ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ШАХРАЙСТВА У КІБЕРПРОСТОРІ

ЛІСІН Сергій Олександрович - заступник начальника сектору кримінальної поліції відділу поліції № 1 Вінницького районного управління поліції Головного управління Національної поліції у Вінницькій області.

УДК 343.985:343.72:004
DOI: https://doi.org/10.71404/EP.2021.2.40

У статті здійснено комплексне дослідження особливостей розслідування шахрайства у кіберпросторі як складного різновиду кримінально протиправної діяльності, у межах якої традиційне введення в оману поєднується з використанням цифрових технологій, електронних комунікацій, платіжних сервісів, мережевої інфраструктури та засобів приховування особи правопорушника. Обґрунтовано, що кіберпростір має розглядатися не лише як технічне середовище вчинення злочину, а як специфічна криміналістична обстановка, у якій формуються особливі електронні сліди, виникають складні зв'язки між потерпілим, правопорушником, цифровими платформами, фінансовими інструментами, провайдерами та інформаційною інфраструктурою. Визначено, що розслідування такого шахрайства потребує не ізольованого застосування окремих слідчих дій, а побудови цілісної моделі, у якій криміналістична методика, цифрова форензика, процесуальне доказування, інформаційна безпека та міжнародна взаємодія функціонують як взаємопов'язані елементи єдиної системи. Розкрито значення криміналістичної методики для планування розслідування, формування типових версій, аналізу способу введення потерпілого в оману, встановлення використаних платформ, каналів комунікації, платіжних маршрутів, ролі посередників і повторюваних шахрайських сценаріїв. Охарактеризовано цифрову форензику як інструментально-аналітичний блок, спрямований на виявлення, збереження, вилучення, перевірку цілісності та інтерпретацію електронних доказів. Наголошено, що процесуальне доказування надає цифровій інформації юридичної сили лише за умови належного документування її походження, автентичності, незмінності та зв'язку з конкретним суб'єктом. Доведено значення інформаційної безпеки для збереження матеріалів кримінального провадження та міжнародної взаємодії для отримання даних у справах із транскордонним цифровим елементом. Сформульовано перспективи досліджень, пов'язані з удосконаленням режимів електронних доказів, аналізом цифрових схем обману та методикою ідентифікації правопорушника.

Ключові слова. кіберпростір, шахрайство, розслідування, цифрові докази, цифрова форензика, криміналістична методика, інформаційна безпека.

Постановка

Шахрайство у кіберпросторі є однією з найбільш динамічних форм злочинної діяльності, оскільки поєднує корисливу спрямованість із технологічними механізмами приховування особи, джерел комунікації, фінансових потоків і цифрових слідів. Його специфіка полягає не лише у використанні комп'ютерних систем, мереж, електронних платіжних інструментів, соціальних платформ чи фішингових ресурсів, а й у транснаціональному характері злочинної взаємодії, коли потерпілий, виконавець, серверна інфраструктура, платіжний посередник і цифрові докази можуть перебувати в різних юрисдикціях. Унаслідок цього розслідування кіберпросторового шахрайства потре-

бує не механічного перенесення класичних криміналістичних методик у цифрове середовище, а формування спеціального підходу, орієнтованого на швидке збереження електронних доказів, встановлення ланцюга цифрових подій, аналіз технічних артефактів і координацію між правоохоронними органами, провайдерами, банківськими установами та суб'єктами кібербезпеки.

На наше переконання, актуальність піднятої в цій статті теми зумовлена тим, що кіберпростір трансформувався у самостійне середовище злочинної діяльності, де шахрайські схеми швидко адаптуються до змін цифрової поведінки населення, розвитку електронної комерції, дистанційного банкінгу, криптовалютних розрахунків і соціальної інженерії. Досліджуючи роботу слідчих, які спеціалізуються на розслідуванні кіберзлочинах, М. Ноух, Дж. Р. К. Нерс, Г. Вебб та М. Голдсміт зазначають, що окрім технічних труднощів, суттєвий деструктивний вплив мають соціально-організаційні чинники: брак зручних інструментів, складність робочих процесів, проблеми міжвідомчої взаємодії та висока адаптивність правопорушників [1]. Це засвідчує, що ефективне розслідування шахрайства у кіберпросторі залежить від здатності слідства поєднувати криміналістичну логіку, цифрову форензику, аналітику великих масивів даних і правову оцінку електронних доказів.

