Міністерство внутрішніх справ України

Дніпровський державний університет внутрішніх справ

Національна поліція України

Департамент забезпечення діяльності Голови Національної поліції України

ТЕОРЕТИЧНІ ТА ПРАКСЕОЛОГІЧНІ ЗАСАДИ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ

Монографія

КОЛЕКТИВ АВТОРІВ

Дніпро
2025

УДК 343.98.06:343.102:[343.9.024:343.74]
Т 30

Рецензенти:

Шевчишен Артем Вікторович – заступник начальника Головного слідчого управління Національної поліції України – начальник управління організації роботи та методичного забезпечення, доктор юридичних наук, професор, заслужений юрист України, полковник поліції;

Чорноус Юлія Миколаївна – професор кафедри криміналістики та судової медицини Національної академії внутрішніх справ, доктор юридичних наук, професор;

Юсупов Володимир Васильович – головний спеціаліст-криміналіст управління криміналістичного забезпечення Головного слідчого управління Національної поліції України, доктор юридичних наук, професор

Рекомендовано до друку
Вченою радою Дніпровського державного університету
внутрішніх справ
(протокол № 6 від 27 листопада 2025 року)

Т 30 Теоретичні та праксеологічні засади розслідування кримінальних правопорушень у кіберпросторі : монографія / Ю. О. Виходець, В. Г. Дрозд, М. М. Єфімов, В. Б. Коба, І. О. Луговий, Н. В. Павлова, К. О. Чаплинський ; МВС України, ДЗДГ Національної поліції України, Дніпр. держ. ун-т внутр. справ. Дніпро : ДДУВС, 2025. 212 с.

ISBN 978-617-560-103-7

У монографії здійснено теоретико-правовий аналіз теоретичних і праксеологічних засад розслідування кримінальних правопорушень у кіберпросторі. Дослідження проведено крізь призму сучасного розвитку теорії кримінального процесу, науки криміналістики та правозастосовної практики.

Схарактеризовано криміналістичну характеристику кіберзлочинів, зокрема способи їх учинення, умови реалізації, особу правопорушника й потерпілого. Визначено типові риси кіберзлочинця, віктимогенні групи потерпілих, особливості організації та планування досудового розслідування.

Розроблено алгоритми дій правоохоронців відповідно до типових слідчих ситуацій, окреслено напрями взаємодії підрозділів Національної поліції, державних і приватних структур. Проаналізовано тактичні засади проведення слідчих (розшукових) дій, у тому числі негласних, та особливості застосування спеціальних знань.

Монографія призначена для викладачів, науковців, аспірантів, докторантів, курсантів і студентів закладів вищої освіти зі специфічними умовами навчання, працівників органів прокуратури, Бюро економічної безпеки України, оперативних і слідчих підрозділів Національної поліції України, усіх тих, хто виявляє інтерес до юридичної науки та правозастосовної практики.

Авторський колектив

ВИХОДЕЦЬ Юрій Олександрович – начальник Департаменту кіберполіції Національної поліції України, доктор філософії в галузі права, генерал поліції третього рангу;

ДРОЗД Валентина Георгіївна – начальник консультативно-контрольного відділу Департаменту забезпечення діяльності Голови Національної поліції України, доктор юридичних наук, професор, заслужений юрист України;

ЄФІМОВ Микола Миколайович – професор кафедри криміналістики та домедичної підготовки Дніпровського державного університету внутрішніх справ, доктор юридичних наук, професор;

КОБА Валерій Борисович – начальник Департаменту забезпечення діяльності Голови Національної поліції України, кандидат юридичних наук, полковник поліції;

ЛУГОВИЙ Ігор Олександрович – помічник Голови організаційно-аналітичного відділу Департаменту забезпечення діяльності Голови Національної поліції України, кандидат юридичних наук, доцент, полковник поліції;

ПАВЛОВА Наталя Валеріївна –доцент кафедри правоохоронної діяльності Університету митної справи та фінансів, кандидат юридичних наук, доцент;

ЧАПЛИНСЬКИЙ Костянтин Олександрович – помічник Голови організаційно-аналітичного відділу Департаменту забезпечення діяльності Голови Національної поліції України, доктор юридичних наук, професор, полковник поліції

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АКЕ	–	апаратно-комп’ютерна експертиза
АРК	–	Автономна Республіка Крим
БЕБ	–	Бюро економічної безпеки України
ВПО	–	внутрішньо переміщена особа
ГСУ	–	Головне слідче управління
ГУНП	–	Головне управління Національної поліції
ЕОМ	–	електронно-обчислювальна машина
ЕОТ	–	електронно-обчислювальна техніка
ЕПС	–	електронні платіжні системи
ЄРДР	–	Єдиний реєстр досудових розслідувань
ЗМІ, медіа	–	засоби масової інформації
ЗО	–	злочинна організація
ЗСУ	–	Збройні Сили України
ІКЕ	–	інформаційно-комп’ютерна експертиза
КК України	–	Кримінальний кодекс України
КМЕ	–	комп’ютерно-мережева експертиза
КПК України	–	Кримінальний процесуальний кодекс України
КТЕ	–	комп’ютерно-технічна експертиза
МВС України	–	Міністерство внутрішніх справ України
НСРД	–	негласна слідча (розшукова) дія
НТЗ	–	науково-технічні засоби
ОГ	–	організована група
ОРД	–	оперативно-розшукова діяльність
ОТЗ	–	оперативно-технічні заходи
ПЕОМ	–	персональна електронно-обчислювальна машина
ПКЕ	–	програмно-комп’ютерна експертиза
ПК	–	персональний комп’ютер
СБ України	–	Служба безпеки України
СКТЕ	–	судова комп’ютерно-технічна експертиза
СОГ	–	слідчо-оперативна група
СРД	–	слідча (розшукова) дія

Технології – це всього лише інструмент.
Білл Гейтс

Технології, насправді, про людей, а не про апаратне або програмне забезпечення.
Роберт Вейд

Стало жахливо очевидно, що наші технології перевершили нашу людяність.
Ейнштейн

ПЕРЕДМОВА

Нині кіберзлочинність становить глобальну загрозу для стабільного функціонування суспільства, держав та їх інституцій. Для України з огляду на триваючу військову агресію російської федерації кіберзагрози мають особливо небезпечний характер, адже діяльність більшості хакерських угруповань держави-агресора спрямована на підрив національної безпеки шляхом дестабілізації роботи державних органів та критичної інфраструктури – Парламенту, Уряду, силових і безпекових структур.

За офіційними даними Офісу Генерального прокурора, у 2017 році до Єдиного реєстру досудових розслідувань внесено 4845 відомостей про шахрайські дії з використанням інформаційних технологій, тоді як підозру вручено лише у 2112 випадках. Схожа ситуація спостерігалася й щодо інших кримінальних правопорушень у кіберпросторі, зокрема: за статтею 200 КК України – 390 фактів зареєстровано, 369 – пред'явлено підозру; статтею 222 – 61 зареєстровано, 41 – пред'явлено підозру; статтею 361 – 1795 зареєстровано, 610 – пред'явлено підозру; статтею 361^1 – 35 зареєстровано, 7 – пред'явлено підозру; статтею 361^2 – 64 зареєстровано, 47 – пред'явлено підозру; статтею 362 – 670 зареєстровано, 607 – пред'явлено підозру; статтею 363^1 – 3 зареєстровано, а випадки пред'явлення підозри взагалі відсутні. Для порівняння наведемо статистичні дані за перше півріччя 2025 року, оскільки в попередні роки показники щодо зареєстрованих кримінальних правопорушень та повідомлень про підозру загалом залишалися на приблизно однаковому рівні. Отже, за статтею 200 КК України – 409 фактів зареєстровано, 388 – пред'явлено підозру; статтею 222 – 43 зареєстровано, 23 – пред'явлено підозру; статтею 361 – 1029 зареєстровано, 779 – пред'явлено підозру; статтею 361^1 – 52 зареєстровано, 45 – пред'явлено підозру; статтею 361^2 – 95 зареєстровано, 55 – пред'явлено підозру; статтею 362 – 827 зареєстровано, 598 – пред'явлено підозру;

статтею 363^1 – 31 зареєстровано, за якими особам підозру не пред'явлено. Указані відомості свідчать, що кількість вчинених кримінальних правопорушень у кіберпросторі з року в рік дедалі зростає, а кількість осіб, яким пред'явлено підозру, – залишається на вельми невисокому рівні. Також варто наголосити на відносній латентності досліджуваних протиправних діянь, унаслідок чого значна їх кількість навіть не обліковується.

Теоретичне підґрунтя монографічного дослідження становлять фундаментальні праці науковців з різних напрямів юридичної науки (кримінального процесу, криміналістики, оперативно-розшукової діяльності, кримінального права, кримінології), які зробили змістовний вклад в опрацювання загальних засад розслідування кримінальних правопорушень, зокрема: Ю. П. Аленіна, Л. І. Аркуші, І. В. Басистої, В. П. Бахіна, В. Д. Берназа, В. К. Весельського, А. Ф. Волобуєва, В. І. Галагана, В. Г. Гончаренка, І. В. Гори, О. М. Джужі, В. Г. Дрозд, М. М. Єфімова, В. А. Журавля, А. В. Іщенка, Н. С. Карпова, А. М. Кислого, Н. І. Клименко, В. О. Коновалової, В. П. Корж, В. С. Кузьмічова, В. В. Лисенка, Л. М. Лобойка, В. Г. Лукашевича, Б. Є. Лук'янчикова, Є. Д. Лук'янчикова, Г. А. Матусовського, Д. Й. Никифорчука, О. В. Одерія, І. В. Пирога, М. А. Погорецького, О. В. Пчеліної, М. В. Салтевського, Д. Б. Сергєєвої, С. М. Стахівського, Р. Л. Степанюка, В. М. Тертишника, В. В. Тіщенка, Л. Д. Удалової, І. Ф. Хараберюша, П. В. Цимбала, М. С. Цуцкірідзе, К. О. Чаплинського, С. С. Чернявського, Ю. М. Чорноус, В. Ю. Шепітька, А. В. Шевчишена, М. Г. Щербаковського, В. В. Юсупова, О. О. Юхна та ін.

Важливий доробок в опрацювання кримінального процесуального, криміналістичного та оперативно-розшукового забезпечення розслідування кримінальних правопорушень у кіберпросторі зробили такі дослідники, як: А. І. Анапольська, О. В. Герасимов, С. В. Головкін, О. В. Доброва, О. Ю. Довженко, А. Е. Жилін, В. Б. Коба, І. О. Коваленко, Т. В. Коршикова, О. В. Курман, Е. В. Малютін, О. І. Мотлях, В. Р. Мойсик, О. Л. Мусієнко, Н. О. Опанасенко, Т. В. Охрімчук, В. І. Пазиніч, Д. А. Птушкін, А. В. Рейнгольд, А. В. Реуцький, О. А. Самойленко, С. В. Самойлов, В. В. Сисолятін, Т. Л. Тропіна, В. Г. Хахановський, Д. М. Цехан, К. О. Чередник, С. В. Чучко та ін.

Серед праць зазначених учених-криміналістів варто виокремити дотичні до нашої тематики. Для прикладу, у 2020 році О. Ю. Довженко у дисертаційному дослідженні «Основи методики розслідування кіберзлочинів» (м. Харків, 2020 р.) 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 та обвинувачуваних у справах про кіберзлочини, виявив особливості отримування доказів та проведення експертиз у

справах про кіберзлочини. А вже О. А. Самойленко в монографії «Основи методики розслідування злочинів, вчинених у кіберпросторі» (м. Одеса, 2020 р.) схарактеризувала кіберпростір як об'єкт криміналістичного дослідження, визначила окремі особливості використання спеціальних знань у досліджуваній категорії кримінальних проваджень, сформулювала тактичні операції, а також опрацювала окремі елементи криміналістичної характеристики таких протиправних діянь. Крім того, В. В. Сисолятін у дисертації «Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу» (м. Київ, 2024 р.) підсумував генезу наукових поглядів стосовно кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, запропонував їх криміналістичну класифікацію, схарактеризував окремі елементи криміналістичної характеристики досліджуваної категорії кримінальних правопорушень, конкретизував типові слідчі ситуації, що виникають на початковому етапі розслідування, а також навів відповідні кожній з них алгоритми дій працівників правоохоронних органів.

Водночас слід зауважити, що наведені вище праці зазначених дослідників, попри їх важливість, висвітлили лише окремі аспекти проблематики розслідування кримінальних правопорушень у кіберпросторі. Зважаючи на високу латентність таких протиправних діянь, виникають істотні труднощі в організаційно-тактичному забезпеченні процесу їх доказування, особливо в умовах правового режиму воєнного стану. Крім того, проблематику протидії кіберзагрозам з боку хакерських підрозділів збройних сил російської федерації у наведених роботах було розглянуто досить поверхнево.

Зазначене зумовлює необхідність ужиття невідкладних заходів для вдосконалення криміналістичного забезпечення організації досудового розслідування кримінальних правопорушень у кіберпросторі, а також процесуального супроводу проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних заходів.

На сьогодні наявні методи досудового розслідування не забезпечують повною мірою ефективної протидії кримінальним правопорушенням у кіберпросторі. Стрімкі зміни у законодавстві, поєднані з відсутністю чіткої стратегії з боку правоохоронних органів, дедалі більше ускладнюють боротьбу зі злочинною діяльністю у цій сфері. Це, своєю чергою, потребує розроблення ефективних криміналістичних засобів, прийомів і методів розслідування таких правопорушень, особливо в умовах дії правового режиму воєнного стану.

Наведені чинники зумовлюють об'єктивну необхідність оновлення наявних підходів, вироблення чіткої стратегії та визначення конкретних алгоритмів дій для правоохоронних органів, насамперед органів і підрозділів Національної поліції України. Зазначені обставини підтверджують актуальність обраної теми монографічного дослідження, а також її наукове, теоретичне й практичне значення.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ

1.1. Генеза наукових поглядів стосовно кримінальних правопорушень у кіберпросторі та їх криміналістична класифікація

Новітні технології пронизують практично всі сфери нашого життя. Тотальна діджиталізація суспільства сприяє активному розвитку сучасних видів кримінальних правопорушень у кіберпросторі як в Україні, так і в усьому світі.

Згідно з даними Департаменту кіберполіції Національної поліції України спостерігається значна кількість фактів учинення зазначеного виду шахрайства. Зокрема, у 2023 році кіберполіцейськими було виявлено 3,6 тис. кіберзлочинів, а у 2024 році в Україні зареєстровано 2,5 тис. таких правопорушень. Нині, у зв'язку з безпрецедентною військовою агресією російської федерації, зазначені протиправні дії дедалі частіше спрямовуються на підрив нормальної діяльності державних установ та правоохоронних органів України.

Як приклад, наведемо таку ситуацію. *Зокрема, гр. Х., який раніше був військовослужбовцем Служби безпеки України та займав посаду начальника відділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки ГУ СБ України в АРК, разом з гр. Є., який раніше був його заступником, увійшли до складу хакерського угруповання за безпосереднього кураторства співробітників ФСБ рф, завданням якого була розвідувально-підривна діяльність проти України в інформаційній сфері. Указане хакерське угруповання з березня 2014 року та щонайменше по березень 2021 року координувалося співробітниками ФСБ рф. Головною метою його діяльності було проведення цілеспрямованих акцій кіберрозвідки проти державних органів України для отримання розвідувальної інформації. Так, хакерське угруповання в зазначений період часу здійснювало кіберрозвідку та кібератаки, направлені на несанкціоноване втручання в роботу ЕОТ та автоматизованих систем органів державної влади, правоохоронних органів і спецслужб України, а саме: Секретаріату Кабінету Міністрів України; Міністерства розвитку економіки, торгівлі та сільського господарства України; Міністерство закордонних справ України; Міністерства оборони України, Національної комісії зі стандартів державної мови; Державної інспекції ядерного регулювання України, військових частин (сфера управління Міністерства оборони України), ко-*

ристувацьких ПЕОМ співробітників Державного бюро розслідувань, Служби безпеки України, Національної поліції тощо, з метою створення прихованих технічних каналів витоку інформації, збору конфіденційної інформації, викрадення ідентифікаторів доступу та персональних даних насамперед співробітників правоохоронних органів, військових підрозділів, блокування роботи державних і корпоративних електронних ресурсів України, проведення акцій кібернетичного впливу в інтересах спеціальних та розвідувальних органів рф[1]. І це, на жаль, не поодинокий випадок.

Зазначене вище підтверджується й інформацією з відкритих джерел. Приміром, окремі автори наголошують, що «… урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, у 2024 році опрацювала 4315 кіберінцидентів. Це на 69,8 % більше, ніж роком раніше, коли кіберзлочинці атакували український кіберпростір 2541 раз. Найчастіше зловмисники атакують місцеві органи влади, уряд та урядові організації, сектор безпеки та оборони, енергетичний сектор, комерційні організації, телекомунікації. Найпоширенішими типами інцидентів є розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису або системи. Метою зловмисників є викрадення чутливої інформації, а також знищення даних та інформаційних систем. В урядовій команді припускають, що рф продовжить застосовувати усі можливі методи для отримання інформації важливої для ворога. Не припинятимуться й деструктивні атаки проти об'єктів критичної інфраструктури, зокрема енергетики»[2].

У розрізі сказаного вважаємо доречним навести тезу О. А. Самойленко, яка на основі аналізу сучасного контенту інтернет-простору серед умовних сфер суспільного життя учасників відносин у кіберпросторі виокремила такі, як:

– фінансово-економічна – пов'язана зі здійсненням розрахункових операцій та укладанням цивільно-правових угод;

– соціальна – пов'язана із системою соціальних зв'язків між користувачами електронних мереж як суб'єктами кібернетичного соціуму з приводу реалізації ними своїх соціальних потреб (ідеться про організацію людиною свого дозвілля; задоволення освітніх, інтелектуальних та інших потреб, оплатно або безоплатно);

– державно-політична – пов'язана із запровадженням так званого «електронного уряду», що має забезпечити надання органами влади послуг фізичним та юридичним особам, а також зі створенням централізованих баз даних,

[1] Справа № 760/8515/23. Архів Солом'янського районного суду м. Києва, 2024 р.

[2] Хакери за рік посилили атаки на український кіберпростір майже на 70 % – Держспецзв'язку. URL: https://sprotyv.info/news/hakeri-za-rik-posilili-ataki-na-ukraïnskij-kiberprostir-majzhe-na-70-derzhspeczzvyazku/ (дата звернення: 12.09.2025).

заснованих на технології забезпечення електронного документообігу в державних органах, у різних галузях промисловості й економіки, зокрема на підприємствах, що мають стратегічне значення для безпеки держави, під час організації та проведення виборів;

– світоглядна (ідейна чи духовна) – пов'язана із впливом на масову свідомість система цінностей членів певної групи суспільства (за мовним критерієм, національною, расовою або релігійною приналежністю, іншою ознакою, наприклад, професією)[3].

Також варто наголосити на постійній «цифровізації» усіх процесів, а також розвиток криптовалютної індустрії. З цього приводу окрема група дослідників констатувала, що криптовалютна індустрія поки що перебуває на стадії становлення, а її надскладні технології далеко не завжди достатньо захищені. Крім того, малодосвідчені користувачі часто припускаються серйозних помилок у захисті своїх активів. Це дає кваліфікованим хакерам різноманітні можливості отримати доступ як до криптовалютних бірж, так і до приватних криптогаманців. Найвідоміші викрадення сягають десятків мільйонів доларів:

1. Криптовалютна компанія Bybit – викрадено 1,5 млрд дол. США в ETH[4] (Ethereum). Злом відбувся 21 лютого 2025 року. Тоді криптобіржа Bybit повідомила, що зловмисники викрали активи з її ethereum-гаманця. Дубайська платформа втратила колосальну суму у вигляді 400 000 ETH за лічені хвилини через витік приватного ключа в системі так званих гарячих гаманців (тобто криптогаманців, до яких можна підєднатися через інтернет). Хакери використали вразливості безпеки, щоб вивести активи. Цей інцидент вважається найбільшою крадіжкою в історії криптоіндустрії на сьогодні.

2. Блокчейн-проєкт Ronin – викрадено 615 млн дол. США. 23 березня 2022 року зловмисники викрали з мережі Ronin приблизно 173 600 токенів Ethereum і 25,5 млн USDC[5]. Згодом стало відомо, що хакер отримав доступ до викрадених приватних ключів, необхідних для управління криптоактивами. Це й дозволило йому вивести кошти.

3. Обмінний сервіс Coincheck – викрадено 534 млн дол. у NEM[6]. У січні 2018 року хакери зламали Coincheck, викравши криптовалюту NEM. Біржа одразу призупинила всі операції, проте збитків уже було завдано. Coincheck повідомила, що, можливо, не зможе повністю компенсувати втрати користувачів. Для здійснення злочину хакери використали фішингову атаку для прони-

[3] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

[4] Ether (ETH) – головна криптовалюта, що забезпечує функціонування мережі Ethereum.

[5] USD Coin (USDC) – централізована криптовалюта, ціна якої прив'язана до долара США (стейблкоїн).

[6] NEM, New Economy Movement (новий рух економіки) – криптовалюта, написана на Java і JavaScript. Запущена 31 березня 2015 року.

кнення в гарячі гаманці, після чого встановили шкідливий софт для переведення активів. Хакер у темному капюшоні, який працює за ноутбуком, на екрані якого видно символ біткоїна з тріщиною та код, що символізує кібератаку на криптовалюту.

4. Сервіс обміну криптовалют FTX – викрадено 477 млн дол. США у різних криптовалютах. У листопаді 2022 року криптобіржа FTX оголосила про банкрутство через нецільове управління, незаконне привласнення активів і хакерські атаки. Інцидент, імовірно, пов'язаний з діями інсайдера.

5. Біржа біткоїнів Mt. Gox – викрадено 460 млн дол. у BTC (Bitcoin)[7]. Японська біржа Mt. Gox, що колись була світовим лідером у своїй сфері, зазнала атаки в 2011 році, втративши біткоїни на 8,75 млн дол. Попри обіцянки посилити безпеку, у 2014 році платформа пережила ще один, масштабніший, злом. Хакери викрали біткоїни на суму 460 млн дол., створивши потік фальшивих транзакцій для перевантаження системи. Цей інцидент став одним із перших великих зломів у світі біткоїна. Автори роблять слушний висновок, що зловмисники використовують різноманітні способи для отримання доступу до чужих криптогаманців, але найпоширенішими причинами є фішинг, крадіжка приватних ключів та використання вразливостей у смартконтрактах[8].

Як бачимо, відсутність відповідного регулювання кібервідносин та, найголовніше, обмежена обізнаність пересічних осіб допомагають виникненню вказаних ситуацій.

Однією з перших публікацій з приводу характеристики комп'ютерної злочинності варто вважати статтю Г. В. Загіки, який зауважував, що й великі компанії (приміром, Apple Computer) можуть бути потерпілими від кібератак, як-от: «… у грудні 1987 року ця фірма знайшла вірус у своїй системі електронної пошти. Цьому вірусу вдалося знищити всі мовні повідомлення та відключити систему. … напад на фінансові організації вчинюється у багатьох випадках її службовцями, які є професіоналами своєї справи. Зокрема, дослідник зауважив, що проведені у США опитування показують, що саме службовці, які мають знання в галузі комп'ютерної техніки, відіграють головну роль у вчиненні комп'ютерних протиправних діянь, адже без застосування криптографічних методів захисту інформації практично неможливо реально захистити інформацію. Сучасна криптографія базується на новітніх досягненнях математики, фізики, інженерних дисциплін та в галузі розробки й використання комп'ютерних технологій. До правових норм слід віднести розробку та прийняття норм, які встановлюють відповідальність за порушення інтелектуальної

[7] Bitcoin – однорангова цифрова валюта, усі транзакції відбуваються безпосередньо між рівними, незалежними користувачами мережі без посередника, який би здійснював дозвільні або операційні функції, перша в історії криптовалюта, яка дійсно ввійшла в обіг.

[8] ТОП-5 найбільших криптовалютних зломів в історії. URL: https://datami.ee/ua/blog/top-5-largest-cryptocurrency-hacks-in-history/ (дата звернення: 19.09.2025).

власності, за комп'ютерні правопорушення»[9].

У розрізі зазначеного вважаємо необхідним підтримати твердження О. А. Самойленко, яка констатувала, що специфічні особливості кримінальних правопорушень, які вчиняються в кіберпросторі, зумовлені насамперед тією обстановкою, яка існує в названому середовищі. Як вказує авторка, такі протиправні діяння згідно з Довідником № 9 до на той момент чинного Положення про порядок ведення Єдиного реєстру досудових розслідувань реєструються в Україні, як «вчинені з використанням високих інформаційних технологій і телекомунікаційних мереж», тобто в їх найменуванні акцент робиться на засобах вчинення – інформаційних технологіях і телекомунікаційних мережах. На думку дослідниці, доцільніше вживати термін «кіберпростір», оскільки він акцентує на специфічному середовищі вчинення кримінальних правопорушень. Це середовище характеризується сукупністю факторів, які зумовлюють вибір способів злочинної діяльності, особливості формування її слідів, а відтак – специфіку виявлення та розслідування таких протиправних діянь[10].

Водночас у Довіднику № 9 до чинного Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення, зазначене вище формулювання було звужене до: «з використанням інформаційних телекомунікаційних систем»[11].

Як бачимо, законодавець досі не відреагував на пропозицію А. О. Самойленко. Своєю чергою, ми також радимо дослухатись до нашої думки та все ж таки внести зміни у Довідник № 9 до Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення, а саме: «Кримінальні правопорушення, що вчинені (пов'язані): …89 у кіберпросторі».

Інша група дослідників також застосовує термін «кіберпростір». Зокрема, автори надають характеристику криміналістичних особливостей початкового етапу розслідування протиправних діянь з фінансовими ресурсами у кіберпосторі, визначають його значення, аналіз та обґрунтування як одного з видів кіберзлочинності, що є небезпечним для кожного, і доведення необхідності здійснення невідкладних заходів щодо попередження та протидії такому кримінальному правопорушенню[12].

О. Ю. Довженко зауважував, що злочинна діяльність, так само, як і все людське життя, стає все більш «діджиталізованою». Крім того, автор відзначив, що «… злочини в комп'ютерній сфері (кіберзлочини) виникли практично

---

[9] Загіка Г. В. Кримінологічна характеристика комп'ютерної злочинності. *Правова держава*. 2002. № 4. С. 56–61.

[10] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

[11] Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення : затв. наказом Офісу Генерального прокурора від 30.06.2020 р. № 298. URL: https://zakon.rada.gov.ua/laws/show/v0298905-20#Text (дата звернення: 13.09.2025).

[12] Reznik, O., Fomenko, A., Melnychenko, A., Pavlova, N., Prozorov, A. Features Of The Initial Stage Of Investigating Fraud With Financial Resources In Cyberspace. *Amazonia Investiga.* 2021. Volumer10 . Issue 41: pp. 141–150.

одночасно з виникненням цих технологій та розвивалися паралельно з ними. З удосконаленням технологій удосконалювалися і способи діяльності злочинців. Разом із тим, протягом тривалого часу злочини, які були скоєні за допомогою електронних обчислювальних пристроїв, не усвідомлювалися в якості окремої самостійної кримінально-правової категорії. Вони розглядалися як одна з форм звичайних злочинів, таких, як злочини проти власності чи проти комерційної таємниці. Лише виникнення розвинутих комп'ютерних мереж, а разом з ними й поява можливостей зі злочинного впливу через ці мережі, який міг би призводити до масштабних згубних наслідків, призвів до усвідомлення необхідності виділення комп'ютерних злочинів в особливу групу»[13].

Стосовно досліджень закордонних авторів, одразу процитуємо публікацію Джеймса Е. Льюіса, який ще в 2002 році констатував, що кібератаки, мережева безпека та інформація створюють складні проблеми, які стосуються нових сфер національної безпеки та державної політики. У наведеній статті дослідник розглядає комплекс питань, пов'язаних з кібертероризмом та кібератаками на критичну інфраструктуру та їх наслідками для національної безпеки. Науковець зауважує, що кібертероризм – це використання комп'ютерних мережевих інструментів для вимкнення критичної національної інфраструктури (такої як енергетика, транспорт, державні операції) або для примусу чи залякування уряду чи цивільного населення. Передумовою ж кібертероризму Джеймс Е. Льюіс визначає залежність країн та їх критичних інфраструктур від комп'ютерних мереж, що відповідно створює нові вразливості – «масивну електронну ахіллесову п'яту». Автор робить висновок, що ворожа країна або група може використати ці вразливості, щоб проникнути в погано захищену комп'ютерну мережу та порушити або навіть вимкнути критично важливі функції[14].

Своєю чергою, В. Клейм у 2005 році в публікації для Конгресу США стосовно вразливих місць та політичних питань комп'ютерних атак і кібертероризму зауважував, що на часі велика кількість інтернаціональних терористичних груп застосовують ПЕОМ та мережу Інтернет для дестабілізації комп'ютерної системи США. Крім того, автор відмічає, що вказані кібератаки порушують діяльність цивільних критичних інфраструктур та державних органів[15].

Наразі, як було зазначено вище, Україна вже понад 10 років перебуває під кібератаками хакерських угруповань рф.

---

[13] Довженко О. Ю. Основи методики розслідування кіберзлочинів : автореф. дис. … канд. юрид. наук : 12.00.09 / Харків. нац. ун-т внутр. справ. Харків, 2020. 18 с.

[14] James, A. Lewis Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. URL: https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats (дата звернення: 16.09.2025).

[15] Clay, W. Computer Attack and Cyberterrorism : Vulnerabilities and Policy Issues for Congress. URL: https://digital.library.unt.edu/ark:/67531/metacrs6315/m1/1/ (дата звернення: 06.09.2025).

Як приклад, наведемо таку ситуацію. *Зокрема, у період не пізніше 25 січня 2023 року гр. Ж., перебуваючи в с. Світлогірському Полтавського району Полтавської області, будучи активною учасницею обговорень у телеграм-каналах та групах, що контролювалися представниками рф, отримала від одного з них пропозицію виконувати обов'язки адміністратора телеграм-каналу. Зазначені обов'язки передбачали цілеспрямоване розміщення інформаційних матеріалів, які містили виправдовування, визнання правомірною або заперечення тимчасової окупації рф території України та її збройної агресії проти України, глорифікацію учасників агресії, пропаганду російського нацистського тоталітарного режиму та іншу проросійську пропаганду. На цю пропозицію гр. Ж. погодилася.*

Після цього вона розпочала адміністрування створених представниками держави-агресора телеграм-каналів та спільнот і надалі систематично здійснювала вищезазначені дії як адміністратор[16]*. І знову ж, це, на жаль, не поодинокий випадок.*

Наостанок наведемо твердження Л. М. Танцер, яка відмітила, що кібертероризм – це поєднання тероризму та кіберпростору. Авторка зауважила, що зазвичай під ним розуміють незаконні атаки та погрози атаками на комп'ютери, мережі та інформацію, що зберігається в них, коли вони здійснюються з метою залякування або примусу уряду чи його громадян для досягнення політичних чи соціальних цілей. Крім того, дослідниця констатувала, щоб кваліфікуватися як кібертероризм, атака повинна призвести до насильства стосовно осіб чи майна або принаймні завдати достатньої шкоди, щоб викликати страх. Прикладами можуть бути атаки, що призводять до смерті або тілесних ушкоджень, вибухів, авіакатастроф, забруднення води або серйозних економічних втрат. Серйозні атаки на критичну інфраструктуру можуть бути актами кібертероризму, залежно від їхнього впливу.

У той час, як атаки, на думку авторки, які порушують роботу несуттєвих сфер діяльності, такими вважатися не будуть[17].

Стосовно нормативно-правового забезпечення звернемося до аналізу, проведеного В. В. Сисолятіним[18]. Зокрема, автор вказував, що в Конвенції про кіберзлочинність, ратифікованій Україною 07 вересня 2005 року, визначено,

[16] Справа № 953/9907/24. Архів Київського районного суду м. Харкова, 2024 р.

[17] Tanczer, L. M. (2017) The Terrorist – Hacker/Hacktivist Distinction: An Investigation of Self-Identified Hackers and Hacktivists. *NATO Science for Peace and Security Series – E : Human and Societal Dynamics*, Volume 136, pp. 77–92. URL: https://ebooks.iospress.nl/volumearticle/46545 (дата звернення: 13.09.2025).

[18] Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2024. 230 с.

які правопорушення вчиняються за допомогою комп'ютерних систем. У зазначеному документі вказано такі групи протиправних діянь: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ (стаття 2), нелегальне перехоплення (стаття 3), втручання у дані (стаття 4), втручання у систему (стаття 5), зловживання пристроями (стаття 6); правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами (стаття 7), шахрайство, пов'язане з комп'ютерами (стаття 8); правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією (стаття 9); правопорушення, пов'язані з порушенням авторських та суміжних прав (стаття 10)[19].

В. В. Сисолятін констатував, що ще на початку 2000-х років міжнародні законодавці розуміли необхідність визначити конкретні протиправні діяння, які можуть здійснюватися з використанням комп'ютерних систем[20].

Також у визначеній Конвенції передбачено, що сторонами вживаються:

– законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до внутрішнього законодавства за навмисну допомогу чи співучасть у вчиненні будь-якого зі злочинів (стаття 11);

– законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і в якості частини органу такої юридичної особи (стаття 12);

– законодавчі та інші заходи, які можуть бути необхідними для визначення повноважень і процедур, передбачених цією частиною, з метою конкретних кримінальних розслідувань або переслідувань (стаття 14);

– встановлення, імплементацію і застосування повноважень і процедур, передбачених цією частиною, регулювалися умовами і запобіжними заходами, передбаченими її внутрішньодержавним правом, які б забезпечували адекватний захист прав і свобод людини (стаття 15)[21].

З огляду на зазначене В. В. Сисолятін робить висновок, що вказані заходи відображають максимально широкі повноваження кожної держави, яка ратифікувала зазначену конвенцію (у тому числі й України)[22].

---

[19] Конвенція про кіберзлочинність : підписана в м. Будапешті 23 листопада 2001 року. URL: http://zakon0.rada.gov.ua/laws/show/994_575 (дата звернення: 06.09.2025).

[20] Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2024. 230 с.

[21] Конвенція про кіберзлочинність : підписана в м. Будапешті 23 листопада 2001 року. URL: http://zakon0.rada.gov.ua/laws/show/994_575 (дата звернення: 06.09.2025).

[22] Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2024. 230 с.

Крім того, менше ніж через два роки було підписано Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, ратифікований Україною 21 липня 2006 року. У цьому документі надано визначення расистського та ксенофобного матеріалу, а саме вказано, що це будь-який письмовий матеріал, будь-яке зображення чи будь-яке інше представлення ідей або теорій, які захищають, сприяють або підбурюють до ненависті, дискримінації чи насильства проти будь-якої особи або групи осіб за ознаками раси, кольору шкіри, національного або етнічного походження, а також віросповідання, якщо вони використовуються як привід для будь-якої з цих дій (стаття 2)[23].

Тобто, у Додатковому протоколі визначено нагальні на той час питання дискримінації осіб за ознаками раси, кольору шкіри, національного або етнічного походження, а також віросповідання. Указані аспекти є й зараз актуальними в Україні, адже неодноразово виникають ситуації, пов'язані з нетерпимістю осіб через національне або етнічне походження та віросповідання[24].

У Додатковому протоколі теж передбачено, що сторонами вживаються такі заходи:

– законодавчі й інші заходи, які можуть бути необхідними для визнання у її національному законодавстві злочинами, у разі умисного вчинення без права на це, таких дій: розповсюдження або іншим чином надання громадськості доступу через комп'ютерні системи до расистського та ксенофобного матеріалу (стаття 3);

– законодавчі й інші заходи, які можуть бути необхідними для визнання у її національному законодавстві злочинами, у разі умисного вчинення без права на це, таких дій: погроза, зроблена через комп'ютерну систему, вчинення тяжкого злочину, визначеного в її національному законодавстві, проти (і) осіб з причини їх належності до групи, яка відрізняється за ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням, якщо вони використовуються як привід для будь-якої з цих дій; або (і) групи осіб, яка відрізняється за будь-якою з цих характеристик (стаття 4);

– законодавчі й інші заходи, які можуть бути необхідними для визнання у її національному законодавстві злочинами, у разі умисного вчинення без права на це, таких дій: публічна образа через комп'ютерну систему (і) осіб з причини їх належності до групи, яка відрізняється за ознаками раси, кольору шкіри, національним або етнічним походженням, а також віросповіданням,

[23] Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : підписаний в м. Страсбург 28 січня 2003 року. URL : http://zakon0.rada.gov.ua/laws/show/994_687 (дата звернення:06.09.2025).

[24] Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2024. 230 с.

якщо вони використовуються як привід для будь-якої з цих дій; або (і) групи осіб, яка відрізняється за будь-якою з цих характеристик (стаття 5);

– законодавчі й інші заходи, які можуть бути необхідними для визнання таких дій кримінальними правопорушеннями у її національному законодавстві, у разі умисного вчинення без права на це: розповсюдження або іншим чином надання громадськості доступу через комп'ютерні системи до матеріалу, який заперечує, значно мінімізує, схвалює або виправдовує дії, які є геноцидом або злочинами проти людства (стаття 6);

– законодавчі й інші заходи, які можуть бути необхідними для визнання кримінальними правопорушеннями у її національному законодавстві, у разі умисного вчинення без права на це, пособництва або підбурювання до вчинення будь-якого з правопорушень, визначених відповідно до цього Протоколу, з наміром вчинити таке кримінальне правопорушення[25].

Ми підтримуємо позицію В. В. Сисолятіна, який, проаналізувавши КК України[26] та ряд інших нормативно-правових актів, зробив висновок, що заходи, визначені як Конвенцією, так і Додатковим протоколом до неї, майже повністю імплементовані в правове поле нашої держави[27].

Зокрема, рішенням Ради національної безпеки і оборони України ще 2016 р. було схвалено проєкт Стратегії кібербезпеки України[28], відповідно до якої було прийнято ряд законодавчих та інших актів. Для прикладу, у тому самому році Указом Президента України було створено Національний координаційний центр кібербезпеки, серед основних завдань якого було визначено такі: «… здійснення координації та контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку; здійснення аналізу: стану кібербезпеки; стану кіберзахисту критично важливих об'єктів інфраструктури» та інші[29].

А вже в Законі України «Про основні засади забезпечення кібербезпеки України» надано ряд основоположних визначень: індикатори кіберзагроз; інформація про інцидент кібербезпеки; інцидент кібербезпеки (кіберінцидент);

[25] Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : підписаний в м. Страсбург 28 січня 2003 року. URL: http://zakon0.rada.gov.ua/laws/show/994_687 (дата звернення: 06.09.2025).

[26] Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14/page#Text (дата звернення: 12.09.2025).

[27] Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2024. 230 с.

[28] Про Стратегію кібербезпеки України : рішення Ради національної безпеки і оборони України від 27.01.2016 р. Уведено в дію Указом Президента України від 15 березня 2016 року № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/n0003525-16#Text (дата звернення: 05.09.2025).

[29] Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 р. № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 05.09.2025).

кібератака; кібербезпека; кіберзагроза; кіберзахист; кіберзлочин (комп'ютерний злочин); кіберзлочинність; кібероборона; кіберпростір; кіберрозвідка; кібертероризм; кібершпигунство; критична інформаційна інфраструктура та інші. Також у вказаному законодавчому акті визначено відповідних суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки:

– міністерства та інші центральні органи виконавчої влади;

– місцеві державні адміністрації;

– органи місцевого самоврядування;

– правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

– Збройні Сили України, інші військові формування, утворені відповідно до закону;

– Національний банк України;

– підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

– суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Крім того, у вказаному Законі зазначено основних суб'єктів національної системи кібербезпеки, а саме: Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України[30].

У статті 1 Закону України «Про захист інформації в інформаційно-комунікаційних системах» надано перелік термінів, які використовуються для позначення окремих категорій досліджуваної тематики, як-от:

– виток інформації – результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

– захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

– інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які в процесі обробки інформації діють як єдине ціле;

– криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних

[30] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2163-19 (дата звернення: 06.09.2025).

(ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

– порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст тощо[31].

Також і в статті 3 Закону України «Про електронну комерцію» наведено ряд понять, що використовуються для позначення окремих категорій досліджуваної тематики, зокрема:

– електронний підпис одноразовим ідентифікатором – дані в електронній формі у вигляді алфавітно-цифрової послідовності, що додаються до інших електронних даних особою, яка прийняла пропозицію (оферту) укласти електронний договір, та надсилаються іншій стороні цього договору;

– інтернет-магазин – засіб для представлення або реалізації товару, роботи чи послуги шляхом вчинення електронного правочину;

– реалізація товару дистанційним способом – укладення електронного договору на підставі ознайомлення покупця з описом товару, наданим продавцем у порядку, визначеному цим Законом, шляхом забезпечення доступу до каталогів, проспектів, буклетів, фотографій тощо з використанням інформаційно-комунікаційних систем, телевізійним, поштовим, радіозв'язком або в інший спосіб, що виключає можливість безпосереднього ознайомлення покупця з товаром або із зразками товару під час укладення такого договору[32].

Стосовно нових правил посиленої кібербезпеки в Євросоюзі. Зокрема, прийнята нова директива з кібербезпеки NIS 2 із січня 2023 року запроваджує обов'язкові заходи інформаційної безпеки та вимоги до звітності про інциденти інформаційної безпеки. Серед них слід вказати те, що за невиконання цих вимог багато компаній у певних секторах будуть піддаватися значним штрафам. До 9 травня 2018 року всі країни – члени ЄС повинні були внести цей акт у своє національне законодавство. NIS2 набула чинності 16 січня 2023 року та повністю замінила попередню директиву про безпеку мереж та інформаційних систем (NIS) 17 жовтня 2024 року. Адже вказана директива встановлює вимоги до організацій, що надають найважливіші послуги у сфері енергетики, логістики, фінансів, охорони здоров'я, комунальних служб, цифрової інфраструктури, промисловості, державного управління та досліджень[33].

Як слушно зауважив В. В. Сисолятін, поки що Україна не входить до країн ЄС та не зобов'язана ратифікувати згадану вище Директиву. Проте, незважаючи на прийняті нормативно-правові акти, кількість звернень за фактами

[31] Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL : https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 09.09.2025).

[32] Про електронну комерцію : Закон України від 03.09.2015 р. № 675-VIII. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text (дата звернення: 09.09.2025).

[33] Директива кібербезпеки NIS 2. URL: https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua#:~:text=NIS%20(the%20security%20of%20network,пошуковиків%20і%20сервісів%20хмарних%20обчислень (дата звернення: 15.09.2025).

вчинення кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, 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[34].

Стосовно класифікації кримінальних правопорушень у кіберпросторі згадаємо, приміром, Б. В. Щура, який зауважив, що «… спроби створити криміналістичні класифікації протиправних діянь за криміналістичними критеріями є схвальними та потребують подальших наукових досліджень. Не можна обмежуватися у класифікаційних побудовах лише криміналістичними ознаками (критеріями), а необхідно виходити з кримінально-правової класифікації злочинів, яка у цьому сенсі, фактично є базовою. Прагматична роль криміналістичної класифікації злочинів, на думку автора, полягає в тому, що вона є основою для вироблення цілеспрямованих наукових рекомендацій та розроблення окремих криміналістичних методик. При цьому криміналістична класифікація злочинів передбачає врахування криміналістично значущих ознак»[35].

Своєю чергою, О. А. Самойленко у результаті узагальнення розгорнутих фабул кримінальних правопорушень, зареєстрованих Національною поліцією України в період з 30 листопада 2012 року до 01 листопада 2018 року (без урахування закритих за пунктами 1, 2, 4 і 6 частини 1 статті 284 КПК України), що відповідно позначені в обліку як «вчинені з використанням високих інформаційних технологій і телекомунікаційних мереж», з'ясувала, що вони охоплювали види протиправних діянь, кваліфікованих за такими статями КК України:

– 176 (Порушення авторського права і суміжних прав);

– 185 (Крадіжка);

– 190 (Шахрайство), частинами 3 і 4;

– 200 (Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення);

– 229 (Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару);

– 231 (Незаконне збирання з метою використання або використання відомостей, що становлять комерційну чи банківську таємницю);

– 301 (Ввезення, виготовлення, збут і розповсюдження порнографічних предметів), частинами 3, 4 та 5;

---

[34] Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2024. 230 с.

[35] Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : автореф. дис. … д-ра юрид. наук : 12.00.09 / Нац. юрид. ун-т імені Ярослава Мудрого. Харків, 2011. 32 с.

– 361–363[1] (розділ XVII «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж та мереж електрозв'язку»)[36].

Зі свого боку, О. Ю. Довженко констатував, що слід застосувати в кваліфікації кіберзлочинів розділи КК України, а саме:

«1. Злочини проти конституційних прав і свобод людини і громадянина. До них можна віднести порушення права на особисте та сімейне життя, порушення таємниці листування, порушення авторських і суміжних прав, що скоюються за допомогою комп'ютерних технологій чи мережі Інтернет.

2. Злочини проти життя та здоров'я населення, зокрема використання мережі Інтернет для розповсюдження заборонених чи обмежених у обігу речовин, таких як наркотики, психотропні речовини, ліки.

3. Злочини проти честі та гідності особи. До них можна віднести використання комп'ютерних технологій та мережі Інтернет для розповсюдження відомостей, що порочать честь та гідність особи.

4. Злочини проти власності. До них можна віднести викрадення грошових коштів з банківських рахунків, шахрайство та інші корисливі злочини, що ставлять на меті заволодіти власністю іншої особи з використанням комп'ютерних технологій і мережі Інтернет.

5. Злочини в сфері комп'ютерної інформації, зокрема неправомірний доступ до інформації, а також створення та використання шкідливих комп'ютерних програм.

6. Злочини проти суспільної моралі (найбільш відомим прикладом є виготовлення, зберігання й поширення порнографії, у тому числі дитячої).

7. Злочини проти безпеки держави, в тому числі, проти державної таємниці, скоєні з використанням комп'ютерних технологій чи мережі Інтернет.

8. Злочини терористичного характеру, зокрема заклики до тероризму, фінансування тероризму та безпосередньо акти кібертероризму»[37].

А вже В. В. Сисолятін привів класифікацію кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, засновану на характерних ознаках, таких як спосіб та умови їх вчинення, а саме:

«– кримінальні правопорушення, пов'язані з використанням інтернет-банкінгу, у сфері власності;

– кримінальні правопорушення, пов'язані з використанням інтернет-банкінгу, у сфері господарської діяльності;

– кримінальні правопорушення, пов'язані з використанням інтернет-ба-

[36] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

[37] Довженко О. Ю. Класифікація кіберзлочинів у криміналістиці. *Південноукраїнський правничий часопис*. 2019. № 1. С. 19–22.

нкінгу, у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку»[38].

На основі аналізу наведених вище праць науковців надамо власну класифікацію кримінальних правопорушень у кіберпросторі, як-от:

– кримінальні правопорушення у кіберпросторі проти основ національної безпеки України;

– кримінальні правопорушення у кіберпросторі у сфері власності;

– кримінальні правопорушення у кіберпросторі у сфері господарської діяльності;

– кримінальні правопорушення у кіберпросторі у сфері моральності;

– кримінальні правопорушення у кіберпросторі у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– кібертероризм, який поєднує перераховані вище кримінальні правопорушення.

Констатуючи зазначене, варто вказати, що дослідження методики розслідування кримінальних правопорушень у кіберпросторі є перспективними як для науки, так і для практичної діяльності працівників правоохоронних органів.

1.2. Криміналістична характеристика як складова методики розслідування кримінальних правопорушень у кіберпросторі

Будь-яка методика розслідування окремих видів кримінальних правопорушень має певну структуру, важливим елементом якої є криміналістична характеристика. Поняття криміналістичної характеристики як елемента методики, кількість, зміст і значення структурних елементів цієї наукової категорії залишаються невизначеними та суперечливими. Більше того, на межі тисячоліть гостро постало питання щодо доцільності існування криміналістичної характеристики як наукової категорії загалом. Тому слід мати на увазі, що значення криміналістичної характеристики можна розділити на практичне та теоретичне. Для працівників поліції, які безпосередньо займаються розслідуванням, найбільш важливим є практичне застосування того чи іншого засобу, що допоможе у процесі розслідування. Тобто, дійсна цінність криміналістичної характеристики того чи іншого виду кримінального правопорушення – це можливість її практичного застосування, можливість вирішити певні питання з

[38] Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2024. 230 с.

огляду на неї та, звичайно, можливість, спираючись на неї, спростити розслідування певної категорії протиправних діянь[39].

Загалом, стосовно методики розслідування окремих видів кримінальних правопорушень окрема група вчених-криміналістів (Б. Є. Лук'янчиков, Є. Д. Лук'янчиков, С. Ю. Петряєв) зауважує, що вказана наукова категорія має такі складові:

– криміналістична характеристика такого виду злочинів;

– обставини, що підлягають доказуванню; типові слідчі ситуації, що виникають на різних етапах розслідування, слідчі версії та планування;

– особливості виявлення того чи іншого виду злочинів (внесення відомостей до ЄРДР);

– початковий етап розслідування, тактика проведення першочергових слідчих (розшукових) дій гласного та негласного характеру;

– наступний етап розслідування, тактика проведення окремих слідчих (розшукових) дій на цьому етапі;

– особливості взаємодії слідчого з оперативними підрозділами;

– особливості використання слідчим спеціальних знань в процесі розслідування;

– заходи криміналістичної профілактики за матеріалами досудового розслідування[40].

У розрізі зазначеного вважаємо доречною думку В. А. Журавля, який відмічав, що «… криміналістична методика виникла в результаті інтеграції та диференціації наукових знань та об'єднує в собі передові досягнення криміналістичної техніки й тактики, відповідно, щодо оптимальної організації розслідування злочинів і судового розгляду певних категорій кримінальних проваджень»[41].

Окрема група дослідників (К. О. Чаплинський, О. В. Лускатов, В. М. Плетенець) визначили в структурі вказаної криміналістичної категорії такі складові:

– криміналістична характеристика злочину окремого виду (групи);

– організація та планування розслідування на початковому етапі стосовно існуючих типових слідчих ситуацій;

– слідчі (розшукові) й інші дії та заходи відповідно до типових слідчих ситуацій на подальшому етапі розслідування;

---

[39] Єфімов М. М. Криміналістична характеристика як елемент методики розслідування кримінальних правопорушень проти моральності. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. № 3. С. 161–167.

[40] Лук'янчиков Б. Є., Лук'янчиков Є. Д., Петряєв С. Ю. Криміналістика : навч. посіб. для студ. юрид. спец. вищ. навч. закл. : у 2 ч. Ч. II : Криміналістична тактика. Методика розслідування. Київ : НТУУ «Київський політехнічний інститут ім. Ігоря Сікорського», 2017. 505 с.

[41] Журавель В. А. Криміналістичні методики: сучасні наукові концепції. Харків : Апостіль, 2012. 304 с.

– профілактична діяльність слідчого[42].

Своєю чергою, інша група науковців у структурі методики розслідування окремих видів кримінальних правопорушень вирізняє такі елементи:

– криміналістична характеристика кримінальних правопорушень;

– аналіз первинної інформації та початок кримінального провадження; обставини, що підлягають встановленню у кримінальному провадженні;

– типові слідчі ситуації досудового розслідування;

– особливості проведення початкових слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів;

– особливості проведення подальших слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів;

– особливості використання спеціальних знань під час розслідування кримінальних правопорушень;

– профілактична діяльність уповноважених осіб;

– особливості діяльності уповноважених осіб на завершальному етапі досудового розслідування[43].

О. М. Дуфенюк вказувала, що методика розслідування кримінальних правопорушень – це логічна побудова, «…складові якої повинні різнобічно забезпечувати уповноважену особу теоретичними знаннями щодо оптимального та ефективного ходу досудового розслідування. У структурі окремої криміналістичної методики виділяються наступні складові:

1. Криміналістична характеристика злочину.

2. Особливості збирання, аналізу та оцінювання інформації на стадії внесення відомостей до ЄРДР.

3. Обставини, що підлягають установленню під час кримінального провадження.

4. Типові слідчі ситуації, що виникають під час розслідування злочину.

5. Типові слідчі версії та планування досудового розслідування злочину.

6. Типові слідчі дії на початковому, подальшому та завершальному етапах розслідування злочину.

7. Особливості застосування науково-технічних засобів і спеціальних знань.

8. Профілактична робота слідчого за матеріалами розслідування.

9. Взаємодія слідчих, оперативно-розшукових, експертних та інших підрозділів у практичній діяльності розслідування злочинів»[44].

Водночас цілком поділяємо думку групи науковців (А. В Іщенко, В. В. Тіщенко), які зауважили, що під міжвидовою (комплексною) методикою

---

[42] Криміналістика : підруч. для студ. вищ. навч. закл. / К. О. Чаплинський та ін. Дніпро : Дніпропетр. держ. ун-т внутр. справ ; Ліра ЛТД, 2017. 419 с.

[43] Єфімов М. М., Пиріг І. В. Методика розслідування окремих видів кримінальних правопорушень : підручник. Дніпро : Видавець Біла К. О., 2022. 271 с.

[44] Криміналістика : підручник / за заг. ред. Є. В. Пряхіна. 3-тє вид., переробл. та допов. Львів : ЛьвДУВС, 2016. 948 с.

розуміється не просто сукупність окремих видових методик, а їх загальна інтегрована модель, що виконує системоутворювальну й методологічну функцію. Тобто, розробки теоретичних основ криміналістичної методики ведуться в різних напрямах, що народжують нові підходи, уточнюючи, доповнюючи й оновлюючи відомі і, здавалося б, усталені наукові поняття та положення. Науковці вказують на те, що не завжди відрізняються принципи науково-теоретичної розробки приватних методик розслідування, з одного боку, і принципи застосування та побудови методики розслідування злочинів у практичній діяльності – з другого. У цьому зв'язку вчені підкреслюють, що формування криміналістичної методики розслідування обумовлюється визначенням тих теоретичних і методологічних передумов, на основі яких можна виявити загальні закономірності та взаємозв'язки, властиві основним об'єктам криміналістичного наукового дослідження: діяльності з розслідування злочинів, з одного боку, та діяльності з їх вчиненню – з іншого. Автори наголошують на тому, що зазначена мета може бути досягнута за допомогою дієвого, системного та функціонального підходів, що утворюють у своїй системі загальний комплексний підхід, і, будучи засобом пояснення, конструювання та прогнозування науково-методичних розробок[45][46].

Тобто, варто зробити висновок, що це дослідження є аналізом особливостей міжвидової методики – методики розслідування кримінальних правопорушень у кіберпросторі.

Структура вказаної наукової категорії, на нашу думку, має такий вигляд:

1) криміналістична характеристика;

2) аналіз первинних відомостей про вчинення кримінального правопорушення у кіберпросторі;

3) обставини, які підлягають встановленню;

4) типові слідчі ситуації та відповідний їм порядок дій уповноважених осіб;

5) взаємодія підрозділів правоохоронних органів та інших структур під час розслідування кримінальних правопорушень у кіберпросторі;

6) профілактична діяльність уповноважених осіб для встановлення причин та умов, що сприяли учиненню протиправних дій;

7) особливості реалізації початкових процесуальних дій та інших заходів;

8) особливості проведення подальших процесуальних дій та

[45] Тіщенко В. В. Криміналістичні технології в теорії і практиці розслідування. *Актуальні проблеми держави і права*. 2008. Вип. 44. С. 18–24.

[46] Іщенко А. В. Фундаментальні та прикладні криміналістичні категорії. *Актуальні проблеми розкриття та розслідування злочинів у сучасних умовах* : Міжнарод. наук.-практ. конф. (05 листоп. 2010 р., м. Запоріжжя). У 3 ч. Запоріжжя, 2010. Ч. 1. С. 180–182.

інших заходів;

9) особливості використання спеціальних знань.

Водночас, як було зазначено вище, неодмінною складовою визначеної наукової категорії ми вбачаємо такий елемент, як криміналістична характеристика кримінальних правопорушень у кіберпросторі.

Одразу наголосимо на тому, що єдина позиція щодо визначення сутності та наповнення вказаної категорії серед учених-криміналістів відсутня. Так, наприклад, А. В. Старушкевич визначає її як засновану на практиці правоохоронних органів і криміналістичних досліджень модель системи зведених відомостей про криміналістично значущі ознаки виду, групи або конкретного злочину, яка має на меті оптимізацію процесу розслідування злочинів[47].

На думку В. В. Лисенка, практична цінність цієї наукової категорії проявляється не лише у встановленні типових зв'язків між її елементами. Дослідник зауважив, що криміналістична характеристика може бути застосована лише за наявності нетипових особливостей окремих елементів чи зв'язків. Як підсумок, автор констатував, що до її змісту варто долучати інформацію про протиправні діяння, які мають одиничні прояви, оскільки зазначені нетипові прояви злочинної діяльності можуть мати поширення у майбутньому[48].

Також вважаємо досить доречним твердження А. Е. Жиліна, який стосовно розглядуваної криміналістичної категорії зауважив, що з приводу неї «… між дослідниками, починаючи з моменту її введення в структуру методики розслідування та до даного часу, ведуться постійні суперечки щодо нагальності існування вказаного елементу методики. Більшість науковців все ж таки підтримують обов'язковість її наявності в окремих методиках. Ба навіть деякі противники її існування наголошують на тому, що у випадках правильно побудованих кореляційних зв'язків криміналістична характеристика має право на існування»[49].

Як бачимо, автор указав на певну проблематику стосовно загальної обов'язковості включення вказаного елементу в структуру методики розслідування окремих видів кримінальних правопорушень.

Зі свого боку, В. В. Пясковський, Ю. М. Чорноус та А. В. Самодін формулюють криміналістичну характеристику злочинів як систему узагальнених

[47] Старушкевич А. В. Криміналістична характеристика злочинів : навч. посіб. Київ, 1997. 44 с.

[48] Лисенко В. В. Криміналістичне забезпечення діяльності податкової міліції (Теорія та практика) : монографія. Київ : Логос, 2004. 324 с.

[49] Жилін А. Е. Наукові диспути стосовно визначення криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів. *Науковий вісник публічного та приватного права*. 2022. Вип. 6. С. 122–127.

даних про найбільш типові ознаки певного виду (групи) кримінальних правопорушень, закономірний взаємозв'язок яких слугує основою наукового і практичного вирішення завдань розслідування[50].

Своєю чергою, окрема група науковців (О. В. Батюк, Р. І. Благута, О. М. Гумін) сформулювали її як систему відомостей про криміналістично значущі ознаки злочинів цього виду. Автори наголосили, що вона відображає закономірні зв'язки між цими ознаками і сприяє побудові й перевірці слідчих версій, що висуваються в процесі розслідування злочинів. Учені вказали, що криміналістичну характеристику можна уявити як ідеальну модель типових зв'язків і джерел доказової інформації, що дозволяють спрогнозувати оптимальний шлях і найбільш ефективні засоби розслідування окремих категорій злочинів[51].

Підтримуючи вказані позиції, дійсно зазначимо про те, що вважаємо криміналістичну характеристику інформаційною моделлю групи протиправних діянь певної категорії[52].

Також варто відмітити, що результати опитування працівників правоохоронних органів (додаток А) дозволили зробити висновок, що 91 % респондентів вказали одним із найбільш перспективних напрямів підвищення ефективності розслідування саме побудову системи сталих кореляційних зв'язків між елементами криміналістичної характеристики кримінальних правопорушень у кіберпросторі.

А вже О. М. Селезньова вказує на те, що немає потреби вважати інформаційні правовідносини такими, які створюються тільки в інформаційній сфері, оскільки розглядувані відносини можуть виникати і в інших сферах життєдіяльності, наприклад, у сфері цивільно-правового обороту, коли певний об'єкт інформаційних відносин стає предметом цивільного договору[53]. Тому ми поділяємо позицію Р. Л. Степанюка, який кореляційні зв'язки між елементами криміналістичної характеристики певної групи злочинів і можливість їх встановлення й використання при вирішенні завдань щодо виявлення і розслі-

[50] Криміналістика : підручник / за заг. ред. В. В. Пясковського. 2-ге вид., переробл. і допов. Харків : Право, 2020. 752 с.

[51] Методика розслідування окремих видів злочинів, підслідних органам внутрішніх справ : навч. посіб. / за заг. ред. Є. В. Пряхіна. Львів : ЛьвДУВС, 2011. 324 с.

[52] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[53] Селезньова О. М. Теоретико-методологічні основи інформаційного права України : монографія. Чернівці : Місто, 2014. 407 с.

дування злочинів має найбільше значення при дослідженні окремих кримінальних правопорушень[54]. Тобто, автор вказує на наявність сталих кореляційних зв'язків між елементами досліджуваної наукової категорії.

Крім того, Т. В. Вискарка досить слушно зауважує, що «… криміналістична характеристика є відносно новою категорією в сучасній криміналістиці, оскільки перші згадки про неї почалися лише в сімдесятих роках минулого сторіччя. Найбільшого розквіту її дослідження на теренах української науки почалося приблизно з 2010 року. Саме тоді майже всі вчені-криміналісти при висвітленні питань окремих методик розслідування кримінальних правопорушень вважали за необхідне розглянути і вказану складову. Як наслідок, зазначена категорія стала невід'ємною частиною будь-якої окремої методики»[55].

Наостанок наведемо думку В. Ю. Шепітько, який влучно вказує, що «… криміналістична характеристика злочинів – досить нова наукова категорія криміналістики, яка посідає центральне місце в методиці розслідування окремих видів злочинів. Криміналістична характеристика – це результат наукового аналізу та узагальнення типових ознак певного виду або роду злочинів. Вона відображає злочин і його складові елементи. Крім криміналістичної характеристики злочинів, існують кримінально-правова, кримінально-процесуальна, кримінологічна характеристики. Криміналістичною характеристикою називається система відомостей про криміналістично значущі ознаки злочинів даного виду, що відображає закономірні зв'язки між ними і слугує побудові та перевірці слідчих версій у розслідуванні злочинів. Її метою є оптимізація процесу розкриття і розслідування злочину. Призначення криміналістичної характеристики полягає в тому, що вона сприяє:

– розробленню окремих методик досудового розслідування;

– побудові типових програм і моделей розслідування злочинів;

– визначенню напряму розслідування конкретного злочину.

Ця характеристика слугує слідчому своєрідною інформаційною базою, набором відомостей про даний вид злочинів»[56].

Переходячи до питання наповнення елементами криміналістичної характеристики кримінальних правопорушень у кіберпросторі, одразу наведемо позицію вчених-криміналістів (В. С. Кузьмічов, Г. І. Прокопенко), які вказують на наявність серед її елементів:

– предмета безпосереднього злочинного посягання (найрізноманітніші об'єкти органічного та неорганічного походження);

– способу вчинення злочинів в його широкому розумінні (обставини

[54] Степанюк Р. Л. Сутність і практичне значення криміналістичної характеристики злочинів. *Порівняльно-аналітичне право.* 2014. № 5. С. 398–400.

[55] Вискарка Т. В. Криміналістична характеристика як елемент методики розслідування шахрайства у сфері використання банківських електронних платежів. *Науковий вісник публічного та приватного права*. 2021. Вип. 2. Т. 2. С. 105–110.

[56] Криміналістика : підручник / за ред. проф. В. Ю. Шепітька. 4-е вид., перероб. і допов. Харків : Право, 2008. 464 с.

приготування, вчинення і приховування злочину, характеристика дії суб'єкта, що використовується для досягнення поставленої мети);

– типової слідової картини злочину в її широкій інтерпретації (сукупність джерел матеріальних та ідеальних відображень у навколишній матеріальній обстановці вчиненого злочину);

– особи злочинця (опис людини як соціально-біологічної системи, властивості та ознаки якої відображуються у матеріальному середовищі);

– особи потерпілого (для окремих видів чи груп злочинів: демографічні дані, відомості про спосіб життя, риси характеру, звички, зв'язки і стосунки, ознаки віктимності тощо)[57].

