МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ОРГАНІЗАЦІЯ РОЗКРИТТЯ ШАХРАЙСТВ, УЧИНЕНИХ В КІБЕРПРОСТОРІ

Монографія

За загальною редакцією
доктора юридичних наук, професора,
Заслуженого юриста України, полковника поліції
Вітвіцького С. С.

КИЇВ • АЛЕРТА • 2023

УДК 343.98:004 (477)(02)
О-64

Рекомендовано до друку Вченою радою
Донецького державного університету внутрішніх справ
(протокол № 2 від 26.09.2023 року)

Рецензенти:
Тетерятник Ганна – завідувач кафедри кримінального процесу Одеського державного університету внутрішніх справ, доктор юридичних наук, професор;
Кисельов Андрій – доцент кафедри оперативно-розшукової діяльності Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент.

О-64 Організація розкриття шахрайств, учинених в кіберпросторі : монографія / Шевчишен А. В., Романов М. Ю., Волобоєв А. О., Лунгол О. М., Габорець О. А., Головкін С. В.; за заг. ред. С. С. Вітвіцького. Київ: Алерта, 2023. 200 с.

ISBN 978-617-566-803-0

Монографія присвячена теоретичному узагальненню та новому вирішенню наукового завдання стосовно комплексного аналізу та наукового обґрунтування засад організації розкриття шахрайств, учинених в кіберпросторі. Визначено стан наукових досліджень проблем організації розкриття шахрайств, учинених в кіберпросторі. Розкрито зміст оперативно-розшукової характеристики. Конкретизовано процес оцінки первинної інформації, коло обставин, що підлягають встановленню, планування та взаємодії, а також організаційно-тактичне забезпечення розкриття шахрайств, учинених в кіберпросторі. З'ясовано основні напрями розкриття шахрайств, учинених в кіберпросторі, та отримання інформації з відкритих джерел (OSINT).

Призначена для використання в практичній і науково-дослідній діяльності та в освітньому процесі.

УДК 343.98:004 (477)(02)

ISBN 978-617-566-803-0

Відомості про авторів

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.

Романов Максим Юрійович – заступник начальника управління організації наукової діяльності та інновацій – начальник організаційно-наукового відділу Департаменту освіти, науки та спорту Міністерства внутрішніх справ України, доктор філософії в галузі права, майор поліції.

Волобоєв Артур Олегович – завідувач кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ, доктор філософії в галузі права.

Лунгол Ольга Миколаївна – доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ, кандидат педагогічних наук.

Габорець Ольга Андріївна – доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету підготовки фахівців для підрозділів кримінальної поліції Донецького державного університету внутрішніх справ, доктор філософії в галузі педагогіки.

Головкін Сергій Вікторович – доцент кафедри поліцейської діяльності Луганського навчально-наукового інституту імені Е. О. Дідоренка Донецького державного університету внутрішніх справ, кандидат юридичних наук, доцент.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

МВС України	–	Міністерство внутрішніх справ України
НПУ	–	Національна поліція України
ОГП	–	Офіс Генерального прокурора
ДКІБ	–	Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України
ДКП	–	Департамент кіберполіції Національної поліції України
КК України	–	Кримінальний кодекс України
КПК України	–	Кримінальний процесуальний кодекс України
ЄРДР	–	Єдиний реєстр досудових розслідувань
СРД	–	Слідчі (розшукові) дії
НСРД	–	Негласні слідчі (розшукові) дії
ОРЗ	–	Оперативно-розшукові заходи

ПЕРЕДМОВА

У крок з сучасним етапом цифрової трансформації суспільства та викликів гібридної війни проти України зросла питома вага злочинної діяльності у віртуальному просторі. Суспільні відносини, що відбуваються в такому середовище, все частіше стають об'єктом для порушення прав громадян на володіння, користування і розпорядження своєю власністю, а також результатами своєї інтелектуальної та творчої діяльності. Як результат, форми правовідносин в Інтернеті залишаються не досить врегульованими, зростає кількість протиправних діянь, порушуючи основоположні приписи статті 41 Конституції України (далі – КУ).

За статистичними даними Офісу Генерального прокурора (далі – ОГП), протягом останніх п'яти років у середньому реєструється 204,7 тис. кримінальних правопорушень проти власності, де шахрайство займає друге місце після вчинення крадіжок. У 2018 році зареєстровано 33,2 тис. кримінальних правопорушень, пов'язаних із шахрайством; у 2019 році – 32,3 тис.; у 2020 році – 26,8 тис.; у 2021 році – 23,8 тис.; у 2022 році – 32 тис. (Додаток Б). З них, близько 12 % становить досліджувана категорія злочину, – шахрайство, учинене шляхом незаконних операцій з використання електронно-обчислювальної техніки (Додаток В).

Оцінити реальні масштаби таких шахрайських проявів вкрай важко через високу латентність, особливості обстановки їх вчинення та тонку межу між цивільно-правовими і кримінально-правовими відносинами, що ускладнює прийняття правильного рішення про притягнення особи до відповідальності в міру своєї вини. Тим паче, в період військової агресії спостерігається тенденції до збільшення злочинних схем, що реалізовуються за допомогою електронно-обчислювальної техніки у віртуальному просторі, а рівень їх розкриття залишається достатньо низьким, що свідчить про безсистемну протидію цьому Національної поліції України.

Так, середній показник розкриття шахрайств, учинених шляхом незаконних операцій з використанням електронно-обчислювальної техніки у порівнянні з видовим кримінальним правопорушенням становить 14,17 %, у співвідношенні до кримінальних правопорушень проти власності 1,47 %, стосовно загальної кількості облікових кримінальних правопорушень 0,72 % (Додаток Г).

Окремо слід звернути увагу на кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що у деяких випадках є джерелом для реалізації способів шахрайств у кіберпросторі та досягнення бажаного результату – заволодіти майном або правом на це майно. Середній показник за звітний період ілюструє 2,7 тис. зареєстрованих кримінальних правопорушень, де у 71 % випадків повідомлено про підозру, з них 85,8 % – матеріали кримінальних проваджень спрямовані до суду. Залишаються нерозкритим близько 35 % таких злочинних проявів (Додатки Б, В).

Вказане безсумнівно ставить перед наукою завдання щодо розробки новітніх прийомів, методів і засобів розслідування кримінальних правопорушень, що вчиняються у віртуальному просторі (середовище).

У нашому контексті важливим є узагальнення наукових ідей і підходів до створення якісного нового механізму організації розкриття шахрайств, учинених в кіберпросторі.

Як правило, вивчення шахрайства як негативного суспільного явища є предметом досліджень науковців різних галузей знань. Із-поміж науковців соціальних поведінкових наук слід відзначити О. В. Кравченка, О. М. Кулініча, С. С. Мельника, О. М. Залєтова, Т. О. Петрішину. Серед учених науки кримінального права та кримінології значний внесок у дослідження цієї проблематики зробили Р. А. Запорожець, О. Г Кальман, П. М. Коваленко, В. Р. Мойсик, В. В. Пивоваров, О. В. Смаглюк, Г. М. Чернишов, Ю. Л. Шуляк та ін.

Загальні питання розслідування та розкриття окремих видів шахрайств досліджували у своїх працях: А. І. Анапольська, Г. С. Бідняк, С. В. Головкін, Є. В. Дехтярьов, С. М. Князєв, С. С. Кузьменко, Х. М. Михайлова, Т. О. Мудряк, О. Л. Мусієнко, Т. В. Охрімчук, Н. В. Павлова, Д. А. Птушкін, І. Г. Проскурняк, С. С. Чернявський, М. В. Яцков та ін.

Окремі питання розслідування та розкриття кримінальних правопорушень, що вчиняються в сфері інформаційних технологій та з використанням електронно-обчислювальної техніки були предметом дослідження таких вітчизняних та іноземних учених, як: Ю. П. Аленіна, Д. С. Азарова, Б. В. Андрєєва, І. В. Басистої, В. П. Бахіна, В. Д. Берназа, Р. С. Бєлкіна, М. С. Вертузаєва, О. І. Возгріна, А. Ф. Волобуєва, В. І. Гагаліна, В. Г. Гончаренка, В.О. Голубєва, О. М. Джужі, Л. Я. Драпкіна, В. А. Журавля, А. В. Іщенка, О. В. Кириченка, В. О. Коновалової, В. В. Крилов, Л. М. Лобойка, В. Г. Лукашевича, Є. Д. Лук'янчикова, С. І. Мічнека, О. В. Одерія, М. А. Погорецького, М. В. Салтевського, О. В. Смаглюка, Р. Л. Степанюка, М. П. Стрельбицького, В. Є. Тарасенка, Р. В. Тарасенка, В. М. Тертишника, В. В. Тіщенка, Л. Д Удалової, І. Ф. Хараберюша, М. С. Цуцкірідзе, К. О. Чаплинського, В. В. Шедрика, В. Ю. Шепітька, М. Г. Щербаковського, О. М. Юрченка та ін.

Особливу увагу заслуговують сучасні дослідження шахрайств, учинених через мережу Інтернет, таких учених, як: С. В. Самойлова («Розслідування шахрайств, учинених із використанням мережі «Інтернет», Донецьк 2014 рік), О. В. Герасимова («Протидія злочинності у банківській сфері», Харків 2019 рік), О. А. Самойлека («Основи методики розслідування злочинів, вчинених у кіберпросторі», Одеса 2020 рік), О. В. Ковальчук («Методика розслідування шахрайств, пов'язаного з діяльністю кредитної спілки», Львів 2020 рік), Т. В. Коршикової («Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки», Київ 2021 рік), С. В. Чучкі («Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет,

Дніпро 2021 рік), І. О. Коваленка («Розслідування шахрайств у сфері використання банківських електронних платежів», Дніпро 2022 рік) та ін.

З огляду на це вважаємо, що багато результатів проведених досліджень спрямовані на удосконалення розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки, проте опубліковані роботи не вирішили всіх нагальних питань організації розкриття шахрайств, тим паче вчинених в кіберпросторі, що обумовлює вибір зазначеної теми, як достатньо актуальної для монографічного дослідження.

Розділ 1
ТЕОРЕТИКО-ПРИКЛАДНІ ЗАСАДИ РОЗКРИТТЯ ШАХРАЙСТВ, УЧИНЕНИХ В КІБЕРПРОСТОРІ

1.1. Стан наукових досліджень проблем організації розкриття шахрайств, учинених в кіберпросторі.

Тенденція цифрової трансформації у світі є невід'ємною частиною розвитку сучасного суспільства. Ця трансформація передбачає перехід від традиційних методів до цифрових технологій в різних сферах життя, включаючи економіку, освіту, охорону здоров'я, комунікації та багато інших. За останні десятиліття цифрова трансформація дуже активно набуває обертів. Однією з ключових характеристик є збільшення доступності та швидкості обміну інформацією завдяки широкому поширенню Інтернету та мобільних технологій. Це впливає на спосіб, яким люди переважно спілкуються, працюють, навчаються та розважаються. Цифрова трансформація також передбачає впровадження автоматизованих та інтелектуальних систем у бізнес-процеси. Штучний інтелект, аналітика даних, хмарні технології та інші інновації допомагають оптимізувати виробничі процеси, знижувати витрати та підвищувати якість послуг. Як результат, цифрова трансформація визначає сучасний спосіб життя та роботи, ставши каталізатором розвитку суспільства в напрямку більш ефективного та зручного використання технологій.

Цифровий розвиток, окрім безлічі позитивних аспектів, викликав збільшення небезпек для користувачів. Зростаюча залежність від цифрових технологій прямо пропорційно призводить до збільшення кіберзагроз. До основних причин збільшення кібернебезпек ми відносимо:

– зростання кількості даних та їх значущості, оскільки сучасне суспільство генерує величезні обсяги даних, що включають особисті, фінансові та інші конфіденційні відомості. Це робить їх привабливими для

кіберзлочинців, які можуть використовувати інформацію для вчинення злочинів, таких як шахрайство, крадіжка особистої ідентичності тощо;

– розвиток Інтернету речей (англ. Internet of Things, IoT), спричинив значне збільшення підключених до Інтернету пристроїв: від розумних телефонів та домашніх пристроїв до медичних інструментів та обладнання бізнес-центрів. Це створює більше можливостей для потенційних кібератак;

– різноманіття програмного забезпечення, оскільки зі зростанням обсягів та видів програмного забезпечення стає важче відстежити всі можливі вразливості. Це дає злочинцям змогу знаходити і використовувати слабкі місця програм та додатків, якими активно користуються певні категорії;

– можливість анонімності, віддаленої роботи та невідстежуваності, що дозволяє вчиняти кібератаки з різних частин світу;

– активний розвиток соціальної інженерії та фішингу, коли злочинці використовують психологічні методи, щоб здобути доступ до конфіденційної інформації;

– застосування можливостей штучного інтелекту, блокчейну та інших передових технологій для здійснення кібератак.

Особливість розкриття шахрайств, учинених у кіберпросторі, полягає в тому, що ці злочини відбуваються в електронному середовищі, і це викликає певні труднощі у відстеженні та ідентифікації. В Законі України «Про основні засади забезпечення кібербезпеки України»[1] (далі – ЗУ) дефініція кіберпростору визначена наступним чином: «кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних».

[1] Про основні засади забезпечення кібербезпеки України : закон України від 17.08.2022 № 2163-VIII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

Поняття «кіберпростір» може використовуватися для позначення не тільки технічного інфраструктурного середовища, але й соціокультурного, політичного та економічного простору, який об'єднує цифрову взаємодію між людьми, організаціями та системами. Тому науковці по-різному тлумачать поняття «кіберпростір», внаслідок чого існує певна термінологічна невпорядкованість щодо самого поняття «кіберпростір» і поєднаних понять, як «кіберзлочин», «кіберзлочинність», «кіберрозвідка», «кібертероризм», «кібершпигунство» тощо. Загалом, термін «кіберпростір» ввів у використання Уїльям Гібсон, американський письменник наукової фантастики, в своєму романі «Neuromancer», опублікованому в 1984 році. Цей термін описував віртуальне середовище, яке складається з комп'ютерних систем, мереж та інших цифрових ресурсів, де відбуваються комунікації, обмін даними та інші дії, що мають цифровий характер. Сучасні науковці дають наступне визначення дефініції «кіберпростір». Так, О. О. Балакінська[2] зазначає, що кіберпростір – це новий канал для створення і поширення різноманітної інформації, який став новим двигуном зростання економіки, новою платформою соціального управління, новим способом міжнародного співробітництва, до того ж і зовсім новою сферою державного суверенітету. Науковиця звертає увагу, що забезпечення безпеки в кіберпросторі не обмежується лише державними регуляторами та контролем; часто воно покладається на усвідомлену та відповідальну поведінку учасників правовідносин, зокрема суб'єктів господарювання. Виклик для безпеки в кіберпросторі в першу чергу виникає через зростаючий інтерес кіберзлочинців до ринку криптовалют та електронної комерції. Вони вдосконалюють методи атак, зокрема викрадення електронних грошей, нерідко від самого власника, чи використовують наявні ресурси, такі як гаманці, біржі та інші, для досягнення своїх цілей.

Відповідно до ДСТ України ISO/IEC 27032:2016 кіберпростір є складним середовищем взаємодії людей, програмного забезпечення та послуг у мережі

[2] Бакалінська О. О. Правове забезпечення кіберзахисту в Україні. *Платформа стратегічної та законотворчої аналітики. Серія «Право власності»*. 2020. URL: https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini.

Інтернет та функціонує за підтримки об'єднаних мереж і пристроїв інформаційних та комунікаційних технологій. Головну увагу цього стандарту приділено вирішенню проблем безпеки в кіберпросторі (так званої кібербезпеки), які виникають унаслідок прогалин у безпеці різних частинах кіберпростору. Цей стандарт містить технічні рекомендації для подолання ризиків кіберпростору, зокрема: атаки соціальної інженерії; злам (хакінг); поширення шкідливого програмного забезпечення («шкідливих програм»); шпигунські програми; інші потенційно небажані програми[3].

Науковці О. Г. Данильян та О. П. Дзьобань[4] зазначають, що реальність позначена концептом «кіберпростір» стала одним з основних факторів соціокультурного середовища, особливим середовищем споживання, з яким пов'язані усі сфери суспільного життя – економічна, соціальна, політична, духовна. Крім того, поява кіберпростору сприяє формуванню глобального інфопростору, становлення «мережевого суспільства», основою функціонування якого стає генерування, обробка, передача та оновлення інформаційного соціокультурного простору.

Отже, кіберпростір має велике значення в сучасному світі, де віртуальна діяльність та обмін інформацією відіграють ключову роль в багатьох сферах життя. Але з іншого боку кіберпростір окрім можливостей, також несе в собі численні небезпеки, які можуть впливати на окремих громадян, організації та навіть держави.

Військова агресія російської федерації проти України з 24 лютого 2022 року[5] призвела до збільшення кількості та видів шахрайств, учинених в кіберпросторі. Так, за даними Департаменту кіберполіції Національної поліції України (далі – ДКП) у 2022 році припинено діяльність 23 організованих груп і

[3] ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 2018. Дата початку дії: 01.01.2018. Дата прийняття: 27.12.2016. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128.

[4] Данильян О. Г., Дзьобань О. П. Віртуальна реальність і кіберпростір як атрибути сучасного суспільства. *Інформація і право.* Вип. № 4 (35). 2020. С. 9–21.

[5] Про введення воєнного стану в Україні. Указ Президента України № 64 / 2022. *Президент України Володимир Зеленський: Офіційне інтернет-представництво.* URL: https://www.president.gov.ua/documents/642022-41397.

злочинних організацій, що діяли в кіберпросторі. До складу зазначених угруповань входив 81 учасник (23 організатори та 51 активний виконавець), якими вчинено 269 кримінальних правопорушень (у тому числі 240 тяжких та особливо тяжких), а саме: 178 – шахрайств, 59 – у сфері використання електронно-обчислювальних машин, 12 – у сфері обігу наркотичних засобів, 3 – за ст. 255 (Створення, керівництво злочинною спільнотою, а також участь у ній) Кримінального кодексу України (далі – КК України), 2 – крадіжок, 3 – у сфері господарської діяльності (легалізації (відмиванню) майна, одержаних злочинним шляхом), 1 – привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем. У 2022 році кіберполіцейськими здійснювалось супроводження 5 тис. кримінальних правопорушень, виявлено 2,3 тис. кіберзлочинів, повідомлено про підозру 1 тис. особам за вчинення 2,3 тис. кримінальних правопорушень. Затримано понад 100 кіберзлочинців, задокументовано та притягнуто до відповідальності 30 педофілів та 10 хакерів. До суду з обвинувальними актами скеровано 2,7 тис. кримінальних правопорушень за обвинуваченням 840 осіб[6].

Отже, активізація Інтернет-шахраїв, які маніпулюють вразливим населенням України, поширення обсягу кіберзлочинів, особливо шахрайства в Інтернеті – нагальна проблема, з якою веде боротьбу правоохоронна система нашої держави.

Проблемі розслідування шахрайств, які вчиняються в кіберпросторі, присвячена низка досліджень вітчизняних та зарубіжних науковців. Так, науковці Львівського державного університету внутрішніх справ М. Майстренко та І. Татарин досліджують етапи розслідування кібершахрайств. Вони визначають фіксацію виявлених слідів основоположним моментом під час розслідування шахрайств, вчинених із використанням інформаційних технологій[7]. Науковці зазначають, що для побудови належної і цілісної системи

[6] Звіт про результати роботи Департаменту кіберполіції у 2022 році. *Офіційний сайт Кіберполіції України*. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczi-969/.

[7] Майстренко М., Татарин І. Проблемні аспекти доказування шахрайств, вчинених у кіберпросторі. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція»*. Вип. № 52. 2021. С. 85–89. DOI: https://doi.org/10.32841/2307-1745.2021.52.19.

доказів, тобто перетворення невидимої інформації та слідів кіберзлочинів на докази, є проведення судової експертизи, наприклад, комп'ютерно-технічної. Предметом такої експертизи мають бути закономірності формування і дослідження комп'ютерних систем і руху цифрової інформації, дослідження фактів і обставин, пов'язаних із проявом цих закономірностей[8]. В. Коршенко стверджує, що ефективним способом виявлення слідів кіберзлочинів та формування на їх основі доказів є судова телекомунікаційна експертиза. Об'єктами телекомунікаційної експертизи виступають електронні комунікаційні системи, такі, як системи мобільних операторів зв'язку, телевізійні системи, радіо системи тощо; мобільні термінали, наприклад, телефони, смартфони, планшети та інші мобільні пристрої, із встановленим програмним забезпеченням; білінгові системи мобільних операторів, білінгові системи банків, системи державних реєстрів тощо; спеціалізовані технічні пристрої – станції активних перешкод, пульти керування доступом, програматори активних ключів для автомобілів та іммобілайзерів тощо[9]. Науковці М. П. Климчук, Ю. А. Комісарчук, С. І. Марко та Б. В. Стецик у результатах своїх напрацювань[10] описують алгоритм дій слідчого та прокурора щодо залучення експерта до проведення судової комп'ютерно-технічної експертизи при розкритті шахрайств, учинених в кіберпросторі. Вони конкретизують методику проведення судової комп'ютерно-технічної експертизи та проводять аналіз типових помилок при проведенні подібного роду експертизи.

На активізації шахрайств у кіберпросторі внаслідок воєнного стану наголошують і науковці Національного юридичного університету імені Ярослава Мудрого[11]. Т. А. Діброва, Д. О. Пісенко та М. В. Сметаніна у

[8] Майстренко М., Татарин І. Проблемні аспекти доказування шахрайств, вчинених у кіберпросторі. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція».* Вип. № 52. 2021. С. 85–89. DOI: https://doi.org/10.32841/2307-1745.2021.52.19.

[9] Коршенко В. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *National law journal: theory and practice.* Вип. № 2. 2017. С. 197–199.

[10] Климчук М. П., Комісарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні: навч. посіб. Львів: Львівський державний університет внутрішніх справ, 2022. 112 с.

[11] Діброва Т. А., Пісенко Д. О., Сметаніна М. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний журнал.* Вип. № 11. 2022. С. 546–549. DOI: https://doi.org/10.32782/2524-0374/2022-11/132.

результатах своїх досліджень виділяють найбільш поширені схеми шахрайств у воєнний час, такі, як пропозицію оренди неіснуючого чи вже зайнятого житла для осіб, які були вимушені покинути власні домівки через небезпеки воєнних дій, фейкові перевезення та неіснуючі квитки переїзду, підробні талони на паливо, маніпуляції з продажу актуальних під час війни товарів, різного роду збори у соціальних мережах на допомогу військовим або постраждалим особам, імітація можливості отримання грошової допомоги тощо.

Розслідуванню нових форм кіберзлочинності (фішингу та кіберсквотінгу) присвячені роботи Т. П. Яцика та В. А. Шкелебей[12]. Науковці зазначають, що важливо розробити на національному рівні стратегію для боротьби з кіберзлочинністю, яка буде містити конкретні заходи ефективної боротьби та профілактики, спрямовані на зниження ризику вчинення злочинів, нейтралізацію потенційно шкідливих наслідків як для окремих осіб, так і суспільства загалом.

Дослідженню проблеми розкриття шахрайств, учинених в кіберпросторі, присвячена низка робіт зарубіжних науковців. Так, науковці з Індії Ч. Р. Неха та П. Шрілеакха досліджують кібершахрайства у банківській системі. Автори пропонують концептуальну основу запобігання внутрішньому кібершахрайству, задля створення надійного середовища у банківській екосистемі, шляхом своєчасного та швидкого виявлення кібершахрайств. Науковці стверджують, що їх інноваційний підхід до запобігання кібершахрайству, керований інсайдерами, швидко виявляє шахрайство, визначає його пріоритети та основні причини, а потім пропонує стратегії для забезпечення економічно ефективної банківської екосистеми[13].

І. Кара та М. Айдос вказують на способи боротьби із програмами-вимагачами в Інтернет-просторі[14]. Дослідники зазначають, що широке

[12] Yatsyk T. P., Shkelebei V. A. Investigation of new forms of cyber crime (phishing and cybersquatting). *Науковий вісник УжНУ. Серія: Право.* Вип. 53. Т. 2. 2018. С. 121–123.

[13] Neha Chhabra Roy, Sreeleakha Prabhakaran. Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritization and prevention. *Aslib Journal of Information Management.* Vol. 75, Issue 2. 2023. URL: https://www.emerald.com/insight/content/doi/10.1108/AJIM-11-2021-0339/full/html.

[14] Kara I. and Aydos M. Cyber Fraud: Detection and Analysis of the Crypto-Ransomware. *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA.* 2020. Pp. 0764-0769. Doi: 10.1109/UEMCON51285.2020.9298128.

використання віртуальних грошових одиниць (таких як Bitcoin, Ethereum, Ripple, Litecoin), призводить до активної розробки та використання програм-вимагачів задля викрадення віртуальної валюти. У більшості випадків програмне забезпечення-вимагач проникає в систему жертви за допомогою певних методів і шифрує файли в системі користувача. Після шифрування кіберзлочинець залишає повідомлення з вимогою викупу у віртуальній валюті за відкриття доступу до зашифрованих файлів і попереджає, що в іншому випадку файли будуть недоступні або видалені. І. Кара та М. Айдос[15] зазначають, що наразі програми-вимагачі становлять одну з найбільших загроз інформаційній безпеці.

Дослідники університету Ахмада Дахлана вказують на збільшення кількості Інтернет-користувачів в Індонезії на 175,4 мільйона та на 4,83 мільярда у всьому світі[16], що впливає на збільшення кількості випадків кібершахрайства. Провадження про кібершахрайства вимагають нової структури для розслідування, оскільки в таких провадженнях існують цифрові докази, які дуже легко пошкодити, втратити або змінити. В організації розкритті шахрайств, учинених в кіберпросторі Х. Нур, Аніса, Ріаді, Р. Імам, А. Еріка та Сара[17] пропонують використовувати метод розробки концептуальної структури Jabareen. Термін «структура Jabareen» ввів науковець Махмуд Халіль Джабарін для описування концептуальних структур у наукових дослідженнях. Ця концепція структури допомагає аналізувати взаємозв'язки між елементами досліджуваної теми та розкривати їхні взаємодії й характеристики. Структура Jabareen включає три основні рівні:

– рівень ядра (Core level) – це базові елементи або поняття, які складають основу дослідження. Це ключові аспекти теми, які є найважливішими для розуміння;

[15] Nur H., Anisa, Riadi, Imam R., Erika A., Sarah. Development of conceptual framework for cyber fraud investigation. *Jurnal Ilmiah Teknologi Sistem Informasi.* 7. 2021. Pp.125-135. Doi: 10.26594/register.v7i2.2263.

[16] Головні цифрові тенденції. *Datareporta.* URL: https://datareportal.com/.

[17] Nur H., Anisa, Riadi, Imam R., Erika A., Sarah. Development of conceptual framework for cyber fraud investigation. *Jurnal Ilmiah Teknologi Sistem Informasi.* 7. 2021. Pp.125-135. Doi: 10.26594/register.v7i2.2263.

– рівень периферії (Periphery level) – цей рівень містить додаткові аспекти або поняття, які доповнюють та розширюють основні поняття з рівня ядра;

– рівень концентричних кілець (Concentric level) – на цьому рівні розташовані зовнішні аспекти, які можуть бути менш прямо пов'язані з темою, але все ще мають певний вплив на неї.

Структура Jabareen допомагає науковцям аналізувати аспекти досліджуваної теми та розкривати їхні взаємозв'язки, розробляти концептуальні моделі у різних галузях наукових досліджень.

Як результат використання структури Jabareen в організації розкриття кібершахрайств, науковці[18] виділяють 6 етапів, а саме: відображення вибраного джерела даних, детальна категоризація вибраних даних, проведення ідентифікації об'єктів, деконструкція та категоризація концепції, інтеграція концепції, синтез та ресинтез. За такою схемою, при розслідуванні кібершахрайств можливе використання 22 цифрових криміналістичних фреймворки та 8 фреймворків для розслідувань аудиту шахрайства.

Ч. Ванг та Х. Жу пропонують використовувати графічне виявлення поведінкових аномалій у кібербезпеці як один із засобів вирішення проблеми організації розкриття шахрайств, учинених в кіберпросторі[19]. Науковці стверджують, що так зване виявлення цифрових аномалій поведінки (BAD) ефективно вирішуватиме різноманітні проблеми безпеки в кіберпросторі шляхом виявлення відхилень від нормальних моделей поведінки роботи програм і додатків. Вони пропонують нову парадигму поведінкового моделювання на основі графів, що має явні переваги перед існуючими методами завдяки глибокому аналізу асоціацій на рівні властивостей у поведінкових даних, які моделюються як сутності та зв'язки графа відповідно. Крім того, поведінкові властивості та події контролюються за допомогою розробленої композиційної

[18] Nur H., Anisa, Riadi, Imam R., Erika A., Sarah. Development of conceptual framework for cyber fraud investigation. *Jurnal Ilmiah Teknologi Sistem Informasi.* 7. 2021. Pp.125-135. Doi: 10.26594/register.v7i2.2263.

[19] Wang C. and Zhu H. Wrongdoing Monitor: A Graph-Based Behavioral Anomaly Detection in Cyber Securit. *Transactions on Information Forensics and Security,* Vol. 17. 2022. Pp. 2703-2718. Doi: 10.1109/TIFS.2022.3191493.

моделі «подія – властивість». Представлена дослідниками[20] робота з удосконалення поведінкового моделювання для виявлення аномалій шляхом інтеграції внутрішніх (на рівні подій або властивостей) асоціацій поведінки в єдиний графік і простір може бути використана для виявлення шахрайства в сервісах онлайн-платежів (за поведінкою транзакцій), встановлення вторгнень у сервіси мережевого зв'язку (за поведінкою трафіку), визначення внутрішніх загроз в організаційних інформаційних системах (за поведінкою системи) та виявлення компрометації в соціальних мережах (за траєкторією поведінки).

Спільні міжнародні дослідження з розкриття шахрайств, учинених в кіберпросторі, є надзвичайно важливими в контексті сучасного цифрового світу. Ці дослідження впливають на різні аспекти суспільства, економіки та безпеки, і їх значущість є надзвичайно великою. Це обумовлено глобальним характером кіберзлочинів, оскільки вони не мають кордонів і можуть впливати на будь-яку країну чи організацію. Співпраця між різними країнами дозволяє краще розуміти та виявляти злочинців, які можуть діяти з різних кутів світу. Об'єднані зусилля дозволяють залучити велику кількість вчених, експертів і дослідників, що призводить до більш глибокого розуміння та аналізу різних аспектів кіберзлочинів. Спільні дослідження допомагають виявити нові методи та стратегії злочинців, а також прогнозувати їхні можливі дії. Це дозволяє адекватно реагувати на зміни у кіберзлочинності. Обмін знаннями про нові технології та методи захисту від кіберзлочинів сприяє підвищенню рівня кібербезпеки в різних країнах. Спільні дослідження сприяють обміну досвідом та найкращими практиками в розслідуванні кіберзлочинів, що значно покращує якість розкриття шахрайств і допомагає вчасно реагувати на нові загрози та події.

Такого роду спільні дослідження на міжнародному рівні проводять, наприклад, науковці з Пакистану, Нігерії, Кіпру, Саудівської Аравії, Єгипету та Норвегії[21]. Особливу увагу вони приділяють проблемі шахрайства та аномалій у

[20] Wang C. and Zhu H. Wrongdoing Monitor: A Graph-Based Behavioral Anomaly Detection in Cyber Securit. *Transactions on Information Forensics and Security,* Vol. 17. 2022. Pp. 2703-2718. Doi: 10.1109/TIFS.2022.3191493.

[21] Ashfaq T., Khalid R., Yahaya A.S., Aslam S., Azar A.T., Alsafari S., Hameed I. A. A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors.* 2022; 22 (19): 7162. https://doi.org/10.3390/s22197162.

мережі Bitcoin – це поширені проблеми в електронному банкінгу та онлайн-транзакціях. Науковці зазначають, що із розвитком фінансового сектора змінюються й методи шахрайства та аномалій. Хоча технологія блокчейн впроваджується як найбезпечніший метод, інтегрований у фінанси, однак разом із цими передовими технологіями з кожним роком зростає кількість випадків шахрайства. Як результат, дослідники пропонують безпечну модель виявлення шахрайства на основі машинного навчання та блокчейну та нову версію більш надійних смарт-контрактів на основі блокчейну, у якому розгортається модель машинного навчання для прогнозування характеру нових вхідних транзакцій[22]. Особливістю результатів дослідження виступає використання техніки балансування та обробки даних. Під час попередньої обробки дані поділяються на навчальний набір даних і тестовий набір даних. Для класифікації і прогнозування моделей транзакцій використовуються два алгоритми машинного навчання — XGboost і Random Forest (RF). Вони класифікують дані як шахрайські або не шахрайські. Обидва класифікатори передбачають тип даних. Ці моделі машинного навчання безпосередньо пов'язані з блокчейном. Модель блокчейну використовується для ініціювання транзакцій, а потім моделі машинного навчання використовуються для класифікації цих транзакцій як зловмисних або законних. Також дослідниками реалізовано дві моделі захисту від атак блокчейну.

Т. Арора, М. Шарма та С. К. Хатрі[23] пропонують використовувати Random Forest, але для виявлення кіберзлочинності в соціальних мережах. Дослідники акцентують увагу на тому, що розвиток Інтернет-технологій призвів до зростання кіберзлочинності, проблем із безпекою, збільшенням кількості зловмисників і хакерів. Особливу увагу звертають на платформи соціальних медіа, які набули величезної популярності, оскільки на сьогодні це

[22] Ashfaq T., Khalid R., Yahaya A.S., Aslam S., Azar A.T., Alsafari S., Hameed I. A. A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors.* 2022; 22(19): 7162. https://doi.org/10.3390/s22197162.

[23] Arora T., Sharma M., Khatri S. K. Detection of Cyber Crime on Social Media using Random Forest Algorithm. *2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC), Greater Noida, India.* 2019. Pp. 47–51. Doi: 10.1109/PEEIC47157.2019.8976474.

найефективніший спосіб спілкування та обміну інформацією. Понад мільярд користувачів підключені через соціальні мережі, і недостатня обізнаність щодо конфіденційності та безпеки призводить до збільшення кіберзлочинності. Алгоритм Random Forest можна використовувати для прогнозування та виявлення злочинів. Як результат, автори пропонують дієву модель для автоматичної класифікації загроз та виявлення кіберзлочинців у соціальних мережах.

У результаті спільних досліджень вчених з Ірландії та Іспанії[24] визначено алгоритми використання закону Бенфорда для виявлення кібератак в оцінювачах стану енергосистем. Закон Бенфорда, також відомий як Закон антиподібних розподілів та є статистичним законом, що описує нерівномірність цифр у списках чисел, які отримані з природних процесів або наборів даних. Згідно закону Бенфорда у числовому наборі перші цифри (від 1 до 9) не розподілені рівномірно, але мають певні статистичні властивості. Закон Бенфорда використовується в різних галузях, зокрема: фінанси і облік (деякі фінансові шахрайства можуть бути виявлені через порушення Закону Бенфорда у фінансових даних), дослідження даних (цей закон може бути застосований для перевірки автентичності даних та виявлення аномалій), аудит і контроль (закон Бенфорда може служити інструментом для перевірки точності фінансової звітності та виявлення можливих фактів шахрайства) та ін. Ф. Мілано та А. Гомес-Експозіто, зазначають, що важливою властивістю цього закону є його висока чутливість до маніпуляцій і, по суті, він часто використовується для виявлення шахрайств. Виходячи з цієї функції, актуальним є використання закону Бенфорда для виявлення шкідливих даних, внесених хакерами в систему диспетчерського контролю та збору даних.

Наукові дослідження проблеми організації розкриття шахрайств, учинених в кіберпросторі, мають велике значення в сучасному цифровому світі, де кіберзлочини та шахрайства стають все більш серйозними загрозами.

[24] Milano F., Gomez-Exposito A. Detection of Cyber-Attacks of Power Systems Through Benford's Law. *Transactions on Smart Grid,* Vol. 12, no. 3. 2021. Pp. 2741–2744. Doi: 10.1109/TSG.2020.3042897.

Проаналізовані нами дослідження в цій області націлені на розробку ефективних методів виявлення, аналізу та розкриття кіберзлочинів з метою запобігання та реагування на них. Сучасний стан наукових досліджень в цій області характеризується наступним:

1. Дослідники різних країн розуміють важливість розкриття шахрайств, учинених у кіберпросторі та розробки методів боротьби з ними. Вони вивчають різні типи кібершахрайств, їхні методи та наслідки, що допомагає визначити потребу в нових підходах до розкриття та виявлення цих злочинів.

2. У дослідженнях активно вивчаються сучасні технічні засоби для виявлення шахрайств, учинених у кіберпросторі. Це можуть бути програмні рішення для моніторингу мереж, аналізу великих обсягів даних (Big Data), використання штучного інтелекту та машинного навчання для виявлення аномалій.

3. Вітчизняні та зарубіжні дослідники розробляють методи й алгоритми аналізу підозрілих дій в кіберпросторі та профілактичні заходи для запобігання шахрайствам. Це включає розробку алгоритмів виявлення підозрілих активностей, створення баз даних з відомими сценаріями шахрайств та інше.

4. Дослідники поєднують знання з різних галузей, таких як інформаційна безпека, кібербезпека, кримінальна судова експертиза, техніка, статистика та інші. Це дозволяє більш комплексно розглядати проблему та розробляти ефективні стратегії розкриття шахрайств.

5. Дослідники співпрацюють з правоохоронними органами та органами державного управління для впровадження розробок в реальну практику. Це допомагає ефективно боротися з кібершахрайствами та розкривати їх.

Працювати на випередження для уникнення шахрайств, які можуть бути учинені в кіберпросторі, є критично важливим завданням для ефективної боротьби зі злочинами в цифровому середовищі та захисту індивідуальних, корпоративних і громадських інтересів. Випереджаючі заходи дозволяють попередити злочини та мінімізувати збитки, які можуть виникнути внаслідок шахрайств, учинених у кіберпросторі. Це особливо важливий фактор, оскільки

наслідки кібератак можуть бути серйозними і мати далекосяжні ефекти на особисту безпеку, фінансові активи, ділову репутацію, суспільний порядок тощо. Превентивні заходи допомагають захищати конфіденційну інформацію, яка може бути цільовою для кіберзлочинців. Доволі актуально в сучасному світі, де особисті та корпоративні дані мають велику цінність. Відкритість та вчасне реагування на можливі загрози допомагають зберегти довіру громадськості, споживачів та бізнес-партнерів. Випередження учинення шахрайств в кіберпросторі має бути засноване на дослідженні причин, методів та наслідків таких дій, що дозволить розробити ефективні стратегії та заходи для забезпечення кібербезпеки. З цією метою, наприклад, науковці Б. Абдулкадір та С. Руя[25] розробили систему управління діями та провели прикладне дослідження щодо її використання для запобігання кібершахрайству та аналізу ризиків. Розроблена система управління діями забезпечує виконання необхідних дій автоматично, щоб захистити користувачів від ризиків у кіберпросторі. Ця система самостійно визначає дії та обробляє їх у зручний для користувача спосіб. Система управління діями забезпечує швидкі й точні дії завдяки своїй гнучкій і модульній конфігурації та була апробована в телекомунікаційній компанії в Туреччині. Автори зазначають наступні переваги системи: скорочення часу прийняття рішень та черги очікування транзакцій, автоматизація процесу прийняття рішень, оптимізація використання ресурсів, скорочення експлуатаційних витрат, раціональне використання людських ресурсів, підвищення продуктивності, швидка адаптація до мінливих випадків.

Як результат проведеного аналізу досліджень вітчизняних та зарубіжних науковців, статистичних даних ДКП, ми виділили фактори, які сприяють зростанню кількості шахрайств, вчинених у кіберпросторі:

1. *Зростання використання Інтернету*, оскільки із популярністю Інтернету зростає і кількість користувачів, що надає злочинцям більше можливостей для цифрового шахрайства. Зростання використання Інтернету

[25] Abdulkadir B., Ruya S. An Action Management System Design and Case Study on Its Usage for Cyber Fraud Prevention and Risk Analysis. *Journal of Innovative Science and Engineering.* 2021. 5(2). Pp. 143–161.

відбувається через розширення цифрового простору внаслідок розвитку технологій, популяризації соціальних мереж, активності електронної комерції, розширення Інтернет-послуг, створення «цифрових» професій тощо. Сучасні технології, такі як смартфони, планшети та ноутбуки, стали більш доступними для широкого кола користувачів, що призвело до зростання популярності Інтернету, оскільки люди можуть з легкістю підключатися до нього. Все більшого попиту набувають соціальні мережі, оскільки вони дозволяють підтримувати зв'язки з друзями, сім'єю та колегами, навіть на великій відстані, популяризувати себе або власний бізнес. Це спонукає багатьох людей постійно перебувати в онлайн-середовищі. Зростає популярність онлайн-магазинів і сервісів для купівлі-продажу товарів та послуг. З'являються різноманітні Інтернет-послуги, такі як онлайн-навчання, трансляції відео, геймінг, що забезпечує більше можливостей для розваг, навчання та розвитку у зручний для користувача час. Бізнес та робочі процеси все більше переходять в онлайн-режим, включаючи відеоконференції, віддалену роботу та онлайн-інструменти співпраці. Розширена доступність Wi-Fi покриття і швидкого Інтернет-з'єднання робить Інтернет більш доступним для соціуму.