У зв'язку з цим дослідження особливостей розслідування зазначеного виду шахрайства зумовлене потребою систематизації способів виявлення, фіксації, вилучення, перевірки та процесуального використання цифрових доказів із дотриманням їх цілісності, автентичності й доказової придатності. Зокрема, А. Дімітріадіс та інші акцентують увагу на потребі впорядкованих моделей аналізу цифрових даних у справах про кіберзлочини та кіберфрод, що особливо важливо для реконструкції події, встановлення ролей учасників і відстеження електронних транзакцій [2]. Саме тому розслідування шахрайства у кіберпросторі має розглядатися як комплексна криміналістична проблема, у межах якої технічні засоби, процесуальні гарантії, міжнародне співробітництво та аналітична робота утворюють єдину систему доказування.

Огляд останніх наукових розвідок

Українська криміналістична думка поступово перейшла від загального осмислення кіберзлочинності до формування спеціалізованих методичних підходів, орієнтованих на цифрове середовище, електронні сліди, транснаціональний характер злочинної діяльності та доказову специфіку інформації, що існує в електронній формі. Проблематика кіберпросторового шахрайства розглядалася не ізольовано, а в ширшому контексті криміналістичної характеристики злочинів, учинених із використанням комп'ютерних систем, мережевої інфраструктури, електронних комунікацій і цифрових сервісів. Зважаючи на це, науковий доробок О. Самойленко, Г. Муляр, О. Ховпуна, Я. Неділько, Н. Ахтирської, Я. Найдьон, Г. Чернишова, І. Каланчі та А. Столітнього становить вагоме теоретичне підґрунтя для аналізу шахрайства у кіберпросторі як складного різновиду злочинів проти власності, де спосіб посягання є невіддільним від цифрового середовища його реалізації.

Концептуальне значення для окресленої проблематики має обґрунтована О. Самойленко криміналістична методика розслідування злочинів, учинених із використанням обстановки кіберпростору. Зокрема, дослідниця зміщує акцент із вузького розуміння комп'ютера як технічного засобу злочину на ширше бачення кіберпростору як особливої обстановки кримінального правопорушення, що має принципове значення для розслідування шахрайства, оскільки шахрайська схема в мережевому середовищі охоплює не лише обман потерпілого, а й цифрову комунікацію, використання платіжних інструментів, реєстраційних даних, IP-адрес, облікових записів, серверної інфраструктури та електронних повідомлень. Такий підхід формує підстави для розгляду кіберпросторового шахрайства як криміналістично специфічного явища, де спосіб вчинення, слідова картина й механізм доказування мають самостійні цифрові ознаки [3].

Подальший розвиток окресленої позиції простежується також в іншому дослідженні

О. Самойленко, присвяченому основам методики розслідування злочинів, учинених у кіберпросторі, значущість якого полягає в систематизації розслідування кіберзлочинів як окремого напряму криміналістичної методики, а не як допоміжного різновиду традиційного розслідування [4]. Для теми шахрайства наведене означає необхідність поєднання класичних елементів доказування, зокрема події кримінального правопорушення, способу обману, причинного зв'язку, розміру шкоди, вини особи, із технічною реконструкцією цифрового маршруту злочинної активності. У цьому контексті предмет доказування кіберзлочинів ускладнюється, оскільки слідство має установити не тільки факт заволодіння майном або правом на майно, а й цифровий механізм впливу на потерпілого, джерело комунікації, інструменти маскування та зв'язок конкретної особи з електронними діями.

Виклад основного матеріалу

У наукові літературі окремі вчені, приміром Г. Муляр та О. Ховпун, акцентують увагу на особливостях доказування кіберзлочинів, що безпосередньо пов'язано з проблемою розслідування кіберпросторового шахрайства [5]. Зокрема, дослідники зосереджують увагу не лише на виявленні цифрової інформації, а й на її процесуальній придатності. Наприклад, у справах про шахрайство в мережі слідчий часто працює з електронним листуванням, даними акаунтів, інформацією провайдерів, банківськими транзакціями, історією входів, технічними журналами та файлами, які швидко змінюються або зникають. За таких умов доказування набуває підвищеної складності: недостатньо виявити цифровий слід, необхідно забезпечити його цілісність, належність, допустимість і зв'язок із конкретною шахрайською дією.