Загалом, Ю. Я. Хамига надає власне визначення поняття фінансового шахрайства як «сукупності економічних відносин, які реалізуються юридичними або фізичними особами (як правило, без насильницьких дій) у процесі формування, розподілу і використання фінансових ресурсів (доходів) шляхом обману або зловживання довірою чи службовим становищем з метою отримання економічної та/або іншої вигоди (особистої, корпоративної чи на користь третіх осіб), у результаті яких відбувається отримання економічних вигід шахраєм та збитків – жертвою шахрайських дій. Такий підхід, на відміну від наявних, системно і всебічно розкриває сутність фінансового шахрайства та акцентує увагу передусім на фінансових аспектах цього поняття, конкретизації мети, способів та наслідків фінансового шахрайства, а також дає можливість сформувати комплекс заходів щодо попередження і мінімізації фінансового шахрайства як цілісної системи, спроможної докорінним чином вплинути на подолання цього суспільно-небезпечного явища»[58].

Крім того, зазначимо, що збут товарів і послуг між суб'єктами в інтернеті відбувається через низку платформ. Характеристику дії таких платформ у своєму дослідженні надає група авторів (С. М. Ілляшенко, Т. Є. Іванова), зазначаючи, що створення власного сайту дає змогу повноцінно представити себе в інтернеті, максимально розповісти про свою компанію і товари споживачу, розвивати товарну марку, виділитися серед конкурентів, відстежити дії відвідувачів. Проте розроблення сайту інтернет-магазину – це лише початковий етап. Щоб забезпечити обсяги продажу, необхідно просувати сайт у пошукових системах, удосконалювати його структуру та контент. Електронні дошки оголошень – це вебсайти для зберігання та публікації оголошень, де кожен бажаючий може викласти свою рекламну інформацію. Для зручності використання такого майданчика віртуальна дошка оголошень зазвичай поділена на розділи згідно з тематикою оголошень. Рекламна публікація на дошці оголошень може бути як платною, так і безкоштовною. Як правило, це впливає на рейтинг реклами на сайті. Як самостійний спосіб продажів дошки оголошень

[57] Кузьмічов В. С., Прокопенко Г. І. Криміналістика : навч. посіб. / за заг. ред. В. Г. Гончаренка та Є. М. Моісєєва. Київ : Юрінком Інтер, 2001. 368 с.

[58] Khamyha Yu. Financial pyramids as a type of financial fraud : theoretical-motivational aspect. *European Journal of Economics and Management*. 2020. Vol. 6. Issue 3. pp. 15–22.

можуть бути цікаві лише приватним особам для одноразових операцій, здебільшого продажу вживаних товарів. Наступною платформою є соціальні мережі, що набирають свою силу як інструмент маркетингу для багатьох галузей торгівлі. Їх використовують як підприємці-початківці для створення нового бізнесу, так і великі компанії для формування додаткового каналу збуту або забезпечення зв'язків із громадськістю. Однак у цього способу збуту продукції є певні обмеження. Ступінь успішності продажів залежить від унікальності продукту. Чим більш стандартизованим є товар, тим складніше його продавати, тим більше дисконт, який необхідно запропонувати покупцю. Через наявність високого ризику ціна продукту є дуже вагомим фактором. Торгові центри – це платформи для продажів товарів і послуг в інтернеті, що об'єднують тисячі компаній з різних галузей бізнесу. Здебільшого продавцями на цьому сегменті інтернет-ринку є компанії, а не приватні особи. Загалом цей спосіб збуту є досить ефективним, але він має низку недоліків порівняно з власним інтернет-магазином. Одним із них є щорічна плата за публікацію сайту на платформі, що часом дорівнює витратам на створення власного інтернет-магазину з більш широкими функціональними можливостями, індивідуальним дизайном, не говорячи вже про можливості переходу на сайт магазину в пошукових системах[59].

А вже А. Ф. Волобуєв зазначає, що, зокрема, криміналістична характеристика розкрадань майна повинна відбивати традиційні елементи їх механізму але з урахуванням тієї специфіки, яку накладає на них підприємницька діяльність, а також взаємні зв'язки з іншими злочинами, оскільки вони утворюють єдину технологію злочинної діяльності:

– особливості предмета посягання (матеріальні цінності, грошові кошти, цінні папери);

– обстановку вчинення злочину (загальноекономічні і правові умови підприємницької діяльності, організаційно-правові форми підприємств, стан контролю з боку відповідних державних органів, місцезнаходження суб'єктів підприємництва та існування між ними певних відносин тощо);

– способи підготовки, вчинення і приховування розкрадання (прийоми створення сприятливих умов для заволодіння майном, прийоми безпосереднього заволодіння майном та його використання, заходи щодо маскування розкрадання, вчинення супутніх розкраданню злочинів);

– сліди розкрадання (документів та речових доказів, свідчень осіб, що вказують на протиправне заволодіння майном);

– особливості суб'єкта розкрадання та супутніх злочинів (підприємця-фізичної особи, посадових осіб і службовців юридичної особи – суб'єкта підприємництва);

[59] Ілляшенко С. М., Іванова Т. Є. Перспективи та основні проблеми розвитку інтернет-торгівлі в Україні. *Механізм регулювання економіки*. 2014. № 3. С. 113–119.

– особливості потерпілого від розкрадання (підприємця, окремих громадян)[60].

На нашу думку, криміналістична характеристика злочинів є категорією динамічною. Іншими словами, вона може змінюватися залежно від конкретних умов дійсності. Проте її використання може мати різні напрями у діяльності працівників правоохоронних органів. Наприклад, за ознаками способу, місця та часу його вчинення може бути висунута версія щодо особи злочинця і, навпаки, при затриманні правопорушника та наявності даних про обставини злочину може бути побудована версія про вчинення цією особою інших, ще нерозкритих злочинів[61].

Водночас С. В. Самойлов у своєму дисертаційному дослідженні, розглянувши криміналістичну характеристику шахрайств, що вчиняються з використанням інтернету, докладно розкрив зміст основних її елементів, окремо висвітлив класифікацію способів учинення, а також розробив теоретичні основи та практичні рекомендації щодо досудового розслідування зазначеної категорії кримінальних правопорушень[62].

У розрізі зазначеного вважаємо за потрібне навести думку С. В. Чучко, який вказує на те, що дотепер залишається ряд невирішених питань щодо конкретних прийомів і операцій, спрямованих на підготовку, безпосереднє вчинення та приховування шахрайств, пов'язаних із придбанням товарів через інтернет[63].

Тому дійсно вбачаємо потребу у виокремленні вказаного елементу криміналістичної характеристики визначеного протиправного діяння.

Як доречно наголошує Т. В. Коршикова, наразі є об'єктивна потреба в узагальненні та впорядкуванні наявних методичних рекомендацій щодо розслідування шахрайств, учинених з використанням ЕОТ, з метою формування комплексної криміналістичної методики. Об'єднані в єдиній класифікаційній групі ідеї та теоретичні положення стають цілісною теоретичною концепцією. В основі цієї концепції – характеристика різних видів кримінальних правопорушень, урахування якої дозволяє об'єднати окремі рекомендації в єдину ме-

[60] Волобуєв А. Ф. Криміналістична характеристика розкрадань майна у сфері підприємницької діяльності. *Вісник Університету внутрішніх справ*. 1997. Вип. 2. С. 26–37.

[61] Єфімов М. М. Пріоритетні напрями розслідування злочинів проти моральності в розрізі євроінтеграційних процесів. *Інновації юридичної науки в євроінтеграційному процесі* : матеріали Міжнарод. наук.-практ. конф. (10–11 берез. 2017 р., м. Сладковічево). Словацька Республіка. Університет Данубіус, юридичний факультет Янко Єсенського. 2017. С. 268–271.

[62] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : дис. … канд. юрид. наук : 12.00.09 / Дон. юрид. ін-т. Донецьк, 2014. 226 .

[63] Chuchko, S. Fraud methods, related to purchase of goods through the Internet. *Visegrad Journal on Human Rights*. 2019. 6 (volume 3). Pp. 234–238.

тодику. До допоміжних компонентів цієї концепції відносимо положення криміналістичної[64].

Стосовно наповнення криміналістичної характеристики, то для початку наведемо тезу О. В. Герасимова, який виокремлює такі складові в кримінологічній характеристиці злочинів у банківській сфері, зокрема: кількісні та якісні показники групи досліджуваних злочинів; характеристику способів указаних протиправних діянь; мотивів їх вчинення; інформацію про типові особливості суб'єктів їх учинення[65].

Зі свого боку, Е. В. Малютін констатував наявність таких складових криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу, як-от: «спосіб і обстановка учинення кримінального правопорушення, слідова картина, особа злочинця, особа потерпілого»[66].

А вже на основі вивчення матеріалів кримінальних проваджень В. В. Сисолятін визначив такий перелік основних елементів криміналістичної характеристики правопорушень, пов'язаних з використанням інтернет-банкінгу, а саме: «… спосіб вчинення правопорушення; обстановка вчинення правопорушення; слідова картина протиправного діяння; особа правопорушника; особа потерпілого»[67].

На основі дослідження матеріалів кримінальних проваджень (додаток Б) стосовно наявності елементів криміналістичної характеристики кримінальних правопорушень у кіберпросторі, можна серед них виокремити такі:

– спосіб підготовки, учинення та приховування протиправного діяння;

– обстановка вчинення кримінального правопорушення;

– слідова картина;

– особа правопорушника (кіберзлочинець);

– особа потерпілого.

[64] Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … д-ра філос. : 081 – Право / Національна академія внутрішніх справ, Київ, 2021. 255 с.

[65] Герасимов О. В. Кримінологічна характеристика та аналіз злочинів у банківській сфері. *Вісник ХНУ імені В. Н. Каразіна*. 2017. Вип. 24. С. 203–207.

[66] Малютін Е. В. Наукові підходи до побудови криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Інноваційні підходи до реформування сучасного законодавства* : матеріали Міжнарод. наук.-практ. конф. (м. Київ, 20–21 квіт. 2023 р.). Київ : НДІ публ. права, 2023. С. 144–146.

[67] 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 Міжнарод. наук.-практ. конф. (м. Київ, 22–23 вересня 2021 р.). Київ : НДІ публ. права, 2021. С. 22–24.

Констатуючи зазначене вище, зауважимо, що вказані складові є взаємопов'язаними та характеризуються чіткою розшуковою спрямованістю, що, своєю чергою, забезпечує найбільш оптимальне їх використання у процесі доказування. У цілому, дослідження криміналістичної характеристики кримінальних правопорушень у кіберпросторі потрібно для більш якісного та швидкого проведення розслідування.

1.3. Характеристика окремих елементів криміналістичної характеристики кримінальних правопорушень у кіберпросторі

Серед зазначених вище складових криміналістичної характеристики кримінальних правопорушень у кіберпросторі центральне місце посідають способи підготовки, безпосереднього вчинення та приховування досліджуваних протиправних діянь.

Стосовно їх значення, то, зокрема, Н. В. Павлова вказала, що спосіб вчинення правопорушення є центральним у криміналістичній характеристиці, адже за його допомогою можна опрацювати виявлені у процесі аналізу зв'язки між всіма структурними елементами досліджуваної наукової категорії[68]. Загальні умови діджиталізації як українського, так і загальнодержавного суспільства надали змогу протиправній діяльності змінювати власні форми і методи, кіберзлочинці на разі досить часто застосовує складні та нетипові способи учинення та приховання власних протиправних дій.

В. А. Журавель констатує, що потрібно застосовувати функціональний аспект поведінки правопорушника для характеристики способу вчинення протиправного діяння як системи дій, прийомів, операцій, що спрямовані на досягнення певного злочинного результату. Автор наголошує на тому, що знання типових способів вчинення кримінальних правопорушень дозволяє ефективно застосовувати одну з найбільш ефективних і практичних схем їх розслідування, яка представляється науковцями у послідовності: від слідів правопорушення – до способу його вчинення; від способу вчинення – до особи правопорушника[69].

Зі свого боку, Е. В. Малютін вказує, що криміналістична характеристика нараховує ряд елементів, кожен з яких з огляду на конкретне протиправне діяння матиме своє значення. Стосовно кримінальних правопорушень, пов'язаних з використанням е-банкінгу, автор зауважує, що найбільш важливе значення з усіх складових визначеної наукової категорії буде мати спосіб їх учи-

[68] Павлова Н. В. Розслідування шахрайства при укладанні цивільно-правових угод щодо відчуження житла : монографія. Дніпропетровськ : ДДУВС, 2008. 176 с.

[69] Журавель В. А. Розслідування легалізації (відмивання) доходів, одержаних злочинним шляхом : наук.-практ. посіб. Харків : Одіссей, 2005. 112 с.

нення. Дослідник аргументує вказану позицію такими фактами: «… зазначений елемент породжує утворення багатьох кореляційних зв'язків, як-от: «спосіб учинення» – «особа злочинця»; «спосіб учинення» – «особа потерпілого»; «спосіб учинення» – «слідова картина». Адже саме через спосіб учинення впливає на всі інші елементи: особа злочинця обирає той спосіб, який найбільш їй притаманний; особа потерпілого стає жертвою, позаяк їй притаманні певні риси, які зумовлюють використання відповідного способу вчинення кримінальних правопорушень, пов'язаних з використанням е-банкінгу»[70].

В свою чергу, Т. В. Охрімчук відмічає, що основним елементом криміналістичної характеристики шахрайства з фінансовими ресурсами є спосіб його вчинення, який відповідно складається з системи взаємопов'язаних дій щодо підготовки, вчинення та приховування слідів кримінального правопорушення. Крім того, авторка поставила правильний акцент на тому, що спосіб вчинення досліджуваного протиправного діяння «…полягає, перш за все, в обмані, в наданні завідомо недостовірної інформації, зокрема, шляхом подання підроблених документів кредитору»[71].

А вже А. Е. Жилін, досліджуючи схожу тематику, констатував, що кожен елемент криміналістичної характеристики має своє індивідуальне значення для структури в цілому та побудови кореляційних зв'язків зокрема. Практичне значення вказаної категорії, як слушно наголошує науковець, полягає «… у допомозі уповноваженим особам, які беруть участь у розслідуванні окремих протиправних діянь, шляхом використання відомостей, що визначені нами як ознаки та властивості окремих її елементів. Вказаною інформацією можливо скористатися при проведенні окремих слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних заходів. Крім того, її необхідно застосовувати під час побудови версій та аргументації відповідних слідчих ситуацій»[72].

Для прикладу, Ю. Я. Хамига акцентував увагу на тому, що «… специфіка функціонування фінансового ринку (зокрема, значна концентрація готівкових і безготівкових коштів, блискавичність проведення фінансових транзакцій, розмаїття фінансових послуг та інструментів із різним рівнем захищеності й ліквідності, стрімке поширення інтернет-технологій та зростання клієнт-

[70] 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.

[71] Охрімчук Т. В. Способи вчинення шахрайства з фінансовими ресурсами. *Правова держава: історія, сучасність та перспективи формування в Україні* : матеріали ІІІ Всеукр. наук.-практ. конф. (м. Запоріжжя, 23 квіт. 2010 р.). Запоріжжя : Юрид. ін-т ДДУВС, 2010. Ч. ІІ. С. 94–96.

[72] Жилін А. Е. Наукова полеміка відносно опису ознак та властивостей окремих елементів криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів. *Науковий вісник публічного та приватного права.* 2023. Вип. 1. С. 89–94.

ської бази, великі масштаби здійснення міжнародних угод та їх висока адаптивність) формують сприятливе підґрунтя для реалізації різного роду шахрайських схем на фінансовому ринку»[73].

Зі свого боку, В. О. Фінагеєв наголошує на тому, що «незаконний доступ до банківських рахунків технологічно поєднує пов'язані між собою кримінально карані діяння проти власності (ст. ст. 185, 190, 191 Кримінального кодексу (КК) України), у сфері господарської діяльності (ст. ст. 200, 205, 209, 231 КК України), використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж (ст. ст. 361, 361[1], 362 КК України), службової діяльності»[74].

Зазначеними вище науковцями проблему розглянуто в межах тем їхніх досліджень, натомість у цій роботі ми зосереджуємося на способах вчинення кримінальних правопорушень у кіберпросторі. Крім того, варто привести твердження В. Б. Коби, який констатував, що «… спосіб учинення злочину є центральним елементом у більшості криміналістичних характеристик. Вказана категорія як складова криміналістичної характеристики кіберзлочинів не втрачає свого значення, навіть навпаки – дослідження способу вчинення кримінальних правопорушень дозволить слідчим вчасно висувати конкретні версії стосовно злочинної події та особи кіберзлочинця, а також окремих обставин кримінального провадження. Окрім того, з огляду на типові способи протиправних посягань можна побудувати або відтворити типову слідову картину кіберзлочинів та визначити окремі ознаки особи потерпілого. Слід зазначити, що для комплексної боротьби з визначеними протиправними діяннями та своєчасної їх профілактики потрібні спільні зусилля держави, громадян та міжнародної спільноти, оскільки на часі кіберзлочинність є однією з найбільших загроз нормальної діяльності будь-якого соціуму»[75].

Варто навести думку О. І. Коваленка, який зазначив, що «… у період пандемії значно зріс обсяг онлайн-платежів в усіх сферах споживчого попиту, крім туризму. Споживачі стали активніше використовувати методи безконтактної і безготівкової оплати. Учасників ринку це змусило більш уважно вивчити платіжні інструменти і почати підключати нові. Епідемія і суворі обмеження за короткий період привели до значних змін на споживчому ринку, спровокувавши зростання довіри споживачів до безготівкової оплати і масовий перехід у електронну комерцію, зростання числа мерчантів (торговців),

[73] Хамига Ю. Я. Фінансове шахрайство: критерії ідентифікації та напрями мінімізації : дис. … д-ра філос. : 072 – Фінанси, банківська справа та страхування / Західноукраїнський нац. ун-т. Тернопіль, 2020. 308 с.

[74] Фінагеєв В. О. Способи вчинення злочинів, пов'язаних із використанням засобів доступу до банківських рахунків. *Науковий вісник Національної академії внутрішніх справ*. 2016. № 1. С. 63–82.

[75] Коба В. Б. Спосіб учинення кіберзлочинів як елемент криміналістичної характеристики: теоретична та практична проблематика. *Наукові перспективи*. 2025. № 4. С. 1156–1167.

транзакцій і, при цьому, кратне зростання числа шахраїв і «сірих схем»[76].

Досить слушною вважаємо думку В. В. Білоуса, який констатував, що «… під час готування до злочину, при вчиненні злочину і після нього особа керується логікою досягнення злочинного результату та уникнення відповідальності. Злочинець, маючи наміри приховати злочин, ретельно обмірковує спосіб його вчинення з тим, щоб надійно приховати сліди злочину. Крім вибору місця і часу вчинення злочину, підготовка до нього включає визначення: а) способу вчинення злочину; б) знарядь злочину; в) способу приховування (дійсного приховування і притворної поведінки, що відображає позицію, обрану злочинцем) г) способу приховування слідів. Таким чином, злочинець уявно формулює модель майбутньої події, реальне втілення якої буде залежати від ситуації, що об'єктивно складеться. Моделювання включає і варіанти зміни намірів і злочинної поведінки у випадку, якщо обрана схема не може бути реалізована»[77].

Говорячи безпосередньо про спосіб учинення протиправного діяння, для початку приведемо тезу С. М. Зав'ялова, який вказує, що визначена наукова категорія: «…виступає різновид діяльності людини, якій притаманні соціально-психологічні якості, орієнтувальні, сенсомоторні особливості суб'єкта»[78].

Зі свого боку, О. Г. Кривопуск констатує, що «… спосіб скоєння злочину дає найбільший обсяг криміналістичної інформації, який у подальшому допомагає слідчому, прокурору, суду чи іншим посадовим особам правоохоронних органів визначити найбільш ефективні методи, спрямовані на розкриття та розслідування злочину, дасть змогу слідчому висунути необхідні версії та ініціювати проведення необхідних слідчих (розшукових) дій, визначити правильний порядок та послідовність їх проведення»[79].

А вже Н. В. Павлова зауважила, що вказаний елемент є головним та єднальним, «… за допомогою якого можна дослідити виявлені у процесі аналізу зв'язки між всіма структурними елементами криміналістичної характеристики злочину»[80].

---

[76] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[77]Білоус В. В. Проблеми методики розслідування фіктивного підприємництва : дис. ... канд. юрид. наук : 12.00.09 / Нац. юрид. акад. імені Ярослава Мудрого. Харків, 2004. 179 с.

[78] Зав'ялов С. М. Спосіб вчинення злочину: сучасні проблеми вивчення та використання у боротьбі зі злочинністю : автореф. дис. … канд. юрид. наук : 12.00.09 / Нац. акад. внутр. справ України. Київ, 2005. 20 с.

[79]Кривопуск О. Г. Способи вчинення злісного невиконання обов'язків по по догляду за дитиною або за особою, щодо якої встановлена опіка чи піклування. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 3. С. 369–376.

[80] Павлова Н. В. Розслідування шахрайства при укладанні цивільно-правових угод щодо відчуження житла : монографія. Дніпропетровськ : ДДУВС, 2008. 176 с.

Найбільш оптимальним ми вважаємо формулювання, надане В. В. Тіщенком, який до змісту способів учинення злочину зараховує комплекс діянь злочинця з підготовки, вчинення і приховування злочину, обумовлених метою злочинного діяння, властивостями особи злочинця й обстановкою (об'єктивними і суб'єктивними факторами), результати яких відбиваються на матеріальних та інтелектуальних слідах, що характеризують психічні й фізичні риси особи злочинця[81].

Наведене визначення можна цілком підтримати і будемо розглядати спосіб вчинення кримінальних правопорушень у кіберпросторі в цьому розрізі. З огляду на узагальнення матеріалів кримінальних проваджень (додаток Б) можна зробити висновок, що спосіб учинення кримінального правопорушення має місце у 100 % випадків.

Першою складовою способу кримінального правопорушення є його підготовка. Наприклад, О. В. Баланюк щодо підготовчих дій виділяв такі їх групи:

– підготовчі дії щодо приховування особистої участі (розроблення плану із забезпечення неправдивого алібі, що включає в себе комплекс дій, спрямованих на створення в певних осіб неправильного уявлення про істинне місце перебування злочинця в конкретний час, попередню домовленість із неправдивими свідками та ін.);

– підбір, придбання засобів, призначених для знищення слідів злочинця, а також призначених для ускладнення використання службово-пошукового собаки тощо;

– підготовчі дії з приховання злочину в цілому і маскування окремих його обставин (виготовлення чи складання підроблених документів з метою приховання злочинних фінансово-господарських операцій чи справжніх обставин події);

– планування і підбір засобів та створення умов для вчинення інсценування події тощо;

– підготовчі дії зі створення умов для ухилення від відповідальності та продовження злочинної діяльності (вчинення дій, спрямованих на створення уявлення про винність у злочині інших осіб, або «об'єктивних» обставин, що призвели до злочинних наслідків);

– вербування й установка корумпованих зв'язків із відповідними посадовими особами органів влади та управління тощо[82].

[81] Тіщенко В. В. Концептуальні основи розслідування корисливо-насильницьких злочинів : автореф. дис. … д-ра юрид. наук : 12.00.09 / Нац. юрид. акад. України імені Ярослава Мудрого. Харків, 2003. 34 с.

[82] Баланюк О. В. Підготовка до злочину : поняття та криміналістична класифікація. *Актуальні проблеми держави і права*. 2006. С. 192–196.

А. І. Кунтій зазначає, що протиправні діяння у сфері ЕОТ учиняються з попередньою підготовкою. Серед заходів такої підготовки дослідник виокремив:

– підбір знарядь та програмного забезпечення для вчинення злочину;

– вибір об'єкта, стосовно якого буде вчинено злочин;

– підбір співучасників і розподіл ролей;

– установлення спостереження за об'єктом, вивчення режиму роботи чи розпорядку дня;

– вибір місця зберігання викраденої інформації;

– підшукування зацікавлених в інформації осіб (юридичних осіб)[83].

Своєю чергою, К. Д. Заяць зауважував, що «… основні проблеми у слідчих виникають на стадії прийняття рішення про відкриття кримінального провадження, коли необхідно встановити ознаки складу протиправного діяння. Труднощі пов'язані з потребою прийняти ключове процесуальне рішення на підставі аналізу дуже обмеженої інформації про подію. Навіть у рамках відкритого кримінального провадження дуже складно сформувати систему доказів наявності злочинного наміру в діях шахрая[84]. Інакше кажучи, доведення ретельної підготовки до вчинення шахрайських дій буде запорукою доведення вини особи.

А вже С. В. Чучко вказував на існування таких способів підготовки до шахрайства:

– визначення найменування товару, що пропонуватиметься для продажу, створення його характеристик та отримання презентабельних фотографій;

– реєстрація та створення облікового запису особи в інформаційній телекомунікаційній системі під вигаданими анкетними даними;

– розміщення даних про товар;

– створення рівня довіри у покупців шляхом здійснення успішних цивільно-правових дистанційних угод та заповнення шкали позитивних оцінок;

– створення «окремої» електронної адреси для здійснення переписки із потенційним споживачем;

– придбання «окремого» телефонного номеру для здійснення переговорів із потенційним споживачем;

– обрання способу здійснення розрахунків;

– реєстрація «електронних гаманців» у відповідних сервісах або отримання платіжної картки для перерахування грошей тощо[85].

---

[83] Криміналістика : підручник / за заг. ред. Є. В. Пряхіна. 3-тє вид., переробл. та допов. Львів : ЛьвДУВС, 2016. 948 с.

[84] Заяць К. Особливості сучасних форм вчинення шахрайств та їх криміналістичне значення. *Підприємництво, господарство і право*. 2017. № 11. С. 207–210.

[85] Чучко С. В. Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2021. 276 с.

Т. В. Коршикова щодо підготовчих дій до протиправних діянь з використанням ЕОТ вказала такі: «… 1) вчиненню шахрайства сприяв несанкціонований доступ до ЕОТ; 2) вчинення шахрайства здійснювалось із використанням шкідливих програмних чи технічних засобів; 3) вчиненню шахрайства сприяло розповсюдження рекламної чи іншої продукції про предмет посягання (надання послуг)»[86].

А вже В. Б. Коба на основі опрацювання судово-слідчої практики встановив такі підготовчі заходи до вчинення кіберзлочинів:

«– добір потрібної електронно-обчислювальної техніки;

– підготовка вказаної техніки;

– підбір учасників злочинної групи;

– розподіл ролей між учасниками злочинної групи;

– несанкціонований збут через мережу Інтернет даних з обмеженим доступом, яка зберігається на відповідній електронно-обчислювальній техніці;

– несанкціоноване розповсюдження через мережу Інтернет даних з обмеженим доступом, яка зберігається на вказаній техніці;

– створення шкідливого програмного забезпечення з метою злочинного використання, розповсюдження або збуту;

– створення спеціальних технічних засобів з метою злочинного використання, розповсюдження або збуту;

– виготовлення повідомлень електрозв'язку для подальшого їх масового розповсюдження, здійснене без попередньої згоди адресатів»[87].

На основі аналізу й узагальнення матеріалів кримінальних проваджень (додаток Б), можна дійти висновків, що переважно мали місце такі підготовчі заходи до вчинення кримінальних правопорушень у кіберпросторі:

– підбір та підготовка необхідної ЕОТ (комп'ютерів, ноутбуків, планшетів);

– створення шкідливих програмних чи технічних засобів з метою протиправного використання, розповсюдження або збуту;

– несанкціоновані збут або розповсюдження через мережу «Інтернет» інформації з обмеженим доступом, яка зберігається в комп'ютерах;

– створення повідомлень електрозв'язку для подальшого їх масового розповсюдження, здійснене без попередньої згоди адресатів;

– створення сприятливих умов для здійснення протиправних

[86] Коршикова Т. В. Способи вчинення шахрайств із використанням електронно-обчислювальної техніки як елемент їх криміналістичної характеристики. *Visegrad journal on human rights*. 2020. № 4. С. 129–135.

[87] Коба В. Б. Спосіб учинення кіберзлочинів як елемент криміналістичної характеристики: теоретична та практична проблематика. *Наукові перспективи*. 2025. № 4. С. 1156–1167.

дій;

– вибір об'єкта, що буде предметом протиправних дій;

– вибір кола осіб, які стануть потерпілими від протиправних дій та ін.

Приклад: *гр. Ю. не пізніше 13 липня 2023 року – 22 лютого 2024 року, перебуваючи за місцем свого проживання та використовуючи належну їй інформаційну систему, що має доступ до її облікового запису в додатку для спілкування Телеграм, здійснювала перегляд інформації, що розповсюджується в інтернеті, зокрема, у деяких телеграм-каналах та інших ресурсах, що створені та функціонують в інтересах держави-агресора рф з метою впливу на свідомість громадян України та інших країн щодо виправдовування, визнання правомірною, заперечення тимчасової окупації рф території України, збройної агресії рф проти України, глорифікації учасників збройної агресії рф проти України, дискредитації української державності, закликів до зміни меж території або державного кордону України тощо. Керуючись власними політичними поглядами та ідеологічними переконаннями, гр. Ю. виокремила публікації вказаного телеграм-каналу, у яких містилися заклики до вчинення дій, направлених на зміну меж території або державного кордону України, на порушення порядку, встановленого Конституцією України, та бажаючи поширення вищевказаної інформації іншим особам, у період не пізніше 13 липня 2023 року, перебуваючи за адресою свого проживання, сформувала у себе протиправний умисел, направлений на розповсюдження матеріалів, що містять вищевказані заклики. У подальшому гр. Ю., перебуваючи за адресою свого проживання, використовуючи належну їй інформаційну систему, що має доступ до її облікового запису у додатку для спілкування «Телеграм», поширила у телеграм-спільноті таку інформацію: «Харьков – русский город! Харьковчане – русские люди! Мы идем в Россию. Мы всей душой любим нашу большую Родину. То, что происходит сейчас на так называемой Украине, временно. Киевская нацистская нечисть будет изгнана с русской земли! В меру своих сил и возможностей, харьковчане тоже приближают это время», унаслідок чого вони стали доступні для перегляду необмеженому колу осіб. Ці матеріали відповідно до висновків лінгвістичної (семантико-текстуальної) експертизи містяться заклики до зміни меж території та державного кордону України*[88].

[88] Справа № 643/11884/24. Архів Московського районного суду м. Харькова, 2024 р.

Щодо способу безпосереднього вчинення кримінальних правопорушень у кіберпросторі вважаємо за потрібне зазначити таке. С. М. Зав'ялов доречно вказував на те, що реалізація сформованого злочинного наміру, що втілюється в окремих практичних діях суб'єкта, займає велику частину способу вчинення злочину. Крім того, автор відмічав, що реалізуючи злочинний намір, зловмисник опановує та аналізує низку обставин, за яких має діяти, зважає на можливості осіб, з якими планує вчинити злочин. З огляду на зазначене, автор підсумував, що на вказаному етапі правопорушник окреслює план своїх дій, обмірковує послідовність виконання деяких з них, готує знаряддя та засоби вчинення протиправного діяння, обирає спосіб їх застосування, продумує усунення певних перешкод, способи маскування слідів[89].

А вже С. В. Самойлов запропонував «… класифікувати способи вчинення досліджуваних шахрайств за наступними підставами:

– шахрайства, які пов'язані із купівлею/продажем у мережі Інтернет;

– шахрайства, сутність яких полягає в отриманні коштів (майна) шляхом надсилання листів чи повідомлень;

– шахрайства, які для заволодіння коштами (майном) потребують розробки та розміщення в мережі Інтернет дублікатів або вузькоспеціалізованих сайтів для надання псевдопослуг;

– шахрайства, які спрямовані на отримання персональних (реєстраційних) даних (так званий «фішинг»);

– шахрайства, пов'язані з обігом електронних грошей;

– шахрайства, для вчинення яких використовується спеціалізоване та/чи шкідливе програмне забезпечення;

– комбіновані способи шахрайств»[90].

Своєю чергою, О. А. Самойленко на основі аналізу матеріалів слідчо-судової практики визначила типові на цей час в Україні способи вчинення кримінальних правопорушень у кіберпросторі, зокрема:

«1. Способи злочинних дій, пов'язані з функціонуванням соціально-орієнтованих мереж (від англ. social networks), діяльність яких заснована на так званій вікі(viki)-технології.

2. Способи злочинних дій, пов'язані з функціонуванням технології BitTorrent, створеної для передавання великих за обсягом файлів одним користувачем іншому або громадськості.

3. Способи злочинних дій, пов'язані з функціонуванням сервісів електронної дошки оголошень (від англ. абревіатури «ВВС»).

4. Способи злочинних дій, пов'язані з функціонуванням технологій електронної комерції, створені для здійснення торгівлі через мережу Інтернет.

---

[89] Зав'ялов С. М. Спосіб вчинення злочину : сучасні проблеми вивчення та використання у боротьбі зі злочинністю : дис. … канд. юрид. наук : 12.00.09 / Нац. акад. внутр. справ України. Київ, 2005. 231 с.

[90] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : дис. … канд. юрид. наук : 12.00.09 / Дон. юрид. ін-т. Донецьк, 2014. 226 .

5. Способи злочинних дій, пов'язані з функціонуванням технології електронної розсилки (e-mail, від англ. electronic mail); IP-телефонії (найчастіше через комп'ютерну програму Viber; програмне забезпечення із закритим кодом Skype), призначені для відправлення/отримання електронних повідомлень між користувачами комп'ютерної/телекомунікаційної мережі.

6. Способи злочинних дій, пов'язані з функціонуванням технологій електронних платіжних систем (англ. electronic payment systems), призначені для здійснення платіжних операцій через мережу Інтернет.

7. Способи злочинних дій, пов'язані з функціонуванням технології зберігання та обробки інформації.

8. Способи злочинних дій, пов'язані з функціонуванням шкідливого програмного забезпечення. (з англ. «crimeware», де «crime – злочинність, software – програмне забезпечення; часто як синонім застосовують «вірус»)»[91].

А вже С. В. Чучко стверджував, що «… шахрайські дії здійснюються різними особами. Втім, залежно від суб'єкта, способи вчинення шахрайства у мережі Інтернет можна поділити на ті, що: вчинені від імені особи, яка діє як фізична особа-підприємець, що пропонувала товар; вчинені від імені юридичної особи, що оформила відповідні документи для здійснення підприємницької діяльності, дані про яку розміщені в Єдиному державному реєстрі юридичних осіб; вчинені від імені вигаданої особи, анкетні дані якої не відповідають дійсності; вчинені особою, яка мала намір придбати товар (покупцем)»[92].

Аналіз судово-слідчої практики (додаток Б), нормативно-правової бази та вищенаведених досліджень матеріалів кримінальних проваджень дозволив виокремити перелік способів безпосереднього вчинення кримінальних правопорушень у кіберпросторі, а саме:

1) протиправні дії у сфері власності (фішинг, смішинг, сніфферінг, 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 інтернету;

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.

---

[91] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

[92] Chuchko, S. Fraud methods, related to purchase of goods through the Internet. *Visegrad Journal on Human Rights*. 2019. № 6 (volume 3). Pp. 234–238.

Дамо окремим із них характеристику. Зокрема, *фішинг* – це кібератака, яка використовує замаскований електронний лист як приманку. Мета фішингу полягає в тому, щоб ввести в оману одержувача електронної пошти, щоб жертва повірила, що повідомлення є достовірним, на кшталт запиту від банківської установи, або повідомлення від близької людини, і виконати перехід через посилання або завантажити вкладення до електронного листа[93]. Що насправді відрізняє фішинг – це форма повідомлення: зловмисники маскуються під так звану довірену особу, часто справжню або схожу на реальну людину, або компанію, з якою жертва може вести бізнес. Це один із найдавніших типів кібератак, починаючи з 1990-х років, який досі залишається одним із найпоширеніших і згубних, через що фішингові повідомлення та техніки стають все більш досконалими[94].

Переважно використовується метод проведення масових розсилок від імені популярних компаній або організацій, які містять посилання на помилкові сайти, що зовні майже не відрізнити від справжніх. Зовні здається, що фішингові повідомлення приходять від імені популярних організацій або компаній (як LiqPay, Skrill, UPS, урядові організації або банківські установи), однак насправді вони є підробленими[95].

Часто трапляється так, що шахраї при цьому отримують інформацію про клієнтів банку від недобросовісних банківських співробітників, що може ввести жертву в ще більший обман. Крім цього, розсилка може проводитися не від імені банку, а від імені сервісу онлайн-платежів (наприклад, LiqPay), а також соціальних мереж (Instagram, Facebook)[96].

Також розрізняють такий вид фішингу, як *смішинг* (англ. *SmiShing*) – протиправні дії за допомогою смс-повідомлень. У цьому випадку посилання на підроблений сайт відправляється через смс, або шахраї просять надіслати їм необхідну інформацію про банківську карту у відповідному повідомленні. Схожий на фішинг також *фарминг* (англ. *Farming*, від слова «*farm*» – «фе-

[93] Методичні рекомендації щодо управління операційним ризиком (у тому числі кіберризиком та безперервністю діяльності) та забезпечення зберігання інформації про клієнтів об'єктами платіжної інфраструктури. URL: https://bank.gov.ua/ua/news/all/metodichni-rekomendatsiyi-schodo-upravlinnya-operatsiynim-rizikom-u-tomu-chisli-kiberrizikom-ta-bezperervnistyu-diyalnosti-ta-zabezpechennya-zberigannya-informatsiyi-pro-kliyentiv-obyektami-platijnoyi-infrastrukturi (дата звернення: 03.09.2025).

[94] Єфімов М. М. Криміналістичний аналіз окремих сучасних видів шахрайства: проблемні питання. *Науковий вісник публічного та приватного права.* 2021. Вип. 5. С. 116–121.

[95] Самойлов С. В. «Фішинг» як спосіб вчинення Інтернет-шахрайств. *Актуальні питання сучасних державотворчих та правотворчих процесів*: матеріали Міжнарод. наук.-практ. конф. (24 лют. 2011 р., м. Запоріжжя) : у 3 ч. Запоріжжя : Запоріз. міська громад. орг. «Істина», 2011. Ч. 3. С. 102–104.

[96] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

рма»). Він полягає в перенаправленні клієнта на помилкову адресу за допомогою шкідливої програми. Жертва обману вводить в пошуковий рядок адресу сайту свого банку, але ця програма відправляє його на підроблений шахрайський сайт. Різновидами фішингу, як доречно наголошує Т. В. Коршикова, є:

– фішингові сайти;

– фішингові електронні листи;

– фішингові смс-повідомлення[97].

Так, наприклад, у ході досудового розслідування було з'ясовано, що невстановлені особи, які шахрайським шляхом, шляхом обману під приводом купівлі товару заволодівають коштами громадян через фішингові (підроблені) сайти Нової Пошти та OLX, у подальшому ці кошти перекидають на відповідні карткові рахунки. Під час досудового розслідування виникла необхідність отримання відповідних документів, що слугували підставою для відкриття цих рахунків, зокрема копії паспортів, заяв та анкет, оскільки орган досудового розслідування зможе використати їх як докази у вказаному кримінальному провадженні, а також вилучення унеможливить їх зміну або знищення у зв'язку із закінченням термінів зберігання зазначеної вище документації та інформації з інших причин. Тому судом було прийнято рішення задовільнити ухвалу[98].

Сніфферінг (сніффінг, *Sniffing*, від англ. *«Sniff»*, що означає «нюхати», «винюхувати») – спосіб кримінальних правопорушень у кіберпросторі, що виражається в перехопленні даних. Спеціальна комп'ютерна програма, яка називається «Сніффер» може перехопити дані клієнта (наприклад, реквізити банківської карти або паролі від платіжних акаунтів) у мережі Wi-Fi. Як місце «лову даних» шахраї часто вибирають кафе, вокзали, інші місця з великим скупченням людей. Шахрай приходить в громадське місце, наприклад, ресторан, з ноутбуком, на якому встановлена програма-сніффер. Він активує точку доступу Wi-Fi, назва якої співзвучна з назвою ресторану. І якщо клієнт, не підозрюючи про обман, підключається до цієї точки Wi-Fi, то весь його трафік буде перехоплено й проаналізовано сніффером[99], зокрема на предмет імен і паролів користувача платіжних систем, номерів кредитних карт, паролів підтвердження оплати та ін. Фактично перехоплюється весь трафік, але за умови, що жертва підключилася саме до псевдомережі шахрая. Довгий час JS-сніффери залишалися поза полем зору антивірусних аналітиків, а банки й платіжні системи не бачили в них серйозної загрози. Експерти Group-IB проаналізували 2440 заражених онлайн-магазинів, відвідувачі яких (сумарно близько 1,5 млн чоловік у день) піддавалися ризику компрометації. Серед постраждалих – не

[97] Коршикова Т. В. Способи вчинення шахрайств із використанням електронно-обчислювальної техніки як елемент їх криміналістичної характеристики. *Visegrad journal on human rights*. 2020. № 4. С. 129–135.

[98] Справа № 463/7254/21. Архів Личаківського районного суду м. Львова, 2021 р.

[99] Коваленко І. О. Криміналістичний аналіз шахрайства у сфері банківських електронних платежів. *Прикарпатський юридичний вісник.* 2020. № 5 (34). С. 137–140.

тільки користувачі, але й онлайн-магазини, платіжні системи та банки, що випустили скомпрометовані карти[100].

Group-IB – єдина приватна компанія у сфері кібербезпеки, яка брала участь в операції, надала європейським правоохоронним органам інформацію про 90 000 банківських карт, скомпрометованих за допомогою фішингових вебсайтів, банківських троянів під ПК, Android, а також JS-сніфферів, які зловмисники впроваджують на сайти інтернет-магазинів для перехоплення інформації, яка вводиться користувачем даних – номерів банківських карт, імен, адрес, логінів, паролів і ін. Увесь цей величезний масив розрізненої інформації був ретельно зібраний із закритих джерел хакерських соціальних мереж – кардшопів, форумів, ботнетів, JS-сніфферів, і проаналізований системою для дослідження кіберзагроз і полювання за атакуючими Group-IB Threat Intelligence & Attribution. Щоб запобігти незаконному використанню вкрадених даних, співробітники Європолу в режимі реального часу координували обмін інформацією між правоохоронними органами Великобританії, Італії, Угорщини, банками і платіжними системами. У результаті операції Carding Action 2020 європейським фінансовим установам, за даними Європолу, вдалося запобігти потенційним збиткам на суму близько 40 млн євро[101].

Вішинг (англ. *Vishing* – від *voice phishing*) – вид телефонного шахрайства, що дозволяє красти у клієнтів банків конфіденційну інформацію. Клієнт отримує дзвінок від автоінформатора, який повідомляє, що з картою, наприклад, здійснюються шахрайські дії, і дає інструкції – передзвонити за певним номером. Далі, слідуючи інструкціям автовідповідача, клієнт повинен повідомити або ввести на клавіатурі телефону реквізити карти. Іноді зловмисники самі дзвонять жертвам, переконуючи, що є співробітниками банку. У банках стверджують, що в телефонних розмовах з клієнтом ніколи не запитують повний номер карти, тим більше не вимагають повідомляти пін-код.[102].

Так, наприклад, у вересні 2020 року в м. Мелітополі співробітники Служби безпеки України блокували діяльність колл-центру, учасники якої викрадали кошти з банківських рахунків Сбербанку. Слідство встановило, що злочинну схему організували троє жителів Мелітополя. У центрі міста вони обладнали незаконний колл-центр, де «працювало» 54 оператора. Вони видавали себе за співробітників банку, дзвонили клієнтам та отримували від них інформацію про CVV-коди, номери і пін-коди платіжних карт. Для «роботи» з клієн-

[100] Єфімов М. М. Криміналістичний аналіз окремих сучасних видів шахрайства: проблемні питання. *Науковий вісник публічного та приватного права.* 2021. Випуск 5. С. 116–121.

[101] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[102] Там само.

нтами банків з росії зловмисники використовували маршрутизацію міжнародного телефонного трафіку[103].

Кардінг – рід кримінальних правопорушень у кіберпросторі, для здійснення якого використовуються банківські картки. Указані дії можуть відбуватися через викрадення або незаконне отримання карти – це або фізичний вплив на власника, або пошук уразливості в процесі видачі, доставки або оформлення банківського продукту та використання карти зловмисником. Крім того, також можлива компрометація даних карти для подальшого виготовлення підробки. Насамперед ідеться про копіювання даних магнітної смуги карти і крадіжки пін-коду. Найбільш поширеним цей вид кримінальних правопорушень у кіберпросторі був до масового переведення карт на чіпові технології. Сьогодні така схема зустрічається рідко, оскільки майже по всьому світу діє Chip Liability Shift – обов'язок банку-еквайра обслуговувати карту з чипом виключно за чипом. Серед інших можливих прикладів кардінгу варто вказати такий, як: компрометація реквізитів картки для здійснення операцій CNP (без присутності карти). Яскравий приклад – оплата покупок або послуг в інтернеті. Кінцева мета шахраїв у всіх випадках – отримати доступ до грошей. Для реалізації своїх задумів кіберзлочинці винаходять надто хитрі схеми, нерідко користуючись довірливістю й неуважністю громадян[104].

Деякі махінації в інтернеті також пов'язані з крадіжкою особистих даних – незаконним отриманням та протиправним використанням чиїхось особистих даних, зазвичай в економічних цілях. Додамо кілька прикладів з досвіду правоохоронних органів США. Як з'ясувалося в ході одного федерального процесу, відповідачі взяли імена та ідентифікаційні номери соціального забезпечення офіцерів Збройних сил США з вебсайту, а потім використовували понад 100 з цих імен і номерів для отримання кредитних карт в одному з банків штату Делавер через інтернет. В іншому федеральному процесі відповідачі, як зазначається, взяли особисті дані з сайту федерального органу, а потім використовували ці особисті дані для подачі в режимі онлайн 14 заяв про отримання кредиту для покупки машини в один із банків Флориди[105].

Приклад. *У серпні 2023 року гр. Л. отримав пропозицію від гр. Ж. вчиняти шахрайство із використанням ЕОТ та легалізувати майно, одержане злочинним шляхом, на що дав згоду. У подальшому гр. Ж., маючи навички та вміння працювати з*

[103] Коваленко І. О. Криміналістичний аналіз шахрайства у сфері банківських електронних платежів. *Прикарпатський юридичний вісник.* 2020. № 5 (34). С. 137–140.

[104] Єфімов М. М. Криміналістичний аналіз окремих сучасних видів шахрайства: проблемні питання. *Науковий вісник публічного та приватного права.* 2021. Вип. 5. С. 116–121.

[105] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

комп'ютерною технікою та досвід роботи з інформаційними технологіями, використовував спеціальне програмне забезпечення – бот у месенджері «Телеграм», який створює фішингові посилання – вебсторінки, головний розділ яких імітує офіційні урядові, міжнародні та банківські вебсайти, які пропонують отримання грошової допомоги та в яких є спеціальні поля для введення особистої інформації по банківських рахунках, а саме: номери банківських карток, строк їх дії, CVV-коди, коди-підтвердження дворівневої аутентифікації, логіни та паролі до облікових записів онлайн-банкінгу користувачів послуг, надсилав вказані фішингові посилання гр. Л. Після чого останній на виконання вказівки організатора здійснював розсилку фішингових посилань у соціальних мережах, для викрадення банківських даних потерпілих осіб, надавав власний номер телефону як засіб вчинення шахрайства, погоджував зі співробітниками магазинів Varus питання, що виникали в ході оформлення інтернет-замовлень та надавав засоби для вчинення таких кримінальних правопорушень. Зокрема, 30 серпня 2023 року гр. Ю. зайшла зі свого мобільного телефону у месенджер «Телеграм» та перейшла у телеграм-канал, створений зловмисниками, знайшла рекламне оголошення з таким змістом: «Фінансова допомога від ООН! Грошова допомога від міжнародних організацій мешканцям України. Подати заявку онлайн на виплату грошової допомоги від ЮНІСЕФ, Червоного Хреста, ООН, МОМ відповідно до меморандумів із …» та фішинговим посиланням. Будучи введеною в оману, потерпіла здійснила перехід за посиланням на вебсайт, який зовні подібний до вебсайту онлайн-банкінгу «Приват24», на якому їй було запропоновано ввести свої особисті дані у вигляді логіну (фінансового номера) та паролю, для подальшого входу у власний обліковий запис банкінгу[106].

З приводу останньої складової способу, то окрема група вчених-криміналістів (В. К. Весельський, С. М. Зав'ялов та В. В. Пясковський) серед них виділяли такі види:

«– способи приховування матеріальних слідів, що відбилися в навколишній обстановці внаслідок готування і вчинення злочину;

– способи приховування предметів посягання та наслідків заволодіння ними, розпорядження й використання;

– способи вживання заходів з маскування і фальсифікації слідів злочину;

– способи вживання заходів з протидії розшуку злочинця;

[106] Справа № 210/3688/24. Архів Дзержинського районного суду м. Кривого Рогу Дніпропетровської обл., 2024 р.

– способи вживання заходів з протидії щодо встановлення істини загалом»[107].

А вже М. В. Салтевський наголошував, що спосіб приховування реалізується як самостійне явище лише тоді, коли протиправне діяння вчинено. Вчений зазначив, що коло можливих дій суб'єкта значно розширюється і може включати обмову, неправдиві показання, залякування свідків, наклеп, підроблення документів тощо. У злочинах, учинених у співучасті, спосіб учинення може бути один, а способи приховування – різні в кожного співучасника[108].

На основі аналізу й узагальнення матеріалів кримінальних проваджень (додаток Б), встановлено, що кіберзлочинці використовували такі способи приховування своєї протиправної діяльності:

– використання перетворення ідентифікатора місця знаходження устаткування, за допомогою якого вчинюються протиправні дії – 88 %;

– приховування створеного шкідливого програмного забезпечення за допомогою легального програмного забезпечення – 51 %;

– відмова від дачі показань – 45 %;

– знищення обладнання, що використовувалось для вчинення протиправних дій – 44 %;

– дача неправдивих показів при проведенні окремих процесуальних дій (у тому числі – неправдиве алібі) – 42 %.

Підбиваючи підсумки, зазначимо, що нами було надано характеристику сучасним способам безпосереднього вчинення кримінальних правопорушень у кіберпросторі, а також опрацьовано способи підготовки та приховування вказаних протиправних діянь.

Щодо обстановки вчинення кримінальних правопорушень у кіберпросторі вважаємо за потрібне зупинитися на формулюванні її визначення. Наприклад, В. В. Тіщенко вдало наголошує на тому, що вчинення протиправного діяння, як і будь-яка інша складна система, випливає з обстановки його вчинення та дій правопорушника. Вчений зауважує, що «… злочинець вчинює, а також у разі наявності готує та приховує злочин у конкретних умовах обстановки. Відповідно, зловмисник може зайняти активну або пасивну позицію. При активній позиції суб'єкта він не тільки враховує конкретну обстановку в дина-

[107] Весельський В. К., Зав'ялов С. М., Пясковський В. В. Сучасні можливості використання даних про спосіб учинення злочину в боротьбі зі злочинністю : навч. посіб. для студ. вищ. навч. закл. Київ : КНТ, 2009. 160 с.

[108] Салтевський М. В. Криміналістика (у сучасному викладі) : підручник. Київ : Кондор, 2005. 588 с.

міці сприятливих і несприятливих факторів, але й намагається змінити її, створити такі умови, які сприяли б здійсненню його злочинного задуму та приховуванню злочину. Пасивна позиція злочинця автором визначається як сукупність умов, що складаються поза його волею і на які він впливати не може. При плануванні злочину особа оцінює обстановку, з'ясовує та аналізує умови, що сприяють або перешкоджають реалізації його намірів. Оскільки умови, у яких перебуває об'єкт, що цікавить злочинця, є динамічними у тому чи іншому ступені, і він намагається підібрати для здійснення його задуму найбільш сприятливі»[109].

Своєю чергою, Е. В. Малютін зауважував, що обстановка вчинення протиправного діяння наявна майже в кожній існуючій криміналістичній характеристиці. І це зрозуміло, адже місце, час, умови вчинення мають сталі кореляційні зв'язки як зі способом вчинення, так і з іншими елементами визначеної наукової категорії[110].

Доцільною також убачаємо позицію Б. В. Черняховського, який засвідчує, що «… середовище вчинення злочину, пов'язаного із застосуванням комп'ютерних технологій, умовно можна поділити на матеріальне (комп'ютерно-технічне устаткування, приміщення, у якому воно знаходиться) і нематеріальне інформаційне середовище в цифровій (електронній) формі»[111].

А вже В. А. Динту розкриває зміст поняття обстановки злочину як системи даних, що відображає матеріальні, мікросоціальні та морально-психологічні умови підготовки, вчинення та приховування злочину[112].

Проведений аналіз засвідчує, що більшість учених передбачають фізичну (матеріальну) складову у змісті обстановки вчинення злочину. Проте, на наш погляд, не можна розглядати обстановку вчинення злочину тільки в межах сукупності матеріальних (фізичних) умов, у яких діяв злочинець[113].

М. В. Куратченко констатував, що «… обстановка вчинення злочину – це широке поняття, що включає ряд елементів, які характеризують середо-

---

[109] Тіщенко В.В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса : Фенікс, 2007. 260 с.

[110] 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 Міжнарод. наук.-практ. конф. (м. Київ, 12–13 серп. 2020 р.). Київ : НДІ публ. права, 2020. С. 132–134.

[111] Черняховський Б. В. Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 2. С. 58–68.

[112] Динту В. А. Обстановка злочину як елемент криміналістичної характеристики злочинів : автореф. дис. … канд. юрид. наук : 12.00.09 / Ун-т «Одеська юридична академія». Одеса, 2014. 20 с.

[113] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

вище, у якому вчинюється суспільно-небезпечне діяння. Поміж них обов'язково необхідно виділяти час, місце і умови вчинення злочину, що мають значення для його повного дослідження. … Місце вчинення злочину слід досліджувати з різних боків. Зокрема, з однієї сторони, як географічне поширення досліджуваного кримінально караного посягання, з іншої – конкретне місце його вчинення. … Воно містить великий об'єм відомостей щодо способу скоєння кримінального правопорушення, певних даних про особу злочинця»[114].

Зі свого боку, В. В. Апопій досліджуючи питання е-торгівлі, акцентує увагу на повністю безконтактному способі спілкування між злочинцем і потерпілим Автор наголошує, що «… за змістом своєї діяльності інтернет-торгівля сильно відрізняється від звичайної роздрібної торгівлі. Їй властиві певні функції та особливості, серед яких основними є: віртуальність, тобто відсутність особистого контакту між окремими особами – учасниками процесу купівліпродажу; інтерактивність, тобто адекватне інформаційне забезпечення покупця його запиту у вигляді беззвучного діалогу; глобальність, тобто відсутність часових, просторових, адміністративних, соціально-демографічних, асортиментних кордонів; динамічність, тобто здатність онлайн-торгівлі до моментальних змін та адаптації до нових умов; ефективність, тобто здатність забезпечувати прибуток, інші економічні вигоди та соціальний ефект»[115].

Слід зауважити, що обстановка вчинення кримінальних правопорушень у кіберпросторі може виходити за межі фізичної (матеріальної) складової. На цьому наголошує й А. І. Анапольська, на думку якої обстановка вчинення злочинів з використанням конфіденційних даних про реквізити справжніх платіжних карток включає в себе речові, технічні, соціально-психологічні, а також просторові чинники[116].

Користуючись поняттям обстановки, О. В. Курман хоча й має на увазі матеріальне середовище, але при цьому враховує у її змісті технічну оснащеність, систему обліку, технологію проведення кредитних операцій, використання обчислювальної техніки, сучасних методів обліку, електронного зв'язку з кореспондентами банку тощо[117].

У цьому розрізі слід звернути увагу на думку Б. В. Черняховського, який зазначає, що середовище вчинення злочину, пов'язаного із застосуванням

---

[114] Куратченко М. В. Обстановка вчинення сутенерства та втягнення особи в заняття проституцією. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2016. № 3. С. 236–242.

[115] Апопій В. В. Інтернет-торгівля : проблеми і перспективи розвитку. *Регіональна економіка*. 2003. № 1. С. 25–32.

[116] Анапольська А. І. Розслідування шахрайств і пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : дис. ... канд. юрид. наук : 12.00.09 / Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ, 2010. 243 с.

[117] Курман О. В. Методика розслідування шахрайства з фінансовими ресурсами : дис. ... канд. юрид. наук : 12.00.09 / Нац. юрид. акаде. України ім. Ярослава Мудрого. Харків, 2002. 227 с.

комп'ютерних технологій, умовно можна поділити на матеріальне (комп'ютерно-технічне устаткування, приміщення, у якому воно знаходиться) і нематеріальне інформаційне середовище в цифровій (електронній) формі[118].

Завдяки електронним пристроям різного рівня складності, підключеним до глобальної або локальної мережі, виникає віртуальне середовище[119].

Натомість слід наголосити, що сервери, з яких кіберзлочинці здійснюють банківські операції, знімають кошти з рахунків потерпілих чи втручаються в облікові записи користувачів мережі Інтернет, розташовані у фізичному просторі та мають власну IP-адресу. Отже, обстановку вчинення кримінальних правопорушень у кіберпросторі доцільно розглядати як у фізичному вимірі – з урахуванням місця розташування комп'ютерно-технічного устаткування, з якого здійснювались протиправні дії, – так і у віртуальному, тобто просторі передачі та зчитування цифрової інформації.

У цьому розрізі К. В. Преловський, проводячи аналіз інфраструктури банківської системи України, наголошував, що в нашій державі станом на 2018 рік функціонує ряд платіжних систем, серед яких:

– 2 державні («Система електронних платежів», «Національна платіжна система «Український платіжний простір»);

– 12 внутрішньобанківських платіжних систем (Freesend, «Гроші блискавкою», «Металкарт», «Миттєвий переказ», «Фінекспрес», «За мить», Eximcash, «Онікс», Unite express, «Аваль-експрес», «Акордбанк-експрес», «Глобус»);

– 9 платіжних систем, платіжними організаціями яких є банки (Welsend, «Софт», Privatmoney, Flashpay, The money, «Система термінових переказів», «Швидка копійка», Telegraf, Ibox money transfer, Avers №1);

– 15 платіжних систем, платіжними організаціями яких є небанківські установи («Поштовий переказ», «Інтерпейсервіс», «Фінансовий світ», «Розрахункова фондова система», «Глобалмані», Tyme, Webmoney.ua, «Укркарт», Mosst payments, Forpost, Paypong, «Електрум», «Лео», «Платисервіс», City 24);

– 3 міжнародні карткові платіжні системи (American express, Mastercard, Visa);

– 7 міжнародних систем переказу коштів (Moneygram, Western union, Meest, Ria, «Хазри», Intelexpres», Sigue money transfer)[120].

За повідомленням Н. О. Коваль та М. В. Борщ, функціонування платіжних систем в Україні взагалі має тенденцію до глобалізаційних процесів і все

[118] Черняховський Б. В. Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 2. С. 58–68.

[119] Яременко О. І. Сучасне праворозуміння відносин в інформаційній сфері та методологія їх систематизації. *Інформація і право*. 2017. № 3 (22). С. 30–42.

[120] Преловський К. В. Сутність і зміст поняття критичної інфраструктури банківської системи України. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2018. № 2. С. 94–98.

більше використовуються міжнародні платіжні системи різних типів, незважаючи на існування внутрішньодержавних. Це можна пояснити більшою надійністю, досвідом їх використання у провідних банківських системах світу[121].

Зі слів А. І. Анапольської, основними умовами, що сприяють вчиненню кримінальних правопорушень у кіберпросторі, є:

– відсутність практики постійної зміни паролів та кодів доступу до системи електронних розрахунків;

– відсутність між працівниками банку розмежування доступу до комп'ютерної інформації про електронні рахунки;

– надання комплекту комп'ютерної техніки у безконтрольне користування співробітникам;

– відсутність контролю за порядком проведення електронних розрахунків тощо[122].

У цьому розрізі пропонуємо до складу обстановки вчинення кримінальних правопорушень у кіберпросторі віднести й систему інформаційних ресурсів, пов'язаних із функціонуванням платіжних систем, через які проводяться транзакції.

Досліджуючи обстановку функціонування платіжних систем у банківській сфері, низкою дослідників виявлено, що в умовах зменшення кількості клієнтів, що утримують або знімають кошти з банківських рахунків завдяки доступності цифрового банкінгу та безготівкових платежів, необхідність фізичної присутності клієнтів при наданні банківських послуг постійно зменшується. Водночас із зменшенням кількості банківських філій та зростанням кількості користувачів цифрового банкінгу виникає необхідність у розширенні автоматизації банків з метою запобігання загрозам цифрового шахрайства, що постійно еволюціонують. Крім того, пришвидшення процесингу платежів може нести новий виклик, оскільки банки матимуть менше часу на аналіз операцій на предмет шахрайства. Пришвидшення платежів також несе в собі ризик зменшення розміру відшкодування збитків, понесених у результаті шахрайства, оскільки проходження офшорних платежів через велику кількість рахунків здійснюватиметься за лічені секунди. У пошуках збалансованості між заходами із запобігання ризику шахрайства та відносинами з клієнтами, банки застосовують засоби запобігання та виявлення шахрайства у режимі реального часу та встановлюють обмеження й додаткові засоби аутентифікації для операцій з високим ступенем ризику шахрайства, прагнучи зменшити його під час онлайн-платежів. Аутентифікація псевдонімів також є ключовим моментом, зокрема у випадку операцій із стягнення платежів у режимі онлайн (pull

[121] Коваль Н. О., Борщ М. В. Особливості функціонування платіжних систем Україні на сучасному етапі їх розвитку. *Ефективна економіка.* 2012. № 10. URL: http://www.economy.nayka.com.ua/?op=1&z=1441 (дата звернення: 04.09.2025).

[122] Анапольська А. І. Розслідування шахрайств і пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : дис. ... канд. юрид. наук : 12.00.09 / Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ, 2010. 243 с.

payments), коли шахраї можуть вимагати здійснити платіж, представившись як комунальне підприємство або підприємство зв'язку[123].

Указане свідчить, що обстановку та умови здійснення розслідування кримінальних правопорушень у кіберпросторі визначає також рівень інформаційної безпеки у банківській сфері (на думку 87 % працівників Національної поліції).

Адже банки, які є членами платіжних систем, не завжди приділяють достатню увагу безпеці розрахунків та захисту інформації, а також не здійснюють належним чином моніторинг та відеоспостереження за банкоматами. Більше того, майже всі картки міжнародних платіжних систем, що їх емітують українські банки, є недостатньо захищеними, адже носієм інформації такого платіжного інструменту є магнітна смуга, а не чип. Шахрайство з використанням реквізитів платіжних карток в інтернеті характеризується збільшенням кількості фішингових сайтів, електронних листів та смс-повідомлень, за допомогою яких зловмисники отримують реквізити платіжних карток у держателів платіжних карток, емітованих банками України. Наявність в інтернеті багатьох різних електронних платіжних систем, пропонування великою кількістю банків послуг інтернет-банкінгу, доступність інтернету та розповсюдження зловмисниками інформації щодо реквізитів платіжних карток перетворили фішинг у дуже поширений та прибутковий вид шахрайства. Усі ці фактори дають можливість, особливо для молодих громадян, отримувати «легкі гроші» фактично безкарно, тому такий вид шахрайства набуває все більшого розповсюдження у країнах СНД та Європи. Щодня встановлюються тисячі підроблених фішингових вебсайтів у режимі онлайн, які, заманюючи будь-яку кількість споживачів, спричиняють проблеми та втрати ними коштів[124].