2. *Технічний розвиток* безумовно вплинув на збільшення шахрайств, учинених у кіберпросторі. З ростом доступності комп'ютерів, смартфонів та іншого технічного обладнання з'явилося більше можливостей для кіберзлочинців вчиняти злочини в онлайн-середовищі. Швидке та стабільне Інтернет-з'єднання дозволяє кіберзлочинцям здійснювати атаки незалежно від місцезнаходження. Інтернет-платіжні системи та онлайн-магазини роблять шахрайства з використанням фінансових даних більш доступними та простими для виконання. З'являються потужні кіберінструменти, які дозволяють виконувати складні атаки навіть людям з мінімальними технічними знаннями. Через розвиток технологій майже кожна сфера має онлайн-присутність – це збільшує вектори атак та можливості для кібершахрайств. Нові технології дозволяють кіберзлочинцям легко приховати свою ідентичність та залишити мінімальний цифровий слід, що ускладнює виявлення та покарання. Злочинці

зацікавлені до використання нових технологій, оскільки бачать можливість отримати значний прибуток з вчинення кіберзлочинів новими способами та засобами.

3. *Анонімність та віддаленість* дозволяє кіберзлочинцям діяти анонімно та з будь-якої точки світу, що робить їхнє виявлення та припинення дій складним завданням. Анонімність та віддаленість грає значущу роль у вчиненні кіберзлочинів і охоплює такі аспекти, як складність відстеження, використання інструментів для збільшення анонімності, псевдоніми тощо. Кіберзлочинці активно використовують віртуальні приватні мережі (VPN) для приховання своєї реальної IP-адреси та ускладнення виявлення, анонімні браузери, які не зберігають історію перегляду та особисті дані, а також криптовалюти для анонімних транзакцій. За допомогою соціальних мереж та форумів із використанням псевдонімів, кіберзлочинці можуть активно вести протиправну діяльність у кіберпросторі. Популярним є використання чужих гаджетів або злам профілів для вчинення шахрайств в кіберпросторі.

4. *Соціальна інженерія* – використання психологічних прийомів дозволяє злочинцям отримувати доступ до особистої інформації та даних користувачів, що активно використовується для учинення шахрайства в кіберпросторі.

1.2. Оперативно-розшукова характеристика шахрайств, учинених в кіберпросторі.

Теорія оперативно-розшукової діяльності, як наука, широко використовує моделі, які назагал можна представити у вигляді результатів аналізу та оцінки первинної інформації (відомостей), – опису реальних явищ, подій та систем.

З її розвитком відбувалось вироблення нових знань у галузі, насамперед, протидії різним видам злочинності з використанням оперативно-розшукових методів, форм та засобів, що призвело до появи різноманітних термінів, понять, категорій, які в подальшому потребували особливого підходу під час вивчення.

Одним із нових запроваджених термінів в оперативно-розшуковій діяльності вважається термін «оперативно-розшукова характеристика злочину».

Взагалі поняття «характеристика» є поширеним у різних сферах життя й науки. Її усвідомлюють як сукупність визначених параметрів об'єкта, явища в кількісному та якісному виявах. У словниках її тлумачать як опис, визначення суттєвих особливостей, ознак того-, чого-небудь[26].

У контексті нашого дослідження, актуальним є дослідити основні складові оперативно-розшукової характеристики як інформаційної моделі для розкриття шахрайств, учинених в кіберпросторі.

Загальні теоретичні аспекти оперативно-розшукової характеристики кримінальних правопорушень викладені в працях провідних учених-юристів: К. В. Антонова, А. В. Баб'яка, В. І. Василинчука, В. Б. Вишні, Д. В. Гбелельського, В. Я. Горбачевського, О. М. Джужі, Е. О. Дідоренка, В. П. Захарова, О. В. Кириченко, Д. Й. Никифорчуку, В. А. Некрасова, Ш. Л. Шелухіна, В. В. Шендрика та ін. За їхніми висновками оперативно-розшукову характеристику слід розглядати з позиції системного підходу через сукупність кримінально-правових, криміналістичних, кримінологічних, психологічних ознак злочинів, серед яких виділяють пошукові, які в сукупності формують більш глибоке уявлення про суб'єкт злочину, що дає змогу прийняти правильне рішення щодо застосування сил, засобів і заходів оперативно-розшукової діяльності, гарантують ефективне здійснення оперативно-профілактичних заходів.

Як пише В. Д. Пчолкіна, сутність оперативно-розшукової характеристики злочинів визначені в її кримінально-правових, криміналістичних, кримінологічних, психологічних та інших упорядкованих і взаємозалежних між собою ознаках, що мають розвідувально-пошуковий характер і розглядаються з позиції ефективності розкриття та розслідування злочинів[27].

---

[26] Василинчук В. І. Організаційно-правові та тактичні засади оперативно-розшукової профілактики злочинів у бюджетній сфері : навчальний посібник. Київ : Заграй, 2012. 210 С. 12.

[27] Пчолкін В. Д. Поняття характеристики злочинів у теорії оперативно-розшукової діяльності. *Вісник ЛАВС МВС України ім. 10-річчя незалежності України.* Спецвип. № 2 Ч. 1. 2004. С. 68.

Ми поділяємо позицію науковців, вважаємо доцільним дослідити оперативно-розшукову характеристику з огляду системного підходу взаємопов'язаних кримінально-правових, кримінологічних та криміналістичних ознак досліджуваного злочину.

Так, на думку М. А. Погорецького та В. П. Шеломенцева до складу цього інституту мають входити такі типові елементи, як відомості про: вид злочину та його суспільну небезпечність; предмет злочинного посягання та його пошукові ознаки; середовище вчинення злочину, особливості слідоутворення у ньому та специфіку фіксації слідів; способи готування до злочину та їх пошукові ознаки; способи вчинення злочину, їх пошукові ознаки та специфіку фіксації злочинних дій; способи приховання слідів злочину (маскування злочинних дій) та їх пошукові ознаки; типові знаряддя (засоби) вчинення злочинів та їх пошукові ознаки; типові обставини вчинення злочинів: місце, час, обстановка; сліди злочинів, їх пошукові ознаки та специфіку фіксації; типові джерела інформації про злочини цього виду; особу злочинця та його пошукові ознаки (зовнішні ознаки, психологічний портрет, особливості поведінки при готуванні, вчиненні злочину, а також після його вчинення тощо), типову мотивацію злочинної поведінки, чинники, що мали вплив на формування злочинної мети; склад та схема взаємозв'язків у злочинній групі; розподіл ролей між співучасниками тощо; потерпілу сторону (ознаки віктимності, відомості про спосіб життя, риси, характеристику, звички, зв'язки тощо); типові наслідки злочинів (матеріальна та моральна шкода, заподіяні злочином; зміни, викликані злочином у матеріальній обстановці тощо)[28].

На думку В. І. Василинчука оперативно-розшукова характеристика шахрайства має містити складові: кримінально-правової складової (предмет злочинного посягання, об'єкт, об'єктивна сторона, суб'єкт, суб'єктивна сторона); кримінологічної складової (стан, динаміка, форми вияву злочину, особа злочинця, причини й умови, що сприяють учиненню злочину);

[28] Погорецький М. А., Шеломенцев В. П. Поняття оперативно-розшукової характеристики злочинів. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* Вип. № 1 (47). 2010. С. 215–222.

криміналістичної складової (типові та оригінальні способи вчинення і маскування злочину, сліди його вчинення)[29].

А. М. Абрамов значно ширше визначає систему оперативно-розшукової характеристики, зокрема стосовно шахрайства визначає такі елементи:

1) кримінально-правові, – недоліки судочинства у провадженнях, де постановлені необґрунтовані вироки;

2) кримінологічні: рівень загального і спеціального рецидиву; стійкість окремих криміногенних груп і професіоналізація злочинів, прояв останніми агресивності при скоєнні злочинів, підвищений ступінь віктимності в поведінці потерпілого тощо.

Слід зазначити, що на думку автора означена складова значною мірою обумовлює специфіку всієї оперативної роботи.

3) криміналістичні: використання злочинцями різних прийомів і хитрощів при підготовці, здійсненні і приховуванні протиправних діянь, їх різновиди, структура, динаміка тощо;

4) морально-психологічні, тобто особливості особи злочинців і потерпілих, обізнаність злочинців з прийомами та методами оперативної роботи, характерні ознаки поведінки в кризових умовах тощо;

5) спеціальні: особливості використання негласних співробітників; обставини, що полегшують і ускладнюють в різних ситуаціях процес оперативної розробки; особи, які перебувають на оперативному обліку з числа раніше судимих, від яких можна очікувати вчинення злочинів[30].

Вочевидь чимало представників наукової спільності досліджували проблематику структури оперативно-розшукової характеристики шахрайства. Абсолютна їх більшість акцентували на її внутрішні взаємозв'язки структурних елементів та сутності цього кримінального правопорушення.

[29] Василинчук В. І. Оперативно-розшукова профілактика злочинів у бюджетній сфері: монографія. Київ: ФОП Кандиба, 2013. С. 147.

[30] Єгоров С. О. Оперативно-розшукова характеристика кишенькових крадіжок. *Науковий вісник Дніпропетровського університету внутрішніх справ.* Вип. № 3. Дніпро, 2019. С. 171.

Ураховуючи це, вбачаємо доцільним додатково розглянути питання сутності шахрайства в кіберпросторі як самостійного виду злочину.

Так, Міжнародна спільнота визначає класифікатор кіберзлочинів, розроблений Генеральним секретаріатом Інтерполу, що було покладено в основу автоматизованої інформаційно-пошукової системи створеної у 1991 році. Відповідно до цього класифікатора кіберзлочини мають певні кодифікатори, зокрема:

1) кодифікатор QA – незаконний доступ і перехоплення;

2) кодифікатор QD – зміна комп'ютерних даних;

3) кодифікатор QF – комп'ютерне шахрайство;

4) кодифікатор QR – незаконне копіювання;

5) кодифікатор QS – комп'ютерний саботаж;

6) кодифікатор QZ – інші комп'ютерні злочини[31].

До структури кодифікатора QF увійшли такі комп'ютерні шахрайства:

Шахрайство пов'язане з автоматами по видачі готівки (банкоматами) (кодифікатор QFC). Цей вид шахрайства полягає у маніпулюванні електронною інформацією, записаною на магнітному носії пластикової картки, отриманої шляхом обману або зловживанням довірою потерпілого.

Комп'ютерна підробка (кодифікатор QFF). Сутність цього шахрайства полягає у виготовленні підроблених засобів із застосуванням комп'ютерних технологій. Підроблятися може як програмне забезпечення або деталі електронно-обчислювальної техніки, так і підробка грошових банкнотів за допомогою сучасних лазерних принтерів.

Шахрайства пов'язані з ігровими автоматами (кодифікатор QFG). Програми, чіпи, за допомогою яких контролюється діяльність ігрових автоматів мають великий попит серед шахраїв у віртуальному середовищі, і становляться

[31] Viacheslav V. Vapniarchuk, Iryna I. Puchkovska, Oleksii V. Tavolzhanskyi, Roman I. Tashian Protection of ownership right in the court: the essence and particularities (Захист права власності в суді). *Asia life science, Supplement 21(2), December2019.* Iss. 2. P. 863-879. Філіпини. (Scopus). URL: https://www.scopus.com/record/display.uri?eid=2-s2.0- 85077221643&origin=resultslist.

об'єктом не тільки шахрайства, а також і несанкціонованого копіювання, заміни даних та крадіжки.

Шахрайства шляхом маніпулювання програмним забезпеченням (кодифікатор QFM). Вид шахрайства класифікується як введення чи виведення з комп'ютерної системи інформації, або маніпуляцією з комп'ютерними програмами. Програмне забезпечення, як предмет такого виду шахрайства можна виокремити наступним чином:

1) комп'ютерні програмні продукти для комерційного продажу;

2) безкоштовне експериментальне програмне забезпечення;

3) спеціальні комп'ютерні програми, написані для злочинних цілей[32].

Шахрайства пов'язані з платіжними засобами та системами реєстрації платежів (кодифікатор QFP). Предметом цього злочину виступають системи, що належать банкам, захищенні від стороннього доступу, оскільки ними передається інформація про переказ платежів, тобто усі різновиди магнітних карток.

Останню позицію займає *телефонне шахрайство* (кодифікатор QFT). Під телефонним шахрайством розуміється неправильне використання електронних комунікаційних послуг з метою уникнення від сплати рахунків за послуги чи уникнення підслуховування. Окремим видом телефонного шахрайства можна виділити дзвінки злочинця з метою заволодіння матеріальним благом шляхом обману чи зловживання довірою.

Відповідно до чинного законодавства України, шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою.

Шахрайство у формі заволодіння чужим майном – це обманне, протиправне і безоплатне вилучення чужого майна та обернення його на користь винної чи іншої особи, що спричиняє шкоду власнику майна. Для цієї форми шахрайства характерне:

[32] Пфо О. М. Основні поняття і класифікація кіберзлочинності. *Матеріали Всеукраїнської науково-практичної конференції «Актуальні задачі та досягнення у галузі кібербезпеки».* 2016. С. 32.

– дії (обман) шахрая спрямовані на безпосереднє заволодіння чужим майном (вилучення його з володіння власника);

– вилучення майна відбувається, як правило, негайно (у крайньому разі між обманом і вилученням майна проходить незначний час);

– вилучення майна завжди здійснює злочинець;

– потерпілий під впливом обману добровільно передає своє майно у володіння іншої особи;

– потерпілий на момент передачі майна не усвідомлює, що став жертвою злочину (був введений в оману)[33].

Обман може бути як активним, так і пасивним. Активний обман полягає у навмисному введені в оману шляхом повідомлення неправдивих даних, надання підроблених документів та вчинення інших дій, що створюють в особи помилкове уявлення про підстави передачі майна винному та викликають у неї впевненість у законності та необхідності цих дій. Пасивний обман полягає у приховуванні відомостей про юридично значущі фактичні обставини, повідомити які винний був зобов'язаний, унаслідок чого особа, яка передає майно, помиляється стосовно наявності законних підстав щодо цієї передачі.

Як приклад, П. С. Матишевський наводить такі види пасивного обману:

1) умисне замовчування винним обставин, що призвели до виникнення помилки потерпілого стосовно правомірності передачі майна винному;

2) свідоме використання чужої помилки (яка виникла без участі винного), що призвело до передачі майна винному[34].

Становить інтерес думка С. С. Чернявського, що обман може полягати у вчиненні конклюдентних дій, тобто поведінки особи, що виражає її волю встановити правовідносини, але не у формі усного чи письмового волевиявлення, а поведінкою, за якою можна дійти висновку про сам намір. Наприклад, застосування винним завідомо неправильних ваг, гір чи

[33] Пазинич Т. А. Особливості сучасних шахрайств та їх вплив на методику розслідування. *Вісник Луганського державного університету внутрішніх справ.* Вип. № 4. Луганськ : ЛДУВС, 2005. С. 126.

[34] Мельник С. С. Виявлення та запобігання фінансовому шахрайству у забезпеченні фінансової безпеки комерційних банків / С. С. Мельник : дис. ... канд. економ. наук. Київ, 2019. С. 43.

вимірювальних пристроїв; вживання товарів під виглядом готовності сплатити їхню вартість; зміну зовнішнього вигляду, форми чи властивостей різних предметів та видачу їх за інші предмети тощо[35].

Змістом обману як способу шахрайства можуть бути різноманітні обставини стосовно яких шахрай вводить в оману потерпілого. Зокрема, це може стосуватися характеристики певних предметів, зокрема їх кількості, тотожності, дійсності (обман у предметі), особистості винного або інших осіб (обман у особі), певних подій, юридичних фактів, дій окремих осіб тощо[36].

Зловживання довірою полягає у недобросовісному використанні довіри з боку потерпілого: для заволодіння чужим майном чи правом на нього винний використовує довірчі стосунки, які склалися між ним та власником чи володільцем майна. Як шахрайство, вчинене шляхом зловживання довірою, належить розглядати отримання кредиту, попередньої оплати за товари чи виконання робіт (авансу), укладення договору позики, укладення договору прокату тощо без наміру повернути отримані кошти чи інші матеріальні цінності, виконати відповідну роботу, повернути борг чи отримані у користування речі.

З огляду на це, доречно Л. І. Казміренко висловив думку про маніпуляцію як виду приховання психологічної дії, факт якої не має бути поміченим об'єктом маніпуляції, а також спонукання людини до дій, що не збігаються з її актуальними бажаннями[37].

Стосовно предмета посягання, то О. В. Кришевич відносить до нього рухоме та нерухоме майно. Рухоме майно це:

1) коштовні речі різного призначення – автомобілі, коштовності, відео- та аудіотехніку та інше, гроші, зокрема у валюті, цінні папери, кольорові метали;

2) гроші, вилучені з обігу, але які підлягають обміну та знаходяться в обігу в банківській чи іншій системі;

---

[35] Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : монографія. Київ : Хай-Тек Прес, 2010. С 49.

[36] Науково-практичний коментар до Кримінального кодексу України / М. І. Мельника, М. І. Хавронюка. 6-те вид., перероблене і доповнене. Київ : Юридична думка, 2009. С. 505.

[37] Казміренко Л. І. Про засади маніпуляційного впливу на суспільну свідомість. *Філософські, методологічні та психологічні проблеми права: матеріали II Всеукраїнської науково-теоретичної конференції (м. Київ, 31 січня 2009 року).* Київ : КНУВС, 2009. С. 203.

3) гроші, давно вилучені з обігу, але які представляють які-небудь цінність і певну вартість. Наприклад, зроблені з дорогоцінних металів, що представляють історичну цінність – рідкі або дуже старовинні тощо.

4) безготівкові гроші, що зберігаються на рахунках у банках і кредитних організаціях;

5) цінні папери, зокрема, іменні[38].

Крім того автор, враховуючи обставини, що можуть виникнути під час вчинення шахрайств до його предмета також відносить: проїзні квитки на транспорт і транспортні абонементи, за винятком іменних квитків і бланків квитків, що вимагають додаткового оформлення; квитки та абонементи на відвідування театральних спектаклів, концертів, кіносеансів, циркових та інших вистав, виставок; квитки різних лотерей (грошово-речових лотерей); знаки поштової оплати (конверти, марки, листівки тощо); жетони, що заміняють гроші; оплачені магазинні чеки; талони на пально-мастильні матеріали тощо.

Під нерухомим майном О. В. Кришевич, посилаючись на цивільне законодавство, розуміє:

1) земельні ділянки, ділянки надр, відособлені водні об'єкти та все, що міцно пов'язане із землею, тобто об'єкти, переміщення яких без збитку, нерозмірного їх призначенню, неможливе, у т. ч. ліс, багаторічні насадження, будинки, споруди;

2) предмети державної реєстрації, повітряні й морські судна, судна внутрішнього плавання, космічні об'єкти;

3) надра в межах території України, включаючи підземний простір і корисні копалини, що перебувають у надрах, енергетичні та інші ресурси[39].

Розкрадання таких об'єктів нерухомості можливе не на рівні розкрадання майна, а тільки на рівні розкрадання прав на нього. Про розкрадання може

[38] Кришевич О. В. Кримінально-правова характеристика предмета шахрайства. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. Вип. № 24, 2011. С. 184-186.

[39] Кришевич О. В. Кримінально-правова характеристика предмета шахрайства. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. Вип. № 24, 2011. С. 186-187.

свідчити лише офіційний переказ права на нерухомість на ім'я винного або осіб, на яких він вкаже.

Також слушною є позиція Л. В. Борисової та О. В. Тарасова, які до предмета посягання шахрайства відносять й інформацію, що поділяється на:

1) особисту конфіденційну інформацію – таємниця листування, телефонних розмов, поштової, телеграфної чи іншої кореспонденції, що передається засобами зв'язку або через комп'ютер; таємниця всиновлення; особисте життя особи та його таємниця; інформація, яка є об'єктом авторських і суміжних прав; персональні дані, тобто інформація, яка безпосередньо порушує права та свободи громадян; адвокатська таємниця; лікарська (медична) таємниця; таємниця страхування;

2) конфіденційна інформація юридичних осіб: службова таємниця; комерційна або банківська таємниця; редакційна і журналістська таємниця;

3) державна конфіденційна інформація, тобто інформація, яка належить державі чи його суб'єктам: службова таємниця; дані досудового розслідування; відомості про заходи безпеки, що застосовуються по відношенню до посадової особи правоохоронними або контролюючими органами;

4) інша категорія інформаційних ресурсів – інформація загального користування для необмеженого кола осіб тощо[40].

Тут доцільно зазначити, що інформаційні відносини не існують самі по собі, і як сфера правового регулювання, передбачають участь у цьому й інших правових норм. Розглядаючи злочин у віртуальному просторі, слід керуватися не лише нормами інформаційного права, але й низкою галузей права (цивільного, адміністративного, господарського, банківського, кримінального та ін.), а неправомірні дії у такому середовищі розглядаються з позиції того права, норми якого були порушені. Загалом законодавство у сфері регулювання правовідносин у віртуальному просторі має значну кількість прогалин і колізій, тому потребує

[40] Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження / Л. В. Борисової : дис. ….. канд. юрид. наук. Київ, 2007. 217 с. (с. 42); Тарасов О. В. Об'єкт шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Право і суспільство. Вип. № 1, 2013. С. 106-111 (с. 109).

вдосконалення. Крім того, форми цивільних правовідносин у мережі Інтернет наразі є досить врегульованими, що тягне за собою значну кількість порушень, зокрема й у сфері зв'язку та надання послуг, а велика їх кількість може мітити склад шахрайства.

У доктрині кримінального права законодавець не оперує поняттям «кібершахрайство», а використовує таке формулювання, як «… обман чи зловживання довірою вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки».

На наш погляд, шахрайство, учинене у кіберпросторі – це суспільно небезпечне діяння, спрямоване на заволодіння чужим майном або придбання права на майно шляхом незаконних операцій з використанням електронно-обчислювальної техніки у віртуальному просторі (середовищі), де надається можливість комунікацій та/або реалізації суспільних відносин.

Розглянемо детальніше складові оперативно-розшукової характеристики досліджуваного злочину.

Кримінально-правова складова оперативно-розшукової характеристики шахрайства, учиненого в кіберпросторі.

У кримінально-правовому вимірі підставою кримінальної відповідальності є вчинення особою діяння, яке містить склад кримінального правопорушення, передбаченого КК України. Криміналізація цього діяння пов'язана і обумовлена його суспільною небезпечністю, що визначається важливістю об'єкта кримінально-правової охорони (в аспекті визначених ст. 1 КК України завдань цього кодексу) та вартісним критерієм предмету злочину, який віддзеркалює ступінь небезпечності конкретного злочину.

Складовою підстави притягнення до кримінальної відповідальності за шахрайство є усвідомлення суб'єктом злочину того факту, що предмет злочину є для нього чужим, що він заволодіває чужим майном за відсутності будь-якого дійсного чи уявного права на нього. Кримінальна відповідальність за шахрайство пов'язана зі встановленням усвідомлення винним факту заволодіння чужим майном з метою його безоплатного, безповоротного обернення на свою користь

(чи третіх осіб) за відсутності законних підстав, збільшення внаслідок цього власних або третьої особи майнових фондів.

Усвідомлення винною особою, кому саме належить чуже майно та на яких підставах, чи заволодіває він майном, використавши обман власника цього майна, чи обман іншої особи, у володінні якої воно перебуває, не є вирішальним для встановлення ознак кримінального правопорушення, передбаченого ст. 190 КК України.

Оскільки обман є особливим видом інформаційного (дезінформаційного) впливу, його застосування спрямоване на відображення в свідомості обманутого у перекрученому, спотвореному вигляді фактів чи обставин, що обумовлюють рішення про передачу майна. Винний втручається в сферу психічної (інтелектуальної та вольової) діяльності іншої особи, фальсифікує її уявлення про відповідні обставини, вводить цю особу в оману, внаслідок чого вона обирає ту чи іншу лінію поведінки без знання і судження фальсифікації, а волевиявлення та вчинки обумовлені обманними діями винного.

При цьому виникнення умислу передує заволодінню чужим майном, а обман як спосіб учинення злочину може виявлятися як у формі дії, так і бездіяльності або поєднувати зазначені форми впливу з метою введення в оману чи підтримання омани, яка виникла поза протиправними діями винуватої особи. Тут слід зазначити, що точний час зустрічі не має вирішального значення для встановлення ознак злочину за ст. 190 КК України.

Головною кваліфікуючою обставиною досліджуваного злочину становить вчинення шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Таку ознаку утворюють лише операції, здійснення яких без використання електронно-обчислювальної техніки є неможливим (здійснення електронних платежів, отримання Інтернет-послуг, здійснення операцій через реквізити платіжних карток та банківські послуги тощо). Якщо за допомогою такої техніки здійснюються операції, які можливі при використанні іншої техніки (набір тексту, виготовлення документу), зокрема без

підключення до віртуального простору (середовища), то така кваліфікуюча ознака відсутня.

Шахрайство є закінченим злочином з моменту заволодіння винним майном або придбання права на майно. Обман або зловживання довірою, які призвели до цього, залежно від сформованих обставин слід кваліфікувати як готування або замах на шахрайство.

Отже, ураховуючи наведений опис кримінально-правової складової зазначимо, що о*б'єктом злочину* є право на власність, відповідно до якого здійснюється володіння, користування й розпорядження майном.

Предметом шахрайства є майно, яке має певну вартість і є чужим для винної особи: речі (рухомі й нерухомі), грошові кошти, ціні метали, цінні папери тощо[41].

Стаття 177 Цивільного кодексу України під об'єктами цивільних прав розуміє речі, у тому числі гроші та цінні папери, інше майно, майнові права, результати робіт, послуги, результати інтелектуальної, творчої діяльності, інформація, а також інші матеріальні і нематеріальні блага[42].

Об'єктивна сторона злочину – діяння, які характеризуються протиправним корисливим зверненням до чужого майна, що заподіює прямий збиток власникові.

Шахрайство вчиняється шляхом обману або зловживанням довірою. Обман (повідомлення потерпілому неправдивих відомостей або приховування певних обставин) чи зловживання довірою (недобросовісне використання довіри потерпілого) при шахрайстві застосовуються винною особою з метою викликати у потерпілого впевненість у вигідності чи обов'язковості передачі їй майна або права на нього.

Обман охоплює собою різноманітні прийоми з боку винного і між цією дією та заволодінням майном необхідна наявність причинного зв'язку.

[41] Про судову практику у справах про злочини проти власності : Постанова Верховного суду України від 06.11.20009 № 10. *Офіційний вебпортал Верховної ради України.* URL: https://zakon.rada.gov.ua/laws/show/v0010700-09#Text.

[42] Цивільний кодекс України від 16.01.2003 № 435-IV. *Офіційний вебпортал Верховної ради України.* URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.

Зловживання довірою – це використання винним відносин довіри, які є основою правовідносин або існують в особистих стосунках. При шахрайському заволодінні майном зловживання довірою часто переплітається з обманом. Проте зловживання довірою є другорядним по відношенню до обману, але не втрачає свого самостійного значення як спосіб заволодіння майном при шахрайстві. Обов'язковою ознакою шахрайства є добровільна передача потерпілим майна чи права на нього.

У випадку, коли потерпіла особа через вік, фізичні чи психічні вади або інші обставини не могла правильно оцінювати і розуміти зміст, характер і значення своїх дій або керувати ними, передачу нею майна чи права на нього не можна вважати добровільною.

Якщо особа заволодіває чужим майном, свідомо скориставшись чужою помилкою, виникненню якої вона не сприяла, та за відсутності змови з особою, яка ввела потерпілого в оману, вчинене не слід інкримінувати як шахрайство. Тим паче, якщо обман або зловживання довірою були лише способом отримання доступу до майна, а саме вилучення майна відбувалося таємно чи відкрито, то об'єктивна сторона шахрайства також відсутня.

Проте отримання майна за умови виконати будь-яке зобов'язання може розглядатися як шахрайство. Наприклад, коли винна особа ще в момент заволодіння цим майном мала на меті його привласнити, а не виконати зобов'язання.

Шахрайство, учинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки додаткової кваліфікації не потребує. Такий злочин направлений не на стабільність функціонування електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та/або комп'ютерних мереж, мереж електрозв'язку, а на суспільні відносини з огляду заволодіння майном або правом на це майно. Тому предметом досліджуваного виду шахрайства не може бути електронно-обчислювальні машини (комп'ютери), автоматизовані системи та/або комп'ютерні мережі, мережі електрозв'язку.

Також слід зазначити, що зміст, значення і обсяг поняття потерпілого в кримінальному праві не збігається з поняттям потерпілого в кримінальному процесуальному аспекті, адже вони мають різне правове значення. У кримінальному процесуальному аспекті особа визначається потерпілим відповідно до приписів кримінального процесуального закону, внаслідок чого набуває процесуальні права задля реалізації власних інтересів у кримінальному провадженні з моменту, визначеного приписами ч. ч. 2, 3 ст. 55 Кримінального процесуального кодексу України (далі – КПК України). При цьому, жодна з норм КПК України не виключає здійснення досудового розслідування, судового провадження за інкримінованим особі правопорушенням, за відсутності зазначених вище підстав брати участь фізичній чи юридичній особі в кримінальному провадженні як потерпілий. Кримінальний процесуальний закон як форма реалізації кримінально-правових відносин не пов'язує їх втілення за інкримінованим за ст. 190 КК України кримінальним правопорушенням з набуттям процесуального статусу потерпілого конкретну особу.

Суб'єкт злочину – загальний, тобто фізична осудна особа, яка досягла 16-річного віку.

Суб'єкт вчинення шахрайства характеризується своєю багатогранністю, тому слід враховувати такі ознаки, як: соціально-демографічні, соціальні прояви, моральні якості, психологічні особливості тощо.

У більшості випадків шахрайство – це «індивідуальна» злочинна діяльність, що вчиняється будь-якою особою, яка використовує електронно-обчислювальну техніку у власних інтересах, а також особою, яка надає відповідні послуги у цій сфері. Здійсненні операції можуть бути цілком законними, не порушуючи стабільного функціонування електронно-обчислюваних машин (комп'ютери), автоматизованих систем та/або комп'ютерних мережі, мережі електрозв'язку.

Суб'єктивна сторона шахрайства представлена прямим умислом, а також корисливою метою. Тобто характеризується прямим наміром заволодіти чужим майном або правом на це майно з корисливих спонукань. Винний розуміє, що

вчиняє протиправне діяння і передбачає розвиток причинного зв'язку й настання суспільно небезпечних наслідків.

Умисел при шахрайстві за часом виникнення й формування, як правило, заздалегідь обдуманий.

Кримінологічна складова оперативно-розшукової характеристики шахрайств, учинених в кіберпросторі.

Шахрайство є традиційним кримінальним правопорушенням проти власності для багатьох кримінально-правових систем, зокрема й для української. Шахрайство є кримінальним правопорушенням, що ставить під загрозу не тільки власність окремих осіб, але й функціонування економічної системи нашої держави. Досвідчені фахівці стверджують, що збитки, завдані таким кримінальним правопорушенням, обчислюються десятками та сотнями тисяч гривень. З огляду на тенденцію до збільшення кількості розкрадань, здійснених шляхом шахрайства, можна стверджувати, що боротьба з такими протиправними діями є одним із пріоритетних напрямів діяльності правоохоронних органів[43].

Стан. Маємо відмітити, що кримінальні правопорушення проти власності становлять левову частину усіх кримінальних правопорушень, що вчиняються в Україні. Середні статистичні показники за період 2018-2022 років ілюструють, що співвідношення кримінальних правопорушень проти власності із загальною кількістю облікових кримінальних правопорушень становить 51,8 %. Шахрайство є другим за поширеністю загальнокримінальним правопорушенням проти власності після крадіжок. Щороку в середньому реєструється близько 30 тисяч таких діянь, що становить 7,5 % кримінальних правопорушень у структурі зареєстрованої злочинності і, відповідно, 14,5 % у структурі кримінальних правопорушень проти власності (Додатки Б, Г).

До 2020 року в офіційній статистичній звітності офісу Генерального прокурора було передбачено самостійній критерій для шахрайства – злочини за

[43] Трач С. С. Деякі аспекти оперативно-розшукової профілактики шахрайств у сфері кредитних операцій банків. *Матеріали Міжнародної науково-практичної конференції «Актуальні питання виявлення, досудового розслідування та попередження корупційних правопорушень» (м. Дніпропетровськ, 24 квітня 2015 року).* Дніпропетровськ : ДДУВС, 2015. С. 185.

ч. 3 ст. 190 КК України (тобто ті, що вчинялись шляхом здійснення незаконних операцій з використання електронно-обчислювальної техніки). Дослідивши таку звітність з 2016 по 2019 роки встановлено, що шахрайства, учинені шляхом використання електронно-обчислювальної техніки в структурі видового кримінального правопорушення становить 12,03 %, у структурі кримінальних правопорушень проти власності – 1,74 % та в структурі загальних показників облікових кримінальних правопорушень – 0,9 % (Додаток Г). Після 2019 року зазначений критерій зник з офіційної статистичної звітності, що унеможливлює достовірного встановлення відповідного відсоткового співвідношення. Однак, з урахуванням тенденції цифрового розвитку суспільства, його соціально-економічний стан, політично-культурну кризу, а також умови військової агресії, можемо обґрунтовано стверджувати, що кожне соте кримінальне правопорушення – це шахрайство, учинене в кіберпросторі.

Динаміка. Усього за досліджуваний період було зареєстровано 148411 шахрайств, питома вага розкриття яких у середньому дорівнює 29,31 %, проте тільки 24,31 % відповідних матеріалів кримінальних проваджень було скеровано до суду (Додаток В).

Взагалі простежується тенденція щорічного зниження кількісних показників реєстрації кримінальних правопорушень, а ось показників шахрайств – динаміка росту.

Так, за середніми показниками реєстрація облікових кримінальних правопорушень становить -6,42 %, кримінальних правопорушень проти власності -21,66 %, шахрайств 0,89 % (за 2022 рік цей показник у порівнянні з попереднім роком становить 34,55 %), кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж, мереж електрозв'язку 11,2 % (Додаток Б). З них середні показники розкриття для облікових кримінальних правопорушень 42,91 %, для кримінальних правопорушень проти власності 41,82 %, для шахрайств 29,37 %, для кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів),

автоматизованих систем та комп'ютерних мереж, мереж електрозв'язку 71,02 % (Додаток В).

Слід зазначити, що загальний показник розкриття вказаних кримінальних правопорушень у період військової агресії зменшився від 5 до 17 % (Додаток В). Стосовно шахрайств, учинених шляхом незаконних операцій з використанням електронно-обчислювальної техніки, то в структурі видового кримінального правопорушення показник розкриття становить 14,17 %, у структурі кримінальних правопорушень проти власності 1,74 %, у структурі загальних показників облікових кримінальних правопорушень 0,72 % (Додаток Г). Тобто успішно розкривається кожне 3 шахрайство, учинене в кіберпросторі, в інших випадках, – не представляється можливим встановити особу злочинця.

Стосовно *особа злочинця*, то це полінаукова категорія, що є предметом вивчення багатьох наук. Ми поділяємо думку В. О. Коновалової та В. Ю. Шепітька, які під особою злочинця розуміють соціально-психологічне поняття, що охоплює сукупність типових психологічних і моральних якостей індивіда, яка формуються в результаті вчинення злочину[44]. Кожному злочину притаманний свій тип злочинця, оскільки набір індивідуальних властивостей та рис особи злочинця відрізняється від специфіки злочинної діяльності.

Як правило, шахраїв поділяють на кілька груп:

1) «нові» шахраї, які використовують механізми ринкових відносин, можливості кредитно-банківських операцій, лжефірм, страхової, інвестиційної і довірчої діяльності;

2) шахраї-гастролери, які постійно роз'їжджають і негайно зникають з місць вчинення кримінально протиправних діянь;

3) шахраї-гравці, які використовують азартні ігри (карточні шулери, «катали», «червоні валети» тощо;

4) шахраї, які не мають постійного місця роботи чи проживання, неодноразово судимі за шахрайство чи інші злочини;

[44] Коновалова В. О., Шепітько В. Ю. Юридична психологія : академічний курс / В. О. Коновалова. Київ : Ін Юре, 2004. С. 358.

5) шахраї, які вчинили злочин вперше, за легковажністю, під впливом інших осіб чи ситуацій;

6) шахраї-одинаки і шахраї, які вчиняють злочин, групою, зокрема з розподілом ролей[45].

Стосовно злочинців, які вчиняють шахрайства у кіберпросторі, то їх можна віднести до першої, п'ятої та шостої груп. У зв'язку з цим, на наш погляд, доцільно виділити типи злочинців залежно від рівня їхньої компетенції: дилетант, досвідчений фахівець, професіонал.

Під компетенцією злочинця розуміємо певний рівень знань, умінь та навичок використання психологічних методів впливу, враховуючи потенційний інтерес у кіберпросторі – досягнення бажаного результату.

Такий підхід може використовуватися значно в розширеній формі, враховуючи суміжні фактори проявів (поведінку, конкретні мотиви, мету та ін.) та зовнішнього впливу (соціально-економічні, політичні та інші ланки).

У запропонованому переліку ми взяли до уваги потенційний інтерес злочинця, оскільки особа вже може володіти достатнім рівнем знань, умінь та навичок психологічних методів впливу, проте під зовнішніми факторами (наприклад, низький рівень достатку або безробіття) обирає свій шлях досягнення бажаного результату, – здійснити цілком законі операції із застосуванням електронно-обчислювальної техніки у кіберпросторі або прибігти до шахрайських схем.

Вважаємо, що дилетант – це той, хто володіє базовим уявленням про шахрайські схеми, але не має сформованого достатнього рівня умінь та навичок психологічного впливу. Досвідчений фахівець – той, хто володіє певними (індивідуальними) знаннями про шахрайські схеми, а також достатнім рівнем умінь та навичок психологічного впливу. Професіонал – той, хто володіє спеціальними (поглибленими) знаннями про витонченість шахрайських схем, професійними вміннями та навичками психологічного впливу.

[45] Настільна книга слідчого : науково-практичне видання для слідчих і дізнавачів / М. І. Панов, В. Ю. Шепитько, В. О. Коновалова та ін. Київ : Ін ре, 2003. С. 431.

У залежності від потенційного інтересу їх можна розрізнити, як:

– корисливі – особи, які вчиняють шахрайство у кіберпросторі для досягнення своїх особистих жадібних цілей;

– самоствердежі – особи, які вчиняють шахрайство у кіберпросторі для самоствердження, як для себе, так і в очах інших осіб. Як правило, серед співучасників;

– побутові – особи, які вчиняють шахрайство у кіберпросторі для забезпечення потреб свого оточення, - родичів, близьких осіб, осіб з якими перебувають у спорідненості внаслідок сформованих особистих взаємин;

– егоїстичні – особи, які вчиняють шахрайство у кіберпросторі, внаслідок власного низького морально-культурного розвитку та антигромадських рис характеру (нахабність, зухвалість, заздрість, егоїзм), ігноруючи законні приписи недоторканності чужого майна.

– дезадаптовані – особи, які вчиняють шахрайство у кіберпросторі для сталого злочинного доходу. Тобто це для них є основним чи єдиним джерелом доходу, зокрема тих, хто відноситься до засуджений осіб чи шахраїв-професіоналів.

Отже, характеристика особи злочинця, яка вчиняє шахрайство у кіберпросторі, складна й динамічна, вона охоплює широкий спектр внутрішніх позицій особистості в різних сферах соціального буття. За результатами нашого дослідження встановлено, що шахрайства в кіберпросторі здебільшого вчиняються чоловіками. Шахрай є соціально благополучною особою, позитивно характеризуються за місцем проживання, роботи, навчання. Вік чоловіків-шахраїв: від 25 до 45 років – понад 65 %. Більшість шахраїв мають сильний дар уяви, здатність впливу і вміння переконувати. До особистих якостей шахрая належать його хитрість, брехливість, уміння прихилити до себе оточуючих, знання способів підроблення документів. За своїм зовнішнім виглядом – це звичайні люди, які вміють себе «подати», обізнані в галузі психології. Вони спостережливі і мають швидку реакцію на обстановку, що змінюється. Шахраї використовують можливість перевтілення, встановлюють контакт з людьми

різних типів, обирають стиль поведінки від конкретно сформованої обстановки. Внутрішній прояв такої особи полягає у відсутності в неї морально-вольових (етичних) стримуючих факторів, що спричиняє характерну зневагу до загальноприйнятих моральних цінностей суспільства. Тобто особа, яка вчиняє шахрайство є психологічно готовою для нехтування нормами моралі, діловими, дружніми стосунками. У зв'язку із тим, що шахрайство вчиняється з прямим умислом особа бажає настання суспільно небезпечних наслідків свого діяння, впливаючи на благополуччя потерпілого. Інколи, – ставлячи під загрозу виживання останнього. Потерпілими від шахрайства можуть бути будь-які фізичні особи, підприємства, організації, установи, споживачі товарів і послуг у віртуальному просторі (середовищі).

Причини та умов, що сприяють вчиненню злочину.

Установлення причин та умов, що сприяють вчиненню шахрайств у кіберпросторі має превентивне й профілактичне значення, проте до редакції чинного КПК України такого роду обставини не увійшли. Як результат – у 60 % вивчених матеріалах кримінальних проваджень вони не були встановлені (Додаток Е). Такі обставини рідко відображаються і в матеріалах кримінальних проваджень, пов'язаних із розслідуванням фактів несанкціонованого втручання в роботу або обробкою даних електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Не вдаючись до полеміки, приєднуємось до позиції науковців, які вважають, що під причинами шахрайства слід розуміти фактори, що безпосередньо обумовлюють його вчинення, а під умовами – що сприяють, створюють можливість вчинення злочину. Ці фактори є детермінаційним комплексом, в якому причини можуть спрацювати без умов та шахрайство буде вчиненим, а ось без наявності причин та умови не працюють. Тобто шахрайство не може бути вчиненим.