Важливе теоретико-практичне значення має проведений Я. Найдьоном аналіз віртуальних слідів як самостійної криміналістичної категорії [6]. У контексті кіберпросторового шахрайства такі сліди становлять не периферійний, а центральний елемент доказової системи, оскільки фіксують комунікацію між правопорушником і потерпілим, технічні параметри доступу, створення фіктивних сторінок, використання електронних адрес, месенджерів та платіжних сервісів. Цей підхід дає змогу чітко розмежувати матеріальні, ідеальні та віртуальні сліди, що безпосередньо оптимізує процеси планування огляду електронних носіїв, вилучення цифрової інформації, призначення експертиз і побудови слідчих версій.

Поняття кіберзлочинів, їх класифікація, обстановка та слідова картина, розроблені Я. Нєдільком, становлять основу для формування сучасної криміналістичної характеристики правопорушень у цифровій сфері [7–9]. Зміст цього поняття інтегрує в собі й специфічні ознаки суб'єкта злочину: за відсутності фізичного контакту з потерпілим його особа реконструюється через аналіз способів комунікації, вибору платформи, характеру легенди та використання посередників. У такий спосіб праці дослідника трансформують підходи до розуміння кіберзлочину, зміщуючи вектор уваги із суто зовнішніх ознак на структуровану поведінку особи в цифровому середовищі.

Посилення особистісного аспекту в дослідженнях криміналістичної характеристики особи кіберзлочинця, запропоноване Н. Ахтирською та Я. Нєдільком, має вагоме доказове значення [10]. Це зумовлено тим, що правопорушник нерідко діє під вигаданою ідентичністю, використовує технічні засоби анонімізації, фальшиві профілі, чужі банківські реквізити або проміжні акаунти. За таких умов класичні прийоми встановлення особи потребують доповнення цифровим аналізом: зіставленням технічних даних, поведінкових патернів, часу активності, стилістики повідомлень, фінансових зв'язків і повторюваності шахрайських сценаріїв. Зазначений підхід свідчить про поступовий перехід української науки від описового аналізу кіберзлочинності до побудови криміналістично придатних моделей ідентифікації суб'єкта.

Розуміння кіберзлочинності як глобалізаційного виклику та загрози світовій безпеці представлено у дослідженні Г. Чернишова [11]. Автор робить особливий акцент на транснаціональності, мережевій природі та високій адаптивності сучасних кіберзлочин-

них практик. Дослідник зазначає, що шахрайство в цифровому середовищі часто виходить за межі однієї держави: потерпілий може перебувати в Україні, платіжна операція – проходити через іноземний сервіс, сервер – розміщуватися в іншій юрисдикції, а виконавець – використовувати проміжну технічну інфраструктуру. У зв'язку з цим розслідування зазначених діянь не зводиться до локального збору доказів, а потребує міжнародної правової взаємодії, швидкого збереження даних і належної координації між правоохоронними та приватними суб'єктами цифрової інфраструктури.

Питання інформаційної безпеки електронного кримінального провадження, які мають виняткове значення для оптимізації розслідування шахрайства у кіберпросторі, ґрунтовно висвітлено у працях І. Каланчі [12]. У таких провадженнях цифрові докази не тільки збираються з електронних джерел, а й надалі зберігаються, передаються, аналізуються та використовуються в межах кримінального процесу. Внаслідок цього питання захисту процесуальної інформації, цілісності електронних матеріалів, контролю доступу, фіксації дій із доказами та надійності інформаційно-телекомунікаційних систем набувають методологічного значення. Без належної інформаційної безпеки доказова основа справи про кіберпросторове шахрайство може втратити переконливість через сумніви щодо незмінності, походження або процесуального режиму цифрових даних.