Своєю чергою, Л. Брич зауважує, що при визначенні місця вчинення шахрайства варто виходити з таких чинників, як:

– чи охоплюється поняттям «місце вчинення кримінального правопорушення» лише місце вчинення шахрайства – розташування ЕОТ за місцем проживання (роботи) злочинця чи за місцем проживання потерпілої особи;

– чи поширюється поняття місце вчинення шахрайства на місцезнаходження інших ознак складу кримінального правопорушення;

– як відрізнити випадки, коли певні просторові характеристики є місцем вчинення суспільно небезпечного діяння й, відповідно, самостійною ознакою шахрайства – місцем його вчинення, від випадків, коли ті чи інші просторові

[123] Багатостороння загроза шахрайства: чи готові банки гідно протистояти виклику. Глобальне дослідження з питань шахрайства у банківській сфері. URL: https://assets.kpmg/content/dam/kpmg/ua/pdf/2020/01/Global-Banking-Fraud-Survey.pdf (дата звернення: 01.09.2025).

[124] Харчук М. В. Аналіз масштабів та основні напрями мінімалізації ризиків шахрайства членів міжнародних платіжних систем. *Ефективна економіка*. 2013. № 6. URL: http://www.economy.nayka.com.ua/?op=1&z=2120 (дата звернення: 05.09.2025).

характеристики стосуються інших ознак складу шахрайства[125].

Проведений аналіз дозволяє зробити висновки, що більшість науковців здебільшого розглядають ознаки місця, часу та обстановки у взаємозв'язку. Проте, є й протилежні думки. Зокрема, С. І. Селецький вважає, що місце і час не входять у зміст поняття «обстановка», проте в поєднанні з останнім утворюють ситуацію вчинення злочину. На його думку, компоненти ситуації доповнюють один одного, зумовлюють якісно новий зміст зовнішнього оточення злочинного діяння, збільшують або зменшують комплекс норм, що забороняють якість дії або вимагають певної поведінки[126].

С. В. Самойлов серед місць вчинення шахрайства вирізняє такі як: «… місцезнаходження банкоматів (магазин, вулиця тощо); місцезнаходження підключених до мережі «Інтернет» комп'ютерних систем (місце роботи, навчання, проживання, «Інтернет-кафе», зона вільного підключення до мережі «Інтернет» із використанням технології «Wi-Fi» – так звані «FrceWi-Fi-zone» тощо); місцезнаходження установ, де впроваджено системи розрахунків за допомогою пластикових кредитних карток»[127].

А вже О. І. Мотлях зауважував, що «… проблеми вибору місця та часу злочинцем у здійсненні власних умислів зостається вкрай спірним серед учених-криміналістів». З-поміж указаних місць вчений виокремлює:

«– адміністративні та службові приміщення різного типу суб'єктів господарювання (підприємств, організацій, компаній, фірм тощо), які використовують у своїй виробничій діяльності операційні комп'ютерні системи та їх периферійні устаткування;

– власні та орендовані житлові приміщення (офіси, квартири, кімнати та інше), в яких встановлені комп'ютери (комп'ютер), що забезпечені виходом до всесвітньої мережевої системи Інтернет;

– приміщення комунальної власності або ж споріднені з ними (цокольні, напівпідвальні чи ті, що примикають до житлових будинків приміщення), котрі на правах власності чи оренди можуть використовуватися під комп'ютерні клуби, інтернет-кафе тощо»[128].

Натомість, ми не можемо погодитися з позицією щодо утворення ситуації через компоненти місця та часу замість обстановки вчинення злочину. Не можемо підтримати й тезу щодо неможливості існування часу та простору, не

---

[125] Брич Л. Місце вчинення злочину і його значення у розмежуванні складів злочинів та відмежуванні їх від складів інших правопорушень. *Вісник Львівського університету.* Серія: Юридична. 2011. Вип. 52. С. 267–280.

[126] Селецький С. І. Кримінальне право України. Загальна частина. Київ : Центр учбової літератури, 2008. 248 с.

[127] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … канд. юрид. наук. : 12.00.09. Донецьк : Донец. юрид. ін-т, 2014. 18 с.

[128]Мотлях О. І. Питанням методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09 / Акад. праці і соц. відносин Федерації профспілок України. Київ, 2005. 198 с.

пов'язаного з матеріальними об'єктами[129].

В контексті даної проблематики звернемо увагу на той факт, що місце вчинення злочину у криміналістиці традиційно розуміється як ділянка місцевості або приміщення, будівля, в межах яких було вчинено злочин та виявлено сліди[130].

Водночас О. Л. Мусієнко наголошує на тому, що при розслідуванні шахрайства місце вчинення злочину та місце події не завжди становлять єдиний комплекс. Місце злочину одне – це місце вчинення шахрайства, а місць події, пов'язаних із цією подією, може бути кілька: місце виготовлення підроблених документів, місце транспортування вилучених матеріальних цінностей тощо[131].

На основі вивчення й узагальнення матеріалів судово-слідчої практики (додаток В) можна визначити такі місця вчинення кримінальних правопорушень у кіберпросторі, а саме:

– місця розташування ЕОТ, з якої вчинялись протиправні дії (стаціонарне комп'ютерне обладнання, ноутбук, планшет, телефон) – 74 %;

– місця розташування ЕОТ, стосовно якої вчинялись протиправні дії (ПЕОМ, ноутбук, планшет, телефон) – 61 %;

– місця знаходження (розташування) банкоматів, фінансових установ, підприємств та організацій фінансової сфери – 21 %;

– місце знаходження потерпілого, який виявив факт вчинення кримінальних правопорушень у кіберпросторі – 12 %.

– інші – 6 %.

Хоча аналіз криміналістичної літератури засвідчив, що не всі вчені погоджуються зі складністю визначення часу. Зокрема, В. О. Голубєв стверджує, що встановлення часу вчинення кримінальних правопорушень з використанням ЕОТ не складає великих проблем, адже за допомогою програм загальносистемного призначення можна встановити поточний час роботи комп'ютерної системи. Це дозволить за відповідною командою вивести на екран дисплею інформацію про день, години, хвилини та секунди виконання тієї або іншої операції[132].

---

[129] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[130]Криміналістика : підручник / за ред. проф. В. Ю. Шепітька. 4-е вид., перероб. і допов. Харків : Право, 2008. 464 с.

[131]Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / за ред. проф. В. Ю. Шепітька. Харків : Право, 2009. 168 с.

[132] Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : монографія. Запоріжжя, 2003. 250 с.

З цього приводу Н. В. Павлова та В. В. Рец констатують, що «… з'ясування початку і закінчення злочинних дій та їх тривалості у часі має велике значення для визначення часу безпосереднього закінчення шахрайства»[133].

У цьому розрізі слід звернути увагу на думку М. В. Карчевського та Ю. О. Кучера, які пропонують розмежовувати юридичний і фактичний час вчинення злочину. Юридичний час вчинення злочину, на думку дослідників, – це загальна нормативна інформація про темпоральний вимір юридичного діяння та причинно пов'язаних із ним передбачених кримінальним законом наслідків. Фактичний час вчинення злочину – конкретна фактична інформація про тривалість реального діяння та причинно пов'язаних із ним певних наслідків, що настали в межах відповідного темпорального виміру, передбаченого певною нормою Особливої частини Кримінального кодексу України[134].

Так, Г. К. Авдєєва та С. В. Стороженко вважають, що час роботи користувача в мережі «Інтернет» на певній електронно-обчислювальній техніці можна встановити за спеціальним лог-файлом (журналом), а додаткові відомості про вид, порядок і час підключень користувача до мережі і збіг цих даних з лог-файлом провайдера може слугувати вагомим доказом використання саме цієї електронно-обчислювальної техніки для вчинення шахрайства[135].

Досить правильною в розрізі дослідження кримінальних правопорушень у кіберпросторі вважаємо думку Т. В. Коршикової, яка констатувала, що «цифрові сліди шахрайств, учинених з використанням ЕОТ, можуть утворюватися:

– на фізичних носіях комп'ютерної інформації (жорсткі диски, компакт-диски, флешкарти, накопичувачі інформації тощо), якими користувався злочинець;

– в оперативному запам'ятовуючому пристрої ЕОТ злочинця;

– в оперативному запам'ятовуючому пристрої периферійних пристроїв злочинця;

– в електронній поштовій скриньці злочинця (тут можуть міститися сліди переписки злочинця з потерпілим і, навпаки, а також переписка злочинця з іншими злочинцями);

– на інтернет-сайті, який використовувався злочинцем з метою вчинення шахрайства;

– як профіль у соціальних мережах злочинця («ВКонтакте», «Instagram», «Facebook», «Одноклассники», «Twitter» тощо);

---

[133]Павлова Н. В., Рец В. В. Визначення місця та часу вчинення шахрайства на первинному ринку нерухомості. *Науковий вісник Дніпропетровського університету внутрішніх справ.* 2018. № 3 (66). С. 139–143.

[134] Кримінальне право. Загальна частина : підручник / за ред. А. С. Беніцького, В. С. Гуславського, О. О. Дудорова, Б. Г. Розовського. Київ : Істина, 2011. 1121 с.

[135] Авдєєва Г. К., Стороженко С. В. Електронні сліди: поняття та види. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2017. № 1 (77). С. 168–174.

– внаслідок проведення банківських платежів між потерпілим і злочинцем (рахунок в електронних платіжних системах («Qiwi-гаманець», Perfect Money тощо);

– під час зняття злочинцем у банкоматах коштів, отриманих злочинним шляхом»[136].

Також варто привести тезу П. Д. Біленчука, О. П. Дубового, М. В. Салтевського та П. Ю. Тимошенка стосовно того, що «… безумовно, що частіше від комп'ютерних злочинів страждають більш розвинуті у технічному відношенні країни, однак й інші країни, з початком процесу комп'ютеризації стають родючим ґрунтом для вчинення таких злочинів. Зокрема, глобальна комп'ютерна мережа Інтернет надає можливість увійти до будь-якої американської відомчої комп'ютерної системи, у тому числі і військової. До того ж, це можливо зробити майже з будь-якої точки світу. У порівнянні з США, національна безпека України поки що залежить від комп'ютерних мереж значно менше. На сьогодні, ми стикаємось з комп'ютерними злочинами, в основному, у фінансово-кредитній сфері. Але у недалекому майбутньому такі злочини можуть привести до глобальних катастроф – екологічних, транспортних тощо. Введення сучасної системи управління повітряним рухом, поширення телекомунікаційної мережі, впровадження системи електронних платежів, використання комп'ютерів у діяльності правоохоронних органів та керуванні військами значно розширили сферу діяльності для хакерів»[137].

У криміналістичній літературі справедливо підкреслюється необхідність врахування у криміналістичній характеристиці кримінального правопорушення даних про сліди[138].

Для прикладу, С. М. Зав'ялов відмічав, що «… подія злочину – це один із матеріальних процесів дійсності, що перебуває у зв'язку і взаємообумовлена з іншими процесами, подіями і явищами, відбивається в них і сама є відображенням якихось процесів. Будь-яка подія пов'язана зі змінами в навколишньому середовищі, і для того щоб дізнатися про подію злочину, необхідно виокремити пов'язані з ним зміни. Лише за слідами, які досліджуються в ході розслідуваної події, можна судити про його зміст»[139].

Прихильниками класичного підходу, що містить в собі єдність матеріальних та ідеальних слідів злочину, є М. В. Салтевський, В. Я. Сегай та інші

---

[136] Коршикова Т. В. Особливості слідової картини шахрайств, що вчиняються в мережі Інтернет. *Молодий вчений*. 2016. № 1 (28). Ч. 2. С. 51–54.

[137] Біленчук П. Д., Дубовий О. П., Салтевський М. В., Тимошенко П. Ю. Криміналістика : підруч. для слухачів, ад'юнктів, викладачів вузів системи МВС України / за ред. акад. П. Д. Біленчука. Київ : АТІКА, 1998. 416 с.

[138] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[139] Зав'ялов С. М. Спосіб вчинення злочину: сучасні проблеми вивчення та використання у боротьбі зі злочинністю : автореф. дис. … канд.. юрид. наук : 12.00.09. Київ, 2005. 20 с.

вчені[140].

Натомість, як засвідчили результати емпіричних досліджень та аналіз криміналістичної літератури, механізм слідоутворення при вчиненні шахрайства в сфері банківських електронних платежів доволі специфічний, адже ряд операцій здійснюється у віртуальному форматі[141].

На цьому наголошує й О. А. Самойленко, стверджуючи, що використання кіберпростору для вчинення традиційного злочину суттєво детермінує механізм його вчинення. Застосування технологій кіберпростору (телекомунікаційних мереж, комп'ютерних систем й пристроїв), як знарядь досягнення протиправної мети призводить до утворення специфічних змін (слідів в криміналістичному сенсі) в самому кіберпросторі як інформаційному просторі взаємодії людей[142].

А. В. Рейнгольд констатував, що «… шахрайство в інтернет-комерції характеризується специфікою слідів, що можуть залишатися на таких носіях:

– пам'яті телефону – 78 %;

– сім-картці – 48 %;

– комп'ютері – 81 %;

– сервері мобільного оператора – 18 % або інтернет-провайдера – 17 %;

– флешці чи зовнішньому вінчестері – 38 %;

– пам'яті електронного журналу банкомату (терміналу) – 67%;

– історії платіжних переказів через банківську систему – 78 %;

– квитанціях і роздруківках про електронні банківські платежі – 51 %;

– банківських картках – 37 %;

– пам'яті системи відеоспостереження (зал інтернет-кафе, фойє банку, місце біля банкомату) – 31 %;

– слідах папілярних ліній на засобах комп'ютерної техніки, клавіатурі терміналу – 38 % та ін.»[143].

Отже, із появою нових можливостей здійснення фінансових операцій за допомогою різних технологій – інтернету, мобільних, безконтактних пристроїв, спеціальних програмних додатків набувають особливого значення віртуальні сліди[144]. При цьому, сліди вчинення таких злочинів рідко

---

[140] Салтевський М. В. Криміналістика : підручник у 2-х ч. Харків : Консум ; Основа, 1999. Ч. 1. 416 с.

[141]Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос.ї : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[142] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса :ТЕС, 2020. 372 с.

[143] Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції : автореф. дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2023. 20 с.

[144]Яровенко Г. М., Ковач В. О. Моделювання портретів потенційних шахрая та жертви банківських шахрайств. *Ефективна економіка*. URL: http://www.economy.nayka.com.ua/pdf/10_2018/63.pdf (дата звернення: 05.09.2025).

залишаються у вигляді видимих змін навколишнього середовища. Вони в основному не розглядаються сучасною трасологією, оскільки в більшості випадків мають інформаційний характер, тобто є тими або іншими змінами в комп'ютерній інформації, що виражається у формі її блокування, копіювання, модифікації, знищення. Скоєння особою протиправних дій, пов'язаних з використанням комп'ютерних технологій, спричиняє виникнення певної кількості слідів, у тому числі й специфічних, притаманних лише зазначеній категорії злочинів. Використання цих інформаційних даних при розслідуванні злочинів є необхідною умовою забезпечення всебічного, повного й об'єктивного дослідження обставин кримінального провадження[145].

А вже Т. В. Охрімчук підтверджувала те, що сліди шахрайства з фінансовими ресурсами у криміналістичній площині можуть визначатися з двох сторін: «… як особливості матеріальної шкоди, спричиненої вчиненням злочину; особливості механізму слідоутворення та змісту слідів (інформації)». Авторка з'ясувала, що «в цілому слідова картина злочину, передбаченого статтею 222 КК України, визначена способом вчинення такого виду протиправного діяння та характеризується наявністю матеріальних та ідеальних джерел інформації. Тобто слідова картина злочину шахрайства з фінансовими ресурсами обумовлена способом вчинення злочину та характеризується наявністю матеріальних (документи різного виду та значення) та ідеальних (показання осіб, які володіють необхідними відомостями про обставини вчинення злочину) джерел інформації»[146].

У цьому розрізі слід погодитися із А. С. Білоусовим, що необхідність виокремлення слідів такого роду в самостійну групу як окремих об'єктів пов'язана з особливістю протиправних дій з комп'ютерною інформацією, що полягає в тому, що місце вчинення безпосередніх протиправних дій і місце, де наступають наслідки злочину й де вони можуть бути виявлені, можуть перебувати на досить таки великій відстані одне від одного[147].

А вже Е. В. Малютін зауважував, що «… більшість протиправних дій відображаються у віртуальних, цифрових або комп'ютерних слідах. Вказані електронні сліди здебільшого вилучаються з таких місць як: з профілів соціальних мереж та онлайн-магазинів, кеш-пам'яті акаунтів і web-браузерів, флеш-носіїв, месенджерів (Telegram, Facebook, Instagram, Twitter) для криптовалютних переписок, пам'яті та кеш-пам'яті ЕОТ, бази інтернет-провайдерів. У випад-

[145] Дуда Х. І. Поняття комп'ютерних слідів злочину. *Науковий вісник Національного університету біоресурсів і природокористування України.* 2014. Вип. 197. Ч. 1. С. 262–267.

[146] Охрімчук Т. В. Криміналістична характеристика шахрайства з фінансовими ресурсами. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. № 23. С. 369–374.

[147] Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : автореф. дис. … канд. юрид. наук : 12.00.09 / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2008. 20 с.

ках безпосередньої зустрічі зі злочинцем чи спілкуванні з ним у форматі відеоконференції потерпілий може вказати відомості про його зовнішність злочинця»[148].

Зі свого боку, Б. М. Головкін, О. І. Денькович, В. В. Луцик та Д. М. Цехан відмічали, що «… в окремих слідчих ситуаціях, а саме, коли об'єкти сфери високих інформаційних технологій використовувались як засоби зв'язку злочинців, для розповсюдження порнографічних предметів, розміщення інформації про продаж заборонених товарів тощо, виникає необхідність надання статусу доказів інформації, яка розміщення в мережі Інтернет. На сьогодні, на фрагментарному рівні практикою вироблені окремі методи фіксації змісту веб-сайту з метою подальшого використання у кримінальному судочинстві: роздруківка веб-сторінки через браузер; роздруківка та подання рапорту працівником поліції; огляд веб-сайту слідчим у присутності понятих – аналогічний огляд разом зі спеціалістом; відповідь провайдера на запит щодо змісту сайту. З метою забезпечення допустимості «цифрових доказів» необхідно використовувати можливості сучасних судових техніко-криміналістичних експертиз, зокрема: експертизи комп'ютерної техніки і програмних продуктів, інформаційно-комп'ютерної експертизи та комплексної експертизи. При цьому увага експерта має зосереджуватися на виявленні ознак модифікації цифрової інформації, її способів та меж»[149].

З цього виходить, що віртуальні сліди (їх ще називають електронно-цифрові) є проміжним явищем між традиційними матеріальними та ідеальними слідами, адже процес передачі інформації, що полягає у передачі електронно-цифрового коду, здійснюється завдяки матеріальним носіям (комп'ютерам, телефонам тощо). Утім, на відміну від ідеальних слідів, які залишаються у пам'яті людини, процес здійснення передачі електронної інформації залишається в пам'яті комп'ютерних та інших цифрових пристроїв[150].

У контексті окресленої проблематики слід звернути увагу на думку А. С. Білоусова, який наголошує, що віртуальні сліди існують об'єктивно на матеріальних носіях, але не доступні для безпосереднього сприйняття. Для їх сприйняття потрібне обов'язкове застосування програмно-технічних засобів, отже наявність таких слідів на матеріальному носієві наближує цю групу до

[148] Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції : автореф. дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2023. 20 с.

[149] Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посіб. / Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL: law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (дата звернення: 07.09.2025).

[150] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

матеріальних слідів, але не робить їх такими. Отримані з матеріального носія та сприйняті віртуальні сліди внутрішньо ненадійні завдяки природі їх існування, тому що їх можна неправильно прочитати, наприклад, застосувавши інші програмно-технічні засоби, легко підробити, легко втратити. Це близько до суб'єктивного сприйняття та наближає такі сліди до ідеальних, але не може бути ототожненим з останніми. Віртуальні сліди зберігаються в ідеальному вигляді, але не в пам'яті людини, а в машинній пам'яті і на матеріальних носіях машинної інформації, їх виявляють з використанням технічних засобів відповідно до певних алгоритмів[151].

Як підсумок, за місцем вчинення кримінальних правопорушень у кіберпросторі існують такі сліди:

– ЕОТ (ПЕОМ, їх системні блоки, ноутбуки);

– монітори, принтери, дисководи, модеми, сканери, клавіатури, маніпулятори, джойстики та інше, комунікаційні прилади комп'ютерів і обчислювальних мереж;

– жорсткі диски, оптичні диски, флешпам'ять

– засоби зв'язку (у разі їх використання під час вчинення протиправних дій) – на стільникових апаратах, засобах телекомунікації, спеціальних електронних картках, електронних ключах доступу до персонального комп'ютера; пристроях упізнання користувача;

– електронні записні книжки, інші електронні носії текстової або цифрової інформації, технічна документація до них;

– сліди пальців рук і мікрочастинки або мікрооб'єкти (наприклад, частки волосся), які можуть залишатися на вказаних вище предметах;

– сліди, що залишаються на «робочому» місці кіберзлочинця, (наприклад, які-небудь рукописні записи – списки паролів, коди, чернетки тощо)[152].

Телефонні дзвінки з мобільного телефону та тексти смс-повідомлень також автоматично фіксуються й накопичуються на сервері оператора мобільного зв'язку та можуть бути отримані слідчим[153] Сліди можуть міститися також в історії голосових повідомленнях і відеодзвінках (відеододатки Skype, Google Hangouts, Zoom тощо). Утім, найцінніша інформація криється у доменній адресі (IP), що дозволяє встановити місцезнаходження точки доступу до

[151] Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів: автореф. дис. … канд. юрид. наук : 12.00.09 / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2008. 20 с.

[152]Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … д-ра філос. : 081 – Право / Нац. акад. внутр. справ, Київ, 2021. 255 с.

[153] Авдєєва Г. К. Сутність цифрових слідів у криміналістиці. *Актуальні питання судової експертизи та криміналістики* : зб. матеріалів Міжнарод. наук.-практ. конф., присвяч. 95-річчю створення Харків. НДІ суд. експертиз ім. засл. проф. М. С. Бокаріуса (Харків, 10–11 жовт. 2018 р.). Харків, 2018. С. 90–93.

комп'ютера, з якого здійснювалося спілкування[154].

Виходячи з викладеного вище, а також на основі опрацювання дисертаційного дослідження І. О. Коваленка[155] та аналізу й узагальнення матеріалів кримінальних проваджень (додаток Б) було визначено, що при розслідуванні кримінальних правопорушень у кіберпросторі домінуюче місце посідають електронно-цифрові (віртуальні) сліди, що містяться:

– у пам'яті ЕОТ, планшетів (98 %);

– у пам'яті мобільного телефону (IMEI-код; історія телефонних з'єднань, історія голосових повідомлень; історія текстових повідомлень; програмне забезпечення для проведення банківських операцій з телефону тощо) (84 %);

– у електронній поштовій скриньці (77 %);

– на флешкарті (файли, папки тощо) (75 %);

– інформація в електронному вигляді, яка відображає суми грошових коштів, переказаних через певну систему електронних платежів («ПриватБанк», «Qiwi-гаманець», MoneyGram, Western Union, Perfect Money та ін.) (59 %);

– на сервері мобільного оператора (56 %);

– профіль у соціальних мережах, інформація на сайтах (43 %) тощо;

– у пам'яті сім-карти (32 %);

– на сервері інтернет-провайдера (сервер зберігання flow-статистики и біллінгової інформації, сервер баз даних тощо) (21 %).

Як слушно зазначає В. В. Сисолятін, «… особа правопорушника є одним з основних елементів майже всіх сучасних криміналістичних характеристик. Це пояснюється кількома чинниками. По-перше, вказаний елемент має чітко виражені кореляційні зв'язки з іншими складовими досліджуваної наукової категорії. А по-друге, він у будь-якому випадку має місце в криміналістичній характеристиці, адже без його встановлення не буде повним склад кримінального правопорушення. Тому вважаємо за необхідне здійснити криміналістичний аналіз особи, яка вчиняє протиправні діяння, пов'язані з використанням

[154] Чучко С. В. Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет: дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2021. 276 с.

[155] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

інтернет-банкінгу[156].

У розрізі зазначеного вважаємо доцільним привести твердження групи вчених-криміналістів (П. Д. Біленчука, О. П. Дубового, М. В. Салтевського, П. Ю. Тимошенка), які акцентували увагу на тому, що криміналістика насамперед вивчає «професійні» звички злочинця. Також дослідники зауважили, що вони «… проявляються, в основному, в певних способах і прийомах учинення злочинів, залишають на місці вчинення злочинів характерний «почерк» злочинця: результати кожної злочинної діяльності містять сліди людини, яка їх залишила. Виявлення на місці вчинення злочину речових доказів проливають світло як на відомості про деякі його особисті соціально-психологічні ознаки, так і на відомості про його злочинний досвід, професію, соціальні знання, стать, вік, особливості взаємодії з потерпілим. Криміналістично значущі дані про особу злочинця в даний час базуються на двох специфічних групах інформації.

Перша група включає до себе дані про особу невідомого злочинця по залишених ним слідах як на місці події, в пам'яті свідків, так і за іншими джерелами з метою встановлення напрямку і прийомів його розшуку і затримання. Така інформація дає уяву про загальні ознаки певної групи осіб, серед яких може бути і злочинець. Такі відомості слід співставляти з наявними криміналістичними даними про особу, яка скоріше всього вчинює злочини розслідуваного типу.

Друга група об'єднує інформацію, яка отримана за допомогою вивчення особи затриманого підозрюваного чи обвинувачуваного з метою вичерпної криміналістичної оцінки особи – суб'єкта злочину. З цією метою збираються відомості не тільки про ціннісні орієнтації, особливості антисуспільних поглядів, але і про те, яка інформація найбільше характеризує особу суб'єкта злочину, його зв'язки, особливості поведінки до, під час і після вчинення злочину може допомогти слідчому чи оперативному працівнику знайти зі злочинцем необхідний психологічний контакт, отримати правдиві свідчення, а також вибрати найбільш дієві способи профілактичного впливу на нього. Вважається, що ця інформація, з врахуванням відомостей про злочинців, які відображаються в інших елементах криміналістичної характеристики, може бути покладена в основу типізації злочинців. Формування банку типових моделей різних категорій злочинців, вивчення загальних рис цих людей, дозволяє оптимізувати процес виявлення кола осіб, серед яких потрібно вести пошук злочинця»[157].

Інша група науковців (Ю. В. Александров, А. П. Гель, Г. С. Семаков)

[156] 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 Міжнарод. наук.-практ. конф. (м. Київ, 13–14 березня 2023 р.). Київ : НДІ публічного права, 2023. С. 31–33.

[157] Криміналістика : підруч. для слухачів, ад'юнктів, викладачів вузів системи МВС України / за ред. акад. П. Д. Біленчука. Київ : АТІКА, 1998. 416 с.

вказує, що «особа злочинця – це сукупність соціальних властивостей, ознак, зв'язків і відносин, що характеризують особу, яка порушує кримінальний закон, і в поєднанні з іншими (не особистісними) умовами й обставинами спонукають особу до антисуспільної поведінки»[158].

Тобто бачимо, що друге визначення розширене шляхом додавання таких характеристик, як зв'язки та відносини, що характеризують особу.

Своєю чергою, В. В. Бедь указував на те, що злочинна поведінка зумовлена взаємодією особистості із соціальним середовищем. Автор наголошував на тому, що політичні, соціально-економічні, духовні сторони суспільства здійснюють зовнішній вплив на формування механізму злочину, а психічні особливості формують механізм злочину з середини. Учений робить висновок, що психологія організованої злочинності характеризується спільністю злочинних цілей та інтересів її учасників. При цьому, злочинна група створюється з метою здійснення не одного єдиного кримінального правопорушення, а для постійної та довготривалої протиправної діяльності[159].

Водночас окрема група вчених (В. І. Курило, О. Є. Михайлов, О. С. Яра) зазначає, що кримінологічний аспект вивчення особи злочинця припускає різні «рівні» узагальнення цього поняття: конкретна особа, різні категорії злочинців, загальне поняття злочинця і містить у собі вивчення всіх зовнішніх і внутрішніх обставин, що сформували її як особу. Автори акцентують увагу на тому, що в цьому плані кримінологічний аспект найбільш широкий і містить у собі як кримінально-правовий, так і процесуальний моменти[160].

Зі свого боку, І. В. Пиріг та В. В. Самсонова зазначили, що «… для повної характеристики особи злочинця необхідно мати такі дані:

– фізико-біологічні властивості особи (стать, вік, зріст, статура, фізичні дані тощо);

– соціально-демографічні (національність, освіта, сімейний стан тощо); морально-психологічні (світогляд, переконання, риси характеру, звички, емоції, темперамент тощо);

– соціально-побутові (місце проживання, роботи, навчання, суспільні відносини у при виконанні окремих видів діяльності);

– соціально-правові (злочинний досвід, наявність судимості, ставлення до вчиненого тощо)»[161].

Своєю чергою, Л. В. Сорокіна вказує, що «… слід вивчати не тільки тих,

---

[158] Александров Ю. В., Гель А. П., Семаков Г. С. Кримінологія : курс лекцій. Київ : МАУП, 2002. 296 с.

[159] Бедь В. В. Юридична психологія : навч. посіб. Київ : Каравелла ; Львів : Новий світ-2000, Магнолія плюс, 2003. 376 с.

[160] Курило В. І., Михайлов О. Є., Яра О. С. Кримінологія: загальна частина : курс лекцій. Київ : Кондор, 2006. 192 с.

[161] Самсонова В. В., Пиріг І. В. Методика розслідування крадіжок, вчинених на території садівницьких товариств і дачних кооперативів : монографія. Дніпропетровськ : ДДУВС ; Ліра ЛТД, 2017. 212 с.

хто вже вчинив злочин, а й тих, чий спосіб життя, спілкування, погляди й орієнтації ще тільки свідчать про можливість учинення злочину. Тобто у сфері кримінологічних інтересів знаходяться також і ті особи, поведінка яких має антигромадський характер. Отже, предметом вивчення кримінології є не тільки особа власне злочинця, а й ті, хто може стати на злочинний шлях, що вкрай важливо для боротьби зі злочинністю»[162].

Підбиваючи підсумок з цього питання, вважаємо за доцільне вказати, що кіберзлочинець характеризується такими групами ознак: 1) загальнодемографічні (стать, національність, вік); 2) соціальної ролі (вид занять, сімейний стан, належність до певних соціальних груп); 3) мотив, відношення до вчиненого протиправного діяння та поведінка в ході досудового розслідування; 4) рецидив діяння.

Переходячи до розгляду вказаних обставин, вважаємо за потрібне привести класифікації шахраїв, надані різними науковцями. Так, окрема група вчених (П. Д. Біленчук, В. В. Кравчук, О. В. Кравчук, В. М. Кулик) виділяє дві групи злочинців:

– внутрішні користувачі;

– зовнішні користувачі як суб'єкти, що звертаються до інформаційної системи як посередника, аби отримати необхідний доступ для користування інформацією. Такий підхід загалом набув підтримки багатьох криміналістів, до кола інтересів яких належить дослідження особи комп'ютерного злочинця[163].

Своєю чергою, О. Л. Мусієнко, проаналізувавши особу шахрая як елемент криміналістичної характеристики, визначив необхідність наявності таких її ознак: соціально-демографічні, кримінально-правові, морально-психологічні[164].

О. А. Самойленко стверджує, що з огляду на аналіз слідів вчинення шахрайства уповноважена особа може зробити висновок щодо професіонального рівня користувача як правопорушника, що зумовлене певною сукупністю ознак, зокрема:

– здатність злочинця використовувати технології анонімізації доступу до ресурсів інтернету (проксі-сервісів (комплексів програм), віртуальних приватних мереж, інших засобів – анонімайзерів);

---

[162] Сорокіна Л. В. Особа злочинця, яка вчиняє злочини у сфері пенсійного забезпечення. *Правовий часопис Донбасу.* 2019. № 1 (66). С. 99–106.

[163] Біленчук П. Д., Кравчук В. В., Кравчук О. В., Кулик В. М. Комп'ютерний тероризм: практика запобігання, протидії, розслідування : навч. посіб. / за заг. ред. П. Д. Біленчука. Хмельницький : Хмельн. ЦНТЕІ, 2008. 258 с.

[164] Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / за ред. проф. В. Ю. Шепітька. Харків : Право, 2009. 168 с.

– мобільність злочинця (індивідуальна професійна, соціальна або географічна);

– психологічні характеристики (ознаки) злочинця, що впливають на формування й реалізацію злочинної мети;

– роль у складі організованої групи[165].

Цікаво розкриває розглядуваний елемент криміналістичної характеристики О. В. Курман, зокрема: «… характеризуючи особу шахрая з фінансовими ресурсами, що це, перш за все, «білокомірцевий» тип злочинця. Дані особи вчинюють злочини без застосування насильства, з використанням неправдивих методів з метою здобуття фінансових прибутків. За своїм суспільним станом вони належать до підприємців, є професіоналами високого або середнього рівня у сфері кредитно-фінансових відношень, у більшості випадків добре орієнтуються у законодавстві – податковому, банківському, володіють знаннями в бухгалтерському обліку. У минулому багато з них мають досвід роботи в державному секторі на посадах, пов'язаних з виконанням організаційно-розпорядчих або адміністративно-господарських обов'язків. Для особи шахрая з фінансовими ресурсами також характерно вчинення злочину як однією особою (50 %), так і групою, і, як правило, через корисливі мотиви (84,4 %). … у переважній більшості випадків шахрайство з фінансовими ресурсами вчинюють чоловіки (74,8 %) віком від 31 до 50 років (31–40 років – 41,5 %; 41–50 років – 47,4 %), які мають вищу освіту (53,3 %), займають керівні посади на підприємствах (у господарських товариствах) (69,6 %) і вчинюють злочин, як правило, у межах одного населеного пункту (88,2 %). Тривалість злочинних дій складає, у більшості випадків, – від шести місяців (16,3 %) до двох років (57 %).

За цей час злочинці встигають незаконно одержати кредит або скористатися правом на пільгове оподаткування від одного до восьми раз (один раз – 50,9 %; два рази – 20 %; три – 13,6 %; п'ять разів – 6,4 %; шість – 4,6 %; вісім – 2,7 %)»[166]. Отже, почнемо виклад власного дослідження.

Так, на підставі аналізу й узагальнення кримінальних проваджень (додаток Б) визначено, що кримінальні правопорушення у кіберпросторі переважно вчиняють чоловіки – 75 %.

Така характеристика, як вік особи є обов'язковою позицією у протоколах допиту підозрюваного та у повідомленні про підозру, і, про що свідчить аналіз кримінальних проваджень (додаток Б), кримінальні правопорушення у кіберпросторі вчинюються у такому

[165] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

[166] Курман О. В. Методика розслідування шахрайства з фінансовими ресурсами : автореф. дис. … канд. юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2002. 16 с.

віці: на момент вчинення протиправного діяння кіберзлочинці перебували у віці 18–25 років (33 %), 25–35 років (42 %), 35–45 (19 %), 45 років і старше (11 %). Отже, найбільш криміногенну групу становлять особи віком 25–35 років.

Залежно від рівня освіти кіберзлочинців з'ясовано (додаток Б), що базову середню освіту має 1 %, середню – 1 %, середню спеціальну - 4 %, базову вищу – 17 %, повну вищу – 77 %.

Як зазначає певна група науковців (М. І. Стрюк, С. О. Семеріков, А. М. Стрюк), «… у кіберпросторі злочинець-користувач може бути суб'єктом багатьох соціальних спільнот (груп) у соціальних мережах, мати багато активних акаунтів (з англ. *account*) чи профілів, облікових записів, або ж узагалі не мати потреби в цьому. Варто додати, що географічна мобільність не завжди пов'язана з професійною, адже людина може мати високий ступінь географічної мобільності без можливості змінити особистий вибір і компетентність (роз'їзна робота з низьким рівнем професійної, соціальної та економічної мобільності)»[167]. Тобто, рівень освіти впливає, звичайно, і на професійний стан кіберзлочинця.

Так, щодо професійної зайнятості (додаток Б) було зроблено висновок, що переважна більшість кіберзлочинців (57 %) працювали у сфері підприємницької діяльності та сфері комп'ютерних технологій.

Доречною вважаємо позицію О. А. Самойленко, яка пропонує правопорушників, які вчиняють протиправне діяння із застосуванням становища кіберпростору, розділити на п'ять типів: 1) злочинець – користувач початкового рівня; 2) злочинець – користувач; 3) злочинець – упевнений користувач; 4) злочинець – досвідчений користувач; 5) злочинець – користувач-професіонал. Авторка робить висновок, що злочинець – користувач початкового рівня з урахуванням своїх професійних навичок роботи з комп'ютером не використовує технології анонімізації доступу до ресурсів інтернету; характеризується високою соціальною мобільністю з різних причин (нереалізованість комунікаційних потреб (людина з обмеженими фізичними можливостями, наявність психічних хвороб), наявність географічної мобільності, за відсутності професійної та економічної мобільності (сезонний працівник; робота за кордоном вахтовим методом; кур'єр; водій; сортувальник тощо, причому злочинець виконує роботи низької кваліфікації). Учена виснує, що проблеми конкуренції мотивів вчинення злочину він не має, його злочинна діяльність зазвичай ста-

[167] Стрюк М. І., Семеріков С. О., Стрюк А. М. Мобільність: системний підхід. *Інформаційні технології і засоби навчання.* 2015. № 5. Т. 49. С. 41–49.

новить собою елементарну вольову дію, як-от розміщення в інтернеті інформації певного місту[168]. Як бачимо, це підтверджує наші емпіричні відомості.

З огляду на сказане слід відмітити досить низький показник кількості раніше засуджених осіб – лише 6 % (додаток Б).

Також було з'ясовано (додаток Б), що кримінальні правопорушення у кіберпросторі вчиняють як члени ОГ та ЗО (26 %), так і окремі особи (74 %). Організатор групи безпосередньо управляє її діяльністю.

Підсумовуючи, відмітимо, що кримінальні правопорушення у кіберпросторі в основному вчиняють особи чоловічої статі у віці 25–35 років, які мають вищу освіту, працюють у сфері підприємницької діяльності та сфері комп'ютерних технологій та характеризуються високим інтелектуальним розвитком.

Стосовно особи потерпілого у частині 1 статті 55 КПК України міститься поняття: потерпілим у кримінальному провадженні може бути фізична особа, якій кримінальним правопорушенням завдано моральної, фізичної або майнової шкоди, юридична особа, якій кримінальним правопорушенням завдано майнової шкоди, а також адміністратор за випуском облігацій, який відповідно до положень Закону України «Про ринки капіталу та організовані товарні ринки» діє в інтересах власників облігацій, яким кримінальним правопорушенням завдано майнової шкоди[169].

Крім того, М. В. Сенаторов «… завдяки дослідженню теорії кримінального права, положень кримінального закону та практики його застосування зробив висновок, що потерпілий від злочину та обставини, пов'язані з ним, мають значення для встановлення соціальної сутності злочину, з'ясування характеру та ступеня його суспільної небезпечності, криміналізації та декриміналізації діянь, диференціації кримінальної відповідальності. Чітка вказівка на потерпілого та обставини, пов'язані з ним:

– дозволяють відмежувати один злочин від іншого;

– виступають ознаками складу переважної частини злочинів;

– сприяють конкретизації інших ознак складу;

– враховуються при кваліфікації злочинів та призначенні покарання, а також при вирішенні питань чинності закону про кримінальну відповідальність у просторі, звільнення від кримінальної відповідальності та відбування

[168] Самойленко О. А. Типізація особи, що вчиняє злочин, пов'язаний із використанням обстановки кіберпростору (з позицій криміналістичної науки). *Підприємництво, господарство і право*. 2018. № 8. С. 195–201.

[169] Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.09.2025).

покарання»[170].

Водночас С. В. Чучко зауважує, що «… потерпілими від шахрайства, пов'язаного із купівлею-продажем товарів через мережу Інтернет, можуть виступати будь-які фізичні особи, підприємці, інші споживачі товарів та послуг. Втім, бажання швидкого придбання товару при мінімальних витратах, небажання прискіпливо та ретельно перевіряти історію постачальників товару та незахищеність конфіденційної інформації про себе роблять таких осіб жертвами шахраїв. Натомість, оцінити реальний відсоток потерпілих від таких шахрайств дуже складно, адже особи, яких ошукали, не завжди звертаються до правоохоронних органів. В основному причиною цьому є небажання таких осіб переживати довготривалу процедуру розслідування та невір'я у притягнення винних до кримінальної відповідальності через малу суму заподіяної шкоди. Хоча, мало потерпілих замислюються над тим, що у випадку наявності декількох епізодів загальна сума спричиненої шкоди від дій шахраїв поступово збільшується, і, за наявності доказової бази, можна притягнути винних до кримінальної відповідальності за значні збитки»[171].

А вже С. В. Головкін з огляду на проведене дослідження наголошує на тому, що «… віктимність поведінки потерпілих виражена не лише у довірливості до інших людей чи у наявності негативних соціальних характеристик. Іноді самі власники майна створюють всі підстави для вчинення стосовно них шахрайства, наприклад, купують певне майно за значно заниженими цінами, не звертають уваги на інформацію про власника повідомлення (наявність установчих даних, телефону), користуються під час купівлі підозрілими сайтами і т. ін.»[172].

Зі свого боку, В. А. Журавель наголосив на тому, що «… інформація про вказану категорію осіб або ж відомості, надані потерпілим, можуть бути використані під час висунення слідчих версій, планування початкового та подальшого етапів розслідування, розроблення заходів криміналістичної профілактики тощо. Актуальність та практична корисність опрацювання особи потерпілого детермінували появу віктимологічного підходу у криміналістиці, відповідно до якого збір даних про правопорушника починається безпосередньо з дослідження особи та поведінки потерпілого»[173].

---

[170] Сенаторов М. В. Потерпілий від злочину в кримінальному праві : автореф. дис. … канд. юрид. наук : 12.00.08 / Нац. юрид. акад. України. Харків, 2005. 20 с.

[171] Чучко С. В. Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2021. 276 с.

[172] Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2008. 18 с.

[173] Журавель В. А. Початок досудового розслідування: деякі процесуальні та організаційно-тактичні проблеми. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2015. № 1. С. 251–258.

Досить цікавою є думка О. І. Резнікової, яка зауважила, що про криміналістичну віктимологію йдеться в тих випадках, коли експерти в сфері побудови психологічного портрета визначають формулювання віктимології як дослідження жертви або жертв конкретного протиправного діяння[174].

Цікавою в розрізі останніх думок є позиція С. В. Самойлова, який зазначає, що для дослідження особи потерпілого всіх потерпілих поділено на дві категорії:

– активних користувачів мережі, які постраждали внаслідок недобросовісного виконання обов'язків за договором купівлі/продажу (обміну);

– користувачів, які мають невеликий досвід використання мережі та стали потерпілими внаслідок відсутності необхідних знань про заходи обережності в інтернеті.

Вчений наголошує, що серед потерпілих обох категорій наявні особи, які навмисно порушують вітчизняне законодавство чи законодавство інших країн[175]. Як бачимо, поділ на відповідні групи має місце в науковій літературі.

Р. І. Благута, О. І. Гарасимів та О. М. Дуфенюк констатували, що типова особа потерпілого є системою соціально-демографічних показників (стать, вік, освіта, місце праці, навчання, роботи, сімейний стан, судимість тощо), які дають змогу сформувати комплексний портрет особи в суспільстві[176].

Своєю чергою, М. Ю. Литвинов вказує, що «… потерпілими можна вважати й магазини електронної торгівлі в тих випадках, коли зловмисники використовували точну копію сайту реально існуючого магазину з метою отримання конфіденційної фінансової інформації про клієнтів магазину (наприклад, дані кредитних карт). В цьому випадку репутація магазину може постраждати. Наприклад, добре підготовлені в технічному плані шахраї, досконально вивчили механізми електронних угод, можуть зламати локальну мережу інтернет-магазину і скопіювати звідти все програмне забезпечення, включаючи бухгалтерські програми і списки імен і паролів. Після цього, увійшовши в Мережу, вони стають клонами цього магазину і можуть відслідковувати всі операції. Як тільки, нічого не підозрюючи, покупець здійснить покупку, до шахраїв потрапляє інформація про його кредитну картку. Після цього злочинець, використовуючи викрадене програмне забезпечення, списує з рахунку покупця гроші за покупку ще раз і переводить їх на рахунок магазину. Після цього, знову від імені магазину, оформляє повернення. Однак гроші повертати не законному власнику, а на рахунок шахрая»[177].

---

[174] Резнікова О. І. Проблеми використання віктимологічних даних у криміналістичній характеристиці злочинів. *Питання боротьби зі злочинністю*. 2014. Вип. 27. С. 288–294.

[175] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … канд. юрид. наук : 12.00.09. Донецький юридичний інститут. Донецьк, 2014. 18 с.

[176] Криміналістика : підручник / за заг. ред. Є. В. Пряхіна. 3-тє вид., переробл. та допов. Львів : ЛьвДУВС, 2016. 948 с.

[177] Літвінов М. Ю. Світова та українська практика боротьби з кіберзлочинністю. *Право і безпека*. 2017. № 1. С. 85–89.

Крім зазначеного, не варто забувати й про державні організації та правоохоронні органи, працівники яких, а також в цілому їх технічне забезпечення, може піддаватися хакерським атакам.

Опрацювання матеріалів судово-слідчої практики (додаток Б) дозволило виокремити такі віктимогенні групи потерпілих:

– особи, які піддалися впливу знайомих і родичів при здійсненні різноманітних операцій на ЕОТ (ПЕОМ, планшети, смартфони);

– особи, які піддалися обману незнайомих осіб при здійсненні різноманітних операцій на ЕОТ (ПЕОМ, планшети, смартфони);

– особи, які з огляду на негативні психічні стани піддалися впливу незнайомих осіб при здійсненні різноманітних операцій на ЕОТ (ПЕОМ, планшети, смартфони);

– працівники державних організацій та правоохоронних органів при здійсненні різноманітних службових операцій на ЕОТ (ПЕОМ, планшети, смартфони);

– юридичні особи, які через специфіку своєї діяльності зазнали хакерських нападів.

Як бачимо, особа потерпілого має важливе значення для кримінальних проваджень за фактом вчинення кримінальних правопорушень у кіберпросторі.

Визначення ознак особи правопорушника (кіберзлочинця) та потерпілого має важливе значення для організації розслідування кримінальних правопорушень у кіберпросторі.

РОЗДІЛ 2
ОРГАНІЗАЦІЙНІ ЗАСАДИ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ

2.1. Криміналістичний аналіз первинної інформації та обставини, що підлягають встановленню у кримінальному провадженні

Криміналістичний аналіз та оцінка початкової інформації є одним із етапів здійснення досудового розслідування. На жаль, чинний КПК України досить обмежив вказаний етап у часовому плані – лише 24 години після отримання повідомлення про вчинене кримінальне правопорушення. Водночас з усіх слідчих (розшукових) дій та НСРД є можливість провести лише одну – огляд місця події, що ще більш ускладнює процес доказування відповідних протиправних діянь. Оскільки кіберпростір – досить специфічний об'єкт дослідження, який потребує наявності відповідних спеціалістів та техніко-криміналістичного забезпечення.

У розрізі сказаного наведемо позицію В. В. Сисолятіна, який зауважив, що «… аналіз первинної інформації має важливе значення майже у більшості кримінальних проваджень. Стосовно кримінальних правопорушень, пов'язаних з використанням Інтернет-банкінгу, слід зазначити, що вказаний етап дозволяє вирішити питання: а чи взагалі наявний факт скоєння визначеної категорії протиправних діянь? Тому беззаперечно уповноважені особи повинні ретельно і швидко аналізувати всі отримані та наявні відомості будь-якого характеру»[178].

Як зазначає О. А. Самойленко, «… специфічність механізму вчинення злочинів у кіберпросторі, зокрема, особливості їх слідів, які можуть бути легко фальсифіковані або взагалі знищені, обумовлює й особливості початку кримінального провадження щодо цих злочинів. Тут йдеться про ті особливості, які вимагають їх врахування з точки зору забезпечення судової перспективи таких справ»[179]. Тому, з одного боку, безсумнівно, користуватися безготівковим розрахунком за допомогою онлайн-банкінгу набагато зручніше, ніж готівкою. Не доводиться носити з собою грошові суми, а в тих випадках, якщо їх не вистачає при розрахунку за покупку, знову ж на допомогу приходить банківська карта,

[178] 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 Міжнарод. наук.-практ. конф. (м. Київ, 14–15 червня 2022 р.). Київ : НДІ публічн. права, 2022. С. 21–23.

[179] Самойленко О. А. Інформаційний продукт як предмет посягання при вчиненні злочинів із використанням обстановки кіберпростору. *Вчені записки Таврійського національного університету імені В. І. Вернадського.* 2018. Т. 29 (68). № 4. С. 165–169.

за якою можливо отримати кредит миттєво за допомогою смартфона й додатку банку. З другого боку, усі ці зручності та переваги шахраї використовують у своїх корисливих цілях і, отримавши верифікаційні дані протиправним шляхом, можуть здійснювати різні операції, розраховуючись за їх вчинення чужим майном, тобто грошовими коштами, які їм не належать[180].

А вже Ю. П. Аленін акцентує увагу на тому, що процесуальний порядок, встановлений у статті 214 КПК України, не враховує загальні положення процесуальної діяльності та національні правові традиції. Вчений наголошує, що будь-яка галузь процесуального права має передбачати попередній, перевірочний, фільтраційний етап перед основним провадженням[181]. Тому одразу необхідно вказати, які джерела формують первинну інформацію про кримінальні правопорушення досліджуваної категорії.

Згідно з частиною 1 статті 214 КПК України досудове розслідування розпочинається у конкретний момент: слідчий, дізнавач, прокурор невідкладно, але не пізніше 24 годин після подання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення ним з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, зобов'язаний внести відповідні відомості до Єдиного реєстру досудових розслідувань, розпочати розслідування та через 24 години з моменту внесення таких відомостей надати заявнику витяг з Єдиного реєстру досудових розслідувань. Слідчий, який здійснюватиме досудове розслідування, визначається керівником органу досудового розслідування, а дізнавач – керівником органу дізнання, а в разі відсутності підрозділу дізнання – керівником органу досудового розслідування[182].

Відповідно до Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення, затвердженого наказом Генерального прокурора від 30.06.2020 р. № 298, факт внесення відомостей до Єдиного реєстру досудових розслідувань прокурором, слідчим, дізнавачем ще не надає останнім права проводити слідчі (розшукові) та інші процесуальні дії, спрямовані на забезпечення дієвості кримінального провадження і досягнення мети розслідування, оскільки, вказані відомості підлягають перевірці керівником органу прокуратури, органу досудового розслідування, органу дізнання. Факт реєстрації кримінального правопорушення (провадження) настає лише з моменту підтвердження керівником органу прокуратури або органу досудового

[180] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[181] Аленін Ю. П. Початок досудового розслідування за КПК України 2012 р. *Юридичний часопис Національної академії внутрішніх справ.* 2013. № 1. С. 199–208.

[182] Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VIII URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.09.2025).

розслідування, органу дізнання таких відомостей[183].

З приводу безпосереднього внесення інформації С. В. Самойлов серед джерел первинної інформації про правопорушення та прийняття рішення про початок кримінального провадження визначив такі: «… 1) заяви чи повідомлення представника інтернет-сервісу, на якому було виявлено шахрайство – 15%; 2) заяви чи повідомлення від потерпілого – 85%. Поряд з тим, наголошено що теоретично не можна виключати й інших джерел, найбільш імовірним серед яких можна вважати безпосереднє виявлення ознак кримінального правопорушення працівниками правоохоронних органів:

– під час перевірки одержаної з оперативних джерел інформації про правопорушення, яке вчинено чи готується;

– під час проведення оперативно-розшукових заходів, спрямованих на запобігання злочинам у мережі Інтернет, у ході яких було виявлено ознаки шахрайства;

– під час досудового розслідування слідчим іншого кримінального правопорушення, якщо під час такого розслідування будуть виявлені обставини, що вказують на шахрайства, вчинені з використанням мережі Інтернет»[184].

Своєю чергою, окрема група науковців (В. В. Вапнярчук, Ю. М. Грошевий, В. Я. Тацій) стверджує, що «… зазначена діяльність відповідає критеріям самостійного провадження, оскільки є системою процесуальних дій у межах кримінальної процесуальної форми досудового провадження, які зумовлюють виникнення певної сукупності процесуальних відносин та спрямовані на виконання єдиного завдання, і цілком правомірним є розуміння й дослідження цієї діяльності саме як самостійного провадження»[185].

Водночас О. А. Самойленко вказує на те, що у зв’язку з цим важливим є врахування таких міркувань: «… завданням початку досудового розслідування є своєчасна реакція з боку вповноважених державних органів на інформацію про кримінальне правопорушення (полягає в невідкладній реєстрації в ЄРДР і початку кримінального провадження) поєднана з аналізом отриманих відомостей, які можуть не утримувати ознак саме кримінального правопорушення або взагалі бути помилковими чи неправдивими; на цій стадії не лише приймаються заяви, повідомлення про вчинене кримінальне правопорушення та здійснюється їх перевірка, але й приймається обґрунтоване рішення щодо проведення досудового розслідування за іншими джерелами інформації; ця стадія не залежить від інших етапів кримінального провадження, зміст її зумовлений колом вирішуваних питань». Авторка робить висновок,

---

[183] Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення : затв. наказом Офісу Генерального прокурора від 30.06.2020 р. № 298. URL: https://zakon.rada.gov.ua/laws/show/v0298905-20#Text (дата звернення: 25.09.2025).

[184] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … канд. юрид. наук : 12.00.09 / Дон. юрид. ін-т. Донецьк, 2014. 18 с.

[185] Кримінальний процес : підручник / за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. 648 с.

що сутність стадії початку досудового розслідування виявляється в процесуальній діяльності слідчого, прокурора з розгляду первинної інформації про кримінальне правопорушення (її прийняття, реєстрація, перевірка та прийняття рішення)[186].

Також доречною є думка С. В. Самойлова з приводу того, що мають місце характерні ознаки, які виокремлено на підставі вивченого емпіричного матеріалу. Зокрема, серед них визначено такі, наявність яких у первинному матеріалі орієнтує слідчого на викриття ознак шахрайства, вчиненого саме з використанням мережі «Інтернет», зокрема:

– факт взаємодії потерпілого та зловмисника через інтернет;

– факт передачі коштів, майна чи права на майно;

– факт невиконання іншою стороною зобов'язань у межах домовленості[187].

А вже С. В. Чучко на основі аналізу матеріалів судово-слідчої практики встановив, що «… початкові відомості, які були підставою для внесення відомостей в ЄРДР за фактом учинення шахрайства при купівлі-продажу товарів через мережу Інтернет, надходили до правоохоронних органів з таких джерел: а) заяви, листи та повідомлення, що надійшли від громадян, які отримали інформацію про вчинене правопорушення – 91 %; в) заяви, листи й повідомлення від громадян, які стали свідками злочинної події – 3 %; г) повідомлення працівників установ й організацій – 3 %; д) матеріали слідства, виділені з інших кримінальних проваджень – 2 %; е) матеріали, отримані під час проведення НСРД та розшукових заходів – 1 %»[188].

Інша група науковців (В. С. Кузьмічов, Ю. М. Чорноус) вказують на те, що кримінальне провадження розпочинають у результаті виявлення безпосередньо слідчим іншого кримінального правопорушення під час здійснення досудового розслідування в уже дорученому для здійснення розслідування кримінальному провадженні («ініціативна форма»). Автори зазначають, що традиційно діяльність із розслідування злочинів є специфічним видом соціальної практики, що полягає в пізнанні подій протиправного характеру за допомогою передбачених законом засобів і прийомів, з-поміж яких і примусова реалізація їх у разі чинення протидії[189]. І дійсно, дані форми можуть мати місце в досліджуваній категорії проваджень.

Відповідно до Положення про Єдиний реєстр досудових розслідувань,

---

[186] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

[187] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … канд. юрид. наук : 12.00.09 / Дон. юрид. ін-т. Донецьк, 2014. 18 с.

[188] Чучко С. В. Оцінка первісної інформації та коло обставин, що підлягають встановленню під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет : окремі аспекти. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2020. № 3. С. 304–310.

[189] Кузьмічов В. С., Чорноус Ю. М. Розслідування злочинів: міжнародне і національне законодавство. Теорія і практика *:* навч. посіб. Київ : КНТ, 2008. 248 с.

порядок його формування та ведення облік кримінальних правопорушень за заявами, повідомленнями, які надійшли до органів прокуратури, досудового розслідування чи дізнання, або щодо виявлених прокурором, слідчим, дізнавачем з інших джерел обставин, що свідчать про вчинення кримінального правопорушення, здійснюється Реєстратором за дорученням керівника органу прокуратури або органу досудового розслідування, органу дізнання шляхом внесення до Реєстру відомостей, визначених частиною п'ятою статті 214 КПК України[190].

Отже, на основі аналізу й узагальнення матеріалів судово-слідчої практики (додаток Б) нами було зроблено висновок, що первинна інформація, яка була підставою для внесення даних до ЄРДР за фактом учинення кримінальних правопорушень у кіберпросторі, надходила до правоохоронних органів з таких джерел:

1) усна заява (повідомлення) про кримінальне правопорушення – 53 %;

2) матеріали правоохоронних, судових та контролюючих державних органів про виявлення фактів вчинення чи підготовки до вчинення кримінальних правопорушень – 31 %;

3) повідомлення підприємств, установ, організацій і посадових осіб – 9 %;

4) повідомлення в медіа – 4 %;

5) самостійне виявлення слідчим або дізнавачем (уповноваженою особою іншого підрозділу) кримінального правопорушення, у тому числі під час досудового розслідування – 3 %.

Як слушно вказує А. Е. Жилін, КПК України «… надає уповноваженим особам 24 години на перевірку будь-якого повідомлення про вчинене протиправне діяння. Тобто слідчий, дізнавач чи прокурор повинні самостійно наявними силами та засобами перевірити відповідність заяви як дійсності, так і порушенню будь-яких прав і свобод особи. З огляду на це, слід визначити, які можливості криміналістичного аналізу первісної інформації про вчинене шахрайство у сфері використання банківських електронних платежів є в уповноважених осіб, а також які подальші їх дії мають бути для правильного визначення основних напрямів розслідування»[191].

---

[190] Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення : затв. наказом Офісу Генерального прокурора від 30.06.2020 р. № 298. URL: https://zakon.rada.gov.ua/laws/show/v0298905-20#Text (дата звернення: 25.09.2025).

[191] Жилін А. Е. Особливості криміналістичного аналізу первісної інформації та визначення основних напрямів розслідування шахрайства у сфері використання банківських електронних платежів. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі :* матеріали Міжнарод. наук.-практ. конф. (м. Київ, 14–15 черв. 2022 р.). Київ : НДІ публ. права, 2022. С. 21–23.

Існують різні погляди на зміст обставин, що підлягають встановленню. Підтримуємо позицію В. В. Сисолятіна щодо того, що однією зі складових методики розслідування окремих кримінальних правопорушень є обставини, які підлягають встановленню. Автор констатує, що цей елемент у своїх роботах опрацьовують майже всі науковці, предметом дослідження яких є вказана тематика. Також дослідник зауважує, що наведена наукова категорія акумулює в собі загальні відомості стосовно самого протиправного діяння, а також характеристик його учасників, що служить для побудови конкретних слідчих ситуацій в кримінальних провадженнях досліджуваної категорії[192].

Крім того, вони передбачені статтею 91 КПК України, як-от:

– подія кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення);

– винуватість обвинуваченого у вчиненні кримінального правопорушення, форма вини, мотив і мета вчинення кримінального правопорушення;

– вид і розмір шкоди, завданої кримінальним правопорушенням, а також розмір процесуальних витрат;

– обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, характеризують особу обвинуваченого, обтяжують чи пом'якшують покарання, які виключають кримінальну відповідальність або є підставою закриття кримінального провадження;

– обставини, що є підставою для звільнення від кримінальної відповідальності або покарання;

– обставини, які підтверджують, що гроші, цінності та інше майно, які підлягають спеціальній конфіскації, одержані внаслідок вчинення кримінального правопорушення та/або є доходами від такого майна, або призначалися (використовувалися) для схиляння особи до вчинення кримінального правопорушення, фінансування та/або матеріального забезпечення кримінального правопорушення чи винагороди за його вчинення, або є предметом кримінального правопорушення, у тому числі пов'язаного з їх незаконним обігом, або підшукані, виготовлені, пристосовані або використані як засоби чи знаряддя вчинення кримінального правопорушення;

– обставини, що є підставою для застосування до юридичних осіб заходів кримінально-правового характеру[193].

Обставини, викладені у цій статті, являються узагальнювальними для всіх видів кримінальних проваджень, і в теорії доказів називаються загальним предметом доказування на всіх етапах кримінального провадження. Заразом уособлення предмета доказування в кожному окремому провадженні здійсню-

[192] 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. Вип. 4. С. 127–132.

[193] Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL: http://zakon4.rada.gov.ua/laws/show/4651-17 (дата звернення: 20.09.2025).

ється зважаючи на вимоги диспозиції статті КК України, за якою кваліфікується дане правопорушення, що підлягає встановленню[194].

Відповідно до Закону України «Про електронну комерцію» електронний договір вважається укладеним з моменту одержання особою, яка направила пропозицію укласти такий договір, відповіді про прийняття цієї пропозиції в порядку, визначеному частиною шостою цієї статті. При цьому, місцем укладення електронного договору є місцезнаходження юридичної особи або місце фактичного проживання фізичної особи, яка є продавцем (виконавцем, постачальником) товарів, робіт, послуг. Момент виконання продавцем обов'язку передати покупцеві товар визначається згідно з положеннями Цивільного кодексу України про купівлю-продаж, якщо інше не встановлено цим Законом[195].

Розслідування кримінальних правопорушень у кіберпросторі залишається досить складним завданням для більшості співробітників органів досудового розслідування, що зумовлено специфікою такого роду протиправних діянь.

У розрізі зазначеного вважаємо доцільним навести твердження Ю. М. Чорноус, яка констатувала, що «… для кримінального провадження діяльність щодо встановлення обставин конкретного характеру виражається в: фіксації ходу і результатів проведення процесуальних, слідчих (розшукових) дій, негласних слідчих (розшукових) дій; виявленні, фіксації, збиранні, дослідженні слідів злочину; веденні систем кримінальної реєстрації та криміналістичних обліків; залученні спеціальних знань до проведення процесуальних, слідчих (розшукових) дій, негласних слідчих (розшукових) дій; залученні експертів та проведенні судових експертиз тощо»[196].

При розслідуванні кримінальних правопорушень у кіберпросторі можна виділити такі обставини, що підлягають встановленню:

– використання розрахункових рахунків, що належать одному зі співучасників розкрадання грошових коштів;

– використання фіктивних розрахункових рахунків, що належать випадковим учасникам злочинного процесу;

– використання сервісів обміну грошових коштів;

---

[194] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[195] Про електронну комерцію : Закон України від 03.09.2015 р. № 675-VIII. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text (дата звернення: 20.09.2025).

[196] Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів: наукові засади та напрями реалізації. *Сучасні тенденції розвитку криміналістики та кримінального процесу* : тези доп. Міжнарод. наук.-практ. конф. до 100-річчя від дня народження проф. М. В. Салтевського (08 листоп. 2017 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2017. С. 220–222.

– використання фіктивної юридичної особи, яка уклала договір з банком про обслуговування розрахунків з використанням електронних засобів платежу;

– переведення в готівку грошових коштів, що містяться на рахунку потерпілого, дані авторизації якого виявилися в руках зловмисників;

– оплата товарів через інтернет з використанням персональних даних потерпілого.

