початковому етапі кримінального провадження. Конкретизовано організаційно-тактичні особливості проведення окремих слідчих (розшукових) та процесуальних дій.

Визначено тактику огляду. Виокремлено вузлові ділянки, де можуть бути зосереджені сліди протиправних дій: робоче місце потерпілого, робоче місце підозрюваного, банкомати, місця доступу до загальної мережі Wi-Fi.

Розкрито організаційно-підготовчі заходи і тактику обшуку. Окреслено перелік об'єктів, які необхідно вилучати під час обшуку: 1) електронно-обчислювальна техніка, за допомогою якої здійснювалось втручання в роботу інтернет-мереж для їх дестабілізації або отримання відомостей, необхідних для реалізації операцій в інтернет-банкінгу (комп'ютери, планшети, ноутбуки, смартфони); 2) реквізити карток, що викрадені з серверів магазинів електронної торгівлі, платіжних і розрахункових систем, з персональних ґаджетів користувачів; 3) фотографії, відеозаписи, на яких наявні дані, що мають значення для кримінального провадження; 4) квитанції про здійснення банківських операцій; 5) смартфони або інші ґаджети, в яких наявна адресна книга (ПІБ й адреси клієнтів фінансових установ, підприємств та організацій різних форм власності); 6) записні книжки, журнали, рукописні тексти з наявними даними про особу потерпілого або інших зацікавлених осіб та ін.

Значну увагу присвячено тактиці проведення окремих НСРД, зокрема,

спостереження за об’єктом та прослуховування телефонних переговорів.

Зосереджено увагу на допиті потерпілого та окреслено основні його завдання: з’ясувати обставини вчинення протиправного діяння (час, місце, зокрема, з доступом до загальної мережі Wi-Fi, наявність поблизу сторонніх осіб – можливість віддаленого підключення з іншого ґаджету); проаналізувати його передумови (чи були надіслані на номер потерпілого та прийняті повідомлення – в якому месенджері та якого змісту, чи були наявні дзвінки – в якому месенджері та якого змісту); встановити послідовність дій потерпілого після вчинення кримінального правопорушення (одразу повідомив в правоохоронні органи чи своїм знайомим, родичам, що зробив з ґаджетом – вимкнув, перезавантажив, продовжив користуватися). Визначено, що під час допиту потерпілого або свідка доцільно демонструвати певні об’єкти: а) скріншоти повідомлень переписки зі злочинцем; б) зображення (скріншот) документу, який підтверджує зняття коштів з рахунку потерпілого; в) виписку з банківського рахунку потерпілого; г) у випадках розмови зі злочинцем в телефонному режимі чи в режимі відео-конференції з’ясувати у потерпілого чи зробив він її запис – якщо так, то долучити до кримінального провадження для подальшого використання під час проведення пред’явлення для впізнання.

7. Охарактеризовано подальший етап розслідування кримінальних правопорушень, пов’язаних із використанням інтернет-банкінгу. Встановлено, що на даному етапі розслідування, як правило, визначене коло підозрюваних, тому характерного значення набувають заходи щодо подолання їхньої протидії під час проведення слідчих (розшукових) дій.

Наголошено на обов’язковому проведенні пред’явлення підозрюваного для впізнання.

Визначено безконфліктні й конфліктні ситуації *допиту підозрюваного*. З’ясовано, що для вирішення конфліктних ситуацій застосовуються різноманітні тактичні прийоми допиту. Найбільш ефективним серед них вказано пред’явлення речових доказів, серед яких можуть демонструватись наступні об’єкти: свідчення потерпілих; протоколи пред’явлення для впізнання з позитивним результатом (підозрюваного впізнано за голосом чи в натурі); флеш-накопичувачі та жорсткі диски з інформацією про банківські операції з грошовими коштами; скріншоти хмарних сховищ; скріншоти переписки з потерпілими.

Розкрито тактику проведення одночасного допиту двох або більше раніше допитаних осіб.