На наш погляд, причини, що впливають на кількісні та якісні показники шахрайств, а також що сприяють учиненню таких дій у кіберпросторі пов'язані з:

– збройним конфліктом на сході України до 24.02.2022 року (незаконні схеми формування капіталів, зловживання повноваженнями окремих посадових осіб, безкарність у зв'язку з відсутності влади та представників правоохоронних органів);

– військовою агресією після 24.02.2022 року (дестабілізація нормального буття соціуму, функціонування державних інституцій; внутрішня міграція; зростання попиту на гуманітарні та матеріальні потреби, зокрема серед внутрішньо переміщених осіб; загибель громадян працездатного віку; руйнування житла; зневіра у перспективах розвитку українського суспільства; зростання навантаження на правоохоронні органи через посилений режим службової діяльності);

– соціально-економічною нестабільністю (стрімкий ріст злочинності за матеріально-економічними мотивами; низький рівень достатку; втрата роботи; або пошук альтернативних джерел підвищення матеріального становища);

– соціально-політичним впливом (використання правоохоронних органів у політичній боротьбі, – деморалізація та дискредитація співробітників; розбіжність думок під час військової агресії; дезінформація; психологічний вплив через соціальний доказ «роби як інші – не помилишся» тощо);

– соціально-культурним загостренням (легалізація частини рядового криміналітету, їхніх керівників як представників влади; омолодження злочинності; дисбаланс між умовами життя різних верств населення);

– організаційно-управлінськими та технічними проблема (виконання правоохоронними органами невластивих їм функцій; недостатній рівень фінансового та матеріально-технічного забезпечення, що сприяє

безрезультатним заходам щодо розкриття та припинення злочинної діяльності);

– правовими прогалинами (відсутність єдиної нормативної бази для інституцій, що забезпечують кібербезпеку та протидію кіберзлочинності; ускладнення і погіршення діяльності правоохоронних органів внаслідок прийняття більш ліберального (європейського) законодавства; недостовірність чинного законодавства, зокрема в законодавстві про кримінальну відповідальність – конструкції шахрайства, де галузеві закони та підзаконні акти створюють хибне уявлення про умови безкарності).

Криміналістична складова оперативно-розшукової характеристики шахрайств, учинених в кіберпросторі.

Унікальність криміналістичної характеристики полягає в оптимальній структурі, що охоплює виключно криміналістично значущі ознаки досліджуваного злочину, адже її елементи не мають сталого характеру та змінюються за сучасними (на певних етапах розвитку держави) соціально-економічними, політичними та іншими чинниками, і можуть бути доповнені іншими закономірними взаємозв'язками з наук кримінально-правової та соціальної галузі, що, у свою чергу, дозволяє спрогнозувати вчинення повторних чи серійних злочинів та зрозуміти їхній інформаційний «портрет» з різних кутів.

Так, *типові способи вчинення шахрайств* шляхом незаконних операцій з використанням електронно-обчислювальної техніки є значущою складовою для описання інших елементів характеристики.

Слід відрізняти способи вчинення шахрайств від способів учинення інших кримінальних правопорушень, пов'язаних із шахрайством. Насамперед, це стосується таких суспільно небезпечних діянь, як: завдання майнової шкоди шляхом обману або зловживання довірою (ст. 192 КК України); шахрайство з фінансовими ресурсами (ст. 222 КК України); несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України); несанкціоновані дії з інформацією, яка обробляється в електронно-

обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України).

За результатами аналізу правозастосовної практики способи шахрайств, учинені в кіберпросторі, можна розрізнити за наступними критеріями:

1) залежно від періодичності вчинення злочину:

– одноразові – шахрайство вчиняється з метою обману однієї визначеної особи задля заволодіння певним товаром, що їй належить, або сумою грошей за продаж неіснуючого товару;

– тривалі – шахрайство вчиняється з метою обману та заволодінням майно невизначеного кола осіб;

2) залежно від сфери надання послуг:

– банківська сфера – шахрайство вчиняється шляхом виманювання або інших дій щодо отримання конфіденційних даних особи про її банківських рахунок, реквізити, вклади з подальшим перерахунком грошових коштів або отримання кредитів;

– побутова сфера – шахрайство вчиняється шляхом отримання коштовних речей за документами родичів, за викраденими чи знайденими документами, а також здійснення операцій (платежів, переказів тощо) через електронно-обчислювальні машини (комп'ютери) осіб, з якими встановлені близькі стосунки, без подолання логічного захисту;

– сфера страхування – шахрайство вчиняється шляхом надання неіснуючих страхових полісів;

– туристична галузь – шахрайство вчиняється шляхом надання неіснуючих туристичних послуг;

3) залежно від кількості задіяних до вчинення шахрайств:

– вчинено за участю однієї особи;

– вчинено групою осіб, за попередньою домовленістю;

– вчинено організованою групою осіб;

4) залежно від предмета посягання:

– грошові кошти;

– матеріальні (коштовні) цінності;

– персональні дані особи, її профіль або банківські реквізити (картку);

– право на майно, зокрема на нерухоме;

5) залежно від способів введення в оману або зловживання довірою:

– маніпулювання інформацією, спотворення деяких фактів або навмисне укриття інформації;

– маніпулювання достовірністю інформацію, її перекручування або спростування деяких фактів;

– повідомлення двозначної або неконкретизованої інформації;

– повідомлення помилкової інформації, – попередньо спотвореної.

6) залежно від місця вчинення шахрайства (шляхом встановлення місця реєстрації IP-адреси електронно-обчислювальної техніки):

– територія України, де постійно дії державна адміністрація;

– територія України тимчасово окупована до 24.02.2022 року – окрема територія Донецької та Луганської областей, Автономної Республіки Крим;

– територія України тимчасово окупована після 24.02.2022 року – окрема територія Донецької, Луганської, Харківської, Запорізької та Херсонської областей, Автономної Республіки Крим;

– територія іншої країни;

– територія країни не встановлено;

7) залежно від способу підготовки до вчинення шахрайства:

– сприяв несанкціонований доступ до електронно-обчислювальних маниш (комп'ютера), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

– сприяло шкідливе програмне чи технічне забезпечення, що містилось на електронно-обчислювальній техніці;

– сприяло фішингове розповсюдження інформаційної продукції, надання певних послуг.

Респондентами також визначено найбільш популярні види шахрайств у кіберпросторі, як:

1) Фішинг (англ. Phishing) (74,7 %) – вид шахрайства, що вчиняється з використанням соціальної інженерії, який полягає в імітуванні діяльності реально існуючих компаній або банків-емітентів, використовуючи неголосові засоби комунікації. Комунікація здійснюється під різним приводом, виманюючи у власників платіжних карток реквізити та іншу конфіденційну інформацію.

Різновидами фішингу є:

– фішингові сайти або посилання;
– фішингові електронні листи;
– фішингові SMS-повідомлення.

2) Сніферінг (4,3 %) – один із складних видів шахрайства, спрямований на захоплення та розбору мережевого трафіку. Тобто шляхом сніферінгу шахрай може отримати відомості про топологію мережі, потоки, адреси в ній тощо.

3) Вішинг (англ. Vishing) (7,5 %) – вид телефонного шахрайства, спрямованого на отримання конфіденційної інформації стосовно реквізитів банківських карток або інших даних, примушення до переказу коштів на картку злочинця.

4) Кардинг (англ. Carding) (7,1 %) – вид шахрайських дій, при яких здійснюється операція з допомогою платіжної картки чи її реквізитів, не ініційованої чи не підтвердженої її власником. У такому випадку реквізити платіжних карток, як правило, зловмисник отримує з пошкоджених (без елементів логічного захисту) серверів інтернет-магазинів, платіжних і розрахункових систем, у тому числі з персональних комп'ютерів через програми віддаленого доступу або шкідливе програмне забезпечення («трояни», «боти» з функцією формграббера тощо) (Додаток Д).

Загалом існує безліч способів учинення шахрайств у кіберпросторі, надати вичерпний перелік не є можливим, оскільки така злочинна діяльність постійно трансформується і з'являються нові види шахрайських дій.

Проте, основним способом учинення шахрайств у кіберпросторі є заволодіння коштами фізичних (інколи, – юридичних) осіб шляхом створення у потерпілого уяви необхідності передати кошти сторонній особі. Таке уявлення створюється за допомогою різноманітних методів психологічного впливу (як правило, використовуючи соціальну інженерію). Аналіз матеріалів кримінальних проваджень дозволів дійти висновку, що типовими в умовах воєнного стану залишаються такі способи вчинення шахрайства, як:

– отримання у власників платіжних карток реквізитів та іншої конфіденційної інформації про картку (50 %);

– отримання даних про банківську картку з використанням електронно-обчислюваної техніки (34 %);

– дублювання фінансових номерів (34 %);

– створення і забезпечення діяльності фіктивного інтернет-магазину або кур'єрської служби (30 %);

– створення інтернет-аукціонів шляхом надання недостовірних даних і пропозиції продажу неіснуючих (або якості нижче заявленого) товару (16 %);

– створення або використання вебсторінок (програм-підтримки) благодійних організацій (16 %): спекуляція на почуттях, змушуючи брати участь у благодійних фінансових зборах (пожертвуваннях); нав'язування посилкової думки, внаслідок якої особа свідомо сплачує послуги до фонду підробленої організації;

– забезпечення підтримки: псевдоблагодійність; пропозиції оренди неіснуючого житла; несправжні пасажирські перевезення (70 %);

– створення та забезпечення діяльності фіктивних фінансових бірж (6 %) (Додаток Е).

Розглянемо декілька типових шахрайських схем.

«Фішингове посилання на платформі оголошень «ОЛХ». Ця схема пов'язаний з переходом жертви за фішинговим посиланням, а саме: злочинець знаходить оголошення про продаж будь-якого товару на сайті «ОЛХ», та

намагається переконати жертву здійснити продаж через послугу «ОЛХ – доставка». Якщо жертва не розбирається в цій послузі, злочинець залучає до розмови нібито «ОЛХ підтримку», яка переконує про безпечність та вигідність такої операції. Коли жертва погоджується, їй надсилається фішингове посилання за яким вона повинна перейти та ввести свої дані та дані банківської карти, номер рахунку, CVV код та дату видачі карти. Після виконаного всіх дій, кошти списуються з рахунку жертви на рахунки злочинців.

Вказана схема працює в різноманітних інтерпретаціях – необхідно заповнити форму для повернення коштів, бо товар не було надіслано; заповнити форму для отримання грошового призу тощо.

«Дублікат сім-картки, що є фінансовим номером». Злочинець телефонує на «гарячу лінію» мобільного оператора та від імені своєї жертви блокує sim-карту потерпілого у зв'язку з втратою мобільного телефону. При цьому проходить ідентифікацію при якій необхідно назвати декілька номерів на які постійно телефонує жертва, баланс рахунку, або сума останнього поповнення, дата.

Номер після ідентифікації реєструється за «пустою» сім-картою. Зробивши клон сім-карти, злочинець телефонує до банку (банківська система розпізнає його як номер клієнта) та проходить ідентифікацію з метою зміни паролю входу до банківського додатку («ПУМБ-онлайн», «Приват24» та ін.). Для ідентифікації необхідно знати ПІБ, ІНН, номер паспорта, ким і коли виданий, секретне слово (як правило це дівоче прізвище матері клієнта). Його злочинець отримує шляхом омани від самої жертви – телефонує їй під виглядом працівника мобільної компанії, розповідаючи про проведення технічних робіт, та попереджає про те, що буде вимкнено зв'язок на деякий час та коли він з'явиться для підключення номеру необхідно буде його пройти ідентифікацію. Пропонує придумати секретне слово, наприклад як в банку дівоче прізвище матері. Жертва погоджується та надає дані злочинцю.

Також існує багато баз даних з особистими даними громадян, які вони надали самостійно реєструючись на різноманітних сайтах з продажу товарів. У месенджері телеграм існує декілька ботів для «пробиття інформації», які за

номером телефону надають інформацію про його власника, дату народження, стать, ІНН, паспорт, місце реєстрації, родинні зв'язки з такими само даними, електронну пошту.

Використовуючи телефонний номер жертви, злочинець «зламує» банківські додатки, gmail профіль, сторінки соціальних мереж тощо.

Частіше злочинець не обмежується викраденням грошей, а оформлює на свою жертву ще позики в установах швидкого займу (Швидко гроші, Кредит каса тощо), використовуючи скан-копії документів, які він міг знайти на google диску.

«Установлення переадресації на номер телефона шахрая». В Інтернет магазині шахрай знаходить оголошення про продаж будь-яких товарів або оренду житла, де вказаний контактний телефон та ім'я особи. Шахрай телефонує на номер, називає абонента за його ім'ям, та представляється фінансовім оператором «Приватбанка». Після цього повідомляє, що пропонується послуга по банківській карті: «розширення кредитного ліміту», якщо особа погоджується, їй пропонується для підтвердження операції залишатись на зв'язку та набрати на телефоні комбінацію: *21*номер телефона (з якого телефонує шахрай)# з клавішою виклику. Така операція застосовується компанією стільникового зв'язку Київстар для переадресації усіх вхідних дзвінків. Далі особі повідомляється, що банківська система вимагає надати відповідь про останні чотири цифри картки. Коли надані ці дані, шахрай повідомляє, що їй потрібно зателефонувати на «гарячу лінію» «Приватбанка» за номером 3700 та дочекавшись голосових підказок (два варіанта відповіді: або розширити кредитну лінію, натисніть 1, або відмовитись, натисніть 2).

Коли жертва шахрайства телефонує на «гарячу лінію» «Приватбанка» за номером 3700, банківська система відповідає на дзвінок та повідомляє, що абоненту передзвонять протягом двох хвилин. Оскільки на телефоні потерпілого було встановлено послугу: переадресація усіх вхідних дзвінків, дзвінок з банку надходить на номер телефона шахрая. Останній за допомогою голосових підказок поповнює рахунок свого мобільного телефону, кошти на поповнення якого йдуть з карткового рахунку потерпілого.

Потім, за допомогою сервісу «Мобільні гроші» компанії Київстар, гроші кошти з мобільного рахунку переводяться на картковий, а далі в готівковій формі отримуються у банкоматах «Приватбанка».

Способи приховування реалізуються як самостійне явище лише тоді, коли злочин вчинений, у багатьох випадках зареєстрований і щодо якого проводиться досудове розслідування.

Як вірно зазнач М. В. Салтевський, перспективи приховування кримінально протиправних діянь злочинець найчастіше формує так звані «штучні» умови для ефективної реалізації задуманого. У результаті чого в обстановці злочину відображаються основні властивості ознак вибраного способу злочину[46]. Приховування – це діяльність, спрямована на протидію розкриттю та розслідуванню шляхом приховання, знищення, маскування і фальсифікації слідів злочину, даних про особу злочинця та їх носіїв[47].

Типовим способом приховування шахрайства, учиненого в кіберпросторі є приховування електронних (цифрових) слідів, що здійснюється через відключення електронно-обчислювальної техніки; видалення електронних (цифрових) слідів (як-то: профіль у соціальній мережі, оголошення на платформі, переписку в месенджерах тощо) та інших джерел криміналістично значущої інформації (приховування, обмін, витрата злочинного доходу); використання спеціального програмного забезпечення, що приховує або змінює ідентифікатор IP-адреси і забезпечує конфіденційний зв'язок; знищення обладнання, яке використовувалось для вчинення злочину; надання неправдивих показань під час проведення слідчих (розшукових), негласних слідчих (розшукових) дій та інших процесуальних заходів; відома від дачі показань; забезпечення алібі; застосування впливу на співучасників, потерпілих, свідків та очевидців (використання компрометуючих матерів, залякування, фізична розправа тощо).

[46] Салтевський М. В. Криміналістика (у сучасному викладі) : підручник. Київ : Кондор, 2005. С. 430.

[47] Ковальчук О. В. Методика розслідування шахрайств, пов'язаного з діяльністю кредитної спілки / О. В. Ковальчук : дис …. доктор філософії. Львів, 2020. С. 69.

Типові сліди вчинення злочину посідають принципово важливе значення в системі криміналістичної складової, адже отримана слідова інформація при належному процесуальному оформленні набуває значення доказів.

Відповідно до загальноприйнятих положень криміналістики, сліди злочину трактують або як результат будь-якої матеріальної зміни початкової обстановки учинення злочину (слід у широкому розумінні), або як матеріально-фіксоване відображення зовнішньої будови одного об'єкта на іншому (слід у вузькому розумінні) – сліди-відображення. Останні складають головний зміст трасології[48]. Разом з тим дослідження механізму слідоутворення та самих слідів злочину є одним із напрямів дослідження наслідків злочину.

Традиційно сліди злочину поділяються на матеріальні (відбитки події на предметах, зміна обстановки події) та ідеальні (відбитки події у свідомості людей). Між тим, із розвитком технологій, суспільні відносини були трансформовані у кіберпростір, де внаслідок злочинної діяльності з'явився новий вид слідів – віртуальний. Окремі науковці-криміналісти ще визначають їх як «електронні (цифрові) сліди», під якими розуміють матеріальні невидимі сліди, що можуть бути виявлені, зафіксовані й вивчені за допомогою електронних (цифрових) пристроїв і містять будь-яку криміналістично значущу інформацію (відомості, дані), зафіксовану в електронному (цифровому) форматі на матеріальних носіях[49].

Тобто, для шахрайства, учиненого в кіберпросторі не є характерними типові сліди, залишені на місці події. Може навіть не існувати й самого місця події.

Проте, аналіз матеріалів правозастосовної практики дає підстави стверджувати, що джерелом електронних (цифрових) слідів, які свідчать про шахрайство, учинене в кіберпросторі, можуть бути:

1) електронні пристрої (комп'ютери, ноутбуки, планшети, смартфони тощо) (100 %);

---

[48] Шепітько В. Ю. Криміналістика. Енциклопедичний словник / В. Я. Тація. Харків : Право, 2001. С. 202.

[49] Авдєєва Г. К., Стороженко С. В. Електронні сліди: поняття та види. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* Вип. № 1 (77). Сєвєродонецьк, 2017. С. 170.

2) носії електронних даних (флеш-накопичувачі, компакт-диски, зовнішні вінчестери та ін.) (48 %);

3) електронні дані в інформаційних та комунікаційних системах (електронна скринька, профіль у соціальних мережах, Інтернет-сайти, платформи, додатки) (64 %);

4) електронні дані в комерційних системах (46 %);

5) мережеві маршрутизатори (22 %);

6) системи відеоспостереження (26 %);

7) продукти програмного забезпечення (14 %) (Додаток Е).

Задля якісного вилучення зазначених слідів злочину доцільно залучити фахівця з інформаційних систем та технологій.

Особливістю утворення ідеальних слідів є відсутність прямого контакту між взаємодіючими особами. Оскільки ідеальне відображення здійснюється у формі свідомості, то об'єктом, що відображає, є тільки людина як єдиний його носій[50]. До таких слідів відносяться показання потерпілого, свідків та підозрюваного. Їхнє оцінювання, насамперед про спосіб учинення шахрайства в кіберпросторі, повинно здійснюватися комплексно з урахуванням слідів інших видів, що знаходяться в синхронічному або поліхронічному зв'язку відносно конкретного досліджуваного проміжку часу.

Отже, підводячи підсумки, зазначено, що оперативно-розшукова характеристика шахрайств, учинених в кіберпросторі узагальнює особливості досліджуваного злочину, демонструє кореляційні зв'язки між її складовими та у практичному значені дозволяє ефективніше організувати процесу розкриття цього злочину, визначитись з його напрямом та необхідним комплексом слідчих (розшукових), негласних слідчих (розшукових) дій (далі – СРД, НСРД), а також правильних рішень щодо ефективного застосування сил, засобів і заходів оперативно-розшукової діяльності.

[50] Затенацький Д. В. Ідеальні сліди в криміналістиці (техніко-криміналістичні та тактичні прийоми їх актуалізації) : автореферат дис. … канд. юрид. наук. Харків, 2008. С. 14.

* * *

Отже, з'ясовано, що сучасний стан наукових досліджень характеризується тим, що: 1) дослідники різних країн розуміють важливість розкриття шахрайств, учинених в кіберпросторі та розробки методів боротьби з ними; 2) у дослідженнях активно вивчаються сучасні технічні засоби для виявлення шахрайств, учинених в кіберпросторі; 3) вітчизняні та зарубіжні дослідники розробляють методи й алгоритми аналізу підозрілих дій в кіберпросторі та профілактичні заходи для запобігання шахрайствам; 4) дослідники поєднують знання з різних галузей, таких як інформаційна безпека, кібербезпека, кримінальна судова експертиза, техніка, статистика тощо; 5) дослідними співпрацюють з правоохоронними органами та органами державного управління для впровадження розробок в реальну практику.

Акцентовано на основні причини збільшення кібернебезпек. Визначено, що кіберпростір має велике значення в сучасному світі, де віртуальна діяльність та обмін інформацією відіграють ключову роль в багатьох сферах життя. А з іншого боку, – окрім можливостей, несе в собі численні небезпеки, які можуть впливати на окремих громадян, організації та навіть держави.

Особливість розкриття, учинених у кіберпросторі, полягає у тому, що ці злочини відбуваються в електронному середовищі, і це викликає певні труднощі у відстеженні та ідентифікації.

Виокремлено фактори, які сприяють зростанню кількості шахрайств, учинених в кіберпросторі, а саме через: 1) зростання використання Інтернету; 2) технічний розвиток; 3) анонімність та віддаленість; 4) соціальну інженерію.

Надано авторське поняття «шахрайство, учинене в кіберпросторі» як суспільно небезпечне діяння, спрямоване на заволодіння чужим майном або придбання права на майно шляхом незаконних операцій з використанням електронно-обчислювальної техніки у віртуальному просторі (середовищі), де надається можливість комунікацій та/або реалізації суспільних відносин.

Розкрито складові оперативно-розшукової характеристики шахрайств, учинених в кіберпросторі. Зокрема, досліджено:

– кримінально-правову складову шахрайств, учинених в кіберпросторі (проаналізовано сутність злочину, визначено його об'єкт, предмет, об'єктивну сторону, суб'єкт, суб'єктивну сторону).

Наголошено, що головною кваліфікуючою ознакою є вчинення шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Таку ознаку утворюють лише такі операції, здійснення яких без електронно-обчислювальної техніки є неможливим. При цьому, злочин направлений не на стабільність функціонування електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та/або комп'ютерних мереж, мереж електрозв'язку, а на суспільні відносини з огляду заволодіння майном або правом на це майно.

– кримінологічну складову шахрайств, учинених в кіберпросторі (проаналізовано стан, динаміку та надано характеристику особи злочинця).

З'ясовано, що за останні роки простежується динаміка росту кількісних показників реєстрації досліджуваного злочину, проте успішно розкривається лише кожне 3 шахрайство, а в інших випадках, – не представляється можливим встановити особу злочинця. У зв'язку з цим, визначено типи злочинців залежно від рівня їхньої компетенції: дилетант, досвідчений фахівець, професіонал. У залежності від потенційного інтересу в кіберпросторі, як: корисливі, самоствердженні, побутові, егоїстичні, дезадаптовані.

Наголошено, що характеристика особи злочинця, яка вчиняє шахрайство у кіберпросторі, складна й динамічна, вона охоплює широкий спектр внутрішніх позицій особистості в різних сферах соціального буття.

З'ясовано, що шахрайство в кіберпросторі здебільшого вчиняються чоловіками, які є соціально благополучними, позитивно характеризуються за місцем проживання, роботи, навчання, віком від 25 до 45 років. Більшість шахраїв мають сильний дар уяви, здатність впливу і вміння переконувати. До особистих якостей шахрая належать його хитрість, брехливість, уміння

прихилити до себе оточуючих, знання способів підроблення документів. За своїм зовнішнім виглядом – це звичайні люди, які вміють себе «подати», обізнані в галузі психології. Вони спостережливі і мають швидку реакцію на обстановку, що змінюється. Шахраї використовують можливість перевтілення, встановлюють контакт з людьми різних типів, обирають стиль поведінки від конкретно сформованої обстановки. Внутрішній прояв такої особи полягає у відсутності в неї морально-вольових (етичних) стримуючих факторів, що спричиняє характерну зневагу до загальноприйнятих моральних цінностей суспільства. Тобто особа, яка вчиняє шахрайство є психологічно готовою для нехтування нормами моралі, діловими, дружніми стосунками. У зв'язку із тим, що шахрайство вчиняється з прямим умислом особа бажає настання суспільно небезпечних наслідків свого діяння, впливаючи на благополуччя потерпілого. Інколи, – ставлячи під загрозу виживання останнього.

Окремо встановлено основні причини та умови, що сприяють вчиненню шахрайства в кіберпросторі.

– криміналістичну складову шахрайств, учинених в кіберпросторі (з'ясовано типові способи, сліди вчинення та приховування злочину).

Здійснено розподіл способів учинення шахрайств залежно від: періодичності вчинення злочину; сфери надання послуг; кількості задіяних злочинців; предмета посягання; способів введення в оману або зловживання довірою; місця вчинення злочину (через встановлення місця реєстрації IP-адреси електронно-обчислювальної техніки); способу підготовки до вчинення злочину.

Визначено типові способи вчинення та приховування шахрайств у кіберпросторі в умовах воєнного стану. З'ясовано джерела електронних (цифрових) слідів, які свідчать вчинення шахрайств у кіберпросторі.

Розділ 2
ОРГАНІЗАЦІЯ РОЗКРИТТЯ ШАХРАЙСТВ, УЧИНЕНИХ В КІБЕРПРОСТОРІ

2.1. Оцінка первинної інформації та коло обставин, що підлягають встановленню під час розкриття шахрайств, учинених в кіберпросторі.

Розкриття будь-якого злочину розпочинається з моменту його виявлення. Процес виявлення є кримінальною процесуальною діяльністю, спрямованою на перевірку первинних фактичних відомостей про ознаки підготовки чи вчинення злочинцем такого суспільно небезпечного діяння. Тобто, полягає в отриманні первинної інформації про кримінальну подію та належній її фіксації у відповідних процесуальних документах, а сама діяльність із розкриття злочину реалізується через пошук та виявлення необхідної інформації, яка свідчить про вчинення злочину.

Сутність розкриття злочину тісно пов'язано з розшуковою діяльністю і значною мірою залежить від ефективності проведення процесуальних дій і оперативно-розшукових заходів (далі – ОРЗ), що здійснюється слідчим у взаємодії з уповноваженими оперативними підрозділами.

Слід зазначити, що у системі розкриття злочину одним із важливих напрямів є робота слідчого та оперативних підрозділів по «гарячих слідах», за результатами чого можна:

– установити просторово-часові зв'язки між окремими слідами злочину та обставинами події;

– ідентифікувати особу злочинця та затримати її в установленому законом порядку;

– з'ясувати причини відсутності або наявності окремих фактів, що суперечать природному перебігу аналогічних подій (негативні обставини).

Підтвердженням такої думки, є позиція О. А. Самойленка, який зазначає, що 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, що вимагають їх врахування з огляду забезпечення судової перспективи таких проваджень[51].

Як правило, ознаки кримінального правопорушення можуть бути виявлені трьома способами:

– ужиття оперативно-розшукових заходів, які передують початку досудового розслідування;

– звернення громадян, а також представниками державних організацій під час здійснення перевірки та контрольних заходів;

– безпосередньо слідчим, прокурором і судом.

Відповідно до чинного кримінального процесуального законодавства України, будь-яка процесуальна діяльність, – зокрема розслідування кримінального правопорушення, у тому числі й шахрайства, учиненого в кіберпросторі, можлива лише в межах здійснення досудового розслідування після внесення відповідних відомостей до Єдиного реєстру досудових розслідувань (далі – ЄРДР).

Процесуальний порядок внесення відомостей до ЄРДР регламентований ч. 1 ст. 214 КПК України, відповідно до якого уповноважені суб'єкти (прокурор, слідчий, дізнавач), зобов'язані невідкладно, але не пізніше 24 годин після отримання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення ним із будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, внести відповідні відомості до ЄРДР, розпочати розслідування та через 24 години з моменту внесення таких відомостей надати заявнику витяг із зазначеного реєстру[52].

[51] Самойленко О. А. Криміналістичний та правовий аналіз злочинної діяльності в мережі Інтернет. *Порівняльно-аналітичне право*. Вип. № 4. 2015. С. 409.

[52] Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. *Офіційний вебпортал Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

Відмова у прийнятті та реєстрації заяви чи повідомлення про кримінальне правопорушення не допускається.

Крім того, відповідно до Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події, затвердженого наказом МВС України від 08.02.2019 № 100, а також Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України, затвердженої наказом МВС від 27.04.2020 № 357 (далі – Інструкція № 357)[53], оперативний черговий органу (підрозділу) поліції або інша уповноважена службова особа, отримавши інформацію про вчинення кримінального правопорушення, відразу реєструє її в журналі єдиного обліку заяв і повідомлень про кримінальні правопорушення та інші події з використанням інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України». Типовий алгоритм попередніх дій та заходів групи реагування передбачений Інструкцією № 357, Інструкцією з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушення, їх виявленні та розслідуванні, затвердженої наказом МВС від 07.07.2017 № 575, Інструкцією про порядок залучення працівників органів досудового розслідування поліції та Експертної служби МВС України як спеціалістів для участі в проведені огляду місця події, затвердженої наказом МВС України від 03.11.2015 № 1339[54].

[53] Порядок ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події : Наказ МВС України від 08.02.2019 № 100. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0223-19#Text; Інструкція з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України : наказ МВС України від 27.04.2020 № 357. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0443-20#Text.

[54] Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07.07.2017 № 575. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text; Інструкція про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведення огляду місця події : наказ МВС України від 03.11.2015 № 1339. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z1392-15#Text.

Також Порядок введення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події, затвердженого наказом МВС України від 08.02.2019 № 100, конкретизує, що саме відноситься до джерел інформації про кримінальні правопорушення й інші події, а саме ними є:

- заяви (повідомлення) осіб, які надходять до органу (підрозділу) поліції, особи, уповноваженої на здійснення досудового розслідування, або службової особи, уповноваженої на прийняття та реєстрацію заяв (повідомлень);
- самостійно виявлені слідчим (дізнавачем) або іншою посадовою особою органу (підрозділу) поліції з будь-якого джерела обставин кримінального правопорушення;
- повідомлення осіб, які затримали підозрювану особу під час учинення або замаху на вчинення кримінального правопорушення чи безпосередньо після вчинення кримінального правопорушення, чи під час безперервного переслідування особи, яка підозрюється в його вчиненні тощо.

Вивчення матеріалів кримінальних проваджень, пов'язаних із розкриттям шахрайств, учинених в кіберпросторі, свідчить про те, що приводом для початку досудового розслідування є:

1) отримання заяв від громадян, які стали жертвами шахрайських дій – 60 %;

2) отримання заяв від громадян про роботу сумнівної вебсторінки чи діяльність організацій – 8 %;

3) повідомлення від підприємств, установ, організацій, представників влади, посадових осіб, журналістів тощо – 12 %;

4) повідомлення від невстановленої особи (анонімний дзвінок на лінію «102» або анонімний лист з викладеними обставинами вчинення злочину) – 4 %;

5) самостійне виявлення уповноваженою особою з різних джерел обставин, що свідчили про вчинення злочину (як правило, при моніторингу інтернет-ресурсів, медіа, форумів тощо) – 16 % (Додаток Е).

Слід зазначити, що інформацію про вчинення шахрайства в кіберпросторі не отримується взагалі або отримується вкрай рідко з такого джерела як повідомлення осіб, які затримали підозрювану особу під час учинення або замаху на вчинення злочину чи безпосередньо після вчинення злочину, або під час безперервного переслідування особи, яка підозрюється в його вчиненні.

Причиною цьому, – як пише С. В. Самойлов, є технічна сторона способу вчинення злочину, його географічне розташування злочинця та потерпілого, а також велика розбіжність у часі між вчиненими діями та настанням наслідків[55].

Вочевидь це є змістом початкового етапу розслідування та впливає на подальший його хід, безпосередньо залежить саме від повноти відомостей на момент внесення їх до ЄРДР, з одночасним вивченням та оцінкою. Адже підстави для початку досудового розслідування визначає слідчий шляхом правової оцінки джерел отриманої інформації про наявність у них обставин, що можуть свідчити про вчинення злочину (його ознаки) та кола причетних осіб (ч. 1, пп. 3-5 ч. 5, ч. 6 ст. 214 КПК України).

На цьому етапі – оцінки первинної інформації, слідчий обмежений у проведенні процесуальних заходів, бо чинне законодавство забороняє проводити будь-які процесуальні дії, а їх проведення до внесення відомостей до ЄРДР або без такого внесення тягне за собою відповідальність, установлену законом.

У такому контексті доречна позиція окремої плеяди науковців, які стверджують, 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 промірним є розуміння й дослідження цієї діяльності саме як

[55] Самойлов С. В. Шахрайства на Інтернет-аукціонах як один із способів скоєння шахрайств з використанням мереж Інтернет (криміналістична характеристика способу вчинення). *Форум права.* Вип. № 4. 2011. С. 648.

самостійного провадження»[56]. Тобто, слідчий у взаємодії з оперативним підрозділом на етапі оцінки первинної інформації можуть визначити основні напрями розкриття злочину та вибору спектру процесуальних заходів. Обсяг такого інструментарію залежить від визначення попередньої правової кваліфікації кримінального правопорушення із зазначенням статті (частини статті) Закону України про кримінальну відповідальність, відомості про які обов'язково необхідно зазначити під час внесення відомостей до ЄРДР відповідно до ч. 5 ст. 214 КПК України. Правильна попередня правова кваліфікація кримінального правопорушення впливає і на порядок проведення досудового розслідування.

О. В. Тарасова у своїх дослідженнях акцентує увагу на цій проблематиці, бо як свідчить правозастосовна практика практичні працівники та судді по-різному кваліфікують шахрайство, учинене в кіберпросторі. Наприклад, злочинні дії з розміщення на певних сайтах неправдивої інформації про продаж неіснуючих товарів та отримання винним за них передоплати деякі суди кваліфікують як шахрайство, учинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки (ч. 4 ст. 190 КК України). Інші суди подібні діяння перекваліфіковують на ч. 1 або ч. 2 ст. 190 КК України, обґрунтовуючи це тим, що перерахування грошей потерпілими на рахунок винного не є незаконною операцією з використанням електронно-обчислювальної техніки[57]. Теж і стосується вчинення такого діяння під час дії воєнного стану. Перекваліфікація діяння на ч. 3 ст. 190 КК України.

Нагальна проблема полягає в конструкції складу злочину, бо поза увагою залишається сам механізм злочинних дій, наприклад, реєстрація на сайтах, розміщення неправдивих оголошень, незаконне отримання грошових коштів у віртуальному просторі (середовищі), там де і відбуваються суспільні відносини. Оскільки шахрайство, вчинене у кіберпросторі характеризується різними

[56] Кримінальний процес : підручник / В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. С. 334.

[57] Тарасова О. В. Удосконалення законодавства щодо кримінальної відповідальності за шахрайство, учинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки. *Актуальні проблеми держави і права.* Вип. № 72. 2014. С. 485–487.

способами за допомогою новітніх технологій, то кваліфікуюча ознака, передбачена ч. 4 ст. 190 КК України у повній мірі не відображає всіх цих можливостей.

Задля мінімізації ускладнень, з якими стикаються слідчі та оперативні підрозділи під час оцінки первинної інформації, доцільно:

– уніфікувати окремі норми КПК України, розширивши спектр процесуальних дій (можливостей) до внесення відомостей в ЄРДР;

– деталізувати момент початку розслідування, розмежувавши та позбавивши залежності в цьому питані від норм Положення про ЄРДР, порядок його формування та ведення, затвердженого наказом Генерального прокурора від 30.06.2020№ 298;

– консолідувати норми КК України з урахуванням нормативної бази про забезпечення безпеки у кіберпросторі, визначити єдину термінологію для використання правозастосовними інституціями.

Як вже зазначалось, після оцінки первинної інформації, визначаються напрями розкриття будь-якого кримінального правопорушення, у тому числі і шахрайства, учиненого в кіберпросторі, що тісно пов'язано з обставинами, що підлягають доказуванню у кримінальному провадженні.

Відповідно до ч. 2 ст. 91 КПК України, доказування – це збирання, перевірка та оцінка доказів із метою встановлення обставин, що мають значення для кримінального провадження. Предметом доказування вважається сукупність типових обставин, передбачених чинним кримінальним процесуальним законодавством, що мають загальний і, в окремих випадках, спеціальний характер. У кожному кримінальному провадженні коло цих обставин не може бути однаковими, оскільки межі доказування орієнтовані на кримінально-правові ознаки кримінального правопорушення, що, у свою чергу, визначають особливості як самого процесу розслідування та розкриття, так і процесу доказування.

Крім того, під час розкриття злочину часто виникає необхідність встановлювати обставини, що не мають правового значення і які не потребують

доведення, але мають вагоме методичне та тактичне значення для ефективного розслідування кримінального правопорушення.

Відповідно до ч. 1 ст. 91 КПК України визначено низку обставин, які підлягають доказуванню:

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

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

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

4) 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;

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

6) обставини, які підтверджують, що грошові кошти, 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 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;

7) обставини, що є підставою для застосування до юридичних осіб заходів кримінально-правового характеру[58].

[58] Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

Вказані обставини є визначальними, базовими для всіх злочинних діянь без винятку, а також означенням для спрямовані діяльності слідчого та оперативних підрозділів. Ураховуючи, що кримінальний процес є частиною галузі кримінально-правового циклу та задля конкретизації обставин досліджуваного злочину доречно використати й інший термін, як «обставини, що підлягають встановленню».

Це видається логічним, оскільки коло обставин, пов'язаних з доказуванням події кримінального правопорушення, винуватості особи в його вчиненні, форми вини, мети і мотивів, деталізується і залежить від того, як сформульовано склад кримінального правопорушення у відповідній нормі кримінального закону. Встановлення цих обставин має послідовно давати відповіді на класичне запитання юриспруденції: «що?», «де?», «коли?», «ким?», «яким чином?» тощо[59].

Також вважаємо доречним урахувати думку попередників за останні роки.

Так, С. В. Чучко виокремлює чотири групи обставин, що підлягають встановлення, під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет:

1) обставини, що стосуються події шахрайства при купівлі-продажу товарів через мережу Інтернет (відомості про час, місце вчинення шахрайства, відомості про спосіб його вчинення; відомості про знаряддя (засоби) злочину; відомості про сліди злочину; відомості про предмет злочинного посягання;

2) 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);

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

[59] Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. …. доктор філософії. Київ, 2021. С 94.

4) 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)[60].

На думку Т. В. Коршикової, на попередньому етапі досудового розслідування кримінального провадження, пов'язаного з шахрайством, учиненого з використанням електронно-обчислювальної техніки, доцільно об'єднати в наступні групи:

1) обставини, що стосуються самої події кримінального правопорушення;

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

3) вид і розмір шкоди, завданої кримінальним правопорушення, - відомості про предмет злочинного посягання (його кількісні та якісні характеристики);

4) відомості, що характеризують особу підозрюваного;

5) обставини, які пом'якшують та обтяжують покарання;

6) звільнення від кримінальної відповідальності;

7) обставини, що є підставою для застосування до юридичних осіб заходів кримінально-правового характеру[61].

І. О. Коваленко визначив систему обставин, що підлягають встановлення у кримінальному провадженні за фактом вчинення шахрайств у сфері використання банківських електронних платежів. До її складу входять:

1) обставини, що характеризують вчинення шахрайства у сфері використання банківських електронних платежів (відомості про час, місце

[60] Чуйко С. В. Розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет : дис. ... доктор філософії. Дніпро, 2021. С. 108–109.

[61] Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки :.дис. ... доктор філософії. Київ, 2021. С. 96.

вчинення шахрайства, відомості про спосіб його вчинення, наприклад: використання ботів для спаму та потрапляння шкідливих програм до комп'ютерного забезпечення потерпілого; використання реквізитів картки, які викрадені з серверів магазинів електронної торгівлі, платіжних та розрахункових систем, із персональних комп'ютерів користувачів; відомості про сліди протиправного діяння; визначення 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 шахрайських програм, технічних прийомів); засоби, що використовуються при скоєнні правопорушення: це можуть бути як технічні, такі як електронно-обчислювальна техніка, смартфони, планшети, модеми, маршрутизатори, так і програмні, такі як VPN, браузери, графічні редактори, програми кодування інформації);

2) обставини, котрі відносяться до характеристики особи злочинця та потерпілого (кількість правопорушників – визначення ролі кожного з них);

3) причинно-наслідкові зв'язки: наявність певного зв'язку між діями винних осіб та їх результатами; з'ясування причин та умов, що сприяли вчиненню протиправного діяння);

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

5) кваліфікуючі ознаки стосовно розміру шкоди завданої протиправним діянням та обставини, що є підставою для звільнення від кримінальної відповідальності;

6) вид та розмір шкоди, завданої вчиненням шахрайства у сфері використання банківських електронних платежів[62].

З огляду на вказане та враховуючи узагальнення правозастосовної практики, пропонуємо зміст обставин, що підлягають встановленню під час

[62] Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. ... доктор філософі. Дніпро, 2022. С. 107–108.