Своєю чергою, С. В. Самойлов вказує, що вивчення слідчої практики дозволило визначити особливості протиправного діяння, суть яких полягає в тому, що:

– фізичне місцезнаходження шахрая, як і засобів учинення злочину, переважно не збігаються з місцем перебування потерпілого та настанням негативних наслідків злочину (місцем завдання матеріальної шкоди), а за певних випадків такі обставини можуть мати навіть транснаціональний (трансконтинентальний) характер;

– встановлено відсутність залежності пори року та інших сезонних проявів, які б прямо впливали на злочинну активність шахраїв[197].

За даними Служби безпеки України, великі атаки, здійснені з серйозними напрацюваннями по вірусам типу BlackEnegry, які можна назвати кіберзброєю, досить складно порахувати. Можна дивитися тільки за непрямими ознаками. Цілком можна дійти висновків, що йдеться про роботу, яка коштує мільйони доларів. Ті ж типи вірусів використовуються і в інших країнах: Німеччині, США. Організація атак на Україну може йти з боку рф. Дуже багато ознак про це свідчить. Якщо говорити про внутрішню впевненість, то вона є. Потрібно провести розслідування й отримати юридично значущі факти. У нас є з рф договір про надання правової допомоги. Але, зі зрозумілих причин, він не працює. А значить, і неможливо в правовому сенсі до кінця розкрити того, хто стоїть за атакою, що йде з боку росії[198]. Іншими словами, уже на той час відбувалося протистояння України зі своїм східним «сусідом».

А вже С. В. Чучко запропонував виокремити певні групи обставин, що підлягають встановленню під час розслідування шахрайств при купівлі-продажу товарів через інтернет, а саме:

– обставини, що стосуються події шахрайства при купівлі-продажу товарів через інтернет (відомості про час, місце вчинення шахрайства, відомості про спосіб його вчинення, наприклад: розміщення фейкової інформації про продаж товару з подальшим отриманням на платіжну карту суми повної його

[197] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … канд. юрид. наук : 12.00.09 / Дон. юрид. ін-т. Донецьк, 2014. 16 с.

[198] Кібератаки на Україну коштують мільйони доларів – СБУ. URL: https://detector.media/infospace/article/122774/2017-02-02-kiberataky-na-ukrainu-koshtuyut-milyony-dolariv-sbu/ (дата звернення: 20.09.2025).

вартості; розміщення фейкової інформації про продаж товару за умов накладного платежу з подальшим отриманням частини його вартості на платіжну карту (передоплати); створення сайтів магазинів у інтернеті або їх копій, що діють за принципом фірм-одноденок; отримання покупцем товару, щодо якого передбачений накладний платіж, без його оплати тощо); відомості про знаряддя (засоби) злочину; відомості про сліди злочину; відомості про предмет злочинного посягання (його кількісні та якісні характеристики) тощо);

– обставини, що стосуються особи потерпілого та злочинця (ознаки суб'єкта злочину: фізична особа, осудність, вік, кваліфікуючі ознаки, які стосуються суб'єкта; кількість злочинців (наявність розподілу ролей серед шахраїв, функції кожного з них);

– причинові обставини: наявність причинного зв'язку між діями винних осіб та їх наслідками; виявлення причин та умов, які сприяли вчиненню злочину; заходи, яких необхідно вжити для їх усунення тощо;

– решта обставин (вид і розмір шкоди, завданої кримінальним правопорушенням; кваліфікуючі ознаки щодо розміру шкоди завданої злочином; обставини, що обтяжують чи пом'якшують покарання; обставини, що виключають кримінальну відповідальність, чи є підстава для закриття кримінального провадження; обставини, що є підставою для звільнення від кримінальної відповідальності, а також обставини, що виключають факт вчинення підозрюваною особою іншого злочину тощо[199].

Зі свого боку, В. В. Сисолятін зауважував, що «… обставини, які підлягають встановленню під час розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, акумулюють у собі загальні відомості стосовно самого протиправного діяння, а також характеристик його учасників, що служить для побудови конкретних слідчих ситуацій в кримінальних провадженнях досліджуваної категорії»[200].

Наостанок зауважимо, що ключове значення мають також обставини, що сприяли вчиненню діяння. Незважаючи на те, що статтею 24 Закону України «Про захист персональних даних» передбачено, що суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від незаконної обробки, а також від незаконного доступу до них[201], в інтернеті існують різноманітні сайти-форуми, торгівельні онлайн-майданчики, де зловмисники успішно продають величезні об'єми персональних даних, здо-

[199] Чучко С. В. Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет : дис. … д-ра філос. : 081 – Право / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2021. 276 с.

[200] 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.

[201] Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. URL : http://zakon5.rada.gov.ua/laws/show/2297-17 (дата звернення:20.09.2025).

буті злочинним шляхом, імена, адреси реєстрації, контактні дані осіб, що можуть бути використані для верифікації фіктивного клієнта банку, а також дані доступу до банківської інформації, кредитних і дебетових карток, дані доступу до онлайн-банкінгу, надають послуги створення підробних фото-ID тощо[202].

З огляду на дисертаційне дослідження В. В. Сисолятіна, яке було присвячено, як ми вказували у вступі, проблематиці розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу[203], надамо перелік обставин, що підлягають встановленню під час розслідування кримінальних правопорушень у кіберпросторі, а саме:

1) обставини, що розкривають окремі обставини вчинення кримінальних правопорушень у кіберпросторі (інформація про час, місце та способи їх вчинення, дані про використання шкідливих програм чи вірусів, які занесені до комп'ютерного забезпечення потерпілого, дублювання за їх допомогою акаунту на приватний гаджет (смартфон, планшет, ноутбук, комп'ютер); використання реквізитів картки, які вилучені з серверів онлайн-магазинів, платіжних чи розрахункових систем, з персональних гаджетів потерпілих; дані про електронні сліди протиправного діяння; встановлення місця отримання неправомірного доступу та входу до мережі (зсередини чи ззовні), а також способи здійснення неправомірного підключення (зміну програм захисту відомостей, роботу з електронними відомостями та командами, застосовування шпигунських програм); засоби, що використовуються при вчиненні кіберзлочину (технічні – ЕОМ, планшети, ноутбуки, смартфони, модеми, маршрутизатори; програмні – шкідливі віруси, шпигунські програми, VPN);

2) обставини, які характеризують кіберзлочинця (кількість правопорушників та можливий розподіл серед них функціональних обов'язків, визначення задач кожного кіберзлочинця окремо);

3) характеристика потерпілої сторони (фізична чи юридична особа; відповідні віктимогенні групи, їх характеристики; можливі функції з державної оборони);

4) причинно-наслідкові взаємозв'язки (з'ясування наявності певного взаємозв'язку між діями кіберзлочинців та їх результатами);

5) обставини, що обтяжують або пом'якшують покарання, чи взагалі виключають кримінальну відповідальність (наявні умови та підстави для закриття кримінального провадження);

6) вид і розмір шкоди, завданої скоєнням кримінальних правопорушень у кіберпросторі;

---

[202] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[203] Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2024. 230 с.

7) чинники, які сприяли вчиненню кримінальних правопорушень у кіберпросторі.

2.2. Алгоритми дій працівників правоохоронних органів під час розслідування кримінальних правопорушень у кіберпросторі відповідно до типових слідчих ситуацій

Типові слідчі ситуації є однією з тих криміналістичних категорій, які постійно розробляються вченими-криміналістами у зв'язку з їх практичним значенням, оскільки завдяки їм найбільш повно та ефективно здійснюється розслідування будь-яких кримінальних правопорушень.

З огляду на зазначене вважаємо доречним твердження В. В. Сисолятіна, який констатував, що «… алгоритмізація є обов'язковою складовою для будь-якого процесу, звичайно, лише в тих випадках, коли у його організатора на меті буде послідовна та цілеспрямована діяльність. Розслідування кримінальних правопорушень, пов'язаних з використанням інтернет-банкінгу, не є виключенням. В той же час, алгоритмізація повинна бути побудована відповідно до певної системи. В цьому розрізі, процес розслідування будується на типових слідчих ситуаціях. Адже в собі вказані ситуації можуть акумулювати як криміналістичні версії, так і окремі відомості про подію протиправного діяння та її учасників (потерпілих, свідків, підозрюваних)»[204].

Також зауважимо, що в ході розслідування слідчий ознайомлюється з великою кількістю речових доказів, документів. Означена уповноважена особа реалізує це з метою безпосереднього отримання інформації в результаті проведення оперативно-розшукових і слідчих (розшукових) дій. Враховуючи це, приймаються відповідні рішення про організацію та планування процесу розслідування злочинів, використання допомоги спеціалістів та інших підрозділів правоохоронних органів. Дані про обставини вчинення злочину є предметом аналізу в процесі розслідування. Сукупність зазначеної інформації, отриманої з різних джерел, становить зміст слідчої ситуації[205].

С. В. Веліканов ще на початку 2000-х зазначав, що органам розслідування доводиться діяти в різних умовах та обставинах, які складаються під впливом особливостей протиправних діянь, дефіциту часу та доказової інформації, специфіки відносин між учасниками кримінального процесу. Також автор акцентував увагу на тому, що в такому аспекті процес розслідування вбачається як система слідчих ситуацій, які змінюються протягом усього періоду

[204] 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.

[205] Єфімов М. М. Методика розслідування кримінальних правопорушень проти моральності: наукові та праксеологічні основи : монографія. Одеса : Видавничий дім «Гельветика», 2020. 392 с.

кримінального провадження. Крім того, науковець зазначав, що виділення слідчої ситуації об'єктом власного наукового дослідження зумовлюється потребою виявлення особливостей криміналістичного підходу до вивчення процесу досудового слідства як стадії кримінального судочинства. Наостанок учений-криміналіст сформулював таке визначення окресленої наукової категорії: «… це сукупність сформованих на певному етапі умов – положення, стану й обстановки – розслідування, що сприймаються, оцінюються і використовуються слідчим для вирішення тактичних задач і досягнення загальних (стратегічних) цілей досудового розслідування»[206].

А вже інша група вчених-криміналістів (А. Іщенко, Г. Щербакова) наголошували, що опрацьовування питання слідчої ситуації як наукової категорії має теоретичне та прикладне значення. Також дослідники відмітили, що теоретичне значення опрацювання вказаного питання загалом полягає в об'єктивній закономірності конкретизації змісту й поняття вказаної криміналістичної категорії. Стосовно ж її практичного значення науковці вказали, що воно полягає в тому, що визначення змісту слідчих ситуацій, їх класифікація, аналіз і оцінка дають можливість об'єктивно обґрунтувати вибір варіантів методики розслідування, які найбільшою мірою відповідали б обставинам і завданням розслідування на певному етапі[207]. Інакше кажучи, слідча ситуація має важливе не тільки теоретичне, а й практичне значення.

Але й у цьому напрямі є певні розбіжності. Так, більшість учених при класифікації слідчих ситуацій беруть за основу передусім критерій складності: прості та складні. При цьому, слідча ситуація є складною й тоді, коли реальна інформаційна невизначеність вимагає побудови кількох її імовірнісних моделей. Якщо ж інформації про ситуацію достатньо для побудови її однозначної моделі, то така ситуація буде простою. В основі поділу лежить характеристика одного з компонентів інформаційного характеру – поінформованості слідчого[208].

Зі свого боку, Р. Л. Степанюк стверджував, що типова слідча ситуація – «… це сформульована на підставі аналізу практики розслідування певної категорії злочинів абстрагована штучна модель, яка відображає стан наявної у слідчого інформації про обставини злочину й обставини, що склалися на відповідному етапі розслідування»[209].

---

[206] Веліканов С. В. Класифікація слідчих ситуацій в криміналістичній методиці : автореф дис. ... канд. юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2002. 16 с.

[207] Іщенко А., Щербаков Г. Проблема слідчих ситуацій як складова навчального курсу криміналістики. *Вісник Одеського інституту внутрішніх справ*. 2003. № 2. С. 57–63.

[208] Шевчук В. М. Слідча ситуація: повнота, структура, види та її значення для оптимізації розслідування злочинів. *Юридичний науковий електронний журнал*. 2014. № 1. С. 142–150.

[209] Степанюк Р. Л. Ситуаційний підхід у формуванні методик розслідування злочинів, вчинених у бюджетній сфері України. *Право і безпека*. 2013. № 3 (50). С. 110–115.

Наступний підхід передбачає класифікацію слідчих ситуацій на конфліктні та безконфліктні, що ґрунтується на характеристиці одного з психологічних компонентів – зайнятій позиції учасників та рівні протидії розслідуванню[210].

Динамічність слідчих ситуацій, які змінюють свій зміст, структуру і форму в результаті впливу різних зовнішніх і внутрішніх чинників, дає підставу розрізняти серед них вихідні (з точки зору процесу розслідування), проміжні та кінцеві.

Слушною з цього приводу є думка В. К. Весельського, який акцентує увагу на тому, що в основі всіх загальноприйнятих у криміналістиці класифікацій лежить якась одна ознака. Підставою ж для загальної класифікації слідчих ситуацій є її якісна, стосовно можливості досягнення цілей розслідування, характеристика. Тому він поділяє всі слідчі ситуації на сприятливі та несприятливі для розслідування і вважає, що досягнення слідчим будь-якої з намічених цілей має починатися з оцінки наявної слідчої ситуації й, за необхідності, – з ужиття заходів щодо зміни її в сприятливу сторону[211].

С. В. Веліканов, характеризуючи слідчу ситуацію через опрацювання її природи та структури, зробив такі висновки:

«– криміналістична сутність слідчих ситуацій виявляється у специфіці обстановки та стану розслідування в процесі їх формування, розвитку й вирішення;

– соціолого-правовий аспект полягає в тому, що слідча ситуація розвивається і складається в рамках, установлених чинним законодавством (матеріальним і процесуальним) при відповідному рівні сформованих відносин;

– інформаційно-психологічний аспект полягає в тому, що всяка ситуація представляється у вигляді сприйнятої слідчим сукупності даних, що характеризують стан і обстановку розслідування, використовуваних для оцінки і моделювання як слідчих ситуацій, так і засобів їх вирішення відповідними методами»[212].

Як бачимо, дослідник провів паралелі між криміналістичною, соціально-правовою та інформаційно-психологічною складовою досліджуваної наукової категорії.

Також, залежно від наявності (відсутності) в розпорядженні правоохоронних органів інформації стосовно події злочину та особи, яка його вчинила, пропонує типізувати слідчі ситуації В. М. Шевчук, який також вважає, робити

---

[210] Журавель В. А. Ситуаційний підхід до формування окремих криміналістичних методик розслідування злочинів. *Теорія та практика судової експертизи і криміналістики*. 2008. Вип. 8. С. 151–162.

[211] Весельський В. К. Слідча ситуація як категорія криміналістичної тактики. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2011. № 25. С. 193–199.

[212] Веліканов С. В. Класифікація слідчих ситуацій в криміналістичній методиці : дис. ... канд. юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2002. 218 с.

це доцільно за одним із основних компонентів. Автор вказує, що зазвичай така умова обирається наявністю інформації про подію злочину та її учасників. Також учений наголошує на тому, що типовими є ті ситуації, з якими стикається слідчий на початку чи наступному етапі розслідування злочину залежно від повноти вихідних даних[213].

Тобто, принцип систематизації типових слідчих ситуацій надалі дозволить виокремити більшу кількість слідчих версій для розслідування того чи іншого протиправного діяння та пришвидшить розумні строки проведення слідчих (розшукових) дій, що безпосередньо й буде впливати на більш швидкісне та якісне реагування оперативних співробітників Національної поліції України на факт вчиненого кримінального правопорушення та на відсоток їх розкриття[214].

Відповідно до характеру та обсягу отриманої інформації на початковому етапі розслідування Б. Є. Лук'янчиков, Є. Д. Лук'янчиков та С. Ю. Петряєв виокремили такі ситуації:

– є відомості про факти незаконного втручання в роботу ЕОМ та їхню систему (перекручування чи знищення комп'ютерної інформації та її носіїв), при цьому відомості про спосіб доступу до неї та осіб, що вчинили це діяння, відсутні;

– встановлені факти злочинного заволодіння комп'ютерною інформацією, при цьому відомості про спосіб доступу до неї та осіб, що вчинили це діяння, відсутні;

– встановлені порушення правил експлуатації ЕОМ та їхніх систем (крадіжка, перекручування, копіювання, істотне порушення роботи ЕОМ), при цьому відомості про осіб, що вчинили це діяння, відсутні;

– встановлені факти злочинного впливу на комп'ютерну інформацію (заволодіння, перекручення або руйнування), при цьому є відомості про спосіб доступу й осіб, що вчинили це діяння[215].

Своєю чергою, О. І. Мотлях зауважив, що слідча ситуація – «… це пізнана суб'єктом доказування об'єктивна реальність (матеріальні та ідеальні джерела), яка існує на даний момент розслідування злочину. Показано, що формування слідчої ситуації у злочинах з використанням інформаційних комп'ютерних технологій відбувається під впливом об'єктивних та суб'єкти-

[213] Шевчук В. М. Слідча ситуація : повнота, структура, види та її значення для оптимізації розслідування злочинів. *Юридичний науковий електронний журнал*. № 1. 2014. С. 142–150.

[214] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[215] Лук'янчиков Б. Є., Лук'янчиков Є. Д., Петряєв С. Ю. Криміналістика : навч. посіб. для студ. юрид. спец. вищ. навч. закл. : у 2 ч. Ч. ІІ : Криміналістична тактика. Методика розслідування. Київ : НТУУ «Київський політехнічний інститут ім. Ігоря Сікорського», 2017. 505 с.

вних факторів. З метою більш доступного сприйняття слідчим та іншими учасниками процесу нетрадиційних видів злочину, автором сформульовано та запропоновано кілька типових слідчих ситуацій, що можуть скластися при розслідуванні справ, пов'язаних з комп'ютерними технологіями, залежно від впливу на комп'ютерну інформацію»[216].

О. Ю. Довженко наголошував, що «… типова слідча ситуація на початковому етапі розслідування кіберзлочинів характеризується, зазвичай, як виявлення ознак злочину, що відбувається одразу після його скоєння або через певний час. Показується, що з урахуванням особливостей кіберзлочину здійснення більшості невідкладних слідчих дій, що передбачені процесуальним законом для звичайних злочинів, уявляється неможливим, через фізичну відсутність злочинця в місці настання злочинного результату та здійснення злочинного впливу на відстані»[217].

Проблема поширення кримінальних правопорушень у кіберпросторі виходить з недостатньої урегульованості нормативно-правових документів з приводу вимог до захищеності систем дистанційного банківського обслуговування клієнтів.

У розрізі зазначеного підтримуємо думку О. І. Коваленка, який зауважив, що «… багато вчених сходяться на думці, що законодавством України чітко не визначено поняття ключових термінів «кіберпростір», «кібербезпека», «кіберзахист», «кібератака», «кібервійна», «кібертероризм», «кіберзброя», а лише узагальнене поняття злочинів й правопорушень, які вчиняються з використанням комп'ютерних систем та мереж»[218].

Кіберзлочинці відчувають себе вільно не тільки через низький рівень фінансової грамотності українців, а й вельми лояльне кримінальне законодавство. В Україні шахрай при першій судимості несе відповідальність у вигляді лише штрафу. Водночас навіть ліберальний ЄС рекомендує за кібершахрайство призначати перше покарання у вигляді позбавлення волі не менш, ніж на один рік. В Іспанії за це можна отримати 12 років, у Польщі – до 25 років, у США – три-чотири довічні терміни. В Україні у 2016 році потрапили до в'язниці лише десять шахраїв[219].

З приводу безпосереднього поняття слідчої ситуації Р. Л. Степанюк вказував, що зазначена категорія може бути визначена як сформульована на підставі аналізу практики розслідування певної категорії злочинів абстрагована

---

[216] Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. … канд. юрид. наук : 12.00.09 / Акад. пр. і соц. відносин Федерації профспілок України. Київ, 2005. 21 с.

[217] Довженко О. Ю. Основи методики розслідування кіберзлочинів : дис. … канд. юрид. наук : 12.00.09 / Харків. нац. ун-т внутр. справ. Харків, 2020. 229 с.

[218] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[219] Некрасов В. Атака по телефону: Україну накрила хвиля кібершахрайства. URL: https://www.epravda.com.ua/rus/publications/2017/01/30/619178/(дата звернення: 05.09.2025).

штучна модель, яка відображає стан наявної у слідчого інформації про обставини злочину й обставини, що склалися на відповідному етапі розслідування[220].

А В. К. Весельський зазначав, що слідча ситуація належить до кола понять криміналістичної тактики і вже в цій якості, як і інші тактико-криміналістичні поняття, реалізується в криміналістичній методиці. Автор сформував перелік об'єктивних та суб'єктивних чинників, які формують вказані ситуації.

Зокрема, до об'єктивних чинників вчений відніс: «…наявність і характер доказової та орієнтуючої інформації, яка є в розпорядження слідчого; наявність і стійкість існування ще не використаних джерел доказової інформації та надійних каналів надходження орієнтуючої інформації; інтенсивність процесів зникнення доказів і сила чинників, які впливають на ці процеси; наявність у даний момент у розпорядженні слідчого необхідних сил, засобів, часу і можливість їх оптимально використання; існуюча в даний момент кримінально-правова оцінка розслідуваної події».

Суб'єктивними чинниками, на думку вченого, є: «…психологічний стан осіб, які фігурують у розслідуваній справі; психологічний стан слідчого, рівень його знань і вмінь, практичний досвід, здатність приймати і реалізовувати рішення в екстремальних умовах; протидія встановленню істини з боку злочинця та його зв'язків, а іноді потерпілого та свідків; сприятливий (безконфліктний) перебіг розслідування; зусилля слідчого, спрямовані на зміну слідчої ситуації в бажану сторону; наслідки помилкових дій слідчого, оперативного працівника, експерта; наслідки розголошення даних досудового слідства; непередбачені дії потерпілого або осіб, не причетних до розслідування»[221]. Зі свого боку, окрема група науковців (В. В. Зарубей, О. В. Ілляшенко) акцентувала увагу на тому, що підставами для висунення типових версій можуть слугувати дані щодо оперативної обстановки[222]. Ми повністю підтримуємо зазначені позиції та вважаємо за необхідне сформулювати типові слідчі ситуації, які можуть виникнути при розслідуванні кримінальних правопорушень у кіберпросторі, з огляду на вказане.

Наостанок наведемо визначення С. С. Чернявського, який типову слідчу ситуацію формулює як інформаційну модель з найбільш значущими властивостями та ознаками процесу розслідування в кримінальних провадженнях щодо

[220] Степанюк Р. Л. Ситуаційний підхід у формуванні методик розслідування злочинів, вчинених у бюджетній сфері України. *Право і безпека*. 2013. № 3 (50). С. 110–115.

[221] Весельський В. К. Слідча ситуація як категорія криміналістичної тактики. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2011. № 25. С. 193–199.

[222] Зарубей В. В., Ілляшенко О. В. Особливості висунення та планування версій при розслідуванні квартирних крадіжок, вчинених іноземцями. *Сучасний стан криміналістичного забезпечення досудового розслідування* : зб. матеріалів конф. (м. Київ, 20 квіт. 2017 р.). Київ : ННІ № 2 НАВС, 2017. С. 139–142.

злочинів певної категорії[223].

Підсумовуючи, сформулюємо авторське визначення типової слідчої ситуації – це сформована на підставі аналізу практики досудового розслідування певної категорії кримінальних правопорушень інформаційна модель з найбільш значущими властивостями та ознаками визначеної категорії протиправних діянь.

З приводу класифікації типових слідчих ситуацій також наведемо думки деяких науковців. Зокрема, С. В. Самойлов виокремлював серед них такі:

– виявлено ознаки шахрайства, що вчиняється з використанням інтернету. Особу злочинця або встановлено, або достатньо даних для її встановлення;

– виявлено ознаки шахрайства, що вчиняється з використанням інтернету. Особу злочинця не встановлено, однак є певні відомості, що можуть вказувати на неї;

– виявлено ознаки шахрайства, що вчиняється з використанням інтернету. Особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї[224].

Зі свого боку, Л. В. Борисова за результатами аналізу типових (найпоширеніших) обставин вчинення протиправних діянь досліджуваної категорії виокремлювала такі ситуації на початковому та наступному етапах розслідування:

– встановлено час несанкціонованого доступу до комп'ютерної інформації, однак немає відомостей про спосіб доступу й особу (осіб), яка вчинила злочинні діяння;

– встановлені час і місце несанкціонованого доступу до комп'ютерної інформації, проте особи, які володіють необхідними професійними знаннями, заперечують свою причетність до злочину;

– встановлено час несанкціонованого доступу до комп'ютерної інформації, відома особа (особи), яка зацікавлена в цій інформації; бракує відомостей про спосіб доступу й особу (осіб), яка вчинила злочинні діяння;

– встановлено час несанкціонованого доступу до комп'ютерної інформації; є сліди, що вказують на конкретного підозрюваного, але він заперечує свою причетність до вчиненого злочину;

– визначено місце злочинного заволодіння комп'ютерною інформацією, для здійснення якого використовували механічний вплив; немає відомостей

[223] Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : дис. … д-ра юрид. наук : 12.00.09 / Нац. акад. внутр. справ. Київ, 2010. 610 с.

[224] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … канд. юрид. наук : 12.00.09. Донецький юридичний інститут. Донецьк, 2014. 18 с.

про особу (осіб), яка вчинила це діяння[225].

Зі свого боку, Т. В. Коршикова зробила висновок, що існують дві типові слідчі ситуації. На думку авторки, перша з них має такий вигляд – встановлено факт шахрайства з використанням ЕОТ, є первинна інформація про особу (групу осіб), які можуть бути причетні до вчинення цього кримінального правопорушення або особу злочинця встановлено чи є достатньо даних для її встановлення. Другу типову слідчу ситуацію авторка формулює так – встановлено факт шахрайства з використанням ЕОТ, особу злочинця не встановлено та відсутні будь-які дані, що можуть вказувати на неї[226].

У розрізі зазначеного вище слід навести позицію Д. В. Пашнєва та М. Г. Щербаковського, які з приводу кримінальних проваджень, розпочатих за статтями 361–363[1] КК України, зауважили, що їх можна розпочати за зверненням (заявою) власника комп'ютерної інформації (юридичної або фізичної особи) або в результаті виявлення ознак протиправного діяння правоохоронним органом. Стосовно характеру отриманої інформації про ознаки протиправного діяння вчені-криміналісти виокремлюють такі типові слідчі ситуації початкового етапу розслідування:

– ситуація 1. Кримінальне провадження відкрито за зверненням (матеріалами) заявника, у якому встановлено ознаки злочину, вчиненого невідомою особою;

– ситуація 2. Кримінальне провадження відкрито за зверненням (матеріалами) заявника, у якому зафіксовано ознаки злочину, вчиненого встановленою особою;

– ситуація 3. Кримінальне провадження відкрито в результаті виявлення ознак злочину правоохоронним органом у процесі розслідування іншого злочину[227].

Цікавою також є позиція О. Л. Мусієнка, який наводить таку загальну класифікацію слідчих ситуацій, пов'язаних з окремими етапами розслідування шахрайства, прийняттям процесуальних і тактичних рішень, а саме:

– ситуації, що виникають у ході перевірки повідомлень і заяв про злочини;

– ситуації, що виникають при вирішенні питання про початок кримінального провадження;

– ситуації, що виникають під час висування та перевірки слідчих версій і планування розслідування;

---

[225] Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09 / Київ. нац. ун-т внутр. справ. Київ, 2007. 217 с.

[226] Коршикова Т. В. Типові слідчі ситуації та програми дій слідчого на початковому етапі розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки. *Південноукраїнський правничий часопис.* 2020. Вип. 4. С. 123–131.

[227] Криміналістика : підручник : у 2 т. Т. 2 / за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. 312 с.

– ситуації підготовки та проведення слідчих дій та організаційно-технічних та інших заходів;

– ситуації забезпечення слідчим взаємодії з органом дізнання, наглядовими й контролюючими органами в розслідуванні злочинів;

– ситуації пошукової діяльності слідчого;

– ситуації зупинення кримінального провадження (по нерозкритому злочину);

– ситуації поновлення кримінального провадження;

– ситуації складання обвинувального висновку (аналіз матеріалів кримінальної справи);

– ситуації, пов'язані з передачею матеріалів до суду;

– ситуації, пов'язані з припиненням кримінального провадження[228].

Інакше кажучи, вказані ситуації виникають із загального процесу досудового розслідування.

А вже О. Ю. Довженко констатує, що «… типова слідча ситуація на початковому етапі розслідування кіберзлочинів характеризується, зазвичай, як виявлення ознак злочину, що відбувається одразу після його скоєння, або через певний час. Показується, що з урахуванням особливостей кіберзлочину, здійснення більшості невідкладних слідчих дій, що передбачені процесуальним законом для звичайних злочинів, уявляється неможливим, через фізичну відсутність злочинця в місці настання злочинного результату та здійснення злочинного впливу на відстані»[229].

Соєю чергою, за результатами аналізу типових (найпоширеніших) обставин вчинення транснаціональних комп'ютерних злочинів Л. В. Борисова визначила ситуації одного з видів комп'ютерного злочину на початковому та наступному етапах розслідування, а саме:

– встановлено час несанкціонованого доступу до комп'ютерної інформації, однак немає відомостей про спосіб доступу й особу (осіб), яка вчинила злочинні діяння;

– встановлені час і місце несанкціонованого доступу до комп'ютерної інформації, проте особи, які володіють необхідними професійними знаннями, заперечують свою причетність до злочину;

– встановлено час несанкціонованого доступу до комп'ютерної інформації, відома особа (особи), яка зацікавлена в цій інформації; бракує відомостей про спосіб доступу й особу (осіб), яка вчинила злочинні діяння;

– встановлено час несанкціонованого доступу до комп'ютерної інформації; є сліди, що вказують на конкретного підозрюваного, але він заперечує свою причетність до вчиненого злочину;

– визначено місце злочинного заволодіння комп'ютерною інформацією,

---

[228] Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / за ред. проф. В. Ю. Шепітька. Харків : Право, 2009. 168 с.

[229] Довженко О. Ю. Основи методики розслідування кіберзлочинів : дис. … канд. юрид. наук : 12.00.09 / Харків. нац. ун-т внутр. справ. Харків, 2020. 229 с.

для здійснення якого використовували механічний вплив; немає відомостей про особу (осіб), яка вчинила це діяння[230].

Зі свого боку, О. А. Самойленко за результатами узагальнення матеріалів слідчо-судової практики розслідування злочинів, вчинених у кіберпросторі, сформувала наступний перелік слідчих ситуацій, як-от:

– ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як імовірного злочинця;

– ситуації, що характеризуються наявністю неперсоналізованих відомостей про користувача як імовірного злочинця;

– ситуації, що характеризуються відсутністю будь-яких відомостей про особу злочинця[231].

А вже І. О. Коваленко на початковому етапі розслідування шахрайства у сфері використання банківських електронних платежів виокремив такі ситуації:

– вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай відомий – 19 %;

– вчинено шахрайство у сфері використання банківських електронних платежів, наявна особистісна доказова інформація, шахрай невідомий – 47 %;

– вчинено шахрайство у сфері використання банківських електронних платежів, наявна матеріальна й особистісна доказова інформація, шахрай відомий, але його дії замасковані під вид законних фінансових операцій – 11 %;

– вчинено шахрайство у сфері використання банківських електронних платежів, наявна заява від потерпілого, відсутня достатня доказова інформація – 23 %[232].

Під час типізації слідчих ситуацій на початковому етапі досудового розслідування кримінальних правопорушень у кіберпросторі, вважаємо доцільним у їх зміст покласти дані відносно способу вчинення правопорушення та особи, яка його вчинила. На основі вивчення й узагальнення матеріалів слідчо-судової практики (додаток Б) можна визначити такі типові слідчі ситуації:

1) вчинено кримінальне правопорушення у кіберпросторі, наявна достатня доказова інформація, кіберзлочинець невідомий – 52 %;

[230] Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09 / Київ. нац. ун-т внутр. справ. Київ, 2007. 217 с.

[231] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

[232] Коваленко І. О. Типові слідчі ситуації під час розслідування шахрайства у сфері банківських електронних платежів. *Науковий журнал «Visegrad Journal on Human Rights» («Пан'європейський університет» Словацької Республіки)*. 2020. № 1. С. 99–103.

2) вчинено кримінальне правопорушення у кіберпросторі, наявна заява від потерпілого, відсутня достатня доказова інформація – 24 %;

3) вчинено кримінальне правопорушення у кіберпросторі, наявна достатня доказова інформація, кіберзлочинець відомий – 18 %;

4) вчинено кримінальне правопорушення у кіберпросторі, наявна матеріальна й особистісна доказова інформація, кіберзлочинець відомий, але його дії замасковані під вид законних фінансових операцій – 6 %.

З приводу алгоритмів дій, то у першій ситуації, коли був виявлений факт вчинення кримінального правопорушення у кіберпросторі, наявна достатня доказова інформація, а кіберзлочинець відомий, повинні бути здійснені наступні заходи. В зазначеній ситуації напрямками розслідування будуть виступати такі як:

– виявлення максимальної кількості доказової інформації, яка характеризує кіберзлочинця та потерпілого;

– виявлення та закріплення доказів скоєного кримінального правопорушення;

– встановлення виду та розміру заподіяної матеріальної шкоди;

– виявлення причин і умов, що сприяють вчиненню протиправного діяння.

Приклад. *Зокрема, гр. Й. у період з 11 травня 2024 року по 16 серпня 2024 року, переслідуючи мету перешкоджання законній діяльності військових формувань щодо забезпечення комплектування особовим складом Збройних сил України та інших військових формувань в особливий період, будучи «учасником» тематичної групи в месенджері «Вайбер» (кількість підписантів якої становить 4183 особи), де забезпечував збір і публікацію разом з іншими учасниками повідомлень про розташування уповноважених представників районних (міських) територіальних центрів комплектування та соціальної підтримки, утворених у районах та містах Волинської області, з відомостями про місце і час проведення відповідних заходів указаними військовими формуваннями, для своєчасного інформування громадян України, які мають намір ухилитися від виконання своїх обов'язків із захисту Вітчизни, незалежності та територіальної цілісності України під час мобілізації в особливий період. Так, гр. Й., використовуючи особистий мобільний телефон, поширював інформацію про місцеперебування представників військових формувань та проведення останніми мобілізаційних заходів.*

Після затримання гр. Й. повністю визнав власну вину та співпрацював з органами досудового розслідування[233].

У другій ситуації, коли був виявлений факт вчинення кримінального правопорушення у кіберпросторі, наявна достатня доказова інформація, але кіберзлочинець невідомий, необхідно провести такі заходи. Зокрема, за відсутності інформації про особу кіберзлочинця основні напрями розслідування полягають у:

– виявленні максимальної кількості відомостей, що характеризують правопорушника (кіберзлочинця);

– визначенні кола його знайомих, вивченні поведінки та способу життя.

Також обов'язкове документування усіх наявних обставин протиправного діяння шляхом проведення слідчих (розшукових) дій (допити потерпілих, свідків, огляду ЕОТ), реалізація відповідних НСРД (оперативна перевірка особи на причетність до його вчинення, зняття інформації з електронних комунікаційних мереж), а також здійснення окремих розшукових заходів.

Приклад. *Громадянин Ї., достовірно знаючи, що діяльність територіальних центрів комплектування та соціальної підтримки зі здійснення мобілізаційних заходів викликала широкий резонанс у суспільстві, у тому числі й серед осіб, які мають намір ухилитися від мобілізації або не виявляють бажання бути призваними на військову службу, а в соціальних мережах та інтернет-месенджерах виник посилений попит на поширення інформації про діяльність вказаного органу, у період з 30 травня 2024 року по 20 червня 2024 року умисно перешкоджав законній діяльності Збройних Сил України під час здійснення ними призову громадян України на військову службу в особливий період. Зокрема, наприкінці травня 2024 року правопорушник пристав на пропозицію організатора щодо адміністрування каналу в інтернет-месенджері «Телеграм», у якому публічно поширювалася інформація про місця, де представники місцевого ТЦК та СП здійснюють заходи з оповіщення населення, а також інформація про маршрути пересування його представників, використовуючи умовні позначення нібито погодних умов у регіоні. На виконання вказаного вище злочинного умислу з кінця травня 2024 року гр. Ї., перебуваючи у місті Гайворон Голованівського району Кіровоградської області, із використанням належного йому мобільного телефону почав здійснювати функції адміністратора телеграм-каналу. До функцій адміністратора належало додавання та видалення учасників групи, видалення реклами, а також розмі-*

[233] Справа № 170/827/24. Архів Шацького районного суду Волинської обл., 2024 р.

щення повідомлень про розташування патрулів з прив'язкою до місцевості. При цьому, повідомлення з метою конспірації містили умовні слова ХХХ, що означало відсутність представників ТЦК та СП і поліції; ООО, що означало відповідно наявність зазначених підрозділів. Єдиною метою створення цього телеграм-каналу було поширення серед його учасників інформації про точні місця, де представники ТЦК та СП здійснюють заходи з оповіщення населення (вручають повістки), а також інформації про маршрути пересування їх представників. Завдяки комплексу слідчих (розшукових) дій, НСРД та розшукових заходів гр. Ї. було встановлено та пред'явлено підозру[234].

Третя ситуація є більш проблематичною, адже хоча й був виявлений факт вчинення кримінального правопорушення у кіберпросторі та наявна достатня доказова інформація, але кіберзлочинець маскує свої протиправні дії під вид законних фінансових операцій. Тому варто у визначеному випадку завдяки застосуванню окремих слідчих (розшукових) дій і НСРД (відповідних експертиз та оглядів ЕОТ), а також залучення спеціалістів для виявлення незаконності дій ймовірних підозрюваних, з'ясувати ознаки, спосіб вчинення протиправних дій та встановити наявність співучасників злочинної діяльності.

Вважаємо за необхідне навести твердження Г. В. Захарової, що у випадках, коли особи не переховуються від правоохоронних органів, але свою причетність до вчинення протиправних дій заперечують, «… перед слідчим постають завдання щодо необхідності виявлення, зібрання та отримання певної сукупності належних, обґрунтованих і достатніх обвинувальних доказів шляхом з'ясування у потерпілих осіб всіх обставин, за яких розпочиналися та завершилися шахрайські дії, і роль кожної причетної (підозрюваної) до цього особи, здійснення детального огляду місця події, вилучення слідів, які вказують на факт шахрайства. Встановлення можливих його свідків. Проведення впізнання осіб причетних до шахрайських дій, термінове проведення обшуків житла та іншого їх володіння, з метою вилучення електронних носіїв, та інших документів і предметів, які свідчать про вчинення шахрайських дій. Для покращення результативності розслідування доцільно проводити й негласні слідчі (розшукові) дії з метою встановлення злочинних зв'язків шахрая, його образу життя, можливого місця знаходження, речей предметів, документів, що підтверджують причетність до шахрайства та інших доказів, які цікавлять слідство»[235].

[234] Справа № 385/1402/24. Архів Гайворонського районного суду Кіровоградської обл., 2024 р.

[235]Захарова Г. В. Теоретичні засади методики розслідування шахрайства у сфері туризму, вчиненого організованою групою : дис. … канд. юрид. наук : 12.00.09 / ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом. Київ, 2021. 246 с.

Четверта ситуація є однією з найбільш складних, адже наявна заява від потерпілого про вчинення кримінального правопорушення у кіберпросторі, але відсутня достатня доказова інформація. Оскільки повідомлення про вчинення протиправного діяння надійшло від потерпілого, а кіберзлочинець невідомий, варто для початку переконатися в тому, що дійсно мала місце подія вказаного кримінального правопорушення. Адже в судово-слідчій практиці відомі випадки, коли заявник вводить в оману правоохоронні органи, повідомляючи про протиправне діяння з метою інсценування або приховування слідів іншого кримінального правопорушення. У цій ситуації необхідно опитати заявника по суті змісту повідомлення про протиправні дії, встановити всі можливі його обставини, зібрати відомості про особу, яка вчинила вказані дії.

2.3. Взаємодія працівників органів і підрозділів Національної поліції України, а також державних, громадських і приватних підприємств, установ та організацій під час розслідування кримінальних правопорушень у кіберпросторі

Ефективність будь-якої діяльності залежить від якості виконання відповідних заходів. Розслідування кримінальних правопорушень у кіберпросторі не є виключенням, адже під час цього процесу можуть бути залучені як співробітники підрозділів правоохоронних органів, так і працівники державних, приватних і громадських підприємств, установ та організацій. Своєчасна і належна взаємодія зазначених структур надає можливість максимально швидко й ефективно здійснювати кримінальне провадження[236].

Як слушно відмічає Е. В. Малютін, «… для досягнення оптимальної мети спільної діяльності як окремі індивіди, так і групи осіб повинні чітко співпрацювати. Зазначений процес за своєю суттю є взаємодією між певними суб'єктами, яка реалізується для здобутку конкретної цілі. Процес розслідування в цьому аспекті характеризується досить специфічною взаємодією залежно від конкретного кримінального правопорушення, за фактом учинення якого було внесено відомості в ЄРДР, оскільки кожне протиправне діяння відрізняється за багатьма ознаками. Зокрема, серед них варто виокремити: склад кримінального правопорушення відповідно до положень Кримінального кодексу України; особливості проведення окремих слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних заходів; залучення до кримінального провадження відповідних підрозділів правоохоронних органів тощо. Остання ознака, тісно переплітаючись з іншими, і визначає специфіку взаємодії під час розслідування кримінальних правопорушень будь-якої

[236] Єфімов М. М. Теоретичні та практичні засади методики розслідування кримінальних правопорушень проти моральності : дис. … д-ра юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2021. 514 с.

категорії»[237].

Також поділяємо позицію О. А. Самойленко, яка на основі узагальнення наукових поглядів щодо форм взаємодії слідчого із суб'єктами взаємодії конкретизувала підстави їх класифікації, а саме:

«1) нормативно-правова регламентація:

– процесуальні форми (передбачені КПК України): надання доручень співробітникам оперативних підрозділів щодо проведення СРД та НСРД (ч. 3 ст. 39, ч. 4 ст. 40, ч. 3 ст. 41 КПК України); залучення до участі в процесуальній дії співробітників оперативних підрозділів як спеціалістів чи інших учасників кримінального провадження, залучення інших спеціалістів, які мають спеціальні знання та навички (психологи, перекладачі), зокрема підчас огляду місця події, обшуку, одержання зразків для експертизи тощо (ст. ст. 40, 228, 236, 237 та інші);

– непроцесуальні (організаційно-тактичні) форми: створення слідчо-оперативних груп (тимчасових чи постійно діючих); забезпечення слідчим методичного супроводження ведення ОРС; залучення співробітників до забезпечення організаційних умов проведення охорони, конвоювання, затримання тощо; спільне планування слідчих (розшукових) та негласних слідчих (розшукових) дій, розслідування в цілому; взаємний обмін інформацією; узгоджених спільних дій та заходів кримінального провадження; обмін інформацією; залучення громадськості до участі у проведенні процесуальних дій та організаційних заходів);

2) рівень взаємодії:

– міжнародна взаємодія;

– міжвідомча взаємодія;

– внутрішньовідомча взаємодія (між різними підрозділами одного відомства);

3) стадія кримінально-процесуальної діяльності:

– взаємодія до початку кримінального провадження (в рамках ОРС та підчас попередньої перевірки інформації про злочин);

– взаємодія в ході здійснення досудового розслідування;

– взаємодія на стадії судового розгляду»[238].

Ми поділяємо позицію М. В. Куратченка, який зауважував, що під час розслідування взаємодія слідчих та оперативних підрозділів є важливою умовою того, що кримінальне провадження буде швидко й ефективно завершене. Автор акцентував увагу на тому, що завдяки злагодженій взаємодії збирається достатня доказова база для проведення подальших процесуальних дій, висуваються оптимальні слідчі версії та планується процес розслідування. Крім того,

[237] 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.

[238] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

науковець зазначив, що працівники Національної поліції України повинні реагувати на обставини, які характеризують кожний конкретний момент процесу досудового розслідування, та визначати свої функції залежно від обов'язків. Наостанок дослідник підбив підсумок, що взаємодія різних підрозділів правоохоронних органів займає важливе місце в будь-якому кримінальному провадженні[239].

Інша група авторів відмічає, що одним із ключових завдань правоохоронних органів є створення ефективної та стабільної системи підготовки фахівців, які володітимуть технологіями розслідування кримінальних правопорушень, пов'язаних з легалізацією (відмиванням) доходів, одержаних незаконним шляхом. Науковці вказують, що з метою недопущення використання зловмисниками доходів, отриманих протиправним шляхом, доцільно застосовувати заходи своєчасного накладення арешту на майно відповідно до справ. Дослідники встановили, що кількість і різноманітність способів інтернет-шахрайства зростає буквально щосекунди, оскільки зловмисники застосовують новітні технології та обладнання, дуже швидко адаптуючи їх до своїх злочинних цілей. Крім того, вчені-криміналісти зауважили, що серед усіх видів інтернет-шахрайства можна виділити основні та найпоширеніші: фішинг, сніфінг, вішинг, кардинг[240].

А вже А. Е. Жилін зауважував, що «… взаємодія є обов'язковою складовою для будь-якого соціального процесу. Під час розслідування кримінальних правопорушень вказана категорія не зменшує свого значення, а, навпаки, необхідність її застосування лише збільшується. Тим паче, у кримінальних провадженнях за фактом вчинення шахрайства у сфері використання банківських електронних платежів. Це пояснюється такими чинниками. Наприклад, завжди виникає потреба в реалізації негласних слідчих (розшукових) дій, що одразу вказує на обов'язкове залучення спеціалістів різних підрозділів правоохоронних органів. Крім того, реалізація окремих тактичних операцій також викликає необхідність у взаємодії не тільки працівників Національної поліції, але й інших відомств»[241].

Враховуючи зазначене, ми підтримуємо позицію вчених-криміналістів (Р. І. Благута, О. М. Дуфенюк, Є. В. Пряхін), які однією з важливих умов досягнення успіху в розслідуванні протиправних діянь визначають взаємодію органів, які беруть участь у цій діяльності. У протидії злочинності, як доречно наголошують вказані автори, правоохоронні органи становлять єдину систему

[239] Куратченко М. В. Розслідування сутенерства та втягнення особи в заняття проституцією : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2017. 192 с.

[240] Yefimov M., Pavlova N., Fedchenko V., Pletenets V., Kryvopusk O. Foreign Experience In Legal Regulation Of Fraud Investigation. *Revista De La Universidad Del Zulia*. 13 (38). 2022. Pp. 159–168.

[241] Жилін А. Е. Взаємодія різних підрозділів правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів: актуальні питання. *KELM.* 2023. № 3. С. 119–123.

та здійснюють свої функції відповідно до Конституції України й інших законів. Водночас правоохоронна система характеризується тим, що до її складу входять управлінські структури різної відомчої підпорядкованості. Спільність мети, завдань, принципів і характеру діяльності пов'язують їх у цілісну систему. Це стосується також органів і посадових осіб, які реалізують свої повноваження під час досудового розслідування, проблема взаємодії яких є нині актуальною, оскільки безпосередньо пов'язана з посиленням ефективності боротьби зі злочинністю[242].

Окрема група науковців, враховуючи велику суспільну небезпеку окремих категорій кримінальних правопорушень, вказала, що вони вже давно набули транснаціонального характеру, тому слід звернути особливу увагу на питання співпраці між Національною поліцією України та різними міжнародними поліцейськими організаціями. Дослідники дійшли висновку, що зміцнення взаємодії оперативних підрозділів Національної поліції України, які здійснюють боротьбу з кримінальними правопорушеннями, з міжнародними поліцейськими органами, що провадять оперативно-розшукову діяльність, є обов'язковою умовою ефективної протидії злочинності в усіх її проявах. Крім того, автори наголосили на тому, що фактичні помилки пов'язані з недостовірністю і неповнотою оперативно-розшукових даних, які перед застосуванням повинні бути ретельно перевірені та співвіднесені з уже наявною доказовою базою. Також серед розповсюджених помилок науковцями було виокремлено ті, що пов'язані з неправильною організацією та плануванням слідчих (розшукових) дій, НСРД та інших процесуальних дій, інформаційною складовою яких є отримання результатів оперативно-розшукової діяльності[243].

В. М. Малюга вказує на те, що в сучасній юридичній науці під взаємодією слідчого з оперативними підрозділами й іншими суб'єктами у кримінальному провадженні розуміється передбачене в законі, відомчих нормативних актах або ж рекомендоване криміналістичною наукою сумісне функціонування зовнішньо (юридично, організаційно, професійно) не підпорядкованих суб'єктів взаємодії з притаманною їм комунікативно-діяльнісною чи/та специфічно-професійною компетенцією, спеціалізацією, що спрямовується й узгоджується слідчим (прокурором – процесуальним керівником) за часом, місцем, формами, а також засобами та методами реалізації для вирішення конкретних завдань, обумовлених характером слідчої ситуації, з метою забезпечення швидкого, повного та неупередженого розслідування злочинів і їх запобігання[244].

---

[242] Криміналістика : підручник / за заг. ред. Є. В. Пряхіна. 3-тє вид., переробл. та допов. Львів : ЛьвДУВС, 2016. 948 с.

[243] Chaplynskyi, K., Yefimov, M., Pletenets, V., Harashchuk, D., Demchenko, I. Features Of Interaction Between Law Enforcement Agencies During The Investigation Of Criminal Offenses According To International Standards. *Cuestiones Politicas*. 2023. Volume 41. Issue 76. Pp. 469–481.

[244] Малюга В. М. Взаємодія слідчого з оперативними підрозділами та іншими суб'єктами в системі методики розслідування злочинів : дис. … канд. юрид. наук : 12.00.09 / Львів. нац. ун-т ім. І. Франка. Львів, 2016. 289 с.

Підбиваючи підсумок, зазначимо, що взаємодія правоохоронних та інших органів – це засноване на нормативно-правових актах, погоджене за метою й обстановкою функціонування незалежних один від одного в адміністративному відношенні відповідних органів, що полягає в оптимальному поєднанні властивих їм засобів і методів, які направлені на профілактику та розслідування кримінальних правопорушень під єдиним керівництвом уповноваженої особи.

З приводу форм взаємодії, то М. А. Погорецький підкреслював, що вони «… поділяються на процесуальні, які врегульовані кримінально-процесуальним законом, та організаційно-тактичні (непроцесуальні), що врегульовані відомчими нормативними актами (наказами, інструкціями, вказівками), а також нормами службової етики та вироблені практикою»[245].

Під формами взаємодії слідчого та працівників дізнання, наприклад, О. С. Саінчин розуміє організаційні прийоми та методи, способи, порядок зв'язків між ними, засновані на кримінально-процесуальному законі та відомчих нормативних актах правоохоронних органів, а також передовому досвіді слідчої практики, спрямовані на забезпечення узгодженої їх діяльності та правильне сполучення властивих кожному з цих органів методів і засобів роботи[246].

Доречними також вважаємо результати дисертаційного дослідження, проведеного О. П. Бойком, який зробив висновок, що серед процесуальних форм взаємодії варто виділити такі: «… під час проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій за дорученням слідчого; при застосуванні заходів забезпечення кримінального провадження; при оголошенні в розшук підозрюваного». Стосовно непроцесуальних форм взаємодії, то дослідник серед них зазначив:

«– взаємне інформування;

– надання інформації при отриманні необхідних відомостей;

– спільний аналіз при отриманні інформації;

– спільне планування оперативно-розшукових заходів, а також слідчих (розшукових) дій;

– консультації;

– взаємодію у разі направлення матеріалів за результатами оперативно-розшукової діяльності;

– спільний аналіз причин та умов, які сприяють вчиненню кримінального правопорушення, та обговорювання оперативно-профілактичних заходів; досудове розслідування у складі слідчо-оперативних груп;

– проведення оперативних нарад щодо проблемних питань взаємодії;

[245] Погорецький М. А., Хотенець В. М. Процесуальні і організаційно-тактичні форми взаємодії органів дізнання і досудового слідства. *Право і безпека*. 2002. № 1. С. 178–183.

[246] Саінчин О. С. Криміналістичні умови розкриття умисних вбивств. *Правова держава*. 2008. № 10. С. 267–273.

– аналіз за результатами проведення спільних дій у конкретних кримінальних провадженнях;

– надання допомоги наявними силами й засобами;

– підбиття підсумків спільної діяльності з метою усунення недоліків та підвищення ефективності здійснення взаємодії у майбутньому»[247].

Процесуальні форми є тим видом кримінально-процесуальних правовідносин, які регламентовані чинним законодавством, тобто закріплені в нормах права. Ця форма взаємодії стосується питань:

– передачі слідчому матеріалів про виявлені шляхом оперативно-розшукових заходів ознаки правопорушення для вирішення питання про початок досудового розслідування;

– проведення слідчим процесуальних дій одночасно зі здійсненням оперативним підрозділом узгоджених оперативно-розшукових заходів; в) проведення оперативно-розшукових заходів у кримінальному провадженні, у якому не встановлено особу, що вчинила правопорушення;

– виконання доручень слідчого щодо проведення негласних слідчих (розшукових) дій;

– здійснення заходів щодо встановлення особи, яка вчинила кримінальне правопорушення;

– отримання інформації та документів про операції, рахунки, внески, внутрішні й зовнішні економічні угоди фізичних та юридичних осіб[248].

У свою чергу, окрема група науковців (В. Д. Пчолкін, В. М. Єчкенко) визначають такі форми, як: «… ознайомлення слідчого з оперативними матеріалами в межах, передбачених відомчими нормативними актами; спільне обговорення й оцінювання даних, одержаних у результаті проведення оперативно-розшукових заходів, щодо їх достатності для внесення відомостей до ЄРДР; спільне планування слідчих (розшукових) дій і тактичних операцій, спрямованих на виявлення доказової інформації; спільна діяльність слідчих і оперативно-розшукових підрозділів на початковому та наступних етапах розслідування; створення слідчо-оперативної групи за конкретним кримінальним провадженням; взаємний обмін усною та письмовою інформацією оперативних працівників і слідчих з питань, що стосуються їхньої діяльності; спільні виїзди слідчого й оперативних працівників для проведення слідчих (розшукових) дій»[249].

Здійснивши аналіз окремих форм взаємодії, О. А. Самойленко вказала

---

[247] Бойко О. П. Взаємодія слідчих з підрозділами карного розшуку на досудовому провадженні : автореф. дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ : Дніпро, 2018. 20 с.

[248] Криміналістика : підручник / за заг. ред. Є. В. Пряхіна. 3-тє вид., переробл. та допов. Львів : ЛьвДУВС, 2016. 948 с.

[249] Пчолкін В. Д., Ечкенко В. М. Поняття, сутність та завдання взаємодії оперативних підрозділів ОВС. *Вісник Луганської академії внутрішніх справ ім. 10-річчя незалежності України* : спецвипуск. 2004. Вип. 3, ч. І. С. 109–121.

на наявність таких суб'єктів взаємодії уповноваженої особи під час розслідування кримінальних правопорушень, вчинених у кіберпросторі: «... 1) державні органи …: спеціально уповноважені державні органи у сфері телекомунікацій, зокрема орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації …; орган державного регулювання у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом, що здійснює також повноваження органу ліцензування, дозвільного органу, регуляторного органу й органу державного нагляду (контролю) …; Національна рада України з питань телебачення і радіомовлення; Державне підприємство «Український державний центр радіочастот»; Національний банк України; 2) громадські об'єднання/організації …; 3) суб'єкт господарювання (оператори та провайдери) у сфері зв'язку та телекомунікацій …; 4) комерційні банківські установи, суб'єкти господарювання у сфері платіжних систем …; 5) засоби масової інформації…; 6) міжнародні правоохоронні організації …; 7) інші власники (розпорядники) систем та володільці інформації»[250].

Згідно з нормами КПК України до процесуальних форм взаємодії необхідно віднести такі:

– надання допомоги слідчому, дізнавачу під час проведення негласних слідчих (розшукових) дій (статті 40, 40[1] КПК України);

– доручення та вказівки слідчого, дізнавача щодо проведення негласних слідчих (розшукових) дій (статті 40, 40[1], 246 КПК України);

– фіксація та надання слідчому (прокурору) результатів проведення негласних слідчих (розшукових) дій (стаття 252 КПК України).

Зі свого боку, провівши власне дослідження взаємодії слідчих та оперативних працівників під час розслідування шахрайства при купівлі-продажу товарів через інтернет, С. В. Чучко виокремив рівень діяльності служб і підрозділів, а також рівень розслідування окремого кримінального провадження. Науковець з приводу вказаних рівнів зробив такі висновки: «… на першому рівні – це, насамперед, підготовка і розподіл висококваліфікованих кадрів слідчих і оперативних працівників, здатних успішно виявляти, розслідувати кримінальні правопорушення у досліджуваній сфері, вчинені з використанням різних

[250] Самойленко О. А. Криміналістичний та правовий аналіз злочинної діяльності в мережі Інтернет. *Порівняльно-аналітичне право.* 2015. № 4. С. 408–411.

способів, в умовах активної, у тому числі організованої, протидії з боку правопорушників і пов'язаних з ними осіб»[251].

Аналіз опитування респондентів (додаток А) уможливив виокремлення таких процесуальних форм взаємодії під час розслідування кримінальних правопорушень у кіберпросторі, а саме:

а) виконання доручення уповноваженої особи щодо проведення СРД або НСРД – 88 %;

б) реалізація розшукових заходів для встановлення осіб, що вчинили кримінальні правопорушення у кіберпросторі, та надання уповноваженій особі відомостей про їх результати – 73 %;

в) допомога уповноваженій особі під час проведення окремих процесуальних дій – 67 %.

Слід визнати досить вдалою думку М. В. Куратченка, який типовими недоліками в організації та здійсненні взаємодії правоохоронних органів при розв'язанні конфліктних слідчих ситуацій у досліджуваних вказаним автором кримінальних провадженнях формулював такі: «… несвоєчасний, із запізненням початок взаємодії; здійснення затримання, огляду, опитування підозрюваних оперативними працівниками без участі слідчого або хоча б попереднього узгодження з ним шляхів і способів одержання й перевірки доказів причетності затримуваного до протиправного діяння; припинення взаємодії (особливо оперативного супроводу розслідування) після завершення початкового етапу досудового розслідування». Також науковець засвідчував, що поміж прийнятих у практичних підрозділах заходів з усунення вказаних вище недоліків варто виокремити такі: «… заходи щодо вдосконалювання нормативної і методичної бази взаємодії зазначених вище суб'єктів; перевірки дотримання діючих наказів і інструкцій з організації взаємодії на місцях, з виїздом керівників органів і служб у підлеглі підрозділи; заслуховування слідчо-оперативних груп, що працюють по конкретних справах і матеріалах, на оперативних нарадах у керівників управлінь і відділів; вивчення проваджень прокурором у порядку нагляду»[252].

Для прикладу, С. В. Самойлов, опрацьовуючи питання особливостей отримання відомостей від установ та організацій під час розслідування шах-

[251] Чучко С. В. До питання взаємодії слідчих та оперативних підрозділів при розслідуванні шахрайства за фактом купівлі-продажу товарів через мережу Інтернет. *Актуальні проблеми кримінально-правового, кримінально-процесуального та криміналістичного забезпечення безпеки України та світу* : матеріали Міжнарод. наук.-практ. конф. (м. Дніпро, 27 листоп. 2020 р.). Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2020. С. 202–205.

[252] Куратченко М. В. Особливості взаємодії слідчих та оперативних підрозділів при розслідуванні сутенерства та втягнення особи в заняття проституцією. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2017. № 2. С. 234–241.

райств, учинених із використанням інтернету, наголошував на потребі застосування цього способу отримання доказових даних. На думку автора, його ефективність безпосередньо залежить від того, наскільки уповноважена особа тактично правильно підготує вказаний запит, чому допомагає додержання таких умов: а) своєчасності запиту; б) законності запиту; в) визначення вичерпного переліку інформації, яку варто з'ясувати шляхом запиту. Крім того, дослідник визначив, що залежно від обставин учинення протиправного діяння окремі запити направляють до: а) адміністрації відповідного сервісу або ресурсу, на якому й було вчинено шахрайські дії; б) постачальника послуги підключення до мережі «Інтернет» (провайдера). Також науковець розгорнуто проаналізував перелік відомостей, які можливо таким чином отримати, та порадив окрему форму запиту із урахуванням специфічності інформації[253].

Аналіз опитування респондентів (додаток А) надав можливість виокремити такі організаційні форми взаємодії під час розслідування кримінальних правопорушень у кіберпросторі, а саме:

а) взаємний обмін інформацією між працівниками підрозділів правоохоронних органів, а також державних, приватних і громадських підприємств, установ і організацій під час кримінального провадження – 89 %;

б) консультування – 77 %;

в) спільне обговорення й оцінювання відомостей, одержаних у результаті проведення розшукових заходів, щодо їх достатності для внесення відомостей до ЄРДР – 73 %;

г) спільні виїзди уповноважених осіб (слідчого, дізнавача) й оперативних працівників для проведення слідчих (розшукових) дій, НСРД – 58 %;

д) колегіальне проведення складних процесуальних дій (огляд місця події, слідчий експеримент) або окремих тактичних операцій – 53 %.

Також варто акцентувати увагу на важливості застосування «взаємного обміну інформацією між працівниками підрозділів правоохоронних органів, а також державних, приватних і громадських підприємств, установ і організацій» як однієї з найбільш ефективних форм взаємодії в досліджуваній категорії кримінальних проваджень, особливо в умовах воєнного стану. Обмін інформацією може стосуватися:

– ознак кримінальних правопорушень проти моральності (вчинених чи

[253] Самойлов С. В. Консультативна та довідкова діяльність обізнаних осіб як форма застосування та використання спеціальних знань при розслідуванні шахрайств, учинених з використанням мережі «Інтернет». *Держава і право в умовах судової реформи* : матеріали всеукр. наук.-практ. конф. студ., аспір. і молод, учен. (м. Донецьк, 8 квіт. 2011 р.). Донецьк : Дон. ун-т економіки і права, 2011. С. 257–259.

тих, що готуються);

– фізичних і юридичних осіб, причетних до кримінальних правопорушень, а також потерпілих осіб;

– складу, структури, сфери діяльності та зв'язків ОГ і ЗО;

– предметів злочинного посягання, які становлять інтерес для розслідування (тварини; предмети порнографічного характеру; твори, що пропагують культ насильства та жорстокості, расову, національну чи релігійну нетерпимість і дискримінацію; документи Національного архівного фонду; тіло (останки, прах) померлого; урна з прахом померлого);

– слідів кримінальних правопорушень проти моральності, речових доказів, які можуть сприяти з'ясуванню обставин розслідуваного кримінальних правопорушень (матеріали ДНК; вилучені відбитки слідів пальців рук) тощо[254].

Окрім того, зазначені дані можуть відображати:

– ознаки кримінального правопорушення (які вже вчинені або ще готуються);

– характеристику членів хакерських груп та організацій (фішерів, спамерів, кардерів), які можуть бути причетні до вчинення протиправних діянь;

– побудову (структуру) та галузь діяльності (фішинг, кардинг) злочинних груп, що задіяні у вчиненні шахрайства або інших кримінальних правопорушень[255].

На основі опитування респондентів (додаток А) серед типових недоліків у процесі виконання взаємодії вказаних підрозділів під час розслідування кримінальних правопорушень у кіберпросторі можна виділити такі:

– невчасний початок здійснення взаємодії – 78 %;

– припинення взаємодії з боку учасників кримінального провадження після закінчення його початкового етапу – 69 %;

– спрямування початкових слідчих (розшукових) дій, НСРД та інших процесуальних дій «визначальній» меті – затриманню кіберзлочинця, у той час як реалізація встановлення обставин вчинення кримінальних правопорушень у кіберпросторі відходить на другий план – 53 %;

– здійснення слідчих (розшукових) дій, НСРД та інших процесуальних дій оперативними працівниками без участі уповноваженої особи – 41 %.

[254] Єфімов М. М. Методика розслідування кримінальних правопорушень проти моральності: наукові та праксеологічні основи : монографія. Одеса : Видавничий дім «Гельветика», 2020. 392 с.

