УДК 343.98
DOI https://doi.org/10.32689/2522-4603.2026.1.1

Лариса АРКУША
доктор юридичних наук, професор, завідувач кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія»,
e-mail: larisa_arkusha@ukr.net
ORCID: 0000-0002-0422-6416

Олександр ЧЕРНОВ
доктор філософії, доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія»,
e-mail: sanjehan.14@gmail.com
ORCID: 0009-0002-6038-9479

Євген ХИЖНЯК
кандидат юридичних наук, доцент, доцент кафедри криміналістики, судових експертиз та поліграфології Національного університету «Одеська юридична академія»,
e-mail: khyzhniak@onua.edu.ua
ORCID: 0000-0001-8263-0353

ДЕЯКІ ОСОБЛИВОСТІ ВИЛУЧЕННЯ ТА АВТЕНТИФІКАЦІЇ ЦИФРОВИХ ДОКАЗІВ ІЗ МОБІЛЬНИХ ПРИСТРОЇВ ПРИ РОЗСЛІДУВАННІ ФІШИНГОВИХ АТАК

У статті досліджуються окремі криміналістичні та організаційно-процесуальні аспекти вилучення і автентифікації цифрових доказів із мобільних пристроїв під час розслідування фішингових атак. Актуальність теми зумовлена стрімким зростанням кількості кіберзлочинів, у яких мобільні телефони виступають основним інструментом комунікації між злочинцем і потерпілим, засобом доступу до банківських сервісів та водночас носієм значної кількості цифрових слідів. У таких умовах мобільний пристрій стає важливим джерелом доказової інформації, що дозволяє відтворити механізм злочинної діяльності, встановити послідовність подій, ідентифікувати причетних осіб та підтвердити факт незаконного отримання конфіденційних даних або коштів. У роботі проаналізовано специфіку формування цифрових слідів у мобільному середовищі під час реалізації фішингових схем, що здійснюються через SMS-повідомлення, електронну пошту, месенджери, соціальні мережі та підроблені вебресурси. Обґрунтовується, що ефективність розслідування таких правопорушень значною мірою залежить від правильності початкових дій щодо виявлення, фіксації, вилучення та збереження даних із мобільних пристроїв.

Особливу увагу приділено технічним і криміналістичним особливостям роботи з цифровою інформацією, що зберігається у смартфонах, зокрема журналам дзвінків, листуванню у месенджерах, історії вебперегляду, системним журналам, метаданим файлів, даним банківських застосунків та іншим артефактам користувацької активності. Розкрито проблемні питання забезпечення цілісності цифрових доказів, що пов'язані з їх динамічним характером, можливістю дистанційного видалення або зміни, використанням сучасних механізмів шифрування, а також синхронізацією даних із хмарними сервісами. У статті проаналізовано сучасні підходи до вилучення даних із мобільних пристроїв, окреслено значення логічного, файлового та фізичного отримання інформації, а також підкреслено необхідність дотримання принципів збереження первісного стану цифрових даних. Окремо розглянуто питання автентифікації цифрових доказів, зокрема застосування криптографічних контрольних сум, забезпечення ланцюга збереження доказів та використання спеціальних знань у галузі цифрової криміналістики.

Зроблено висновок, що належна організація процесу вилучення та автентифікації цифрових доказів із мобільних пристроїв має визначальне значення для встановлення об'єктивних обставин фішингових атак і забезпечення допустимості доказів у кримінальному провадженні. Запропоновано узагальнений підхід до дослідження мобільних пристроїв як джерела криміналістично значущої інформації, що передбачає поєднання технічних методів цифрової криміналістики з процесуальними вимогами доказування.