Потреба в організаційній модернізації слідчої діяльності зумовлює розвиток ідеї інформаційно-телекомунікаційної системи органу досудового розслідування, яку активно розробляють А. Столітній та І. Каланча [13]. Ефективність провадження у справах про кібершахрайство залежить не лише від професіоналізму окремого слідчого, а й від цифрової інфраструктури відомства загалом: оперативності доступу до реєстрів, автоматизації обміну інформацією, надійності фіксації процесуальних дій, взаємодії з експертами та швидкості обробки великих масивів даних. Узагальнення наведених положень свідчить, що розслідування шахрайства у кіберпросторі потребує комплексної моделі, у якій криміналістична методика, цифрова форензика, процесуальне доказування, інформаційна безпека та міжнародна взаємодія становлять єдину систему.

Комплексна модель розслідування шахрайства у кіберпросторі має ґрунтуватися на інтеграції криміналістичної методики, цифрової форензики, процесуального доказування, інформаційної безпеки та міжнародної взаємодії в єдину функціональну систему. Її основою є розуміння кіберпростору не лише як технічного середовища вчинення злочину, а як специфічної криміналістичної обстановки, у якій формуються особливі цифрові сліди, виникають складні зв'язки між суб'єктами, платформами, електронними сервісами, фінансовими інструментами та інформаційною інфраструктурою, тобто, розслідування не може обмежуватися встановленням факту обману і заподіяної шкоди, оскільки потребує реконструкції повного цифрового механізму злочинної діяльності, а саме, від першого контакту з потерпілим до руху коштів, маскування особи правопорушника та використання технічних засобів приховування.

У межах пропонованої моделі криміналістична методика виконує системоутворювальну роль, оскільки визначає логіку планування розслідування, побудови версій, вибору слідчих дій, встановлення типових способів учинення шахрайства та аналізу слідової картини. Зокрема, для кіберпросторового шахрайства особливе значення мають типові версії щодо джерела комунікації, способу введення потерпілого в оману, використаних електронних ресурсів, каналів переказу коштів, ролі посередників, повторюваності шахрайської схеми та зв'язку конкретної особи з цифровими діями. Разом із цим методика має спрямовувати слідство не лише на фіксацію окремих доказів, а й на встановлення стійких закономірностей злочинної поведінки, які відображаються у технічних даних, фінансових операціях, поведінкових патернах і комунікаційних слідах.

Цифрова форензика в запропонованій моделі є інструментально-аналітичним блоком, що забезпечує виявлення, збереження, вилучення, дослідження та інтерпретацію електронних доказів. Її значення полягає у

тому, що цифрові сліди мають нестабільний, змінний і часто розподілений характер: вони можуть міститися на мобільних пристроях, комп'ютерах, серверах, у хмарних сервісах, банківських системах, месенджерах, соціальних мережах, журналах доступу та платіжних платформах. Відповідно форензичний компонент має охоплювати не тільки технічне копіювання інформації, а й перевірку її цілісності, встановлення часу створення та зміни даних, виявлення зв'язків між обліковими записами, IP-адресами, пристроями, транзакціями й електронними повідомленнями. Без такого інструментально-аналітичного блоку цифрова інформація залишається фрагментарною і не формує переконливої доказової бази.

Процесуальне доказування є нормативною основою моделі, оскільки саме воно перетворює технічно виявлену цифрову інформацію на належні, допустимі, достовірні та достатні докази. Зокрема, у справах про шахрайство у кіберпросторі ключовим є дотримання процесуального порядку отримання електронних даних, фіксація джерела їх походження, документування всіх дій із цифровими носіями, забезпечення безперервності ланцюга збереження доказів і підтвердження зв'язку між електронною дією та конкретним суб'єктом. Водночас процесуальний блок моделі також має враховувати ризики оскарження електронних доказів через сумніви щодо їх автентичності, повноти, незмінності або способу отримання. Тому доказування повинно спиратися на поєднання технічних висновків, показань потерпілих, даних фінансових установ, інформації провайдерів, результатів експертиз і логічної реконструкції події.