розкриття шахрайств, учинених в кіберпросторі, виокремити чотири взаємопов'язані групи:

1) обставини стосовно події злочину:

– відомості про факт вчинення шахрайства в кіберпросторі;

– відомості про час учинення шахрайства – тривалість та періодизація;

– відомості про просторові межі, у яких відбулось шахрайство;

– відомості про особу потерпілого;

– відомості про способи вчинення шахрайства;

– відомості про предмет посягання;

– відомості про характер і розмір завданої шкоди;

– відомості про джерела електронних (цифрових) слідів;

2) інші обставини злочину:

2.1) відомості про причинно-наслідковий зв'язок:

– обставини, що сприяли вчиненню шахрайства – відповідні причини та умови;

– обставини стосовно споріднених видів кримінальних правопорушень, як-то вчинення кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

– обставини постзлочинної діяльності;

2.2) відомості про особу свідків;

3) обставини стосовно підозрюваного:

– відомості про особу підозрюваного – дані, що характеризують його як особу та особистість;

– відомості про винуватість, мотив та мету підозрюваного;

– відомості про співучасть у вчиненні шахрайства, у тому числі споріднених видів кримінальних правопорушень;

4) обставини, які можуть мати додаткове значення в кримінальному провадженні:

– обставини, що впливають на ступінь тяжкості вчиненого шахрайства, обтяжують чи пом'якшують покарання;

– обставини, що є підставами для закриття кримінального провадження чи звільнення від кримінальної відповідальності або покарання;

– розмір процесуальних витрат.

На наш погляд, встановлення всіх цих обставин сприятиме швидкому розкриттю шахрайства, учиненого в кіберпросторі, повному і неупередженому розслідуванню – з'ясуванню юридично значущих обставин, які будуть доведені або спростовані в цілях обґрунтованого притягнення певної особи до відповідальності в міру своєї вини.

2.2. Планування та взаємодія під час розкриття шахрайств, учинених в кіберпросторі.

У сучасному цифровому світі, де технології невпинно розвиваються, зростає ймовірність шахрайств, учинених в кіберпросторі – зловживання та недобросовісне використання Інтернету та комп'ютерних систем з метою незаконного здобутку, вивчення конфіденційної інформації, а також завдання шкоди власникам даних. Це створює серйозні загрози для приватності, фінансової стабільності та безпеки як індивідів, так і організацій. З метою протидії цим загрозам, розкриття та подолання шахрайств учинених в кіберпросторі стає надзвичайно важливим завданням для правоохоронних органів, технічних експертів та суспільства в цілому.

Розкриття шахрайств, учинених в кіберпросторі, вимагає комплексного підходу та глибокого розуміння сучасних технологій, адже злочинці вдосконалюють свої методи та використовують складні атаки. Ідентифікація, зупинення та покарання шахраїв у кіберпросторі потребує ефективної співпраці між правоохоронними органами, кібербезпековими експертами, провайдерами послуг та іншими зацікавленими сторонами.

Проблемам планування розкриття шахрайств, учинених в кіберпросторі приділялась увага у роботах багатьох науковців, як: Д. С. Азарова, А. І. Анапольського, Б. В. Андрєєва, Р. С. Атаманова, О. А. Баранова, Ю. М. Батуріна, В. М. Бутузова, Т. В. Варфоломеєва, М. С. Вертузаєва, О. Г. Волєводза, В. Д. Гавловського, С. В. Головкіна, В. О. Голубєва, В. Г. Гончаренка, В. А. Губанова, М. В. Гуцалюка, Д. О. Зикової, М. І. Камлика, М. В. Карчевського, Н. Ю. Кириленка, С. М. Князєва, В. А. Колесника, А. А. Комарова, О. І. Котляревського, А. В. Крижевського, В. В. Крилова, О. В. Курмана, В. Д. Ларичева, А. К. Лебедєва, О. В. Лисодєда, В. Б. Міщенка, О. І. Мотляха, О. Л. Мусієнка, В. І. Оборського, Т. В. Охрімчука, Т. А. Пазинича, Л. П. Паламарчука, Б. В. Романюка, С. В. Самойлова, О. В. Смаглюка, О. М. Стрільціва, О. І. Усова, В. П. Хорста, В. С. Цимбалюка, С. С. Чернявського, В. П. Шеломенцева, О. М. Юрченка та ін. Водночас, на сьогодні потребують подальшого дослідження проблемно-дискусійні аспекти особливостей розкриття шахрайств, учинених в кіберпросторі.

Так, згідно із історичним походженням, поняття «організація» (англ. «organization») виникає з давньогрецького терміну «органон», що перекладається як «інструмент» або «знаряддя». Цей термін належить до сфери багатозначного вживання та широко застосовується в різноманітних галузях наукового пізнання (філософія, математика, економіка, соціологія тощо) і в практичній сфері.

Наприклад, термін «організація» найчастіше ототожнюють із наступними концептуальними аспектами: внутрішня структура, взаємопов'язаність елементів цілісної системи; комплекс процесів та заходів, спрямованих на досягнення передбачених цілей системи; об'єднання індивідів, чиє спільне дієве спрямування прагне реалізувати програми, ґрунтуючись на певних принципах та процедурах. Ця дефініція виокремлює об'єкт, його інтегральні властивості, а також взаємодію та діяльність (процес) у контексті різних семантичних відтінків: від опису соціальної структури чи інституту (аспект статики) до позначення динамічного процесу управління як цілеспрямованої та свідомо скоординованої

діяльності. Відповідно до думки Г. А. Ханя, поняття «управління» інкорпорує методи впливу на систему; термін «структура» відображає статичний опис елементів та взаємозв'язків системи, водночас поняття «організація» описує динамічну компоненту системи, націлену на забезпечення функцій координації та субординації[63].

Наявність рівнів розподілу організаційної структури при розкритті кримінальних правопорушень визначає уніфіковану концепцію цього процесу. Всі рівні організації розкриття взаємодіють між собою, взаємовпливаючи один на одного. Кожен з цих рівнів у певній мірі залежить від інших, конфігуруючи, у свою чергу, інші складові. Загалом, ці рівні утворюють комплексний організаційний процес системи розкриття кримінальних правопорушень.

Проте важливо відрізняти організаційну структуру управління діяльністю слідчого апарату від організації робіт з розкриття кримінальних правопорушень, оскільки перше включає в себе управління, що також має свою власну організаційну структуру, але вона інтегрується в загальний процес управління. Другий аспект відображає істотність організаційної структури під час реалізації діяльності слідчого у взаємодії з оперативними підрозділами під час розкриття кримінальних правопорушень, зокрема шахрайств, учинених в кіберпросторі.

Враховуючи аналіз поглядів провідних вчених на тему організації та управління, можна виокремити кілька течій, зосереджуючи увагу на абстрактно-логічному, конкретно-логічному, управлінсько-організаційному, організаційно-управлінському та спонтанно-організаційному підходах. Залежно від підходу, організацію можна розглядати як важливу складову управління, або як функціональний аспект управління. Водночас, управління передбачає використання організаційних структур. Отож, організація та управління, хоча і переплетені, але мають відмінні семантичні діапазони. Можна зазначити, що організація – це діяльність, що спрямована на створення структурного порядку об'єкта.

[63] Хань Г. А. Теоретичні засади планування та організації розслідування злочинів : дис. … канд. юрид. наук. Донецьк, 2007. С. 98.

Вчений В. О. Олішевський[64] прийшов до висновку, що в сучасних трактуваннях поняття «організація» у криміналістичній науці лежать в основі дві концептуальні парадигми. Перша парадигма передбачає, що «організація» відтворює забезпечення самого процесу розслідування, тоді як друга концепція підкреслює, що «організація» відображає створення внутрішньої структури для розкриття кримінальних правопорушень. Сам же вчений уточнює, що «організація розслідування кримінальних правопорушень» розглядається як сприяльна активність до розслідування, яка досягається через систематизацію елементів розслідування та впровадження сприятливих умов для розкриття кримінального правопорушення.

Цитовані погляди, на наш погляд, виражають загальний тенденційний характер: «організація є постійним активним фактором, що іманентно притаманний діяльності, спрямованій на протидію злочинності». У контексті соціальної діяльності організація та управління взаємодіють через діалектичний та взаємозалежний процес, включаючи структуру системи, її структурування та освоєння через управління. «Організація розкриття» визначає супутню діяльність у вигляді структурного упорядкування, яке визначає ключові структурні компоненти, що створюють основи для методології розкриття шахрайств, учинених в кіберпросторі та його практичної реалізації.

Аналіз правозастосовної практики дає підстави стверджувати, що *організація розкриття шахрайств, учинених в кіберпросторі* сприймається як типова модель, що включає в себе аналіз первинної інформації щодо обставин злочину, формулювання версій, визначення цілей та розробку плану. Як результат, якість та результативність уже під час розслідування залежать від обсягу вихідної та поточної інформації, яка формує підґрунтя для формування діяльності слідчого в рамках кримінального провадження. Версія, як інструмент пізнання, виступає засобом для визначення цілей розслідування та передумова

[64] Олішевський О. В. Поняття організація розслідування злочинів. *Боротьба зі злочинністю та забезпечення громадського порядку: проблеми теорії та практики.* Харьків : ХНУВС, 2009. С. 78–79.

для планування, що спрямовує діяльність слідчого під час збору, дослідження та оцінки доказів.

Цілі формуються через аналіз обставин, що підлягають встановленню в рамках кримінального провадження. Виявлення та аналіз інших обставин, таких як проміжні (наприклад, визначення місцезнаходження винної особи, її затримання), конкретизують окремі завдання розслідування. Ці завдання обумовлені сутністю СРЗ, НСРД та ОРЗ, зокрема, визначенням їхніх цілей, організацією та тактикою проведення[65].

Результати системного аналізу правозастосовної практики вказують на те, що формування цілей та індивідуальних завдань під час розкриття та розслідування шахрайств, зокрема тих, що вчинені в кіберпросторі, обумовлено комплексом умов, які визначають структуру та якість вказаних видів діяльності. До цих умов належать:

– глибоке розуміння слідчими та оперативними підрозділами процесуальних норм і криміналістичних рекомендацій, пов'язаних із встановленням обставин злочину;

– вміння слідчого у взаємодії з оперативними підрозділами визначати тактичний вектор розкриття та розслідування, базуючись на обсязі орієнтовної інформації та наявних доказах у кримінальному провадженні;

– наявність необхідних засобів криміналістичної техніки, матеріально-технічного забезпечення та відповідних ресурсів для своєчасного застосування;

– професійна готовність слідчого та оперативних підрозділів здійснювати вибір та реалізацію належних дій та заходів, відповідно до характеру ситуації на початковому та подальших етапах розслідування;

– обізнаність слідчого щодо учасників розкриття та розслідування, форм їх співпраці, характеру позиції зі сторони підозрюваного та інших зацікавлених осіб.

[65] Вітвітцький С. С., Волобуєва О. О., Волобоєв А. О. Методика розслідування незаконного поводження зі зброєю та бойовими припасами : монографія. Київ : ВД «Дакор», 2021. С. 129.

Взаємодія є необхідною передумовою для успішного виконання будь-якої спільної діяльності. Це також стосується розкриття злочинів, оскільки ефективне поєднання зусиль та ресурсів правоохоронних органів забезпечує швидке здійснення заходів щодо притягнення винних до відповідальності за злочинну діяльність.

Наприклад, розкриття шахрайств, учинених в кіберпросторі потребує спільних заходів та проведення процесуальних дій від відповідних підрозділів Національної поліції.

Процес стратегічного планування розкриття шахрайств, учинених в кіберпросторі, включає такі етапи, як:

– аналіз слідчої ситуації, що передбачає глибокий розгляд наявної інформації, зокрема обставин, вчинення злочину та можливих способів діяльності злочинців;

– вибір основного напрямку розкриття злочину, де необхідно зробити обґрунтований вибір шляхів і методів ведення розслідування з урахуванням особливостей цього виду злочинів у кіберпросторі;

– визначення необхідних сил та засобів, що включає визначення кадрового та матеріально-технічного забезпечення, а також врахування можливих обмежень та викликів;

– розробка письмового плану в разі потреби, де формалізується послідовність дій та заходів, які необхідно здійснити для досягнення успішного результату;

– здійснення контролю над виконанням плану та його корекція, оскільки ускладнення процесу може відбутися через зміни в кіберпросторі, включаючи воєнний стан або інші несподівані фактори.

Взаємодія слідчого з оперативними підрозділами, підприємствами, установами, громадськістю та медіа (засобами масової інформації) передбачає спільну та договірну діяльність, спрямовану на розкриття, розслідування та запобігання злочинам. Ця взаємодія базується на взаємозалежності їхніх дій, яка

допомагає збалансувати повноваження, методи та ресурси, характерні для кожного учасника співробітництва.

Суть співробітництва полягає в гармонійній діяльності різних компонентів однієї чи декількох систем. Кожен суб'єкт співробітництва працює в рамках своїх повноважень, методів та ресурсів. Це сприяє створенню ефективної взаємодії, а роль координатора діяльності зазвичай відводиться слідчому. Особливі способи взаємодії між слідчим та іншими учасниками називаються формами співробітництва.

Аналіз наукових підходів до взаємодії слідчого з іншими учасниками дає можливість уточнити основи їхньої класифікації:

1) нормативно-правова регламентація:

а) процесуальні форми (передбачені КПК України): надання доручень співробітникам оперативних підрозділів щодо проведення С(Р)Д та НС(Р)Д (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);

б) 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:

а) міжнародна взаємодія;

б) міжвідомча взаємодія;

в) внутрішньовідомча взаємодія (між різними підрозділами одного відомства);

3) стадія кримінально-процесуальної діяльності:

а) взаємодія до початку кримінального провадження (в рамках оперативно-розшукової справи та під час попередньої перевірки інформації про злочин);

б) взаємодія в ході здійснення досудового розслідування;

в) взаємодія на стадії судового розгляду.

Взаємодія слідчого з оперативним підрозділом. Оперативний працівник, згідно зі ст. 7 Закону України «Про оперативно-розшукову діяльність»[66], зобов'язується для своєчасного виявлення і припинення злочинів уживати необхідних оперативно-розшукових заходів, тим самим здійснювати оперативно-розшукову діяльність. Термін «оперативно-розшукова діяльність» описує методи розшуку, які використовуються практично, швидко, надійно та конфіденційно, і це може вплинути на хід справи. Деякі експерти підкреслюють важливу роль оперативно-розшукової діяльності у забезпеченні інформаційних потреб кримінального процесу. Проте, форми та засоби такої діяльності чітко визначені законодавством, що підкреслює її виключно правовий характер та незалежність як окремого галузевого напрямку знань.

Злочини в кіберпросторі, особливо через їхній специфічний та недостатньо вивчений характер учинення, представляють значну загрозу для суспільства. Тому відповідно до п. 21 ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України»[67], однією з важливих складових функціонування кібербезпеки є реалізація оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття кіберзлочинів, які загрожують

[66] Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

[67] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

миру та безпеці людства. Також це включає розслідування, переслідування, оперативну реакцію та протидію кіберзлочинам, розвідувально-підривній, терористичній та іншій небезпечній діяльності в кіберпросторі, яка завдає шкоди інтересам України, включаючи використання мережі Інтернету відповідно до воєнних цілей.

Виходячи з вмісту норм законів України «Про оперативно-розшукову діяльність», «Про Національну поліцію» та «Про Службу безпеки України», а також наказів Національної поліції України, суб'єктами оперативно-розшукової діяльності, яким доручено завдання протидіяти кіберзлочинам, є Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України (далі – ДКІБ) та ДКП[68].

Підрозділи ДКІБ є відповідальними за проведення оперативно-розшукових дій з більшістю кіберзлочинів, що здійснюються з політичних мотивів. Це стосується злочинів, які зазвичай підпадають під слідчі органи безпеки, які передбачені статтями 109, 110, 110-2, 111, 112, 113, 114, 114-1, 258-258-5, 330, 436 Кримінального кодексу України. Відповідно до Стратегії кібербезпеки України[69], що була затверджена Указом Президента України від 15.03.2016 року № 96/2016, на Службу безпеки України покладено широкий спектр завдань, включаючи боротьбу із шахрайствами, учинених в кіберпросторі, протидію кібертероризму та кібершпигунству, а також перевірку готовності об'єктів критичної інфраструктури перед можливими кібератаками та кіберінцидентами щодо державних електронних інформаційних ресурсів та в сфері державної безпеки.

Згідно з пунктом 2.1 Положення про Департамент кіберполіції Національної поліції України (ДКП), його підрозділи мають повноваження для

[68] Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.; Про Національну поліції : Закон України від 02.07.2015 № 580-VII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/580-19#Text; Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2229-12.

[69] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.04.2026 року № 96/2016. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text.

протидії кримінальним правопорушенням, вчиненим з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку[70]. Ця сфера діяльності визначається як «протидія кіберзлочинності». Україна має правові основи боротьби з кіберзлочинами, зокрема на основі Конвенції Ради Європи про кіберзлочинність. Отже, оперативні підрозділи ДКП мають обов'язок використовувати власні методи та засоби, згідно з їхніми повноваженнями, для протидії злочинам, які передбачені статтями 163, 176, 185, 190, 200, 301, 361–363-1 Кримінального кодексу України.

Деякі підрозділи ДКП спеціалізуються на забезпеченні досудового розслідування та виконанні доручень слідчого, пов'язаних з отриманням електронних (цифрових) доказів. Ця сфера в наукових колах називається «комп'ютерна криміналістика» або «форензика». Спеціалісти з комп'ютерних технологій, що працюють у цих підрозділах, відіграють важливу роль у здійсненні стратегічних заходів і оперативно-розшукової діяльності.

Слід зазначити, що Національна поліція України, відповідно до § 3 Стратегії кібербезпеки України, входить до складу Національної системи кібербезпеки, діє як орган, що забезпечує захист прав і свобод людини та громадянина, інтересів суспільства й держави від злочинів у кіберпросторі. Вона здійснює заходи для запобігання, виявлення, припинення та розкриття таких злочинів[71]. Однак підрозділи ДКП виконують завдання, спрямовані на сприяння в попередженні, виявленні та припиненні кримінальних правопорушень, які вчинені в кіберпросторі та підпадають під слідчу компетенцію інших департаментів Національної поліції України, наприклад, Департаменту карного розшуку. Таким чином, діяльність міжтериторіальних підрозділів ДКП обмежується застосуванням власних методів і засобів для здійснення своєчасного реагування та отримання інформації про злочини, учинені в кіберпросторі.

[70] Департамент кіберполіції України. *Офіційний сайт.* URL: https://cyberpolice.gov.ua/contacts/.

[71] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про стратегію кібербезпеки України» : Указ Президента України. *Офіційне інтернет-представництво.* URL: https://www.president.gov.ua/documents/4472021-40013.

Перед початком кримінального провадження, слідчі та оперативні підрозділи повинні здійснювати спільну діяльність, зокрема, проводити перевірку отриманих відомостей про злочин. Тільки в цьому випадку суб'єкт перевірки може набути якостей, які не є йому властивими окремо. Наприклад, якщо сутність події вказує на можливість багатьох джерел доказів – засобів комп'ютерної техніки (які містять сліди злочину), то оперативний працівник спільно зі слідчим визначатимуть, які пристрої потрібно підтвердити документально під час перевірки первинних відомостей. Такий підхід сприяє прискоренню процесу збору доказів слідчому, оскільки на початку провадження слідчий зможе зазначити підстави для обґрунтування клопотання до слідчого судді стосовно здійснення обшуку, комплексу НС(Р)Д, а також доступу до речей і документів.

У цьому контексті, можна виділити такі рекомендації для оцінки матеріалів первинної перевірки з приводу злочинів, вчинених у кіберпросторі.

По-перше, намагання персоналізувати інформацію про користувача (можливого злочинця) з гласного джерела є недоцільним. Такі технології як децентралізований обмін та зберігання інформації, анонімізація доступу до ресурсів мережі Інтернет (проксі-сервіси, віртуальні приватні мережі (VPN), анонімайзери) ускладнюють можливість підтвердження персональних даних користувача-злочинця. Власники інформаційних систем та інформації часто знаходяться за межами держави або готові надати інформацію лише на підставі ухвали слідчого судді.

По-друге, інформацію, подану в рапорті інспектора ДКП, слідчий може вважати достовірною на момент внесення її до Єдиної реєстраційної та дослідної роботи. Суб'єкт перевірки володіє спеціальними знаннями у сфері інформаційних (комп'ютерних) технологій, що робить його інформацію доречною на даному етапі. Щодо окремих видів кіберзлочинів, слід перевіряти лише їхню повноту, здійснюючи оперативно-розшукові заходи за участю слідчого (в рамках оперативно-розшукової справи).

Взаємодія слідчого з іншими державними та недержавними підприємствами, установами та організаціями відіграє важливу роль. Щоб уточнити цю взаємодію, акцент варто зробити на особливостях організації національного сегменту кіберпростору.

У першу чергу, враховуючи географічне положення України, її електронні комунікаційні мережі виступають як точки транзиту для передачі даних між Європою та Азією. Організації, що надають послуги обміну трафіком (зазвичай вони використовують термін «піринг»), виконують важливу роль у ринку комунікаційних послуг в Україні. Їхня мережева інфраструктура призначена для забезпечення зв'язку між провайдерами та обміну Internet Protocol (IP-трафіком) між незалежними мережами в Інтернеті. Ці точки обміну трафіком гарантують об'єднання мереж в одній глобальній системі через регіональні та міжнародні вузли. В Україні функціонують три структури, що надають послуги з обміну трафіком: 1) дочірнє підприємство «UA-IX», створене Інтернет-асоціацією України у 2000 році; 2) комерційна структура ТОВ «Українські магістральні мережі» (Giganet.com); 3) корпорація DtelIX. В інших європейських країнах така структура може бути відсутньою.

По-друге, з технічного боку, магістральна мережа Інтернету охоплює весь світ, з'єднуючи континенти, країни та міста. Згідно зі статтею 2 Закону України «Про електронні комунікації»[72], мережа Інтернет (Інтернет) є глобальною електронною комунікаційною мережею, що призначена для передачі даних та складається з фізично та логічно взаємоз'єднаних окремих електронних комунікаційних мереж, взаємодія яких базується на використанні єдиного адресного простору та на використанні інтернет-протоколів, визначених міжнародними стандартами.

Мережі, що забезпечують обмін трафіком між регіонами України та за кордоном, обслуговують великі оператори та провайдери. Вони використовують магістральні оптоволоконні мережі для передачі трафіку від абонентів до точок

[72] Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

обміну. Великі оператори та провайдери мають Інтернет-вузли та магістральні лінії як в Україні, так і за її межами. Регіональні оператори та провайдери охоплюють регіон або декілька областей, а локальні оператори та провайдери обслуговують окремі населені пункти.

По-третє, суб'єкт господарювання отримує дозвіл на здійснення діяльності у сфері зв'язку та інформатизації, як тільки Національна комісія, що регулює зв'язок та інформатизацію (НКРЗІ), включає його до реєстру операторів та провайдерів електронних комунікацій зі статусом «провайдер» або «оператор». Статус «оператора», на відміну від «провайдера», надає право суб'єкту обслуговувати власні мережі на визначеній території діяльності (наприклад, місто або район). Якщо оператор отримав ліцензію від НКРЗІ на технічне обслуговування та експлуатацію електронних комунікаційних мереж, мереж ефірного та провідного теле- та радіомовлення, то він може обслуговувати також мережі інших операторів або провайдерів. Однак ліцензована діяльність оператора обмежена визначеною територією (регіоном, містом) та строком дії (принаймні п'ять років).

Діяльність провайдера обмежена географічною територією, на якій діє певний оператор (зареєстрований суб'єкт або той, що має ліцензію на обслуговування електронних комунікацій). При цьому немає обмежень для співпраці між різними операторами. Наприклад, один оператор може мати ліцензії на фіксований або рухомий зв'язок, тоді як інший, не маючи ліцензії і сплачуючи єдиний податок, може працювати через мережі першого, навіть на іншій території. Важливо зауважити, що деякі провайдери не є зареєстрованими в НКРЗІ, існують так звані «сірі провайдери», які під видом користувачів підключаються до великих інтернет-провайдерів та надають послуги на рівні провайдера іншим користувачам.

По-четверте, у сфері електронних комунікаційних та інформаційних послуг присутні власники інформації в системах. Власник інформації може бути фізичною або юридичною особою, якій належать права на інформацію в інформаційній системі. Інформація набуває форми інформаційного продукту або

інформаційного ресурсу, які включають в себе різні продукти та технології для зберігання та передачі даних. Це можуть бути веб-сайти та електронно-інформаційні системи для різних цілей, такі як платіжні системи, автоматизовані системи виробництва, пошукові системи, робочі місця тощо. Ми розглядали природу прав власності на інформаційний продукт або ресурс в системі. Наприклад, Національний банк України зберігає Реєстр платіжних інфраструктур, систем та операторів платіжної інфраструктури в Україні. Згідно зі статтею 1 Закону України «Про платіжні послуги»[73], платіжна установа - це юридична особа (крім банку, фінансової установи, що має право на надання платіжних послуг, оператора поштового зв'язку, органу державної влади, органу місцевого самоврядування), яка в установленому порядку отримала право на надання всіх або окремих фінансових платіжних послуг (крім платіжної послуги з випуску та використання платіжних операцій з електронними грошима).

Слід відзначити також організації, що забезпечують CDN (мережі доставки контенту) для користувачів в Україні. Ці організації володіють географічно розподіленими серверами, за допомогою яких користувачам надається доступ до контенту сайту або програми залежно від їхнього місця розташування. Корпорації, що надають Інтернет-послуги, такі як Google та Facebook, зацікавлені в тому, щоб їхній контент був доступним для клієнтів на максимально близькій відстані, тому вони відкривають представництва та організовують сервери на території України.

Це допомагає визначити різні суб'єкти взаємодії слідчого під час розслідування шахрайств учинених в кіберпросторі, зокрема:

– державні органи, які виконують функції контролю та ліцензування в сфері електронної комунікації, такі як Державна служба спеціального зв'язку та захисту інформації України, Національна комісія, що здійснює державне регулювання у сфері зв'зку та інформатизації, Національна рада України з питань телебачення і радіомовлення, Український державний

[73] Про платіжні послуги : Закон України від 30.06.2021 № 1591-IX. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text.

центр радіочастот; організації, які надають послуги платіжної інфраструктури, такі як клірингові та процесингові установи, які володіють інформацією про переказ коштів; організації, що надають CDN, забезпечуючи доступ до контенту; оператори, провайдери, власники веб-сайтів та інші суб'єкти, які надають послуги у сфері зв'язку та інформатизації;

– громадські об'єднання та організації (можуть надавати офіційні аналітичні огляди, статистичні дані, повідомляти про виявлення злочинів), такі як Інтернет асоціація України, Всеукраїнська громадська організація «Всеукраїнське агентство з авторських та суміжних прав», Державна організація «Українське агентство з авторських та суміжних прав», Асоціація «Телекомунікаційна палата України» та інші;

– суб'єкти господарювання (оператори та провайдери) у сфері зв'язку та інформатизації (можуть підтверджувати реєстраційні та технічні дані, що допомагають ідентифікувати власника, розробника, адміністратора Інтернет-ресурсу, факт надання послуг зв'язку конкретному користувачу/відправнику/отримувачу, надання послуг хостингу, а також надавати інформацію про фінансово-господарську діяльність, технічні аспекти функціонування мережі та інше);

– комерційні банківські установи та суб'єкти господарювання у сфері платіжних послуг (можуть документально підтверджувати рух (обіг) коштів на рахунках підприємств, установ та організацій, окремих громадян, поточні й депозитні рахунки, а також надавати інформацію про штат співробітників, їхні характеристики та інше);

– медіа (засоби масової інформації можуть документально підтверджувати факти реклами, оголошення, динаміку розвитку ринку товарів і послуг, проведення офіційних заходів, таких як виступи, спортивні події, ярмарки та аукціони, а також надавати результати журналістських розслідувань);

– міжнародні правоохоронні організації (можуть підтвердити місце розташування адміністратора та користувачів Інтернет-ресурсу, використовуваного під час вчинення злочину на території України, навіть якщо сервери розташовані за її межами);

– інші власники (розпорядники) систем та володільці інформації (структури, які забезпечують послуги з обміну трафіком, представники контент-сервісів, власники веб-сайтів, а також будь-які власники чи розпорядники електронно-інформаційних систем, будь-то державні чи недержавні установи, платіжні організації та оператори послуг платіжної інфраструктури, підприємства, організації).

Таким чином, особливості організації протидії кіберзагрозам в Україні та національного сегменту кіберпростору визначають різні суб'єкти взаємодії зі слідчими під час розслідування шахрайств, учинених в кіберпросторі. Взаємодія між слідчими та оперативними підрозділами, власниками (розпорядниками) електронних комунікаційних систем, володільцями інформації в системах та іншими суб'єктами на ринку електронних комунікаційних послуг є невід'ємною частиною процесу виявлення та розкриття шахрайств, що вчиняються в кіберпросторі.

2.3. Основні напрями розкриття шахрайств, учинених в кіберпросторі, та отримання інформації з відкритих джерел (OSINT).

Кримінальні події, які відбуваються в кіберпросторі, мають складну природу та можуть включати різноманітні аспекти: від технічних деталей до психологічних характеристик злочинців. Для швидкого розкриття кіберзлочинів необхідно використовувати комплексний підхід, який включає аналіз технічних аспектів вчинення злочину, вивчення мотивацій та психології злочинців, а також виявлення засобів комунікації та місць їхнього знаходження. Процес

дослідження шахрайств в кіберпросторі також включає аналіз типових ситуацій, які можуть виникати під час розкриття та розслідування злочину.

Слід зазначити, що на сучасному етапі розвитку суспільства, процес інформатизації спричиняє появі нових інноваційних видів злочинів. Ці види злочинів надають можливість розширення сфери застосування різних спрямувань протиправної активності, зокрема, таких як шахрайства, які вчиняються у кіберпросторі. Оскільки слідчі не завжди володіють достатньою обізнаністю щодо різновидів типових ситуацій та відповідних до них версій, це може призводити до погіршення результативності розслідування.

Багато науковців, серед яких А. І. Анапольська, М. П. Бікмурзін, В. В. Кузнєцов, Ю. Ю. Орлов, В. І. Пазиніч, О. Е. Радутний, М. В. Рудик, О. А. Самойленко, С. В. Самойлов, О. М. Стрільців, С. С. Чернявський, О. М. Юрченко та ін., займалися вивченням питань, пов'язаних з розслідуванням злочинів у сфері використання електронно-обчислювальної техніки, систем і комп'ютерних мереж, а також мереж електрозв'язку. Однак, сьогодні залишаються недостатньо дослідженими типові ситуації, що визначають основні напрями розкриття шахрайств, учинених в кіберпросторі.

Пріоритетним аспектом є осмислення поняття «типова ситуація» в контексті криміналістичної науки та теорії оперативно-розшукової діяльності. Термін «слідча ситуація» відзначається важливою історичною еволюцією та в даний момент є однією з найбільш досліджених концепцій, як з теоретичного, так і з практичного поглядів, що не можна сказати за термін «оперативно-розшукова ситуація». Тому серед вчених існують активні дискусії стосовно цих категорій. Одна плеяда порушує питання стосовно місця таких концепцій у правоохоронній галузі, оскільки вчення про «типові ситуації» тісно переплітаються з аналізом методичних аспектів як криміналістичної практики, так і теорії оперативно-розшукової діяльності, де розглядаються у формі конструктивного компоненту окремої діяльності. Друга плеяда, – заперечує існування будь-яких подібних інституцій, крім криміналістичної.

Ми вважаємо, що вказана дефініція може використовуватись і в криміналістиці, і в теорії оперативно-розшукової діяльності. Кожна з них має право на свою самостійній, внутрішню складу, кореляційні зв'язки з поставленими завданнями. Оскільки чинне кримінальне процесуальне законодавство в першу чергу визначає слідчу діяльність, а оперативно-розшукову залишає другорядною, то, не вступаючи в полеміку з іншими дослідниками, будемо використовувати термін «типова ситуація», як джерело для визначення основного напряму розкриття досліджуваного злочину. Задля об'єктивного дослідження, в основу нашої позиції включимо «слідчі ситуації», бо процесуальна діяльність може відбуватись тільки в рамках досудового розслідування та під керівництвом слідчого.

Так, Є. С. Хижняк переконаний у тому, що концепція слідчої ситуації відіграє ключову роль під час розкриття та розслідування злочину. Знання та використання типових ситуацій дозволяють слідчому визначити основні пріоритети, що зменшує втрати часу та зусиль через раціональне спрямування дій. Здійснюючи порівняльний аналіз між типовою ситуацією та ситуацією, що виникла під час розслідування конкретного кримінального правопорушення, слідчий може здійснити оптимальне планування розслідування та ефективно вирішити завдання ідентифікації особи, винної у вчиненні кримінального правопорушення[74].

На думку В. К. Весельського[75], слідча ситуація належить до категорії понять тактики, фактично функціонуючи як компонент методики. Цю тезу він аргументує тим, що саме концепція слідчої ситуації визначає стратегію окремих дій слідчого.

З точки зору автора, об'єктивні фактори, які впливають на формування слідчої ситуації, включають: 1) наявність та характер інформації, яка може слугувати для підтвердження або орієнтування; 2) існування не використаних

[74] Хижняк Є. С. Типові слідчі ситуації при розслідуванні статевих злочинів. *Південноукраїнський правничий часопис.* Вип. № 4. 2012. С. 198.

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

джерел доказів та надійних шляхів отримання орієнтування; 3) інтенсивність процесів приховання доказів та сила впливових факторів на ці процеси; 4) наявність відповідних ресурсів (часу, засобів) для слідчого та можливість їх ефективного використання; 5) поточна кримінально-правова оцінка події.

Суб'єктивні фактори охоплюють: 1) психологічний стан осіб, пов'язаних з розслідуваною подією; 2) психологічний стан слідчого, його рівень знань, практичний досвід, вміння діяти в умовах стресу; 3) спротив злочинця, потерпілого, свідків та інших факторів, які можуть ускладнити проведення розслідування; 4) сприятливий (неконфліктний) хід розслідування; 5) зусилля слідчого, спрямовані на зміну слідчої ситуації у відповідному напрямку; 6) наслідки помилкових дій слідчого, оперативних підрозділів, експертів; 7) наслідки розголошення даних досудового розслідування; 8) непередбачені дії потерпілого чи інших осіб, не пов'язаних з розслідуванням.

Термін «типова ситуація», – пише В. В. Кікінчук, означає комплекс умов, даних і інших факторів, які безпосередньо або опосередковано впливають на особу з правовим статусом в певний момент розкриття та розслідування конкретного виду кримінального правопорушення. Ці фактори формують чітку послідовність інтелектуальної діяльності, що є характерною для будь-якого розумового процесу, іноді навіть на підсвідомому рівні. Ця послідовність виявляється у прийнятті відповідних процесуально обґрунтованих рішень[76].

В. А. Журавель вважає, що «типова ситуація» є науковою абстракцією, яка формується на основі передбачених знань, являє собою результат аналізу і узагальнення значного обсягу емпіричного матеріалу, і в якій відображаються загальні характеристики, що описують хід і стан розслідування на певному етапі[77].

В. М. Шевчук, під «типовими ситуаціями» розуміє ті ситуації, з якими стикається слідчий на різних етапах розслідування кримінального

[76] Кікінчук В. В. Типові слідчі ситуації початкового етапу розслідування викрадень бюджетних коштів в агропромисловому комплексі. *Право і безпека.* Вип. № 2 (49). 2013. С. 132.

[77] Журавель В. А. Ситуаційний підхід до формування окремих криміналістичних методик розслідування злочинів. *Теорія і практика судової експертизи і криміналістики.* Вип. № 8. 2008. С. 106.

правопорушення, в залежності від повноти початкових даних. Типові ситуації відрізняються на підставі обставин, за яких було вчинено кримінальне правопорушення – чи було воно очевидним, чи ні. Виділення типових ситуацій можливе за умови, якщо в основу такої типізації закладено особливості стосовно винної особи до повідомлення їй про підозру[78].

Значущі елементи «типової ситуації», – зазначає Н. А. Запорощенко, формуються не лише набуттям необхідної інформації, але й її оцінкою. Переважаючі фактори, що впливають на оцінку орієнтуючої або доказової інформації, охоплюють: 1) наявність відповідних даних, що свідчать про вчинений злочин, в конкретний момент; 2) доступність наявної та релевантної значущої інформації; 3) швидкість зникнення та знищення слідів кримінального правопорушення та відповідної інформації; 4) проміжок часу від моменту вчинення злочину до появи першоджерельної інформації в розпорядженні правоохоронних органів; 5) активність або пасивність суб'єктів доказування та характер їх взаємодії; 6) виявлення і вплив помилок та недоліків у діях суб'єктів доказування і наслідки таких дій, які виникли в результаті неналежної реалізації оперативно-розшукових заходів[79].

Отже, типові ситуації відіграють суттєву роль у формуванні методології розслідування різних видів кримінальних правопорушень, виступаючи своєрідними моделями для його розкриття. Саме вони відображають загальні характеристики, які визначають перебіг та стан кримінального провадження. Важливо відзначити, що типові ситуації взаємопов'язані, створюючи систему, і залежать від інформації про різні аспекти кримінального правопорушення.

Так, С. В. Самойлов виділяє три типові слідчі ситуації, що характерні для початкового етапу розслідування шахрайств, вчинених у мережі Інтернет. Основні риси кожної з цих ситуацій можуть бути зведені до наступних:

[78] Шевчук В. А. Слідчі ситуації та їх вплив на розробку тактичних операцій. *Науковий вісник Міжнародного гуманітарного університету.* Вип. № 6-3. Т. 2. 2013. С. 126.

[79] Запорощенко Н. А. Розслідування організації або утримання місць для незаконного вживання, виробництва чи виготовлення наркотичних засобів, психотропних речовин або їх аналогів : дис. … канд. юрид. наук. Київ, 2012. С. 85.

Ситуація 1: Встановлено особу злочинця, який вчиняє шахрайство за допомогою мережі Інтернет. У цьому випадку, особу злочинця вже вдалося ідентифікувати або є достатньо інформації для її ідентифікації.

Ситуація 2: Виявлено ознаки шахрайства з використанням мережі Інтернет, але особу злочинця поки що не вдалося встановити. Проте існують деякі дані або індикатори, які можуть вказувати на можливу особу злочинця.

Ситуація 3: Виявлено ознаки шахрайства через мережу Інтернет, але особу злочинця не вдалося встановити, і немає жодних наявних даних, які вказують на ідентифікацію цієї особи.

Ці типові слідчі ситуації визначають можливі постановки розслідування на першому етапі інтернет-шахрайств, аналізуючи наявність і ступінь інформації про осіб, зокрема злочинців, у віртуальному середовищі[80].

Враховуючи погляди С. В. Самойлова та аналіз правозастосовної практики, визначимо дві основні групи типових ситуацій на початковому етапі розслідування залежно від характеру початкової інформації про подію та її учасників.

Перша типова ситуація полягає у встановленні факту шахрайства, яке було вчинено в кіберпросторі. Первинна інформація може стосуватися особи (чи групи осіб), які можуть мати відношення до вчинення цього злочину. Також може бути вже встановлена особа злочинця або наявні достатні дані для її ідентифікації.

Друга типова ситуація передбачає виявлення факту шахрайства в кіберпросторі, але особу злочинця поки що не вдалося встановити, і відсутні будь-які дані, які могли б вказувати на ідентифікацію цієї особи.

Ці дві типові ситуації відображають основні сценарії, які можуть мати місце на початковому етапі розслідування та основними напрямами для розкриття шахрайств, учинених в кіберпросторі.

[80] Самойлов С. В. Типові слідчі ситуації початкового етапу розслідування шахрайств, що вчиняються з використанням мережі «Інтернет», відповідні їм слідчі версії та алгоритми їх перевірки. *Проблеми правознавства та правоохоронної діяльності.* Вип. № 4. 2014. С. 26–27.

Тут зауважимо, що в практиці правоохоронних органів можуть виникати й інші сценарії. Наприклад, можливість існування інформації про вчинення злочину, однак деталі щодо способу скоєння шахрайства залишаються невідомими. Також може мати місце ситуація, коли ініціатором розслідування стає правоохоронний орган на підставі оперативних заходів або аналізу медіа, і кримінальне провадження зареєстровано щодо шахрайських дій стосовно потерпілого.

Такі випадки, хоча й зустрічаються в практиці, але відзначаються рідкісністю та ізольованістю.

Крім того, в ході досудового розслідування шахрайств, учинених в кіберпросторі, можуть виникати ситуації, які характеризуються високою складністю та конфліктністю. Серед них можна виділити ті, де недостатньо доказів, що призводить до відсутності адекватних фактичних даних. Також до цієї категорії можуть належати ситуації, де спостерігається активна протидія слідчим і працівникам оперативних підрозділів. Брак часу, ресурсів та енергії теж може призвести до ускладнення ситуації.

Проблема набуває додаткового важливого аспекту в разі конфліктних ситуацій, які у своєму роді є підкатегорією складних ситуацій. У цих випадках стосунки між суб'єктами розслідування та учасниками кримінального процесу, стають напруженими. Їхні інтереси відрізняються і орієнтовані на різні цілі, що веде до протистояння між ними. Кожен суб'єкт виходить з власних індивідуальних планів та намірів, що робить ситуацію ще більш складною.

Слід зазначити, що такі ситуації можуть виникати і в процесі проведення конкретних слідчих та розшукових заходів, коли різні учасники мають відмінні погляди, що призводить до невирішених конфліктів.