[255] Чаплинський К. О., Єфімов М. М., Жилін А. Е. Методика розслідування шахрайства у сфері використання банківських електронних платежів : монографія. Одеса : Юридика, 2024. 218 с.

Констатуючи наведене вище, зазначимо, що правильно спланована й організована взаємодія різних підрозділів правоохоронних органів забезпечує максимальне отримання доказової інформації для найбільш ефективного проведення процесуальних дій і заходів.

2.4. Профілактична діяльність уповноважених осіб у провадженнях за фактами вчинення кримінальних правопорушень у кіберпросторі

Під час розслідування кримінальних правопорушень у кіберпросторі важливе значення мають заходи профілактики.

Варто зауважити, що деяким кримінальним правопорушенням у кіберпросторі (фітинг, смішинг, сніфферінг, кардінг) можна запобігти окремими профілактичними заходами. Позаяк указані протиправні діяння вчиняються стосовно пересічних громадян, які не мають уявлення про можливі злочинні схеми та про можливості їх виявлення та попередження. Водночас інша категорія протиправних діянь у визначеній сфері, які направлені на порушення нормального функціонування різноманітних структур (на сьогодні досить часто щодо оборонної сфери), є більш складними для здійснення профілактичних заходів.

А вже Е. В. Малютін слушно наголошує на тому, що «… запобігання протиправним діянням з кожним роком стає все більш важливим напрямом діяльності всіх підрозділів правоохоронних органів у демократичних державах. У кримінальних провадженнях, розпочатих за вчиненими правопорушеннями, пов'язаними з використанням е-банкінгу, профілактичні заходи відіграють неабияку роль. Оскільки правильно організовані дії щодо їх реалізації можуть розбити вщент усі намагання злочинців, які скоюють визначені протиправні діяння»[256].

Загалом, щодо предмета криміналістичної профілактики звернемося до наукової статті С. В. Томіна, який зазначав, що «… закономірності утворення, виявлення та дослідження слідів прояву криміногенних обставин під час підготовки, вчинення і приховання окремих видів і категорій злочинів відомими криміналістам способами (незалежно від того, чи застосовувались такі способи злочинцями, чи застосування їх є можливим і прогнозується криміналістами); техніко-криміналістичні засоби захисту об'єктів від злочинних посягань, що сприяють виявленню і припиненню злочинів, а також використовуються з метою отримання, накопичення і видачі інформації про знаряддя і засоби, що використовуються під час вчинення злочинів, та осіб, схильних до їх

[256] 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. 456–460.

вчинення; техніко-криміналістичні засоби, прийоми і методи виявлення, фіксації і дослідження криміногенних обставин; тактичні прийоми і засоби найбільш ефективного виявлення і усунення криміногенних обставин, а також запобігання і припинення злочинів; криміналістичні методи або системи прийомів виявлення і усунення причин і умов вчинення злочинів, а також припинення і попередження злочинів»[257].

Своєю чергою, А. Е. Жилін, на основі проведеного аналізу ряду нормативно-правових актів (закони України «Про Національну поліцію»[258], «Про Службу безпеки України»[259], «Про Державне бюро розслідувань»[260]), констатував, що «… одним із основних завдань правоохоронних органів є здійснення профілактичних заходів щодо усунення причин та умов вчинення кримінальних правопорушень. Стосовно розслідування фактів вчинення шахрайства у сфері використання банківських електронних платежів, одразу відмітимо, що уповноважені особи також проводять окремі заходи попереджувального характеру у визначеній категорії кримінальних проваджень»[261].

Ми повністю підтримуємо вказану позицію, оскільки, як ми зазначили раніше, більшості випадків вчинення досліджуваних протиправних діянь можна запобігти дієвими профілактичними заходами.

Зі свого боку, Е. В. Малютін доречно вказував, що «… запобігання протиправним діянням з кожним роком стає все більш важливим напрямком діяльності всіх підрозділів правоохоронних органів в демократичних державах. В кримінальних провадженнях, розпочатих за вчиненими правопорушеннями, пов'язаними із використанням е-банкінгу, профілактичні заходи відіграють неабияку роль. Оскільки правильно організовані дії щодо їх реалізації можуть розбити вщент всі намагання злочинців, які скоюють визначені протиправні діяння. Усі протиправні діяння, пов'язані з використанням е-банкінгу, вчинюються у кіберпросторі»[262].

А вже В. В. Приловський відмічав, що профілактична діяльність є засо-

---

[257]Томін С. В. Об'єкт та предмет профілактики кримінальних правопорушень як окремого вчення криміналістики. *Прикарпатський юридичний вісник*. 2016. Вип. 3 (12). С. 123–127.

[258] Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 27.09.2025).

[259] Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 27.09.2025).

[260] Про Державне бюро розслідувань : Закон України від 12.11.2015 р. № 794-VIII. URL: https://zakon.rada.gov.ua/laws/show/794-19#Text (дата звернення: 27.09.2025).

[261] Жилін А. Е. Актуальні питання реалізації профілактичних заходів працівниками правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Юридична наука*. 2020. № 2. Т. 2. С. 209–215.

[262] 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. 456–460.

бом попередження вчинення протиправних діянь у майбутньому. Тому працівники правоохоронних органів зобов'язані неодмінно реалізовувати відповідні профілактичні заходи. Водночас учений вірно акцентує увагу на тому, що уповноважені особи можуть виконувати лише ті заходи профілактики, які передбачені їх посадовими обов'язками або нормативно-правовими актами[263].

Також вважаємо за доцільне навести твердження С. М. Школи, який зазначає, що «… профілактика правопорушень здійснюється в рамках адміністративної діяльності поліції – підзаконної, цілеспрямованої виконавчо-розпорядчої діяльності уповноважених суб'єктів з організації та здійснення охорони публічного порядку, забезпечення публічної безпеки, запобігання адміністративним і кримінальним правопорушенням і їх припинення»[264].

Доречним вважаємо судження Л. Шеллі, яка констатувала, що правоохоронні органи в переважній більшості розвинених країн не можуть найняти та утримувати персонал, який потрібен для протидії злочинній діяльності транснаціональних злочинних груп. Авторка це пояснює тим, що через низькі зарплати та корупційну складову правоохоронних органів особи з високорозвиненими технічними навичками не можуть знайти достатньо оплачувану роботу в державному секторі. Тому дослідниця робить відповідний умовивід, що вказані особи в країнах, які розвиваються, вирішують не працювати за низькі зарплати правоохоронців, а обирають приватний сектор, а деякі з них свідомо чи несвідомо працюватимуть на злочинні чи терористичні групи. Крім того, Л. Шеллі слушно вказує на те, що багато з тих, хто працює у високотехнологічному секторі в Європі та Сполучених Штатах, є іммігрантами з менш розвинених країн і не бажають працювати в правоохоронних органах країн, в яких вони народилися. Як приклад, авторка наводить ситуацію, коли один вебсайт, що містив дитячу порнографію, був розміщений в інтернеті в одній з країн Центральної Азії, то понад чотири мільйони осіб завантажили зображення з сайту, перш ніж його було заблоковано, а причина цього якраз полягає в тому, що в цій країні не було комп'ютерних спеціалістів, які могли б закрити вказаний ресурс[265]. Як бачимо, Л. Шеллі акцентує увагу на потребі надавати працівникам правоохоронних органів достойну зарплату.

П. М. Білий та С. О. Баранов констатували, що «… попередження правопорушень уявляє собою сформовану систему дій на антисуспільні явища та їх причинний комплекс з метою реалізації тенденцій зниження їх рівня і масштабів. При цьому попередження правопорушень розглядається як соціально-

[263] Приловський В. В. До питання здійснення профілактичних заходів працівниками правоохоронних органів стосовно виявлення та усунення причин і умов втягнення неповнолітніх у протиправну діяльність. *Юридична наука*. 2019. № 11. С. 191–197.

[264] Школа С. М. Правові засади профілактичної роботи національної поліції України. *Актуальні проблеми вітчизняної юриспруденції*. 2016. № 3. С. 129–132.

[265] Louise, I. Shelley Organized Crime, Terrorism and Cybercrime. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/organized-crime-terrorism-and-cybercrime (дата звернення: 06.09.2025).

правовий процес, знижуючий, обмежуючий, ліквідуючий протиправні явища за допомогою всієї сукупності заходів, що здійснюються державними органами і громадськими формуваннями і спрямовані на удосконалення суспільних відносин»[266].

Загалом, профілактика вчинення кримінальних правопорушень є одним із завдань уповноважених осіб, що здійснюють правоохоронну діяльність. Тобто, профілактична функція повинна виконуватися незалежно від служби, у якій працює той чи інший правоохоронець, та від його посади. Раніше КПК України зобов'язував слідчого здійснювати ряд заходів з усунення причин та умов вчинення протиправних діянь. На жаль, зараз така норма відсутня. Але, на наше переконання, в уповноважених осіб, які здійснюють досудове розслідування (слідчий, дізнавач, прокурор), є можливості хоча б зробити мінімум, щоб уникнути в подальшому вчинення подібних протиправних діянь[267].

У свою чергу, Ю. В. Александров, А. П. Гаврилишин, та О. М. Джужа зазначили, що «… разом з тим практика протидії злочинності свідчить, що при визначенні поняття «профілактики злочинів» потрібно виходити з економічних, соціально-політичних, моральних, психологічних, правових та інших більш широких позицій. Такий підхід дає можливість сформулювати це поняття у широкому розумінні, що включає в себе різні заходи державних органів і громадських організацій. Йдеться про те, щоб не допустити існування злочинності у майбутньому, а у найближчій перспективі – якомога більше обмежувати її прояви. Профілактика злочинності є сформованою системою дій стосовно антисуспільних явищ та їх причинного комплексу з метою розширення тенденції зниження рівня і масштабів злочинності і знешкодження її коріння. Отже, профілактика злочинності розглядається як соціально-правовий процес, що знижує, обмежує, ліквідує явища, породжені злочинністю. У найбільш узагальненому вигляді профілактика злочинності забезпечується усією сукупністю заходів, що здійснюються державними органами і громадськими формуваннями, спрямованими на удосконалення суспільних відносин»[268].

Стосовно профілактичної функції працівників правоохоронних органів, то варто вказати, що вона обов'язково повинна реалізуватися незалежно від служби, де працює той чи інший правоохоронець, та від його посади[269]. Іншими словами, що профілактичну діяльність можна визначити як сукупність

---

[266] Білий П. М., Баранов С. О. Основи профілактики злочинів на транспорті : навч. посіб. Київ : УКРІНФОРМ, 2001. 196 с.

[267] Єфімов М. М. Методика розслідування кримінальних правопорушень проти моральності : наукові та праксеологічні основи : монографія. Одеса : Видавничий дім «Гельветика», 2020. 392 с.

[268] Кримінологія і профілактика злочинів. Курс лекцій у 2-х кн. Особлива частина / Ю. В. Александров та ін. Київ : НАВСУ, 2000. 201 с.

[269] Yefimov, M., Omarov, Y. Scientific Debates On The Preventive Activities Of Authorized Persons As Part Of The Methodology For Investigating Criminal Offences Against Morality. *Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs*. 2021. Special Issue № 1 (114). pp. 114–119.

певних дій (заходів), спрямованих на усунення причин та умов злочинної діяльності, яка повинна здійснюватись будь-якими уповноваженими особами правоохоронних органів.

Водночас І. В. Однолько відмітила, що «… втягнення неповнолітніх у злочинну діяльність вже давно стало однією з глобальних проблем кримінально-правової політики України та інших держав, адже злочинність серед неповнолітніх у певному сенсі є фактором росту злочинності дорослих. І щоб не допустити зростання злочинності слід зосередити увагу на запобіганні й, передусім, – захисті неповнолітніх осіб від негативних явищ, серед яких украй небезпечним є втягнення дорослими особами неповнолітніх у злочинну діяльність. Підвищена увага до захисту неповнолітніх обумовлена особливим психологічним розвитком дитини, якому притаманне її специфічне сприйняття навколишнього світу. Дитина на відмінну від дорослої особи більш психологічно відкрита для сприйняття як позитивного, так і негативного досвіду. Разом із тим її воля слабкіша, а у певних випадках зовсім відсутня у протидії негативному впливу, що пояснюється моральною, інтелектуальною та фізичною незрілістю. Дорослі, розуміючи це, нерідко намагаються використати психологічні особливості розвитку дітей в особистих злочинних та аморальних цілях. Тому необхідним та обґрунтованим є захист дітей від подібних негативних дій»[270].

Стосовно факторів, які впливають на вчинення протиправних діянь, А. Ф. Волобуєв висловлював таку думку: «… причини конкретного злочину – це ті активні фактори, які викликають у певної особи інтереси, мотиви для його вчинення. В основі злочинної мотивації як суб'єктивного психофізіологічного процесу знаходяться певні людські вади: корисливість, правовий нігілізм, егоїзм, кар'єризм, жорстокість, негативні психологічні особливості тощо. Це повністю суб'єктивна сфера, пов'язана з особливостями конкретної людини. Формування особистості злочинця – складний процес, який ще недостатньо вивчений в кримінології і викликає спори, але можна з упевненістю стверджувати, що в ньому переплітаються і взаємодіють біологічне, психологічне і соціальне. Структура будь-якої особистості, в тому числі і злочинця, складається поступово в процесі взаємодії між зовнішнім середовищем і психічною організацією індивіда, яка формуються на основі певних генетичних компонентів. Тому встановлення причин конкретного злочину полягає у вивченні особи обвинуваченого, визначенні її негативних рис, які в конкретній життєвій ситуації призвели до вчинення нею злочину. Зібрані відомості про особу обвинуваченого повинні знайти відбиття у матеріалах кримінальної справи, оскільки вони враховуються судом під час визначення виду і міри покарання»[271].

---

[270] Однолько І. В. Запобігання втягненню неповнолітніх у злочинну діяльність. *Науковий часопис Національної академії прокуратури України*. 2016. № 4. С. 146–154.

[271] Волобуєв А. Ф. Профілактична діяльність при розслідуванні злочинів у сфері підприємництва. *Вісник Університету внутрішніх справ*. 2000. № 12. Ч. 1. С. 62–69.

Пізніше А. Ф. Волобуєв при вивченні матеріалів розслідуваних кримінальних проваджень помітив, що «… застосування різної термінології негативно позначається на практиці розмежування причин і умов. Так, за даними нашого дослідження, у справах про кримінальні правопорушення, вчинені неповнолітніми, слідчі у поданнях найчастіше повністю ототожнюють умови, що сприяли вчиненню злочинів, з причинами їх скоєння. Нерідко слідчі зовсім не виявляють причини і умови злочинів, обмежуючись викладенням обставин вчинення і вини обвинуваченого та пропозицією обговорити його поведінку в трудовому колективі. Фактичне ототожнення причини злочину і його об'єктивної сторони приводить до висновку, що причиною злочину є сам злочин. Таке твердження веде до визнання неможливості усунення причин конкретного злочину, тому що дії злочинця є на момент їх розслідування подією минулого»[272].

На основі опрацювання результатів опитування респондентів (додаток А) нами було встановлено, що серед чинників, які впливають на поширення кримінальних правопорушень у кіберпросторі, є:

– віктимна поведінка (недбалість, необізнаність, зайва довірливість тощо) потерпілих – 93 %;

– недосконалість законодавства у сфері інформаційних відносин – 62 %;

– високий рівень корумпованості органів державної влади та місцевого самоврядування – 58 %;

– відсутність ефективної взаємодії державних органів між собою – 53 %.

А вже О. М. Джужа, Я. Ю. Кондратьєв, О. Г. Кулик та П. П. Михайленко вказують, що «… тільки тепер вони конкретизуються і переходять у психологічну форму, пояснюючи цілі й мотиви поведінки конкретної людини – злочинця. Причини індивідуального злочину визначаються як неузгодженість поведінки особистості з соціальним середовищем, в основі якої лежать негативні риси, що сформувалися у конкретної людини під впливом певних факторів. При цьому підкреслюється можливість переорієнтації і виправлення такого суб'єкта»[273].

Л. О. Махова та А. О. Виприцький вказують на те, що «… як спеціальний різновид правоохоронної діяльності, врегульований нормами адміністративного права; за спеціальними уповноваженими суб'єктами, що здійснюють профілактичну діяльність; за змістом – здійснення комплексних заходів, щодо

[272] Профілактична діяльність слідчого при розслідуванні злочинів : Лекція для всіх форм навчання / Укл. А. Ф. Волобуєв. Харків : Національний університет внутрішніх справ, 2003. 23 с.

[273] Кримінологія : підруч. для студ. вищ. навч. закладів. / За заг. ред. О. М. Джужі. Київ : Юрінком Інтер, 2002. 352 с.

виявлення та усунення факторів, причини та умов скоєння правопорушень; за місцем проведення – громадські місця; за метою – зменшенням кількості правопорушень»[274].

Стосовно формулювання профілактичної діяльності, то, для прикладу, А. Е. Жилін визначив її як систему конкретних дій (заходів), які здійснюють уповноважені особи правоохоронних органів (дізнавачі, слідчі, прокурори та інші), що мають на меті усунення причин та умов вчинення протиправних діянь конкретної категорії[275].

У розрізі зазначеного вважаємо доречним твердження А. В. Микитчика, який констатував, що «… активний розвиток комунікаційних мереж, інформаційних технологій і масової комп'ютеризації призвели до еволюційних змін кримінального середовища не тільки на рівні окремих держав, а й у всьому світовому співтоваристві. Відсутність належного соціального контролю призвела до того, що мережа Інтернет практично безкарно стала використовуватися злочинцями як місце і основний засіб вчинення різних протизаконних посягань, як традиційних (шахрайств, крадіжок), так і інших – викрадень та продажу конфіденційної інформації, вимагань, «геймерських» шахрайств, а так само поширення предметів і послуг, які були виключені з легального обігу (наркотичних засобів, дитячої порнографії). Особливу небезпеку становлять кіберекстремізм і крайня його форма – кібертероризм, тобто дії з дезорганізації роботи інформаційних систем, що створюють небезпеку загибелі людей, заподіяння значної майнової шкоди чи настання інших суспільно небезпечних наслідків, якщо вони вчинені з метою порушення громадської безпеки, залякування населення або здійснення впливу на прийняття рішення державними органами, а також погроза вчинення зазначених дій з тією ж метою»[276].

Щодо конкретних підрозділів, які мають здійснювати профілактичну діяльність з усунення причин та умов учинення кримінальних правопорушень у кіберпросторі, то ми вважаємо серед них основним Департамент кіберполіції Національної поліції України. Оскільки вказаний підрозділ є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кі-

[274] Махова Л. О., Виприцький А. О. Профілактика адміністративних правопорушень у громадських місцях: поняття та види. *Право і суспільство.* 2019. № 2. С. 142–147.

[275] Жилін А. Е. Актуальні питання реалізації профілактичних заходів працівниками правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Юридична наука*. 2020. № 2. Том 2. С. 141–148.

[276] Микитчик А. В. Заходи запобігання кіберзлочинності в Україні. *Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку* : зб. тез доп. міжнар. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 137–139.

берзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність[277].

Окрема група дослідників констатувала, що одним із ключових завдань правоохоронних органів є створення ефективної та стабільної системи підготовки фахівців, які володітимуть технологіями розслідування злочинів, пов'язаних з легалізацією (відмиванням) незаконних доходів, зокрема доходів, отриманих за допомогою протиправних схем. Також, як зазначають автори, щоб запобігти використанню злочинцями доходів, отриманих протиправним шляхом, доцільно застосовувати заходи своєчасного вилучення активів відповідно до справ. Крім того, для мінімізації шахрайства та зловживань компанії, на думку науковців, варто вдосконалити внутрішній контроль, незалежний аудит, а також оптимізувати та вдосконалити наглядові функції[278].

Також варто вказати, що основними завданнями Департаменту кіберполіції Національної поліції України визначено такі, як:

– участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– сприяння в порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень[279].

У розрізі сказаного вважаємо за доцільне навести думку групи дослідників (Д. В. Пашнєв, М. Г. Щербаковський), які зауважили на встановленні таких обставин кримінального правопорушення, як-от: «… місця неправомірного проникнення в комп'ютерну мережу (зсередини організації або ззовні); способу здійснення неправомірного доступу (копіювання, модифікація, знищення інформації, внесення шкідливих програм) і його результати; засобів, що були використані для вчинення злочину (технічні, програмні, носії інформації); способів подолання захисту (підбір ключів і паролів, викрадання паролів, відключення засобів захисту тощо); виявлення слідів протиправного діяння. Крім того, автори зауважили, що для реалізації названих завдань повинні бути здійснені такі першочергові слідчі (розшукові) дії: «… огляд місця події (якщо це не було здійснено до початку кримінального провадження), допит свідків (персоналу організації, де виявлено правопорушення) та потерпілого, призначення комп'ютерно-технічної експертизи. Потім ухвалюються процесуальні

---

[277] *Департамент кіберполіції Національної поліції України* : офіц. сайт. URL: https://cyberpolice.gov.ua/contacts/ (дата звернення: 18.09.2025).

[278] Yefimov, M., Pavlova, N., Fedchenko, V., Pletenets, V., Kryvopusk, O. Foreign Experience In Legal Regulation Of Fraud Investigation. *Revista De La Universidad Del Zulia*. 2022.13 (38). pp. 159–168.

[279] *Департамент кіберполіції Національної поліції України* : офіц. сайт. URL: https://cyberpolice.gov.ua/contacts/ (дата звернення: 18.09.2025).

рішення стосовно тимчасового доступу до документів і заходів щодо встановлення та розшуку винного, пошуку його робочого місця, звідки відбувалося вторгнення в комп'ютер (комп'ютерну систему). Здійснюється перевірка за криміналістичними обліками з метою одержання даних, які дозволяють зробити висновки (висунути версії) про причетність певної особи до вчиненого злочину, скоєння декількох злочинів в один спосіб та ін. На цій підставі можуть бути проведені негласні слідчі (розшукові) дії (аудіо-, відеоконтроль особи – ст. 260 КПК України, арешт, огляд і виїмка кореспонденції – ст. 261–262 КПК України, зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем – ст. 263–264 КПК України, спостереження за особою, річчю або місцем – ст. 269 КПК України, аудіо-, відеоконтроль місця – ст. 270 КПК України та ін.»[280].

Констатуючи наведене вище, вкажемо, що важливого значення набувають заходи попередження кримінальних правопорушень у кіберпросторі задля уникнення такого виду протиправних діянь.

В. В. Сисолятін у своїй дисертаційній роботі в розрізі розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, запропонував таку сукупність запобіжних заходів:

«– застосовування протоколів безпеки, зокрема, використання криптографічних функцій, а також системи аутентифікації користувачів шляхом перевірки правильності внесених даних і запобігання заміні особи;

– застосовування технологій фіксації транзакцій, для прикладу, блокчейн, що допускають фіксувати всю інформацію;

– повідомлення громадян через медіа (ЗМІ), соціальні мережі та месенджери (Viber, Telegram, WhatsApp) про факти скоєння кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу (фішинг, кардинг);

– встановлення осіб, які мають нахили до антисуспільної поведінки в інформаційній сфері та постановка їх на відповідні обліки у підрозділах правоохоронних органів (зокрема, кіберполіції)»[281].

Як приклад профілактичної діяльності Департаменту кіберполіції Національної поліції України, наведемо перелік правил кібергігієни, дотримання яких, на думку фахівців вказаного Департаменту, значно мінімізує ризики постраждати від злочинних дій хакерів:

«…– уважно перевіряйте URL-адресу сайту, на якому збираєтесь розраховуватися банківською карткою;

– використовуйте лише ліцензійні програми, систематично та своєчасно їх оновлюйте;

– здійснюйте регулярне резервне копіювання даних, зберігайте їх на зовнішніх носіях інформації;

[280] Криміналістика : підручник : у 2 т. Т. 2 / за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової ; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. 312 с.

[281] Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2024. 230 с.

– перевірте підозрілі сайти або номери телефону на сайті кіберполіції;

– нікому не повідомляйте пароль або інші персональні дані, використовуйте складний пароль;

– не переходьте за сумнівними посиланнями, навіть якщо лист надійшов від друга, все одно потрібно пам'ятати, що зловмисники могли отримати доступ і до його акаунтів»[282].

А. В. Микитчик на основі власного дослідження кіберзлочинності в Україні підсумував:

– кіберзлочинність є різновидом злочинності, яка існує нарівні з насильницькою, корисливою, корупційною, екологічної та іншими видами;

– вона тісно взаємопов'язана з іншими видами злочинності, оскільки злочини у сфері комп'ютерних технологій доволі часто виступають способом вдосконалення інших кримінальних правопорушень (крадіжка, вимагання, шахрайство та ін.);

– кіберзлочинність має високотехнологічний характер, що викликано використанням ІТ-технологій, інформаційно-телекомунікаційних мереж, комп'ютерних пристроїв, носіїв комп'ютерної інформації та ін., які виступають знаряддями й засобами вчинення кримінальних правопорушень;

– вона має високий ступінь латентності, яка становить від кількох десятків до кількох тисяч відсотків з різних видів злочинних діянь, що зумовлено різними об'єктивними факторами (небажання жертв комп'ютерних злочинів звертатися до правоохоронних органів, неочевидність комп'ютерних злочинів для більшості населення через їх учинення у віртуальному середовищі, складність виявлення комп'ютерних злочинів за відсутності необхідної кількості фахівців у правоохоронних органах та ін.);

– кіберзлочинність має високоорганізований характер і тісно взаємопов'язана з організованою злочинністю, оскільки значна кількість кіберзлочинів (DDoS-атаки, е-банкінг, фішинг, створення ботів та ін.) вчиняється злочинними групами; має «професійний» характер, позаяк особи, які вчиняють кіберзлочини, мають злочинну спеціалізацію, не вчиняючи інших видів злочинних діянь; отримують злочинний дохід (прибуток) у результаті злочинної діяльності;

– кіберзлочинці мають необхідні знання, вміння, навички в сфері ІТ-технологій для вчинення злочину; дотримуються певних правил, законів, понять і термінології, що дозволяють їм спілкуватися, обмінюватися досвідом і знаходити однодумців;

– кіберзлочинність характеризується транскордонністю, оскільки кіберпростір існує поза державними кордонами і, будучи загальнодоступним, дозволяє злочинцю, що знаходиться на території однієї держави, вчиняти злочинні дії щодо осіб, які перебувають в іншій державі;

[282] Як вберегти техніку від шкідливого програмного забезпечення – поради кіберполіції. URL: https://cyberpolice.gov.ua/article/yak-vberegty-texniku-vid-shkidlyvogo-programnogo-zabezpechennya--porady-kiberpolicziyi-4344/ (дата звернення: 18.09.2025).

– кіберзлочинність має транснаціональний характер, оскільки кіберзлочинці внаслідок своєї приналежності до комп'ютерного «андеграунду» для отримання злочинних доходів і спрощення вчинення злочинних діянь на території двох і більше держав змушені, незалежно від національності, об'єднуватися в міжнародні злочинні групи;

– кіберзлочинність перебуває у стані динамічного розвитку, що обумовлено постійним вдосконаленням існуючих і створенням нових ІТ-технологій, залученням до інформаційних відносини нових учасників, розширенням кіберпростору за рахунок збільшення числа користувачів інтернету, мобільних комп'ютерних пристроїв, переходом до електронного документообігу все більшої кількості організацій, підприємств, установ; отримала риси економічної злочинності, так як більшість кіберзлочинів відбувається в банківсько-фінансовому або корпоративному секторі (інтернет-банкінг, банківський фішинг, кібервимагання та ін.), а діяльність злочинців спрямована на вилучення доходів (прибутку);

– кіберзлочинність трансформується в злочинність політичного характеру, що пов'язано з активізацією протиправної діяльності в кіберпросторі представників хакерського руху, спецслужб і силових структур зарубіжних держав, міжнародних екстремістських і терористичних організацій (DDoS-атаки на урядові сайти, кібершпіонаж щодо інформаційних ресурсів органів державної влади, правоохоронних органів, підприємств оборонно-промислового комплексу, дипломатичних представництв та інше[283].

Приклад ситуації, характерної для вчинення фішингової атаки. Так, у гр. А., який перебував у ДУ «Львівська установа виконання покарань (№ 19)», орієнтовно 20 травня 2023 року виник злочинний умисел на заволодіння чужим майном через шахрайські дії шляхом незаконних операцій з використанням ЕОТ. З метою реалізації свого злочинного умислу шахрай, маючи навички та вміння працювати з комп'ютерною технікою та досвід роботи з інформаційними технологіями, використовуючи спеціальне програмне забезпечення – бот у месенджері «Телеграм», який створює фішингові посилання – вебсторінки, головний розділ яких імітує офіційні урядові, міжнародні та банківські вебсайти, які пропонують отримання грошової допомоги, зі спеціальними полями для введення особистої інформації по банківських рахунках, а саме: номера банківських карток, строк їх дії, CVV-коди, коди підтвердження дворівневої автентифікації, логіни та паролі до веббанкінгу користувачів послуг. Введені на таких вебсайтах банківські реквізити в подальшому передаються гр. А. за допомогою спеціального програмного забезпечення – боту в месенджері «Телег-

[283] Микитчик А. В. Заходи запобігання кіберзлочинності в Україні. *Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку* : зб. тез доп. міжнар. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 137–139.

рам». У свою чергу, шахрай, використовуючи отримані банківські реквізити потерпілих, здійснював вхід в їх облікові записи на сайтах банківських установ, після чого прив'язував картки банківських рахунків потерпілих до свого електронного гаманця Google Pay та розраховувався з них у мобільному додатку «Сільпо», який належить ТОВ «СІЛЬПО-ФУД»[284]*. Тобто, фактична можливість вчинення кримінальних правопорушень у кіберпросторі будь-якими кіберзлочинцями є вкрай великою.*

Т. А. Діброва, Д. О. Пісенко та Н. В. Сметаніна вказали, що «… дійсно, можна констатувати підвищення ефективності боротьби з кіберзлочинністю за допомогою посилення відповідальності за наведені кримінальні правопорушення. Розширення меж діяльності правоохоронних органів щодо розслідування кіберзлочинів, посилення санкцій, додаткова криміналізація окремих діянь – стримують потенційних кіберзлочинців, проте проблема постає в тому, що кримінологічні дослідження у більшості випадків спираються на облікові дані злочинності, при цьому відсутнє вивчення соціальних, економічних, політичних, демографічних, організаційних та інших причин кібершахрайства. Пропозицією постає масштабне, глибоке дослідження проблеми з метою розробки більшого кола заходів із протидії кібершахрайству. Необхідно інформувати населення про витончені методи шахраїв, аби не тільки попереджати вчинення нових кримінальних правопорушень, але й виявляти потенційних злочинців»[285].

А. В. Рейнгольд виокремив такі профілактичні заходи:

«– розміщення оголошень у ЗМІ (медіа) щодо способів комерційних інтернет-шахрайств та заходів їх запобігання;

– виявлення ознак кіберзагроз в транзакціях користувачів мобільного та інтернет-банкінгу;

– відслідковування операцій, які потенційно можуть бути шахрайськими з урахуванням кількості карток клієнта, його місцезнаходженням та місцем здійснення операції, місцезнаходженням та адресою доставки тощо;

– використання новітніх електронних систем та досягнень штучного інтелекту щодо запобігання електронного комерційного шахрайства;

– актуалізація законодавчих актів, що регулюють інтернет-відносини;

– підсилення відповідальності за вчинення шахрайства у мережі Інтернет;

– посилення відповідальності адміністраторів баз даних та інших осіб, які забезпечують функціонування мережі Інтернет, електронних вузлів та пристроїв;

– підсилення міжнародного співробітництва у боротьбі із комерційним кібершахрайством;

---

[284] Справа № 461/1901/25. Архів Галицького районного суду м. Львова, 2025 р.

[285] Діброва Т. А., Пісенко Д.О., Сметаніна Н. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2022. № 11. С. 546–549. URL : http://lsej.org.ua/11_2022/132.pdf (дата звернення: 18.09.2025).

– створення Єдиної інформаційної системи, яка поєднуватиме різноманітні інформаційні ресурси, платформи та бази даних про шахраїв, які вчиняють комерційні інтернет-шахрайства;

– залучення громадськості з профілактики шахрайства в сфері електронної торгівлі»[286].

Констатуючи вказане вище, відмітимо, що підтримуємо перелік профілактичних заходів, які варто здійснювати уповноваженим особам правоохоронних органів, наданий А. Е. Жиліним[287], і дещо його переформатуємо під кримінальні провадження за фактами вчинення кримінальних правопорушень у кіберпросторі та визначимо серед них такі, як:

– застосовування протоколів безпеки, зокрема, криптографічні функції та системи аутентифікації користувачів (для перевірки правильності введених відомостей, попередження заміни особи користувача);

– встановлення осіб, ладних вчинювати протиправну діяльність у сфері ЕОТ (хакери, фішери, кардери) та їх подальша постановка на відповідні обліки у Департаменті кіберполіції;

– інформування населення через медіа про юридичну відповідальність за протиправну діяльність у кіберпросторі;

– повідомлення громадянам із застосуванням різноманітних месенджерів та соціальних мереж про ситуації вчинення протиправних дій у сфері використання ЕОТ (фішинг, сніфферінг, кардинг);

– застосовування технологій фіксації транзакцій, які дозволяють записувати всі дані (зокрема, блокчейн);

– попередження повторних (рецидивних) проявів протиправних дій у кіберпросторі.

Як висновок, зазначимо, що профілактика вчинення кримінальних правопорушень у кіберпросторі є одним із головних завдань уповноважених осіб, що здійснюють правоохоронну діяльність. Тобто, профілактична функція повинна виконуватись незалежно від служби, в якій працює той чи інший правоохоронець, та від його посади. На наше переконання, в уповноважених осіб, які здійснюють досудове розслідування (слідчий, дізнавач, прокурор), є можливості хоча б зробити мінімум, щоб уникнути в подальшому вчинення таких протиправних діянь[288].

---

[286] Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2023. 250 с.

[287] Жилін А. Е. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2023. 226 с.

[288] Єфімов М. М. Теоретичні та практичні засади методики розслідування кримінальних правопорушень проти моральності : дис. … д-ра юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2021. 514 с.

РОЗДІЛ 3
ТАКТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ

3.1. Тактичні особливості проведення окремих слідчих (розшукових) дій під час розслідування кримінальних правопорушень у кіберпросторі

Ефективне розслідування кримінальних правопорушень у кіберпросторі залежить від своєчасного проведення слідчих (розшукових) дій і процесуальних заходів як на початковому, так і подальшому етапах досудового розслідування.

В. В. Сисолятін вказував такі процесуальні дії, що варто проводити на початковому етапі розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу, 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 %)»[289].

Водночас О. Ю. Довженко, досліджуючи основи методики розслідування кіберзлочинів, наголосив на проведенні таких слідчих (розшукових) дій, як огляд місця події, допит потерпілих, свідків, підозрюваних і обвинувачуваних, проведення експертиз[290].

На основі аналізу судово-слідчої практики за досліджуваною категорією протиправних діянь (додаток Б) можна виокремити такі слідчі (розшукові) дії:

– допит підозрюваного (100 %);

– допит потерпілого або представника потерпілої сторони (100 %);

– огляд ЕОТ, документів (100 %);

– призначення судових експертиз (100 %);

– обшук (72 %);

– огляд місця події (61 %);

– одночасний допит раніше допитаних осіб (43 %);

[289] Sysoliatin, V. Problematic Aspects Of The Initial Phase Of Criminal Investigation Offences Involving Internet Banking. *Entrepreneurship, Economy and Law.* 2023. № 5. Pp. 112–117.

[290] Довженко О. Ю. Основи методики розслідування кіберзлочинів : дис. … канд. юрид. наук : 12.00.09 / Харків. нац. ун-т внутр. справ. Харків, 2020. 229 с.

– допит свідка (34 %);
– слідчий експеримент (5 %);
– пред'явлення особи для впізнання (4 %);
– освідування (2 %).

Тобто, матеріали кримінальних проваджень підтверджують результати досліджень учених-криміналістів та визначають найбільш поширеними слідчими (розшуковими) діями під час розслідування кримінальних правопорушень у кіберпросторі огляд місця події та ЕОТ, допит потерпілого, представника потерпілої сторони, свідка та підозрюваного, обшук та призначення судових експертиз. З огляду на зазначене почергово дослідимо вказані процесуальні дії.

Особливості огляду місця події та електронно-обчислювальної техніки.

Згідно ч. 1 ст. 237 КПК України з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей та документів[291].

Вивченням судово-слідчої практики (додаток Б) було встановлено, що хоча огляд місця події й проводився в 61 % випадків, але його ефективність спостерігається не більше ніж у 31 % ситуацій, у зв'язку з тим, що переважно вказані кримінальні правопорушення розтягнуті в часі, а місце їх фактичного вчинення важко встановити.

Спершу наведемо твердження О. І. Мотляха, який наголошував, що «… початковий етап розслідування комп'ютерних злочинів вимагає належного відношення до підготовки та порушення кримінальних справ, пов'язаних з інформаційними технологіями. Особлива роль на цьому та інших етапах розслідування відводиться формуванню висококваліфікованої слідчої та оперативно-розшукової групи. Недоцільно, щоб спеціалістами у сфері високих технологій при процесуальних заходах були запрошені сторонні особи, оскільки вони не вболіватимуть за результативність справи. Осередком сформованої слідчо-оперативної групи та фахівців у зазначеній сфері мають бути особи з числа штатних працівників правоохоронних органів. Понятими ж слід запрошувати осіб, які б хоча мінімально володіють знаннями операційних комп'ютерних систем»[292].

Стосовно особливостей його проведення, то, для прикладу, окрема група

[291] Кримінальний кодекс України : Закон України від 05.04.2001 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення:17.09.2025).

[292] Мотлях О. І. Питанням методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. … канд. юрид. наук : 12.00.09 / Акад. праці і соц. відносин Федерації профспілок України. Київ, 2005. 21 с.

дослідників (В. В. Корнієнко, В. І. Стреляний) зауважує, що «… керівник слідчо-оперативної групи має заздалегідь підготуватися до проведення слідчих дій. Адже необхідно ретельно вивчити, до прикладу, територіальне розташування банку, визначити, у якому приміщенні банк знаходиться: у вбудованому, прибудованому, окремо розташованій будівлі, вивчити входи-виходи (основні й запасні), кількість місцезнаходження пунктів обміну валют.

Потрібно чітко з'ясувати розташування внутрішніх приміщень банку: сховища; спеціальної каси; каси перерахунку; вечірньої каси; операційного залу; центру автоматизованої обробки інформації (комп'ютерного центру-серверу, архівування, модему «Банк-клієнт»); приміщень, де знаходяться індивідуальні сейфи для зберігання цінностей; кабінетів керівництва банку, головного бухгалтера (знати в яких кабінетах працюють комп'ютери, які включено в мережу); підсобних приміщень, особливо приміщень перед сховищами (їх треба оглядати ретельно); складських приміщень»[293].

З приводу типових об'єктів огляду, приміром, В. І. Пазиніч виділяє серед них: «… приміщення, автотранспорт та інші місця, де здійснювалося зберігання, клонування мобільних телефонів, виробництво інших радіоелектронних пристроїв, підробка документів; предмети, пов'язані зі вчиненням злочинів у сфері мобільних телекомунікацій: мобільний телефон злочинця, інші радіоелектронні пристрої, засоби комп'ютерної техніки злочинця і оператора мобільного зв'язку, паперові носії інформації»[294].

На основі дослідження судово-слідчої практики (додаток Б) було встановлено такі місця проведення огляду:

– місця зберігання й обробки електронної інформації, що зазнала протиправного впливу (71 %);

– місця знаходження ЕОТ, що застосовувалася при здійсненні протиправного діяння (51 %);

– місця збереження інформації, отриманої протиправним шляхом (39 %);

– місця настання шкідливих наслідків (10 %).

Д. В. Пашнєв та М. Г. Щербаковський зауважують, що «… після прибуття на місце слідчий повинен вжити таких попереджувальних заходів, які забезпечують цілісність і незмінність інформації на комп'ютерному носії:

[293] Корнієнко В. В., Стреляний В. І. Організація розслідування фактів несанкціонованого переказу коштів з рахунків клієнтів банку, які обслуговуються за допомогою систем дистанційного обслуговування : метод. рек. / Харків. нац. ун-т внутр. справ. Харків, 2015. 71 с.

[294] Пазиніч В. І. Особливості порушення кримінальної справи і початкового етапу розслідування злочинів, які пов'язані з втручанням в роботу мереж мобільного зв'язку. *Науковий вісник Іменем закону*. 2007. № 2. С. 27–29.

– захистити та взяти під охорону приміщення, в якому перебувають засоби комп'ютерної техніки;

– віддалити людей від обладнання та джерел живлення;

– виявити стан комп'ютерної техніки (вимкнена або увімкнена);

– переконатися, що за жодних обставин вимкнений комп'ютер не буде ввімкнено.

Під час проведення огляду (обшуку) спеціаліст безпосередньо надає допомогу слідчому:

– у виявленні засобів комп'ютерної техніки, її окремих компонентів, документації та інших об'єктів, які можуть містити сліди неправомірних дій;

– у коректному (з точки зору збереження слідів злочину) відключенні засобів комп'ютерної техніки від енергопостачання;

– в описі засобів комп'ютерної техніки, її окремих компонентів і документації, що вилучаються, у протоколі та додатках до нього;

– у вирішенні питання щодо складу комплекту комп'ютерної техніки або окремих її компонентів, які підлягають вилученню або ізолюванню від вільного доступу;

– у підготовці засобів комп'ютерної техніки до транспортування (їх упаковуванні, опечатуванні)»[295].

Водночас О. В. Курман зазначає, що незаконне втручання в ЕОТ та комп'ютерні мережі можливе за наявності таких умов:

– володільцем інформації повинні бути визначені умови та правила отримання і обробки інформації;

– власник (розпорядник) електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи оператор (провайдер) мереж електрозв'язку повинні розробити заходи захисту інформації в системі;

– власник (розпорядник) комп'ютерів, систем та оператор (провайдер) мереж повинні розробити правила роботи системи;

– між власником (оператором, провайдером) системи та володільцем інформації повинен бути укладений договір щодо захисту інформації в системі;

– злочинець виконав хоча б одну з операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання інформації»[296].

Наостанок наведемо дані, отримані під час аналізу анкетування респондентів (додаток А), стосовно помилок, які допускали уповноважені особи під час проведення огляду місця події, а саме:

[295] Криміналістика : підручник : у 2 т. Т. 2 / за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. 312 с.

[296] Курман О. В. Способи несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство.* 2017. № 4. С. 245–249.

– неаргументоване звуження меж огляду (81 %);

– ігнорування оперативної інформації (73 %);

– непослідовне та поверхневе дослідження на місці події матеріальної доказової інформації (69 %);

– недодержання тактичних рекомендацій щодо деталізованого опису обстановки та об'єктів огляду (58 %);

– несвоєчасне проведення огляду (51 %);

– відсутність додатків до протоколу (39 %).

Констатуючи наведене вище, слід зазначити, що під час проведення огляду місця події та огляду ЕОТ при розслідуванні кримінальних правопорушень у кіберпросторі варто зважати на специфіку об'єктів, які оглядаються. Зокрема, при огляді ЕОТ необхідно залучати відповідних ІТ-фахівці з кібербезпеки із використанням спеціальних технічних засобів для виявлення, встановлення та вилучення певної інформації, яка знаходиться на електронних носіях і слугуватиме доказами за цим кримінальним правопорушенням.

Особливості проведення обшуку.

Під час розслідування кримінальних правопорушень у кіберпросторі своєчасне проведення обшуку має важливе значення, що дозволяє виявити об'єкти, які доводять причетність конкретних осіб до протиправної діяльності.

Стосовно вказаної процесуальної дії, вважаємо досить правльною тезу О. І. Мотляха, який констатував, що пошук предметів протиправної діяльності та осіб, причетних до вчинення кримінальних правопорушень, – це досить трудомісткий процес, що вимагає спеціальних знань, тривалого часу, фахової підготовленості, уміння на практиці застосовувати складні програмні апаратно-технічні засоби та ін. Учений зауважує, що серед дослідників побутує думка про знеструмлення приміщення перед початком обшуку чи виїмки як ефективний тактичний прийом уповноваженої особи. Водночас дослідник вказує на неприпустимість зазначеної дії, адже це може призвести до непередбачуваних наслідків, у тому числі знищення інформації. Крім того, науковець зазначає , що при проведенні цих процесуальних заходів слід уникнути обшуку приміщення на предмет схованок за допомогою приладів, які містять у собі магнітні носії – це також призведе до руйнування електронної інформації[297].

Т. А. Абушов вказував, що «… проведення обшуку складається з низки організаційних і тактичних заходів, спрямованих на виконання таких завдань:

«– ознайомлення обшукуваного з процесуальними документами, що дають дозвіл на проведення обшуку;

– процесуальне оформлення залучення учасників обшуку, роз'яснення прав та обов'язків, мети й порядку проведення обшуку, повідомлення про застосування технічних засобів, забезпечення реалізації їх прав та обов'язків;

[297] Мотлях О. І. Проведення обшуків та виїмок при розслідуванні злочинів, пов'язаних зі сферою комп'ютерних технологій. *Прокуратура, Людина, Держава*. 2005. № 1 (43). С. 57–67.

– створення умов для постійного та якісного безпосереднього контакту учасників обшуку з об'єктом, який досліджують відповідно до попереднього розподілу завдань (шуканий об'єкт, власник приміщення, члени родини);

– забезпечення інформаційної взаємодії між учасниками обшуку та досліджуваними об'єктами за допомогою методів пізнання;

– одержання нової матеріальної доказової та орієнтуючої інформації, визначення її джерел;

– перевірка, уточнення, доповнення наявної у кримінальному провадженні інформації;

– забезпечення цілісності шуканих об'єктів від дій осіб, зацікавлених у їх невиявлені, фальсифікації або знищенні;

– усунення протиріч, що мають місце в матеріалах кримінального провадження, яке розслідують;

– перевірка загальних та окремих криміналістичних версій стосовно розслідування загалом і обставин, що перевіряють під час проведення обшуку, внесення до них відповідних коректив, висунення їх підстав і нових версій;

– одержання слідчим у процесі обшуку доказової та іншої інформації від учасників обшуку;

– фіксація перебігу проведення та результатів обшуку»[298].

Водночас вважаємо за необхідне виокремити такі заходи підготовчого етапу до проведення обшуку:

– вивчення матеріалів кримінального провадження;

– збирання орієнтувальної інформації про: особу правопорушника, а також членів його сім'ї, родичів і знайомих; усі епізоди злочинної діяльності; місця (об'єкти) обшуків; знаряддя (засоби) злочину та предмети, що здобуті злочинним шляхом і підлягають відшуканню, тощо;

– аналіз та оцінка зібраної інформації та слідчої ситуації, що склалася на певному етапі розслідування, до ухвалення рішення про проведення обшуку;

– прийняття (ухвалення) рішення про проведення обшуку;

– планування та визначення часу проведення обшуку;

– створення оптимальних умов для проведення даної слідчої (розшукової) дії;

– визначення та підготовка необхідних науково-технічних і транспортних засобів;

– вирішення питання про застосування службово-розшукового собаки;

– добір необхідних учасників для проведення обшуку;

– визначення способу фіксації ходу та результатів обшуку;

– розробка заходів, що передбачають дії учасників обшуку у випадках виникнення непередбачуваних ситуацій або ускладнень;

– забезпечення безпеки учасників обшуку;

– складання плану проведення обшуку;

[298] Абушов Т. А. Система організаційних і тактичних дій під час проведення обшуку. *Науковий вісник Національної академії внутрішніх справ*. 2011. № 6. С. 198–205.

– проведення інструктивної наради (інструктаж) серед усіх учасників слідчої (розшукової) дії»[299].

Своєю чергою, С. С. Чернявський зауважує, що «… перед обранням організаційних і тактичних прийомів проведення обшуку слід вирішити низку завдань, зокрема визначити об'єкти, на яких слід проводити обшук (об'єкти обшуку), предмети й документи, які потрібно вилучати (об'єкти пошуку), послідовність і конкретні терміни проведення кожної слідчої дії. Відповідні завдання вирішуються на підставі аналізу матеріалів кримінального провадження»[300].

Об'єктами обшуку під час розслідування кримінальних правопорушень у кіберпросторі (додаток Б) здебільшого були:

– житлові приміщення (55 %);

– приміщення підприємств, організацій, установ, у т. ч. банків (29 %);

– підсобні приміщення (5 %);

– інші об'єкти (4 %);

– гаражі (3 %);

– дачі (2 %);

– транспортні засоби (2 %).

З приводу часу проведення обшуку варто вказати, що він визначається з урахуванням особливостей конкретної ситуації розслідування. Ми підтримуємо думку окремої категорії дослідників, які акцентували увагу на тому, що найбільшу інформативність і значущість для подальшого процесу розслідування обшук набуває тоді, коли проводиться:

– за місцем проживання підозрюваного – у ранковий час (з 6.00 до 8.00), коли особа, у якої проводять обшук, знаходиться у стані, що не дозволяє чинити протидію, а відповідно не має можливості приховати сліди своєї протиправної діяльності;

– в організаціях, установах, підприємствах, банках – до початку робочого часу, коли комп'ютерні системи ще не задіяні в процесі проведення електронних розрахункових операцій[301].

Аналіз матеріалів кримінальних проваджень (додаток Б) дозволив встановити, що обшук переважно проводився в місцях:

---

[299] Чаплинський К. О. Організація і тактичні прийоми проведення одночасних обшуків. *Науковий вісник Юридичної академії Міністерства внутрішніх справ* : зб. наук. пр. 2004. № 3 (17). С. 338–344.

[300] Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : монографія. Київ : Хай-Тек Прес, 2010. 610 с.

[301] Криміналістика : підручник / за заг. ред. А. Ф. Волобуєва. Харків : ХНУВС, 2011. 468 с.

– знаходження комп'ютерного обладнання, що використовувалося при здійсненні протиправного діяння (68 %);

– зберігання й обробки даних (59 %);

– збереження відомостей, одержаних протиправним шляхом (47 %);

– настання шкідливих наслідків (27 %).

Стосовно відповідних спеціалістів, яких варто залучати до проведення обшуку, то ми підтримуємо позицію В. В. Ціркаля, який зауважував, що «… до проведення обшуку так само доцільно залучати фахівців, оскільки без їх допомоги слідчі часто виявляються безсилими в пошуку, правильному вилученні й закріпленні слідів кримінального правопорушення.

Основними завданнями фахівців, що залучаються до процесу проведення даного обшуку, є:

– виконання всіх дій з комп'ютерною технікою для надання допомоги слідчому в описі комп'ютерної техніки та периферійного обладнання;

– проведення експрес-аналізу комп'ютерної інформації;

– виявлення інформаційних слідів злочинів;

– запобігання знищенню або пошкодженню комп'ютерної інформації;

– вилучення комп'ютерної інформації і т.д.»[302].

У такому самому розрізі окрема група дослідників зазначає, що при огляді одного комп'ютера, що знаходиться у власності конкретної особи, уповноважена особа може обмежитися залученням до участі у слідчій (розшуковій) дії фахівця-криміналіста, що має спеціальні знання у комп'ютерно-технічній сфері[303].

Якщо ж обшук проводиться в установі, організації або на підприємстві, де використовувалися кілька комп'ютерів, виникає необхідність у залученні групи різнопрофільних спеціалістів, зокрема, спеціаліста-криміналіста і фахівця в області інформаційних (комп'ютерних) технологій. У разі необхідності може знадобитися й допомога більш вузьких фахівців – системного інженера, системного аналітика, фахівця-бухгалтера та ін. Тобто, у будь-якому випадку особа, яка здійснює обшук, повинна залучити спеціаліста у сфері ІТ-технологій.

Доволі правильним вважаємо твердження І. О. Коваленка, який зазначав, що «… особливу увагу на підготовчій стадії доцільно приділити питанням підготовки комп'ютерної техніки, яка використовується для зчитування та видалення комп'ютерної інформації. Для вирішення цього питання хотілося б

---

[302] Ціркаль В. В. Тактика проведення обшуку з участю фахівців. *Вісник Київського національного університету імені Тараса Шевченка*. Серія «Юридичні науки». 2002. С. 45–48.

[303] Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / В. М. Бутузов, В. Д. Гавловський, Л. П. Скалозуб та ін. Київ : Нац. акад. СБУ, 2011. 142 с.

запропонувати комплект науково-технічних засобів, до складу якого включити:

– портативний персональний комп'ютер (повинен бути оснащений максимальним набором контактів (1xLPT (EPP / ECP), 1xCOM, 1xPS / 2,1xFIR (інфрачервоний порт), 1xMonitor port, 4xUSB 2.0, 1xFireWire, 1xRJ45 (LAN), 1xRJ11 (факс / модем), 1xTV-out (S-video), 1xVideo-in, 1x аудіо вихід, 1x вхід для мікрофона, 1xS / PDIF-out, мережевий роз'єм і т.д.) з можливістю підключення якнайбільшої кількості комп'ютерних засобів (хардварного обладнання (зовнішніх модемів), PCMCIA BIOS-ом і DOS-ом (мережева карта), миша і клавіатура, принтер і сканер, зовнішній привід, медіафото, флешдрайв тощо);

– спеціальні програмні засоби (наприклад, програмне забезпечення Vogon International, яке дозволяє створювати точні дублікати або образи жорстких дисків;

– Gen Tree – проводить складні контекстні пошуки і вивчення графічних і інших об'єктів, система Ilook – забезпечує зняття і стиснення копії (образу) змісту досліджуваного носія для подальшого компактного зберігання і прямого доступу до даних досліджуваного носія і т.п.) для всебічного дослідження і аналізу інформації на місці проведення слідчої (розшукової) дії;

– кабелі, шнури, перехідники для підключення до ЕОМ (електронно-обчислюванні машини) додаткових пристроїв;

– набір носіїв інформації: жорсткий диск (вінчестер) з великою місткістю інформації, компакт-диски, флешкарти;

– набір електромонтажних інструментів;

– набір вимірювальних приладів;

– технічна бібліотека в електронному вигляді (може бути корисною для пошуку інформації, щодо якої у фахівця виникають певні сумніви).

На відміну від інших, цей набір спеціалізованих засобів повинен постійно модернізуватися, поповнюватися новими програмами та даними, а технічні засоби – оновлюватися»[304].

Також для проведення обшуку необхідно враховувати ту обставину, що його проведення найчастіше пов'язано із вторгненням у житлове чи інше приміщення, тобто ця дія обмежує деякі конституційні права громадянина. Для проведення обшуку завжди повинні бути вагомі, або, як сформульовано в законі, достатні підстави. Говорячи про достатність підстав, законодавець мав на увазі, що уповноважена особа повинна володіти відомостями, що не викликають у неї сумнівів. Така інформація отримується внаслідок проведення як

[304] Коваленко І. О. Деякі аспекти проведення обшуку при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Правове життя сучасної України* : у 3 т. : матеріали Міжнарод. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.) / відп. ред. М. Р. Аракелян. Одеса : Гельветика, 2020. Т. 3. С. 385–387.

слідчих (розшукових) дій, так і оперативних заходів відповідно до Закону України «Про оперативно-розшукову діяльність»[305].

Досить вдало О. І. Мотлях вказує на те, що «… тактика проведення слідчого обшуку та виїмки об'єктів доказового значення на подальшому етапі розслідування зазначеної категорії злочинів має відповідати таким критеріям: психологічній налаштованості слідчого на проведення процесуальної дії; умінню не реагувати на ознаки певної невизначеності, недостатньої впевненості, передчуття відсутності результативності проведення слідчого заходу; визначенню оптимальних умов (місця, часу, обстановки, обставин, сприятливих умов) успішної реалізації слідчих (розшукових) дій та ін.»[306].

До того ж, «… після потрапляння до місця проведення обшуку, як зазначають окремі науковці, уповноважена особа повинна запропонувати особі видати речі, які передбачені ухвалою слідчого судді, а також інші речі, які вилучені з цивільного обігу чи незаконно отримані. На початковому етапі обшуку важливого значення набуває встановлення психологічного контакту, що досягається через взаємне сприймання сторін та обмін як вербальною, так і невербальною (міміка, жести) інформацією. Такий контакт може бути започатковано, наприклад, коли слідчий перед обшуком пропонує віддати розшукувані об'єкти, мотивуючи це тим, що небажано, щоб діти, повернувшись зі школи, спостерігали картину обшуку. Навіть за умови негативної відповіді такий крок може стати підґрунтям до встановлення подальшого контакту. Якщо обшукуваний тримається скуто, самовпевнено чи агресивно, такий стан можна спробувати зняти бесідою про родинні стосунки, роботу, стан здоров'я тощо»[307].

А. І. Кунтій щодо проведення вказаної слідчої (розшукової) дії зазначав таке:

«– використання принципу раптовості під час прибуття та входження до приміщення, у якому буде проводитись обшук або в якому знаходиться комп'ютерна техніка, що підлягає обшукові;

– об'єктом пошуку є не тільки технічний пристрій чи матеріальний носій комп'ютерної інформації, якими можуть бути жорсткий диск комп'ютера, дискета, оптичний диск, флеш-карта тощо, а й інформація, яка зберігається на них і яка, власне, й є основним об'єктом пошуку та вилучення з метою встановлення обставин учинення комп'ютерного злочину;

– місцем проведення слідчої (розшукової) дії в такому разі буде не просто приміщення, у якому є носій комп'ютерної інформації, а приміщення, технічний засіб та інформаційний масив конкретного комп'ютерного об'єкта;

---

[305] Про оперативно-розшукову діяльність : Закон України від 22.05.2019 р. № 2720-VIII. URL: https://zakon.rada.gov.ua/laws/show/2135-12 (дата звернення: 12.09.2025).

[306] Мотлях О. І. Тактичні основи проведення обшуку у злочинах, пов'язаних з інформаційними технологіями. *Вісник Академії праці і соціальних відносин Федерації профспілок України*. 2002. № 2 (15). С. 157–159.

[307] Юридична психологія : підручник / за заг. ред. Л. І. Казміренко, Є. М. Моісеєва. Київ : КНТ, 2007. 360 с.

– вилучення комп'ютерних об'єктів, що містять інформаційні дані, може здійснюватися по-різному. Можуть бути вилучені носії інформації або навіть комп'ютерна система загалом чи окремі її частини, якщо дані не можуть бути доступі для їх копіювання або вивчення на іншому обладнанні. Для відновлення таких даних потрібні спеціальні програми, інколи – додаткове обладнання, а сам процес відновлення може займати чимало часу. В цих випадках провадити фактично дії з дослідження програмного продукту під час проведення обшуку або виїмки не доцільно. За певних обставин можна визнати припустимим вилучення даних шляхом їх копіювання на окремі носії інформації. У таких випадках необхідно вжити спеціальних заходів, що забезпечують цілісність і збереження вилучених даних, а використані для копіювання носії не повинні містити жодної інформації. Недоцільно копіювати вилучену інформацію на носії, що містять інформацію, яка стосується цієї справи, навіть якщо ця інформація ідентична або містить фрагменти тієї, котра підлягає вилученню. Повинні бути створені умови та гарантії ідентичності копії оригіналу на момент провадження обшуку або виїмки та надійності її зберігання протягом усього розслідування;

– неможливість використання у процесі пошуку тайників із магнітними носіями металошукачів або рентгенівської установки, оскільки їх застосування може призвести до знищення інформації на цих носіях;

– необхідність швидко проаналізувати великий обсяг інформації, яку було виявлено під час проведення обшуку з метою встановлення її цінності для досудового слідства;

– проведення обшуку лише на одному або декількох комп'ютерах, які входять до локальної комп'ютерної мережі»[308].

О. Л. Мусієнко акцентує увагу на тому, що обшук у приміщеннях, особливо обшук житла, дуже складний процес. Необхідно мати уявлення про основні властивості досліджуваних об'єктів, що забезпечить перевірку різних конструктивних порожнин і ділянок, де можуть бути створені сховища (тайники). Методи дослідження житлових приміщень (при обшуку) у кримінальних провадженнях про шахрайство не мають істотних відмінностей від обшуків за іншими категоріями справ. Обшуку в приміщенні має передувати в ряді випадків вивчення родинних, особистісних та інших зв'язків підозрюваного. Це дозволить здійснити обшуки не тільки за місцем проживання підозрюваного. Автор вказує на те, що іноді шахраї залишають або передають на зберігання предмети й документи своїм знайомим, родичам, іншим особам[309].

Ми підтримуємо твердження окремої групи дослідників, які відмічали, що «… в першу чергу огляду підлягає комп'ютерна техніка, яка знаходиться в робочому (увімкненому) стані. Приступаючи до огляду комп'ютера, слідчий і

[308] Криміналістика : підручник / за заг. ред. Є. В. Пряхіна. 3-тє вид., переробл. та допов. Львів : ЛьвДУВС, 2016. 948 с.

[309] Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / за ред. проф. В. Ю. Шепітька. Харків : Право, 2009. 168 с.

фахівець, який безпосередньо виконує всі дії на комп'ютері, повинні дотримуватися наступних вимог:

– перед вимиканням комп'ютера, при можливості, закрити всі запущені на комп'ютері програми (необхідно пам'ятати, що некоректний вихід з деяких програм може викликати знищення інформації або зіпсувати саму програму);

– вжити заходів щодо встановлення пароля доступу до захищених програм; відключити електроживлення всіх комп'ютерів, опечатати їх і вилучити разом з магнітними носіями для дослідження інформації в лабораторних умовах;

– при необхідності, консультації варто отримувати у різних осіб персоналу підприємства шляхом опитування або допиту, який дозволить отримати максимально правдиву інформацію і уникнути нанесення умисної шкоди;

– при вилученні технічних засобів додаткові периферійні пристрої (принтери, стримери, модеми, сканери тощо) доцільно вилучати тільки в тому випадку, якщо на них працювали підозрювані, або якщо у слідства є питання щодо їх працездатності. Якщо ж для слідства важливою є тільки інформація, то вилучати периферійні пристрої не обов'язково; при наявності локальної обчислювальної мережі необхідно мати значну кількість фахівців для додаткового дослідження цієї мережі;

– слід вилучати всі комп'ютери (системні блоки) і магнітні носії (накопичувачі на жорстких і гнучких магнітних дисках, компакт-диски, DVD-диски, ZIP, дискети тощо);

– провести ретельний огляд документації, звертаючи особливу увагу на робочі записи операторів, тому що часто саме в цих записах недосвідчених користувачів можна знайти коди, паролі і іншу дуже корисну інформацію;

– скласти список всіх позаштатних і тимчасово працюючих фахівців організації (підприємства), з метою виявлення програмістів і інших фахівців у галузі інформаційних технологій, які працюють у даній установі. Бажано встановити їх паспортні дані, адреси і місце постійної роботи;

– записати дані всіх людей, які знаходяться в приміщенні на момент приходу слідчої групи, незалежно від пояснення причини перебування їх у даному приміщенні;

– скласти список усіх співробітників підприємства, що мають доступ до комп'ютерної техніки або часто перебувають у приміщенні, де знаходяться комп'ютери»[310].

В. В. Сисолятін наголошував, що «… на початковому етапі розслідування необхідно максимально забезпечити збереження інформації, яка перебуває на флешнакопичувачах, жорстких дисках (носіях), кеш-пам'яті відповідного пристрою, у хмарних сховищах та ін. Для цього обов'язково потрібно застосовувати проведення одночасних обшуків за різними адресами ймовір-

[310] Комп'ютерно-технічна експертиза. *Центр експертиз* : офіц. вебсайт. URL: https://expertise.kiev.ua/uk/kompyuterno-texnichna-ekspertiza/ (дата звернення: 26.09.2025).