Інформаційна безпека та міжнародна взаємодія завершують комплексну модель, надаючи їй організаційної стійкості й практичної придатності в умовах транснаціональної кіберзлочинності. Інформаційна безпека охоплює захист електронних матеріалів кримінального провадження, контроль доступу до них, запобігання втраті або зміні цифрових доказів, а також надійність інформаційних систем органів досудового розслідування. Міжнародна взаємодія набуває особливого значення тоді, коли сервери, платіжні посередники, провайдери, доменні реєстратори або учасники шахрайської схеми перебувають за межами України.

Результати проведеного аналізу дають підстави констатувати, що ефективна модель розслідування кібершахрайства має бути побудована як цілісна система. У ній криміналістична логіка визначає напрям розслідування, цифрова форензика забезпечує технічну основу доказування, процесуальні механізми надають матеріалам юридичної сили, інформаційна безпека гарантує їх збереження, а міжнародна взаємодія розширює можливості встановлення істини у справах із транскордонним цифровим елементом.

Висновки

У результаті проведеного дослідження встановлено, що шахрайство у кіберпросторі є складним різновидом кримінально протиправної діяльності, у межах якої традиційний обман поєднується з використанням цифрових технологій, електронних комунікацій, платіжних сервісів, мережевої інфраструктури та механізмів приховування особи правопорушника. Розслідування таких діянь не може зводитися лише до фіксації факту заволодіння майном або коштами, оскільки доказове значення має повна реконструкція цифрового механізму злочину: встановлення джерела комунікації, способу впливу на потерпілого, маршруту руху коштів, використаних облікових записів, технічних засобів маскування, електронних слідів і зв'язку конкретної особи з відповідними цифровими діями.

Криміналістична методика розслідування шахрайства у кіберпросторі має формуватися як спеціалізована система, орієнтована на особливу обстановку вчинення злочину, цифрову слідову картину, типові шахрайські сценарії, поведінкові патерни правопорушника та підвищену складність його ідентифікації. Своєю чергою, цифрова форензика становить необхідний інструментально-аналітичний компонент розслідування, оскільки забезпечує виявлення, збереження, вилучення, дослідження та інтерпретацію електронних доказів. Особливого значення набувають перевірка ці-

лісності цифрових даних, фіксація джерела їх походження, встановлення часу створення та зміни інформації, аналіз зв'язків між пристроями, IP-адресами, обліковими записами, транзакціями, електронними повідомленнями й технічними журналами. Поряд із цим процесуальне доказування перетворює технічно виявлену інформацію на належні, допустимі, достовірні та достатні докази лише за умови належного документування, збереження ланцюга доказів, підтвердження автентичності даних і встановлення їх зв'язку з конкретним суб'єктом.

Отже, ефективне розслідування шахрайства у кіберпросторі потребує комплексної моделі, у якій криміналістична методика визначає напрям розслідування, цифрова форензика формує технічну основу доказування, процесуальні механізми надають доказам юридичної сили, інформаційна безпека гарантує їх збереження, а міжнародна взаємодія забезпечує отримання даних у справах із транскордонним цифровим елементом.

Перспективним напрямом подальших наукових розвідок є поглиблення криміналістичної характеристики шахрайства у кіберпросторі з урахуванням нових способів цифрового обману, зокрема фішингових схем, шахрайства в соціальних мережах і месенджерах, маніпуляцій із криптовалютними активами, використання фіктивних онлайн-магазинів, підроблених платіжних сторінок, deepfake-технологій та автоматизованих бот-мереж. Особливої уваги потребує дослідження типових цифрових слідів, які виникають під час реалізації таких схем, закономірностей їх формування, збереження, зміни та втрати. Подальшого розвитку також потребує методика ідентифікації особи правопорушника в умовах анонімізації, використання фальшивих профілів, VPN-сервісів, криптовалютних гаманців, підставних банківських рахунків і розподіленої технічної інфраструктури.

Окремої уваги потребує вдосконалення процесуального режиму електронних доказів, зокрема критеріїв їх належності, допустимості, достовірності та достатності у справах про кіберпросторове шахрайство. Доцільним є подальше дослідження процедур збереження електронних даних, фіксації ланцюга їх зберігання, взаємодії з провайдерами, фінансовими установами, адміністраторами платформ і власниками інформаційних систем. Перспективним також є поглиблення досліджень міжнародної взаємодії у справах, де сервери, платіжні сервіси, доменні реєстратори або учасники шахрайської схеми перебувають за межами України. Саме ці напрями формують наукову основу для створення цілісної, практично орієнтованої та технологічно адаптивної методики розслідування шахрайства у кіберпросторі.