Під час розкриття шахрайства, учиненого в кіберпросторі, можна сформулювати наступні типові слідчі версії:

1) стосовно наявної інформації про особу злочинця:

– вчинене шахрайство в кіберпросторі відомою потерпілому особою або особою щодо якої є достатньо даних для її ідентифікації;

– шахрайство в кіберпросторі вчинено невідомою для потерпілого особою;

2) стосовно механізму вчинення шахрайства та побудови вебсторінки для кримінальних дій:

– вчинене шахрайство належить особі з поверхневими знаннями користування мережею Інтернет;

– вчинене шахрайство належить особі, яка є достатнім фахівцем у галузі інформаційних технологій;

– вчинене шахрайство належить особі, яка є професіоналом у галузі інформаційних технологій;

3) стосовно кількості злочинців:

– шахрайство в кіберпросторі вчинено однією особою;

– шахрайство в кіберпросторі вчинено групою осіб;

– шахрайство в кіберпросторі вчинено організованою злочинною групою;

4) стосовно обізнаності осіб про співучасників шахрайства:

– особа (виявлений злочинець) має інформацію про інших співучасників (членів групи) і може їх ідентифікувати;

– особа (виявлений злочинець) не має інформації про інших співучасників групи, оскільки вони були одноразово залучені для виконання певних ролей під час вчинення злочину та між ними не має постійних зв’язків.

– особи, що сприяли вчиненню злочину, не мали наміру заволодіти майном або правами на майно, а лише виконували дії, які вказував їм злочинець та які не порушують законодавство України (наприклад, розробка сайту, надання послуг з розміщення тощо);

5) стосовно кількості вчинених злочинів:

– шахрайство в кіберпросторі вчинено вперше;

– шахрайство в кіберпросторі вчинено неодноразово;

6) стосовно поширеності шахрайства:

– шахрайство в обмеженій кількості випадків;

– шахрайство поширене в певному регіоні;

– шахрайство вчиняється на державному рівні;

– шахрайство вчиняється на міждержавному рівні;

7) стосовно місця розташування електронно-обчислювальної техніки, з яких злочинці здійснювали контакти з потерпілими:

– особи, причетні до шахрайства в кіберпросторі, використовували електронно-обчислювальну техніку, розташовану на території України;

– особи, причетні до шахрайства в кіберпросторі, використовували електронно-обчислювальну техніку, розташовану за межами території України.

– особи, причетні до шахрайства, використовували електронно-обчислювальну техніку, розташовану на тимчасово окупованій території.

8) стосовно кількості потерпілих:

– завдана шкода обмежена тими потерпілими, які звернулися із заявами до правоохоронних органів;

– завдана шкода розповсюджена на певну категорію, які ще не звернулись із заявою до правоохоронних органів та/або не виявили завданої їм шкоди.

Крім того, в процесі розкриття шахрайств, учинених в кіберпросторі, можуть виникнути наступні контрверсії (версії захисту), які вимагають додаткового дослідження та перевірки:

– підозрюваний стверджує, що електронно-обчислювальна техніка, що була використана для вчинення шахрайства, належить іншій особі, а він надавав їй доступ або просто використовував цю техніку на її користь;

– підозрюваний купив електронно-обчислювальну техніку, яка згадується як засіб вчинення шахрайства, і стверджує, що ця покупка не пов’язана з кримінальною діяльністю;

– підозрюваний стверджує, що він не знав про справжній характер своїх дій, і мав намір віддати предмет посягання в майбутньому. Він вважає, що це може бути пов'язано з труднощами доставки чи іншими обставинами;

– підозрюваний стверджує, що він вчиняв незначну або другорядну роль під час шахрайства, і його внесок був незначним чи виконувався за іншими мотивами;

– виявлені записи або матеріали при обшуках можуть бути пояснені підозрюваним як спроба збільшити свій інтелектуальний рівень чи вивчення конкретної теми для власної освіти, не пов'язаної з кримінальними намірами.

Завдяки наявності вказаних контрверсій, слідчому рекомендується включити їх до плану розслідування та вчасно ініціювати проведення оперативних заходів та НСРД для їх перевірки.

Отже, можна дійти висновку, що під час розслідування шахрайств, учинених в кіберпросторі виникають типові ситуації, аналіз яких сприяє вибору ефективного напрямку розкриття злочину та оптимізації дій слідчого у взаємодії з оперативними підрозділами, включаючи висунення і перевірку версій.

З урахуванням початкової інформації, можна стверджувати, що версії формуються стосовно: особи злочинця; механізму вчинення шахрайств у кіберпросторі та створення відповідної онлайн-платформи; кількості злочинців; співучасників шахрайства; кількості подібних злочинів; розповсюдження такої злочинної діяльності; місця, де особи, які вчиняли злочини, зв'язувалися з потерпілими через електронно-обчислювальну техніку; мотивів вчинення шахрайств у кіберпросторі. Процес розкриття шахрайств, учинених в кіберпросторі також може викликати суперечливі точки зору (версії захисту) щодо будь-яких обставин події.

З метою глибокого дослідження кожної з вищезазначених версій, висуваються конкретні гіпотези, що ґрунтуються на наявній інформації, зібраної під час розслідування. Особливо важливі є версії стосовно особи, яка вчинила цю кримінальну протиправну дію.

Не менш важливим є один із методів розкриття шахрайств, учинених в кіберпросторі, як отримання інформації про незаконну діяльність за допомогою відкритих джерел (OSINT)

Слід зазначити, що Open Source Intelligence (OSINT) – це процес збору, аналізу і використання інформації, яка відкрито доступна. Ця інформація може бути отримана з різних джерел, таких як вебсайти, соціальні мережі, публічні бази даних, новинні ресурси, блоги тощо. Основна мета OSINT – зібрати релевантну інформацію для подальшого аналізу і прийняття рішень. Цей підхід застосовується в різних сферах, включаючи правоохоронну діяльність, розвідку, бізнес-аналітику, кібербезпеку та ін. В сучасних умовах, коли велика кількість інформації публікується онлайн, OSINT стає важливим інструментом для здійснення різних видів аналізу та досліджень, у тому числі і розкритті шахрайств, учинених в кіберпросторі.

Розкриття шахрайств, учинених в кіберпросторі, за допомогою відкритих джерел (OSINT), включає в себе процес збору, аналізу та використання публічно доступної інформації. Відкриті джерела включають в себе вебсайти, соціальні мережі, форуми, блоги та інші онлайн-ресурси, де злочинці можуть залишити сліди своєї діяльності. Завдяки використанню OSINT правоохоронці збирають важливі дані про злочинців, їхні методи атак, використані програмні засоби та інші характеристики діяльності. Це також допомагає встановити шаблони поведінки злочинців у віртуальному просторі (середовищі), їх мету та способи ухилення від виявлення. Крім того, аналіз відкритих джерел розкриває можливі зв'язки між різними злочинцями у віртуальному просторі (середовищі), а також надає інформацію для подальшого використання в розслідуванні та судових процесах.

Один із основних аспектів застосування OSINT у розкритті шахрайств, учинених в кіберпросторі, є зіставлення різних джерел інформації, що дозволяє побудувати повну картину діяльності злочинців. Це сприяє виявленню патернів та закономірностей, які використовують для вивчення їхньої поведінки та ідентифікації.

Засоби OSINT залучають широку групу фахівців, включаючи правоохоронців, кібераналітиків та спеціалістів з кібербезпеки, до спільної роботи над виявленням та розслідуванням незаконної діяльності у кіберпросторі.

Використання OSINT для розкриття шахрайств, учинених в кіберпросторі, передбачає кілька етапів, які спрямовані на збір, аналіз та використання публічно доступної інформації. Розглянемо основні етапи цього процесу:

1. *Збір інформації.* Спочатку необхідно ідентифікувати ключові поняття, осіб, компанії чи джерела, пов'язані з підозрілими діями або шахрайствами. Етап може включати пошук в соціальних мережах, форумах, новинах, вебсайтах, відкритих державних базах даних та інших джерелах.

2. *Фільтрація та сортування*. Зібрану інформацію необхідно відфільтрувати та сортувати залежно від релевантності та значущості. Важливо виділити ключові дані, які можуть вказувати на злочинну діяльність.

3. *Аналіз інформації.* На цьому етапі проводиться детальний аналіз зібраної інформації. Встановлюються зв'язки між різними джерелами та особами, розглядаються можливі патерни та закономірності.

4. *Крос-перевірка і підтвердження*. Для забезпечення точності та достовірності інформації проводиться крос-перевірка даних з декількох джерел. Це допомагає підтвердити отримані дані та визначити, які з них є вірогідними.

5. *Створення аналітичних звітів.* На основі аналізу формується аналітичний звіт, який містить важливу інформацію про підозрілі дії або шахрайства, залучення сторін, можливі наслідки та рекомендації для подальших дій.

6. *Спільна робота та співпраця*. Важливо залучити до розслідування спеціалістів з різних областей, які можуть надати цінний внесок у виявленні та аналізі шахрайств, учинених в кіберпросторі.

Як навчальний інструмент та практичний посібник для правоохоронців з використання відкритих цифрових даних для проведення розслідувань, може

бути використаний практичний посібник Протокол Берклі[81]. Документ містить стандарти знаходження, збирання, зберігання, перевірки та аналізу контенту із соцмереж та інших відкритих джерел; міжнародні стандарти для проведення онлайн-розслідування; керівництво про методи та процедури для збирання, аналізу та зберігання цифрової інформації з дотриманням професійних, правових та етичних принципів. Також у посібнику викладено заходи, які слідчі можуть вжити в Інтернеті, щоб забезпечити фізичний та психосоціальний захист самих себе та інших людей, включаючи свідків, постраждалих, громадян, активістів та журналістів[82].

Потужним інструментом, який може бути використаний для розкриття шахрайств, учинених у кіберпросторі, через аналіз відкритих джерел інформації є OSINT Framework[83].

Пошук інформації за іменем користувача з відкритих джерел є однією з ключових функцій OSINT. Такий пошук досить зручно систематизований в OSINT Framework (детальніше в табл. 1, Додаток А).

Альтернативними засобами пошуку інформації за іменем користувача є Sherlock – програма на Python, яка на сайтах соціальних мереж перевіряє, чи зареєстрований там користувач із вказаним іменем. Інша версія цієї програми – Photo Sherlock, шукає в Інтернеті фото з камери чи галереї. Дану програму можна використовувати, щоб знайти інформацію про зображення в Інтернеті, наприклад, щоб перевірити кому дійсно належить фото з соціальної мережі (перевірка на фейк).

Вищезазначені ресурси надають посилання для подальшого пошуку інформації про користувачів за їх іменами, ніками, псевдонімами у:

1. *Соціальних мережах.* Зважаючи на популярність соціальних мереж у наш час, це має бути одним з перших кроків для збору інформації про особу.

[81] Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Практичний посібник. Нью-Йорк і Женева, 2020. 119 с. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

[82] Протокол Берклі щодо розслідування із використанням відкритих цифрових даних. Юрфем.UA. 2022. URL: https://jurfem.com.ua/protokol-berkli-schodo-rozsliduvannia-iz-vykorystannyam-zyfrovych-danych/.

[83] OSINT Framework. URL: https://osintframework.com.

Соціальні мережі дозволяють знайти публічні дописи, фотографії та інші дані і встановити зв'язки між ними.

2. *Публічних форумах і блогах*. Пошук на форумах, відкритих обговореннях та блогах може розкрити більше інформації про користувачів, їхні інтереси та думки.

3. *Публічних базах даних*. Це можуть бути бази даних професійних організацій, реєстраційні системи, відкриті державні реєстри тощо.

4. О*світніх платформах*. Якщо користувач має профілі на освітніх платформах, таких як Coursera, LinkedIn Learning та ін., то це може розкрити не лише навчальні інтереси, але й певну інформацію про користувача.

5. *Новинах та медіа*. Пошук інформації в новинах та статтях може допомогти з'ясувати публічну діяльність та зв'язки користувачів.

6. *Відкритих базах даних та ресурсах.* Інтернет містить різноманітні бази даних та ресурси, які можуть включати інформацію про користувачів, наприклад, реєстри доменних імен, ресурси WHOIS та інші.

7. *Засобах зворотного зв'язку.* Аналіз публічних відгуків, коментарів та відповідей на публічні питання може розкрити деякі аспекти особистості користувача.

8. *Колективних платформах*, таких як GitHub для програмістів, що допоможе зрозуміти інтереси та досвід користувача.

OSINT Framework[84] пропонує широкий функціонал для аналізу електронної пошти: пошук інформації про власника електронної пошти, в яких реєстраціях електронна пошта приймала участь, перевірку на злами, верифікацію, розміщення e-mail у списках чи базах розсилки спаму «Spam Reputation Lists», «Mail Blacklists» тощо (детальніше в табл. 2, Додаток А).

Досить зручним ресурсом в OSINT Framework є розділ «Transportation», який систематизує інструменти та ресурси для збору відкритої інформації про транспортні системи, транспортні засоби та відповідні деталі. Основні можливості цього розділу включають: інструменти збору інформації про

[84] OSINT Framework. URL: https://osintframework.com.

реєстраційні номери автомобілів та інших транспортних засобів, включають деталі про власника, стан транспорту та інші важливі відомості; автомобільні бази даних, які містять інформацію про автомобілі, їх історію, власників та інші характеристики; дані про транспортні компанії, перевізників, їх рейси, маршрути; GPS-дані для відстеження маршрутів руху транспортних засобів, їх розташування в реальному часі; публічні джерела про авіацію – літаки, авіакомпанії, польоти, аеропорти та інші аспекти авіаційної індустрії; дані про громадський транспорт, розклади, маршрути, зупинки, транспортні системи, засоби та зв'язані з ними аспекти (детальніше в табл. 3, Додаток А).

Цей розділ у OSINT Framework дозволяє збирати важливу інформацію про транспорт, яка може бути корисною для різних цілей, включаючи безпеку, дослідження та аналіз.

Роботу з параметрами засобів OSINT для розкриття шахрайств, здійснених у кіберпросторі, пропонуємо здійснювати за наступним алгоритмом:

1. *Визначення ключових параметрів*. Ключовими параметрами та ключовими словами, пов'язаними зі шахрайством або підозрілими діями можуть бути імена, ніки або псевдоніми осіб, веб-сайти, компанії, додатки, номери телефонів, акаунти, сторінки соціальних мереж, геолокації, засоби переміщення тощо.

2. *Пошук інформації за ключовими параметрами*. Використання різних модулів OSINT Framework для збору інформації з різних джерел, таких як соціальні мережі, пошукові системи, домени, IP-адреси, WHOIS-запити тощо. Модулі OSINT Framework дозволять автоматизувати процес збору необхідної інформації.

3. *Аналіз інформації.* Включає оцінку зібраної інформацію, аналіз зв'язків між різними джерелами, пошук патернів та подібностей, які можуть вказувати на злочинну діяльність.

4. *Крос-перевірка та верифікація*. Полягає у використанні різних модулів OSINT Framework для крос-перевірки та верифікації інформації з декількох джерел. Це допомагає підтвердити дані та визначити їх достовірність.

5. *Створення звіту та подання результатів*. На основі зібраної та аналізованої інформації створюється аналітичний звіт. В звіті слід вказати ключові факти, зв'язки та висновки, які можуть вказувати на шахрайство, учинене в кіберпросторі.

Отже, OSINT може значно полегшити процес розкриття шахрайств, оскільки він надає доступ до багатьох джерел інформації та дозволяє ефективно аналізувати дані для виявлення підозрюваного або небажаного вмісту у кіберпросторі.

* * *

Отже, з'ясовано, що приводом для початку досудового розслідування за фактом вчинення шахрайств у кіберпросторі є: 1) отримання заяв від громадян, які стали жертвами шахрайських дій; 2) отримання заяв від громадян про роботу сумнівної вебсторінки чи діяльність організацій; 3) повідомлення від підприємств, установ, організацій, представників влади, посадових осіб, журналістів тощо; 4) повідомлення від невстановленої особи (анонімний дзвінок на лінію «102» або анонімний лист з викладеними обставинами вчинення злочину); 5) самостійне виявлення уповноваженою особою з різних джерел обставин, що свідчили про вчинення злочину (як правило, при моніторингу інтернет-ресурсів, медіа, форумів тощо).

Підставою для початку досудового розслідування за фактом вчинення шахрайств у кіберпросторі визначає слідчий шляхом правової оцінки джерел отриманої інформації про наявність у них обставин, що можуть свідчити про вчинення злочину (його ознаки) та кола причетних осіб (ч. 1, пп. 3-5 ч. 5, ч. 6 ст. 214 КПК України).

Наголошено, що слідчий у взаємодії з оперативним підрозділом на етапі оцінки первинної інформації можуть визначити основні напрями розкриття злочину та вибору спектру процесуальних заходів. Обсяг такого інструментарію залежить від визначення попередньої правової кваліфікації кримінального

правопорушення із зазначенням статті (частини статті) Закону України про кримінальну відповідальність, відомості про які обов'язково необхідно зазначити під час внесення відомостей до ЄРДР відповідно до ч. 5 ст. 214 КПК України. Правильна попередня правова кваліфікація впливає і на порядок проведення досудового розслідування.

Запропоновано, що задля мінімізації ускладнень, з якими стикаються слідчі та оперативні підрозділи під час оцінки первинної інформації, доцільно:

– уніфікувати окремі норми КПК України, розширивши спектр процесуальних дій (можливостей) до внесення відомостей в ЄРДР;

– деталізувати момент початку розслідування, розмежувавши та позбавивши залежності в цьому питані від норм Положення про ЄРДР, порядок його формування та ведення, затвердженого наказом Генерального прокурора від 30.06.2020№ 298;

– консолідувати норми КК України з урахуванням нормативної бази про забезпечення безпеки у кіберпросторі, визначити єдину термінологію для використання правозастосовними інституціями.

Конкретизовано коло обставин, що підлягають встановленню під час розкриття шахрайств, учинених в кіберпросторі: 1) обставини стосовно події злочину (відомості про: факт, час, просторові межі, особу потерпілого, способи вчинення, предмет посягання, характер і розмір завданої шкоди, джерела електронних цифрових слідів); 2) інші обставини, що охоплюються: 2.1) відомості про причинно-наслідковий зв'язок (обставини, що сприяли вчинення шахрайства; обставини стосовно споріднених видів кримінальних правопорушень; обставини постзлочинної діяльності); 2.2) відомості про особу свідків; 3) обставини стосовно підозрюваного (відомості про особу підозрюваного, винуватість, мотив та мету); 4) обставини, які можуть мати додаткове значення в кримінальному провадженні (обставини, що впливають на ступінь тяжкості, обтяжують чи пом'якшують покарання; обставини, що є підставами для закриття кримінального провадження чи звільнення від кримінальної відповідальності або покарання; розмір процесуальних витрат).

Визначено, що організація розкриття шахрайств, учинених в кіберпросторі сприймається як типова модель, що включає в себе аналіз первинної інформації щодо обставин злочину, формулювання версій, визначення цілей та розробку плану.

Сам процес планування розкриття шахрайств, учинених в кіберпросторі має охоплювати: аналіз слідчої ситуації; вибір основного напряму розкриття злочину; визначення необхідних сил та засобів; розробку письмового плану в разі потреби; здійснення контролю над виконанням плану та його корекція.

Наголошено, що взаємодія між слідчими та оперативними підрозділами, власниками (розпорядниками) електронних комунікаційних систем, володільцями інформації в системах та іншими суб'єктами на ринку електронних комунікаційних послуг є невід'ємною частиною процесу виявлення та розкриття шахрайств, що вчиняються в кіберпросторі. Ця взаємодія базується на взаємозалежності їхніх дій, яка допомагає збалансувати повноваження, методи та ресурси, характерні для кожного учасника співробітництва.

Окреслено, дві типові ситуації, що виникають на початковому етапі розслідування та є підґрунтям для основних напрямів розкриття шахрайств, учинених в кіберпросторі. Визначено типові слідчі версії стосовно наявної інформації про особу злочинця; механізму вчинення шахрайства та побудови вебсторінки для кримінальних дій; кількості злочинців; обізнаності осіб про співучасників; кількості вчинених злочинів; поширеності; місця розташування електронно-обчислювальної техніки; кількості потерпілих.

Окремо акцентовано на контрверсіях (версіях захисту), які вимагають додаткового дослідження та перевірки під час розкриття шахрайств, учинених в кіберпросторі.

Визначено сутність застосування OSINT у розкритті шахрайств, учинених в кіберпросторі. Зазначено, що OSINT сприяє виявленню патернів та закономірностей, які використовуються для вивчення поведінки злочинців та їхньої ідентифікації.

Розкрито зміст ресурсів OSINT, за допомогою яких здійснюється пошук інформації про користувачів за іменами, ніками, псевдонімами у: 1) соціальних мережах; 2) публічних форумах і блогах; 3) публічних базах даних; 4) освітніх платформах; 5) новинах та медіа; 6) відкритих базах даних та ресурсах; 7) засобах зворотного зв'язку; 8) колективних платформах.

Запропоновано такий алгоритм роботи з параметрами засобів OSINT для розкриття шахрайств, здійснених у кіберпросторі: 1) визначення ключових параметрів; 2) пошук інформації за ключовими параметрами; 3) аналіз інформації; 4) крос-перевірка та верифікація; 5) створення звіту та подання результатів.

Розділ 3
ОРГАНІЗАЦІЙНО-ТАКТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗКРИТТЯ ШАХРАЙСТВ, УЧИНЕНИХ В КІБЕРПРОСТОРІ

3.1. Організаційно-тактичні аспекти проведення невербальних заходів під час розкриття шахрайств, учинених в кіберпросторі.

Досудове розслідування шахрайств, учинених в кіберпросторі являє собою складну розумову діяльність слідчого у взаємодії з оперативними підрозділами зі встановлення всіх обставин їх вчинення, де головну роль відіграють різні заходи та, у першу чергу, СРД, в ході проведення яких відбувається виявлення, фіксація та вилучення, а іноді й дослідження, оцінка та використання доказів. Успішне закінчення досудового розслідування залежить від ряду факторів, найважливішим з яких є правильне (з точки зору кримінального процесуального закону) і ефективне (в тактичному змісті) проведення СРД. При проведенні будь-якої СРД необхідно розглядати її з двох сторін: процесуальної та тактичної, тільки таке поєднання дає позитивний результат.

Забезпеченню науковості підготовки та проведення СРД сприяє їх криміналістичний розподіл на вербальні і невербальні дії (в залежності від форми отримання інформації та особливостей її джерела).

До невербальних дій традиційно відносяться СРД спрямовані на отримання доказів за допомогою дослідження матеріального середовища. При проведенні таких СРД мовний спосіб збирання інформації поступається місцем іншим методам і прийомам. До них належать різні види огляду, обшук, освідування.

Загальні тактичні рекомендації проведення невербальних заходів полягають в організації підготовки та проведення СРД, послідовності та повноти дослідження матеріальних об’єктів, технічному оснащенню, залученню до участі відповідних спеціалістів.

Розслідування та розкриття шахрайств, учинених в кіберпросторі передбачає використання пошукових дій, які сприяють виявленню джерел доказової та орієнтуючої інформації. Відшукання прихованих об'єктів може бути здійснено під час проведення обшуку, процесуальний порядок проведення якого визначений ч. 3 ст. 208, ст. 223, 234-236 КПК України.

Чинний КПК України під обшуком розуміє СРД, яка проводиться з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукання знаряддя кримінального правопорушення або майна, яке було здобуте у результаті його вчинення, а також встановлення місцезнаходження розшукуваних осіб[85].

Обшук відрізняється від інших СРД передусім примусовим характером, який характеризується тим, що обшук може бути проведений без згоди особи, що обшукується та відповідно передбачає створення напруги між слідчим та обшукуваними особами. Під час проведення обшуку слідчий має право розкривати закриті приміщення і сховища, речі, якщо особа, присутня при обшуку, відмовляється їх відкрити або обшук здійснюється за відсутності осіб зазначених у ч. 3 ст. 236 КПК України. Здійснювати ці та інші дії примусового характеру під час проведення обшуку слідчий може лише за наявності в нього вмотивованої ухвали слідчого судді про надання дозволу на обшук житла чи іншого володіння особи (ст. 30 Конституції України[86], ч. 2 ст. 234 КПК України).

Процес проведення обшуку, як і будь-якої іншої слідчої (розшукової) дії передбачає такі етапи: 1) підготовка до проведення (підготовчий етап); 2) проведення СРД (робочий етап); 3) фіксація перебігу і результатів (завершальний етап). У подальшому слідчий здійснює оцінку отриманих під час проведення СРД результатів і визначає їх значимість та місце у системі доказової інформації[87].

---

[85] Кримінальний процесуальний Кодекс України від 13 квітня 2012 року № 4651-VI. *Офіційний вебпортал Верховної Ради України.* URL: http://zakon3.rada.gov.ua/laws/show/4651-17.

[86] Конституція України від 28 червня 1996 року № 254к/96-ВР. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

[87] Слідчі (розшукові) дії : навчальний посібник / О. В. Авраменко, Р. І. Благута, Ю. В. Гуцуляк та ін.; за заг. ред. Р. І. Благути та Є. В. Пряхіна. Львів: ЛьвДУВС, 2013. С. 212.

Як свідчить практика розслідування та розкриття кримінальних правопорушень, успіх при проведенні обшуку залежить від ступеня підготовки слідчого, правильного визначення об'єктів та ділянок, що підлягають обстеженню, точного визначення об'єктів, які підлягають пошуку та вилученню, законності оформлення та фіксації результатів обшуку.

На підготовчому етапі обшуку слідчому доцільно здійснити наступні заходи:

– визначити місцезнаходження та планування приміщення, яке повинно бути обшукане. З'ясувати характер охорони об'єкта, визначити шляхи можливого відходу шахраїв;

– встановити, які засоби зв'язку та комп'ютерної техніки знаходяться у приміщенні, у якому планується проведення обшуку. Отримана інформація буде використана для визначення меж місця обшуку, внесе визначеність відносно об'єктів пошуку;

– запросити спеціалістів, що мають достатні знання, уміння, навички для надання дієвої допомоги слідчому у підготовці та під час проведення обшуку. Для таких цілей універсальними є товарознавці, криміналісти, мистецтвознавці, бухгалтери, спеціалісти у галузі цифрових засобів зв'язку та комп'ютерної техніки;

– визначити дату, час, місце проведення обшуку, його тривалість, а також заходи, спрямовані на забезпечення його оперативності та конфіденційності. Сприятливою є ситуація відсутності підозрюваного (обвинуваченого) на місці обшуку. Ця обставина дозволяє виключити активну протидію з його боку та надає можливість слідчому швидко виявити та грамотно вилучити об'єкти пошуку. Присутність на місці обшуку рідних або близьких підозрюваного формує у них певне негативне ставлення до вчиненого злочинного діяння. Дана обставина може бути використана для визначення тактики проведення наступних слідчих дій, наприклад, допитів свідків.

– провести інструктаж осіб, що залучаються до участі у обшуку, з постановою конкретних персональних задач.

– вивчити особу підозрюваного. Особливу увагу приділити рівню злочинних навичок та вмінь.

– запросити понятих[88].

Ми повністю підтримуємо Т. В. Коршикову, яка зазначає, що організація та проведення обшуку у кримінальних провадженнях про шахрайство, що вчиняється з використанням електронно-обчислювальної техніки, відрізняються від обшуку, при розслідуванні традиційних видів шахрайств. Це обумовлено небезпекою навмисного знищення інформації, яка зберігається в електронно-обчислювальній техніці, як і самої електронно-обчислюваної техніки, що має доказове значення, а також необережним поводженням слідчого та інших членів СОГ, які можуть зашкодити інформації, знищити сліди в електронно-обчислювальній техніці в результаті неправильного, некваліфікованого поводження з нею.

Саме тому однією з найважливіших умов підготовчого етапу проведення обшуку безпосередньо на місці ймовірного вчинення шахрайства з використанням електронно-обчислювальної техніки є проведення наступних заходів:

– одержання інформації про предмети, які підлягають виявленню: електронно-обчислювальна техніка (стаціонарний комп'ютер, ноутбук, сервер тощо); програмне забезпечення та носії інформації, які необхідно вилучати; особу (осіб), підозрюваної у вчиненні шахрайства, її (їх) професійних навичок з володіння комп'ютерною технікою з урахуванням засобів вчинення злочину і способів подолання інформаційного захисту, можливих дій зі знищення інформації та приховування слідів злочину; видів електронної інформації;

[88] Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : дис. … канд. юрид. наук. Харків, 2008. С. 135–136.

– запрошення спеціалістів – експертів комп'ютерно-технічного відділу Експертної служби МВС України чи працівників підрозділу кіберполіції НП України;

– запрошення понятих, при цьому для вказаних цілей бажано запросити в якості понятих осіб, які розуміються на комп'ютерній техніці;

– підготовка відповідних пристроїв і комп'ютерних засобів, які будуть використовуватися для зчитування та збереження вилученої з електронно-обчислювальної техніки інформації;

– проведення інструктажу членів СОГ (при цьому особливу увагу варто приділити їхнім діям під час обшуку) та інших учасників обшуку (суворе дотримання встановлених правил поводження з комп'ютерною технікою і носіями інформації, технічно грамотне проведення пошуку доказів, потрібної інформації)[89].

Склад слідчо-оперативної групи залежить від мети обшуку та передбачуваної обстановки, яка може скластися при його проведенні. Крім слідчого, понятих, співробітника оперативного підрозділу можуть брати участь спеціаліст-криміналіст, перекладач, кінолог із собакою, а також особи, які виконують різні доручення, що вимагають професійних знань та навичок. У випадку надання активного супротиву з боку осіб на об'єкті обшуку, застосувати слід заходи з нейтралізації протидії та швидкого проникнення до обшукуваних приміщень.

Результати проведеного С. С. Вітвіцьким, О. О. Волобуєвою та А. О. Волобоєвим дослідження свідчать, що обшук (робоча стадія) починається з таких попередніх дій (заходів): непомітне прибуття СОГ (48,4 %); попереднє обстеження прилеглої до об'єкта обшуку території (29,17 %); виставлення постів (групи-перехвату) (37,5 %); супроводження представника громадськості чи житлово-експлуатаційної контори для оперативного проникнення на об'єкт обшуку (25 %); додержання заходів безпеки (69,55 %); застосування технічних

[89] Коршикова Т.В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … доктор філософії. Київ, 2021. С. 140–141.

засобів аудіо-, відеофіксування (68,91 %); проникнення до об'єкта обшуку та його оперативне обстеження (з метою встановлення кількості присутніх і недопущення втечі, опору, знищення речових доказів тощо) (41,99 %); пред'явлення службового посвідчення (47,12 %); ознайомлення обшукуваного з ухвалою слідчого судді (83,65 %); пропонування добровільно видати об'єкти пошуку (63,14 %); обшук присутніх осіб (52,24 %)[90].

Т. А. Абушов зазначає, що проведення обшуку складається з низки організаційних і тактичних заходів, спрямованих на виконання таких завдань: ознайомлення обшуканого 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; 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; 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[91].

[90] Методика розслідування незаконного поводження зі зброєю та бойовими припасами : монографія / С. С. Вітвіцький, О. О. Волобуєва, А. О. Волобоєв. Київ : ВД «Дакор», 2021. С. 174.

[91] Абушов Т. А. Система організаційних і тактичних дій під час проведення обшуку. *Науковий вісник Національної академії внутрішніх справ*. № 6. 2011. С. 198–205.

На особливу увагу заслуговує питання про те, що і де слід шукати. Вихідна інформація міститься у матеріалах кримінального провадження. У кримінальних провадженнях за фактами шахрайств, учинених в кіберпросторі питання про це вирішується на підставі показань потерпілого про вид предмету шахрайства та спосіб заволодіння ним. При проведенні обшуку в кримінальних провадженнях за фактами шахрайств, учинених в кіберпросторі дотримуються загальних тактичних вимог, розроблених наукою криміналістикою: раптовість, планомірність, послідовність, використання криміналістичної техніки. Але обшук у такій категорії кримінальних проваджень має і певні особливості, які стосуються розшукуваного об'єкта, й місця пошуку. Відповіддю на ці запитання може бути наступне: пошуку та вилученню обов'язково підлягають об'єкти, що стали предметом злочинного посягання; об'єкти, що стали знаряддям вчинення злочину; об'єкти, що вилучені із цивільного обігу и незалежно від мети слідчої (розшукової) дії повинні бути вилучені. Судово-слідча практика дозволяє констатувати, що обшуки частіше проводилися за місцем проживання (юридичним або фактичним) підозрюваного - у 55% випадків, за місцем їх роботи - 17%, за місцем проживання родичів та друзів - 20%; у господарських приміщеннях, транспортних засобах - 8%[92].

Переважна частина обшуків в кримінальних провадженнях за фактами шахрайств, учинених у кіберпросторі приходиться на обшук приміщень. Обшуки ділянок місцевості в якості окремого об'єкта мають місце в рамках обстеження будівель та прилеглих до них ділянок. Головним завданням проведення обшуку на будь-якому етапі розслідування є виявлення, фіксація та вилучення предметів та документів, які мають значення для кримінального провадження. Як вірно зазначає С. В. Чучко, під час розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет при проведенні обшуку необхідно виявляти та вилучати:

– документи, які містять відомості про можливих покупців;

[92] Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : дис. … канд. юрид. наук. Харків, 2008. С. 136–137.

– мобільні телефони, де міститься адресна книга (прізвища й адреси покупців, дані про організатора злочину), смс – повідомлення;

– комп'ютерна техніка (ноутбуки, планшети, системні блоки, флеш-накопичувачі), де може міститися інформація про протиправну діяльність шахрая. Значну увагу потрібно приділити вебсайтам, де була розміщена інформація з послуг щодо продажу товарів[93].

Дослідниця Т. В. Коршикова, розглядаючи об'єкти обшуку під час вчинення шахрайства з використанням електронно-обчислювальної техніки, поділяє їх на наступні види:

1) об'єкти, які вказують на належність електронно-обчислювальної техніки до вчинення злочину:

– електронно-обчислювальна техніка (комп'ютери, їх системні блоки);

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

– носії інформації (жорсткі диски, флопі-диски, оптичні диски, флеш-пам'ять, зовнішні та внутрішні диски HDD, SSD тощо);

– роздруківка програмних і текстових файлів;

2) об'єкти, які вказують на належність певної особи до вчинення злочину:

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

– відбитки пальців рук на електронно-обчислювальній техніці, периферійних пристроях, носіях інформації та інших предметів, які використовувались з метою вчинення шахрайства з використанням електронно-обчислювальної техніки;

– предмети, отримані в результаті вчинення злочину (речі, гроші, інше майно)[94].

[93] Чучко С. В. Розслідування шахрайства при купівлі-продажу товарів через мережу інтернет : дис. … доктор філософії. Дніпро, 2021. С. 142.

[94] Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … доктор філософії. Київ, 2021. С. 143.

Вилучення та упакування комп'ютера підпорядковані загальним правилам поводження з предметами та документами. Але особливості природи вінчестеру вимагають особливого підходу під час його огляду. Весь алгоритм такого огляду повинен бути підпорядкований наступним вимогам: 1) безпосередня участь спеціаліста в сфері засобів комп'ютерної техніки; 2) всі дії спеціаліста (відкриття файлів, постановка команд, відновлення видалених файлів) повинні бути оголошені та прокоментовані, протоколюватися дослівно. Огляд за необхідності може супроводжуватися завантаженням допоміжних програм, факт про що, а також отримані результати слід протоколювати; 3) у якості понятих слід запрошувати осіб, які мають хоча б мінімальні пізнання галузі комп'ютерної техніки, які можуть компетентно засвідчити правильність записів у протоколі; 4) за можливості до огляду слід залучати підозрюваного, осіб, що мали доступ до комп'ютера та можуть пояснити певні факти щодо виявленої інформації; 5) виявлена криміналістично значима інформація повинна бути роздрукована, засвідчена підписами понятих та інших учасників слідчої дії. Аналогічно слід поводитися з зовнішніми жорсткими дисками, флеш-накопичувачами тощо.

Після закінчення обшуку вилучаються комп'ютер та диски, які згодом можуть бути досліджені за допомогою відповідної судової комп'ютерно - технічної експертизи[95].

Приступаючи до огляду електронно-обчислювальної техніки, слідчий і фахівець, що безпосередньо виконують всі дії на електронно-обчислюваній техніці, 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

[95] Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : дис. … канд. юрид. наук. Харків, 2008. С. 139–140.

мережі та розетках на робочому місці (столі), де встановлено електронно-обчислювальну техніку, 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 електронно-обчислювальної техніки, її систем та мереж, на якій або за допомогою якої здійснюється несанкціоноване копіювання інформації. У цьому випадку можна виокремити: відбитки пальців рук на корпусі системного блоку електронно-обчислювальної техніки, 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 саме на: електронно-обчислювальній техніці, 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.

У подальшому при працюючій електронно-обчислювальній техніці необхідно:

– зафіксувати (відобразити в протоколі обшуку місцезнаходження електронно-обчислювальної техніки, що цікавить слідчого, та його периферійних пристроїв, вказавши кожен пристрій (назву, серійний номер, комплектацію: наявність і тип дисководів, мережевих карт, роз'ємів і т. ін.), наявність з'єднання з локальною мережею і (або) мережами телекомунікації, стан пристроїв (ціле або із слідами розтину та ін.);

– визначити, яка програма виконується на момент початку обшуку, при виявленні працюючої програми по знищенню інформації зупинити її і почати обшук (огляд) електронно-обчислювальної техніки саме з цього об'єкту;

– після зупинки виконання програми здійснити вхід в операційну систему для з'ясування, яка програма викликалася востаннє;

– встановити наявність у електронно-обчислювальній техніці зовнішніх пристроїв – накопичувачів інформації на жорстких дисках (вінчестері), а також зовнішніх пристроїв віддаленого доступу до системи (підключення до локальної мережі, наявність модему);

– вжити заходів щодо встановлення пароля доступу до захищених програм;

– закрити всі працюючі на електронно-обчислювальній техніці програми (необхідно пам'ятати, що некоректний вихід з деяких програм може викликати знищення інформації або зіпсувати саму програму);

– в разі необхідності скопіювати на з'ємний жорсткий диск, який належить територіальним органам чи підрозділам Національної поліції, програми і файли, які стосуються кримінального провадження;

– відключити від мережі електронно-обчислювальну техніку і вимкнути модем;

– спеціально зафіксувавши у протоколі обшуку порядок проведення СРД;

– опечатати їх і вилучити разом з магнітними носіями для дослідження інформації в лабораторних умовах;

– при вилученні технічних засобів додаткові периферійні пристрої (принтери, стрімери, модеми, сканери тощо) доцільно вилучати тільки в тому випадку, якщо на них працювали підозрювані або якщо у слідства є питання щодо їх працездатності[96].

[96] Доказування у справах про злочини, вчинені шляхом незаконних операцій з використанням електронно-обчислювальної техніки : методичні рекомендації. НАВС. 2020. С. 20–21.

Хід СРД безпосередньо залежить від тієї слідчої ситуації, яка склалася під час проведення обшуку. Зазвичай вчені диференціюють їх на ситуації конфлікту та безконфліктні. За наявності ознак першої ситуації обшук може набути характер тимчасового вилучення майна, коли обшукуваний добровільно видає те, що є об'єктом обшуку. Але така «доброзичливість» може бути ознакою підміни виданих предметів, бажання приховати щось більш важливе (ознаки інших епізодів злочинної діяльності), видачі по факту не всіх предметів, що цікавлять слідство. Але частіше слідчому доводиться працювати у конфліктних ситуаціях, які зумовлюють використання тактичних прийомів і рекомендацій в умовах конфлікту. Якщо така ситуація досить реальна, бажано, щоб об'єкт обшуку, заздалегідь (за кілька годин до прибуття слідчого) був узятий під спостереження, що може бути корисним для фіксації умовних сигналів, призначених для оповіщення співучасників. Якщо учасників обшуку під різними приводами не пускають у приміщення, де повинний проводитися обшук, то щоб уникнути знищення предметів, які передбачається знайти, можуть бути застосовані самі рішучі дії (злам дверей, проникнення на об'єкт обшуку через вікна, горище тощо)[97].

Важливим етапом обшуку є огляд вилучених об'єктів пошуку, фіксація їх ознак та обставин виявлення. Протокол обшуку повинен містити перелік вилучених об'єктів, їх загальні та окремі ознаки та властивості, пошкодження, особливі прикмети, індивідуальні номери, колір, форму, вагу, розмір, кількість, упакування тощо. Все вилучене упаковується, опечатується, скріплюється підписами понятих та учасників СРД.

[97] Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : дис. … канд. юрид. наук. Харків, 2008. С. 148.

3.2. Організаційно-тактичні аспекти проведення вербальних заходів під час розкриття шахрайств, учинених в кіберпросторі.

Допит без перебільшення можна віднести до найбільш поширених та ефективних вербальних заходів отримання доказової інформації в процесі розслідування та розкриття кримінальних правопорушень, у тому числі шахрайств, учинених в кіберпросторі.

Проведення такої СРД вимагає від слідчого не тільки наявності глибоких юридичних знань, тобто знань кримінального права, кримінального процесу, а й знань з області психології, логіки, інших наук, тактики проведення допиту, що розробляється наукою криміналістикою, а також уміння аналізувати ситуацію, що склалась в ході допиту, швидко і чітко реагувати на неї, коригувати лінію поведінки, обрану допитуваним.