Акцентується увага на тому, що поінформованість уповноваженої особи дає їй змогу здобути психологічну перевагу над правопорушником, що є запорукою успішності допиту та одночасного допиту раніше допитаних осіб. З’ясовано, що підозрювані у вчинені досліджуваної категорії протиправних діянь у більшості випадків мають високий рівень технічної підготовки, що переважає рівень знань про електронно-обчислювальну техніку уповноваженої особи, яка проводить допит. З огляду на це виняткове значення мають експертні висновки, які отримані за результатами дослідження виявлених доказів (електронної переписки, акаунтів, електронних операцій). Застосування визначених експертних досліджень, а також пред’явлення результатів проведення інших процесуальних дій надасть

уповноваженій особі можливість подолати опір підозрюваного та підштовхувати його до визнання своєї вини.

8. Виокремлено особливості використання спеціальних знань під час розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

Виділено найбільш поширені форми використання спеціальних знань: використання консультативної допомоги спеціаліста (91 %), призначення і проведення судових експертиз (100 %), участь спеціаліста при проведенні слідчих (розшукових) дій (89 %).

Запропоновано застосовування спеціальних знань у формі залучення спеціаліста відповідного профілю при його безпосередньої участі у процесуальних діях, зокрема: 1) огляду комп'ютерної техніки – спеціаліст в галузі комп'ютерних технологій для ефективного виявлення та вилучення слідів правопорушення; 2) допиту потерпілого – спеціаліста-фоноскопіста для роботи з голосовими даними (запис розмови потерпілого та злочинця), які є в матеріалах кримінального провадження, а також подальшого призначення та проведення відповідних експертиз; 3) обшуку – спеціаліст в галузі комп'ютерних технологій для ефективного вилучення електронно-обчислювальної техніки та носіїв інформації шляхом якісного подолання систем захисту, роботи з пристроями електроживлення, а також правильного зняття цифрових даних.

Наголошено на призначенні судових експертиз при розслідуванні досліджуваної категорії протиправних діянь.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Сисолятін В.В. Наукові диспути щодо кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, та побудови їх криміналістичної характеристики. *Юридичний науковий електронний журнал*. 2021. № 8. С. 457–459 http://www.lsej.org.ua/8_2021/99.pdf

2. Сисолятін В.В. Наукові підходи стосовно типових слідчих ситуацій при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *KELM (Knowledge, Education, Law, Management)*. 2022. № 7 (51). С. 129–133 (Республіка Польща).

3. Сисолятін В.В. Наукова полеміка з приводу обставин, що підлягають встановленню при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Науковий вісник публічного та приватного права*. 2023. Випуск 4. С. 127–132.

4. Sysoliatin, Valerii Problematic aspects of the initial phase of criminal investigation offences involving internet banking. *Entrepreneurship, Economy and Law*. 2023. № 5. pp. 112–117.

5. Сисолятін В.В. Актуальні питання опису ознак та властивостей окремих елементів криміналістичної характеристики правопорушень, пов'язаних із використанням інтернет-банкінгу. *Науковий вісник публічного та приватного права*. 2023. Випуск 5. С. 151–156.

6. Sysoliatin, Valerii The further stage of the investigation of criminal offences involving internet banking (issues of concern). *Entrepreneurship, Economy and Law*. 2023. № 6. pp. 89–94.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Сисолятін В.В. Особливості призначення експертизи при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *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. 35–37.

8. Сисолятін В.В. До питання формування структури криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням інтернет-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. 22–24.

9. Сисолятін В.В. Аналіз первинної інформації при розслідуванні кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матеріали Міжнародної науково-практичної конференції* (м. Київ, 14–15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

10. Сисолятін В.В. Криміналістична характеристика особи, яка вчиняє кримінальні правопорушення, пов'язані з використанням інтернет-банкінгу. *Пріоритетні напрями розвитку юридичної науки в умовах сьогодення : матеріали Міжнародної науково-практичної конференції* (м. Київ, 13–14 березня 2023 р.). Київ : Науково-дослідний інститут публічного права, 2023. С. 31–33.

АНОТАЦІЯ

Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-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. – Дніпропетровський державний університет внутрішніх справ, Дніпро, 2024.

У дисертації на монографічному рівні досліджено наукові та практичні основи методики розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. Запропоновано криміналістичну класифікацію визначеної категорії протиправних діянь, зокрема, кримінальні правопорушення, пов'язані з використанням інтернет-банкінгу, у сфері: а) власності; б) господарської діяльності; в) використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку.