Ключові слова: *розслідування, мобільні пристрої, фішинг, кіберзлочини, цифрова криміналістика, вилучення інформації, автентифікація даних, кримінальне провадження, електронні докази.*

Larysa Arkusha, Oleksandr Chernov, Yevhen Khyzhniak. SOME FEATURES OF EXTRACTING AND AUTHENTICATING DIGITAL EVIDENCE FROM MOBILE DEVICES WHEN INVESTIGATING PHISHING ATTACKS

The article examines certain criminalistic and organizational-procedural aspects of the seizure and authentication of digital evidence from mobile devices during the investigation of phishing attacks. The relevance of the topic is

due to the rapid growth in the number of cybercrimes in which mobile phones are the main tool of communication between the criminal and the victim, a means of accessing banking services, and at the same time a carrier of a significant amount of digital traces. In such conditions, a mobile device becomes an important source of evidence that allows reconstructing the mechanism of criminal activity, establishing the sequence of events, identifying the persons involved, and confirming the fact of illegal acquisition of confidential data or funds. The paper analyzes the specifics of the formation of digital traces in the mobile environment during the implementation of phishing schemes carried out via SMS messages, e-mail, messengers, social networks, and fake web resources.It is argued that the effectiveness of investigating such offenses largely depends on the correctness of the initial actions to identify, record, seize, and preserve data from mobile devices.

Particular attention is paid to the technical and forensic features of working with digital information stored on smartphones, including call logs, messenger correspondence, web browsing history, system logs, file metadata, banking application data, and other artifacts of user activity. The article reveals problematic issues of ensuring the integrity of digital evidence related to its dynamic nature, the possibility of remote deletion or modification, the use of modern encryption mechanisms, and data synchronization with cloud services. The article analyzes modern approaches to extracting data from mobile devices, outlines the importance of logical, file, and physical information retrieval, and emphasizes the need to adhere to the principles of preserving the original state of digital data. The issue of digital evidence authentication is considered separately, in particular the use of cryptographic checksums, ensuring the chain of evidence preservation, and the use of special knowledge in the field of digital forensics.

It was concluded that proper organization of the process of extraction and authentication of digital evidence from mobile devices is crucial for establishing the objective circumstances of phishing attacks and ensuring the admissibility of evidence in criminal proceedings. A generalized approach to the investigation of mobile devices as a source of criminally significant information is proposed, which involves combining technical methods of digital forensics with procedural requirements for evidence.

Key words: *investigation, mobile devices, phishing, cybercrime, digital forensics, information retrieval, data authentication, criminal proceedings, electronic evidence.*

Постановка проблеми зумовлена тим, що фішингові атаки в сучасних умовах набули стійкого, масового та технологічно адаптивного характеру, а мобільні пристрої перетворилися на ключовий вузол, через який реалізується як первинний вплив на потерпілого, так і подальше заволодіння даними та активами. Саме смартфон найчастіше виступає каналом доставки шкідливого повідомлення або посилання, середовищем введення облікових даних, отримання одноразових кодів підтвердження, доступу до мобільного банкінгу, а також носієм слідів мережевої взаємодії, які дозволяють відтворити хронологію та механізм злочинної події. Водночас цифрові докази з мобільних пристроїв відзначаються високою динамічністю, фрагментарністю та залежністю від програмно-апаратної екосистеми, що істотно ускладнює їх виявлення, вилучення, збереження та подальше використання у кримінальному провадженні.

Проблемність ситуації посилюється низкою чинників: по-перше, поширенням наскрізного шифрування, апаратно-програмних механізмів захисту доступу та хмарної синхронізації, через що доказова інформація може бути частково недоступною, швидко змінюватися або переноситися за межі пристрою; по-друге, ризиком дистанційного втручання та знищення даних, що вимагає спеціальних заходів ізоляції, але водночас породжує практичні дилеми щодо вимкнення, розблокування і режимів збереження пристрою; по-третє, багатоканальністю фішингових схем, де цифрові сліди розподіляються між SMS, месенджерами, браузерами, банківськими додатками, системними журналами та серверними логами, а їх доказова цінність виникає лише за умови правильної кореляції та верифікації. По-четверте, наявністю процесуальних ризиків, пов'язаних із недотриманням належної процедури фіксації первинного стану пристрою, створенням копій без контролю цілісності, порушенням ланцюга збереження або застосуванням технічних дій, які можуть бути розцінені як зміна даних.