Сутність допиту полягає в тому, що це процесуальна дія, яка є регламентованим кримінальними процесуальними нормами інформаційно-психологічним процесом спілкування осіб, котрі беруть у ньому участь, що спрямований на отримання інформації про відомі допитуваному факти, які мають значення для встановлення істини в кримінальному провадженні[98].

Допит необхідно проводити в відповідності з вимогами кримінального процесуального закону, що гарантує дотримання прав допитуваної особи, об'єктивність даних, отриманих в ході допиту, стійкість «настрою» допитуваної особи на дачу в подальшому повних і правдивих показань в суді, що забезпечує можливість в подальшому використовувати показання допитаної особи як докази у кримінальному провадженні.

Процесуальний порядок організації та проведення допиту на стадії досудового розслідування закріплено у ст. 65, 95–97, 133, 223–226, 232, 256 КПК України[99].

---

[98] Шепітько В. Ю. Криміналістична тактика (системно-структурний аналіз) : монографія / В. Ю. Шепітька. Харьків: Харків юридичний, 2007. С. 265.

[99] Кримінальний процесуальний Кодекс України від 13 квітня 2012 року № 4651-VI. *Офіційний вебпортал Верховної Ради України.* URL: http://zakon3.rada.gov.ua/laws/show/4651-17.

У криміналістичній літературі допит класифікують за різними підставами: залежно від мети і завдань допиту, а також допитуваної особи (свідка, потерпілого, підозрюваного (а в суді – обвинуваченого), малолітньої або неповнолітньої особи, одночасний допит двох чи більше раніше допитаних осіб, експерта (в суді)); залежно від форми організації взаємодії слідчого з допитуваною особою (безпосередній допит, дистанційний допит (допит в режимі відеоконференції)); залежно від виду та джерела інформації, що повідомляється в ході допиту (допит, пов'язаний з отриманням показань про особисто спостережувані події та допит, пов'язаний з отриманням показань з чужих слів); за послідовністю проведення (первинний, повторний); за обсягом отримуваної інформації (основний, додатковий).

Мета допиту – отримати від допитуваної особи відомості про обставини, що мають значення для встановлення всієї сукупності обставин вчиненого кримінального правопорушення, які становлять предмет допиту.

При проведенні допиту можуть вирішуватись наступні основні завдання: отримання відомостей про кримінальне правопорушення; перевірка вже відомих слідству відомостей про кримінальне правопорушення; отримання фактичних даних про обставини готування, вчинення та приховування кримінального право-порушення; перевірка висунутих версій; збирання відомостей про особу правопорушника, його місцезнаходження; отримання відомостей про спричинену кримінальним правопорушенням шкоду, місцезнаходження предмету посягання, знарядь вчинення кримінального правопорушення[100].

Для того, щоб визначитися з предметом допиту, слідчому, перш за все, потрібно знати не тільки те, якими відомостями може володіти допитувана особа, але і на що конкретно в ході допиту необхідно звертати увагу і фіксувати в протоколі, які саме деталі з'ясовувати щодо розслідуваної події або конкретної особи, яка підозрюється у вчиненні кримінального правопорушення.

[100] Слідчі (розшукові) дії : навчальний посібник / О. В. Авраменко, Р. І. Благута, Ю. В. Гуцуляк та ін.; за заг. ред. Р. І. Благути та Є. В. Пряхіна. Львів : ЛьвДУВС, 2013. С. 254.

Як і більшість інших СРД, допит доцільно розділити на три етапи: підготовчий, робочий та заключний.

Необхідною умовою для отримання достовірних і повних показань при проведенні допиту є ретельна і всебічна підготовка до нього, яка, незалежно від процесуального положення допитуваної особи, включає наступні дії:

1. Спеціальне вивчення матеріалів кримінального провадження. Вивчення матеріалів кримінального провадження при підготовці до допиту конкретної особи має бути цільовим, більш поглибленим. Даною вимогою не варто нехтувати навіть в тому випадку, коли слідчий добре знає матеріали, оскільки це дозволить йому правильно визначитися з предметом допиту, ясно та чітко сформулювати питання, дасть можливість оцінити показання допитуваної особи вже в ході допиту, а не після його закінчення, а при наявності протиріч (недомовленості тощо) – скоригувати тактику допиту, задати відповідні уточнюючі, доповнюючі питання, усунути суперечності або прогалини в показаннях. При вивченні матеріалів кримінального провадження доцільно робити з них виписки з посиланнями на конкретні матеріали, робити закладки, що згодом може полегшити процес складання плану допиту або стане в нагоді при його проведенні.

2. Визначення предмета допиту, питань, що підлягають з'ясуванню. Предмет допиту визначається поінформованістю допитуваного про розслідувану подію і спочатку (попередньо!) визначається за даними, які містяться в матеріалах кримінального провадження виробництва, але коригується далі в ході допиту.

3. Вивчення психологічного портрета допитуваного і його взаємин з іншими учасниками кримінального провадження. Такі дії необхідні, перш за все, для встановлення психологічного контакту з допитуваною особою, вибору тактичних прийомів її допиту і подальшої оцінки отриманих показань. Таке вивчення, по можливості, бажано провести на етапі підготовки до допиту (з використанням матеріалів кримінального провадження, під час спілкування з ким-небудь з кола спілкування особи, яку планується допитати, з оперативних

джерел). Але може мати місце й вивчення даних питань на початку допиту, при особистому спілкуванні слідчого з допитуваною особою, виконанні процесуальної процедури ознайомлення допитуваного з його правами та обов'язками, з'ясуванні відомостей про нього.

4. Попереднє обрання тактики допиту, підготовка необхідних матеріалів, технічних засобів. Тактика допиту визначається з урахуванням особистості допитуваної особи, обсягу питань, які у неї необхідно з'ясувати в ході допиту, а також процесуальних обмежень часу його проведення. Для економії часу і утримання необхідної атмосфери в ході допиту необхідно заздалегідь підготувати матеріали, які планується використовувати при допиті: документи, речові докази, допоміжні матеріали тощо, а також засоби фіксації ходу і результатів допиту.

5. Складання плану допиту. Дана дія, в принципі, не є обов'язковою, особливо якщо предмет допиту не дуже об'ємний, однак все-таки це рекомендується робити, хоча б у вигляді заміток, переліку питань, що підлягають з'ясуванню, посилань на конкретні матеріали кримінального провадження тощо.

6. Визначення місця, часу допиту, забезпечення необхідних учасників даної слідчої (розшукової) дії. Вирішуючи питання про час допиту, слідчий повинен враховувати обсяг роботи, який підлягає виконати в ході допиту з тим, щоб не довелося відкладати його закінчення на наступний день. Місцем допиту є переважно місце провадження досудового розслідування, проте кримінальний процесуальний закон передбачає можливість проведення допиту в інших місцях за погодженням з особою, яку мають намір допитати (ч.1 ст.224 КПК[101]).

Закінчується підготовка прийняттям необхідних заходів до виклику для участі в допиті всіх необхідних осіб: спеціалістів, перекладачів, педагогів, психологів, інших осіб.

7. Якщо допит буде проводитися в режимі відеоконференції, необхідно:

[101] Кримінальний процесуальний Кодекс України від 13 квітня 2012 року № 4651-VI. *Офіційний вебпортал Верховної Ради України.* URL: http://zakon3.rada.gov.ua/laws/show/4651-17.

– своєчасно повідомити відповідний орган розслідування, який буде забезпечувати проведення даної слідчої (розшукової) дії дистанційно, а також особу, яку планується допитати і забезпечити її явку до місця проведення допиту;

– передати (переслати) необхідні матеріали (копії, фотографії та ін.) до органу розслідування, який забезпечує присутність допитуваної особи на допиті в режимі відеоконференції;

– якщо допитуваній особі забезпечується захист, то повинні бути заздалегідь передбачені і вжиті заходи до зміни його зовнішності і голосу, при яких дану особу неможливо було б впізнати (відповідно до ч. 10 ст. 232 КПК[102]).

Робочий етап допиту (безпосередньо сам допит) полягає в отриманні показань у допитуваної особи, складається з чотирьох стадій:

1. Попередня (вступна) стадія. Змістом попередньої стадії допиту є:

– встановлення особи допитуваного;

– роз'яснення йому його прав і обов'язків, а також в залежності від процесуального положення (свідкові, потерпілому) – відповідальності за відмову від надання показань, надання завідомо неправдивих показань;

– встановлення відомостей про інших учасників допиту і роз'яснення їм їх прав та обов'язків;

– повідомлення учасників допиту про застосування технічних засобів фіксації його ходу і результатів;

– встановлення анкетних даних допитуваної особи;

– внесення зазначених відомостей до протоколу допиту.

2. Встановлення психологічного контакту з допитуваним. Передбачає застосування ряду тактичних прийомів, спрямованих на адаптацію допитуваного особи до обстановки допиту, усунення небажаних станів його психіки,

[102] Кримінальний процесуальний Кодекс України від 13 квітня 2012 року № 4651-VI. *Офіційний вебпортал Верховної Ради України.* URL: http://zakon3.rada.gov.ua/laws/show/4651-17.

формування у допитуваного установки на необхідність спілкування зі слідчим, надання повних і правдивих показань.

3. Стадія вільної розповіді. Передбачає можливість допитуваної особи самій визначити сукупність відомостей, які вона повідомить при допиті щодо розслідуваного кримінального правопорушення. На даній стадії слідчий лише задає напрямок, обумовлює предмет допиту, загальне коло питань, в зв'язку з якими особа допитується, надаючи йому право визначити послідовність і ступінь конкретизації відомостей, що повідомляються. Допитуваний вільно викладає відомості про відомі йому події і безпосередньо їм сприймалися, а якщо він не був безпосередньо очевидцем подій - повинен вказати конкретне джерело відомостей, посилання на невідомі йому або невизначені джерела типу «всі знають», «всі говорять» не допускається. За бажанням, допитувана особа може викласти свої показання власноруч - це прямо передбачено ч. 7 ст. 224 КПК України. У цій стадії не рекомендується без необхідності перебивати допитуваного, втручатися в його розповідь доцільно лише при явному ухиленні від теми допиту.

4. Стадія запитань та відповідей. Слідчий, а потім і інші учасники допиту (при необхідності) задають допитуваній особі додаткові питання: уточнюючі, нагадуючі, деталізуючі. Послідовність і характер запитань слідчий визначає виходячи з конкретної ситуації допиту, обраної тактики допиту. Але в будь-якому випадку такі питання не повинні бути навідними, тобто містити в собі відповідь, частину відповіді або підказку до неї, а також такі питання не повинні стосуватися обставин, щодо надання яких є пряма заборона в законі.

Усі дані, встановлені в ході допиту, фіксуються в описовій частині протоколу допиту. При необхідності (як правило в конфліктній ситуації) з урахуванням важливості питань і відповідей на них, слідчий відразу вносить їх до протоколу і допитуваний ставить підпис під кожною відповіддю на питання.

Змістом заключного етапу є:

– остаточне оформлення протоколу допиту, ознайомлення з його змістом допитуваних й інших осіб, які брали в ньому участь, фіксація цього факту

в протоколі допиту, а також внесення до протоколу тих заяв і зауважень, які виникли в учасників допиту щодо порядку його проведення, отриманих відомостей, повноти і об'єктивності їх фіксації в протоколі;

– перевірка показань;

– оцінка результатів допиту з позиції досягнення намічених цілей і отриманих відомостей;

– визначення напрямків використання отриманих даних в ході подальшого розслідування.

Перевірка і оцінка показань може проводитися як в ході допиту, так і після його закінчення. В ході допиту оцінюється, наскільки сповнені і логічні показання допитуваної особи, чи немає в них протиріч, в тому числі і з матеріалами кримінального провадження (якщо у слідчого під рукою виписки з цих матеріалів або самі матеріали), по можливості такі протиріччя, неповнота, неточність усуваються відразу ж в ході допиту, якщо для цього не потрібно проведення окремих слідчих (розшукових) дій (наприклад одночасного допиту двох і більше раніше допитаних осіб). Після закінчення допиту, при необхідності перевірки і оцінки отриманих свідчень, слідчий може додатково збирати докази, проводячи інші слідчі (розшукові) дії (провести слідчий експеримент, призначити ту чи іншу експертизу, допитати осіб, на який посилався допитаний тощо).

Допит потерпілих – найбільш поширене джерело отримання доказів у кримінальних провадженнях за фактами шахрайств, учинених в кіберпросторі.

Потерпілі допитуються про обставини шахрайства, засоби, за допомогою яких відбувалось спілкування з шахраями, прикмети та характеристику предметів злочинного посягання. Оскільки такі особи нерідко відчувають емоційну напругу, необхідна чітка організація допиту, постановка коротких та зрозумілих питань, що виключають виникнення пауз у процесі отримання показань. При цьому детально з’ясовується, з яких обставин відбулось знайомство та спілкування допитуваного, які послуги та цінності пропонував, за яку суму, що конкретно було передано злочинцем, вартість цих речей. Під час

допиту потрібно виявити факт можливого залишення злочинцями повідомлень, документів, інших речових доказів.

На допиті також слід встановити наявність посередників при встановленні знайомств із злочинцем. Слідчий повинен брати до уваги, що потерпілий, не знаючи способу вчинення шахрайства, не завжди може усвідомлювати, скільки було злочинців та яку роль виконував кожен з них. Тому потерпілий потребує уточнюючих відповідей.

Детальний допит потерпілих має важливе значення, оскільки дозволяє встановити обставини, що можуть слугувати невідкладному розшуку злочинців та пошук викраденого майна, висування обґрунтованих версій про особу шахраїв.

При допиті потерпілих з'ясовують наступні обставини:

– де, коли, через кого, за яких обставин потерпілий познайомився із шахраєм;

– яку мету переслідував потерпілий, спілкуючись із шахраями;

– коли, за яких обставин та ким виявлено викрадення майна шляхом обману або зловживання довірою;

– яке майно було викрадено, його кількість, вартість, прикмети, фізичні характеристики, наявність документації, що підтверджують знаходження його у власності потерпілого тощо;

– чи знає особу шахрая, як він поводився с жертвою, що говорив, які маніпуляції виконував;

– що обіцяв потерпілому шахрай;

– що вимагав та отримав від нього;

– хто був свідком вчиненого шахрайства;

– кому першому потерпілий повідомив про те, що сталося та які заходи виконав до переслідування злочинця;

– ступінь участі у шахрайстві кожної з підозрюваних осіб;

– прикмети шахраїв та одягу, звички, манера розмовляти, жестикулювати, ходити;

– чи не говорили злочинці з акцентом, якої національності вони могли бути;

– чи не залишені злочинцями записки, документи, інші речові докази;

– причини несвоєчасного звернення до правоохоронних органів[103].

При допиті потерпілих можливе пред'явлення для впізнання речей, про викрадення яких зроблено заяву. Тому дуже важливо встановити, чи не збереглися у потерпілого певні фрагменти від викрадених об'єктів або об'єкти, аналогічні викраденим, їх фотознімки, чеки, гарантійні талони, ярлики, сервісні книжки, квитанції на придбання товарів тощо. У позитивному випаду ці об'єкти підлягають вилученню та приєднанню до матеріалів кримінального провадження. На подальшому етапі розслідування за умов відшукання викрадених речей та їх впізнання, порівняння із вказаними предметами чи фотознімками допоможе перевірити правильність результатів пред'явлення для впізнання, якщо в ньому виникне сумнів[104].

Особливість механізму шахрайств, учинених в кіберпросторі впливає на визначення категорій свідків. Слід зауважити, що свідками шахрайських дій здебільшого виступають особи (сусіди, близькі, рідні, знайомі), яким стало відомо про обставини шахрайства зі слів потерпілого. Головним завданням слідчого при допиті зазначених свідків є отримання від них показань про факти, безпосереднім свідком яких був він сам.

Формування предмету допиту підозрюваного та обрання для його проведення тактичних прийомів при розслідуванні та розкритті шахрайств, учинених в кіберпросторі визначається багатьма чинниками: ситуацією, що склалась на момент допиту, наявною криміналістично значущою інформацію, особливістю особи допитуваного, а також обраною допитуваним схемою поведінки.

[103] Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : дис. … канд. юрид. наук. Харків, 2008. С. 86–88.

[104] Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : дис. … канд. юрид. наук. Харків, 2008. С. 89–90.

Перелік обставин, який запропонували О. М. Стрільців, В. В. Крижна, О. В. Максименко та ін., вважаємо доцільно використовувати під час допиту особи, яка підозрюється у шахрайстві, учиненому в кіберпросторі:

– прізвище, ім'я, по батькові;

– число, місяць, рік народження;

– адреса місця фактичного проживання, адреса місця реєстрації;

– чи притягався до кримінальної відповідальності. Якщо так, то за які саме кримінальні правопорушення (злочини);

– чи має з числа друзів осіб, які притягалися до кримінальної відповідальності;

– протягом якого часу вона займається протиправною діяльністю, пов'язаною з шахрайством в кіберпросторі;

– що спонукало до вчинення шахрайств в кіберпросторі;

– хто придумав та організував протиправну схему шахрайства в кіберпросторі;

– як давно особа вчиняє шахрайства в кіберпросторі;

– де саме та за які кошти була придбана комп'ютерна техніка, яка використовувалась для шахрайства;

– яким чином використовувалась мережа Інтернет у протиправній діяльності;

– які інтернет-ресурси використовувались для розміщення повідомлення з метою подальшого вчинення шахрайства з використанням комп'ютерної техніки;

– хто створював інтернет-сайт чи допомагав у його створенні, як познайомились (установчі дані, адреса, телефон таких осіб);

– яким саме інтернет-провайдером користувався та під яким ім'ям («ніком») користувалися;

– яка назва інтернет-сайту, яким користувався для вчинення шахрайства з використанням комп'ютерної техніки;

– як часто змінювався інтернет-провайдер і «нік»;

– скільки інтернет-сайтів було створено для організації вчинення шахрайства з використанням комп'ютерної техніки;

– на яких типах інтернет-сайтів він зареєстрований;

– з якого місця (об'єкта) та о котрій годині здійснювався доступ до облікового запису у мережі Інтернет з метою вчинення шахрайства;

– під яким ім'ям (логіном) представлявся під час спілкування з провайдерами інтернет-сервісів;

– яким чином домовлявся з користувачами (потерпілими) з метою вчинення щодо них шахрайських дій;

– який спосіб оплати за придбання коштів або майна був рекомендований підозрюваному (контактний чи безконтактний);

– які інтернет-ресурси використовував для подальшого відтворення протиправної діяльності (назва чату, сайту, номера ICQ, адреси електронної пошти (e-mail));

– яким чином підтримувався подальший зв'язок зі співучасниками (мобільний телефон, ICQ, електронна пошта);

– скільки фактів шахрайства з використанням комп'ютерної техніки було вчинено (по кожному факту окремо допитати зі з'ясуванням усіх необхідних обставин);

– яким чином одержувались гроші та майно від вчинення шахрайства;

– яким чином отримувалось майно від шахрайства, його місця зберігання або збуту;

– на чиє ім'я, коли та при яких обставинах відкривався банківський рахунок;

– яким чином проводилась конвертація та легалізація коштів, отриманих від шахрайства;

– яким чином проводилась перевірка надходження грошових коштів, отриманих від шахрайства;

– яким чином проводився розподіл грошей між учасниками шахрайства з використанням комп'ютерної техніки та яка саме частка залишалась підозрюваному;

– на які потреби витрачались кошти, здобуті від шахрайства;

– хто був задіяний у якості спільників (детально описати функції кожного з них);

– які методи конспірації використовував підозрюваний з метою не притягнення до кримінальної відповідальності;

– яким чином використовувались пристрої мобільного зв'язку в протиправній діяльності;

– скільки часу підозрюваний користується комп'ютерною технікою, яку вилучено;

– хто нею ще користується (користувався);

– скільки комп'ютерної техніки він ще має і де вона встановлена[105].

При розслідуванні та розкритті шахрайств, учинених в кіберпросторі на момент допиту підозрюваного можуть скластися наступні типові ситуації:

– підозрюваний не визнає вини. Невизнання вини зазвичай супроводжується відмовою підозрюваного від надання будь-яких пояснень з приводу підозри (з посиланням на ст. 63 Конституції України), а також визнанням факту свого перебування на місці незаконної порубки, але запереченням її здійснення;

– підозрюваний визнає вину частково. Визнання часткової вини може супроводжуватися відмовою визнати суму завданих збитків підозрюваним, а також зізнанням у факті вчинення дій, які йому інкримінуються, проте пояснення цих дій причинами та обставинами, які, на його думку, виключають або пом'якшують їх злочинний характер;

– підозрюваний визнає вину повністю. Коли підозрюваний визнає вину повністю, це значно спрощує роботу слідчого, оскільки злочинець активно

[105] Стрільців О. М., Крижна В. В., Максименко О. В. та ін. Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту: методні рекомендації / за заг. ред. Ю. Ю. Орлова. Київ : НАВС, 2014. С. 39–41.

співпрацює під час розслідування, надаючи детальну інформацію про вчинене шахрайство.

Загалом, тактичні прийоми проведення допиту підозрюваного обираються залежно від слідчої ситуації: уповноважена особа може застосовувати і пред'явлення доказів, і оголошення показань інших осіб, і методи переконання, і постановку деталізуючих, нагадуючих, контрольних запитань та ін. Якщо підозрюваний дає правдиві показання, завдання слідчого полягає в уточненні цих відомостей, максимальній деталізації показань та ін. Якщо ж він дає неправдиві показання, то необхідно вжити заходів для викриття неправди: роз'яснити положення кримінального процесуального законодавства про обставини, що пом'якшують вину, деталізувати його показання, провести повторні допити з тих самих обставин, пред'явити письмові і речові докази: документи, складені ним, експертні висновки, акти документальних ревізій, показання свідків, інших осіб тощо[106].

3.3. Використання спеціальних знань під час розкриття шахрайств, учинених в кіберпросторі.

Розслідування та розкриття шахрайств, учинених в кіберпросторі неможливе без використання спеціальних знань, адже у слідчого при проведенні СРД виникає необхідність у з'ясуванні окремих обставин, які потребують спеціальних знань.

Спеціальні знання – це наукові, технічні та інші професійні знання, отримані в результаті навчання, а також навички, надбані у процесі роботи в окремих галузях практичної діяльності, які використовуються разом із застосуванням науково-технічних засобів при збиранні та дослідженні слідів

[106] Методика розслідування шахрайств, пов'язаних із купівлею-продажем товарів через мережу «Інтернет»: теоретичні та праксеологічні засади : монографія / М. М. Єфімов, Н. В. Павлова, С. В. Чучко. Одеса : Видавничий дім «Гельветика», 2022. С. 148–149.

злочинів з метою отримання доказової та орієнтуючої інформації, необхідної для розслідування злочинів[107].

Основними формами використання спеціальних знань під час розслідуванні та розкриття шахрайств, учинених в кіберпросторі є: 1) залучення слідчим власних спеціальних знань; 2) участь спеціаліста в СРД; 3) призначення та проведення судових експертиз.

Під час розслідування шахрайств, учинених в кіберпросторі необхідність застосування спеціальних знань виникає практично на кожному етапі кримінального провадження:

– участь спеціаліста у проведенні огляду місця події, обшуку;

– участь спеціаліста у проведенні огляду предметів і документів, які вилучені під час огляду місця події та обшуку;

– участь спеціаліста в організації і проведенні допиту[108].

При проведенні огляду, обшуку в якості спеціалістів можуть залучатися інспектори-криміналісти, старші інспектори-криміналісти, техніки-криміналісти, а в разі утворення секторів техніко-криміналістичного забезпечення слідчих дій – керівники зазначених секторів, які входять до структури відповідних органів досудового розслідування та працівники Експертної служби МВС України у складі спеціалізованої пересувної лабораторії. Зазначені спеціалісти консультують слідчого з питань, що потребують відповідних спеціальних знань і навичок щодо порядку та особливостей пакування слідів та об'єктів-слідоносіїв, можливості дослідження виявлених слідів, об'єктів, речей, документів, доцільності вирішення тих чи інших питань, а також потреби залучення для цього інших спеціалістів, здійснюють фотографування та відеозйомку місця події, визначають алгоритм пошуку доказів (слідів, речей, документів) і методи їх виявлення, під час проведення пошуку та виявлення слідів спеціалісти застосовують наявні технічні

[107] Бідняк Г. С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств : монографія. Дніпро: ДДУВС, 2019. С. 43.

[108] Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … доктор філософії. Київ, 2021. С. 180-181.

засоби, під час фіксації виявленої слідової інформації в протоколі спеціалісти надають допомогу слідчому в описі специфічних ознак (вид та кількість виявлених слідів, їх локалізація, спосіб виявлення)[109].

При розслідуванні та розкритті шахрайств, учинених в кіберпросторі виникає потреба в залученні в якості спеціалістів експертів комп'ютерно-технічного відділу Експертної служби МВС України, коли слідчому необхідно оглянути засоби комп'ютерної техніки, насамперед, які знаходяться в робочому (увімкненому) стані. У цьому випадку спеціаліст повинен надати допомогу: в огляді засобів комп'ютерної техніки на стадії її виявлення, у тому числі встановити в засобах комп'ютерної техніки наявність зовнішніх пристроїв віддаленого доступу до системи (підключення до локальної мережі, наявність модему тощо); фіксування усіх дій з засобами комп'ютерної техніки за допомогою фото- та відеотехніки; здійснення опису екрану та прилеглої обстановки; копіювання наявної в засобах комп'ютерної техніки інформації; вжиття заходів щодо встановлення пароля доступу до захищених програм; належного та безпечного вимикання засобів комп'ютерної техніки; вилучення, упакування та опечатування засобів комп'ютерної техніки, 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[110].

Судова експертиза – один з видів процесуальної форми використання спеціальних знань при розслідуванні кримінальних правопорушень, значення якого у встановленні тих чи інших фактичних даних.

Сьогодні експертиза переживає бурхливий розвиток, обумовлений процесами інтеграції і диференціації наукового знання. Інтеграція створює

[109]Про затвердження Інструкції про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події : Наказ Міністерства внутрішніх справ України від 03.11.2015 року № 1339. *Офіційний вебпортал Верховної Ради України.* URL: http://zakon.rada.gov.ua/laws/show/z1392-15.

[110] Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … доктор філософії. Київ, 2021. С. 181–182.

передумови для використання в практиці розслідування нових досягнень різних галузей науки і техніки, комплексного дослідження об'єктів, що потрапляють в поле судового провадження.

Термін «експертиза» походить від латинського «expertis», що означає «досвідчений». Судова експертиза – це дослідження на основі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об’єктів, явищ і процесів з метою надання висновку з питань, що є або будуть предметом судового розгляду[111].

Загальною підставою для проведення експертизи в кримінальному судочинстві є необхідність застосування спеціальних знань для з’ясування обставин, що мають значення для кримінального провадження (ч. 1 ст. 242 КПК України).

Ініціатором проведення експертизи в таких випадках, відповідно до чинного КПК України, можуть бути:

1. Сторони кримінального провадження:

а) сторона обвинувачення: слідчий; керівник органу досудового розслідування; прокурор; потерпілий, його представник, законний представник;

б) сторона захисту: підозрюваний; обвинувачений (підсудний); засуджений, виправданий; особа, щодо якої передбачається застосування примусових заходів медичного або виховного характеру або вирішувалося питання про їх застосування; їх захисники і законні представники.

2. Слідчий суддя.

3. Суд.

Для кожної із зазначених груп суб'єктів процесуальним законом і підзаконними нормативними актами передбачено порядок так званої «ініціалізації» проведення (призначення) судових експертиз:

[111] Про судову експертизу : Закон України від 25 лютого 1994 року № 4038-XII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text.

Згідно ч. 1 ст. 242 КПК України при необхідності експертиза проводиться експертною установою, експертом або експертами, яких залучають сторони кримінального провадження або слідчий суддя за клопотанням сторони захисту у випадках та порядку, передбачених ст. 244 КПК України.

Посадові особи державних органів, які уповноважені проводити досудове розслідування кримінальних правопорушень і відносяться до сторони обвинувачення (слідчий, керівник органу досудового розслідування, прокурор) виносять постанову про призначення експертизи.

КПК України передбачена можливість сторони захисту самостійно залучити експертів для проведення експертизи на договірних умовах (п. 2 ч. 1 ст. 243 КПК України) або клопотати про це перед слідчим суддею (п. 3 ч. 1 ст. 243 КПК) в порядку передбаченому ст. 244 КПК України.

Що ж стосується суду, то він може призначити експертизу під час судового розгляду в двох випадках:

а) якщо до нього з клопотанням про це звернулася сторона кримінального провадження або потерпілий;

б) за власною ініціативою незалежно від наявності клопотання, якщо суду представлені кілька висновків експерта, які суперечать один одному, а допит експертів не дав можливості усунути виявлені суперечності (ч. 2 ст. 332 КПК України).

При розслідуванні шахрайств, учинених в кіберпросторі призначаються та проводяться судові експертизи, об'єктами яких є:

– 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 електронно-обчислювальної техніки);

– електронно комунікаційні 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).

Відносно осіб, які є підозрюваними у шахрайстві з використанням засобів комп'ютерної техніки, може проводитись судово-медична, судово-психіатрична, дактилоскопічна експертизи.

Залежно від обставин кримінального провадження можуть проводитись інші види експертиз[112].

Розглянемо деякі з зазначених судових експертиз.

Комп'ютерно-технічна експертиза проводиться з метою: визначення статусу об'єкта як комп'ютерного засобу, виявлення і вивчення його ролі в розслідуваному злочині, а також отримання доступу до інформації на електронних носіях з подальшим всебічним її дослідженням.

Предметом комп'ютерно-технічної експертизи є факти (обставини), що мають значення для органів досудового розслідування або суду, та встановлюються на основі дослідження закономірностей розробки та експлуатації комп'ютерних засобів і систем, що забезпечують реалізацію інформаційних процесів.

Об'єктами комп'ютерно-технічної експертизи є: персональні комп'ютери (системні блоки), портативні комп'ютери (ноутбуки, нетбуки); будь-які машинні носії інформації, периферійні пристрої, інтегровані системи та будь-які комплектуючі всіх зазначених компонентів (апаратні блоки, плати розширення і ін.); програмно-апаратні комплекси, де необхідний комплексний підхід до розгляду функцій апаратури та програмного забезпечення; мережеве обладнання

[112] Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. … доктор філософії. Київ, 2021. С. 186.

(сервери, робочі станції, файлові сховища та ін.); офісна периферія (принтери, сканери, багатофункціональні пристрої, модеми, роутери, точки доступу, відеоспостереження та ін.); програми та програмні засоби, їх компоненти (підсистеми) та супроводжуючі аналітичні матеріали й технічні документи (технічні завдання, вимоги, специфікації, моделі та ін.), алгоритми, окремі програмні модулі, вихідні тексти програм, текстові та графічні документи (в електронній формі), дані в форматах мультимедіа, виготовлені з використанням комп'ютерних засобів; інформація в форматах баз даних, журнали (протоколи) роботи спеціалізованих програм, інших додатків прикладного характеру, інформаційні дані; інформація, розміщена на сайтах в мережі Інтернет.

Інформація може міститися на різних типах носіїв, які можна класифікувати за наступними видами: накопичувачі на жорстких магнітних дисках – пристрої для зберігання інформації, робота яких здійснюється за принципом магнітного запису; твердотілі накопичувачі (англ. SSD, solid-state drive) – комп'ютерні запам'ятовувальні пристрої на основі мікросхем пам'яті та контролера керування ними, що не містять рухомих механічних частин, які можуть бути виконані, як окремими так і вбудованими в інше обладнання; USB флеш-накопичувачі – носії інформації, що використовують флешпам'ять для збереження даних та підключаються до комп'ютера чи іншого пристрою через USB-порт; карти пам'яті – носії інформації, що також використовують флеш-пам'ять для збереження даних та підключаються до комп'ютера чи іншого пристрою за допомогою різних спеціалізованих адаптерів.

До основних завдань комп'ютерно-технічної експертизи належать: установлення робочого стану комп'ютерно-технічних засобів; установлення обставин, пов'язаних з використанням комп'ютерно технічних засобів, інформації та програмного забезпечення; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; установлення відповідності програмних продуктів певним версіям чи вимогам на їх розробку.

Питання, що вирішуються при проведенні комп'ютерно-технічної експертизи:

– чи міститься на даному носії необхідна інформація, відповідно до поставлених питань і у якому вигляді?

– чи містить досліджуваний носій інформацію про певні (зазначені) 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 та яка саме інформація, перенесена до досліджуваного комп'ютера (носія)?

– яка технологія та хронологія створення електронного документа (зазначити назву електронного документа та його певний зміст)?

– які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію, пошук якої здійснюється?

– чи містять носії інформації досліджуваного комп'ютера певне програмне забезпечення (яке саме – встановлене, не встановлене)?

– які функціональні несправності має надане 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 забезпечення?

– чи можливе вирішення певного завдання за допомогою даного програмного забезпечення (програмному коду)?

– чи реалізовані у даному програмному забезпеченні (програмному коді) функції, передбачені технічним завданням на його розробку?

При призначенні комп'ютерно-технічної експертизи особливу увагу слід приділяти збору об'єктів дослідження. Найменші некваліфіковані дії з комп'ютерною системою часто закінчується безповоротною втратою цінної розшукової та доказової інформації. У зв'язку з цим, для збору об'єктів дослідження доцільним є залучення фахівця. Для забезпечення збереження

наданих на дослідження носіїв інформації в робочому стані, під час вилучення системних блоків необхідно коректно завершити їх роботу, повністю знеструмити, відключити, запакувати й опломбувати кожний системний блок окремо. Пакування й пломбування необхідно здійснювати таким чином, щоб унеможливити безпосередній доступ до системного блоку та розміщених у ньому носіїв інформації, без можливості пошкодження упаковки та пломб.

Крім запобігання безпосереднього доступу до об'єктів дослідження упаковка повинна забезпечувати їх захист від механічного пошкодження під час транспортування. Підключення таких носіїв даних, як жорсткі магнітні диски, твердотілі накопичувачі, USB флеш-накопичувачі та ін. можливе тільки до комп'ютера експерта з використанням спеціальних апаратних, програмно-апаратних та програмних засобів, що забороняють запис на них. Це дозволяє працювати з носієм даних у режимі «зчитування» та запобігає внесенню будь-яких змін до нього (унеможливлює запис на електронний носій), чим забезпечується повне збереження та цілісність даних. При цьому, підключення будь-яких об'єктів зберігання даних до комп'ютерної техніки в режимі запису є недопустимим.

Для дослідження інформації, що міститься на машинних носіях інформації, експерту надається сам носій, а за потреби й сам системний блок чи комплекс комп'ютерних засобів (до складу якого входить досліджуваний носій). Для встановлення відповідності програмних засобів певним параметрам експерту надається носій з копією досліджуваного програмного засобу або програмного коду. Для дослідження робочого стану комп'ютерно-технічних засобів експерту надаються ці комп'ютерно-технічні засоби, а також технічна документація до них[113].

Експертиза телекомунікаційних систем (обладнання) та засобів. Предметом телекомунікаційної експертизи є фактичні дані, що мають значення для процесу на основі дослідження електронно комунікаційних систем, засобів,

[113] Комп'ютерно-технічна експертиза. URL: https://kndise.gov.ua/kompyuterno-tehnichna/.

мереж і їх складових частин та інформації, що ними передається, приймається та обробляється.

Об'єктами телекомунікаційної експертизи є: електронні комунікаційні системи (наприклад: системи мобільних операторів зв'язку, телевізійні системи, радіо системи тощо); мобільні термінали (наприклад: телефони, смартфони, планшети та інші мобільні пристрої, із встановленим програмним забезпеченням; білінгові системи (наприклад: білінгові системи мобільних операторів, білінгові системи банків, системи державних реєстрів тощо); спеціалізовані технічні пристрої (наприклад станції активних перешкод, телематичні модулі, пульти керування доступом, програматори активних ключів для автомобілів та іммобілайзерів тощо).

До основних завдань телекомунікаційної експертизи належать: визначення характеристик та параметрів електронних комунікаційних систем та засобів; встановлення фактів та способів передачі (отримання) інформації в електронних комунікаційних системах; встановлення фактів та способів доступу до систем, ресурсів та інформації у сфері комунікації; визначення технічних показників якості надання комунікаційних послуг на рівні їх споживання; встановлення конфігурації та робочого стану електронних комунікаційних систем та засобів; встановлення типу, марки, моделі та інших класифікаційних категорій електронних комунікаційних систем та засобів; дослідження алгоритмів обробки інформації та її захисту у сфері комунікацій.

Питання, що вирішуються при проведенні телекомунікаційної експертизи:

– які тип, марка, модель комунікаційного засобу (системи)?
– чи в робочому стані знаходиться комунікаційний засіб (об'єкт)?
– які характеристики підключень до мережі має комунікаційний засіб?
– чи змінювались користувачем електронної комунікаційної мережі налаштування окремих пристроїв, у який час, які їх значення?
– який загальний характер підключень до електронної комунікаційної мережі виконував об'єкт (телекомунікаційна система, засіб)?

– за допомогою яких програмних засобів здійснювалось підключення до електронної комунікаційної мережі?

– яка топологія апаратних засобів, об'єднаних у електрону комунікаційну систему?

– чи відповідає функціонування комунікаційного засобу (системи) технічній документації?

– які технічні характеристики (параметри) має комунікаційний засіб (система)?

– чи мав місце факт доступу до електронної комунікаційної системи та в який спосіб?

– чи мало місце використання ресурсів та інформації в електронній комунікаційній системі та в який спосіб?

– чи мав місце факт передачі (отримання) інформації в електронній комунікаційній системі та в який спосіб?

– чи є ознаки втручання в роботу електронної комунікаційної системи?

– чи могли апаратні засоби об'єднуватись у електронну комунікаційну мережу та за якими ознаками?

– які шляхи маршрутизації даних у електронній комунікаційній системі?

– чи можливо використання комунікаційного засобу (обладнання) для вказаних цілей?

При призначенні телекомунікаційної експертизи особливу увагу слід приділяти збору об'єктів дослідження. Найменша некваліфікована дія з електронною комунікаційною системою часто закінчується безповоротною втратою цінної розшукової та доказової інформації. У зв'язку з цим для збору об'єктів доцільним є залучення фахівця. Зазвичай сучасні смартфони та планшети мають різні ступені захисту (код доступу, графічний код, відбиток пальця, сканер обличчя тощо) та постійне підключення до мережі Інтернет (інформація, яка в них міститься може бути заблокована або видалена віддалено). У таких випадах мобільний телефон, смартфон чи планшет необхідно перевести

у «авіа-режим» та, при можливості, вилучити сім-карту не вимикаючи його й підтримувати пристрій у розблокованому стані до моменту передачі спеціалісту.

Дослідження мобільних пристроїв. Даний напрямок телекомунікаційної експертизи в країнах, де відсутній притаманний українському законодавству досить формалізований поділ судових експертів за відповідними спеціальностями – має назву «Мобільна криміналістика» (MOBILE FORENSICS – англ.). В межах даного напрямку проводяться дослідження інформації користувача мобільного терміналу (мобільний телефон, смартфон, планшет, модем) та мобільних додатків, що на них встановлені (включаючи месенджери та ін.). Левова частка таких досліджень, припадає на пристрої, що функціонують на базі операційних систем iOS, Android і BlackBerry.

За результатами таких досліджень замовнику експертизи надається технічний звіт з всією наявною та видаленою користувачем інформацією (в даному випадку під «видаленою інформацією» – розуміється інформація, що попередньо була видалена користувачем мобільного терміналу, та яку вдалося відновити із застосуванням спеціальних програмно-апаратних комплексів). Практика останніх років направлена на те, щоб надати максимально повну інформацію у вигляді, що дозволяє слідчому, за певними критеріями, виділити ту, що відноситься до предмету розслідування. Як правило, такі експертизи проводяться в кримінальних провадженнях.

У разі, коли органом, що призначено експертизу визначені чіткі критерії щодо інформації, яка відноситься до розслідування або провадження, за результатами експертизи надається технічний звіт лише з інформацією, що відповідає вказаним критеріям.

Наприклад, коли орган досудового розслідування цікавить переписка в месенджері «WhatsApp», то в звіті буде надано саме зміст переписки з відповідними службовими даними: датою та часом повідомлень, вкладенням до повідомлень, ідентифікаторів учасників тощо[114].

[114] Телекомунікаційна експертиза. URL: https://kndise.gov.ua/telekomunikaczijna/.

Технічна експертиза документів – це традиційна криміналістична експертиза, основна мета якої полягає у встановлені способу виготовлення документу, факти та способи зміни його змісту.

До об'єктів експертизи належать наступні документи: грошові знаки, які знаходяться чи знаходилися в офіційному обігу; проїзні документи (квитки на проїзд будь-яким транспортом та на перевезення вантажу); знаки поштової оплати (поштові марки, конверти з марками, листівки з марками тощо); білети тиражних та миттєвих лотерей; документи що засвідчують особу, подію, освіту, трудовий стаж; документи, що обслуговують грошовий обіг (книжки ощадні, чекові, депозитні, марки податкові, митні, акцизні, поліси страхування, ліцензії інші документи та цінні папери, передбачені чинним законодавством); також об'єктами технічної експертизи є матеріали для виготовлення документів, серед яких папір, чорнило, паста для кулькових ручок, фарба тощо, копіювальний папір, стрічки для знакодрукувальних апаратів.

Додатково до об'єктів відносяться технічні засоби для виконання реквізитів. Це прилади що пишуть, знакодрукувальні (знакосинтезуючі) пристрої, засоби розмножувальної техніки, друкарські форми.