Сформовано структуру окремої міжвидової методики кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. Надано теоретичні концепції стосовно інформативного наповнення криміналістичної характеристики визначеної категорії протиправних діянь, в якій почергово

охарактеризовано такі її складові як: спосіб учинення кримінального правопорушення, обстановка правопорушення, слідова картина протиправного діяння, особа правопорушника та особа потерпілого.

Запропоновано окремі аспекти аналізу початкової інформації та на їх основі прийняття обґрунтованого висновку щодо початку досудового розслідування. Виокремлено систему обставин, які підлягають встановленню під час розслідування досліджуваної категорії кримінальних правопорушень.

Сформовано систему типових слідчих ситуацій під час розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу. Надано перелік тактичних завдань, які повинні вирішуватись працівниками правоохоронних органів у кримінальних провадженнях досліджуваної категорії, а також розроблено комплекси дій щодо їх вирішення в рамках реалізації початкового та подальшого етапів розслідування. Визначено сукупність криміналістичних версій, які можна висувати на початковому етапі розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу.

Охарактеризовано принципи інформаційного забезпечення проведення слідчих (розшукових) дій початкового та подальшого етапів розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, в розрізі інформаційного забезпечення допиту підозрюваних, свідків та потерпілих.

Визначено особливості організації і тактики проведення слідчих (розшукових) дій для вилучення інформації з матеріальних та особистісних джерел з урахуванням завдань, що потребують вирішення під час їх підготовки та проведення, а також проведення окремих негласних слідчих (розшукових) дій.

Надано пропозиції відносно застосовування спеціальних знань у формі залучення спеціалістів відповідного профілю при їх безпосередній участі у процесуальних діях.

Ключові слова: *інтернет-банкінг, криміналістична характеристика, досудове розслідування, банківські операції, криміналістична класифікація, шахрайство, кіберзлочини, електронні перекази, кримінальне правопорушення, слідчі (розшукові) дії, спеціальні знання.*

SUMMARY

Sysoliatin V. V. Investigation of criminal offenses related with the using of Internet banking. – *The manuscript.*

The thesis is for candidate's degree of law on specialty 12.00.09 – Criminal Procedure and Criminalistics; Forensic Examination; Operational-Search Activity. – Dnipropetrovskyi State University of Internal Affairs of the Ministry of Internal Affairs of Ukraine, Dnipro, 2024.

The dissertation at the monographic level examines the scientific and practical foundations of the methodology of investigating criminal offenses related to the use of Internet banking. A criminalistic classification of a certain category of illegal acts is proposed, in particular, criminal offenses related to the use of Internet banking, in the field of: a) property; b) economic activity; c) use of electronic computing machines (computers), systems and computer networks and telecommunication networks.

The structure of a separate interspecies methodology of criminal offenses related to the use of Internet banking has been formed. Theoretical concepts are provided regarding the informative content of the forensic characteristics of a certain category of illegal acts, in which such components as: the method of committing the criminal offense, the situation of the offense, the trace pattern of the illegal act, the identity of the offender and the identity of the victim are alternately characterized.

Separate aspects of the analysis of initial information and, based on them, the adoption of a reasoned conclusion regarding the initiation of a pre-trial investigation are proposed. The system of circumstances to be established during the investigation of the investigated category of criminal offenses is singled out.

A system of typical investigative situations during the investigation of criminal offenses related to the use of Internet banking has been formed. A list of tactical tasks that must be solved by law enforcement officers in criminal proceedings of the studied category is provided, as well as sets of actions to solve them as part of the implementation of the initial and subsequent stages of the investigation have been developed. A set of forensic versions that can be put forward at the initial stage of the investigation of criminal offenses related to the use of Internet banking is defined.

The principles of information support for conducting investigative (research) actions of the initial and subsequent stages of the investigation of criminal offenses related to the use of Internet banking, in the context of information support for questioning suspects, witnesses and victims, are characterized.

The specifics of the organization and tactics of conducting investigative (search) actions for the extraction of information from material and personal sources, taking into account the tasks that need to be solved during their preparation and implementation, as well as the conduct of individual covert investigative (search) actions, are determined.

Proposals regarding the application of special knowledge in the form of involving specialists of the appropriate profile with their direct participation in procedural actions have been provided.

Keywords: *Internet banking, forensic characteristics, pre-trial investigation, banking operations, forensic classification, fraud, cybercrimes, electronic transfers, criminal offense, investigative (search) actions, special knowledge.*