Унаслідок цього в практиці досудового розслідування виникає суперечність між об'єктивною необхідністю оперативно отримати цифрові сліди, що швидко деградують або зникають, і вимогою забезпечити їх автентичність, цілісність та процесуальну допустимість. Наявні підходи до роботи з цифровими доказами не завжди враховують специфіку мобільних екосистем і фішингових сценаріїв, що призводить до втрати релевантної інформації, неповноти доказової бази, ускладнення експертного аналізу та зростання ймовірності оспорювання доказів у суді. Відтак потребує наукового та прикладного опрацювання комплекс питань, пов'язаних із формуванням узгоджених процедур вилучення і автентифікації цифрових доказів із мобільних пристроїв у провадженнях щодо розслідування фішингових атак, з урахуванням технологічних обмежень, криміналістичних завдань та процесуальних стандартів доказування.

Аналіз останніх досліджень і публікацій засвідчує, що проблематика вилучення та автентифікації цифрових доказів із мобільних пристроїв у провадженнях про фішингові атаки перебуває на перетині трьох науково-

практичних напрямів: мобільної цифрової криміналістики як техніко-методичного комплексу, стандартів забезпечення цілісності та відтворюваності доказів, а також процесуальної придатності результатів цифрових досліджень у кримінальному судочинстві. Базовий каркас сучасних підходів до мобільної криміналістики сформовано в рекомендаційних документах, що описують повний цикл роботи з мобільним пристроєм від первинних дій до звітування, з акцентом на збереження, вилучення, валідацію та документування процедур. Зокрема, настанови NIST щодо мобільної цифрової криміналістики розглядають мобільний пристрій як складний об'єкт із різнорідними джерелами артефактів та підкреслюють необхідність формалізованих процедур збереження і перевірки цілісності даних протягом усього циклу дослідження. Паралельно міжнародна стандартизація деталізує вимоги до ідентифікації, збирання, вилучення та збереження потенційних цифрових доказів як передумови їх доказової сили, що є особливо актуальним для мобільного середовища, де дані здатні змінюватися автоматично через синхронізацію, оновлення та мережеві події. У цьому контексті ISO/IEC 27037 закріплює універсальні орієнтири щодо збереження цілісності та керованості процедур при роботі з цифровими носіями, що використовується як методологічний базис для побудови локальних протоколів роботи з мобільними пристроями. Додатково, європейський вимір best practice репрезентують матеріали ENFSI, що орієнтують судово-експертну практику на стандартизовані процеси та контроль якості, зокрема в частині управління процедурами, простежуваності та належної організації робіт, що прямо корелює з вимогами до ланцюга збереження та відтворюваності результатів.

У наукових публікаціях останніх років акцент зміщується від опису інструментарію до проблем надійності, відтворюваності та процесуальної стійкості цифрових результатів. Так, дослідження з проблематики валідації та надійності цифрових криміналістичних розслідувань підкреслюють, що ключовими ризиками залишаються варіативність інструментів, різні конфігурації пристроїв, неоднорідність методик, а також недостатня формалізація процесів перевірки, що може впливати на сприйняття доказів судом. У межах такого підходу пропонуються рамкові моделі, орієнтовані на вимірювану відтворюваність, документованість і аудит процедур, що особливо важливо для мобільної криміналістики через швидку зміну версій ОС і механізмів шифрування. Окремий пласт сучасних робіт фокусується на технічних бар'єрах доступу до даних мобільних пристроїв, зокрема на наслідках повнодискового шифрування, захищених контейнерів, хмарної синхронізації та антифорензичних практик, які ускладнюють як повноту вилучення, так і подальшу інтерпретацію артефактів. Автори вказують, що методичні рішення дедалі частіше передбачають поєднання локальних даних із серверними журналами та використання процедур цифрової консервації, коли пріоритетом є не максимальна глибина доступу будь-якою ціною, а гарантована доказова якість того, що реально можна отримати законним і відтворюваним способом. Водночас на практико-орієнтованому рівні набувають поширення публікації, де пропонуються стандартизовані операційні процедури поводження з цифровими доказами з прив'язкою до міжнародних стандартів інцидент-менеджменту та поводження з доказами; такі підходи розглядають мобільний пристрій і дані з нього як компонент ширшого ланцюга реагування на кіберінцидент, що є близьким до потреб розслідування фішингових атак як багатоканальних подій.