Об'єкти технічної експертизи документів поділяються на дві групи: ті що перевіряються та порівняльні.

Об'єкти, що перевіряються це: документи, відношення яких до справи визначається за результатами експертизи; документи, що залучаються до справи

Порівняльні об'єкти це: зразки, надані експерту особою або органом, що призначили експертизу, які поділяються на вільні, умовно-вільні та експериментальні, в окремих випадках зразки, що вміщені до інформаційно-довідкових колекцій; зразки, виготовлені експертом у ході проведення дослідження.

В цілому, технічна експертиза документів, залежно від об'єкта дослідження та задач відповідає на безліч питань залежно від об'єктів дослідження.

За задачами експертизи рукописних об'єктів можуть бути сформовані питання:

– яким способом виконані записи (пишучим пристроєм чи із застосуванням копіювально-множної техніки, шляхом монтажу)?

– пишучим приладом якого роду (виду) виконані записи?

– чи виконаний підпис з попередньою технічною підготовкою, за допомогою факсиміле?

– в якій послідовності нанесені штрихи рукописних записів та інші реквізити, що перетинаються ?

– чи піддавалися зміні рукописні записи шляхом дописки, домальовки окремих штрихів, виконання одних штрихів поверх інших ?

– чи вносилися зміни в рукописні записи шляхом підчистки?

– чи вносилися зміни в рукописні записи шляхом травлення (змивання)?

– який зміст записів, видалених шляхом: травлення, підчистки тощо?

– який зміст заклеєних записів?

– який зміст залитих, закреслених, замазаних записів?

– який зміст вдавлених записів?

– який зміст вицвілих записів?

– чи одним тим самим чи різними пишучими приладами виконані записи в документі?

– чи використовувався наданий на експертизу пишучий прилад для виконання записів в документі?

За задачами експертизи відтисків друкарських форм – відтисків печаток і штампів можуть бути сформовані питання:

– яким способом нанесено зображення відтиску печатки (штампу) в документі?

– яким способом виготовлена печатка (штамп), відтиск якої знаходиться в документі?

– чи відповідає час нанесення відтиску печатки (штампу) даті, вказаній в документі; в який проміжок часу нанесений відтиск печатки (штампу) ?

– в якій послідовності нанесені елементи відтиску печатки (штампу) та інші реквізиті документу з якими він перетинається?

– чи нанесений відтиск в документі наданою печаткою (штампом) ?

– однією чи різними печатками (штампами) нанесені відтиски в документах?

За задачами експертизи текстів виконаних на знакодрукуючих (знакосинтезуючих) пристроях можуть бути сформовані питання:

– яким способом виконаний текст?

– чи відповідає час виконання друкованого тексту даті, вказаній у документі; в якій проміжок часу надрукований текст (на машинці, на принтері)?

– в якій послідовності виконаний друкарський текст та інші реквізити документу?

– чи не виконаний для виконання тексту аркуш паперу або частина іншого документу з вже присутніми на ньому підписом (підписами) та відтиском печатки?

– пишуча машинка якого класу, типу, виду, марки, моделі використовувалася для виконання машинописного тексту?

– знакодрукуючий (знакосинтезуючий) пристрій якого типу використовувався для виконання тексту документу?

– чи піддавався зміні зміст тексту шляхом підчистки?

– чи піддавався зміні зміст тексту шляхом травлення?

– чи піддавався зміні зміст тексту шляхом додрукування?

– який первісний зміст тексту, що піддавався зміні?

– на одній чи різних пишучих машинках (інших знакодрукуючих пристроях) виконані тексти документів?

– чи виконаний текст на тому ж знакодрукуючому (знакосинтезуючому) пристрої, що і надані зразки текстів?

За задачами експертизи поліграфічної продукції можуть бути сформовані питання:

– яким способом виконаний текст та всі реквізити бланку; яким способом виготовлена грошова купюра?

– чи виконаний текст поліграфічним способом?

– чи однаковим способом виготовлені надані на експертизу документи (водійські посвідчення, паспорти, дипломи та інше) ?

– чи виконані окремі реквізити бланків документів шляхом монтажу?

– чи відповідає наданий на дослідження бланк (грошова купюра тощо) аналогічним документам (купюрам), які знаходяться (знаходилися) в офіційному обігу?

– чи відповідає наданий на дослідження бланк аналогічним безсумнівним бланкам, які виготовлені на підприємстві, що здійснює їх виробництво?

– чи з одного набору (форми, кліше) надруковані надані документи;

– чи відбувалася заміна аркушів в паспорті (іншому зброшурованому документі)?

За задачами експертизи наклеєних та скріплених між собою реквізитів можуть бути сформовані питання:

– чи відбувалася заміна (переклейка) фотографії (марки, ярлика) в документі?

– чи замінювалися аркуші в документі?

– чи піддався перешиванню документ (журнал, підшивка документів)?

За задачами експертизи розірваних документів можуть бути сформовані питання:

– частиною якого виробу є відірваний фрагмент аркушу?

– чи належав наданий аркуш паперу документу наданому зошиту (іншому конкретному виробу), в якій відсутня частина аркушів?

– чи складали раніше одне ціле надані фрагменти документу?

– який первісний вид та зміст розірваних документів?

Вимоги до матеріалів, які потрібно надавати для дослідження. Для вирішення більшості наведених вище питань, які ставляться перед технічною

експертизою документів, потрібно надавати оригінали документів, а не його технічні зображення (копії).

При підготовці матеріалів повинні бути виконані певні вимоги поводження з речовими доказами, чітко сформульовано завдання експерту, проведено збір необхідних порівняльних матеріалів, збір інформації, необхідної для проведення експертизи.

Можливості експертизи багато в чому залежать від підготовки матеріалів для її проведення. Відповідно до правил поводження з документами – речовими доказами, розробленими криміналістикою, слідчий (суд) зобов'язаний: надавати експерту документи в тому вигляді та стані, в якому вони були виявлені (надані); зберігати документи – речові докази в окремих конвертах (пакетах, файлах), не наклеювати будь-що на аркуші паперу для залучення до матеріалів справи; згинати та складати листи паперу документів лише за наявними складками; оберігати документи від впливу світла, вологи, високої температури, оскільки це може призвести до суттєвих змін їх властивостей; користуватися при огляді документів пінцетом, щоб не забруднити їх, не залишити на них слідів пальців (це може ускладнити ототожнення особистості за відбитками рук на документах, якщо документи стануть об'єктом трасологічної експертизи); особливу обережність слід дотримуватися при виявленні, фіксації та упакуванні спалених документів; не робити на документах позначок, обведення, вказівок; не скріпляти аркуші або один з аркушів досліджуваного документа будь з чим за допомогою стиплера, діркопробивача тощо, оскільки зайві отвори на папері ускладнюють розв'язання питань із заміни аркушів в документі.

У документі про призначення експертизи необхідно конкретизувати об'єкти, що підлягають дослідженню: вказати повну назву документа, наведену в документі дату його складання; дати інформацію про обставини виявлення документів – речових доказів (дата, місце виявлення, вилучення); вказати безпосередній об'єкт дослідження – описати його зміст (знак, слово, рядок, інше), місце розташування в документі; при направленні на експертизу матеріалів справи вказати місце розташування документа в матеріалах справи –

лист справи; чітко позначити досліджувані документи та порівняльні матеріали, щоб не привести до їх змішування при проведенні експертизи.

При призначенні експертиз, що потребують проведення матеріалознавчих досліджень документа (визначення складу матеріалів письма в штрихах реквізитів, визначення складу і властивостей основи інше); проведенні ідентифікації відтисків печаток, штампів, друкарської техніки, писального приладу; визначення внесення змін у документ та встановлення його первісного змісту не допускається подання на експертизу технічного зображення документу (копії) замість його оригіналу.

Питання експерту не повинні виходити за межі його компетенції, вимагати правової оцінки результатів дослідження. При формулюванні завдання експерту неприпустимо застосовувати терміни, що має двояке тлумачення – технічне і юридичне, а саме: «виправлення», «підробка», як синоніми термінів: «зміна», «невідповідність зразку».

Питання про подібність, однорідність, ідентичність, загальну родову (групову) належність, одночасність є питаннями з невизначеним завданням експерту. Наприклад питання про одночасність виконання декількох документів або фрагментів одного документа є типовим випадком невизначеності завдання експерту.

Термін «одночасність» доречний тільки у відношенні документів, виконаних в один прийом: в одну закладку з використанням копіювального паперу або самокопіювальному паперу. В інших випадках термін «одночасність» вимагає уточнення: який проміжок часу цікавить слідство (суд), або при виконанні тексту за допомогою принтеру аркуші друкуються один за одним, тому «одночасність» в цьому випадку – це виконання всіх аркушів документу за один друкуючий цикл (в один прийом).

Якщо об’єктами експертизи стають технічні засоби: пишучі прилади, знакодрукуючі (знакосинтезуючі) пристрої, засоби розмножувальної техніки, друкарські форми, то в залежності від експертного завдання і конкретної ситуації на експертизу можуть бути представлені або технічні засоби безпосередньо, або

виконані за їх допомогою порівняльні матеріали – зразки наступних видів: експериментальні зразки або (та) вільні зразки.

Деякі методи експертного дослідження пов'язані з частковим пошкодженням об'єкта (зміна властивостей барвної речовини в штрихах підпису, відтиску, тексту) або навіть повним його знищенням (вирізання штрихів). Такі методи застосовуються з дозволу органу або особи, що призначила експертизу. Зазначений дозвіл має міститися у документі про призначення експертизи або у відповідному листі. Дозвіл на часткове знищення документа, взяття проб, вирізок зі штрихів обов'язково для вирішення наступних завдань: встановлення давності виконання документа; встановлення послідовності виконання штрихів, що перетинаються; встановлення факту дописки; ідентифікація пишучого приладу по штрихам; ідентифікація принтера за текстами[115].

* * *

Отже, за результатами дослідження конкретизовано організаційно-тактичне забезпечення розкриття шахрайств, учинених в кіберпросторі, а саме: організаційно-тактичні аспекти вербальних та невербальних заходів, використання спеціальних знань.

Визначено особливості проведення обшуку, огляду електронно-обчислювальної техніки, допитів та підготовку до призначення окремих судових експертиз.

Наголошено, що склад слідчо-оперативної групи під час обшуку залежить від його мети та передбачуваної обстановки, яка може скластися. Крім слідчого, понятих, співробітника оперативного підрозділу можуть брати участь спеціаліст-криміналіст, перекладач, кінолог із собакою, а також особи, які виконують різні доручення, що вимагають професійних знань та навичок.

[115] Технічна експертиза документів. URL: https://kndise.gov.ua/tehnichna-ekspertyza-dokumentiv/.

У випадку надання активного супротиву з боку осіб на об'єкті обшуку, застосувати слід заходи з нейтралізації протидії та швидкого проникнення до обшукуваних приміщень.

Зазначено, що приступаючи до огляду електронно-обчислювальної техніки, слідчий і фахівець, що безпосередньо виконують всі дії на електронно-обчислюваній техніці, повинні дотримуватися певних вимог з метою забезпечення виявлення та вилучення речових доказів (слідів пальців рук та об'єктів біологічного походження).

Акцентовано, що в кримінальних провадженнях за фактами шахрайств, учинених в кіберпросторі питання до допитів формуються на підставі показань потерпілого про вид предмету шахрайства та спосіб заволодіння ним. Сам допит потерпілого має бути детальним, оскільки дозволяє встановити обставин, що можуть слугувати невідкладному розшуку злочинців та пошук викраденого майна, висування обґрунтованих версій про особу шахраїв.

Окремо визначено типові ситуації, які можуть виникнути на момент допиту підозрюваного.

Розкрито сутність та предмет експертного дослідження таких судових експертиз, як: комп'ютерно-технічна експертиза, телекомунікаційна експертиза, технічна експертиза.

ПІСЛЯМОВА

У монографії здійснено теоретичне узагальнення та запропоноване нове вирішення наукового завдання стосовно комплексного аналізу та наукового обґрунтування засад організації розкриття шахрайств, учинених в кіберпросторі. Найсуттєвіші з них такі:

З'ясовано, що сучасний стан наукових досліджень характеризується тим, що: 1) дослідники різних країн розуміють важливість розкриття шахрайств, учинених в кіберпросторі та розробки методів боротьби з ними; 2) у дослідженнях активно вивчаються сучасні технічні засоби для виявлення шахрайств, учинених в кіберпросторі; 3) вітчизняні та зарубіжні дослідники розробляють методи й алгоритми аналізу підозрілих дій в кіберпросторі та профілактичні заходи для запобігання шахрайствам; 4) дослідники поєднують знання з різних галузей, таких як інформаційна безпека, кібербезпека, кримінальна судова експертиза, техніка, статистика тощо; 5) дослідними співпрацюють з правоохоронними органами та органами державного управління для впровадження розробок в реальну практику.

Акцентовано на основні причини збільшення кібернебезпек. Визначено, що кіберпростір має велике значення в сучасному світі, де віртуальна діяльність та обмін інформацією відіграють ключову роль в багатьох сферах життя. А з іншого боку, – окрім можливостей, несе в собі численні небезпеки, які можуть впливати на окремих громадян, організації та навіть держави.

Особливість розкриття, учинених у кіберпросторі, полягає у тому, що ці злочини відбуваються в електронному середовищі, і це викликає певні труднощі у відстеженні та ідентифікації.

Виокремлено фактори, які сприяють зростанню кількості шахрайств, учинених в кіберпросторі, а саме через: 1) зростання використання Інтернету; 2) технічний розвиток; 3) анонімність та віддаленість; 4) соціальну інженерію.

Надано авторське поняття «шахрайство, учинене в кіберпросторі» як суспільно небезпечне діяння, спрямоване на заволодіння чужим майном або

придбання права на майно шляхом незаконних операцій з використанням електронно-обчислювальної техніки у віртуальному просторі (середовищі), де надається можливість комунікацій та/або реалізації суспільних відносин.

Розкрито складові оперативно-розшукової характеристики шахрайств, учинених в кіберпросторі. Зокрема, досліджено:

– кримінально-правову складову шахрайств, учинених в кіберпросторі (проаналізовано сутність злочину, визначено його об'єкт, предмет, об'єктивну сторону, суб'єкт, суб'єктивну сторону).

Наголошено, що головною кваліфікуючою ознакою є вчинення шахрайства шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Таку ознаку утворюють лише такі операції, здійснення яких без електронно-обчислювальної техніки є неможливим. При цьому, злочин направлений не на стабільність функціонування електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та/або комп'ютерних мереж, мереж електрозв'язку, а на суспільні відносини з огляду заволодіння майном або правом на це майно.

– кримінологічну складову шахрайств, учинених в кіберпросторі (проаналізовано стан, динаміку та надано характеристику особи злочинця).

З'ясовано, що за останні роки простежується динаміка росту кількісних показників реєстрації досліджуваного злочину, проте успішно розкривається лише кожне 3 шахрайство, а в інших випадках, – не представляється можливим встановити особу злочинця. У зв'язку з цим, визначено типи злочинців залежно від рівня їхньої компетенції: дилетант, досвідчений фахівець, професіонал. У залежності від потенційного інтересу в кіберпросторі, як: корисливі, самоствердженні, побутові, егоїстичні, дезадаптовані.

Наголошено, що характеристика особи злочинця, яка вчиняє шахрайство у кіберпросторі, складна й динамічна, вона охоплює широкий спектр внутрішніх позицій особистості в різних сферах соціального буття.

З'ясовано, що шахрайство в кіберпросторі здебільшого вчиняються чоловіками, які є соціально благополучними, позитивно характеризуються за

місцем проживання, роботи, навчання, віком від 25 до 45 років. Більшість шахраїв мають сильний дар уяви, здатність впливу і вміння переконувати. До особистих якостей шахрая належать його хитрість, брехливість, уміння прихилити до себе оточуючих, знання способів підроблення документів. За своїм зовнішнім виглядом – це звичайні люди, які вміють себе «подати», обізнані в галузі психології. Вони спостережливі і мають швидку реакцію на обстановку, що змінюється. Шахраї використовують можливість перевтілення, встановлюють контакт з людьми різних типів, обирають стиль поведінки від конкретно сформованої обстановки. Внутрішній прояв такої особи полягає у відсутності в неї морально-вольових (етичних) стримуючих факторів, що спричиняє характерну зневагу до загальноприйнятих моральних цінностей суспільства. Тобто особа, яка вчиняє шахрайство є психологічно готовою для нехтування нормами моралі, діловими, дружніми стосунками. У зв'язку із тим, що шахрайство вчиняється з прямим умислом особа бажає настання суспільно небезпечних наслідків свого діяння, впливаючи на благополуччя потерпілого. Інколи, – ставлячи під загрозу виживання останнього.

Окремо встановлено основні причини та умови, що сприяють вчиненню шахрайства в кіберпросторі.

– криміналістичну складову шахрайств, учинених в кіберпросторі (з'ясовано типові способи, сліди вчинення та приховування злочину).

Здійснено розподіл способів учинення шахрайств залежно від: періодичності вчинення злочину; сфери надання послуг; кількості задіяних злочинців; предмета посягання; способів введення в оману або зловживання довірою; місця вчинення злочину (через встановлення місця реєстрації IP-адреси електронно-обчислювальної техніки); способу підготовки до вчинення злочину.

Визначено типові способи вчинення та приховування шахрайств у кіберпросторі в умовах воєнного стану. З'ясовано джерела електронних (цифрових) слідів, які свідчать вчинення шахрайств у кіберпросторі.

З'ясовано, що приводом для початку досудового розслідування за фактом вчинення шахрайств у кіберпросторі є: 1) отримання заяв від громадян, які стали

жертвами шахрайських дій; 2) отримання заяв від громадян про роботу сумнівної вебсторінки чи діяльність організацій; 3) повідомлення від підприємств, установ, організацій, представників влади, посадових осіб, журналістів тощо; 4) повідомлення від невстановленої особи (анонімний дзвінок на лінію «102» або анонімний лист з викладеними обставинами вчинення злочину); 5) самостійне виявлення уповноваженою особою з різних джерел обставин, що свідчили про вчинення злочину (як правило, при моніторингу інтернет-ресурсів, медіа, форумів тощо).

Підставою для початку досудового розслідування за фактом вчинення шахрайств у кіберпросторі визначає слідчий шляхом правової оцінки джерел отриманої інформації про наявність у них обставин, що можуть свідчити про вчинення злочину (його ознаки) та кола причетних осіб (ч. 1, пп. 3-5 ч. 5, ч. 6 ст. 214 КПК України).

Наголошено, що слідчий у взаємодії з оперативним підрозділом на етапі оцінки первинної інформації можуть визначити основні напрями розкриття злочину та вибору спектру процесуальних заходів. Обсяг такого інструментарію залежить від визначення попередньої правової кваліфікації кримінального правопорушення із зазначенням статті (частини статті) Закону України про кримінальну відповідальність, відомості про які обов'язково необхідно зазначити під час внесення відомостей до ЄРДР відповідно до ч. 5 ст. 214 КПК України. Правильна попередня правова кваліфікація впливає і на порядок проведення досудового розслідування.

Запропоновано задля мінімізації ускладнень, з якими стикаються слідчі та оперативні підрозділи під час оцінки первинної інформації, доцільно:

– уніфікувати окремі норми КПК України, розширивши спектр процесуальних дій (можливостей) до внесення відомостей в ЄРДР;

– деталізувати момент початку розслідування, розмежувавши та позбавивши залежності в цьому питані від норм Положення про ЄРДР, порядок його формування та ведення, затвердженого наказом Генерального прокурора від 30.06.2020№ 298;

– консолідувати норми КК України з урахуванням нормативної бази про забезпечення безпеки у кіберпросторі, визначити єдину термінологію для використання правозастосовними інституціями.

Конкретизовано коло обставин, що підлягають встановленню під час розкриття шахрайств, учинених в кіберпросторі: 1) обставини стосовно події злочину (відомості про: факт, час, просторові межі, особу потерпілого, способи вчинення, предмет посягання, характер і розмір завданої шкоди, джерела електронних цифрових слідів); 2) інші обставини, що охоплюються: 2.1) відомості про причинно-наслідковий зв'язок (обставини, що сприяли вчинення шахрайства; обставини стосовно споріднених видів кримінальних правопорушень; обставини постзлочинної діяльності); 2.2) відомості про особу свідків; 3) обставини стосовно підозрюваного (відомості про особу підозрюваного, винуватість, мотив та мету); 4) обставини, які можуть мати додаткове значення в кримінальному провадженні (обставини, що впливають на ступінь тяжкості, обтяжують чи пом'якшують покарання; обставини, що є підставами для закриття кримінального провадження чи звільнення від кримінальної відповідальності або покарання; розмір процесуальних витрат).

Визначено, що організація розкриття шахрайств, учинених в кіберпросторі сприймається як типова модель, що включає в себе аналіз первинної інформації щодо обставин злочину, формулювання версій, визначення цілей та розробку плану.

Сам процес планування розкриття шахрайств, учинених в кіберпросторі має охоплювати: аналіз слідчої ситуації; вибір основного напряму розкриття злочину; визначення необхідних сил та засобів; розробку письмового плану в разі потреби; здійснення контролю над виконанням плану та його корекція.

Наголошено, що взаємодія між слідчими та оперативними підрозділами, власниками (розпорядниками) електронних комунікаційних систем, володільцями інформації в системах та іншими суб'єктами на ринку електронних комунікаційних послуг є невід'ємною частиною процесу виявлення та розкриття шахрайств, що вчиняються в кіберпросторі. Ця взаємодія базується на

взаємозалежності їхніх дій, яка допомагає збалансувати повноваження, методи та ресурси, характерні для кожного учасника співробітництва.

Окреслено, дві типові ситуації, що виникають на початковому етапі розслідування та є підґрунтям для основних напрямів розкриття шахрайств, учинених в кіберпросторі. Визначено типові слідчі версії стосовно наявної інформації про особу злочинця; механізму вчинення шахрайства та побудови вебсторінки для кримінальних дій; кількості злочинців; обізнаності осіб про співучасників; кількості вчинених злочинів; поширеності; місця розташування електронно-обчислювальної техніки; кількості потерпілих.

Окремо акцентовано на контрверсіях (версіях захисту), які вимагають додаткового дослідження та перевірки під час розкриття шахрайств, учинених в кіберпросторі.

Визначено сутність застосування OSINT у розкритті шахрайств, учинених в кіберпросторі. Зазначено, що OSINT сприяє виявленню патернів та закономірностей, які використовуються для вивчення поведінки злочинців та їхньої ідентифікації.

Розкрито зміст ресурсів OSINT, за допомогою яких здійснюється пошук інформації про користувачів за іменами, ніками, псевдонімами у: 1) соціальних мережах; 2) публічних форумах і блогах; 3) публічних базах даних; 4) освітніх платформах; 5) новинах та медіа; 6) відкритих базах даних та ресурсах; 7) засобах зворотного зв'язку; 8) колективних платформах.

Запропоновано такий алгоритм роботи з параметрами засобів OSINT для розкриття шахрайств, здійснених у кіберпросторі: 1) визначення ключових параметрів; 2) пошук інформації за ключовими параметрами; 3) аналіз інформації; 4) крос-перевірка та верифікація; 5) створення звіту та подання результатів.

Конкретизовано організаційно-тактичне забезпечення розкриття шахрайств, учинених в кіберпросторі, а саме: організаційно-тактичні аспекти вербальних та невербальних заходів, використання спеціальних знань.

Визначено особливості проведення обшуку, огляду електронно-обчислювальної техніки, допитів та підготовку до призначення окремих судових експертиз.

Наголошено, що склад слідчо-оперативної групи під час обшуку залежить від його мети та передбачуваної обстановки, яка може скластися. Крім слідчого, понятих, співробітника оперативного підрозділу можуть брати участь спеціаліст-криміналіст, перекладач, кінолог із собакою, а також особи, які виконують різні доручення, що вимагають професійних знань та навичок. У випадку надання активного супротиву з боку осіб на об'єкті обшуку, застосувати слід заходи з нейтралізації протидії та швидкого проникнення до обшукуваних приміщень.

Зазначено, що приступаючи до огляду електронно-обчислювальної техніки, слідчий і фахівець, що безпосередньо виконують всі дії на електронно-обчислюваній техніці, повинні дотримуватися певних вимог з метою забезпечення виявлення та вилучення речових доказів (слідів пальців рук та об'єктів біологічного походження).

Акцентовано, що в кримінальних провадженнях за фактами шахрайств, учинених в кіберпросторі питання до допитів формуються на підставі показань потерпілого про вид предмету шахрайства та спосіб заволодіння ним. Сам допит потерпілого має бути детальним, оскільки дозволяє встановити обставин, що можуть слугувати невідкладному розшуку злочинців та пошук викраденого майна, висування обґрунтованих версій про особу шахраїв.

Окремо визначено типові ситуації, які можуть виникнути на момент допиту підозрюваного.

Розкрито сутність та предмет експертного дослідження таких судових експертиз, як: комп'ютерно-технічна експертиза, телекомунікаційна експертиза, технічна експертиза.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Abdulkadir B., Ruya S. An Action Management System Design and Case Study on Its Usage for Cyber Fraud Prevention and Risk Analysis. *Journal of Innovative Science and Engineering.* 2021. 5 (2). Pp. 143–161.

2. Arora T., Sharma M., Khatri S. K. Detection of Cyber Crime on Social Media using Random Forest Algorithm. *2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC), Greater Noida, India.* 2019. Pp. 47–51. Doi: 10.1109/PEEIC47157.2019.8976474.

3. Ashfaq T., Khalid R., Yahaya A.S., Aslam S., Azar A.T., Alsafari S., Hameed I. A. A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. *Sensors.* 2022; 22 (19): 7162. https://doi.org/10.3390/s22197162.

4. Kara I. and Aydos M. Cyber Fraud: Detection and Analysis of the Crypto-Ransomware. *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA.* 2020. Pp. 0764-0769. Doi: 10.1109/UEMCON51285.2020.9298128.

5. Milano F., Gomez-Exposito A. Detection of Cyber-Attacks of Power Systems Through Benford's Law. *Transactions on Smart Grid,* Vol. 12, no. 3. 2021. Pp. 2741–2744. Doi: 10.1109/TSG.2020.3042897.

6. Neha Chhabra Roy, Sreeleakha Prabhakaran. Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritization and prevention. *Aslib Journal of Information Management.* Vol. 75, Issue 2. 2023. URL: https://www.emerald.com/insight/content/doi/10.1108/AJIM-11-2021-0339/full/html.

7. Nur H., Anisa, Riadi, Imam R., Erika A., Sarah. Development of conceptual framework for cyber fraud investigation. Jurnal Ilmiah Teknologi Sistem Informasi. 7. 2021. Pp.125-135. Doi: 10.26594/register.v7i2.2263.

8. OSINT Framework. URL: https://osintframework.com.

9. Viacheslav V. Vapniarchuk, Iryna I. Puchkovska, Oleksii V. Tavolzhanskyi, Roman I. Tashian Protection of ownership right in the court: the essence and

particularities (Захист права власності в суді). *Asia life science, Supplement 21(2), December2019.* Iss. 2. P. 863-879. Філіпини. (Scopus). URL: https://www.scopus.com/record/display.uri?eid=2-s2.0-85077221643&origin=resultslist.

10. Wang C. and Zhu H. Wrongdoing Monitor: A Graph-Based Behavioral Anomaly Detection in Cyber Securit. *Transactions on Information Forensics and Security,* Vol. 17. 2022. Pp. 2703-2718. Doi: 10.1109/TIFS.2022.3191493.

11. Yatsyk T. P., Shkelebei V. A. Investigation of new forms of cyber crime (phishing and cybersquatting). *Науковий вісник УжНУ. Серія: Право.* Вип. 53. Т. 2. 2018. С. 121–123.

12. Абушов Т. А. Система організаційних і тактичних дій під час проведення обшуку. *Науковий вісник Національної академії внутрішніх справ*. № 6. 2011. С. 198–205.

13. Авдєєва Г. К. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції : монографія / В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за заг. ред. В. Ю. Шепітька, В. В. Журавля. Харків : Вид. агенція «Апостіль», 2017. 238 с.

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

15. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : монографія. Київ : Атіка, 2007. 304 с.

16. Бакалінська О. О. Правове забезпечення кіберзахисту в Україні. *Платформа стратегічної та законотворчої аналітики. Серія «Право власності».* 2020. URL: https://coordynata.com.ua/pravove-zabezpecenna-kiberzahistu-v-ukraini.

17. Бідняк Г. С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств : монографія. Дніпро: ДДУВС, 2019. 152 с.

18. Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. ... канд. юрид. наук. Київ, 2007. 217 с.

19. Вакуленко О. В., Стрільцов О. М., Тарасенко О. С. та ін. Розслідування злочинців, учинених з використанням шкідливих програмних чи технічних засобів : методичні рекомендації. Київ : НАВС, 2016. 56 с.

20. Василинчук В. І. Оперативно-розшукова профілактика злочинів у бюджетній сфері: монографія. Київ: ФОП Кандиба, 2013. 396 с.

21. Василинчук В. І. Організаційно-правові та тактичні засади оперативно-розшукової профілактики злочинів у бюджетній сфері : навчальний посібник. Київ : Заграй, 2012. 210 с.

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

23. Використання електронних (цифрових) доказів у кримінальних провадженнях : методичні рекомендації / М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.; за заг. ред. О. В. Корнейка. Вид. 2-ге, доповнене. Київ : НАВС, 2020. 104 с.

24. Вітвітцький С. С., Волобуєва О. О., Волобоєв А. О. Методика розслідування незаконного поводження зі зброєю та бойовими припасами : монографія. Київ : ВД «Дакор», 2021. 308 с.

25. Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : дис. … канд. юрид. наук. Харків, 2008. 216 с.

26. Головкін С. В., Іщенко А. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування : монографія. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2013. 160 с.

27. Головні цифрові тенденції. *Datareporta.* URL: https://datareportal.com/.

28. Данильян О. Г., Дзьобань О. П. Віртуальна реальність і кіберпростір як атрибути сучасного суспільства. *Інформація і право.* Вип. № 4 (35). 2020. С. 9–21.

29. Департамент кіберполіції України. *Офіційний сайт.* URL: https://cyberpolice.gov.ua/contacts/.

30. Діброва Т. А., Пісенко Д. О., Сметаніна М. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний журнал.* Вип. № 11. 2022. С. 546–549. DOI: https://doi.org/10.32782/2524-0374/2022-11/132.

31. Доказування у справах про злочини, вчинені шляхом незаконних операцій з використанням електронно-обчислювальної техніки : методичні рекомендації. НАВС. 2020. 60 с.

32. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 2018. Дата початку дії: 01.01.2018. Дата прийняття: 27.12.2016. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128.

33. Єгоров С. О. Оперативно-розшукова характеристика кишенькових крадіжок. *Науковий вісник Дніпропетровського університету внутрішніх справ.* Вип. № 3. Дніпро, 2019. С. 169–174.

34. Журавель В. А. Ситуаційний підхід до формування окремих криміналістичних методик розслідування злочинів. *Теорія і практика судової експертизи і криміналістики.* Вип. № 8. 2008. С. 102–108.

35. Запорощенко Н. А. Розслідування організації або утримання місць для незаконного вживання, виробництва чи виготовлення наркотичних засобів, психотропних речовин або їх аналогів : дис. … канд. юрид. наук. Київ, 2012. 281 с.

36. Затенацький Д. В. Ідеальні сліди в криміналістиці (техніко-криміналістичні та тактичні прийоми їх актуалізації) : автореферат дис. … канд. юрид. наук. Харків, 2008. 20 с.

37. Звіт про результати роботи Департаменту кіберполіції у 2022 році. *Офіційний сайт Кіберполіції України*. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczi-969/.

38. Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС

України від 07.07.2017 № 575. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text.

39. Інструкція з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України : наказ МВС України від 27.04.2020 № 357. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0443-20#Text.

40. Інструкція про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведення огляду місця події : наказ МВС України від 03.11.2015 № 1339. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z1392-15#Text.

41. Казміренко Л. І. Про засади маніпуляційного впливу на суспільну свідомість. *Філософські, методологічні та психологічні проблеми права: матеріали II Всеукраїнської науково-теоретичної конференції (м. Київ, 31 січня 2009 року).* Київ : КНУВС, 2009. С. 201–204.

42. Кікінчук В. В. Типові слідчі ситуації початкового етапу розслідування викрадень бюджетних коштів в агропромисловому комплексі. *Право і безпека.* Вип. № 2 (49). 2013. С. 131–135.

43. Климчук М. П., Коміссарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні: навч. посіб. Львів: Львівський державний університет внутрішніх справ, 2022. 112 с.

44. Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. ... доктор філософі. Дніпро, 2022. 229 с.

45. Ковальчук О. В. Методика розслідування шахрайств, пов'язаного з діяльністю кредитної спілки : дис …. доктор філософії. Львів, 2020. 236 с.

46. Комп'ютерно-технічна експертиза. *Вебресурс.* URL: https://kndise.gov.ua/kompyuterno-tehnichna/.

47. Коновалова В. О., Шепітько В. Ю. Юридична психологія : академічний курс / В. О. Коновалова. Київ : Ін Юре, 2004. 424 с.

48. Конституція України від 28 червня 1996 року № 254к/96-ВР. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

49. Коршенко В. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *National law journal: theory and practice.* Вип. № 2. 2017. С. 197–199.

50. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. …. доктор філософії. Київ, 2021. 255 с.

51. Кримінальний процес : підручник / В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. 824 с.

52. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

53. Кришевич О. В. Кримінально-правова характеристика предмета шахрайства. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* Вип. № 24, 2011. С. 183–191.

54. Майстренко М., Татарин І. Проблемні аспекти доказування шахрайств, вчинених у кіберпросторі. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція».* Вип. № 52. 2021. С. 85–89. DOI: https://doi.org/10.32841/2307-1745.2021.52.19.

55. Мельник С. С. Виявлення та запобігання фінансовому шахрайству у забезпеченні фінансової безпеки комерційних банків / С. С. Мельник : дис. ... канд. економ. наук. Київ, 2019. 252 с.

56. Методика розслідування шахрайств, пов'язаних із купівлею-продажем товарів через мережу «Інтернет»: теоретичні та праксеологічні засади : монографія / М. М. Єфімов, Н. В. Павлова, С. В. Чучко. Одеса : Видавничий дім «Гельветика», 2022. 200 с.

57. Настільна книга слідчого : науково-практичне видання для слідчих і дізнавачів / М. І. Панов, В. Ю. Шепитько, В. О. Коновалова та ін. Київ : Ін ре, 2003. 720 с.

58. Науково-практичний коментар до Кримінального кодексу України / М. І. Мельника, М. І. Хавронюка. 6-те вид., перероблене і доповнене. Київ : Юридична думка, 2009. 1232 с.

59. Олішевський О. В. Поняття організація розслідування злочинів. *Боротьба зі злочинністю та забезпечення громадського порядку: проблеми теорії та практики.* Харьків : ХНУВС, 2009. С. 78–79.

60. Пазинич Т. А. Особливості сучасних шахрайств та їх вплив на методику розслідування. *Вісник Луганського державного університету внутрішніх справ.* Вип. № 4. Луганськ : ЛДУВС, 2005. С. 124-131.

61. Погорецький М. А., Шеломенцев В. П. Поняття оперативно-розшукової характеристики злочинів. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* Вип. № 1 (47). 2010. С. 214–223.

62. Порядок ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події : Наказ МВС України від 08.02.2019 № 100. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0223-19#Text.

63. Про введення воєнного стану в Україні. Указ Президента України № 64 / 2022. *Президент України Володимир Зеленський: Офіційне інтернет-представництво.* URL: https://www.president.gov.ua/documents/642022-41397.

64. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

65. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування : статистика. *Офіційна сторінка Офісу Генерального прокурора.* URL: https://gp.gov.ua/ua/posts/statistika.

66. Про Національну поліції : Закон України від 02.07.2015 № 580-VII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

67. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

68. Про основні засади забезпечення кібербезпеки України : закон України від 17.08.2022 № 2163-VIII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

69. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

70. Про платіжні послуги : Закон України від 30.06.2021 № 1591-IX. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text.

71. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про стратегію кібербезпеки України» : Указ Президента України. *Офіційне інтернет-представництво.* URL: https://www.president.gov.ua/documents/4472021-40013.

72. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.04.2026 року № 96/2016. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text.

73. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2229-12.

74. Про судову експертизу : Закон України від 25 лютого 1994 року № 4038-XII. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text.

75. Про судову практику у справах про злочини проти власності : Постанова Верховного суду України від 06.11.20009 № 10. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/v0010700-09#Text.

76. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Практичний посібник. Нью-Йорк і Женева, 2020. 119 с. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

77. Протокол Берклі щодо розслідування із використанням відкритих цифрових даних. Юрфем.UA. 2022. URL: https://jurfem.com.ua/protokol-berkli-schodo-rozsliduvannia-iz-vykorystannyam-zyfrovych-danych/.

78. Пфо О. М. Основні поняття і класифікація кіберзлочинності. *Матеріали Всеукраїнської науково-практичної конференції «Актуальні задачі та досягнення у галузі кібербезпеки».* 2016. С. 33–34.

79. Пчолкін В. Д. Поняття характеристики злочинів у теореії оперативно-розшукової діяльності. *Вісник ЛАВС МВС України ім. 10-річчя незалежності України.* Спецвип. № 2 Ч. 1. 2004. С. 67–76.

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

81. Самойленко О. А. Криміналістичний та правовий аналіз злочинної діяльності в мережі Інтернет. *Порівняльно-аналітичне право.* Вип. № 4. 2015. С. 408–411.

82. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : дис. … канд. юрид. наук. Донецьк, 2014. 226 с.

83. Самойлов С. В. Типові слідчі ситуації початкового етапу розслідування шахрайств, що вчиняються з використанням мережі «Інтернет», відповідні їм слідчі версії та алгоритми їх перевірки. *Проблеми правознавства та правоохоронної діяльності.* Вип. № 4. 2014. С. 25–31.

84. Самойлов С. В. Шахрайства на Інтернет-аукціонах як один із способів скоєння шахрайств з використанням мереж Інтернет (криміналістична характеристика способу вчинення). *Форум права.* Вип. № 4. 2011. С. 645–650.

85. Слідчі (розшукові) дії : навчальний посібник / О. В. Авраменко, Р. І. Благута, Ю. В. Гуцуляк та ін.; за заг. ред. Р. І. Благути та Є. В. Пряхіна. Львів: ЛьвДУВС, 2013. 416 с.

86. Стрільців О. М., Крижна В. В., Максименко О. В. та ін. Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту: методні рекомендації / за заг. ред. Ю. Ю. Орлова. Київ : НАВС, 2014. 80 с.

87. Тарасова О. В. Удосконалення законодавства щодо кримінальної відповідальності за шахрайство, учинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки. *Актуальні проблеми держави і права.* Вип. № 72. 2014. С. 481–488.

88. Телекомунікаційна експертиза. *Вебресурс.* URL: https://kndise.gov.ua/telekomunikaczijna/.

89. Технічна експертиза документів. *Вебресурс.* URL: https://kndise.gov.ua/tehnichna-ekspertyza-dokumentiv/.

90. Трач С. С. Деякі аспекти оперативно-розшукової профілактики шахрайств у сфері кредитних операцій банків. *Матеріали Міжнародної науково-практичної конференції «Актуальні питання виявлення, досудового розслідування та попередження корупційних правопорушень» (м. Дніпропетровськ, 24 квітня 2015 року).* Дніпропетровськ : ДДУВС, 2015. С. 185–187.

91. Хань Г. А. Теоретичні засади планування та організації розслідування злочинів : дис. … канд. юрид. наук. Донецьк, 2007. 221 с.

92. Хижняк Є. С. Типові слідчі ситуації при розслідуванні статевих злочинів. *Південноукраїнський правничий часопис.* Вип. № 4. 2012. С. 197–199.

93. Цивільний кодекс України від 16.01.2003 № 435-IV. *Офіційний вебпортал Верховної ради України.* URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.

94. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : монографія. Київ : Хай-Тек Прес, 2010. 624 с.

95. Чуйко С. В. Розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет : дис. ... доктор філософії. Дніпро, 2021. 276 с.

96. Шевчук В. А. Слідчі ситуації та їх вплив на розробку тактичних операцій. *Науковий вісник Міжнародного гуманітарного університету.* Вип. № 6-3. Т. 2. 2013. С. 125–129.

97. Шепітько В. Ю. Криміналістика. Енциклопедичний словник / В. Я. Тація. Харків : Право, 2001. 560 с.