ного знаходження правопорушників. Під час проведення обшуку виникає необхідність вилучати як заблоковані, так і розблоковані переносні гаджети (смартфони, смартгодинники, портативні відеореєстратори, GPS-навігатори). Звісно, специфіка їх вилучення відрізняється, адже з розблокованих пристроїв в принципі достатньо дістати, якщо вони є, SIM-карту та карту пам'яті, тоді як заблоковані потрібно ще розблокувати перед вилученням відповідних слотів. А для цього варто залучити для обшуку спеціаліста в галузі комп'ютерних технологій»[311].

Крім того, при проведенні обшуку слід виділити ряд особливостей: насамперед слід звернути увагу на комп'ютерну техніку, що знаходиться в приміщенні, а також на стан інтернет-мережі. При огляді приміщення потрібно провести пошук портативних USB-флешнакопичувачів, у тому числі замаскованих. Неабияке значення має виявлення мобільного телефону, планшету на місті проведення обшуку[312].

Зі свого боку, Т. В. Романенко констатує, що «… приступаючи до огляду ЕОТ, слідчий і фахівець, що безпосередньо виконують всі дії на ЕОТ, повинні дотримуватися певних вимог з метою забезпечення виявлення та вилучення речових доказів (слідів пальців рук та об'єктів біологічного походження). До особливостей вказаного етапу необхідно віднести:

– відображення слідів пальців рук потрібно шукати на клавіатурі комп'ютера, маніпуляторі типу «миша», пристроях змінних накопичувачів даних, вимикачах живлення та інших елементах управління засобами обчислювальної техніки (кнопки, пристрої подачі паперу та ін.), шнурах мережі та розетках на робочому місці (столі), де встановлено ЕОТ, і безпосередньо на корпусі пристроїв, що входять до складу комплексу. Якщо злочинному впливу підпадає інформація на змінному носії (накопичувачі пам'яті, CD–ROM та ін.), то машинний носій та його технологічна упаковка також будуть зберігати на собі відбитки пальців рук злочинця;

– сліди, що утворюються при підключенні апаратури до ЕОТ, систем ЕОТ та їхніх мереж, на якій або за допомогою якої здійснюється несанкціоноване копіювання інформації. У цьому випадку можна виокремити: відбитки пальців рук на корпусі системного блоку ЕОТ, платах та пристроях, що знаходяться всередині блоку, якщо підключення здійснюється зсередини, розняття, за допомогою яких підключається додаткова апаратура;

– виявлення об'єктів біологічного походження (кров, сперма, букальний епітелій, слина, піднігтьовий вміст, кістки і зуби, волосся з цибулиною), які можуть у подальшому слугувати доказами у кримінальному провадженні, а

[311] 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.

[312] Коваленко І. О., Єфімов М. М. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів : монографія. Одеса : Юридика, 2025. 298 с.

саме на: ЕОТ, периферійних пристроях (принтер, сканер, клавіатура, мишка, багатофункціональний пристрій, блок безперервного живлення, накопичувачі пам'яті, роутер тощо), робочому місці (стіл, стілець, підлога, коврик для миші, інші предмети, що знаходяться поруч), одязі тощо»[313].

І. О. Коваленко зазначає, що «… всі дії, що здійснюються в процесі проведення обшуку, повинні бути детально і чітко відображені в протоколі, до якого можуть додаватися плани і схеми, що оглядаються приміщень, з відображенням у них місць розташування комп'ютерного обладнання. Разом з тим відзначимо окремі особливості, пов'язані з підтриманням активності слідчого під час проведення обшуку з метою виявлення та вилучення електронних носіїв і інформації на них:

– організаційно-тактичні зусилля слідчого (розстановка учасників пошуку, координація дій пошукових груп і ін.);

– своєчасне реагування на будь-які зміни в поведінці присутніх під час обшуку осіб (наприклад, спроби вимикання електроенергії, пересування обшукуваних, відволікання уваги учасників слідчо-оперативної групи гучними вигуками, знищення документів і т.п.);

– при виникненні проблемної ситуації зміна тактичних прийомів обшуку, застосування заходів безпеки для учасників слідчої (розшукової) дії, а також способів збереження доказової інформації;

– обговорення з фахівцем ходу і напрямків обстеження об'єктів (вибір місця початку пошуку, визначення прийомів (методів) пошуку, фіксація окремих дій фахівця за допомогою фото або відеозйомки і т.п.)»[314].

Зокрема, Л. П. Паламарчук акцентує увагу на тому, що матеріальні сліди також можуть залишатися на обчислювальній техніці (сліди від пальців рук, мікрочастинки на клавіатурі, дисководах, принтері тощо), а також на магнітних носіях та оптичних дисках. На його думку, до окремого типу належать інформаційні сліди, що утворюються внаслідок впливу на комп'ютерну інформацію (шляхом знищення, перекручення). Автор зазначає, що вони залишаються на магнітних носіях інформації і пов'язані зі змінами, які відбулися у самій інформації порівняно з початковим її станом. Також до інформаційних слідів належать наслідки роботи антивірусних і тестових програм, які можуть бути виявлені під час вивчення комп'ютерного обладнання, робочих записів

[313] Романенко Т. В. Особливості підготовчого етапу проведення обшуку при розслідуванні шахрайств, що вчиняються з використанням електронно-обчислювальної техніки. *Актуальні проблеми кримінального права, процесу та криміналістики та оперативно-розшукової діяльності* : тези доп. IV Всеукр. наук.-практ. конф. (м. Хмельницький, 26 лют. 2021 р.) / Нац. акад. Держ. прикордон. служби. Хмельницький: Вид-во НАДПСУ, 2021. С. 520–522.

[314] Коваленко І. О. Деякі аспекти проведення обшуку при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Правове життя сучасної України* : матеріали Міжнарод. наук.-практ. конф. У 3 т. (м. Одеса, 15 трав. 2020 р.) / відп. ред. М. Р. Аракелян. Одеса : Гельветика, 2020. Т. 3. С. 385–387.

програмістів, протоколів роботи антивірусних програм та програмного забезпечення. Для виявлення подібних слідів необхідно залучати спеціаліста з комп'ютерної техніки та програмного забезпечення[315].

На основі опрацювання слідчої практики Є. С. Хижняк зробив висновок, що з метою виявлення та вилучення електронних носіїв і відомостей на них, варто рекомендувати:

– уточнити мету, завдання й довести їх до учасників пошукових дій;

– слідчому визначити, які об'єкти він обстежуватиме особисто, а які слід доручити обстежити фахівцям, що беруть участь у проведенні обшуку. Звернути увагу на наявність крім самого ЕОМ зовнішніх пристроїв віддаленого доступу;

– визначити та відключити спеціальні засоби захисту інформації і засоби комп'ютерної техніки від несанкціонованого доступу;

– виявити можливий зв'язок між засобами комп'ютерної техніки та каналами електрозв'язку;

– зафіксувати комп'ютерну техніку, яка перебуває в увімкненому стані, визначити запущені й виконувані операційною системою програми та характер проведених операцій. Сфотографувати зображення на екрані монітора. З допомогою фахівця зупинити роботу виконуваних програм, зафіксувавши в протоколі ці дії й реакцію ЕОМ;

– вжити заходів до створення належних умов для пошуку електронних носіїв інформації (освітлення, визначення місця, де буде проводитися детальне обстеження об'єктів тощо)[316].

На детальній стадії здійснення обшуку з метою виявлення й вилучення електронних носіїв та інформації на них дії уповноваженої особи залежать від методів (тактичних прийомів). Найбільш типовими серед них під час розслідування кримінальних правопорушень у кіберпросторі є:

– за обсягом обшукуваних об'єктів пошук може бути послідовним і вибірковим (в останньому випадку обстеженню підлягають найбільш ймовірні місця знаходження шуканого);

– у приміщенні тактично грамотно організувати пошук від напрямку руху пошукових груп: зустрічний та паралельний (наприклад, проведення пошуку в різних кабінетах). Паралельний пошук доцільно проводити в ситуації, коли обшук проводиться в приміщенні, у якому знаходяться кілька персональних комп'ютерів і серверний комп'ютер. Тут одна пошукова група може обшукувати окремо розташовані ЕОМ, інша пошукова група – серверний

---

[315] Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : автореф. дис. … канд. юрид. наук : 12.00.09. Академія прокуратури. Київ, 2005. 21 с.

[316] Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf (дата звернення: 12.09.2025).

комп'ютер;

– залежно від порушення цілісності об'єкта обшук може бути проведено з порушенням його цілісності або без такого. У ситуації, коли доцільно вилучити внутрішній жорсткий диск, а системний блок має захист від несанкціонованого доступу (замок на кришці системного блоку та ін.), слід відшукати ключ від цього замка. У разі, якщо відшукати ключ від замка кришки системного блоку не вдалося, а користувач (власник) цього ПК відмовляється його відкрити, то з метою вилучення жорсткого диска слід порушити цілісність замка. Коли ж потрібне обстеження наявної інформації на жорсткому диску, немає необхідності в порушенні цілісності об'єкта[317].

Стосовно заключного етапу обшуку ми поділяємо позицію Т. В. Коршикової, яка вказала, що «… детально перераховується кожний предмет, який знаходиться всередині приміщення, та описується у тій послідовності, в якій він був виявлений та оглянутий, і в тому вигляді, в якому він знаходився на момент їх виявлення. Під час огляду предметів:

– описуються його характерні ознаки, а саме, точно вказується місцезнаходження ЕОТ та їх взаємне розташування один щодо одного і навколишніх предметів;

– описується зовнішній вигляд ЕОТ та її складові частини, порядок з'єднання різних вузлів і деталей між собою з вказівкою наявних особливостей (кольору, штампів, написів тощо);

– характеризується та індивідуалізується, записуються номер, марка, назви, серії, номер, форма, колір пристроїв;

– описується порядок з'єднання між собою всіх пристроїв із зазначенням особливостей з'єднання (кількість, розміри, характерні індивідуальні ознаки з'єднувальних проводів, кабелів, шлейфів, розняття);

– наявні дефекти на пристрої, інші індивідуальні ознаки;

– усі маніпуляції з ЕОТ та іншими засобами (включаючи натискання клавіш), які зроблені в процесі проведення СРД, їхній результат (наприклад, при копіюванні файлів);

– встановлюється відсутність або наявність комп'ютерної мережі, телекомунікацій (тип зв'язку, апаратура, що використовується, робоча частота);

– якщо здійснювалося копіювання інформації – описується яка саме інформація та на який пристрій; вид упаковки»[318].

Підбиваючи підсумки, слід наголосити, що належна організація підготовчих заходів та системне застосування відповідних тактичних прийомів під час проведення обшуків у кримінальних провадженнях за фактами вчинення

[317] Коваленко І. О., Єфімов М. М. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів : монографія. Одеса : Юридика, 2025. 298 с.

[318] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

правопорушень у кіберпросторі створюють передумови для суттєвого підвищення рівня та якості досудового розслідування таких правопорушень.

Особливості допиту потерпілого, представника потерпілої сторони, свідків і підозрюваних.

Допит – це процесуальна дія, що являє собою регламентований кримінальними процесуальними нормами інформаційно-психологічний процес спілкування осіб, які беруть у ньому участь, спрямований на отримання інформації про відомі допитуваному факти, що мають значення для встановлення істини у кримінальному провадженні[319].

Слід вказати, що більшість учених-криміналістів поділяють думку стосовно того, що допит є найбільш поширеним способом отримання доказової інформації. Для прикладу, С. І. Мотлях спростовує думку окремих дослідників, які вважають, що проведення допиту не становить особливих труднощів. Крім того, автор наголошує, що вказана «… легкість лише удавана, оскільки допитувані далеко не завжди дають правдиві, повні й об'єктивні показання. Для допиту, у тому числі й свідків у злочинах вказаної категорії, слідчому необхідно:

– ознайомитися зі спеціальною літературою, що стосується предмета допиту;

– приділити увагу пізнанням у сфері електронного документообігу, режиму конфіденційної інформації, засобів і методів її захисту та безпечної обробки;

– отримати кваліфіковані консультації відповідних спеціалістів із цього напряму;

– детально ознайомитися з матеріалами проведених першочергових слідчих (розшукових) дій (протоколами, предметами, документами) та ін.[320].

Тому варто зазначити, що, на нашу думку, допит є однією з найбільш складних слідчих (розшукових) дій, адже його ефективне проведення потребує доволі детально прорахованих та реалізованих організаційно-підготовчих заходів для забезпечення максимально повного його здійснення.

Цікавою є думка М. П. Павлика, який відмічав, що «… враховуючи отриману інформацію, слідчий повинен тактично правильно визначити послідовність допитів, особливо, якщо злочини вчинялися у складі групи. Для цього слід максимально бути поінформованим відносно вікових, морально-психологічних характеристик, ролі та характеру участі кожного з учасників, враховувати їх зацікавленість у кінцевому результаті кримінального провадження. Як показує практика, більш ефективним є отримання в першу чергу показань від особи, яка, на думку слідчого, мала другорядну роль у вчиненні злочину та

[319)] Криміналістика : підруч. для студ. юрид. ВНЗ / за ред. В. Ю. Шепітька. Київ : Ін Юре, 2001. 452 с.

[320] Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. … канд. юрид. наук : 12.00.09 / Акад. праці і соц. відносин Федерації профспілок України. Київ, 2005. 21 с.

вчинила злочин вперше. Більш схильні до надання показань також особи, у відношенні яких є велика кількість доказів. З метою тактичного впливу на учасника допиту, необхідно підготувати докази, які почергово пред'являтимуться під час допиту. Найбільш часто з цією метою використовуються висновки експертиз та різноманітні документи, в яких відображається доказова інформація або документи, що були засобом вчинення злочину, а також інші предмети, що можуть бути речовими доказами»[321].

Як бачимо, вказані вище дослідники частково торкнулися питань підготовчого етапу допиту.

На основі вивчення й узагальнення матеріалів судово-слідчої практики (додаток Б) нами було встановлено, що допит проводився у 100 % кримінальних проваджень, розпочатих за фактом вчинення кримінальних правопорушень у кіберпросторі.

Стосовно організаційно-підготовчих заходів до проведення допиту під час розслідування кримінальних правопорушень у кіберпросторі, то ми підтримуємо позицію Т. В. Коршикової, яка на основі опрацювання думок науковців констатувала: «… під час вказаного етапу вирішуються наступні питання:

– визначення кола обставин, що підлягають з'ясуванню. Для цього перед допитом необхідно ще раз звернутися до матеріалів справи, знову продумати план, проаналізувати версії. Підлягають уточненню дані, що безпосередньо відносяться до предмета допиту, і виявлення джерел, з яких допитуваним стали відомі обставини, факти. При підготовці до допиту потрібно заздалегідь з'ясувати, які докази підтверджують його вину, і систематизувати їх для використання в ході допиту. Іноді буває доцільно скласти перелік питань, що цікавлять слідчого;

– вивчення особи допитуваного. Роль у вчиненні шахрайства з використанням ЕОТ (організатор, виконавець, посередник, підбурювач), наявність судимості, риси характеру (хитрість, акторські здібності, вигадливість), сімейний стан, взаємини з родичами та їх відношення до кримінального правопорушення, антисоціальна спрямованість особи, освітній ценз, відношення до вчиненого, психологічний тип, характер взаємин з іншими учасниками кримінального правопорушення. Якщо особа має судимість, бажано витребувати кримінальні провадження (справи), вироки по яких набули законної сили, і ознайомитися з її поведінкою на допитах;

– визначення часу, місця допиту і способу виклику на допит. Таким місцем може бути службовий кабінет слідчого чи інші службові приміщення, місце події, робочий кабінет допитуваної особи чи місце її проживання. Якщо у кримінальному провадженні проходить кілька свідків (потерпілих), обвинувачених (підозрюваних), то тактично важливо визначити черговість їх допиту.

[321]Павлик М. П. Розслідування злочинів у сфері надання послуг із працевлаштування за кордоном : дис. … д-ра філос. : 081 – Право / Нац. акад. внутр. справ. Київ, 2021. 241 с.

Місцем допиту, як правило, є кабінет слідчого. Він повинен бути обладнаний скромно, без відволікаючих увагу предметів. Під час допиту потрібно виключити появу сторонніх осіб, шумові подразники (телефонні дзвінки, радіо). Обстановка в кабінеті повинна розташовувати до відвертої бесіди, сприяти встановленню психологічного контакту з допитуваним. Оскільки, шахрайства на сучасному етапі переважно вчиняються групами, важливо вірно визначити послідовність допиту підозрюваних. Першими рекомендується допитувати рядових членів групи, характеристика особи яких дозволяє припустити їхню схильність до дачі правдивих показань;

– створення необхідної обстановки для допиту. Обстановка, в якій проводиться допит, не повинна відволікати допитуваного, заважати йому зосередитися;

– вивчення обставини вчинення шахрайства з використанням ЕОТ та обставин, які підлягають встановленню під час допиту. Встановлюється, яке відношення має особа, яка буде допитуватися, до цього кримінального правопорушення. Необхідно з'ясовувати, які питання необхідно ставити підозрюваному щодо обставин вчинення кримінального правопорушення;

– вибір відповідних засобів і прийомів для вирішення конкретних завдань допиту. При цьому можливі два варіанти реалізації слідчим наявної в нього сукупності доказів. Перший – це пред'явлення доказів під час проведення декількох допитів, що послідовно змінюють один одного. Другий – всієї сукупності зібраних доказів на одному з допитів підозрюваного. Як правило, послідовне пред'явлення системи доказів на низці допитів здійснюється в тих випадках, коли підозрюваний вчинив декілька кримінальних правопорушень, що не дозволяє одночасно з'ясувати обставини протиправної діяльності під час проведення однієї слідчої дії; за відсутності можливості отримання окремих доказів у короткі терміни (наприклад, у зв'язку з міжрегіональним характером вчинення шахрайства);

– визначення кола учасників допиту, зокрема необхідність залучення спеціаліста та використання консультацій фахівців. У допиті бере участь захисник, у разі необхідності – перекладач, а також педагог, законні представники або родичі – якщо особа, яка допитується, неповнолітня;

– підготовка необхідних матеріалів, а також технічних засобів допиту. Вирішення питання, пов'язаного з використанням технічних засобів – звукозапису (відеозапису), що допоможе запобігти даванню неправдивих показань, зафіксувати психологічну реакцію допитуваного на несподівані запитання та пред'явлення доказів»[322].

Указані підготовчі заходи до проведення допиту повністю відповідають заходам до реалізації зазначеної процесуальної дії й під час розслідування кримінальних правопорушень у кіберпросторі.

[322] Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … д-ра філос. : 081 – Право / Нац. акад. внутр. справ, Київ, 2021. 255 с.

Найбільш важливим з-поміж них вважаємо з'ясування питань, що стосуються обставин справи, зокрема:

– виникнення злочинного задуму;

– відомості про об'єкт посягання, мотив злочину, ставлення особи до злочинних наслідків;

– способи підготовки та вчинення злочинів, послідовність злочинних дій, а також особливості приховування злочинної діяльності (її характер);

– час, місце, обстановка та механізм учинення злочинів;

– відомості про особу злочинця;

– умови, за яких допитуваний спостерігав будь-які предмети або явища; психологічний та фізичний стан особи в момент сприйняття чи після нього; загальна здібність допитуваного до певного сприйняття, запам'ятовування та відтворення;

– обставини, що сприяли або перешкоджали учиненню злочинів;

– способи формування організованої групи та характер злочинної діяльності;

– виявлення психологічної й функціональної структури групи (якісний склад, рівень організованості) та розподілу функціональних обов'язків;

– кількісний склад групи при учиненні кожного епізоду злочинної діяльності, конкретні дії кожного, навички володіння зброєю та прийомами боротьби; виявлення осіб, які не брали безпосередньої участі у вчинених злочинах, але обізнаних про їх підготовку, вчинення або приховання;

– наявність корумпованих зв'язків та зв'язків з іншими злочинними групами; способи протидії розслідуванню та впливу на потерпілих, свідків та членів групи, які дають правдиві показання;

– наявність у групі конфліктів, протиріч та розбіжностей;

– способи легалізації отриманих прибутків та відтворення злочинної діяльності;

– встановлення осіб, які залишилися на волі і продовжують злочинну діяльність або налагоджують зв'язки між членами групи та намагаються створити єдину, вигідну для усіх лінію поведінки та ін.[323].

З огляду на зазначене варто наголосити на тому, що для досягнення більшої ефективності слід заздалегідь скласти перелік питань, що підлягають з'ясуванню. Це дозволить уникнути проведення повторного допиту. У ході допиту потерпілого або свідка за умови повного усвідомлення нею того, що сталося, і бажання допомогти у встановленні істини використовуються такі тактичні прийоми, розроблені в криміналістиці: бесіда, відновлення в пам'яті забутого, уточнення і деталізація показань. Як правило, уповноважені особи при підготовці до допиту звертаються за допомогою до фахівців-криміналістів у галузі ІТ-безпеки, яких, на превеликий жаль, дуже бракує. Такі кримінальні

[323] Чаплинський К. О. Тактичне забезпечення проведення слідчих дій : монографія / Дніпропетровськ : Дніпропетр. держ. ун-т внутр. справ ; Ліра ЛТД, 2010. 560 с.

правопорушення, як правило, здійснюються за допомогою спеціальних програм, які маскують реальне місце знаходження особи шахрая так званих анонімайзерів таких як VPN (скорочена назва від англ. Virtual Privat Network – віртуальна приват мережа), Socks (скорочена назва від англ. Socked Secure – мережевий протокол) та ін. Здебільшого такі протиправні діяння вчиняються або ОГ, або ЗО[324].

Стосовно категорій свідків, то О. І. Мотлях вказує, що ними можуть бути «… як суб'єкти, які були допитані на початковому етапі розслідування злочину, так і суб'єкти, що раніше не фігурували у справі з тих чи інших причин. Особливої уваги слідчому необхідно приділити допиту осіб, які задіяні у виробничому процесі потерпілої сторони, але є свідками у справі – це програмісти, оператори, інженери-системники тощо. Враховуючи, що вказані суб'єкти при допиті можуть оперувати не зовсім зрозумілою слідчому специфічною термінологією, пропонується не лише використовувати допомогу фахівця у цій сфері, а й застосовувати фіксування процесу допиту науково-технічними засобами»[325].

На основі аналізу й узагальнення даних опитування респондентів (додаток А) нами встановлено ймовірні категорії свідків при розслідуванні кримінальних правопорушень у кіберпросторі, як-от:

– особи, яким може бути відома інформація про обставини та умови протиправної діяльності, яку вони спостерігали – 100 %;

– особи, які перебувають у родинному або іншому зв'язку з кіберзлочинцем – 56 %;

– особи, яким відомо умови та обставини тих дій, у яких вони брали участь (програмісти, інженери-системники) – 47 %;

– особи, які певним чином сприяли вчиненню протиправного діяння, але самі про це не знали (оператори ЕОМ, адміністратори комп'ютерної мережі) – 39 %;

– особи, які були обізнані про обставини, що передували вчиненню протиправних дій – 25%;

– працівники державних установ, які були задіяні у вчиненні кримінальних правопорушень у кіберпросторі (оператори ЕОМ, адміністратори комп'ютерної мережі) – 9 %.

[324] Коваленко І. О., Єфімов М. М. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів : монографія. Одеса : Юридика, 2025. 298 с.

[325] Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09 / Акад. праці і соц. відносин Федерації профспілок України. Київ, 2005. 198 с.

У розрізі зазначеного вважаємо за необхідне навести позицію А. І. Кунтія, який констатував, що «… під час допитів операторів ЕОМ варто з'ясувати: правила ведення журналів операторів, порядок прийому-здачі змін, режим роботи операторів; порядок ідентифікації операторів; правила експлуатації, збереження, знищення комп'ютерних роздруківок, категорію осіб, що мають до них доступ; порядок доступу в приміщення, де знаходиться комп'ютерна техніка. ... У процесі допитів програмістів з'ясовується: перелік використовуваного програмного забезпечення в установі, щодо якої було вчинено злочин, його класифікація (ліцензійне чи власного виробництва); паролі захисту програм, окремих пристроїв комп'ютера, частота їхніх змін; технічні характеристики комп'ютерної мережі (у разі її наявності), хто є адміністратором мережі … У співробітника, що відповідає за інформаційну безпеку, чи адміністратора комп'ютерної мережі (за їх наявності) з'ясовують: наявність спеціальних технічних засобів захисту інформації; порядок доступу користувачів у комп'ютерну мережу; порядок ідентифікації користувачів комп'ютерів... У співробітників, що займаються технічним обслуговуванням обчислювальної техніки, з'ясовують: перелік і технічні характеристики засобів комп'ютерної техніки, встановлених в організації, а також перелік захисних технічних засобів; періодичність технічного обслуговування, проведення профілактичних і ремонтних робіт; відомості про випадки виходу, що відбулися за останній час, апаратури з ладу; випадки незаконного підключення до телефонних ліній зв'язку, установка якого-небудь додаткового електроустаткування»[326].

Відносно допиту підозрюваного, то, приміром, О. Л. Мусієнко зазначала, що під час нього варто з'ясувати такі питання:

«– за яких обставин вчинено обман;

– які способи застосовувалися (конкретні прийоми, операції, дії з підготовки, заволодіння майном тощо);

– які ще злочини ним було вчинено;

– хто і з якого часу брав участь у злочинній діяльності, яка роль кожного учасника обманних дій;

– протягом якого періоду вчинявся злочин;

– яка загальна сума матеріальних цінностей або грошових коштів утворилася в результаті вчиненого шахрайства;

– який існував порядок розподілу грошових коштів у членів злочинного угрупування;

– як оформлялися конкретні первинні бухгалтерські документи, який порядок відвантаження матеріальних цінностей;

– чи є в них цінності, здобуті злочинним шляхом»[327].

Підтримуючи наведену позицію, спробуємо сформулювати перелік

[326] Криміналістика : підручник / за заг. ред. Є. В. Пряхіна. 3-тє вид., переробл. та допов. Львів : ЛьвДУВС, 2016. 948 с.

[327] Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / за ред. проф. В. Ю. Шепітька. Харків : Право, 2009. 168 с.

питань, притаманний досліджуваній категорії проваджень.

Отже, підозрюваному у вчиненні кримінальних правопорушень у кіберпросторі варто ставити такі категорії питань:

– за яких обставин вчинено протиправні дії;

– які способи використовувалися (застосовування ботів для спаму та потрапляння шкідливих програм до комп'ютерного забезпечення потерпілого; кардінг; обман потерпілого шляхом використання неправдивих відомостей при особистому чи телефонному (комп'ютерному) спілкуванні);

– які місця отримання неправомірного доступу та інтеграції до мережі (зсередини чи ззовні) та способи вчинення неправомірного підключення (злам програм захисту даних, маніпуляції з даними, командами та інформацією, використання спеціальних програм, технічних прийомів);

– які засоби використовувалися для вчинення протиправного діяння (технічні, зокрема, ЕОТ, смартфони, планшети, модеми, маршрутизатори; програмні, зокрема, VPN, браузери, графічні редактори, програми кодування інформації);

– яка загальна сума матеріальних цінностей або грошових коштів утворилася в результаті вчинення протиправних дій;

– який був порядок розподілу грошових коштів у членів ОГ чи ЗО;

– протягом якого періоду вчинялись протиправні діяння;

– які супутні кримінальні правопорушення було вчинено[328].

Крім того, варто вказати, що на основі аналізу й узагальнення матеріалів анкетування респондентів (додаток А) було визначено найбільш характерні позитивні моменти проведення допиту підозрюваного під час розслідування кримінальних правопорушень у кіберпросторі, зокрема:

– дозволяє отримати відомості про особу кіберзлочинця (95 %);

– дозволяє визначити послідовність проведення інших процесуальних дій (72 %);

– дозволяє вчасно висунути слідчі версії на початковому етапі розслідування (62 %);

– дозволяє з'ясувати дані, що мають тактичне значення (49 %);

– дозволяє отримати відомості про обставини протиправного діяння (41 %);

– дозволяє з'ясувати причини та умови, що сприяли вчиненню кримінальних правопорушень у кіберпросторі (29 %).

[328] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

Також на основі аналізу анкетування працівників правоохоронних органів (додаток А) було з'ясовано тактичні прийоми, які будуть найбільш доцільні під час допиту кіберзлочинця, як-от:

– встановлення психологічного контакту (100 %);

– постановка запитань (100 %);

– пред'явлення доказів (89 %);

– пред'явлення матеріалів кримінального провадження (83 %);

– спостереження за поведінкою допитуваного (кіберзлочинця) (69 %);

– актуалізація забутого у пам'яті допитуваного (59 %);

– залучення до допиту відповідного спеціаліста (48 %);

– використання техніко-криміналістичних засобів (43 %);

– викладення показань у формі вільної розповіді (42 %);

– демонстрація поінформованості слідчого або розповідь допитуваному про ймовірний розвиток злочинної події (19 %).

Констатуючи зазначене вище, зауважимо, що допит підозрюваного варто здійснювати одразу після його затримання. Адже вказана обставина дозволить отримати найбільш якісні показання стосовно факту вчинення кримінальних правопорушень у кіберпросторі.

3.2. Особливості реалізації негласних слідчих (розшукових) дій у кримінальному провадженні

Вчинення кримінальних правопорушень у кіберпросторі передбачає в переважній більшості випадків вельми педантичну підготовку кіберзлочинців до вчинення вказаних протиправних діянь З огляду на те, що більшість досліджуваних правопорушень мають «безконтактну» форму (тобто немає візуального контакту між кіберзлочинцем та потерпілою стороною), виникає потреба у проведенні ряду НСРД та ОТЗ. Указане пояснюється потребою детального негласного документування для ефективного доказування визначених діянь.

Для початку відмітимо, що, як зазначає В. В. Кікінчук, «… вимоги до засобів збирання доказів регламентуються кримінальним процесуальним законодавством. Водночас засоби доказування постійно викликають зацікавленість у фахівців з галузі криміналістичних знань, адже результативність діяльності зі збирання, перевірки й оцінки доказів напряму залежить від вибору правильної тактики застосування засобів доказування, використання сучасних техніко-криміналістичних засобів виявлення, фіксації, вилучення та дослідження доказової інформації, програмування досудового розслідування тощо. Тому цілком очевидно, що засоби доказування загалом і окремі їх різновиди

зокрема постійно стають об'єктами криміналістичних досліджень. Не є виключенням із цього правила і такі засоби доказування, як негласні слідчі (розшукові) дії»[329].

У свою чергу, А. А. Венедіктов зауважував, що «… формально-юридичний підхід дозволяє одночасно віднести оперативне впровадження (виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації) до різних категорій, що належать до окремих, хоча і взаємопов'язаних державно-правових діяльних систем – ОРД та кримінального процесу. Тому, залишаючись незмінним за своїм змістом, оперативне впровадження як засіб пізнавальної діяльності правоохоронних органів може мати дві різні юридичні форми залежно від сфери застосування. Це зумовлює потребу з'ясування взаємозв'язку та відособленості виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації як ОРЗ та як НСРД»[330].

Відповідно до пункту 1.5 Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, а також частини 1 статті 246 КПК України, негласні слідчі (розшукові) дії – це різновид слідчих (розшукових) дій, відомості про факт та методи проведення яких не підлягають розголошенню, за винятком випадків, передбачених Кримінальним процесуальним кодексом України[331][332]. Інакше кажучи, вони є специфічними методами збору доказової інформації.

Зі свого боку В. А. Колесник зауважує, що утаємниченими такі відомості мають бути не лише від осіб, стосовно яких проводяться ці негласні дії, а й від будь-яких інших осіб, зокрема й працівників органів досудового розслідування, оперативних підрозділів, посадових осіб правоохоронних та інших органів, пересічних громадян тощо, які не задіяні в підготовці й проведенні конкретних негласних слідчих (розшукових) дій, навіть якщо вони беруть участь в інших заходах із здійснення досудового розслідування у конкретному кримінальному провадженні. Автор зауважує, що саме негласність виступає тим

---

[329] Кікінчук В. В. Негласні слідчі (розшукові) дії як об'єкт криміналістичного дослідження. *Український політико-правовий дискурс*. 2024. URL: https://ppdnz.com.ua/index.php/home/article/view/99/49 (дата звернення: 14.09.2025).

[330] Венедіктов А. А. Виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації в оперативно-розшуковій діяльності та кримінальному процесі. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2 (33). С. 74–77.

[331] Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : затв. наказом ГПУ, МВС, СБУ, Адміністрації ДПрС, МФ, МЮ від 16.11.2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text (дата звернення: 15.09.2025).

[332] Кримінальний процесуальний Кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.09.2025).

чинником, який істотно впливає на визначення видів НСРД, отримання відповідних дозволів та встановлення порядку їх проведення, визначення основних виконавців і кола учасників, обрання способу фіксування перебігу й результатів проведення. Учений акцентує увагу на тому, що особливі процесуальні вимоги впливають і на розроблення специфічних тактичних прийомів і тактико-криміналістичних рекомендацій з проведення НСРД та використання їх результатів у доказуванні[333]. Як бачимо, необхідність максимально таємного проведення вказаних процесуальних дій викликає потребу в наявності відповідних наказів з грифом «Таємно» або «Цілком таємно».

Водночас глава 21 КПК України присвячена висвітленню повного списку можливих НСРД, а саме:

1) аудіо-, відеоконтроль особи (стаття 260);

2) накладення арешту на кореспонденцію (стаття 261);

3) огляд і виїмка кореспонденції (стаття 262);

4) зняття інформації з електронних комунікаційних мереж (стаття 263);

5) зняття інформації з електронних інформаційних систем (стаття 264);

6) обстеження публічно недоступних місць, житла чи іншого володіння особи (стаття 267);

7) встановлення місцезнаходження радіообладнання (радіоелектронного засобу) (стаття 268);

8) спостереження за особою, річчю або місцем (стаття 269);

9) аудіо-, відеоконтроль місця (стаття 270);

10) контроль за вчиненням злочину, формами якого є контрольована поставка, контрольована та оперативна закупка, спеціальний слідчий експеримент, імітування обстановки злочину (стаття 271);

11) виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (стаття 272);

12) негласне отримання зразків, необхідних для порівняльного дослідження (стаття 274)[334].

А вже в Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні передбачено такі НСРД:

1.11.2. Аудіо-, відеоконтроль особи;

1.11.3. Накладення арешту на кореспонденцію;

1.11.4. Огляд і виїмка кореспонденції;

1.11.5. Зняття інформації з транспортних телекомунікаційних мереж

[333] Колесник В. А. Суб'єкти здійснення та класифікація негласних слідчих (розшукових) дій. *Юридичний часопис Національної академії внутрішніх справ*. 2013. № 1. С. 129–134.

[334] Кримінальний процесуальний Кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.05.2025).

(який поділяється на: контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням відповідних технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв'язок, модемний зв'язок тощо), які передаються телефонним каналом зв'язку, що контролюється; зняття інформації з каналів зв'язку, що полягає в негласному одержанні, перетворенні і фіксації із застосуванням технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються);

1.11.6. Зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача;

1.11.7. Обстеження публічно недоступних місць, житла чи іншого володіння особи;

1.11.8. Спостереження за особою в публічно доступних місцях;

1.11.9. Аудіо-, відеоконтроль місця;

11.11.10. Негласне отримання зразків, необхідних для порівняльного дослідження;

1.11.11. Спостереження за річчю або місцем у публічно доступних місцях;

1.12.1. Контрольована поставка;

1.12.2. Контрольована закупка;

1.12.3. Оперативна закупка;

1.12.4. Спеціальний слідчий експеримент;

1.12.5. Імітування обстановки злочину;

1.13. Виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації;

1.14.1. Зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов'язаний з подоланням системи логічного захисту;

1.14.2. Установлення місцезнаходження радіоелектронного засобу[335].

Як доречно вказує В. В. Кікінчук, «… негласні слідчі (розшукові) дії – це засоби доказування в кримінальному провадженні, які проводяться:

– належним суб'єктом;

– з підстав і у порядку, визначених КПК України;

– з дотриманням прав і свобод людини;

– задля отримання фактичних даних про обставини, які підлягають доказуванню та мають значення для кримінального провадження достовірність

[335] Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : затв. наказом ГПУ, МВС, СБУ, Адміністрації ДПрС, МФ, МЮ № 114/1042/516/1199/936/1687/5 від 16.11.2012 р. URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text (дата звернення:15.09.2025).

чи недостовірність, можливість чи неможливість використання інших доказів.

Вказаним діям властиві такі ознаки:

– обмежувальний, винятковий і конфіденційний характер;

– сфера застосування (кримінальна процесуальна діяльність);

– регламентованість;

– спрямованість (по відношенню до підозрюваного й іншої особи в кримінальних провадженнях щодо кримінальних правопорушень, передбачених у ч. 2 ст. 246 КПК України);

– процесуальна форма фіксування»[336].

А вже М. А. Погорецький та Д. Б. Сергєєва констатували, що не підлягає розголошенню також і факт проведення НСРД. Автори зазначили, що постанова слідчого, прокурора про проведення НСРД, клопотання про дозвіл на проведення НСРД, ухвала слідчого судді про дозвіл на проведення НСРД та додатки до нього, протокол про проведення НСРД підлягають засекречуванню в порядку, встановленому законодавством[337].

Ми однозначно підтримуємо вказану позицію, оскільки зрозуміло, що такі умови максимально забезпечать ефективність проведення досліджуваних процесуальних дій.

У свою чергу, В. В. Кікінчук основними ознаками НСРД, які визначають їх сутність і роль у кримінальному провадженні, визначив такі, які: «… є різновидом процесуальних дій; є засобом доказування; чітко регламентовані кримінальним процесуальним законодавством; здійснюються уповноваженими суб'єктами шляхом використання негласних методів проведення; мають виключний характер; пов'язані з обмеженням прав і свобод людини. Підстави, умови та порядок проведення негласних слідчих (розшукових) дій і використання їх результатів повинні відповідати засадам кримінального провадження та міжнародним правовим стандартам, у тому числі доказування»[338].

Досить доречно А. Слободзян зауважує, що суб'єкти НСРД під час виконання завдань, визначених актами законодавства, виконують кримінально-процесуальні функції, які забезпечують: «… додержання конституційних прав та законних інтересів учасників досудового розслідування, інших осіб; швидке, повне та неупереджене розслідування злочинів; дотримання режиму секретності; захист особи, суспільства і держави шляхом встановлення істини, викриття винної особи, із застосуванням організаційних, практичних прийомів, у тому числі технічних засобів, що дають змогу в порядку, передбаченому

[336] Кікінчук В. В. Негласні слідчі (розшукові) дії як засоби доказування в кримінальному провадженні. *Аналітично-порівняльне правознавство*. 2025. Вип. № 1. С. 714–718. URL: http://journal-app.uzhnu.edu.ua/article/view/324002 (дата звернення: 14.09.2025).

[337] Погорецький М. А., Сергєєва Д. Б. Негласні слідчі (розшукові) дії та оперативно-розшукові заходи: поняття, сутність і співвідношення. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2 (33). С. 137–141.

[338] Кікінчук В. В. Негласні слідчі (розшукові) дії як об'єкт криміналістичного дослідження. *Український політико-правовий дискурс*. 2024. URL: https://ppdnz.com.ua/index.php/home/article/view/99/49 (дата звернення: 14.09.2025).

кримінальним процесуальним законодавством України, отримати інформацію про злочин або особу, яка його вчинила, без її відома»[339]. Ми повністю підтримуємо думку авторки, оскільки лише виконання вказаних функцій забезпечить ефективне виконання НСРД у провадженнях будь-якої категорії.

А вже С. В. Самойлов обґрунтував доцільність застосування такого способу отримання доказової інформації під час досудового розслідування, як витребування інформації від установ та організацій. Автор визначив, що його ефективність прямо залежить від того, наскільки слідчий тактично грамотно зробить відповідний запит, чому сприяє дотримання умов: а) своєчасності запиту; б) законності запиту; в) визначення вичерпного переліку інформації, яку необхідно з'ясувати шляхом запиту. Учений надав перелік адресантів та інформації, яку можливо таким чином отримати, а також запропоновано конкретну форму запиту[340].

Доречною вважаємо позицію О. П. Бабікова, який у власному монографічному дослідженні акцентував увагу на важливості проведення окремих НСРД, як-от:

– зняття інформації з транспортних телекомунікаційних мереж;

– зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача;

– обстеження публічно недоступних місць, житла чи іншого володіння особи;

– спостереження за річчю або місцем у публічно доступних місцях[341].

Досить цікавою є думка В. А. Колесника, який вказує, що запровадження НСРД, що здійснюються слідчим або уповноваженими оперативними підрозділами під час досудового розслідування, не скасовує права оперативно-розшукових підрозділів на здійснення у гласній та негласній формі оперативно-розшукової діяльності, вагома частка результатів якої має значення для встановлення фактичних обставин вчинення злочину і тому використовується в кримінальному провадженні. Автор наголошує на тому, що завдання й способи проведення багатьох НСРД зумовлюють потребу використання їх суб'єктами допомоги співробітників відповідних оперативних підрозділів і застосування спеціальних технічних засобів виявлення й фіксації інформації, що зазвичай використовуються в практиці роботи оперативно-розшукових підрозділів. Учений робить висновок, що порядок, режим, тактичні прийоми ви-

---

[339] Слободзян А. Нормативно-правове регулювання діяльності суб'єктів негласних слідчих (розшукових) дій. *Вісник Національної академії прокуратури України*. 2014. № 2 (35). С. 86–91.

[340] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : дис. … канд. юрид. наук : 12.00.09 / Дон. юрид. ін-т. Донецьк, 2014. 226 .

[341] Бабіков О. П. Теоретико-прикладні засади негласних слідчих (розшукових) дій: ґенеза та перспективи розвитку : монографія / Наук.-дослід. ін-т публічного права. Київ : Норма права, 2024. 446 с.

користання в доказуванні результатів НСРД та результатів негласних оперативно-розшукових заходів, навіть назви яких є іноді подібними, істотно відрізняються. Це зумовлено різною природою походження й різним порядком та суб'єктами отримання таких матеріалів[342].

Водночас окрема група авторів (Л. М. Грібов, С. М. Пугач) наголошують, що при проведенні НСРД у публічно доступних місцях дозволено вільно використовувати технічні засоби аудіо- і відеоконтролю, фотографування, відео- та звукозапису; технічні засоби встановлення місця знаходження конкретних матеріальних об'єктів; оптичні прилади, технічні засоби звязку, транспортні засоби. Вчені зауважують, що місцем проведення НСРД є місце знаходження осіб, що беруть у ній участь, і технічних засобів, що ними використовуються. Крім того, науковці роблять висновок, що уповноважені оперативні підрозділи, виконуючи доручення слідчого, прокурора, можуть використовувати наявні у них засоби, якщо вони відповідають вимогам цього Кодексу щодо засобів, які використовуються при проведенні НСРД[343].

Як бачимо, у деяких випадках можна проводити НСРД в місцях вільного доступу без обов'язкових процесуальних обмежень.

А вже Д. В. Безруков акцентує увагу на тому, що при розслідуванні злочинів проти власності найбільш використовуваними підрозділами карного розшуку оперативно-технічними засобами для негласного отримання інформації можуть бути такі категорії засобів:

– засоби контролю акустичної інформації;

– засоби контролю візуальної інформації;

– засоби контролю телекомунікаційних каналів та вилучення інформації;

– засоби виявлення об'єктів, які представляють оперативний інтерес;

– пристрої, що призначені для визначення місця розташування об'єктів[344].

Стосовно процесу документування, то ми підтримуємо позицію групи науковців (О. М. Джужа, Є. М. Моісеєв, Д. Й. Никифорчук), які розділили вказаний процес на дві групи: «1. Виявлення фактичних даних. 2. Забезпечення можливості їх використання при розслідуванні. Для першого елементу характерне отримання інформації та її перевірка. Автори вказують, що «виявлення фактичних даних – це сукупність оперативно-розшукових дій, які забез-

---

342 Колесник В. А. Негласні слідчі (розшукові) дії: кримінально-процесуальні та криміналістичні аспекти підготовки і проведення : наук.-практ. посіб. / Акад. адвокатури України. Київ : Прецедент, 2014. 135 с.

343 Грібов Л. М., Пугач С. М. Технічні засоби, що використовуються під час проведення негласних слідчих (розшукових) дій. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2 (33). С. 3–6.

344 Безруков Д. В. Використання оперативно-технічних засобів щодо протидії злочинам проти власності підрозділам карного розшуку : дис. ... канд. юрид. наук : 12.00.09 / Дон. юрид. ін-т МВС України. Кривий Ріг, 2015. 230 с.

печують отримання відомостей, що підтверджують злочинні діяння розроблюваних осіб. Це такі фактичні дані: про подію злочину (час, місце, спосіб); про причетність розроблюваного до підготовки або вчинення злочину; про обставини, які сприяли вчиненню злочину; коло осіб, причетних до його вчинення; місцезнаходження документів, предметів, цінностей, отриманих злочинним шляхом; обставини, що характеризують особу, пом'якшуючі, обтяжуючі обставини»[345].

Поряд із тим О. В. Пчеліна формулює такий перелік допустимих заходів гласного та негласного характеру при розслідуванні службових кримінальних правопорушень:

«– оперативна перевірка підозрюваного на причетність до вчинення інших злочинів, у тому числі у сфері службової діяльності;

– здійснення перевірки за інтегрованими ІПС Національної поліції України, єдиними та державними реєстрами, іншими пошуковими системами в електронних мережах загального користування з метою отримання довідково-аналітичної та оперативно-пошукової інформації, у тому числі про аналогічні нерозкриті злочини;

– отримання консультаційної допомоги від фахівців;

– вилучення документації, пов'язаної зі службовою діяльністю підозрюваного, шляхом проведення відповідних обшуків, тимчасового вилучення чи отримання тимчасового доступу до неї;

– огляд вилученої документації, аналіз її змісту та виявлення слідів імовірної фальсифікації;

– призначення технічних і почеркознавчих експертиз документів;

– проведення ревізій, зустрічних та інших перевірок;

– огляд приміщень, земельних ділянок, споруд, устаткування тощо;

– отримання зразків для експертизи, за необхідності негласне отримання зразків, необхідних для порівняльного дослідження;

– призначення судово-економічної, будівельно-технічних та інших судових експертиз;

– допит підозрюваного та свідків;

– здійснення аудіо-, відеоконтролю особи злочинця та місця;

– зняття інформації з транспортних телекомунікаційних мереж, отримання розшифрування телефонних розмов і проведення їх аналізу;

– зняття інформації з інформаційних систем»[346].

Як зазначає О. В. Курман, шахрайство з фінансовими ресурсами належить до таких кримінальних правопорушень, які в більшості випадків виявляються оперативним шляхом (86,4 %). Автор наголошує на тому, що плану-

[345] Оперативно-розшукова діяльність : навч. посіб. / За ред. проф. О. М. Джужі. Київ : Правова єдність, 2009. 310 с.

[346] Пчеліна О. В. Тактичні операції під час розслідування злочинів у сфері службової діяльності. *Підприємництво, господарство і право.* 2017. № 3. С. 290–294.

вання розслідування за справами, внесеними на основі оперативно-розшукових матеріалів, є специфічним. Одна із особливостей планування досудового розслідування за справами цієї категорії – забезпечення зашифровування шляхів одержання даних про осіб, які здійснили протиправне діяння, необхідність поєднання СРД з оперативно-розшуковими заходами в процесі всього розслідування, а також забезпечення можливості легалізації інформації, одержаної оперативним шляхом[347].

Зі свого боку, Д. А. Нескоромний акцентує увагу на тому, що «… провадження НСРД при розслідуванні кримінальних правопорушень, вчинених ОЗГ, крім отримання доказів, дозволяє отримати дані щодо конкретної організованої злочинної групи, здійснювати аналіз отриманої інформації щодо чисельності ОЗГ, її складу, структури, зв'язків між членами ОЗГ, їх пособниками, наявність у них корупційних звязків. НСРД являються ефективним способом отримання відомостей, речей і документів, які мають значення для досудового розслідування»[348]. Тобто для досліджуваної категорії кримінальних проваджень застосування вказаних процесуальних дій однозначно має велике значення.

Своєю чергою, А. Гетьман акцентує увагу на тому, що «… аудіоконтроль та відеоконтроль особи є негласними слідчими (розшуковими) діями, що пов'язані із втручанням у приватне спілкування цих осіб та обмежують їх конституційні права, задекларовані статтями 30, 32 Конституції України. Шляхом аудіо- та відеоконтролю особи може здійснюватися спостереження за діями та розмовами окремих осіб у житлі або іншому володінні особи або ж в інших приміщеннях, транспортних засобах, інших місцях, що не є житлом чи іншим володінням особи. Аудіоконтроль особи полягає у прослуховуванні та фіксації розмов, що відбуваються у зазначених об'єктах. Негласні слідчі (розшукові) дії із аудіоконтролю особи проводяться за допомогою спеціальних технічних засобів фіксації інформації. Порядок проведення таких негласних (розшукових) слідчих дій визначається відомчими нормативно-правовими актами. Аудіоконтроль особи може проводитись як безпосередньо слідчим, що розслідує злочин, а також за його дорученням уповноваженими оперативними підрозділами (ст. 41, ч. 6 ст. 246 КПК). Аудіоконтроль особи може здійснюватися епізодично (на час відвідування цією особою певних місць, проведення зустрічей) або безперервно, на проміжок часу, визначений у рішенні слідчого судді, що надав дозвіл на його проведення (ст. 249 КПК). Безперервний аудіоконтроль з фіксацією та обробкою отриманої за ним інформації здійснюється, як

[347] Курман О. В. Способи несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство.* 2017. № 4. С. 245–249.

[348] Нескоромний Д. А. Проведення негласних слідчих (розшукових) дій працівниками СБ України при розслідуванні кримінальних правопорушень, вчинених організованими злочинними групами. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2 (33). С. 20–23.

правило, цілодобово. Організація та проведення такої негласної слідчої (розшукової) дії переважним чином може відбуватися за участі спеціальних підрозділів уповноважених законом органів, що мають право ведення оперативно-розшукової діяльності. Спеціально підготовлені фахівці оперативно-розшукових органів забезпечують впровадження спеціальних технічних засобів та процес фіксації й обробки отриманої інформації. Аудіоконтроль особи також може проводитись без участі оперативних підрозділів, за умови, якщо технічна фіксація результатів негласної слідчої (розшукової) дії забезпечується безпосередньо слідчим»[349]. Як бачимо, усе перераховане підходить до процесу розслідування шахрайства у кібепросторі.

А вже В. Д. Безруков розділяє НСРД за характером дії суб'єктів кримінального провадження стосовно отримання даних з телекомунікаційних мереж, а саме: «… 1) зняття інформації з транспортних телекомунікаційних мереж (НСРД, передбачена ст. 263 КПК України), що в свою чергу поділяється на: конспіративне перехоплення, контроль телефонних розмов та фіксацію їх змісту з використанням технічних засобів негласного отримання інформації; перехоплення електронних сигналів та повідомлень з використанням технічних засобів негласного отримання інформації; 2) установлення місцезнаходження радіоелектронного засобу шляхом: пеленгування місцезнаходження кінцевого обладнання мереж телекомунікацій оперативно-технічними підрозділами при виконанні доручень у порядку ст. 40 КПК України – як НСРД «установлення місцезнаходження радіоелектронного засобу», передбачена ст. 268 КПК України; затребування компетентними органами розслідування інформації про взаємоз'єднання телекомунікаційних мереж з метою отримання та вибірки відомостей про надані телекомунікаційні послуги – як процесуальна дія, передбачена ст. 93 КПК України»[350].

Доречною є позиція групи науковців (С. С. Кудінов, Р. М. Шехавцов, О. М. Дроздов, С. О. Гриценко), які акцентують увагу на тому, що підставами, достатніми для втручання у приватне спілкування, є: «… фактичні дані, отримані у передбаченому КПК порядку, що розмови особи або інші звуки, рухи, дії, пов'язані з її діяльністю або місцем перебування, поштово-телеграфна кореспонденція певної особи іншим особам або інших осіб, певна електронна інформаційна система можуть містити відомості про обставини, які мають значення для досудового розслідування, або речі і документи, що мають істотне значення для досудового розслідування; можливість отримання відомостей

[349] Гетьман А. Науково-практичний коментар нового Кримінального процесуального кодексу України від 13 квітня 2012 року. URL: http://yport.inf.ua/stattya-audio-videokontrol-50500.html (дата звернення: 14.09.2025).

[350] Безруков Д. В. Використання оперативно-технічних засобів щодо протидії злочинам проти власності підрозділам карного розшуку : дис. ... канд. юрид. наук : 12.00.09 / Дон. юрид. ін-т МВС України. Кривий Ріг, 2015. 230 с.

про зміст приватного спілкування тільки шляхом проведення НСРД, що включають втручання у приватне спілкування»[351].

У розрізі сказаного зазначимо, що при розслідуванні кримінальних правопорушень у кіберпросторі обов'язково повинна бути наявна можливість для втручання у приватне спілкування кіберзлочинців.

Стосовно відеоконтролю особи, то А. Гетьман слушно вказує, що він «… здійснюється технічними засобами, що забезпечують негласне візуальне спостереження за діями, розмовами, поведінкою підозрюваного, обвинуваченого та осіб, що контактують з ними у зв'язку з їх протиправною діяльністю. Відеоконтроль особи забезпечує не лише негласне спостереження за діями окремих осіб, але й відеозапис та аудіофіксацію інформації, що вказує на ознаки вчинення протиправних діянь. Відеоконтроль обстановки та дії осіб, їх фіксація може здійснюватися в житлі або іншому володінні особи, а також у приміщеннях, транспортних засобах та інших місцях, які не відносяться до житла та не є іншим володінням особи. Відеоконтроль особи, як правило, здійснюється за участю спеціальних підрозділів, що забезпечують впровадження та експлуатацію спеціальних технічних засобів. Проведення цього заходу дозволяє виявляти та фіксувати інформацію, що свідчить про підготовку або вчинення окремими особами тяжких та особливо тяжких злочинів; з'ясовувати місця зберігання предметів, документів, а також інших матеріалів, що становлять інтерес для органів досудового розслідування. Відеозапис дозволяє більш детально вивчити дії контрольованих осіб, одержувати зображення предметів, що знаходяться у контрольованому об'єкті, – тобто отримувати максимально об'єктивну інформацію, що стосується протиправної діяльності підозрюваного або обвинуваченого у вчиненні кримінального правопорушення»[352].

О. В. Керевич зі свого боку зауважує, що при реалізації НСРД уповноважені оперативні підрозділи не мають права виходити за межі доручень слідчого, прокурора. Автор наголошує на тому, що «… вони зобов'язані повідомляти їх про виявлення обставин, які мають значення для кримінального провадження або вимагають нових процесуальних рішень слідчого, прокурора. Далі ситуація відбувається у доволі забюрократизованій формі. Так, відповідно до Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні отриману інформацію в ході проведення встановлення місцезнаходження радіоелектронного пристрою та (або) спостереження за особою річчю або місцем, оперативні підрозділи, які залучалися, передають підрозділам ініціаторам для складання про-

[351] Кудінов С. С., Шехавцов Р. М., Дроздов О. М., Гриценко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшукової діяльності у кримінальному провадженні : навч.-практ. посіб. Харків : Оберіг, 2013. 344 с.

[352] Гетьман А. Науково-практичний коментар нового Кримінального процесуального кодексу України від 13 квітня 2012 року. URL: http://yport.inf.ua/stattya-audio-videokontrol-50500.html (дата звернення: 14.09.2025).

токолу. Далі, після складання, протокол і додатки до нього, не пізніше 24 годин після складання, надаються прокурору, зазначеному в дорученні. Після чого прокурор, за необхідності, може ознайомити слідчого, який здійснює розслідування даного кримінального провадження з протоколом і відповідними додатками. Потім відбувається процес розсекречення протоколу й додатків проведення відповідних НСРД та додавання їх до матеріалів кримінального провадження»[353].

На основі аналізу й узагальнення даних анкетування респондентів (додаток А), встановлено, що специфічною ознакою кримінальних правопорушень у кіберпросторі є необхідність проведення цілого ряду НСРД та ОТЗ, пов'язаних із встановленням кіберзлочинця та його зв'язків. Зокрема, дослідження матеріалів судово-слідчої практики (додаток Б) дозволило серед них виокремити такі:

– аудіо-, відеоконтроль особи;

– зняття інформації з електронних комунікаційних мереж;

– зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача;

– спостереження за особою в публічно доступних місцях; аудіо-, відеоконтроль місця.

На основі опрацювання результатів матеріалів анкетування працівників правоохоронних органів (додаток А) нами було виявлено такі труднощі, що виходять зі здійснення зазначених НСРД при розслідуванні кримінальних правопорушень у кіберпросторі, зокрема:

– незлагоджена взаємодія підрозділів правоохоронних органів та працівників установ зв'язку (71 %);

– проблематичність отримання ухвали слідчого судді апеляційного суду стосовно проведення певної НСРД (59 %);

– дефіцит потреби в огляді та вилученні документів (52 %);

– небажання окремих уповноважених осіб поліпшувати процес кримінального провадження, а також пошук більш легких шляхів для отримання доказових даних (39 %).

Наостанок наведемо позицію О. П. Бабікова, який зауважував, що «… питання використання результатів НС(Р)Д з іншою метою (в іншому провадженні, іншому судочинстві) в законодавстві України залишається недостатньо врегульованим і не передбачає достатніх гарантій, що унеможливлюють

[353] Керевич О. В. Особливості проведення окремих невідкладних негласних слідчих (розшукових) дій. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2 (33). С. 101–105.

використання такої інформації, що стосується приватного життя людини з іншою метою ніж та, що зазначалася у клопотаннях перед слідчим суддею, та задля досягнення якої слідчим суддею надано такий дозвіл. Вдосконалення кримінального процесуального законодавства може здійснюватися шляхом запровадження механізму контролю за зберіганням, використанням та знищенням інформації, одержаної під час проведення негласних заходів, якщо вона не підлягає використанню в інтересах кримінального судочинства, розробленням та запровадженням чітких критеріїв можливості використання інформації, одержаної внаслідок проведення негласних заходів»[354].

З цього приводу Д. Б. Сергєєва зауважила, що вони розглядаються лише як матеріально фіксовані джерела, що виникають у процесі проведення негласних слідчих (розшукових) дій та містять певну інформацію, відомості, тобто у вузькому значенні цього терміна. Авторка вказує на те, що результати НСРД для їх подальшого використання, у тому числі й у кримінальному процесуальному доказуванні, мають бути трансформовані в передбачену матеріальну форму – відповідні матеріали НСРД. Учена робить висновок, що сама лише змістовна складова результатів їх проведення – інформація, що отримується в результаті їх проведення, не дозволяє її використовувати в інтересах кримінального судочинства[355].

На основі аналізу матеріалів анкетування працівників правоохоронних органів (додаток А) встановлено чинники, які сприяють успішному проведенню НСРД при розслідуванні кримінальних правопорушень у кіберпросторі, зокрема:

– всебічна та ретельна підготовка (100 %);

– своєчасність у прийнятті рішення (94 %);

– використання спеціальних знань, у тому числі інших осіб (71 %);

– правильне застосування тактичних прийомів та їхніх комплексів (69 %);

– залучення відповідних спеціалістів (68 %);

– інше (43 %).

Підбиваючи підсумки, варто зауважити, що здійснення НСРД згідно з процесуальним порядком, передбаченим чинним кримінальним процесуальним законодавством та відомчими інструкціями, є необхідним чинником того, щоб результати їх реалізації суд убачав допустимими.

[354] Бабіков О. П. Використання результатів негласних слідчих (розшукових) дій з іншою метою, – межі допустимого. *Часопис Київського університету інтелектуальної власності та права*. 2024. Вип. 5. С. 3–8.

[355] Сергєєва Д. Б. Результати негласних слідчих (розшукових) дій: проблемні аспекти визначення. *Право і громадянське суспільство*. 2014. № 1. С. 97–106.

3.3. Теоретико-праксеологічні засади використання спеціальних знань під час розслідування кримінальних правопорушень у кіберпросторі

Одним із надзвичайно важливих засобів отримання доказової інформації в кримінальних провадженнях, розпочатих за фактом вчинення кримінальних правопорушень у кіберпросторі, є використання спеціальних знань. Процес розслідування протиправних діянь вимагає від працівників правоохоронних органів застосовування максимального набору можливих засобів і методів. Одним із найбільш розповсюджених засобів, що застосовується в будь-якому кримінальному провадженні, є використання спеціальних знань. Цей аспект має свої характеристики як стосовно суб'єкта його можливого використання, так і щодо його форм. Крім того, у науковій літературі донині йде полеміка з приводу інформаційного наповнення терміна «спеціальні знання»[356].

З цього приводу С. В. Чучко слушно вказував, що «… процес розслідування кримінальних правопорушень може характеризуватися проведенням різноманітних процесуальних дій. Деякі з них направлені на вилучення та перевірку певної доказової інформації. Під час їх проведення в уповноважених осіб (слідчого, дізнавача, прокурора) може виникнути потреба у з'ясуванні окремих обставин, які викликають необхідність у наявності спеціальних знань. Так, вчинення шахрайства при купівлі-продажу товарів через мережу Інтернет в Україні характеризується багатьма аспектами, які вимагають володіння вказаними знаннями. Іноді без них взагалі неможливо довести вину шахрая. Адже специфічні спосіб і умови вчинення кримінального правопорушення (мережа Інтернет), характерна слідова картина для даної категорії проваджень (ідеальні та віртуальні докази) зумовлюють необхідність залучення фахівців із різних галузей науки для максимально ефективного вилучення доказової інформації»[357].

У розрізі визначеного вбачаємо досить правилльною позицію Г. С. Бідняк, яка наголошувала на тому, що «… поняття спеціальних знань не закріплено в жодному нормативно-правовому акті та вирізняє наступні їх ознаки:

– є комплексом знань і навичок у різних галузях;

– складаються з системи відомостей в галузі науки, техніки та інших сфер людської діяльності;

– використовуються в досудовому розслідуванні та судовому провадженні у випадках і в порядку, визначених кримінальним процесуальним законодавством;

---

[356] Єфімов М. М. Використання спеціальних знань під час розслідування злочинів проти моральності. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. № 2. С. 268–274.

[357] Чучко С. В. Використання спеціальних знань при розслідуванні шахрайств при купівлі-продажу товарів через мережу Інтернет. *Право і суспільство*. 2021. № 2. С. 234–240.

– їх використання здійснюється у взаємозв'язку з науково-технічними засобами;

– реалізуються визначеним суб'єктом кримінального судочинства у процесі практичної діяльності, спеціальної підготовки з урахуванням професійного досвіду і засновані на системі теоретичних знань у відповідній галузі;

– їх реалізація вимагає значних витрат часу й інтелектуальних зусиль;

– сприяють у розробці технічних засобів і прийомів роботи з доказами та встановленню вагомих обставин, що мають значення для доказування»[358].

Водночас Ю. М. Чорноус констатувала, для успішної реалізації діяльності з розслідування злочинів важливо вирішити ряд питань, що входять до сфери техніко-криміналістичного забезпечення та пов'язані із застосуванням технічних засобів при проведенні процесуальних, слідчих (розшукових), негласних слідчих (розшукових) дій, а також процесуальних дій, що проводяться у межах міжнародної правової допомоги й інших форм міжнародного співробітництва у кримінальному провадженні; оцінки та використання фактичних даних, отриманих за допомогою використання спеціальних засобів і технічних засобів у кримінальному провадженні, та ін.[359].