У правничій та криміналістичній літературі регіонального рівня також простежується тенденція до проблематизації цифрових доказів як категорії, що потребує більш чітких процедурних орієнтирів і наближення до міжнародних стандартів поводження з цифровою інформацією. Зокрема, у працях, присвячених використанню цифрових доказів у кримінальному судочинстві, звертається увага на те, що навіть за наявності загальновизнаних стандартів і методичних підходів їх практична імплементація в національних процесуальних практиках залишається нерівномірною, а отже підвищується ризик спорів щодо допустимості, цілісності та достовірності цифрових даних. Разом із тим, попри значний доробок у сфері мобільної криміналістики й стандартизації роботи з цифровими доказами, спеціалізований фокус саме на фішингових атаках у мобільному середовищі часто залишається розпорошеним між дослідженнями про мобільні артефакти, банківські транзакції, соціальну інженерію та загальні питання цифрових доказів. Це обумовлює потребу у подальших прикладних узагальненнях, які б інтегрували технічні методи вилучення даних із мобільних пристроїв, вимоги до верифікації цілісності та простежуваності, а також криміналістичну реконструкцію події фішингу як послідовності цифрових взаємодій, що має бути доведена у процесуально стійкий спосіб.

Постановка завдання. Метою цієї статті є комплексний науковий аналіз особливостей вилучення та автентифікації цифрових доказів із мобільних пристроїв під час розслідування фішингових атак, а також визначення криміналістично значущих підходів до забезпечення їх цілісності, достовірності та процесуальної придатності у кримінальному провадженні. Досягнення зазначеної мети передбачає з'ясування специфіки формування цифрових слідів у мобільному середовищі при реалізації фішингових схем, узагальнення сучасних технічних і організаційних методів вилучення інформації з мобільних пристроїв, дослідження механізмів підтвердження автентичності цифрових даних, а також обґрунтування практичних рекомендацій щодо підвищення ефективності використання таких доказів у діяльності органів досудового розслідування. Особлива увага приділяється визначенню взаємозв'язку між технічними процедурами мобільної цифрової криміналістики та вимогами кримінального процесуального законодавства, що дозволяє сформувати науково обґрунтовані підходи до фіксації, збереження та оцінювання цифрових доказів у провадженнях, пов'язаних із фішинговими атаками.

Виклад основного матеріалу. Стрімка цифровізація суспільних відносин, масове використання смартфонів і залежність щоденних практик від онлайн-сервісів зумовили зростання частки кіберзлочинів, у яких мобільний пристрій виступає центральною ланкою як для вчинення протиправних дій, так і для формування доказової бази. Фішингові атаки належать до найпоширеніших способів незаконного заволодіння конфіденційною інформацією та активами: вони спрямовані на введення користувача в оману шляхом імітації легітимної комунікації від банку, державного сервісу, маркетплейсу, поштового оператора, роботодавця або навіть знайомої особи. У сучасній практиці дедалі частіше фіксується мобільно-орієнтований характер фішингу, коли контакт із жертвою відбувається через SMS, месенджери, push-сповіщення, соціальні мережі або мобільні клієнти електронної пошти, а дії з підтвердження транзакцій ідентифікації та доступу до акаунтів здійснюються саме зі смартфона. Відтак мобільні пристрої потерпілих, підозрюваних і пов'язаних осіб перетворюються на високонасичені носії цифрових слідів: повідомлення, журнали дзвінків, історії браузера, токени сесій, файли кешу, журнали авторизацій, метадані медіафайлів, артефакти мобільного банкінгу, дані двофакторної автентифікації, геолокаційні позначки, записи про мережеві з'єднання, а також синхронізовані елементи з хмарних сховищ. Саме тому вилучення та автентифікація цифрових доказів з мобільних пристроїв під час розслідування фішингових атак потребують не лише технічної вправності, а й процесуальної бездоганності, оскільки будь-які сумніви щодо цілісності походження чи достовірності даних можуть нівелювати доказове значення отриманої інформації.