Література

1. Nouh M., Nurse J. R. C., Webb H., Goldsmith M. Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement. Proceedings of the 2019 Workshop on Usable Security (USEC), Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 24 February 2019. 11 p. DOI: https://doi.org/10.14722/usec.2019.23032.

2. Dimitriadis A., Ivezic N., Kulvatunyou B., Mavridis I. D4I – Digital forensics framework for reviewing and investigating cyber attacks. *Array*. 2020. Vol. 5. 100015. DOI: https://doi.org/10.1016/j.array.2019.100015.

3. Самойленко О. А. Концепція криміналістичної методики розслідування злочинів, вчинених із використанням обстановки кіберпростору. *Право та державне управління*. 2018. № 1 (30). Т. 1. С. 208–213.

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

5. Муляр Г. В., Ховпун О. С. Особливості доказування кіберзлочинів. *Право. Людина. Довкілля*. 2019. Т. 10. № 3. С. 132–138.

6. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право*. 2019. № 5. С. 304–307. DOI: https://doi.org/10.32849/2663-5313/2019.5.56.

7. Неділько Я. В. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України*. 2018. № 4. С. 49–60.

8. Неділько Я. В. Обстановка та «слідова картина» як елементи криміналістичної характеристики кіберзлочинів. *Підприємництво, господарство і право*. 2020. № 7. С. 359–364. DOI: https://doi.org/10.32849/2663-5313/2020.7.61.

9. Неділько Я. В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право. Серія: Юридичні і політичні науки*. 2020. Вип. 88. С. 202–212.

10. Ахтирська Н. М., Неділько Я. В. Криміналістична характеристика: особа кіберзлочинця. *Юридичний науковий електронний журнал*. 2019. № 1. С. 171–174.

11. Чернишов Г. М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. *Прикарпатський юридичний вісник*. 2018. № 3. С. 158–162.

12. Каланча І. Г. Інформаційна безпека електронного кримінального провадження України. *Науковий часопис Національної академії прокуратури України*. 2018. № 3. С. 11–22.

13. Столітній А. В., Каланча І. Г. Концепція інформаційно-телекомунікаційної системи органу досудового розслідування. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 2 (18). С. 14–23. DOI: https://doi.org/10.33270/04191802.14.

Serhii Lisin,
Deputy Head of the Criminal Unit of Police, Police Division No. 1 of Vinnytskyi District Headquarters of the Main Department of the National Police in Vinnitska Region

FEATURES OF INVESTIGATING FRAUD IN CYBERSPACE

The article presents a comprehensive study of the features of investigating fraud in cyberspace as a complex type of criminally unlawful activity, within which traditional deception is combined with the use of digital technologies, electronic communications, payment services, network infrastructure and means of concealing the identity of the offender. It is substantiated that cyberspace should be considered not only as a technical environment for committing a crime, but as a specific forensic environment in which special electronic traces are formed, complex connections arise between the victim, the offender, digital platforms, financial instruments, providers and information infrastructure. It is determined that the investigation of such fraud requires not the isolated application of individual investigative actions, but the construction of a holistic model in which forensic methodology, digital forensics, procedural evidence, information security and international interaction function as interconnected elements of a single system. The importance of forensic methodology for planning an investigation, forming typical versions, analyzing the method of misleading the victim, establishing the platforms used, communication channels, payment routes, the role of intermediaries and recurring fraudulent scenarios is revealed. Digital forensics is characterized as an instrumental and analytical unit aimed at detecting, preserving, retrieving, verifying the integrity and interpreting electronic evidence. It is emphasized that procedural evidence gives digital information legal force only if its origin, authenticity, immutability and connection with a specific subject are properly documented. The importance of information security for preserving criminal proceedings and international interaction for obtaining data in cases with a cross-border digital element is proven. Research prospects related to improving electronic evidence regimes, analyzing digital fraud schemes and methods for identifying the offender are formulated.

Keywords: cyberspace, fraud, investigation, digital evidence, digital forensics, forensic methodology, information security.