А вже Л. Ш. Мамедова зазначала, що під час розслідування кіберзлочинів «… необхідно більше уваги приділити дослідженню так званої цифрової криміналістики (digital forensics), оскільки знання специфіки роботи цифрових криміналістичних засобів і вміння використовувати всі їхні властивості є найважливішою умовою якісного вирішення криміналістичних завдань, що стоять перед спеціалістом, фахівцем (експертом) під час розслідування кіберзлочинів. Крім того, з метою ефективного розслідування та розкриття зазначеної категорії злочинів доцільно приділити увагу підвищенню кваліфікації експертів і спеціалістів, створити передумови для впровадження єдиної системи підготовки та підвищення кваліфікації кадрів, які залучаються до протидії кіберзлочинності. Важливо, ураховуючи специфіку проведення судової експертизи, зокрема цифрових криміналістичних експертиз, створити умови для їхнього розвитку та розробити єдині методи проведення судових експертиз під час розслідування зазначеної категорії злочинів шляхом удосконалення науково-методичних рекомендацій відповідно до міжнародних стандартів. Для вирішення цих питань потребує ретельного дослідження визначення таких понять, як «спеціаліст», «фахівець» та «експерт», а надалі – досягнення узгодженості їх-

[358] Бідняк Г. С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств : монографія. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2019. 152 с.

[359] Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів : монографія. Вінниця : Нілан-ЛТД, 2017. 492 с.

нього правового статусу у чинному законодавстві зарубіжних країн та України»[360].

С. Перлін вказував, що термінологія криміналістичного забезпечення застосовується не тільки в аспекті кримінального провадження, а і щодо інших сфер діяльності. Це пов'язано з тією обставиною, що техніко-криміналістичні засоби (як спеціально розроблені, так і пристосовані для потреб криміналістики) усе ширше впроваджуються не тільки у кримінальну процесуальну, а й в іншу правозастосовну діяльність і в повсякденне життя. Як приклад, можна навести використання в сучасних телекомунікаційних засобах і системах захисту приміщень сканерів відбитків пальців, застосування поліграфа під час прийому на роботу, використання різноманітної техніки (у тому числі і криміналістичної) під час підприємницької діяльності тощо. Проте одним із перших та основних напрямів техніко-криміналістичного забезпечення все ж була та залишається правозастосовна діяльність. Автор зауважує, що саме вона передбачає наявність техніко-криміналістичного забезпечення у будь-якій з її сфер [361].

Стосовно визначення спеціальних знань, ми підтримуємо позицію В. М. Реваки, який їх сформулював як «… сукупність будь-яких пізнань на сучасному етапі їхнього розвитку в галузі науки, техніки, мистецтва, ремесла, отриманих у результаті професійної підготовки та фахової освіти, за винятком професійних правових пізнань суб'єкта доказування (органу дізнання, слідчого, прокурора, суду), використовуваних з метою виявлення та розслідування злочинів у порядку, передбаченому кримінально-процесуальним законом»[362].

Підбиваючи підсумок, зазначимо, що спеціальні знання – це сукупність теоретичних знань, практичних умінь і навичок у галузі науки, техніки, мистецтва, ремесла, отриманих у результаті професійної підготовки та фахової освіти, що використовуються з метою попередження та розслідування кримінальних правопорушень[363].

Щодо форм використання спеціальних знань, то, наприклад, Д. В. Паш-

---

[360] Мамедова Л. Ш. Особливості використання спеціальних знань під час розслідування кіберзлочинів: міжнародний досвід. *Юридичний науковий електронний журнал.* 2021. № 1. С. 392–395. URL: http://www.lsej.org.ua/12_2021/100.pdf (дата звернення: 12.09.2025).

[361] Перлін С. Поняття і види техніко-криміналістичного забезпечення правозастосовної діяльності. *Підприємство, господарство і право*. 2020. № 1. С. 221–226.

[362] Ревака В. М. Форми використання спеціальних пізнань в досудовому провадженні : дис. ... канд. юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2006. 206 с.

[363] Єфімов М. М. Проблемні аспекти формулювання визначення спеціальних знань при розслідуванні кримінальних правопорушень. *Забезпечення правопорядку та протидії злочинності в Україні та у світі : проблеми та шляхи їх вирішення :* матеріали ІІІ Міжнарод. наук.-практ. конф. (м. Дніпро, 16 черв. 2023 р.). Дніпро : Дніпр. гуманітар. ун-т, 2023. С. 91–94.

нєв відмічав, що вони «… можуть бути диференційовані на обов'язкове та факультативне залучення їх при проведенні процесуальних дій. Процесуальні форми використання спеціальних знань поділяються за характером дій, при проведенні яких вони застосовуються, на ті, що використовуються при проведенні слідчих (розшукових) та інших процесуальних дій. Непроцесуальні форми застосування спеціальних знань можуть бути розділені за ознаками сфери використання і суб'єкта їх застосування»[364].

Г. С. Бідняк зазначає, що «… для сучасних шахраїв характерним є використання як традиційних прийомів, пристосованих до нових соціальних умов, так і нових, раніше невідомих. Так, залежно від способу вчинення шахрайства доцільними є такі форми використання спеціальних знань:

– призначення судових експертиз;

– довідково-консультаційна діяльність;

– ревізії та перевірка за обліками;

– залучення спеціаліста при проведенні слідчих (розшукових) дій;

– допит експерта;

– присутність слідчого при проведенні експертизи»[365].

З огляду на сказане ми повністю поділяємо думку С. В. Чучка, який зазначив, що «… у працівників правоохоронних органів, які уповноважені розслідувати шахрайства при купівлі-продажу товарів через мережу Інтернет, є можливість використання різних форм спеціальних знань. Серед основних форм використання спеціальних знань ми вирішили виокремити наступні:

– безпосереднє використання уповноваженою особою спеціальних знань під час проведення окремих слідчих (розшукових), негласних слідчих (розшукових) та інших процесуальних дій;

– призначення судових експертиз;

– залучення спеціаліста до проведення окремих процесуальних дій»[366].

Для вчинення кримінальних правопорушень досліджуваної категорії шахраї активно використовують здобутки новітніх технологій, які зумовлюють утворення відповідних слідів (електронних). А. Ф. Волобуєв, В. О. Малярова, Р. Л. Степанюк до засобів учинення шахрайства залучають такі, як: «… мережу та засоби стільникового зв'язку, глобальну світову телекомунікаційну мережу Інтернет, засоби комп'ютерної техніки, зокрема спеціальне програмне забезпечення, програми-віруси, програми-шкідники, периферійне обладнання

[364] Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09 / Нац. акад. внутр. справ. Київ, 2007. 228 с.

[365] Бідняк Г. С. Висновок експерта як джерело доказів під час розслідування шахрайства. *Криміналістичний вісник*. 2014. № 2 (22). С. 55–59.

[366] Чучко С. В. Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2021. 276 с.

(принтер, CD-ROM-накопичувач, стример), а також носії комп'ютерної інформації («флешки», диски) та засоби телефонного зв'язку. Окрім того, для вчинення шахрайств за допомогою пластикових кредитних карток злочинці можуть користуватися, відповідно, банкоматами, спеціально виготовленими пристроями для зчитування інформації з чужих карток, електронними терміналами, імпрінтерами та декодерами. Усі ці об'єкти можуть бути носіями тієї чи іншої інформації, яка має значення у кримінальному провадженні»[367].

Т. В. Коршикова акцентує увагу на тому, що «… у місцях, де вчиняються такі види шахрайств, є ЕОТ, тому потреба в допомозі спеціаліста-консультанта якими, як правило, виступають експерти комп'ютерно-технічного відділу Експертної служби МВС України, виникає на початковому етапі досудового розслідування, коли слідчому необхідно оглянути ЕОТ, насамперед, яка знаходиться в робочому (увімкненому) стані. У цьому випадку спеціаліст повинен надати допомогу: в огляді ЕОМ на стадії її виявлення, у т.ч. встановити в ЕОТ наявність зовнішніх пристроїв віддаленого доступу до системи (підключення до локальної мережі, наявність модему тощо); фіксування усіх дій з ЕОТ за допомогою фото- та відеотехніки; здійснення опису екрану та прилеглої обстановки; копіювання наявної в ЕОТ інформації; вжиття заходів щодо встановлення пароля доступу до захищених програм; належного та безпечного вимикання ЕОТ; вилучення, упакування та опечатування ЕОТ, інших носіїв інформації (накопичувачі на жорстких і гнучких магнітних дисках, компакт-диски, DVD-диски, ZIP-дискети тощо) та інших предметів і документів для їх дослідження в лабораторних умовах; способів транспортування (перевезення) вилучених предметів»[368].

С. С. Чернявський виділив такі форми використання спеціальних знань: «… участь спеціалістів при проведенні попередньої перевірки інформації про злочин; консультації фахівців при підготовці та проведенні слідчих дій; призначення і проведення документальних ревізій та інших перевірок; призначення судових експертиз. У 91,0 % справ допомога спеціаліста використовувалась у різних формах: фахівці залучалися до проведення слідчих дій (14,2 %); давали поради та консультації (78,8 %); були допитані стосовно обставин, пов'язаних з їх професійною діяльністю (17,3 %)»[369].

---

[367] Криміналістика : підручник : у 2 т. Т. 2 / А. Ф. Волобуєв, О. В. Одерій, Р. Л. Степанюк та ін. ; за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. 312 с.

[368] Коршикова Т. В. Форми використання спеціальних знань при розслідуванні шахрайства, вчиненого із використанням мережі Інтернет. *Актуальні проблеми кримінального права* : тези доп. XI Всеукр. наук.-теорет. конф., присвяч. пам'яті проф. П. П. Михайленка (м. Київ, 20 листоп. 2020 р.) / ред. кол. : В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ : Нац. акад. внутр. справ, 2020. С. 296–298.

[369] Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : автореф. дис. … д-ра юрид. наук : 12.00.09 / Нац. акад. внутр. справ. Київ, 2010. 36 с.

На основі опрацювання матеріалів анкетування респондентів (додаток А) визначено такі форми використання спеціальних знань при розслідуванні кримінальних правопорушень у кіберпросторі:

– призначення експертиз (100 %);
– участь спеціаліста у проведенні СРД, НСРД (61 %);
– інше (29 %);
– консультативно-довідкова допомога (22 %).

Підтримуємо думку О. О. Волобуєвої, яка наголошувала, що «… першорядною, найбільш важливою та складною формою використання спеціальних знань є участь спеціаліста у проведенні СРД. Це пояснюється тим, що в цьому випадку діяльність спеціаліста спрямовано на пошук (сприяння в пошуку) речових доказів (слідів, предметів і об'єктів) – джерел інформації про скоєний злочин, наявність яких є базисом у відтворенні слідчим обставин злочинної події та побудові алгоритму дій, спрямованих на розкриття та розслідування злочину. Крім того, саме від результативності слідчої дії залежить необхідність реалізації інформаційно-доказового потенціалу виявлених речових доказів за допомогою проведення експертних досліджень»[370].

Стосовно участі спеціаліста, то на основі вивчення матеріалів кримінальних проваджень (додаток Б) було з'ясовано, що він був залучений до реалізації таких процесуальних дій:

– зняття інформації з електронних комунікаційних мереж та електронних систем (100 %);
– огляд ЕОТ (100 %);
– огляд місця події (100 %);
– обшук (82 %);
– тимчасовий доступ до речей та документів (65 %);
– допит (43 %).
.

Т. В. Коршикова до предмета консультацій зі спеціалістом у галузі комп'ютерних технологій відносить такі обставини:

– визначення способу та механізму використання ЕОТ під час вчинення шахрайства;

– з'ясування ступеня належності того чи іншого предмета, який належить до ЕОТ, у механізмі вчинення шахрайства;

– способи використання ЕОТ у механізмі вчинення шахрайства;

– порядок збереження вилучених ЕОТ;

[370] Волобуєва О. О. Взаємодія слідчого з фахівцями під час збору інформації про особу, що скоїла злочин : дис. ... канд. юрид. наук : 12.00.09 / Київ. нац. ун-т внутр. справ. Київ, 2006. 236 с.

– можливість використання певного виду технічних засобів для вчинення шахрайства[371].

Також можливими вбачаються такі варіанти допомоги спеціаліста при проведенні огляду місця події та обшуку:

– визначення меж території, яка підлягає огляду;

– установлення способу огляду місць найбільш імовірного відступу злочинця. Перелік об'єктів пошуку залежить від характеру вчиненого злочину. Тому спеціаліст при проведенні оглядів (обшуків) звертає увагу слідчого на об'єкти, які можуть мати значення для розслідування кримінального провадження;

– вибір і використання технічних засобів відповідно до об'єкта огляду;

– проведення пошукових дій з метою виявлення слідів, у тому числі й мікрооб'єктів (наприклад, у кишенях одежі підозрюваного);

– проведення необхідних найпростіших геометричних, вагових та інших вимірювань (наприклад, установлення розміру об'єктів, зважування знайдених об'єктів та ін.);

– проведення попередніх досліджень слідів;

– орієнтувальна інформація, отримана у результаті попередніх досліджень: полегшує та прискорює проведення наступних судових експертиз; має важливе значення для термінового проведення оперативно-розшукових заходів і слідчих (розшукових) дій; є підставою для моделювання події злочину, висування версій та ін.;

– фіксація об'єктів і слідів, що вилучаються, шляхом ретельного опису у протоколі слідчої дії та фото- й відеозйомки;

– вилучення й упакування виявлених об'єктів;

– роз'яснення щодо виявлених об'єктів або слідів;

– надання консультацій щодо подальшого експертного дослідження вилучених об'єктів[372].

В. В. Сисолятін запропонував застосовування спеціальних знань у формі залучення спеціаліста відповідного профілю за його безпосередньої участі у процесуальних діях, як-от: «… 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

[371] Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … д-ра філос. : 081 – Право / Нац. акад. внутр. справ. Київ, 2021. 255 с.

[372] Огляд місця події : виявлення та вилучення об'єктів біологічного походження : методичні рекомендації. Міністерство внутрішніх справ України, Державний науково-дослідний експертно-криміналістичний центр / авт.-упоряд. : С. І. Перлін, С. О. Шевцов, Н. М. Косміна, В. В. Іонова. Харків : ФОП Чальцев О. В. 2009. 100 с.

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»[373].

Як слушно вказує І. В. Пиріг, «…. у деяких випадках спеціаліста доцільно запросити на допит. Спеціаліст, залучений до проведення слідчої (розшукової) дії, володіє необхідними спеціальними знаннями та, користуючись ними, допомагає слідчому»[374].

З метою визначення особливостей призначення експертиз як обов'язкових слідчих (розшукових) дій при розслідуванні шахрайства у сфері використання банківських електронних платежів, а також дослідження окремих заходів щодо її підготовки, розглянемо низку думок вчених, які досліджували проблематику цього питання.

З приводу експертиз, які необхідно проводити під час розслідування кримінальних правопорушень у кіберпросторі, існують різні думки. Для прикладу, Т. В. Охрімчук акцентувала увагу на тому, що особливу увагу слід звернути на проведення судових експертиз. Авторка вказану позицію аргументувала тим, що під час розслідування шахрайства з фінансовими ресурсами виникає потреба у проведенні судово-економічної, судово-бухгалтерської експертизи та судової фінансово-кредитної експертизи. Крім того, вчена зазначала, що може виникнути потреба у проведенні криміналістичних експертиз: технічної експертизи документів, почеркознавчої, авторознавчої тощо[375].

З приводу об'єктів експертного дослідження, то А. В. Реуцький наводив серед них такі, як:

– документи – сліпи, платіжні картки, гроші, цінні папери тощо;

– комп'ютерна техніка, у тому числі банкомати, POS-термінали, енкодери, автоматизовані торговельні термінали, ноутбуки, комунікатори, електронні записні книжки й перекладачі;

– різні типи друкувальних пристроїв – принтери, термопринтери, ембосери, імпринтери; різноманітні машинні носії інформації – дискети, диски, магнітні стрічки (мікрочипи) платіжних карток тощо;

– комп'ютерна інформація – програми, файли та ін.;

– речові докази – цифрові засоби електрозв'язку, пристрої радіозв'язку,

---

[373] 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.

[374] Пиріг І. В. Теоретико-прикладні проблеми експертного забезпечення досудового розслідування : монографія. Дніпропетровськ : Дніпропетр. держ. ун-т внутр. справ ; Ліра ЛТД, 2015. 432 с.

[375] Охрімчук Т. В. Особливості використання спеціальних знань при розслідуванні шахрайства з фінансовими ресурсами. *Фінанси, економіка, право*. 2010. № 8. С. 59–63.

сліди та їхні копії, зразки, приєднані до кримінального провадження тощо[376].

Зі свого боку, Т. В. Коршикова на основі вивчення результатів кримінальних проваджень щодо шахрайств, які вчиняються з використанням ЕОТ, визначила «… наступні види експертизи, які призначались при їх розслідуванні, зокрема щодо вилучених: електронно-обчислювальна техніка (комп'ютерно-технічна експертиза (експертиза технічних комп'ютерних засобів; експертиза даних; експертиза програмного забезпечення), дактилоскопічна експертиза вилучених слідів рук з різних предметів ЕОТ); телекомунікаційні засоби та системи (експертиза телекомунікаційних систем і засобів); документи (експертиза документів, які утворювались внаслідок вчинення шахрайських дій – криміналістична почеркознавча експертиза; технічна експертиза документів; дактилоскопічна експертиза вилучених слідів рук з документів); майно, яке було предметом посягання (криміналістична експертиза матеріалів, речовин і виробів; трасологічна експертиза; дактилоскопічна експертиза вилучених слідів рук з різних предметів)»[377].

Окрема група дослідників (А. Ф. Волобуєв, Р. Л. Степанюк, В. О. Малярова) головними завданнями судової експертизи комп'ютерних засобів вказала такі, як: «… визначення виду (типу, марки) та властивостей апаратного засобу, а також його технічних і функціональних характеристик для вирішення певних функціональних завдань, установлення місця, ролі та функціонального призначення досліджуваного об'єкта в мережі; визначення фактичного стану та справності апаратного засобу й наявності фізичних дефектів, установлення причинного зв'язку між використанням конкретних можливостей апаратних засобів і результатами їх використання, визначення умов (обстановки) застосовування апаратних засобів, виявлення властивостей і характеристик мережі, встановлення її архітектури й конфігурації, виявлення встановлених мережних компонент та організація доступу до даних, визначення відповідності виявлених характеристик типовим для конкретного класу засобів мережної технології та ін. Під час цієї експертизи може здійснюватися ідентифікація конкретних апаратних засобів за встановленими загальними й окремими ознаками, наприклад серійні номери, формфактори, місткість і структура накопичувача, середній час доступу до даних, швидкість передання даних, спосіб і щільність магнітного запису та ін.»[378].

---

[376] Реуцький А. В. Методика розслідування злочинів у сфері виготовлення та обігу платіжних карток : автореф. дис. … канд. юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2009. 19 с.

[377] Коршикова Т. В. Форми використання спеціальних знань при розслідуванні шахрайства, вчиненого із використанням мережі Інтернет. *Актуальні проблеми кримінального права* : тези доп. XI Всеукр. наук.-теорет. конф., присвяч. пам'яті проф. П. П. Михайленка (Київ, 20 листоп. 2020 р.) / редкол. : В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ : Нац. акад. внутр. справ, 2020. С. 296–298.

[378] Криміналістика : підручник : у 2 т. Т. 2 / за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. 312 с.

Цікавою є думка С. С. Чернявського, який зазначає, що узагальнення вітчизняного і зарубіжного досвіду призначення та проведення судово-бухгалтерської, фінансово-економічної почеркознавчої експертиз, техніко-криміналістичної експертизи документів, комп'ютерно-технічних експертиз є необхідною передумовою подальшого удосконалення окремих методик розслідування фінансового шахрайства[379].

А вже О. І. Мотлях відмічав, що логічне завершення розслідування кримінальних правопорушень у сфері інформаційних комп'ютерних технологій залежить від своєчасного і грамотного проведення необхідних експертиз. Учений наголошує, що такими можуть бути будь-які експертизи різної спрямованості залежно від предмета дослідження. Крім того, науковець зауважив, що окрім традиційних (дактилоскопічних, трасологічних, фоноскопічних, фінансово-економічних, техніко-криміналістичних експертиз документів тощо), важливе значення має судова комп'ютерно-технічна експертиза як різновид класу інженерно-технічних експертиз. О. І. Мотляхом було викладено зміст призначення відповідних експертиз, які необхідно проводити при розслідуванні протиправних діянь у сфері інформаційних комп'ютерних технологій. Дослідник констатував, що основу цього виду експертиз становить вирішення діагностичних та ідентифікаційних питань, що ставлять перед експертом. У підсумку науковець зробив висновок, що вони сприяють розв'язанню таких розшукових завдань, як: встановлення факту знаходження пошукової інформації на технічних носіях, які представлені на експертизу; отримання розшукової інформації про професійні якості злочинця; дають можливість ідентифікувати апаратно-комп'ютерні засоби та їх периферійні устаткування, електронну інформацію щодо її носія тощо[380].

Однією з основних процесуальних дій при розслідуванні кримінальних правопорушень у кіберпросторі є призначення судової комп'ютерно-технічної експертизи (СКТЕ) у випадках, коли необхідно отримати фактичні дані для розслідування кіберзлочинів з використанням електронно-обчислюваної техніки, якими являються факти вчинення шахрайства у сфері банківських електронних платежів, для створення доказової бази в кримінальних провадженнях. КТЕ – це підвид інженерно-технічної експертизи[381], за якої досліджу-

[379] Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : автореф. дис. … д-ра юрид. наук : 12.00.09 / Нац. акад. внутр. справ. Київ, 2010. 36 с.

[380] Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. … канд. юрид. наук : 12.00.09 / Акад. праці і соц. відносин Федерації профспілок України. Київ, 2005. 21 с.

[381] Інструкція про призначення та проведення судових експертиз та експертних досліджень та Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень : затв. наказом М-ва юстиції України від 08.10.1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 22.09.2025).

ються певні технічні характеристики обчислювальної техніки, а саме стаціонарних комп'ютерів (ПК), смартфонів, ноутбуків, планшетів, нетбуків тощо, та проводиться детальний аналіз програм, встановлених на цих технічних засобах, з метою виявлення інформації, що знаходиться на них в електронному вигляді, для встановлення факту скоєння кримінального правопорушення. За допомогою експертизи виявляються ознаки кримінального правопорушення, що слугують створенню доказової бази шляхом аналізу виявленої інформації[382].

Як зазначають експерти, до основних завдань експертизи комп'ютерної техніки і програмних продуктів належать:

– встановлення робочого стану комп'ютерно-технічних засобів;

– встановлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях;

– встановлення відповідності програмних продуктів певним версіям чи вимогам на його розробку[383].

З цього приводу, О. А. Самойленко доречно вказує, що аналіз спеціальної літератури й нормативних джерел дав можливість визначити, що КТЕ – це дослідження технічних властивостей комп'ютерного (цифрового) обладнання, програмного забезпечення, інформації, що містяться на цифрових носіях, з метою встановлення фактичних даних, які мають значення для провадження та пов'язані із застосуванням комп'ютерної техніки, а також виявляються на підставі спеціальних знань у галузях комп'ютерної техніки та програмування. Авторка зазначає, що об'єктами судової експертизи є комп'ютери з носіями інформації (будь-які накопичувачі інформації – дискети, жорсткі диски, CD-диски, флеш-карти тощо), програмні продукти й інша комп'ютерна техніка (наприклад, мобільні телефони, банкомати, гральні автомати, картридери, електронні записні книжки, пейджери, принтери тощо), а також документація до обладнання[384]. Тобто ефективність розслідування кримінальних правопорушень у кіберпросторі, залежить від своєчасного виявлення слідів кримінального правопорушення, адже у випадку, якщо слідчі (розшукові) дії будуть проведені невчасно та із запізненням, зловмисники можуть знищити всю доказову базу, а саме виконати форматування жорсткого диску, фізичне знищення жорсткого диску за допомогою мікрохвильової печі, USB-накопичувачів, зовнішніх накопичувачів, CD-, DVD-дисків тощо.

Для того щоб сліди, які знаходяться на електронних носіях, стали доказами, їх необхідно знайти, виявити та зафіксувати процесуальним шляхом, що

---

[382] Експертна служба МВС України. URL: https://dndekc.mvs.gov.ua/ (дата звернення: 22.09.2025).

[383] Комп'ютерно-технічна експертиза. URL: https://nise.com.ua/it-ekspertyza (дата звернення: 14.09.2025).

[384] Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ : КНТ, 2009. 328 с.

регулюється Законом України «Про судову експертизу»[385].

Факти та обставини, що виявляються в процесі аналізу апаратно-технічних засобів та програмного забезпечення, встановленого на цих засобах, які є доказами у матеріалах кримінального провадження, є предметом СКТЕ[386].

Експерти з Національного наукового центру «Інститут судових експертиз імені Засл. проф. М. С. Бокаріуса» Міністерства юстиції України визначили такий орієнтовний перелік вирішуваних питань для КТЕ:

Чи міститься на даному носії інформація стосовно (зазначити, яка інформація цікавить) і у якому вигляді?

Чи містить носій досліджуваного комп'ютера інформацію про певні (зазначити, які саме) дії користувача?

Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації?

Чи могла бути створена зазначена інформація на цьому комп'ютері чи вона перенесена з іншого носія?

Яким чином інформація (зазначити, яка саме) перенесена до досліджуваного комп'ютера (носія)?

Яка технологія та хронологія створення електронного документа (зазначити електронний документ та певний зміст)?

Які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію стосовно... (зазначити зміст)?

Чи містить накопичувач інформації досліджуваного комп'ютера певне (зазначити, яке саме – встановлене, не встановлене) програмне забезпечення?

Які функціональні несправності мають дане комп'ютерне обладнання або його окремі складові та пристрої і як ці несправності впливають на роботу обладнання в цілому?

Чи можливо виконання певних дій за допомогою даного програмного продукту?

Чи можливе вирішення певного завдання за допомогою даного програмного продукту?

Чи реалізовані у даному програмному продукті (програмному коді) функції, передбачені технічним завданням на його розробку?[387].

Залежно від обставин кримінального провадження можуть бути призначені такі види експертиз:

– апаратно-комп'ютерна експертиза (АКЕ);

– програмно-комп'ютерна експертиза (ПКЕ);

---

[385] Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (дата звернення: 22.09.2025).

[386] Експертизи у судочинстві України : наук.-практ. посіб. / заг. ред. В. Г. Гончаренка, І. В. Гори. Київ : Юрінком Інтер, 2014. 504 с.

[387] Комп'ютерно-технічна експертиза. *Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М.С. Бокаріуса»* : офіц. Сайт. URL: https://nise.com.ua/it-ekspertyza (дата звернення: 14.09.2025).

– комп'ютерно-мережева експертиза (КМЕ);

– інформаційно-комп'ютерна експертиза(ІКЕ)[388].

Об'єктом дослідження АКЕ може бути саме техніка, за допомогою якої вчинялося шахрайство у сфері банківських електронних платежів. До апаратних засобів належать: електричні, електронні та механічні схеми, блоки, прилади і пристрої, що становлять матеріальну частину комп'ютерної системи. При проведенні цієї експертизи досліджуються ноутбуки, системні блоки, за якими встановлюється вид та назва процесора (CPU), вид та назва материнської плати (motherboard), вид оперативної пам'яті (RAM), назва відеокарти (GPU), вид жорсткого накопичувача (HDD або SSD). Встановлення видів і назв технічних засобів дозволяє порівняти їх зі слідами, залишеними злочинцем на серверах банківських установ або організацій, що піддалися шахрайським діям. Головним ідентифікаційним фактором комп'ютера, з якого проводилися шахрайські дії, є так званий ідентифікаційний номер ПК (MAC-адреса). MAC-адреса (Media Access Control, адреса управління доступом до середовища) записується в заводську прошивку мережевого адаптера при його виготовленні[389]. Він потрібен для того, щоб ідентифікувати конкретний мережевий адаптер, який знаходиться на материнській платі. Кожен пакет даних, що приймається адаптером, містить його MAC-адресу, для того щоб пристрій міг зрозуміти, що ці дані призначені саме йому. MAC-адреса ПК подібна відбиткам пальців: якщо злочинець при вчиненні шахрайських операцій у сфері банківських електронних платежів був необережний у своїх діях та не замінив MAC-адресу за допомогою спеціальних програм, то його обчислювальна техніка, за допомогою якої шахрай вчиняв суспільно небезпечне діяння, буде ідентифікована.

При проведенні АКЕ експерту необхідно зупинитися на таких моментах:

– виявити відношення досліджуваної техніки до апаратних комп'ютерних засобів;

– визначити тип, марку або модель досліджуваного пристрою;

– встановити технічні характеристики й параметри цього технічного засобу;

– визначити первинну конфігурацію та характеристики пристрою, а також дізнатися, чи були змінені його функціональні властивості порівняно з первісною конфігурацією;

– провести зовнішній огляд техніки на предмет фізичного втручання у його конфігурацію;

---

[388] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

[389] IEEE Standards Association (IEEE SA). URL: https://standards.ieee.org/products-services/regauth/oui36/index.html (дата звернення: 21.09.2025).

– встановити, чи є цей технічний засіб накопичувачем інформації, чи відкритий доступ до такої інформації[390].

Дослідження саме програмного забезпечення, встановленого на техніці потенційного зловмисника, являє собою ПКЕ. Предметом ПКЕ є закономірності розробки програмного забезпечення на ЕОТ, що була передана для дослідження та виявлення слідів кримінального правопорушення, а також закономірності його застосування. Завданням ПКЕ є встановлення наявності певних видів програм, що сприяють вчиненню шахрайських операцій у сфері банківських електронних платежів. Ними можуть бути програми, призначені для віддаленого доступу до інформації та керування комп'ютером, наприклад: AnyDesk, Supremo Remote Desktop, TeamViewer, RemotePC тощо. Важливою є наявність програм, призначених для анонімного та зашифрованого спілкування в мережі інтернет, таких як Jabber, Telegram, WhatsApp та ін. Як правило, зловмисники можуть використовувати графічні редактори для підроблення документів, наприклад Adobe Photoshop, Corel Draw, тощо, тому експерт повинен ідентифікувати їх наявність та встановити історію застосування таких додатків, відновити файли, створені за допомогою цих програм, і в такий спосіб виявити значущі сліди вчинення злочину, що можуть стати важливими доказами в кримінальному провадженні. Не менш вагомою знахідкою можуть бути програми для віддаленого керування банківськими рахунками – інтернет-банкінг, які зловмисники зазвичай використовують на смартфонах та планшетах. За виявлення зазначеного вище програмного забезпечення експерту потрібно встановити або відновити log-файли використання цих програм, що дозволить виявити ланцюг операцій і послідовність дій шахрая[391].

Інформаційно-комп'ютерна експертиза (ІКЕ) як ключовий вид СКТЕ може стати одним з основних доказів, які можуть вказувати на причетність (або непричетність) до кримінального правопорушення та стати підставою при визначенні вини. Завданням ІКЕ є виявлення наявних або видалених файлів, на яких може міститися значуща для слідства інформація. Особливу увагу експерт має приділити файлам документів формату .doc, .docx, .txt, .rtf, .pdf, .xls, .xlsx та ін., log-файлам електронної пошти та месенджерів. Під час виконання ІКЕ також необхідно з'ясувати, чи встановлено на техніці, що була представлена на СТКЕ, програмне забезпечення для шифрування та захисту інформації, що підтверджувала б чи спростовувала здійснення шахрайства у сфері банківських електронних платежів. Шифрування диска створює зашифровані розділи на жорстких дисках або створює

[390] Коваленко І. О. Окремі види експертиз як обов'язкові слідчі (розшукові) дії під час розслідування шахрайства у сфері банківських електронних платежів. *Підприємництво, господарство і право.* 2020. № 12. С. 262–266.

[391] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

віртуальні зашифровані диски у файлі[392].

Після зашифрування дані, що зберігаються в розділі, потребують доступу до пароля. Як правило, шахраї накладають одразу кілька різних паролів для унеможливлення доступу сторонніх осіб до інформації, яка може викрити їх зловмисні дії. Кожен із таких паролів захищено за допомогою алгоритму шифрування AES 128- або 256-бітного ключа, який дуже важко і практично неможливо розшифрувати, зважаючи на щосекундний розвиток технологій і відсталість в обізнаності з новітніми комп'ютерними системами та їх використанням у сучасній криміналістиці. Найбільш розповсюдженими програмами шифрування даних станом на 2020 рік були: Folder Lock, AxCrypt, CryptoExpert, CertainSafe, VeraCrypt, TrueCrypt, Bitlocker, Ciphershed[393].

Комп'ютерно-мережева експертиза (КМЕ) як один із видів СТКЕ багато в чому схожий з ПКЕ, однак у цьому випадку фокус експертної уваги зміщено на дослідження мережевої роботи користувача. У такий спосіб вивчаються дії потенційного правопорушника у сфері банківських електронних платежів із залученням комп'ютерних мереж. Для виконання КМЕ фахівець повинен бути компетентним в області мережевих технологій, щоб ефективно відстежувати рух інформаційних пакетів за допомогою вивчення інформаційного сліду. IP-адреса – це числова послідовність, яка слугує ідентифікатором девайсу для інтернет-сервера[394].

IP-адреса відображається у вигляді серії з чотирьох груп чисел, розділених крапками. Перша група – це число від 1 до 255, а інші групи – число від 0 до 255, наприклад 192.135.174.1. Кожен сервер має свою унікальну адресу, за допомогою якої експерти можуть визначити фізичну адресу місця, де було скоєне кримінальне правопорушення. Саме з цієї причини шахраї намагаються замаскувати такі сліди, використовуючи ряд мережевого програмного забезпечення. Існують такі розповсюджені способи підміни реальної IP-адреси: підключення до проксі-сервера, використання інтернет-браузера TOR, маскування IP-адреси через VPN. Під час КМЕ надзвичайно важливо виявити програмне забезпечення, що було встановлене для приховування IP-адреси. Прикладами можуть бути:

– ProxyCap, Proxyfier, Proxy Switcher – програми для проксі;

– TOR Browser, Tor Control (anonymity layer) for Firefox;

– NordVPN, OpenVPN, ExpressVPN, PureVPN for Teams, ProtonVPN, NetMotion – програми, які забезпечують сервіс VPN[395].

---

[392] Mihir, Bellare Public-Key Encryption in a Multi-user Setting : Security Proofs and Improvements. *Springer Berlin Heidelberg*, 2000. 274 p.

[393] Коваленко І. О. Окремі види експертиз як обов'язкові слідчі (розшукові) дії під час розслідування шахрайства у сфері банківських електронних платежів. *Підприємництво, господарство і право.* 2020. № 12. С. 262–266.

[394] Буров Є. В. Комп'ютерні мережі : підручник. Львів : Магнолія 2006, 2010. 262 с.

[395] Коваленко І. О. Окремі види експертиз як обов'язкові слідчі (розшукові) дії під час розслідування шахрайства у сфері банківських електронних платежів. *Підприємництво, господарство і право.* 2020. № 12. С. 262–266.

Водночас експерти зазначають, що для дослідження інформації, що міститься на комп'ютерних носіях, експерту надається сам комп'ютерний носій, а за потреби – комп'ютерний блок (комплекс комп'ютерних засобів, до складу якого входить досліджуваний носій) та вказують, що «… для збереження наданих на дослідження носіїв інформації в робочому стані вони надаються в окремих пакуваннях. Системні блоки персональних комп'ютерів надаються в пакуваннях, що унеможливлюють доступ до носіїв інформації безпосередньо чи підключення системного блока до мережі живлення. Для встановлення відповідності програмних продуктів певним параметрам експерту надається носій з копією досліджуваного програмного продукту або програмного коду. Для дослідження робочого стану комп'ютерно-технічних засобів експерту надаються ці комп'ютерно-технічні засоби, а також технічна документація до них. З метою визначення, які саме об'єкти слід надати експерту в кожному конкретному випадку, а також як їх відбирати для дослідження, доцільно отримати консультацію експерта (спеціаліста) в галузі комп'ютерної техніки»[396].

Підбиваючи підсумки, зауважимо, що процес розслідування кримінальних правопорушень у кіберпросторі в рази спрощується завдяки правильному та своєчасному використанню спеціальних знань на всіх етапах кримінального провадження.

[396] Комп'ютерно-технічна експертиза. URL: https://nise.com.ua/it-ekspertyza (дата звернення: 14.09.2025).

ВИСНОВКИ

У монографічному дослідженні здійснено теоретичне узагальнення і вирішення наукового завдання з опрацювання та наукового аргументування теоретичних і праксеологічних засад методики розслідування кримінальних правопорушень у кіберпросторі. Серед найбільш важливих результатів створення монографії вбачаємо такі.

Здійснено криміналістичний аналіз кримінальних правопорушень у кіберпросторі. Запропоновано класифікацію кримінальних правопорушень у кіберпросторі, як-от: кримінальні правопорушення у кіберпросторі проти основ національної безпеки України; кримінальні правопорушення у кіберпросторі у сфері власності; кримінальні правопорушення у кіберпросторі у сфері господарської діяльності; кримінальні правопорушення у кіберпросторі у сфері моральності; кримінальні правопорушення у кіберпросторі у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; кібертероризм, який поєднує вищеперераховані кримінальні правопорушення.

Визначено структуру міжвидової методики розслідування кримінальних правопорушень у кіберпросторі, в якій виокремлено такі складові, як: 1) криміналістична характеристика; 2) аналіз первинних відомостей про вчинення кримінального правопорушення у кіберпросторі; 3) обставини, які підлягають встановленню; 4) типові слідчі ситуації та відповідний їм порядок дій уповноважених осіб; 5) взаємодія підрозділів правоохоронних органів та інших структур під час розслідування кримінальних правопорушень у кіберпросторі; 6) профілактична діяльність уповноважених осіб для встановлення причин та умов, що сприяли учиненню протиправних дій; 7) особливості реалізації початкових слідчих (розшукових) і процесуальних дій та інших заходів; 8) особливості проведення подальших слідчих (розшукових) і процесуальних дій та інших заходів; 9) особливості використання спеціальних знань.

Серед елементів криміналістичної характеристики кримінальних правопорушень у кіберпросторі виокремлено й схарактеризовано такі: спосіб підготовки, учинення та приховування протиправного діяння; обстановка вчинення кримінального правопорушення; слідова картина; особа правопорушника (кіберзлочинеця); особа потерпілого.

З'ясовано, що мали місце такі підготовчі заходи до вчинення кримінальних правопорушень у кіберпросторі, як-от: підбір та підготовка необхідної електронно-обчислювальної техніки (комп'ютерів, ноутбуків, планшетів); створення шкідливих програмних чи технічних засобів з метою протиправного використання, розповсюдження або збуту; несанкціоновані збут або розповсюдження через мережу «Інтернет» інформації з обмеженим доступом, яка зберігається в комп'ютерах; створення повідомлень електрозв'язку для пода-

льшого їх масового розповсюдження, здійснене без попередньої згоди адресатів; створення сприятливих умов для здійснення протиправних дій та ін.

Виокремлено перелік способів безпосереднього вчинення кримінальних правопорушень у кіберпросторі, а саме: 1) протиправні дії у сфері власності (фішинг, смішинг, сніфферінг, 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 інтернету; 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.

Установлено, що кіберзлочинці використовували такі способи приховування своєї протиправної діяльності: використання перетворення ідентифікатора місця знаходження устаткування, за допомогою якого вчинюються протиправні дії – 88 %; приховування створеного шкідливого програмного забезпечення за допомогою легального програмного забезпечення – 51 %; відмова від дачі показань – 45 %; знищення обладнання, що використовувалося для вчинення протиправних дій – 44 %; дача неправдивих показів при проведенні окремих процесуальних дій (у тому числі – неправдиве алібі) – 42 %.

Визначено місця вчинення кримінальних правопорушень у кіберпросторі, а саме: місця розташування ЕОТ, з якої вчинялися протиправні дії (стаціонарне комп'ютерне обладнання, ноутбук, планшет, телефон) – 61 %; місця розташування ЕОТ, стосовно якої вчинялись протиправні дії (ПЕОМ, ноутбук, планшет, телефон) – 61 %; місця знаходження банкоматів, установ, підприємств та організацій фінансової сфери – 21 %; місце знаходження потерпілого, який виявив факт вчинення кримінальних правопорушень у кіберпросторі, – 12 %, інші – 6 %.

З'ясовано, що при розслідуванні кримінальних правопорушень у кіберпросторі домінувальне місце займають електронно-цифрові (віртуальні) сліди, що містяться: у пам'яті ЕОТ, планшетів (98 %); у пам'яті мобільного телефону (IMEI-код; історія телефонних з'єднань, історія голосових повідомлень; історія текстових повідомлень; програмне забезпечення для проведення банківських операцій з телефону тощо) (84 %); у пам'яті сім-карти (82 %); у електронній поштовій скриньці (77 %); на флешкарті (файли, папки тощо) (75 %); інформація в електронному вигляді, яка відображає суми грошових коштів, переказаних через певну систему електронних платежів («ПриватБанк», «Qiwi-гаманець», MoneyGram, Western Union, Perfect Money та ін.) (59 %); на сервері мобільного оператора (56 %); профіль у соціальних мережах, інформація на сайтах (43 %); на сервері інтернет-провайдера (сервер зберігання flow-статистики и біллінгової інформації, сервер баз даних тощо) (21 %) тощо.

Встановлено, що кримінальні правопорушення у кіберпросторі в основному вчиняють особи чоловічої статі у віці 25–35 років, які мають вищу освіту, працюють у сферах підприємницької діяльності та комп'ютерних технологій і характеризуються високим інтелектуальним рівнем. Виокремлено віктимогенні групи потерпілих, зокрема: а) особи, які піддалися впливу знайомих і родичів при здійсненні різноманітних операцій на ЕОТ (ПЕОМ, планшети, смартфони); б) особи, які піддалися обману незнайомих осіб при здійсненні різноманітних операцій на ЕОТ (ПЕОМ, планшети, смартфони); в) особи, які з огляду на негативні психічні стани піддалися впливу незнайомих осіб при здійсненні різноманітних операцій на ЕОТ (ПЕОМ, планшети, смартфони); г) працівники державних організацій та правоохоронних органів при здійсненні різноманітних службових операцій на ЕОТ (ПЕОМ, планшети, смартфони); д) юридичні особи, які через специфіку своєї діяльності зазнали хакерських нападів.

Надано перелік обставин, що підлягають встановленню під час розслідування кримінальних правопорушень у кіберпросторі, а саме: 1) обставини, що розкривають окремі обставини вчинення кримінальних правопорушень у кіберпросторі (інформація про час, місце та способи їх вчинення, дані про використання шкідливих програм чи вірусів, які занесені до комп'ютерного забезпечення потерпілого, дублювання за їх допомогою акаунту на приватний гаджет (смартфон, планшет, ноутбук, комп'ютер); використання реквізитів картки, які вилучені з серверів онлайн-магазинів, платіжних чи розрахункових систем, з персональних гаджетів потерпілих; дані про електронні сліди протиправного діяння; встановлення місця отримання неправомірного доступу та входу до мережі (зсередини чи ззовні), а також способи здійснення неправомірного підключення (зміну програм захисту відомостей, роботу з електронними відомостями та командами, застосовування шпигунських програм); засоби, що використовуються при вчиненні кіберзлочину (технічні – ЕОМ, планшети, ноутбуки, смартфони, модеми, маршрутизатори; програмні – шкідливі віруси, шпигунські програми, VPN); 2) обставини, які характеризують кіберзлочинця (кількість правопорушників та можливий розподіл серед них функціональних обов'язків, визначення задач кожного кіберзлочинця окремо); 3) характеристика потерпілої сторони (фізична чи юридична особа; відповідні віктимогенні групи, їх характеристики; можливі функції з державної оборони); 4) причинно-наслідкові взаємозв'язки (з'ясування наявності певного взаємозв'язку між діями кіберзлочинців та їх результатами); 5) обставини, що обтяжують або пом'якшують покарання, чи взагалі виключають кримінальну відповідальність (наявні умови та підстави для закриття кримінального провадження); 6) вид і розмір шкоди, завданої скоєнням кримінальних правопорушень у кіберпросторі; 7) чинники, які сприяли вчиненню кримінальних правопорушень у кіберпросторі.

Зроблено висновок, що первинна інформація, яка була підставою для внесення даних до ЄРДР за фактом учинення кримінальних правопорушень у

кіберпросторі, надходила до правоохоронних органів з таких джерел: усна заява (повідомлення) про кримінальне правопорушення – 54 %; матеріали правоохоронних, судових і контролюючих державних органів про виявлення фактів вчинення чи підготовки до вчинення кримінальних правопорушень – 31 %; повідомлення підприємств, установ, організацій і посадових осіб – 9 %; повідомлення в засобах масової інформації – 4 %; самостійне виявлення слідчим / дізнавачем (уповноваженою особою іншого підрозділу) кримінального правопорушення, у тому числі під час досудового розслідування – 2 %.

При типізації слідчих ситуацій під час розслідування кримінальних правопорушень у кіберпросторі вважаємо доцільним у їх зміст покласти дані відносно способу вчинення правопорушення та особи, яка його вчинила, з огляду на що нами було визначено серед них такі, як: 1) вчинено кримінальне правопорушення у кіберпросторі, наявна достатня доказова інформація, кіберзлочинець невідомий – 52 %; 2) вчинено кримінальне правопорушення у кіберпросторі, наявна заява від потерпілого, відсутня достатня доказова інформація – 24 %; 3) вчинено кримінальне правопорушення у кіберпросторі, наявна достатня доказова інформація, кіберзлочинець відомий – 18 %; 4) вчинено кримінальне правопорушення у кіберпросторі, наявна матеріальна й особистісна доказова інформація, кіберзлочинець відомий, але його дії замасковані під вид законних фінансових операцій – 6 %.

Виокремлено процесуальні форми взаємодії під час розслідування кримінальних правопорушень у кіберпросторі, а саме: а) виконання доручення уповноваженої особи відносно проведення слідчих (розшукових) дій або НСРД (88 %); б) реалізація розшукових заходів для встановлення осіб, що вчинили кримінальні правопорушення у кіберпросторі, та надання уповноваженій особі відомостей про їх результати (73 %); в) допомога уповноваженій особі під час проведення окремих процесуальних дій (67 %).

Виділено такі організаційні форми взаємодії: а) взаємний обмін інформацією між працівниками підрозділів правоохоронних органів, а також державних, приватних і громадських підприємств, установ і організацій під час кримінального провадження (89 %); б) консультування (77 %); в) спільне обговорення й оцінювання відомостей, одержаних у результаті проведення розшукових заходів, щодо їх достатності для внесення відомостей до ЄРДР (73 %); г) спільні виїзди уповноважених осіб (слідчого, дізнавача) й оперативних працівників для проведення слідчих (розшукових) дій, НСРД (58 %); д) колегіальне проведення складних процесуальних дій (огляд місця події, слідчий експеримент) або окремих тактичних операцій (53 %).

Визначено перелік профілактичних заходів у кримінальних провадженнях за фактами вчинення кримінальних правопорушень у кіберпросторі, а саме: застосовування протоколів безпеки, зокрема криптографічні функції та системи аутентифікації користувачів (для перевірки правильності введених відомостей, попередження заміни особи користувача); встановлення осіб, ладних вчинювати протиправну діяльність у сфері ЕОТ (хакери, фішери, кардери)

та їх подальша постановка на відповідні обліки у Департаменті кіберполіції; інформування населення через засоби масової інформації про юридичну відповідальність за протиправну діяльність у кіберпросторі; повідомлення громадянам із застосуванням різноманітних месенджерів та соціальних мереж про ситуації вчинення протиправних дій у сфері використання ЕОТ (фішинг, сніфферінг, кардинг*);* застосовування технологій фіксації транзакцій, які дозволяють записувати всі дані (зокрема, блокчейн); попередження повторних (рецидивних) проявів протиправних дій у кіберпросторі.

Виділено організаційно-тактичні аспекти проведення окремих слідчих (розшукових) дій, спрямованих на отримання інформації з матеріальних та особистісних джерел, серед яких виокремлено такі процесуальні дії, як: допит підозрюваного (100 %); допит потерпілого або представника потерпілої сторони (100 %); огляд ЕОТ, документів (100 %); призначення судових експертиз (100 %); обшук (72 %); огляд місця події (61 %); одночасний допит двох чи більше раніше допитаних осіб (43 %); допит свідка (34 %); слідчий експеримент (5 %); пред'явлення особи для впізнання (4 %); освідування (2 %).

Виявлено, що хоча огляд місця події проводився у 61 % випадків, його ефективність становила не більше 31 %, що зумовлено тим, що більшість таких кримінальних правопорушень є розтягнутими в часі, а місце їх фактичного вчинення часто неможливо точно встановити. Визначено такі місця проведення огляду: місця зберігання й обробки електронної інформації, що зазнала протиправного впливу (71 %); місця знаходження ЕОТ, що застосовувалося при здійсненні протиправного діяння (51 %); місця збереження інформації, отриманої протиправним шляхом (39 %); місця настання шкідливих наслідків (9 %).

З'ясовано помилки, які допускали уповноважені особи під час проведення огляду місця події, зокрема: неаргументоване звуження меж огляду (81 %); ігнорування оперативної інформації (73 %); непослідовне та поверхневе дослідження на місці події матеріальної доказової інформації (69 %); недодержання тактичних рекомендацій щодо деталізованого опису обстановки та об'єктів огляду (58 %); несвоєчасне проведення огляду (51 %); відсутність додатків до протоколу (39 %). Наголошено на тому, що при огляді ЕОТ необхідно залучати відповідних ІТ-фахівці з кібербезпеки із використанням спеціальних технічних засобів для виявлення, встановлення та вилучення певної інформації, яка знаходиться на електронних носіях та слугуватиме доказами за кримінальним правопорушенням.

Об'єктами обшуку під час розслідування кримінальних правопорушень у кіберпросторі визначено: житлові приміщення (55 %); приміщення підприємств, організацій, установ, в т.ч. банків (29 %); підсобні приміщення (5 %); інші об'єкти (4 %); гаражі (3 %); дачі (2 %); транспортні засоби (2 %). Виявлено, що обшук у більшості випадків проводився в таких місцях: місця знаходження комп'ютерного обладнання, що використовувалося при здійсненні протиправного діяння (68 %); місця зберігання й обробки даних (59 %); місця

збереження відомостей, одержаних протиправним шляхом (47 %); місця настання шкідливих наслідків (27 %).

Встановлено ймовірні категорії свідків при розслідуванні кримінальних правопорушень у кіберпросторі: особи, яким може бути відома інформація про обставини та умови протиправної діяльності, яку вони спостерігали – 100 %; особи, які перебувають у родинному або іншому зв'язку з кіберзлочинцем – 56 %; особи, яким відомо умови та обставини тих дій, у яких вони брали участь (програмісти, інженери-системники) – 47 %; особи, які певним чином сприяли вчиненню протиправного діяння, але самі про це не знали (оператори ЕОМ, адміністратора комп'ютерної мережі) – 39 %; особи, які були обізнані про обставини, що передували вчиненню протиправних дій – 25%; працівники державних установ, які були задіяні у вчиненні кримінальних правопорушень у кіберпросторі (оператори ЕОМ, адміністратора комп'ютерної мережі) – 9 %.

Допит зазначених учасників кримінального провадження дозволяє: отримувати відомості про особу правопорушника (кіберзлочинця) (95 %); визначати послідовність проведення інших процесуальних дій (72 %); вчасно висувати слідчі версії на початковому етапі розслідування (62 %); з'ясовувати дані, що мають тактичне значення у кримінальному провадженні (49 %); отримувати відомості про обставини протиправного діяння (41 %); з'ясовувати причини та умови, що сприяли вчиненню кримінальних правопорушень у кіберпросторі (29 %), та ін.

З'ясовано найбільш доцільні тактичні прийоми, які слід застосовувати під час допиту кіберзлочинця, як-от: встановлення психологічного контакту (100 %); постановка запитань (100 %); пред'явлення доказів (89 %); пред'явлення матеріалів кримінального провадження (83 %); спостереження за поведінкою кіберзлочинця (69 %); актуалізація забутого у пам'яті допитуваного (59 %); залучення відповідного спеціаліста (48 %); використання техніко-криміналістичних засобів (43 %); викладення показань у формі вільної розповіді (42 %); демонстрація поінформованості слідчого про обставини справи або розповідь про ймовірний розвиток події (19 %).

Встановлено, що вчинення кримінальних правопорушень у кіберпросторі передбачає здебільшого вельми педантичну підготовку кіберзлочинців до вчинення вказаних протиправних діянь З огляду на те, що більшість досліджуваних правопорушень мають «безконтактну» форму (тобто немає візуального контакту між кіберзлочинцем та потерпілою стороною), виникає потреба у проведенні ряду НСРД та ОТЗ. Указане пояснюється потребою детального негласного документування для ефективного доказування визначених діянь. Зокрема, серед них виокремити такі: аудіо-, відеоконтроль особи; зняття інформації з електронних комунікаційних мереж; зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача; спостереження за особою в публічно доступних місцях; аудіо-, відеоконтроль місця. Виявлено також труднощі, що виходять зі здійснення зазначених НСРД

при розслідуванні кримінальних правопорушень у кіберпросторі, зокрема: непогоджена взаємодія підрозділів правоохоронних органів та працівників установ зв'язку (71 %); проблематичність отримання ухвали слідчого судді апеляційного суду стосовно проведення певної НСРД (59 %); дефіцит потреби в огляді та вилученні документів (52 %); небажання окремих уповноважених осіб вдосконалювати процес кримінального провадження, а також пошук найбільш легких шляхів для отримання доказових даних (39 %).

Виоермлено такі чинники, які сприяють успішному проведенню НСРД при розслідуванні кримінальних правопорушень у кіберпросторі: всебічна та ретельна підготовка (100 %); своєчасність у прийнятті рішення (94 %); використання спеціальних знань, у тому числі інших осіб (71 %); правильне застосування тактичних прийомів та їх комплексів (69 %); залучення відповідних спеціалістів (68 %); інше (43 %).

З'ясовано, що одним із надзвичайно важливих засобів отримання доказової інформації у кримінальних провадженнях, розпочатих за фактом вчинення кримінальних правопорушень у кіберпросторі, є використання спеціальних знань. Визначено такі форми використання спеціальних знань у досліджуваній категорії кримінальних проваджень: зняття інформації з електронних комунікаційних мереж та електронних систем (100 %); призначення експертизи (100 %); участь спеціаліста у проведенні слідчих (розшукових) дій, НСРД та інших процесуальних заходах (61 %); інше (29 %); консультативно-довідкова допомога (22 %). Стосовно участі спеціаліста було з'ясовано, що здебільшого він залучався до реалізації таких процесуальних дій: огляд ЕОТ (100 %); огляд місця події (100 %); обшук (82 %); тимчасовий доступ до речей та документів (65 %); допит (43 %).

ДОДАТКИ

Додаток А

Зведені результати опитувань
215 працівників оперативних підрозділів (у тому числі – 28 працівників кіберполіції) 122 слідчих, 97 працівників органів прокуратури та 85 працівників експертних установ МВС України

	З а п и т а н н я	**%**
1.	**Вкажіть Ваш вік:**	
	до 25 років	**23**
	25–30 років	**37**
	31–40 років	**28**
	41 рік і старше	**12**
2.	**Вкажіть Ваш стаж практичної роботи:**	
	до 1 року	**3**
	від 1 до 3 років	**7**
	від 3 до 5 років	**18**
	від 5 до 10 років	**31**
	понад 10 років	**41**
3.	**Чи мали місце у Вашому підрозділі випадки розслідування кримінальних правопорушень у кіберпросторі, і чи можете Ви надати інформацію з цього приводу?**	
	так	**100**
	ні	**0**
4.	**Чи розслідували Ви особисто або брали участь у розслідуванні кримінальних правопорушень у кіберпросторі?**	
	так	**56**
	ні	**44**
5.	**Чи вважаєте Ви, що розслідування кримінальних правопорушень зазначеної категорії потребує відповідної кваліфікації уповноваженої особи у цьому напрямі?**	
	так	**96**
	ні	**4**
6.	**Чи вважаєте Ви одним із найбільш перспективних напрямів підвищення ефективності розслідування побудову системи сталих кореляційних зв'язків між елементами криміналістичної характеристики кримінальних правопорушень у кіберпросторі?**	
	так	**91**
	ні	**9**

7.	**Які процесуальні форми взаємодії застосовувались під час розслідування кримінальних правопорушень у кіберпросторі?**	
	виконання доручення уповноваженої особи щодо проведення слідчих (розшукових) дій або НСРД	**88**
	реалізація розшукових заходів для встановлення осіб, що вчинили кримінальні правопорушення у кіберпросторі, та надання уповноваженій особі відомостей про їх результати	**73**
	допомога уповноваженій особі під час проведення окремих процесуальних дій	**67**
8.	**Які організаційні форми взаємодії застосовувалися під час розслідування кримінальних правопорушень у кіберпросторі?**	
	взаємний обмін інформацією між працівниками підрозділів правоохоронних органів, а також державних, приватних і громадських підприємств, установ та організацій під час кримінального провадження	**89**
	консультування	**77**
	спільне обговорення й оцінювання відомостей, одержаних у результаті проведення розшукових заходів, щодо їх достатності для внесення відомостей до ЄРДР	**73**
	спільні виїзди уповноважених осіб (слідчого, дізнавача) й оперативних працівників для проведення слідчих (розшукових) дій та НСРД	**58**
	колегіальне проведення складних процесуальних дій (огляд місця події, слідчий експеримент) або окремих тактичних операцій	**53**
9.	**Які, на Вашу думку, можуть виникати типові недоліки в процесі виконання взаємодії вказаних підрозділів під час розслідування кримінальних правопорушень у кіберпросторі?**	
	невчасний початок здійснення взаємодії	**78**
	зупинка взаємодії з боку учасників кримінального провадження після закінчення його початкового етапу	**69**
	направлення початкових слідчих (розшукових) дій, НСРД та інших процесуальних дій «визначальній» меті – затриманню кіберзлочинця, у той час як реалізація встановлення обставин вчинення кримінальних правопорушень у кіберпросторі відходить на другий план	**53**
	здійснення СРД, НСРД та інших процесуальних заходів оперативними працівниками без участі уповноваженої особи	**41**
10.	**Як Ви вважаєте, які чинники впливають на поширення кримінальних правопорушень у кіберпросторі?**	
	віктимна поведінка (недбалість, необізнаність, зайва довірливість тощо) потерпілих	**93**
	недосконалість законодавства у сфері інформаційних відносин	**62**

	високий рівень корумпованості органів державної влади та місцевого самоврядування	**58**
	відсутність ефективної взаємодії державних органів між собою	**53**
11.	**Які помилки, на Вашу думку, допускали уповноважені особи під час проведення огляду місця події?**	
	неаргументоване звуження меж огляду	**81**
	ігнорування оперативної інформації	**73**
	непослідовне та поверхневе дослідження на місці події матеріальної доказової інформації	**69**
	недодержання тактичних рекомендацій щодо деталізованого опису обстановки та об'єктів огляду	**58**
	несвоєчасне проведення огляду	**51**
	відсутність додатків до протоколу	**39**
12.	**На Вашу думку, які ймовірні категорії свідків при розслідуванні кримінальних правопорушень у кіберпросторі?**	
	особи, яким може бути відома інформація про обставини та умови протиправної діяльності, яку вони спостерігали	**100**
	особи, які перебувають у родинному або іншому зв'язку з кіберзлочинцем	**56**
	особи, яким відомо умови й обставини тих дій, у яких вони брали участь (програмісти, інженери-системники)	**47**
	особи, які певним чином сприяли вчиненню протиправного діяння, але самі про це не знали (оператори ЕОМ, адміністратори комп'ютерної мережі)	**39**
	особи, які були обізнані про обставини, що передували вчиненню протиправних дій	**25**
	працівники державних установ, які були задіяні у вчиненні кримінальних правопорушень у кіберпросторі (оператори ЕОМ, адміністратори комп'ютерної мережі)	**9**
13.	**Яке, на Вашу думку, значення вчасного проведення допиту підозрюваного?**	
	дозволяє отримати відомості про особу кіберзлочинця (інших співучасників протиправної діяльності)	**95**
	дозволяє визначити послідовність проведення інших процесуальних дій	**72**
	дозволяє вчасно висунути слідчі версії	**62**
	дозволяє з'ясувати дані, що мають тактичне значення	**49**
	дозволяє отримати відомості про обставини протиправного діяння	**41**
	дозволяє з'ясувати причини й умови, що сприяли вчиненню кримінальних правопорушень у кіберпросторі	**29**
14.	**Які, на Вашу думку, найбільш доцільні тактичні прийоми під час допиту підозрюваного (кіберзлочинця)?**	

	встановлення психологічного контакту	**100**
	постановка запитань	**100**
	пред'явлення доказів	**89**
	пред'явлення матеріалів кримінального провадження	**83**
	спостереження за поведінкою допитуваного (кіберзлочинця)	**69**
	актуалізація забутого у пам'яті допитуваного	**59**
	залучення відповідного спеціаліста	**48**
	використання техніко-криміналістичних засобів	**43**
	викладення показань у формі вільної розповіді	**42**
	створення уявлення про поінформованість слідчого або розповідь про ймовірний розвиток події	**19**
	інше (вкажіть)	**12**
15.	**Чи є необхідність, на Вашу думку, у проведенні НСРД та ОТЗ, пов'язаних зі встановленням кіберзлочинця та його зв'язків?**	
	так	**98**
	ні	**2**
	важко відповісти	**0**
16.	**Як Ви вважаєте, які труднощі впливають на здійснення таких НСРД при розслідуванні кримінальних правопорушень у кібе-рпросторі:**	
	незлагоджена взаємодія підрозділів правоохоронних органів та працівників установ зв'язку	**71**
	проблематичність одержання ухвали слідчого судді апеляційного суду стосовно проведення певної НСРД	**59**
	дефіцит потреби в огляді та вилученні документів	**52**
	небажання окремих уповноважених осіб удосконалювати процес досудового розслідування, а також пошук більш легких шляхів для отримання доказових даних	**39**
17.	**Які чинники сприяють успішному проведенню НСРД при розслідуванні кримінальних правопорушень у кіберпросторі?**	
	всебічна та ретельна підготовка	**100**
	своєчасність у прийнятті рішення	**94**
	використання спеціальних знань, у тому числі інших осіб	**71**
	правильне застосування тактичних прийомів та їх комплексів	**69**
	залучення відповідних спеціалістів	**68**
	інше (вкажіть)	**43**
18.	**Які, на Вашу думку, основні форми використання спеціальних знань при розслідуванні кримінальних правопорушень у кіберпросторі?**	
	призначення експертизи	**100**
	участь спеціаліста у проведенні слідчих (розшукових) дій, НСРД	**61**
	інше (вкажіть)	**29**
	консультативно-довідкова допомога	**22**

Додаток Б

Результати вивчення
169 кримінальних справ та 245 кримінальних проваджень за фактами вчинення кримінальних правопорушень у кіберпросторі (Вінницька, Волинська, Дніпропетровська, Донецька, Запорізька, Кіровоградська, Київська, Львівська, Луганська, Миколаївська, Одеська, Полтавська, Тернопільська, Харківська, Херсонська області та м. Київ)

№	Досліджувані питання	%
	КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА	
1.	**Способи вчинення кримінальних правопорушень у кіберпросторі**	
	1.1. Повноструктурний	**100**
	1.2. Підготовка до вчинення	**100**
	вибір кола осіб, які стануть потерпілими від протиправних дій	**100**
	вибір об'єкта, що буде предметом протиправних дій	**100**
	підбір та підготовка необхідної ЕОТ (комп'ютерів, ноутбуків, планшетів)	**100**
	створення сприятливих умов для здійснення протиправних дій	**67**
	створення шкідливих програмних чи технічних засобів з метою протиправного використання, розповсюдження або збуту	**56**
	створення повідомлень електрозв'язку для подальшого їх масового розповсюдження, здійснене без попередньої згоди адресатів	**34**
	несанкціоновані збут або розповсюдження через інтернет інформації з обмеженим доступом, яка зберігається в комп'ютерах	**22**
	1.3. Способи безпосереднього вчинення кримінальних правопорушень у кіберпросторі	**100**
	протиправні дії у сфері власності (фішинг, смішинг, сніфферінг, кардінг)	**87**
	несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж	**68**
	незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення	**65**
	розповсюдження шкідливих програмних чи технічних засобів або їх збут з використанням мережі «Інтернет»	**56**
	умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи комп'ютерів	**34**

	несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах	**22**
	1.4. Способи приховування	**100**
	використання перетворення ідентифікатора місця знаходження устаткування, за допомогою якого вчинюються протиправні дії	**88**
	приховування створеного шкідливого програмного забезпечення за допомогою легального програмного забезпечення	**51**
	відмова від дачі показань	**45**
	знищення обладнання, що використовувалося для вчинення протиправних дій	**44**
	дача неправдивих показань при проведенні окремих процесуальних дій (у тому числі – неправдиве алібі)	**42**
2.	**Обстановка вчинення кримінального правопорушення**	
	2.1. Місце вчинення протиправних дій	
	місця розташування ЕОТ, з якої вчинялись протиправні дії (стаціонарне комп'ютерне обладнання, ноутбук, планшет, телефон)	**74**
	місця розташування ЕОТ, стосовно якої вчинялись протиправні дії (ПЕОМ, ноутбук, планшет, телефон)	**61**
	місця знаходження банкоматів, установ, підприємств та організацій фінансової сфери	**21**
	місце знаходження потерпілого, який виявив факт вчинення кримінальних правопорушень у кіберпросторі	**12**
	інші	**6**
3.	**Відомості про слідову картину протиправного діяння**	
	3.1. Матеріальні сліди:	**52**
	3.2. Електронно-цифрові (віртуальні) сліди:	**100**
	у пам'яті ЕОТ, планшетів	**98**
	у пам'яті мобільного телефону (IMEI-код; історія телефонних з'єднань, історія голосових повідомлень; історія текстових повідомлень; програмне забезпечення для проведення банківських операцій з телефону тощо)	**84**
	у електронній поштовій скриньці	**77**
	на флешкарті (файли, папки тощо)	**75**
	інформація в електронному вигляді, яка відображає суми грошових коштів, переказаних через певну систему електронних платежів («Приват-банк», «Qiwi-гаманець», MoneyGram, Western Union, Perfect Money та ін.)	**59**
	на сервері мобільного оператора	**56**
	профіль у соціальних мережах, інформація на сайтах	**43**
	у пам'яті сім-карти	**32**
	на сервері інтернет-провайдера (сервер зберігання flow-статистики й біллінгової інформації, сервер баз даних тощо)	**21**

	3.3. Ідеальні сліди:	**31**
4.	**Відомості про особу правопорушника (кіберзлочинця)**	
	4.1. Стать:	
	1) чоловіча	**75**
	2) жіноча	**25**
	4.2. Вік:	
	від 18 до 25 років	**33**
	від 25 до 35 років	**42**
	від 35 до 45	**19**
	особи віком 45 років і старші	**11**
	4.3. Освіта:	
	базова середня	**1**
	середня	**1**
	середня спеціальна	**4**
	базова вища	**17**
	повна вища	**77**
	4.4. Сімейний стан:	
	1) у шлюбі	**37**
	2) ні	**63**
	4.5. Рід занять:	
	працівник	**78**
	у сфері підприємницької діяльності та сфері комп'ютерних технологій	**57**
	учень (студент)	**28**
	4.6. Наявність судимості:	**6**
	4.7. Протиправні діяння вчинено у стані сп'яніння:	
	наркотичного	**7**
	алкогольного	**1**
	4.8. Вчинено організованою групою або злочинною організацією:	
	так	**26**
	ні	**74**
	4.9. Особи, які вчиняють кримінальні правопорушення у кіберпросторі, відрізняються досить високим інтелектуальним рівнем розвитку	
	так	**84**
	ні	**16**
5.	**Особа потерпілого**	
	5.1. Віктимогенні групи потерпілих:	
	особи, які піддалися обману незнайомих осіб при здійсненні різноманітних операцій на ЕОТ (ПЕОМ, планшети, смартфони)	**62**
	особи, які з огляду на негативні психічні стани піддалися впливу незнайомих осіб при здійсненні різноманітних операцій на ЕОТ	**13**

	(ПЕОМ, планшети, смартфони)	
	працівники державних організацій і правоохоронних органів при здійсненні різноманітних службових операцій на ЕОТ (ПЕОМ, планшети, смартфони)	**11**
	особи, які піддалися впливу знайомих і родичів при здійсненні різноманітних операцій на ЕОТ (ПЕОМ, планшети, смартфони)	**9**
	юридичні особи, які через специфіку своєї діяльності зазнали хакерських нападів	**5**
	ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ТА ПЛАНУВАННЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ	
6.	**Первинна інформація, яка була підставою для внесення даних до ЄРДР за фактом учинення кримінальних правопорушень у кіберпросторі, надходила до правоохоронних органів з таких джерел:**	
	усна заява (повідомлення) про кримінальне правопорушення	**53**
	матеріали правоохоронних, судових і контролюючих державних органів про виявлення фактів вчинення чи підготовки до вчинення кримінальних правопорушень	**31**
	повідомлення підприємств, установ, організацій і посадових осіб	**9**
	повідомлення в медіа	**4**
	самостійне виявлення слідчим або дізнавачем (уповноваженою особою іншого підрозділу) кримінального правопорушення, у тому числі під час досудового розслідування	**3**
7.	**Типові слідчі ситуації розслідування кримінальних правопорушень у кіберпросторі**	
	вчинено кримінальне правопорушення у кіберпросторі, наявна достатня доказова інформація, кіберзлочинець невідомий	**52**
	вчинено кримінальне правопорушення у кіберпросторі, наявна заява від потерпілого, відсутня достатня доказова інформація	**24**
	вчинено кримінальне правопорушення у кіберпросторі, наявна достатня доказова інформація, кіберзлочинець відомий	**18**
	вчинено кримінальне правопорушення у кіберпросторі, наявна матеріальна й особистісна доказова інформація, кіберзлочинець відомий, але його дії замасковані під вид законних фінансових операцій	**6**
	СЛІДЧІ (РОЗШУКОВІ) ДІЇ ТА НЕГЛАСНІ СЛІДЧІ (РОЗШУКОВІ) ДІЇ	
8.	**Які слідчі (розшукові) дії проводились під час розслідування кримінальних правопорушень у кіберпросторі?**	
	допит підозрюваного	**100**

	допит потерпілого або представника потерпілої сторони	**100**
	огляд ЕОТ, документів	**100**
	призначення судових експертиз	**100**
	обшук	**72**
	огляд місця події	**61**
	одночасний допит двох і більше раніше допитаних осіб	**43**
	допит свідка	**34**
	слідчий експеримент	**5**
	пред'явлення особи для впізнання	**4**
	освідування	**2**
9.	**Огляд**	
	9.1. Проводився:	**100**
	огляд ЕОТ, документів	**100**
	огляд місця події	**61**
	огляд предметів	**18**
	огляд житла чи іншого володіння особи	**7**
	огляд живих осіб (освідування)	**2**
	огляд місцевості або приміщення, що не є місцем події	**1**
	9.2. Місця проведення:	
	місця зберігання й обробки електронної інформації, що зазнала протиправного впливу	**71**
	місця знаходження ЕОТ, що застосовувалася при здійсненні протиправного діяння	**51**
	місця збереження інформації, отриманої протиправним шляхом	**39**
	місця настання шкідливих наслідків	**10**
	9.3. Оформлювалися додатки до протоколу огляду:	
	фототаблиці	**48**
	плани та схеми	**29**
	9.4. Ефективність огляду місця події:	
	так	**31**
	ні	**69**
10.	**Обшук**	
	10.1. Об'єкти обшуку:	
	житлові приміщення	**55**
	приміщення підприємств, організацій, установ, у т.ч. банків	**29**
	підсобні приміщення	**5**
	інші об'єкти	**4**
	гаражі	**3**
	заміські будинки (дачного типу)	**2**
	транспортні засоби	**2**
	10.2. Місця проведення обшуку:	

	місця знаходження комп'ютерного обладнання, що використовувалося при здійсненні протиправного діяння	**68**
	місця зберігання і обробки даних	**59**
	місця збереження відомостей, одержаних протиправним шляхом	**47**
	місця настання шкідливих наслідків	**27**
11.	**Допит**	
	11.1. Проводився:	**100**
12.	**Негласні слідчі (розшукові) дії**	
	зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача	**86**
	зняття інформації з електронних комунікаційних мереж	**81**
	спостереження за особою в публічно доступних місцях; аудіо-, відеоконтроль місця	**79**
	аудіо-, відеоконтроль особи	**75**
13.	**Залучення спеціаліста до проведення процесуальних дій**	
	зняття інформації з електронних комунікаційних мереж та електронних систем	**100**
	огляд ЕОТ	**100**
	огляд місця події	**100**
	обшук	**82**
	тимчасовий доступ до речей та документів	**65**
	допит	**43**

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

1. Абушов Т. А. Система організаційних і тактичних дій під час проведення обшуку. *Науковий вісник Національної академії внутрішніх справ*. 2011. № 6. С. 198–205.