ДОДАТКИ

Додаток А

Таблиці до підрозділу 2.3 в частині отримання інформації з відкритих джерел (OSINT)

Таблиця 1

Ресурс OSINT Framework	*Адреса ресурсу*	*Короткий опис ресурсу*
Namechk	https://namechk.com	Namechk перевіряє 36 різних доменних імен і понад 100 веб-сайтів соціальних мереж і онлайн-платформ. До найпопулярніших соціальних мереж, які перевіряються, належать: Facebook, Twitter, YouTube, Blogger, Twitch, Tumblr, TikTok, WordPress, eBay, Yelp, Flickr, PayPal. Namechk бере введене ім'я користувача (навіть випадкові слова) і перевіряє його доступність як ім'я домену та ім'я користувача на десятках соціальних каналів і онлайн-платформ. Якщо назва доступна на певному каналі, дана інформація буде відображена на сайті Namechk.
Namechk (T)	https://github.com/GONZOsint/Namechk	GitHub-репозиторій є інструментом для перевірки доступності імен користувачів на різних платформах та соціальних мережах. Основна можливість цього інструмента – перевірка ім'я користувачів на різних веб-сайтах одночасно, а саме: перевірка доступності ім'я на багатьох різних платформах та соціальних мережах, сервісах для обміну фотографіями, форумах та ін.; збір результатів; відстеження брендування; збір інформації про власника: заголовок профілю, фотографію профілю та іншу публічно доступну інформацію.
NameCheckr	https://www.namecheckr.com	Мета створення даного інструменту – це дослідження доступності домену та ім'я користувача в соціальних мережах для пошуку назви нового чи існуючого проєкту.
UserSearch.org	https://usersearch.org	Записи ім'я користувачів поповнюють базу безпосередньо під час пошуку на сотнях веб-сайтів і в базах даних, що містять мільйони профілів. Використовуючи дану інноваційну пошукову систему можливо зробити безкоштовний і швидкий пошук ім'я користувача, пов'язаного з онлайн-ідентифікатором людини. Ресурс дозволяє знайти повну інформацію про облікові записи, включаючи профілі в соціальних

		мережах, профілі знайомств, номери телефонів та адреси електронної пошти. Є можливість відслідкувати онлайн-активність, приховані фотографії та приховані профілі. За результатами пошуку можливо отримати: справжнє ім'я, вигадані ім'я та псевдоніми, ймовірну адресу, використані адреси електронної пошти, номери телефонів, картинки та приховані зображення, активність облікового запису онлайн, статус стосунків з іншими користувачами, пов'язані онлайн-профілі, облікові записи тощо.
WhatsMyName (T)	https://github.com/WebBreacher/WhatsMyName	Мета створення ресурсу – виявлення, чи використовувалися ім'я користувачів на різних платформах та соціальних мережах для аналізу присутності користувачів в Інтернеті. Ось деякі можливості WhatsMyName: автоматична перевірка доступності введених ім'я користувачів на різних платформах і соціальних мережах; підтримка багатьох платформ; конфігурування платформ; збереження результатів перевірки ім'я; індексація ім'я для подальшого аналізу тощо.
Thats Them	https://thatsthem.com	Дозволяє здійснювати пошук за іменем для отримання інформації про користувача, включаючи адресу, номер телефону, електронну адресу тощо. Функція «Зворотний пошук адреси» дозволяє встановити особу проживання за певною адресою, оновлену інформацію про власника будинку, дані про іпотеку, оціночну вартість будинку тощо. Ресурс надає можливість пошуку інформації про особу за номером телефону. Функція «Зворотний пошук електронної пошти» робить можливим отримання ім'я, адреси та номеру телефону, пов'язаних з відомою адресою електронної пошти. Функція «Пошук IP-адреси» повертає географічне розташування та Інтернет-провайдера. Функція «Пошук транспортного засобу» надає інформацію про автомобіль, контактну інформацію попередніх власників.
Check Usernames	https://checkusernames.com	Перевіряє доступність введеного ім'ям користувача в понад 500 соціальних мережах.
Instant Username Search	https://instantusername.com/#/	Перевіряє введене ім'я користувача в понад 100 сайтах соціальних мереж.

Таблиця 2

Ресурс OSINT Framework		*Адреса ресурсу*	*Короткий опис ресурсу*
Email Search	ThatsThem	https://thatsthem.com	Має функцію «Зворотний пошук електронної пошти» робить можливим отримання ім'я, адреси та номеру телефону, пов'язаних з відомою адресою електронної пошти. Більш детально описаний в табл. 1.
	Hunter	https://hunter.io	Сервіс Hunter (раніше відомий як Hunter.io) – це інструмент, який надає можливість знаходити електронні адреси підприємств, організацій та осіб, які пов'язані з певними доменами. Основні можливості сервісу Hunter включають: пошук електронних адрес підприємств за їх доменами, валідацію електронних адрес, знаходження контактних даних (сервіс здійснює пошук інформації про імена та посади осіб, які пов'язані з вказаним доменом), перевірку наявності пошти на домені (тобто чи існує домен з вказаною поштою), інтеграцію з іншими сервісами (Hunter надає можливість інтеграції з іншими інструментами та CRM-системами для зручного управління зібраними даними), підтримку API (можливість автоматизованого доступу для програмістів).
	Melissa	https://www.melissa.com	Веб-сервіс Melissa є платформою для управління та оптимізації даних, яка надає різноманітні можливості для покращення якості та точності даних. Основні можливості та функції веб-сервісу Melissa включають: адресну верифікацію, валідацію електронних адрес (може бути використане для підтвердження дійсності контактних даних), знаходження геолокації, перевірку телефонних номерів (інформацію про код країни та інші атрибути номера), виявлення дублікатів, перевірку даних на наявність помилок, API та інтеграцію, аналіз даних (можливість проводити аналіз та робити витяги даних) тощо.
	Pipl	https://pipl.com	Pipl (https://pipl.com) – це онлайн-платформа, яка надає різноманітні можливості для пошуку та збору інформації про людей з різних джерел в Інтернеті. Основні

			можливості та функції, які пропонує Pipl, включають: пошук за ім'ям, прізвищем та іншими персональними даними для знаходження інформації про конкретну особу; пошук за електронними адресами (знаходить профілі та аккаунти осіб в різних онлайн-сервісах); пошук за телефонними номерами інформацію про власника номера та його активність в мережі; аналіз даних з різних соціальних мереж та інших відкритих джерел, надаючи інформацію про профілі особи в Інтернеті; пошук за адресою проживання та пов'язані з нею дані; збір інформації про особу; пошук за публічними записами та документами; аналіз зв'язків та контактів особи у соціальних мережах; функцію мапування (Pipl надає інтерактивну карту, на якій можна побачити розташування пов'язаних з особою точок) тощо.
	Skymem	http://www.skymem.info	Здійснює пошук електронних адрес компаній та людей. Для цього потрібно лише ввести в пошуковий рядок ім'я домену організації або ім'я та прізвище особи з доменним ім'ям.
	theHarvester	http://www.edge-security.com/theharvester.php	Ресурс призначений для збору інформації з різних відкритих джерел для використання в розслідуваннях, аналізі безпеки та зборі інформації про цільову систему чи організацію. Основні можливості цього інструмента включають: збір інформації про домени (про піддомени, електронну пошту, сервери та інше); знаходження електронних адрес, пов'язаних з введеним доменом або ключовим словом; збір інформації з соціальних мереж; відстеження доменів, які пов'язані з основним доменом, отримання інформації про IP-адреси, пов'язані з доменом або організацією тощо.
Email Verification	BytePlant Email Validator	https://www.email-validator.net	Засіб перевірки електронної пошти та номерів телефонів.
	Read Notify	https://www.readnotify.com/rea	Платформа, яка надає певні інструменти для відстеження та контролю за електронними листами, а саме: є функція, яка дозволяє відстежувати, коли отримувач відкриває лист

			(можливо отримати підтвердження про те, коли та де був відкритий лист, а також іншу інформацію, наприклад, чи було відкрите посилання у листі); відстеження місцезнаходження отримувача на момент відкриття листа; відстеження часу, коли саме був відкритий лист, а також скільки часу тривав перегляд; надсилання зашифрованих листів, які можна відкривати тільки за допомогою спеціального пароля або посилання тощо.
	Email Reputation	https://emailrep.io	Інструмент, який надає аналіз та оцінку електронних адрес для виявлення потенційно небезпечних або шахрайських активностей. Основна функціональність включає: аналіз ризику електронної адреси (чи є ця адреса поміченою у здійсненні шахрайських або небезпечних дій); перевірку репутації домену; перевірка IP-адреси відправника листа для виявлення можливих загроз; виявлення потенційних спроб фішингу через електронну пошту тощо.
Breach Data	Have I been pwned?	https://haveibeenpwned.com	Веб-сервіс, який надає можливість перевірити, чи було порушення безпеки даних та витоків інформації з e-mail користувача. Основні можливості Have I Been Pwned включають: перевірку облікового запису щодо втрати або викрадення унаслідок витоку інформації в різних онлайн-сервісів; підписку на сповіщення щодо ймовірних витоків інформації; перевірку паролів у витоках даних; API, яке дозволяє розробникам інтегрувати функціональність перевірки витоків інформації у свої додатки та сервіси.
	DeHashed	https://dehashed.com	Онлайн-сервіс для перевірки витоків даних та пошуку інформації з відкритих джерел для покращення кібербезпеки. Основні можливості Dehashed включають: пошук витоків даних за електронною адресою або ім’ям користувача); пошук хешів паролів, що допомагає перевірити, чи використовується певний пароль в інших облікових записах; пошук інформації про користувачів, включаючи їхні електронні адреси, ім’я користувачів, IP-адреси тощо; API для

			розробників для інтеграції з іншими системами та додатками; можливість експортувати результати пошуку в CSV-форматі для подальшого аналізу та обробки; підписку на сповіщення.
	Intelligence X	https://intelx.io	Інформаційний пошуковий ресурс, який дозволяє здійснювати пошук і аналіз даних з різних джерел. Основні можливості IntelligenceX включають: пошук інформації за ключовими словами, доменами, IP-адресами та іншими параметрами; моніторинг доменів щодо змін на веб-сайтах та доменах; пошук зображень за ключовими словами або хешами зображень; пошук пов'язаної інформації за електронними адресами; можливість перевіряти веб-сайти на наявність вразливостей, знаходити сторінки та архіви, пов'язані з конкретним доменом; можливість пошуку інформації, що походить з різних соціальних мереж та форумів; API для інтеграції з іншими сервісами та розробкою власних інструментів.
Spam Reputation Lists	DNS Blackhole Lists	https://dnslytics.com	Онлайн-інструмент для аналізу доменних імен та DNS-записів. Основні можливості цього інструменту включають: аналіз DNS-записів; перевірку безпеки (надає інформацію про ризики безпеки, пов'язані з доменом, включаючи можливість виявлення підозрілих або шахрайських веб-сайтів); мережевий аналіз (надає інформацію про мережеві пристрої, пов'язані з доменом, включаючи IP-адреси, мережевих провайдерів тощо); перегляд історії DNS-записів для конкретного домену; інформацію про SSL-сертифікати, WHOIS-дані та інші параметри домену.
Mail Blacklists	MxToolbox	https://mxtoolbox.com	Комплексний інструмент для аналізу та діагностики поштових серверів і доменів. Основні можливості цього інструмента включають: перевірку MX-записів домену для визначення поштових серверів, які відповідають за прийом електронної пошти для даного домену; діагностику проблем з поштовими серверами, такими як некоректно налаштовані DNS-записи, блеклістинг IP-адрес, проблеми з SPF, DKIM та DMARC;

			перевірку блеклістингу, а саме, чи знаходиться IP-адреса поштового сервера в блеклистах, що допомагає виявити можливі проблеми з доставкою електронної пошти; аналіз DNS-записів для визначення налаштувань домену; тестування електронної пошти для перевірки відповідності налаштувань; виявлення відкритих та закритих портів на вказаному сервері; перевірку TLS на поштових серверах.

Таблиця 3

Ресурс OSINT Framework		*Адреса ресурсу*	*Короткий опис ресурсу*
Vehicle Records	VinCheck	https://www.nicb.org/vincheck	Ресурс створений Національнм агентством зі злочинів в галузі страхування (NICB) і надає можливість перевірити інформацію про автомобіль за його унікальним номером (VIN – Vehicle Identification Number). Основні можливості цього сервісу включають: перевірку автомобіля за VIN для отримання інформації про його історію, стан, деталі моделі та інші характеристики; історію крадіжок авто; інформацію про страхові виплати на автомобіль у зв'язку зі збитками, крадіжками або іншими подіями; історію власності, тобто інформацію про попередніх та поточних власників автомобіля; доступ до бази даних викрадених автомобілів.
	TRAVIC – Public Transportation Tracking	https://mobility.portal.geops.io/en/world.geops.transit	Це інтерактивний мапінговий інструмент, який надає можливість відстеження громадського транспорту та мобільності у різних містах світу. Основні можливості цього сервісу включають: відстеження громадського транспорту, такого як автобуси, трамваї, метро тощо на мапі в режимі реального часу (можна побачити поточне розташування транспорту та передбачити час прибуття на певну локацію); планування маршруту, тобто можна вказати початковий і кінцевий пункти, а також переглянути доступні маршрути та прогнозований час подорожі; інформацію про зупинки, станції громадського транспорту, станції метро; розклад руху громадського транспорту на певному маршруті; інформацію про маршрути, такі як довжина, кількість зупинок тощо; інтерактивність – взаємодіяю з мапою, натискаючи на конкретні зупинки та транспорт можливо отримувати детальнішу інформацію.

Air Traffic Records	FlightAware - Live Flight Tracker	https://www.flightaware.com	Платформа для відстеження руху повітряних суден, надання інформації про рейси та пов'язані дані. Основні можливості цього сервісу включають: відстеження польотів в реальному часі на мапі: поточне розташування, висоту, швидкість та напрямок руху; інформацію про рейси: розклади рейсів, статуси злету і посадки, запізнення, прогнозований час прибуття та відправлення; подробиці про повітряні судна: модель, виробник, рік випуску, реєстраційний номер тощо; інформацію про аеропорти: графік роботи, гейти, заплановані та актуальні рейси; глобальне покриття: рух повітряних суден у багатьох країнах світу, що дозволяє відстежувати польоти на різних континентах; додаткові дані: метеорологічні умови, статистика руху повітряних суден, інформацію про власників та операторів; карти повітряного руху: загальний рух повітряних суден у певній області.
	Flightradar24.com	https://www.flightradar24.com	Платформа для відстежування руху повітряних суден та надання інформації про авіаційний рух. Основні можливості цього сервісу включають: відстеження польотів на мапі в реальному часі: поточне розташування, швидкість, висоту, напрямок руху, плановану і приблизну часову рамку для злету та посадки; інформацію про рейси: номер рейсу, пункти призначення, тип повітряного судна, час вильоту та приземлення, запізнення тощо; деталі повітряних суден: інформацію про конкретне повітряне судно, включаючи модель, рік виробництва, виробника, реєстраційний номер тощо; режими перегляду мапи, включаючи вид зверху, режим карти, а також показ прямого вигляду на мапі; історію руху суден; метеорологічну інформація: дані про погоду, включаючи погодні умови у місцях приземлення та вильоту: пошук рейсів за номером або маршрутом тощо.

Marine Records	Marine Traffic	https://www.marinetraffic.com/	Платформа для відстеження руху морських суден та надання інформації про морський трафік. Основні можливості цього сервісу включають: відстеження суден в реальному часі на карті: поточне розташування, швидкість, напрямок руху, класифікацію судна та інші деталі; інформацію про судна: характеристики, історію руху, власників та операторів; режими перегляду: вид зверху, режим карти, режим супутникового зображення та інші; пошук конкретних морських суден за їх назвою або номером; маршрути суден, історію руху, а також плановані маршрути; метеорологічну інформація про погодні умови у місцях руху суден; порти та термінали, включаючи судна, що прибувають та відправляються тощо.
	Vessel Tracker	https://www.vesseltracker.com	Платформа для відстеження руху морських суден та надання інформації про морський трафік. Основні можливості цього сервісу включають: відстеження суден в реальному часі на карті: поточне розташування, швидкість, напрямок руху та інші деталі; інформацію про судна: характеристики, історію руху, власників та операторів; режими перегляду: вид зверху, режим карти, режим супутникового зображення та інші; пошук суден; маршрути суден, історію руху суден, плановані маршрути; сигнали AIS – сигнали автоматичної ідентифікації суден, які передають інформацію про судно, його розташування та інші параметри; інформацію про порти: діяльність, судна, що прибувають та відправляються; події та новини у сфері морського транспорту тощо.

Додаток Б

Динаміка злочинності та прокурорсько-слідчої діяльності[116]

		2018	2019	2020	2021	2022	З/П	С/П
Загальні відомості про реєстрацію КП	Облік КП	487133	444130	360622	321443	362636	1975964	395193
		-	-8,83 %	-18,80 %	-10,86 %	12,82 %		-6,42 %
	Підозра	191856	171691	167098	172494	132418	835557	167111
		-	-10,51 %	-2,68 %	3,23 %	-23,23 %		-8,30 %
	До суду	173257	154585	152348	156695	114916	751801	150360
		-	-10,78 %	-1,45 %	2,85	-26,66 %		-9,01 %
	Залишок	303604	281119	204754	160929	242190	1192596	238519
		-	-7,41 %	-27,16 %	-21,40 %	50,49 %		-1,37 %
Кримінальні правопорушення проти власності	Облік КП	303850	257608	190258	158729	113137	1023582	204716
		-	-15,22 %	-26,14 %	-16,57 %	-28,72 %		-21,66 %
	Підозра	106413	90441	82321	81985	49846	411006	82201
		-	-15,01 %	-8,98 %	-0,41 %	-39,20 %		-15,90 %
	До суду	98663	83399	75470	75660	42668	375860	75172
		-	-15,47 %	-9,51 %	0,25 %	-43,61 %		-17,08 %
	Залишок	201289	170856	113160	81049	68606	634960	126992
		-	-15,12 %	-33,77 %	-28,38 %	-15,35 %		-23,15 %
Шахрайства	Облік КП	33290	32358	26830	23847	32086	148411	29682
		-	-2,80 %	-17,08 %	-11,12 %	34,55 %		0,89 %
	Підозра	8699	8241	8713	9406	7490	42549	8510
		-	-5,26 %	5,73 %	7,95 %	-20,37 %		-2,99 %
	До суду	7019	6865	7399	8027	5778	35088	7018
		-	-2,19 %	7,78 %	8,49 %	-28,02 %		-3,49 %
	Залишок	25235	24695	19141	15122	25808	110001	22000
		-	-2,14 %	-22,49 %	-21,00 %	70,67 %		6,26 %
Кримінальні правопорушення у сфері використання ЕОМ	Облік КП	2301	2204	2498	3310	3415	13728	2746
		-	-4,22 %	13,34 %	32,51 %	3,17 %		11,20 %
	Підозра	1608	1481	1675	2435	2643	9842	1968
		-	-7,90 %	13,10 %	45,37 %	8,54 %		14,78 %
	До суду	1330	1259	1492	1953	2435	8469	1694
		-	-5,34 %	18,51 %	30,90 %	24,68 %		17,19 %
	Залишок	771	836	944	1291	909	4751	950
		-	8,43 %	12,92 %	36,76 %	-29,59 %		7,13 %

[116] Розрахунок відсоткового співвідношення звітних показників ОГП здійснювався шляхом порівняння поточного року з попереднім за формулою: ((А/В)*100)-100= %).

Додаток В

Співвідношення результатів прокурорсько-слідчої діяльності[117]

		2018	2019	2020	2021	2022	З/П	С/П
Загальні відомості про реєстрацію КП	Облік КП	487133	444130	360622	321443	362636	1975964	395193
		35,57 %	34,81 %	42,25 %	48,75 %	31,69 %		38,61 %
	Підозра	191856	171691	167098	172494	132418	835557	167111
		39,38 %	38,66 %	46,34 %	53,66 %	36,52 %		42,91 %
	До суду	173257	154585	152348	156695	114916	751801	150360
		90,31 %	90,04 %	91,17 %	90,84 %	86,78 %		89,83 %
	Залишок	303604	281119	204754	160929	242190	1192596	238519
		62,32 %	63,30 %	56,78 %	50,06 %	66,79 %		59,85 %
Кримінальні правопорушення проти власності	Облік КП	303850	257608	190258	158729	113137	1023582	204716
		32,47 %	32,37 %	39,67 %	47,67 %	37,71 %		37,98 %
	Підозра	106413	90441	82321	81985	49846	411006	82201
		35,02 %	35,11 %	43,27 %	51,65 %	44,06 %		41,82 %
	До суду	98663	83399	75470	75660	42668	375860	75172
		92,72 %	92,21 %	91,68 %	92,29 %	85,60 %		90,90 %
	Залишок	201289	170856	113160	81049	68606	634960	126992
		66,25 %	66,32 %	59,48 %	51,06 %	60,64 %		60,75 %
Шахрайства	Облік КП	33290	32358	26830	23847	32086	148411	29682
		21,08 %	21,22 %	27,58 %	33,66 %	18,01 %		24,31 %
	Підозра	8699	8241	8713	9406	7490	42549	8510
		26,13 %	25,47 %	32,47 %	39,44 %	23,34 %		29,37 %
	До суду	7019	6865	7399	8027	5778	35088	7018
		80,69 %	83,30 %	84,92 %	85,34 %	77,14 %		82,28 %
	Залишок	25235	24695	19141	15122	25808	110001	22000
		75,80 %	76,32 %	71,34 %	63,41 %	80,43 %		73,46 %
Кримінальні правопорушення у сфері використання ЕОМ	Облік КП	2301	2204	2498	3310	3415	13728	2746
		57,80 %	57,12 %	59,73 %	59,00 %	71,30 %		60,99 %
	Підозра	1608	1481	1675	2435	2643	9842	1968
		69,88 %	67,20 %	67,05 %	73,56 %	77,39 %		71,02 %
	До суду	1330	1259	1492	1953	2435	8469	1694
		82,71 %	85,01 %	89,07 %	80,21 %	92,13 %		85,83 %
	Залишок	771	836	944	1291	909	4751	950
		33,51 %	37,93 %	37,79 %	39,00 %	26,62 %		34,97 %

[117] Розрахунок відсоткового співвідношення звітних показників ОГП щодо КП, у яких особам вручено повідомлення про підозру (Підозра); КП, за якими провадження направлені до суду (До суду) та КП, у яких на кінець звітного періоду рішення не прийнято (Залишок) здійснювався шляхом порівняння показників Підозри з Облік КП; До суду з Підозрою; Залишку до Облік КП за формулою: (А*100)/В= %.

Додаток Г

Співвідношення кількісних показників досліджуваного злочину за принципом «від загального до окремого»

	Загальні показники	Кримінальні правопорушення проти власності	Шахрайства	Шахрайства, учинені шляхом використання ЕОМ
Облік КП	395193	204716	29682	3572
	-	51,80 %	14,50 %	12,03 %
Підозра	167111	82201	8510	1206
	-	49,19 %	10,35 %	14,17 %
До суду	150360	75172	7018	956
	-	49,99 %	9,34 %	13,62 %
Залишок	238519	126992	22000	2526
	-	53,24 %	17,32 %	11,48 %

Співвідношення кількісних показників досліджуваного злочину за принципом «від окремого до загального»

	Загальні показники	Кримінальні правопорушення проти власності	Шахрайства	Шахрайства, учинені шляхом використання ЕОМ
Облік КП	395193	204716	29682	3572
	0,90 %	1,74 %	12,03 %	-
Підозра	167111	82201	8510	1206
	0,72 %	1,47 %	14,17 %	-
До суду	150360	75172	7018	956
	0,64 %	1,27 %	13,62 %	-
Залишок	238519	126992	22000	2526
	1,06 %	1,99 %	11,48 %	-

Додаток Д

Зведені дані
опитування 107 працівників Національної поліції України

1.	**Ваш стаж практичної роботи**	
	до 1 року	17,8 %
	від 2 до 5 років	43,9 %
	від 5 до 10 років	29,9 %
	понад 10 років	8,4 %
2.	**Ваша освіта**	
	неповна вища («бакалавр»)	25,2 %
	повна вища («спеціаліст», «магістр»)	70,1 %
	власний варіант	4,7 %
3.	**Як Ви оцінюєте свій рівень навичок користування інформаційними та комунікаційними технологіями, а також обізнаності в ІТ-сфері?**	
	низький («побутовий»)	26,2 %
	середній («розвинений»)	56,1 %
	високий («фахівець»)	17,7 %
	важко відповісти	0 %
4.	**Що Ви розумієте під поняттям «кіберпростір»?** *(відповідь у довільній формі)*	
	вказали	85 %
	не вказали	15 %
5.	**Чи брати участь у розкритті шахрайств, учинених в кіберпросторі?**	
	так	78,5 %
	ні	21,5 %
6.	**На Вашу думку, чи є потреба в розроблені науково-практичних рекомендацій (алгоритмів), які б дозволили ефективно розкривати шахрайства?**	
	так	76,6 %
	ні	18,7 %
	важко відповісти	4,7 %
7.	**На Вашу думку, який вид шахрайства найбільш типовий у кіберпросторі?**	
	фішинг	74,7 %
	сніферінг	4,3 %
	вішинг	7,5 %
	кардинг	7,1 %
	власна відповідь	6,4 %
8.	**На Вашу думку, первинна інформація про шахрайство, учинене в кіберпросторі, є результатом**	
	оперативно-розшукової діяльності оперативних підрозділів	11,2 %
	слідчої діяльності в рамках кримінального провадження	9,3 %

	заяви та повідомлення громадян	78,2 %
	важко відповісти	1,3 %
9.	**На Вашу думку, предметом шахрайств, учинених в кіберпросторі є**	
	майно (рухоме та нерухоме)	4 %
	право на майно	12,1 %
	кошти	68,9 %
	інформація	10,3 %
	важко відповісти	3,7 %
10.	**Де найчастіше можуть бути виявленні сліди під час розкриття шахрайств, учинених в кіберпросторі?** *(можливо декілька відповідей)*	
	електронні пристрої	60,7 %
	носії електронних даних	51,4 %
	електронні дані в інформаційних та комунікаційних системах	80,4 %
	електронні дані в комерційних системах	63,6 %
	мережеві маршрутизатори	7,4 %
	системи відеоспостереження	7,4 %
	продукти програмного забезпечення	4,7 %
	власна відповідь	1,9 %
11.	**Які форми взаємодії є найбільш ефективними під час розкриття шахрайств, учинених в кіберпросторі?**	
	процесуальна	79,4 %
	непроцесуальна (організаційна)	20,6 %
	важко відповісти	0 %
12.	**Чи є потреба в організації розкриття шахрайств, учинених в кіберпросторі?**	
	так, у будь-якому випадку	25,2 %
	так, лише у найбільш складних кримінальних провадженнях	72,9 %
	ні	1,9 %
13.	**Чи є специфіка в організації розкриття шахрайств, учинених в кіберпросторі?**	
	так	80,4 %
	ні	14,9 %
	важко відповісти	4,7 %
14.	**Який найбільш ефективний вид заходів для організаційно-тактичного забезпечення розкриття шахрайств, учинених в кіберпросторі?** *(можливо декілька відповідей)*	
	невербальні заходи	65,8 %
	вербальні заходи	93,5 %
	використання спеціальних знань	77,6 %
	важко відповісти	0 %

Додаток Е

ЗВЕДЕНІ ДАНІ
вивчення 50 матеріалів кримінального провадження, пов'язаних з розкриттям шахрайств, учинених в кіберпросторі

1.	**Привід початку досудового розслідування**	
	отримання заяв від громадян, які стали жертвами шахрайських дій	60 %
	отримання заяв від громадян про роботу сумнівної вебсторінки чи діяльності організації	8 %
	повідомлення від підприємств, установ, організацій, представників влади, посадових осіб, журналістів тощо	12 %
	повідомлення від невстановленої особи (анонімний дзвінок на лінію «102» або анонімний лист з викладеними обставинами вчинення злочину)	4 %
	самостійне виявлення уповноваженою особою з різних джерел обставин, що свідчили про вчинення злочину	16 %
2.	**Спосіб вчинення шахрайства у кіберпросторі** *(є декілька варіантів одночасно, внаслідок значної тривалості злочинної діяльності та її епізодів)*	
	отримання у власників платіжних карток реквізитів та іншої конфіденційної інформації про картку	50 %
	отримання даних про банківську картку з використанням електронно-обчислювальної техніки	34 %
	дублювання фінансових номерів	34 %
	створення і забезпечення діяльності фіктивного інтернет-магазину або кур'єрської служби	30 %
	створення або використання вебсторінок (програм-підтримки) благодійних організацій	16 %
	створення інтернет-аукціонів шляхом надання недостовірних даних і пропозицій	16 %
	забезпечення підтримки: псевдоблагодійність, пропозиції оренди неіснуючого житла, несправжні пасажирські перевезення	70 %
	створення та забезпечення діяльності фіктивних фінансових бірж	6 %
3.	**Предмет шахрайства, учиненого в кіберпросторі**	
	майно (рухоме та нерухоме)	18 %
	право на майно	4 %
	кошти	72 %
	інформація	6 %
4.	**Джерела електронних (цифрових) слідів вчинення шахрайства у кіберпросторі** *(є декілька варіантів одночасно)*	

	електронні пристрої	100 %
	носії електронних даних	48 %
	електронні дані в інформаційних та комунікаційних системах	64 %
	електронні дані в комерційних системах	46 %
	мережеві маршрутизатори	22 %
	системи відеоспостереження	26 %
	продукти програмного забезпечення	14 %
5.	**Досудове розслідування проводилось**	
	одноособово слідчим	78 %
	слідчою групою	14 %
	слідчо-оперативною групою	8 %
6.	**Інформація, що містилась у матеріалах кримінального провадження на початковому етапі розслідування**	
	відповідала дійсності	18 %
	частково відповідала дійсності (за окремими елементами події або епізодами злочинної діяльності)	76 %
	не відповідала дійсності	6 %
7.	**У матеріалах кримінального провадження інформація про причини та умови вчинення шахрайств у кіберпросторі**	
	установлена, зафіксована в процесуальних документах	50 %
	установлена та зафіксована в процесуальних документах частково	10 %
	не була установлена та зафіксована в процесуальних документах	40 %
8.	**Види експертиз, які призначалися під час розслідування шахрайств, учинених в кіберпросторі**	
	експертиза комп'ютерної техніки і програмних продуктів (комп'ютерно-технічна експертиза)	100 %
	експертиза телекомунікаційних систем і засобів	64 %
	технічна експертиза документів	26 %
	дактилоскопічна експертиза стосовно вилучених слідів рук з різних предметів	14 %
	експертиза матеріалів і засобів звукозапису стосовно записів дій та переговорів злочинця, а також щодо технічних засобів знімання й фіксації такої інформації	46 %
	судово-психіатрична експертиза	2 %
	судово-наркологічна експертиза	0 %

ГЛОСАРІЙ

Адреса мережі Інтернет – визначений чинними в мережі Інтернет міжнародними стандартами символьний та/або цифровий ідентифікатор.

Адресний простір мережі Інтернет – сукупність адрес мережі Інтернет.

Безпека мереж і послуг – здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються передаються чи обробляються, та пов'язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги.

Близькі родичі та члени сім'ї – чоловік, дружина, батько, мати, вітчим, мачуха, син, дочка, пасинок, падчерка, рідний брат, рідна сестра, дід, баба, прадід, прабаба, внук, внучка, правнук, правнучка, усиновлювач чи усиновлений, опікун чи піклувальник, особа, яка перебуває під опікою або піклуванням, а також особи, які спільно проживають, пов'язані спільним побутом і мають взаємні права та обов'язки, у тому числі особи, які спільно проживають, але не перебувають у шлюбі.

Блокування інформації в системі – дії, внаслідок яких унеможливлюється доступ до інформації в системі.

Вебсайт – сукупність програмних засобів, розмішених за унікальною адресою в обчислювальній мережі, у тому числі в мережі Інтернет, разом з інформаційними ресурсами, що перебувають у розпорядженні певних суб'єктів і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інших інформаційних послуг через обчислювальну мережу.

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

Віртуальна електронна комунікаційна мережа – електронна комунікаційна мережа оператора, призначення для надання власних електронних комунікаційних послуг, що функціонує на умовах договору користування

електронною комунікаційною мережею або її окремими складовими іншого оператора.

Вішинг – вид телефонного шахрайства, спрямованого на отримання конфіденційної інформації стосовно реквізитів банківських карток або інших даних, примушення до переказу коштів на картку злочинця.

Дані – інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки, технічними та програмними засобами.

Дезадаптований тип злочинця – особи, які вчиняють шахрайство у кіберпросторі для сталого злочинного доходу (що є основним чи єдиним джерелом).

Документ – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

Домен – частина ієрархічного адресного простору мережі Інтернет, що має унікальну назву (доменне ім'я), що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється.

Доступ до інформації в системі – отримання користувачем можливості обробляти інформацію в системі.

Егоїстичний тип злочинця – особи, які вчиняють шахрайство у кіберпросторі, внаслідок власного низького морально-культурного розвитку та антигромадських рис характеру (нахабність, зухвалість, заздрість, егоїзм), ігноруючи законні приписи недоторканності чужого майна.

Електронна ідентифікація – процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичних особи.

Електронна комунікаційна мережа – комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг.

Електронна комунікаційна послуга – послуга, що полягає в прийманні та/або передачі інформації через електронні комунікаційні мережі, крім послуг

з редакційним контролем змісту інформації, що передається за допомогою електронних комунікаційних мереж і послуг.

Електронна комунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Електронна комунікація (телекомунікація, електрозв'язок) – передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій.

Електронна послуга – будь-яка послуга, що надається через інформаційно-комунікаційну систему.

Електронна обчислювальна техніка (ЕОТ) – комплекс електронних технічних засобів, побудованих на основі мікропроцесорів і призначених для автоматичної обробки інформації при вирішенні обчислювальних та інформаційних завдань.

Електронна обчислювальна машина (ЕОМ) – програмно-керований пристрій для обробки інформації.

Електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис.

Електронні дані – будь-яка інформацій в електронній формі.

Електронні інформаційні ресурси – будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів.

Засіб електронної ідентифікації – носій інформації, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг.

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Зловживання довірою – недобросовісне використання довіри.

Ідентифікаційні дані особи – унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи.

Ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи.

Індикатори кіберзагроз – показними (технічні дані), що використовуються для виявлення та реагування на кіберзагрози.

Інтернет (мережа Інтернет) – глобальна електронна комунікаційна мережа, що призначена для передачі даних та складається з фізично та логічно взаємоз'єднаних окремих електронних комунікаційних мереж, взаємодія яких базується на використанні єдиного адресного простору та на використанні інтернет-протоколів, визначених міжнародними стандартами.

Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Інцидент кібербезпеки (кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного,

помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Кардинг – вид шахрайства дій, при яких здійснюється операція з допомогою платіжної картки чи її реквізитів, не ініційованої чи не підтвердженої її власником.

Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів.

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Кіберзлочинність – сукупність кіберзлочинів.

Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

Кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням.

Комп'ютерний злочин (кіберзлочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Компетенція злочинця, який вчиняє шахрайство у кіберпросторі – певний рівень знань, умінь та навичок використання психологічних методів впливу, враховуючи потенційний інтерес – досягнення бажаного результату.

Комунікаційна система (системи електронних комунікацій) – система передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.

Корисливий тип злочинця – особи, які вчиняють шахрайство у кіберпросторі для досягнення своїх особистих жадібних цілей.

Користувач інформації в системі – фізична або юридична особа, яка в установленому законодавством порядку отримали право доступу до інформації в системі.

Кримінальне правопорушення – суспільно небезпечне винне діяння (дія або бездіяльність) передбачене Кримінальним кодексом України, вчинене суб'єктом кримінального правопорушення.

Криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Мета OSINT – збір релевантної інформації для подальшого аналізу і прийняття рішень.

Мобільний зв'язок – електронні комунікації із застосуванням радіотехнологій, під час яких кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах усіх пунктів закінчення електронної комунікаційної мережі.

Національна телекомунікаційна мережа – сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захист національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам.

Несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Обман – повідомлення неправдивих відомостей або приховування певних обставин.

Обробка інформації в системі – використання однієї або кількох операцій, збирання, введення, записування, перетворення, зчитування,

зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Оперативно-розшукова характеристика – система взаємопов'язаних кримінально-правових, кримінологічних та криміналістичних ознак досліджуваного злочину.

Організація – діяльність, що спрямована на створення структурного порядку об'єкта.

Організація розкриття шахрайств, учинених в кіберпросторі – типова модель, що включає аналіз первинної інформації щодо обставин злочину, формулювання версій, визначення цілей та розробку плану.

Open Source Intelligence (OSINT) – процес збору, аналізу і використання інформації, яка відкрито доступна.

Платіжна установа – це юридична особа (крім банку, фінансової установи, що має право надання платіжних послуг, оператора поштового зв'язку, органу державної влади, органу місцевого самоврядування), яка в установленому порядку отримала право на надання всіх або окремих фінансових платіжних послуг (крім платіжної послуги з випуску та використання платіжних операцій з електронними грошима).

Побутовий тип злочинця – особи, які вчиняють шахрайство у кіберпросторі для забезпечення потреб свого оточення.

Порядок доступу до інформації в системі – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації.

Послуга доступу до мережі Інтернет – електронна комунікаційна послуга, що забезпечує доступ до мережі Інтернет і можливість логічного з'єднання з кінцевими точками мережі Інтернет незалежно від технології, що застосовується в електронній комунікаційній мережі, і кінцевого (термінального) обладнання, що використовується.

Самоствердений тип злочинця – особи, які вчиняють шахрайство у кіберпросторі для самоствердження, як для себе, так і в очах інших осіб.

Сніферінг – вид шахрайства, спрямований на захоплення та розбору мережевого трафіку.

Спам – електронні, текстові та/або мультимедійні повідомлення, що без попередньої згоди (замовлення) користувачів неодноразово (більше п'яти повідомлень одному абоненту) надсилаються на їхні адреси електронної пошти або кінцеве (термінальне) обладнання, крім повідомлень постачальника електронних комунікаційних послуг щодо надання ним електронних комунікаційних послуг або повідомлень від органів державної влади чи органів місцевого самоврядування з питань, що належать до їх повноважень.

Спеціальні знання – наукові, технічні та інші професійні знання, отримані в результаті навчання, а також навички, надбані у процесі роботи в окремих галузях практичної діяльності, які використовуються разом із застосуванням науково-технічних засобів при збиранні та дослідженні слідів злочинів з метою отримання доказової та орієнтуючої інформації, необхідної для розслідування злочинів.

Судова експертиза – один з видів процесуальної форми використання спеціальних знань при розслідуванні кримінальних правопорушень, значення якого у встановленні тих чи інших фактичних даних.

Технічна система (система управління технологічними процесами) – автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами незалежно від наявності доступу системи до мереж Інтернет та/або інших глобальних мереж передачі даних.

Транзит трафіка – процес встановлення та підтримки електронною комунікаційною мережею фізичних та/або логічних з'єднань з метою проходження трафіка між двома іншими електронними комунікаційними мережами.

Трафік – сукупність інформаційних сигналів, що передаються електронною комунікаційною мережею за визначений інтервал часу, у тому числі інформаційні дані споживача та/або службова інформація.

Фішинг – вид шахрайства, що вчиняється з використанням соціальної інженерії. Полягає в імітуванні діяльності реально існуючих компаній або банків-емітентів, використовуючи неголосові засоби комунікації.

Шахрайство – заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою.

Шахрайство, учинене у кіберпросторі – суспільно небезпечне діяння, спрямоване на заволодіння чужим майном або придбання права на майно шляхом незаконних операцій з використанням електронно-обчислювальної техніки у віртуальному просторі (середовищі), де надається можливість комунікацій та/або реалізації суспільних відносин.

Information about the authors

Artem Viktorovych Shevchyshen – Deputy Head of the Main Investigation Department of the National Police of Ukraine - Head of the Department of Work Organization and Methodological Support, Doctor of Law, Professor, Honored Lawyer of Ukraine, Police Colonel.

Maxim Yuriiovych Romanov – Deputy Head of the Department of Organization of Scientific Activity and Innovation - Head of the Organizational and Scientific Department of the Department of Education, Science, and Sports of the Ministry of Internal Affairs of Ukraine, PhD in Law, Police Major.

Artur Olehovych Voloboiev – Head of the Department of Operational Investigation and Information Security of the Faculty of Specialist Training for Criminal Police Units of the Donetsk State University of Internal Affairs, PhD in Law.

Olha Mykolaivna Lunhol – Associate Professor of the Department of Operative and Investigative Activities and Information Security of the Faculty of Specialist Training for Criminal Police Units of the Donetsk State University of Internal Affairs, PhD in Pedagogy.

Olha Andriivna Haborets – Associate Professor of the Department of Operative and Investigative Activities and Information Security of the Faculty of Specialist Training for Criminal Police Units of the Donetsk State University of Internal Affairs, PhD in Pedagogy.

Serhii Victorovych Holovkin – Associate Professor of the Department of Police Activities of the E. O. Didorenko Luhansk Educational and Scientific Institute of the Donetsk State University of Internal Affairs, PhD in Law, Associate Professor.

Для нотаток

Для нотаток

Для нотаток

Наукове видання

***Шевчишен** Артем Вікторович; **Романов** Максим Юрійович;
Волобоєв Артур Олегович; **Лунгол** Ольга Миколаївна;
Габорець Ольга Андріївна; **Головкін** Сергій Вікторович*

ОРГАНІЗАЦІЯ РОЗКРИТТЯ ШАХРАЙСТВ, УЧИНЕНИХ В КІБЕРПРОСТОРІ

Монографія

*Під загальною редакцією
доктора юридичних наук, професора,
Заслуженого юриста України, полковника поліції
Вітвіцького С. С.*

Відповідальний за випуск О. В. Діордійчук
Комп'ютерна верстка Д. М. Алексєєв

Підписано до друку 04.12.2023 р. Формат 60 x 84 $^{1}/_{16}$.
Папір офсетний. Гарнітура «Times New Roman».
Друк офсетний. Умовн.-друк. арк. 11,63.

Видавництво «Алерта»
04210, м. Київ, а/с 112.
Тел.: (044) 223-15-25; (099) 607-97-62.
E-mail: alerta@ukr.net, веб-сайт: alerta.kiev.ua
Свідоцтво суб'єкта видавничої справи ДК № 788 від 29.01.2002 р.