2. Авдєєва Г. К. Сутність цифрових слідів в криміналістиці. *Актуальні питання судової експертизи та криміналістики* : зб. матеріалів Міжнарод. наук.-практ. конф., присвяч. 95-річчю створення Харків. НДІ суд. експертиз ім. засл. проф. М. С. Бокаріуса (м. Харків, 10–11 жовт. 2018 р.). Харків, 2018. С. 90–93.

3. Авдєєва Г. К., Стороженко С. В. Електронні сліди: поняття та види. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2017. № 1 (77). С. 168–174.

4. Александров Ю. В., Гель А. П., Семаков Г. С. Кримінологія : курс лекцій. Київ : МАУП, 2002. 296 с.

5. Аленін Ю. П. Початок досудового розслідування за КПК України 2012 р. *Юридичний часопис Національної академії внутрішніх справ*. 2013. № 1. С. 199–208.

6. Анапольська А. І. Розслідування шахрайств і пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : дис. ... канд. юрид. наук : 12.00.09 / Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ, 2010. 243 с.

7. Апопій В. В. Інтернет-торгівля: проблеми і перспективи розвитку. *Регіональна економіка*. 2003. № 1. С. 25–32.

8. Бабіков О. П. Використання результатів негласних слідчих (розшукових) дій з іншою метою, – межі допустимого. *Часопис Київського університету інтелектуальної власності та права*. 2024. Вип. 5. С. 3–8.

9. Бабіков О. П. Теоретико-прикладні засади негласних слідчих (розшукових) дій: генеза та перспективи розвитку : монографія / Наук.-дослід. ін-т публ. права. Київ : Норма права, 2024. 446 с.

10. Багатостороння загроза шахрайства: чи готові банки гідно протистояти виклику. Глобальне дослідження з питань шахрайства у банківській сфері. URL: https://assets.kpmg/content/dam/kpmg/ua/pdf/2020/01/Global-Banking-Fraud-Survey.pdf (дата звернення: 01.09.2025).

11. Баланюк О. В. Підготовка до злочину : поняття та криміналістична класифікація. *Актуальні проблеми держави і права*. 2006. С. 192–196.

12. Бедь В. В. Юридична психологія : навч. посіб. Київ : Каравелла ; Львів : Новий світ-2000, Магнолія плюс, 2003. 376 с.

13. Безруков Д. В. Використання оперативно-технічних засобів щодо протидії злочинам проти власності підрозділам карного розшуку : дис. ... канд. юрид. наук : 12.00.09 / Дон. юрид. ін-т МВС України. Кривий Ріг, 2015. 230 с.

14. Бідняк Г. С. Висновок експерта як джерело доказів під час розслідування шахрайства. *Криміналістичний вісник*. 2014. № 2 (22). С. 55–59.

15. Бідняк Г. С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств : монографія. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2019. 152 с.

16. Біленчук П. Д., Дубовий О. П., Салтевський М. В., Тимошенко П. Ю. Криміналістика : підруч. для слухачів, ад'юнктів, викладачів вузів системи МВС України / за ред. акад. П. Д. Біленчука. Київ : АТІКА, 1998. 416 с.

17. Біленчук П. Д., Кравчук В. В., Кравчук О. В., Кулик В. М. Комп'ютерний тероризм: практика запобігання, протидії, розслідування : навч. посіб. / за заг. ред. П. Д. Біленчука. Хмельницький : Хмельн. ЦНТЕІ, 2008. 258 с.

18. Білий П. М., Баранов С. О. Основи профілактики злочинів на транспорті : навч. посіб. Київ : УКРІНФОРМ, 2001. 196 с.

19. Білоус В. В. Проблеми методики розслідування фіктивного підприємництва : дис. ... канд. юрид. наук : 12.00.09 / Нац. юрид. акад. ім. Ярослава Мудрого. Харків, 2004. 179 с.

20. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : автореф. дис. … канд. юрид. наук : 12.00.09 / Київ. нац. ун-т ім. Тараса Шевченка. Київ, 2008. 20 с.

21. Бойко О. П. Взаємодія слідчих з підрозділами карного розшуку на досудовому провадженні : автореф. дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2018. 20 с.

22. Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09 / Київ. нац. ун-т внутр. справ. Київ, 2007. 217 с.

23. Брич Л. Місце вчинення злочину і його значення у розмежуванні складів злочинів та відмежуванні їх від складів інших правопорушень. *Вісник Львівського університету*. Серія: Юридична. 2011. Вип. 52. С. 267–280.

24. Буров Є. В. Комп'ютерні мережі : підручник. Львів : Магнолія 2006, 2010. 262 с.

25. Веліканов С. В. Класифікація слідчих ситуацій в криміналістичній методиці : автореф дис. ... канд. юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2002. 16 с.

26. Веліканов С. В. Класифікація слідчих ситуацій в криміналістичній методиці : дис. ... канд. юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2002. 218 с.

27. Венедіктов А. А. Виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації в оперативно-розшуковій діяльності та кримінальному процесі. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2 (33). С. 74–77.

28. Весельський В. К. Слідча ситуація як категорія криміналістичної

тактики. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2011. № 25. С. 193–199.

29. Весельський В. К., Зав'ялов С. М., Пясковський В. В. Сучасні можливості використання даних про спосіб учинення злочину в боротьбі зі злочинністю : навч. посіб. для студ. вищ. навч. закл. Київ : КНТ, 2009. 160 с.

30. Вискарка Т. В. Криміналістична характеристика як елемент методики розслідування шахрайства у сфері використання банківських електронних платежів. *Науковий вісник публічного та приватного права*. 2021. Вип. 2. Т. 2. С. 105–110.

31. Волобуєв А. Ф. Криміналістична характеристика розкрадань майна у сфері підприємницької діяльності. *Вісник Харківського національного університету внутрішніх справ*. 1997. Вип. 2. С. 26–37.

32. Волобуєв А. Ф. Профілактична діяльність при розслідуванні злочинів у сфері підприємництва. *Вісник Харківського національного університету внутрішніх справ*. 2000. № 12. Ч. 1. С. 62–69.

33. Волобуєва О. О. Взаємодія слідчого з фахівцями під час збору інформації про особу, що скоїла злочин : дис. ... канд. юрид. наук : 12.00.09 / Київ. нац. ун-т внутр. справ. Київ, 2006. 236 с.

34. Герасимов О. В. Кримінологічна характеристика та аналіз злочинів у банківській сфері. *Вісник Харківського національного університету імені В. Н. Каразіна*. 2017. Вип. 24. С. 203–207.

35. Гетьман А. Науково-практичний коментар нового Кримінального процесуального кодексу України від 13 квітня 2012 року. URL: http://yport.inf.ua/stattya-audio-videokontrol-50500.html (дата звернення: 14.09.2025).

36. Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2008. 18 с.

37. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : монографія. Запоріжжя, 2003. 250 с.

38. Грібов Л. М., Пугач С. М. Технічні засоби, що використовуються під час проведення негласних слідчих (розшукових) дій. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2 (33). С. 3–6.

39. *Департамент кіберполіції Національної поліції України* : офіційний сайт. URL: https://cyberpolice.gov.ua/contacts/ (дата звернення: 18.09.2025).

40. Динту В. А. Обстановка злочину як елемент криміналістичної характеристики злочинів : автореф. дис. … канд. юрид. наук : 12.00.09 / Ун-т «Одеська юридична академія». Одеса, 2014. 20 с.

41. Директива кібербезпеки NIS 2. URL: https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua#:~:text=NIS%20(the%20security%20of%20network,пошукових%20і%20сервісів%20хмарних%20обчислень) (дата звернення: 15.09.2025).

42. Діброва Т. А., Пісенко Д.О., Сметаніна Н. В. Кіберзлочинність та

кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2022. № 11. С. 546–549. URL: http://lsej.org.ua/11_2022/132.pdf (дата звернення: 18.09.2025).

43. Довженко О. Ю. Класифікація кіберзлочинів у криміналістиці. *Південноукраїнський правничий часопис*. 2019. № 1. С. 19–22.

44. Довженко О. Ю. Основи методики розслідування кіберзлочинів : автореф. дис. … канд. юрид. наук : 12.00.09 / Харків. нац. ун-т внутр. справ. Харків, 2020. 18 с.

45. Довженко О. Ю. Основи методики розслідування кіберзлочинів : дис. … канд. юрид. наук : 12.00.09 / Харків. нац. ун-т внутр. справ. Харків, 2020. 229 с.

46. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : підписаний в м. Страсбург 28 січня 2003 року. URL: http://zakon0.rada.gov.ua/laws/show/994_687 (дата звернення: 06.09.2025).

47. Дуда Х. І. Поняття комп'ютерних слідів злочину. *Науковий вісник Національного університету біоресурсів і природокористування України*. 2014. Вип. 197. Ч. 1. С. 262–267.

48. Експертизи у судочинстві України : наук.-практ. посіб. / за заг. ред. В. Г. Гончаренка, І. В. Гори. Київ : Юрінком Інтер, 2014. 504 с.

49. Експертна служба МВС України. URL: https://dndekc.mvs.gov.ua/ (дата звернення: 22.09.2025).

50. Єфімов М. М. Використання спеціальних знань під час розслідування злочинів проти моральності. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. □ 2. С. 268–274.

51. Єфімов М. М. Криміналістична характеристика як елемент методики розслідування кримінальних правопорушень проти моральності. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. □ 3. С. 161–167.

52. Єфімов М. М. Криміналістичний аналіз окремих сучасних видів шахрайства: проблемні питання. *Науковий вісник публічного та приватного права*. 2021. Вип. 5. С. 116–121.

53. Єфімов М. М. Методика розслідування кримінальних правопорушень проти моральності: наукові та праксеологічні основи : монографія. Одеса : Гельветика, 2020. 392 с.

54. Єфімов М. М. Пріоритетні напрями розслідування злочинів проти моральності в розрізі євроінтеграційних процесів. *Інновації юридичної науки в євроінтеграційному процесі* : матеріали Міжнарод. наук.-практ. конф. (10–11 берез. 2017 року, м. Сладковічево) / Словацька Республіка. Ун-т Данубіус, юридичний факультет Янко Єсенського. 2017. С. 268–271.

55. Єфімов М. М. Проблемні аспекти формулювання визначення спеціальних знань при розслідуванні кримінальних правопорушень. *Забезпечення правопорядку та протидії злочинності в Україні та у світі: проблеми та шляхи їх вирішення* : матеріали ІІІ Міжнарод. наук.-практ. конф. (м. Дніпро, 16 черв. 2023 р.). Дніпро : Дніпров. гуманітар. ун-т, 2023. С. 91–94.

56. Єфімов М. М. Розслідування злочинів проти громадського порядку та моральності : навч. посіб. 2-е вид., допов. і переробл. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2018. 188 с.

57. Єфімов М. М. Теоретичні та практичні засади методики розслідування кримінальних правопорушень проти моральності : дис. … д-ра юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2021. 514 с.

58. Єфімов М. М., Лазарєв В. О. Теоретичні засади методики розслідування втягнення неповнолітнього в заняття проституцією і сутенерства : монографія. Херсон : Гельветика, 2020. 232 с.

59. Єфімов М. М., Пиріг І. В. Методика розслідування окремих видів кримінальних правопорушень : підручник. Дніпро : Біла К. О., 2022. 271 с.

60. Жилін А. Е. Актуальні питання реалізації профілактичних заходів працівниками правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Юридична наука*. 2020. № 2. Т. 2. С. 209–215.

61. Жилін А. Е. Взаємодія різних підрозділів правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів: актуальні питання. *KELM*. 2023. № 3. С. 119–123.

62. Жилін А. Е. Наукова полеміка відносно опису ознак та властивостей окремих елементів криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів. *Науковий вісник публічного та приватного права*. 2023. Вип. 1. С. 89–94.

63. Жилін А. Е. Наукові диспути стосовно визначення криміналістичної характеристики шахрайства у сфері використання банківських електронних платежів. *Науковий вісник публічного та приватного права*. 2022. Вип. 6. С. 122–127.

64. Жилін А. Е. Особливості криміналістичного аналізу первісної інформації та визначення основних напрямів розслідування шахрайства у сфері використання банківських електронних платежів. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі* : матеріали Міжнарод. наук.-практ. конф. (м. Київ, 14–15 черв. 2022 р.). Київ : НДІ публічного права, 2022. С. 21–23.

65. Жилін А. Е. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2023. 226 с.

66. Журавель В. А. Криміналістичні методики: сучасні наукові концепції. Харків : Апостіль, 2012. 304 с.

67. Журавель В. А. Початок досудового розслідування: деякі процесуальні та організаційно-тактичні проблеми. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2015. № 1. С. 251–258.

68. Журавель В. А. Розслідування легалізації (відмивання) доходів, одержаних злочинним шляхом : наук.-практ. посіб. Харків : Одіссей, 2005. 112 с.

69. Журавель В. А. Ситуаційний підхід до формування окремих криміналістичних методик розслідування злочинів. *Теорія та практика судової експертизи і криміналістики*. 2008. Вип. 8. С. 151–162.

70. Зав'ялов С. М. Спосіб вчинення злочину: сучасні проблеми вивчення та використання у боротьбі зі злочинністю : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2005. 20 с.

71. Зав'ялов С. М. Спосіб вчинення злочину: сучасні проблеми вивчення та використання у боротьбі зі злочинністю : дис. … канд. юрид. наук : 12.00.09 / Нац. акад. внутр. справ України. Київ, 2005. 231 с.

72. Загіка Г. В. Кримінологічна характеристика комп'ютерної злочинності. *Правова держава*. 2002. № 4. С. 56–61.

73. Зарубей В. В., Ілляшенко О. В. Особливості висунення та планування версій при розслідуванні квартирних крадіжок, вчинених іноземцями. *Сучасний стан криміналістичного забезпечення досудового розслідування* : зб. матеріалів конф. (м. Київ, 20 квіт. 2017 р.). Київ : ННІ № 2 НАВС, 2017. С. 139–142.

74. Захарова Г. В. Теоретичні засади методики розслідування шахрайства у сфері туризму, вчиненого організованою групою : дис. … канд. юрид. наук : 12.00.09 / ПрАТ «Вищ. навч. закл. «Міжрегіональна Акад. управління персоналом». Київ, 2021. 246 с.

75. Заяць К. Особливості сучасних форм вчинення шахрайств та їх криміналістичне значення. *Підприємництво, господарство і право*. 2017. № 11. С. 207–210.

76. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2023 році. *Департамент кіберполіції Національної поліції України* : офіц. сайт. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-4792/ (дата звернення: 19.09.2025).

77. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році. *Департамент кіберполіції Національної поліції України* : офіц. сайт. URL: https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/ (дата звернення: 19.09.2025).

78. Ілляшенко С. М., Іванова Т. Є. Перспективи та основні проблеми розвитку інтернет-торгівлі в Україні. *Механізм регулювання економі*ки. 2014. № 3. С. 113–119.

79. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : затв. наказом ГПУ, МВС, СБУ, Адміністрації ДПрС, МФ, М-ва юстиції України № 114/1042/516/1199/936/1687/5 від 16.11.2012 р. URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text (дата звернення: 15.09.2025).

80. Інструкція про призначення та проведення судових експертиз та експертних досліджень та Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень : затв. наказом М-ва юстиції України від 08.10.1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text (дата звернення: 22.09.2025).

81. Іщенко А. В. Фундаментальні та прикладні криміналістичні категорії. *Актуальні проблеми розкриття та розслідування злочинів у сучасних умовах* : Міжнарод. наук.-практ. конф. (м. Запоріжжя, 05 листоп. 2010 р.). У 3 ч. Запоріжжя, 2010. Ч. 1. С. 180–182.

82. Іщенко А., Щербаков Г. Проблема слідчих ситуацій, як складова навчального курсу криміналістики. *Вісник Одеського інституту внутрішніх справ*. 2003. № 2. С. 57–63.

83. Керевич О. В. Особливості проведення окремих невідкладних негласних слідчих (розшукових) дій. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2 (33). С. 101–105.

84. Кібератаки на Україну коштують мільйони доларів – СБУ. URL: https://detector.media/infospace/article/122774/2017-02-02-kiberataky-na-ukrainu-koshtuyut-milyony-dolariv-sbu/ (дата звернення: 13.08.2025).

85. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посіб. / Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан; за ред. канд. юрид. наук, доц. Ольги Денькович, д-ра права, проф. Габріеле Шмельцер. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL: law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (дата звернення: 14.07.2025).

86. Кікінчук В. В. Негласні слідчі (розшукові) дії як засоби доказування в кримінальному провадженні. *Аналітично-порівняльне правознавство*. 2025. Вип. № 1. С. 714–718. URL: http://journal-app.uzhnu.edu.ua/article/view/324002 (дата звернення: 14.09.2025).

87. Кікінчук В. В. Негласні слідчі (розшукові) дії як об’єкт криміналістичного дослідження. *Український політико-правовий дискурс*. 2024. URL: https://ppdnz.com.ua/index.php/home/article/view/99/49 (дата звернення: 02.09.2025).

88. Коба В. Б. Взаємодія слідчого з іншими правоохоронними органами, а також представниками державних і приватних установ, як складова організації розслідування шахрайства в інтернет-комерції. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі* : матеріали Міжнарод. наук.-практ. конф. (м. Київ, 14–15 черв. 2022 р.). Київ : НДІ публ. права, 2022.

С. 21–23.

89. Коба В. Б. Загальні напрями організації розслідування шахрайства у сфері е-комерції. *Правові новели*. 2020. № 11. С. 413–419.

90. Коба В. Б. Засоби криміналістичної профілактики у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *Криміналістичний вісник*. 2024. № 2 (42). С. 63–75.

91. Коба В. Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління*. 2022. № 3. С. 291–295.

92. Коба В. Б. Значення тактичних завдань для побудови алгоритму розслідування у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *Виклики сучасності та наукові підходи до їх вирішення* : матеріали Міжнарод. наук.-практ. конф. (м. Київ, 12–13 серп. 2020 р). Київ : НДІ публ. права, 2020. С. 32–34.

93. Коба В. Б. Кібербезпека в Україні: сучасний стан та основні напрями забезпечення. *Безпека у кіберсфері* : зб. матеріалів Міжнарод. наук.-практ. конф. (м. Кам'янець-Подільський, 28 трав. 2025 р.) / МВС України, Харків. нац. ун-т внутр. справ, Нац. акад. правових наук України, Організація з безпеки та співробітництва в Європі. Кам'янець-Подільський : ХНУВС, 2025. 246 с. С. 158–160.

94. Коба В. Б. Криміналістичний аналіз причин та умов, що сприяють учиненню шахрайств у сфері е-комерції. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення* : матеріали Міжнарод. наук.-практ. конф. (м. Київ, 22–23 верес. 2021 р.). Київ : НДІ публ. права, 2021. С. 53–56.

95. Коба В. Б. Наукова полеміка стосовно проведення окремих видів огляду під час розслідування кіберзлочинів. *Актуальні питання у сучасній науці*. Серія «Право». 2025. № 4 (34). С. 659–670.

96. Коба В. Б. Наукові диспути щодо комплексів тактичних операцій при розслідуванні шахрайств у сфері е-комерції. *Держава та регіони*. Серія: Право. 2020. № 2 (68). С. 303–307.

97. Коба В. Б. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайств у сфері е-комерції. *Юридичний науковий електронний журнал*. 2021. № 9. С. 418–420.

98. Коба В. Б. Особливості використання сучасних технологій в сфері е-комунікації. *Сучасні проблеми правового, економічного та соціального розвитку держави* : тези доп. XIII Міжнарод. наук.-практ. конф., присвяч. 30-річчю Харків. нац. ун-ту внутр. справ у статусі ун-ту (м. Вінниця, 22 листоп. 2024 р.) / МВС України, Харків. нац. ун-т внутр. справ, Нац. акад. правових наук України. Вінниця : ХНУВС, 2024. С. 73–76.

99. Коба В. Б. Приводи і підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції: проблеми теорії та практики. *Актуальні проблеми взаємодії правової науки та практики її застосування* :

матеріали Міжнарод. наук.-практ. конф. (м. Київ, 16–17 березня 2022 р.). Київ : НДІ публ. права, 2022. С. 33–36.

100. Коба В. Б. Спосіб учинення кіберзлочинів як елемент криміналістичної характеристики: теоретична та практична проблематика. *Наукові перспективи*· 2025· □ 4· С. 1156–1167.

101. Коба В. Б. Теоретичні та праксеологічні аспекти використання спеціальних знань під час розслідування шахрайств у сфері е-комерції. *Право і суспільство*. 2021. № 6. С. 369–374.

102. Коба В. Б., Чаплинський К. О. Теоретичні та практичні основи формування методики розслідування шахрайства у сфері е-комерції : монографія. Одеса : Юридика, 2024. 376 с.

103. Коваленко І. О. Деякі аспекти проведення обшуку при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Правове життя сучасної України* : матеріали Міжнарод. наук.-практ. конф. У 3 т. (м. Одеса, 15 трав. 2020 р.) / відп. ред. М. Р. Аракелян. Одеса : Гельветика, 2020. Т. 3. С. 385–387.

104. Коваленко І. О. Криміналістичний аналіз шахрайства у сфері банківських електронних платежів. *Прикарпатський юридичний вісник*. 2020. № 5 (34). С. 137–140.

105. Коваленко І. О. Окремі види експертиз як обов'язкові слідчі (розшукові) дії під час розслідування шахрайства у сфері банківських електронних платежів. *Підприємництво, господарство і право*. 2020. № 12. С. 262–266.

106. Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2022. 234 с.

107. Коваленко І. О. Типові слідчі ситуації під час розслідування шахрайства у сфері банківських електронних платежів. *Visegrad Journal on Human Rights* («Пан'європейський університет» Словацької Республіки). 2020. № 1. С. 99–103.

108. Коваленко І. О., Єфімов М. М. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів : монографія. Одеса : Юридика, 2025. 298 с.

109. Коваль Н. О., Борщ М. В. Особливості функціонування платіжних систем України на сучасному етапі їх розвитку. *Ефективна економіка*. 2012. № 10. URL: http://www.economy.nayka.com.ua/?op=1&z=1441 (дата звернення: 04.09.2025).

110. Колесник В. А. Негласні слідчі (розшукові) дії: кримінально-процесуальні та криміналістичні аспекти підготовки і проведення : наук.-практ. посіб. / Академія адвокатури України. Київ : Прецедент, 2014. 135 с.

111. Колесник В. А. Суб'єкти здійснення та класифікація негласних слідчих (розшукових) дій. *Юридичний часопис Національної академії внутрішніх справ*. 2013. № 1. С. 129–134.

112. Комп'ютерно-технічна експертиза. URL: https://nise.com.ua/it-ekspertyza (дата звернення: 27.09.2025).

113. Комп'ютерно-технічна експертиза. *Центр експертиз* : офіц. вебсайт. URL: https://expertise.kiev.ua/uk/kompyuterno-texnichna-ekspertiza/ (дата звернення: 26.09.2025).

114. Конвенція про кіберзлочинність : підписана в м. Будапешті 23 листопада 2001 року. URL: http://zakon0.rada.gov.ua/laws/show/994_575 (дата звернення: 12.08.2025).

115. Корнієнко В. В., Стреляний В. І. Організація розслідування фактів несанкціонованого переказу коштів з рахунків клієнтів банку, які обслуговуються за допомогою систем дистанційного обслуговування : метод. рек. / Харків. нац. ун-т внутр. справ. Харків, 2015. 71 с.

116. Коршикова Т. В. Особливості слідової картини шахрайств, що вчиняються в мережі Інтернет. *Молодий вчений*. 2016. № 1 (28). Ч. 2. С. 51–54.

117. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … д-ра філос. : 081 – Право / Нац. акад. внутр. справ. Київ, 2021. 255 с.

118. Коршикова Т. В. Способи вчинення шахрайств із використанням електронно-обчислювальної техніки як елемент їх криміналістичної характеристики. *Visegrad journal on human rights*. 2020. № 4. С. 129–135.

119. Коршикова Т. В. Типові слідчі ситуації та програми дій слідчого на початковому етапі розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки. *Південноукраїнський правничий часопис*. 2020. Вип. 4. С. 123–131.

120. Коршикова Т. В. Форми використання спеціальних знань при розслідуванні шахрайства, вчиненого із використанням мережі Інтернет. *Актуальні проблеми кримінального права* : тези доп. XI Всеукр. наук.-теорет. конф., присвяч. пам'яті проф. П. П. Михайленка (м. Київ, 20 листоп. 2020 р.) / редкол. : В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ : Нац. акад. внутр. справ, 2020. С. 296–298.

121. Кривопуск О. Г. Способи вчинення злісного невиконання обов'язків по по догляду за дитиною або за особою, щодо якої встановлена опіка чи піклування. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 3. С. 369–376.

122. Криміналістика : підручник : у 2 т. / А. Ф. Волобуєв, О. В. Одерій, Р. Л. Степанюк та ін. ; за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. Т. 2. 312 с.

123. Криміналістика : підруч. для слухачів, ад'юнктів, викладачів вузів системи МВС України / за ред. акад. П. Д. Біленчука. Київ : АТІКА, 1998. 416 с.

124. Криміналістика : підруч. для студ. вищ. навч. закл. / К. О. Чаплинський та ін. Дніпро : Дніпропетр. держ. ун-т внутр. справ ; Ліра ЛТД, 2017. 419 с.

125. Криміналістика : підруч. для студ. юрид. ВНЗ / за ред. В. Ю. Шепітька. Київ : Ін Юре, 2001. 452 с.

126. Криміналістика : підручник / за заг. ред. А. Ф. Волобуєва. Харків : ХНУВС, 2011. 468 с.

127. Криміналістика : підручник / за заг. ред. В. В. Пясковського. 2-ге вид., переробл. і допов. Харків : Право, 2020. 752 с.

128. Криміналістика : підручник / за заг. ред. Є. В. Пряхіна. 3-тє вид., переробл. та допов. Львів : ЛьвДУВС, 2016. 948 с.

129. Криміналістика : підручник / за ред. проф. В. Ю. Шепітька. 4-е вид., переробл. і допов. Харків : Право, 2008. 464 с.

130. Кримінальне право. Загальна частина : підручник / за ред. А. С. Беніцького, В. С. Гуславського, О. О. Дудорова, Б. Г. Розовського. Київ : Істина, 2011. 1121 с.

131. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14/page#Text (дата звернення: 19.08.2025).

132. Кримінальний процес : підручник / за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. 648 с.

133. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VIII URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.09.2025).

134. Кримінологія і профілактика злочинів. Курс лекцій у 2-х кн. Особлива частина / Александров Ю. В та ін. Київ : Нац. акад. внутр. справ України, 2000. 201 с.

135. Кримінологія : підручник для студ. вищих навч. закладів. / за заг. ред. О. М. Джужі. Київ : Юрінком Інтер, 2002. 352 с.

136. Кудінов С. С., Шехавцов Р. М., Дроздов О. М., Гриценко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшукової діяльності у кримінальному провадженні : навч.-практ. посіб. Харків : Оберіг, 2013. 344 с.

137. Кузьмічов В. С., Прокопенко Г. І. Криміналістика : навч. посіб. / за заг. ред. В. Г. Гончаренка та Є. М. Моісєєва. Київ : Юрінком Інтер, 2001. 368 с.

138. Кузьмічов В. С., Чорноус Ю. М. Розслідування злочинів: міжнародне і національне законодавство. Теорія і практика : навч. посіб. Київ : КНТ, 2008. 248 с.

139. Куратченко М. В. Обстановка вчинення сутенерства та втягнення особи в заняття проституцією. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2016. № 3. С. 236–242.

140. Куратченко М. В. Особливості взаємодії слідчих та оперативних підрозділів при розслідуванні сутенерства та втягнення особи в заняття проституцією. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2017. № 2. С. 234–241.

141. Куратченко М. В. Розслідування сутенерства та втягнення особи в

заняття проституцією : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2017. 192 с.

142. Курило В. І., Михайлов О. Є., Яра О. С. Кримінологія: Загальна частина : курс лекцій. Київ : Кондор, 2006. 192 с.

143. Курман О. В. Методика розслідування шахрайства з фінансовими ресурсами : автореф. дис. … канд. юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2002. 16 с.

144. Курман О. В. Методика розслідування шахрайства з фінансовими ресурсами : дис. ... канд. юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2002. 227 с.

145. Курман О. В. Способи несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство*. 2017. № 4. С. 245–249.

146. Лисенко В. В. Криміналістичне забезпечення діяльності податкової міліції (теорія та практика) : монографія. Київ : Логос, 2004. 324 с.

147. Літвінов М. Ю. Світова та українська практика боротьби з кіберзлочинністю. *Право і безпека*. 2017. № 1. С. 85–89.

148. Лук'янчиков Б. Є., Лук'янчиков Є. Д., Петряєв С. Ю. Криміналістика : навч. посіб. для студ. юрид. спец. вищ. навч. закл. : у 2 ч. Ч. ІІ : Криміналістична тактика. Методика розслідування. Київ : НТУУ «Київський політехнічний інститут ім. Ігоря Сікорського», 2017. 505 с.

149. Малюга В. М. Взаємодія слідчого з оперативними підрозділами та іншими суб'єктами в системі методики розслідування злочинів : дис. … канд. юрид. наук : 12.00.09 / Львів. нац. ун-т ім. І. Франка. Львів, 2016. 289 с.

150. 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.

151. Малютін Е. В. Наукові підходи до побудови криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням е-банкінгу. *Інноваційні підходи до реформування сучасного законодавства* : матеріали Міжнарод. наук.-практ. конф. (м. Київ, 20–21 квіт. 2023 р.). Київ : НДІ публ. права, 2023. С. 144–146.

152. 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 Міжнарод. наук.-практ. конф. (м. Київ, 12–13 серп. 2020 р.). Київ : НДІ публ. права, 2020. С. 132–134.

153. 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. 456–460.

154. 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.

155. Мамедова Л. Ш. Особливості використання спеціальних знань під час розслідування кіберзлочинів: міжнародний досвід. *Юридичний науковий електронний журнал*. 2021. № 1. С. 392–395. URL: http://www.lsej.org.ua/12_2021/100.pdf (дата звернення: 12.09.2025).

156. Махова Л. О., Виприцький А. О. Профілактика адміністративних правопорушень у громадських місцях: поняття та види. *Право і суспільство*. 2019. № 2. С. 142–147.

157. Методика розслідування окремих видів злочинів, підслідних органам внутрішніх справ : навч. посіб. / за заг. ред. Є. В. Пряхіна. Львів : ЛьвДУВС, 2011. 324 с.

158. Методичні рекомендації щодо управління операційним ризиком (у тому числі кіберризиком та безперервністю діяльності) та забезпечення зберігання інформації про клієнтів об'єктами платіжної інфраструктури. *Національний банк України* : офіц. вебсайт. URL: https://bank.gov.ua/ua/news/all/metodichni-rekomendatsiyi-schodo-upravlinnya-operatsiynim-rizikom-u-tomu-chisli-kiberrizikom-ta-bezperervnistyu-diyalnosti-ta-zabezpechennya-zberigannya-informatsiyi-pro-kliyentiv-obyektami-platijnoyi-infrastrukturi (дата звернення: 03.09.2025).

159. Микитчик А. В. Заходи запобігання кіберзлочинності в Україні. *Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку* : зб. тез доп. Міжнарод. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 137–139.

160. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. … канд. юрид. наук : 12.00.09 / Акад. праці і соц. відносин Федерації профспілок України. Київ, 2005. 21 с.

161. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09 / Акад. праці і соц. відносин Федерації профспілок України. Київ, 2005. 198 с.

162. Мотлях О. І. Проведення обшуків та виїмок при розслідуванні злочинів, пов'язаних зі сферою комп'ютерних технологій. *Прокуратура, Людина, Держава*. 2005. № 1 (43). С. 57–67.

163. Мотлях О. І. Тактичні основи проведення обшуку у злочинах, пов'язаних з інформаційними технологіями. *Вісник Академії праці і соціальних відносин Федерації профспілок України*. 2002. № 2 (15). С. 157–159.

164. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах : монографія / за ред. проф. В. Ю. Шепітька. Харків : Право, 2009. 168 с.

165. Некрасов В. Атака по телефону: Україну накрила хвиля кібершахрайства. URL: https://www.epravda.com.ua/rus/publications/2017/01/30/619178/ (дата звернення: 05.09.2025).

166. Нескоромний Д. А. Проведення негласних слідчих (розшукових) дій працівниками СБ України при розслідуванні кримінальних правопорушень, вчинених організованими злочинними групами. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2 (33). С. 20–23.

167. Огляд місця події: виявлення та вилучення об'єктів біологічного походження : метод. рек. / МВС України, ДНДЕКЦ / авт.-упоряд. : С. І. Перлін, С. О. Шевцов, Н. М. Косміна, В. В. Іонова. Харків : ФОП Чальцев О. В., 2009. 100 с.

168. Однолько І. В. Запобігання втягненню неповнолітніх у злочинну діяльність. *Науковий часопис Національної академії прокуратури України*. 2016. № 4. С. 146–154.

169. Оперативно-розшукова діяльність : навч. посіб. / за ред. проф. О. М. Джужі. Київ : Правова єдність, 2009. 310 с.

170. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / В. М. Бутузов, В. Д. Гавловський, Л. П. Скалозуб та ін. Київ : Нац. акад. СБ України, 2011. 142 с.

171. Охрімчук Т. В. Криміналістична характеристика шахрайства з фінансовими ресурсами. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. № 23. С. 369–374.

172. Охрімчук Т. В. Особливості використання спеціальних знань при розслідуванні шахрайства з фінансовими ресурсами. *Фінанси, економіка, право*. 2010. № 8. С. 59–63.

173. Охрімчук Т. В. Способи вчинення шахрайства з фінансовими ресурсами. *Правова держава: історія, сучасність та перспективи формування в Україні* : матеріали ІІІ Всеукр. наук.-практ. конф. (м. Запоріжя, 23 квіт. 2010 р.). Запоріжжя : Юрид. ін-т ДДУВС, 2010. Ч. ІІ. С. 94–96.

174. Павлик М. П. Розслідування злочинів у сфері надання послуг із працевлаштування за кордоном : дис. … д-ра філос. : 081 – Право / Нац. акад. внутр. справ. Київ, 2021. 241 с.

175. Павлова Н. В. Розслідування шахрайства при укладанні цивільно-правових угод щодо відчуження житла : монографія. Дніпропетровськ : Дніпропетр. держ. ун-т внутр. справ, 2008. 176 с.

176. Павлова Н. В., Рец В. В. Визначення місця та часу вчинення шахрайства на первинному ринку нерухомості. *Науковий вісник Дніпропетровського університету внутрішніх справ*. № 3 (66). 2018. С. 139–143.

177. Пазиніч В. І. Особливості порушення кримінальної справи і початкового етапу розслідування злочинів, які пов'язані з втручанням в роботу мереж мобільного зв'язку. *Іменем закону*. 2007. № 2. С. 27–29.

178. Паламарчук Л. П. Криміналістичне забезпечення розслідування

незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : автореф. дис. … канд. юрид. наук : 12.00.09 / Акад. прокуратури. Київ, 2005. 21 с.

179. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09 / Нац. акад. внутр. справ. Київ, 2007. 228 с.

180. Перлін С. Поняття і види техніко-криміналістичного забезпечення правозастосовної діяльності. *Підприємництво, господарство і право*. 2020. № 1. С. 221–226.

181. Пиріг І. В. Теоретико-прикладні проблеми експертного забезпечення досудового розслідування : монографія. Дніпропетровськ : Дніпропетр. держ. ун-т внутр. справ ; Ліра ЛТД, 2015. 432 с.

182. Погорецький М. А., Сергєєва Д. Б. Негласні слідчі (розшукові) дії та оперативно-розшукові заходи: поняття, сутність і співвідношення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2 (33). С. 137–141.

183. Погорецький М. А., Хотенець В. М. Процесуальні і організаційно-тактичні форми взаємодії органів дізнання і досудового слідства. *Право і безпека*. 2002. № 1. С. 178–183.

184. Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення : затв. наказом Офісу Генерального прокурора від 30.06.2020 р. № 298. URL: https://zakon.rada.gov.ua/laws/show/v0298905-20#Text (дата звернення: 13.09.2025).

185. Преловський К. В. Сутність і зміст поняття критичної інфраструктури банківської системи України. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2018. № 2. С. 94–98.

186. Приловський В. В. До питання здійснення профілактичних заходів працівниками правоохоронних органів стосовно виявлення та усунення причин і умов втягнення неповнолітніх у протиправну діяльність. *Юридична наука*. 2019. № 11. С. 191–197.

187. Про Державне бюро розслідувань : Закон України від 12.11.2015 р. № 794-VIII. URL: https://zakon.rada.gov.ua/laws/show/794-19#Text (дата звернення: 27.09.2025).

188. Про електронну комерцію : Закон України від 03.09.2015 р. № 675-VIII. URL: https://zakon.rada.gov.ua/laws/show/675-19#Text (дата звернення: 20.09.2025).

189. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 09.09.2025).

190. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: http://zakon5.rada.gov.ua/laws/show/2297-17 (дата звернення: 20.09.2025).

191. Про Національний координаційний центр кібербезпеки : Указ

Президента України від 07.06.2016 р. № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text (дата звернення: 05.09.2025).

192. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 27.09.2025).

193. Про оперативно-розшукову діяльність : Закон України від 22.05.2019 р. № 2720-VIII. URL: https://zakon.rada.gov.ua/laws/show/2135-12 (дата звернення: 12.09.2025).

194. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2163-19 (дата звернення: 06.09.2025).

195. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 27.09.2025).

196. Про Стратегію кібербезпеки України : рішення Ради національної безпеки і оборони України від 27.01.2016 р. Введено в дію Указом Президента України від 15.03.2016 р. № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/n0003525-16#Text (дата звернення: 05.09.2025).

197. Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text (дата звернення: 22.09.2025).

198. Профілактична діяльність слідчого при розслідуванні злочинів : лекція для всіх форм навчання / укл. А. Ф. Волобуєв. Харків : Харків. нац. ун-т внутр. справ, 2003. 23 с.

199. Пчеліна О. В. Тактичні операції під час розслідування злочинів у сфері службової діяльності. *Підприємництво, господарство і право*. 2017. № 3. С. 290–294.

200. Пчолкін В. Д., Ечкенко В. М. Поняття, сутність та завдання взаємодії оперативних підрозділів ОВС. *Вісник Луганської академії внутрішніх справ імені 10-річчя незалежності України*. Спецвип. 2004. Вип. 3, ч. І. С. 109–121.

201. Ревака В. М. Форми використання спеціальних пізнань в досудовому провадженні : дис. ... канд. юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2006. 206 с.

202. Резнікова О. І. Проблеми використання віктимологічних даних у криміналістичній характеристиці злочинів. *Питання боротьби зі злочинністю*. 2014. Вип. 27. С. 288–294.

203. Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції : автореф. дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2023. 20 с.

204. Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т

внутр. справ. Дніпро, 2023. 250 с.

205. Реуцький А. В. Методика розслідування злочинів у сфері виготовлення та обігу платіжних карток : автореф. дис. … канд. юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2009. 19 с.

206. Романенко Т. В. Особливості підготовчого етапу проведення обшуку при розслідуванні шахрайств, що вчиняються з використанням електронно-обчислювальної техніки. *Актуальні проблеми кримінального права, процесу та криміналістики та оперативно-розшукової діяльності* : тези доп. IV Всеукр. наук.-практ. конф. (м. Хмельницький, 26 лют. 2021 р.) / Нац. акад. Держ. прикордон. служби. Хмельницький : НАДПСУ, 2021. С. 520–522.

207. Саінчин О. С. Криміналістичні умови розкриття умисних вбивств. *Правова держава*. 2008. № 10. С. 267–273.

208. Салтевський М. В. Криміналістика (у сучасному викладі) : підручник. Київ : Кондор, 2005. 588 с.

209. Салтевський М. В. Криміналістика : підручник : у 2-х ч. Харків : Консум ; Основа, 1999. Ч. 1. 416 с.

210. Самойленко О. А. Інформаційний продукт як предмет посягання при вчиненні злочинів із використанням обстановки кіберпростору. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. 2018. Т. 29 (68). № 4. С. 165–169.

211. Самойленко О. А. Криміналістичний та правовий аналіз злочинної діяльності в мережі Інтернет. *Порівняльно-аналітичне право*. 2015. № 4. С. 408–411.

212. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

213. Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ : КНТ, 2009. 328 с.

214. Самойленко О. А. Типізація особи, що вчиняє злочин, пов'язаний із використанням обстановки кіберпростору (з позицій криміналістичної науки). *Підприємництво, господарство і право*. 2018. № 8. С. 195–201.

215. Самойлов С. В. «Фішинг» як спосіб вчинення Інтернет-шахрайств. *Актуальні питання сучасних державотворчих та правотворчих процесів* : матеріали Міжнарод. наук.-практ. конф. (м. Запоріжжя, 24 лют. 2011 р.) : у 3 ч. Запоріжжя : Запоріз. міська громад. орг. «Істина», 2011. Ч. 3. С. 102–104.

216. Самойлов С. В. Консультативна та довідкова діяльність обізнаних осіб як форма застосування та використання спеціальних знань при розслідуванні шахрайств, учинених з використанням мережі «Інтернет». *Держава і право в умовах судової реформи* : матеріали Всеукр. наук.-практ. конф. студ., аспір. і молод, учен. (м. Донецьк, 08 квіт. 2011 р.). Донецьк : Дон. ун-т економіки і права, 2011. С. 257–259.

217. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … канд. юрид. наук. : 12.00.09. Донецьк : Дон. юрид. ін-т, 2014. 18 с.

218. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : дис. … канд. юрид. наук : 12.00.09 / Дон. юрид. ін-т. Донецьк, 2014. 226 .

219. Самсонова В. В., Пиріг І. В. Методика розслідування крадіжок, вчинених на території садівницьких товариств і дачних кооперативів : монографія. Дніпропетровськ : Дніпропетр. держ. ун-т внутр. справ ; Ліра ЛТД, 2017. 212 с.

220. Селезньова О. М. Теоретико-методологічні основи інформаційного права України : монографія. Чернівці : Місто, 2014. 407 с.

221. Селецький С. І. Кримінальне право України. Загальна частина. Київ : Центр учбової літератури, 2008. 248 с.

222. Сенаторов М. В. Потерпілий від злочину в кримінальному праві : автореф. дис. … канд. юрид. наук : 12.00.08 / Нац. юрид. акад. України. Харків, 2005. 20 с.

223. Сергєєва Д. Б. Результати негласних слідчих (розшукових) дій: проблемні аспекти визначення. *Право і громадянське суспільство*. 2014. № 1. С. 97–106.

224. 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 : НДІ публ. права, 2022. С. 21–23.

225. 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 Міжнарод. наук.-практ. конф. (м. Київ, 22–23 верес. 2021 р.). Київ : НДІ публ. права, 2021. С. 22–24.

226. 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 Міжнарод. наук.-практ. конф. (м. Київ, 13–14 берез. 2023 р.). Київ : НДІ публ. права, 2023. С. 31–33.

227. 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. Вип. 4. С. 127–132.

228. 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.

229. 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 Міжнарод. наук.-практ. конф. (м. Київ, 12–13 серп. 2020 р). Київ : НДІ публ. права, 2020. С. 35–37.

230. Сисолятін В. В. Розслідування кримінальних правопорушень, пов'язаних із використанням інтернет-банкінгу : дис. … канд. юрид. наук : 12.00.09 / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2024. 230 с.

231. Слободзян А. Нормативно-правове регулювання діяльності суб'єктів негласних слідчих (розшукових) дій. *Вісник Національної академії прокуратури України*. 2014. № 2 (35). С. 86–91.

232. Сорокіна Л. В. Особа злочинця, яка вчиняє злочини у сфері пенсійного забезпечення. *Правовий часопис Донбасу*. 2019. № 1 (66). С. 99–106.

233. Справа № 170/827/24. Архів Шацького районного суду Волинської обл., 2024 р.

234. Справа № 210/3688/24. Архів Дзержинського районного суду м. Кривого Рогу Дніпропетровської обл., 2024 р.

235. Справа № 385/1402/24. Архів Гайворонського районного суду Кіровоградської обл., 2024 р.

236. Справа № 461/1901/25. Архів Галицького районного суду м. Львова, 2025 р.

237. Справа № 463/7254/21. Архів Личаківського районного суду м. Львова, 2021 р.

238. Справа № 643/11884/24. Архів Московського районного суду м. Харькова, 2024 р.

239. Справа № 760/8515/23. Архів Солом'янського районного суду м. Києва, 2024 р.

240. Справа № 953/9907/24. Архів Київського районного суду м. Харкова, 2024 р.

241. Старушкевич А. В. Криміналістична характеристика злочинів : навч. посіб. Київ, 1997. 44 с.

242. Степанюк Р. Л. Ситуаційний підхід у формуванні методик розслідування злочинів, вчинених у бюджетній сфері України. *Право і безпека*. 2013. № 3 (50). С. 110–115.

243. Степанюк Р. Л. Сутність і практичне значення криміналістичної характеристики злочинів. *Порівняльно-аналітичне право*. 2014. № 5. С. 398–400.

244. Стрюк М. І., Семеріков С. О., Стрюк А. М. Мобільність: системний підхід. *Інформаційні технології і засоби навчання*. 2015. № 5. Т. 49. С. 41–49.

245. Тіщенко В. В. Концептуальні основи розслідування корисливо-насильницьких злочинів : автореф. дис. … д-ра юрид. наук : 12.00.09 / Нац. юрид. акад. України ім. Ярослава Мудрого. Харків, 2003. 34 с.

246. Тіщенко В. В. Криміналістичні технології в теорії і практиці розслідування. *Актуальні проблеми держави і права*. 2008. Вип. 44. С. 18–24.

247. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса : Фенікс, 2007. 260 с.

248. Томін С. В. Об'єкт та предмет профілактики кримінальних правопорушень як окремого вчення криміналістики. *Прикарпатський юридичний вісник*. 2016. Вип. 3 (12). С. 123–127.

249. ТОП-5 найбільших криптовалютних зломів в історії. URL: https://datami.ee/ua/blog/top-5-largest-cryptocurrency-hacks-in-history/ (дата звернення: 19.09.2025).

250. Фінагеєв В. О. Способи вчинення злочинів, пов'язаних із використанням засобів доступу до банківських рахунків. *Науковий вісник Національної академії внутрішніх справ*. 2016. № 1. С. 63–82.

251. Хакери за рік посилили атаки на український кіберпростір майже на 70 % – Держспецзв'язку. URL: https://sprotyv.info/news/hakeri-za-rik-posililiataki-na-ukraïnskij-kiberprostir-majzhe-na-70-derzhspeczzvyazku/ (дата звернення: 12.08.2025).

252. Хамига Ю. Я. Фінансове шахрайство: критерії ідентифікації та напрями мінімізації : дис. … д-ра філос. : 072 – Фінанси, банківська справа та страхування / Західноукр. нац. ун-т. Тернопіль, 2020. 308 с.

253. Харчук М. В. Аналіз масштабів та основні напрями мінімалізації ризиків шахрайства членів міжнародних платіжних систем. *Ефективна економіка*. 2013. № 6. URL: http://www.economy.nayka.com.ua/?op=1&z=2120 (дата звернення: 05.09.2025).

254. Хижняк Є. С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf (дата звернення: 12.09.2025).

255. Ціркаль В. В. Тактика проведення обшуку з участю фахівців. *Вісник Київського національного університету імені Тараса Шевченка*. Серія «Юридичні науки». 2002. С. 45–48.

256. Чаплинський К. О. Організація і тактичні прийоми проведення одночасних обшуків. *Науковий вісник Юридичної академії Міністерства внутрішніх справ*. 2004. № 3 (17). С. 338–344.

257. Чаплинський К. О. Тактичне забезпечення проведення слідчих дій : монографія. Дніпропетровськ : Дніпропетр. держ. ун-т внутр. справ ; Ліра ЛТД, 2010. 560 с.

258. Чаплинський К. О., Єфімов М. М., Жилін А. Е. Методика розслідування шахрайства у сфері використання банківських електронних платежів : монографія. Одеса : Юридика, 2024. 218 с.

259. Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : автореф. дис. … д-ра юрид. наук : 12.00.09 / Нац. акад. внутр. справ. Київ, 2010. 36 с.

260. Чернявський С. С. Теоретичні та практичні основи методики розслідування фінансового шахрайства : дис. … д-ра юрид. наук : 12.00.09 / Нац. акад. внутр. справ. Київ, 2010. 610 с.

261. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : монографія. Київ : Хай-Тек Прес, 2010. 610 с.

262. Черняховський Б. В. Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 2. С. 58–68.

263. Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів: наукові засади та напрями реалізації. *Сучасні тенденції розвитку криміналістики та кримінального процесу* : тези доп. Міжнарод. наук.-практ. конф. до 100-річчя від дня народження проф. М. В. Салтевського (м. Харків, 08 листоп. 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2017. С. 220–222.

264. Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів : монографія. Вінниця : Нілан-ЛТД, 2017. 492 с.

265. Чучко С. В. Використання спеціальних знань при розслідуванні шахрайств при купівлі-продажу товарів через мережу Інтернет. *Право і суспільство*. 2021. № 2. С. 234–240.

266. Чучко С. В. До питання взаємодії слідчих та оперативних підрозділів при розслідуванні шахрайства за фактом купівлі-продажу товарів через мережу Інтернет. *Актуальні проблеми кримінально-правового, кримінально-процесуального та криміналістичного забезпечення безпеки України та світу* : матеріали Міжнарод. наук.-практ. конф. (м. Дніпро, 27 листоп. 2020 р.). Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2020. С. 202–205.

267. Чучко С. В. Оцінка первісної інформації та коло обставин, що підлягають встановленню під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет : окремі аспекти. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. № 3. С. 304–310.

268. Чучко С. В. Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет : дис. … д-ра філос. : 081 – Право / Дніпропетр. держ. ун-т внутр. справ. Дніпро, 2021. 276 с.

269. Шевчук В. М. Слідча ситуація: повнота, структура, види та її значення для оптимізації розслідування злочинів. *Юридичний науковий електронний журнал*. 2014. № 1. С. 142–150.

270. Школа С. М. Правові засади профілактичної роботи національної поліції України. *Актуальні проблеми вітчизняної юриспруденції*. 2016. № 3. С. 129–132.

271. Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : автореф. дис. … д-ра юрид. наук : 12.00.09 / Нац. юрид. ун-т ім. Ярослава Мудрого. Харків, 2011. 32 с.

272. Юридична психологія : підручник / за заг. ред. Л. І. Казміренко,

Є. М. Моісеєва. Київ : КНТ, 2007. 360 с.

273. Як вберегти техніку від шкідливого програмного забезпечення – поради кіберполіції. URL: https://cyberpolice.gov.ua/article/yak-vberegty-texniku-vid-shkidlyvogo-programnogo-zabezpechennya--porady-kiberpolicziyi-4344/ (дата звернення: 18.09.2025).

274. Яременко О. І. Сучасне праворозуміння відносин в інформаційній сфері та методологія їх систематизації. *Інформація і право*. № 3 (22). 2017. С. 30–42.

275. Яровенко Г. М., Ковач В. О. Моделювання портретів потенційних шахрая та жертви банківських шахрайств. *Ефективна економіка*. URL: http://www.economy.nayka.com.ua/pdf/10_2018/63.pdf (дата звернення: 05.09.2025).

276. Chaplynskyi, K., Yefimov, M., Pletenets, V., Harashchuk, D., Demchenko, I. Features Of Interaction Between Law Enforcement Agencies During The Investigation Of Criminal Offenses According To International Standards. Cuestiones Politicas. 2023. Volume 41. Issue 76. pp. 469–481.

277. Chuchko, S. Fraud methods, related to purchase of goods through the Internet. *Visegrad Journal on Human Rights*. 2019. 6 (volume 3). Pp. 234–238.

278. Clay, W. Computer Attack and Cyberterrorism : Vulnerabilities and Policy Issues for Congress. URL: https://digital.library.unt.edu/ark:/67531/metacrs6315/m1/1/ (дата звернення: 06.09.2025).

279. IEEE Standards Association (IEEE SA). URL: https://standards.ieee.org/products-services/regauth/oui36/index.html (дата звернення: 21.09.2025).

280. James, A. Lewis Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. URL: https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats (дата звернення: 16.08.2025).

281. Khamyha Yu. Financial pyramids as a type of financial fraud : theoretical-motivational aspect. *European Journal of Economics and Management*. 2020. Vol. 6. Issue 3. Pp. 15–22.

282. Louise, I. Shelley Organized Crime, Terrorism and Cybercrime. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/organized-crime-terrorism-and-cybercrime (дата звернення: 06.09.2025).

283. Mihir, Bellare Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements. Springer Berlin Heidelberg, 2000. 274 p.

284. Reznik, O., Fomenko, A., Melnychenko, A., Pavlova, N., Prozorov, A. Features Of The Initial Stage Of Investigating Fraud With Financial Resources In Cyberspace. *Amazonia Investiga*. 2021. Volumer10 . Issue 41: pp. 141–150.

285. Sysoliatin, V. Problematic Aspects Of The Initial Phase Of Criminal Investigation Offences Involving Internet Banking. *Entrepreneurship, Economy and Law*. 2023. № 5. Pp. 112–117.

286. Tanczer, L. M. (2017) The Terrorist – Hacker/Hacktivist Distinction:

An Investigation of Self-Identified Hackers and Hacktivists. NATO Science for Peace and Security Series – E : Human and Societal Dynamics, Volume 136, pp. 77–92. URL: https://ebooks.iospress.nl/volumearticle/46545 (дата звернення: 13.09.2025).

287. Yefimov, M., Pavlova, N., Fedchenko, V., Pletenets, V., Kryvopusk, O. Foreign Experience In Legal Regulation Of Fraud Investigation. *Revista De La Universidad Del Zulia*. 2022.13 (38). Pp· 159–168.

288. Yefimov, M., Omarov, Y. Scientific Debates On The Preventive Activities Of Authorized Persons As Part Of The Methodology For Investigating Criminal Offences Against Morality. *Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs*. 2021. Special Issue № 1 (114). Pp. 114–119.

Наукове видання

ВИХОДЕЦЬ Юрій Олександрович
ДРОЗД Валентина Георгіївна
ЄФІМОВ Микола Миколайович
КОБА Валерій Борисович
ЛУГОВИЙ Ігор Олександрович
ПАВЛОВА Наталя Валеріївна
ЧАПЛИНСЬКИЙ Костянтин Олександрович

Теоретичні та праксеологічні засади розслідування кримінальних правопорушень у кіберпросторі

Монографія

Редагування *Т. В. Каленіченко-Соловей*
Комп'ютерне верстання

Підп. до друку 12.12.2025. Формат 60х84/16. Друк – цифровий. Папір офісний.
Гарнітура – Times. Ум.-друк. арк. 12,32. Обл.-вид. арк. 13,25. Зам. № 09/25-м

Надруковано у Дніпровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Науки, 26, sed@dduvs.edu.ua
Свідоцтво про внесення до Державного реєстру видавців ДК № 8112 від 13.06.2024