Цифрові докази, на відміну від традиційних матеріальних слідів, характеризуються нематеріальною природою, залежністю від програмно-апаратного середовища і високою мінливістю. Вони легко копіюються, можуть бути модифіковані внаслідок автоматичних процесів операційної системи, роботи додатків, оновлень, синхронізації або резервного копіювання. На мобільних платформах додатковою складністю є відсутність єдиного місця зберігання інформації, оскільки дані розподіляються між локальною пам'яттю пристрою, зовнішніми картами, віртуальними контейнерами додатків, а також хмарними сервісами, що підтримують синхронізацію в реальному часі. У фішингових схемах зловмисники використовують короткоживучі посилання, динамічні домени, редиректи, одноразові сторінки з підробленими формами, а також тимчасові акаунти й віртуальні номери [1]. Тому доказова інформація на мобільному пристрої нерідко існує як фрагментарний набір артефактів, які необхідно зібрати, належно зафіксувати та інтерпретувати в сукупності: зокрема, час отримання повідомлення з посиланням, факт переходу, збережені параметри веб-сесії, введені дані, подальші дії в банківському додатку, отримання одноразового коду, підтвердження транзакції, листування з псевдопідтримкою, зміна пароля, спроби відновлення доступу, а також ознаки встановлення шкідливого ПЗ або підробленого додатка. В умовах сучасного кримінального провадження орган досудового розслідування має забезпечити, щоб спосіб отримання таких даних відповідав вимогам законності, а технічні процедури гарантували незмінність та відтворюваність результатів.

Розслідування фішингових атак за участю мобільних пристроїв зазвичай починається з фіксації повідомлення або іншого контакту, що став початковою точкою інциденту. У потерпілих це може бути SMS з вимогою оновити дані, повідомлення в месенджері від особи, що видає себе за працівника банку, лист у пошті із вкладенням або посиланням, оголошення в соціальній мережі з пропозицією

роботи чи компенсації, а також телефонний дзвінок із використанням соціальної інженерії. Уже на цьому етапі виникає питання збереження первинних даних у найбільш автентичному вигляді. Практично важливо, щоб повідомлення не було видалено, щоб не змінювалися параметри додатка, не очищувався кеш і не відбувалося оновлення, здатне перезаписати журнали або артефакти. Водночас не можна ігнорувати потреби потерпілої особи в безпеці: наприклад, необхідність терміново блокувати картку, змінювати паролі чи звертатися в банк. Тому слідчим доводиться балансувати між завданням збереження слідів і невідкладними заходами для мінімізації шкоди, документуючи, які саме дії були здійснені, коли, ким і за яких умов. Важливим є отримання від потерпілого максимально конкретних відомостей: через який канал надійшло повідомлення, що саме було написано, чи здійснювався перехід за посиланням, чи вводилися дані, чи встановлювався додаток, чи надавалися дозволи, чи надходили коди підтвердження і чи були дзвінки від невідомих осіб. Такі відомості допомагають сформувати первинну слідчу версію й визначити, які цифрові артефакти шукати на пристрої та в суміжних системах.

Процесуальне вилучення мобільного пристрою є критичним моментом, оскільки з ним пов'язані ризики зміни даних і подальшої критики з боку сторони захисту щодо допустимості. Виявлення і вилучення пристрою зазвичай здійснюється під час огляду, обшуку, затримання або тимчасового доступу. На практиці найпоширеніші помилки пов'язані з увімкненням або розблокуванням смартфона без фіксації первинного стану, підключенням до зарядного пристрою або комп'ютера без контролю, вимиканням пристрою без розуміння наслідків для шифрування, а також із відсутністю належної ізоляції від мережі. Сучасні смартфони підтримують віддалене стирання, а також механізми автоматичного очищення даних після певної кількості невдалих спроб розблокування. Додатково дані можуть змінюватися через синхронізацію, яка запускається одразу після підключення до інтернету, або через автоматичні резервні копії. Тому після виявлення пристрою доцільно забезпечити фіксацію від сигналу або переведення в режим, що мінімізує мережеву активність, а також задокументувати точний стан: увімкнений чи вимкнений, заблокований чи розблокований, які програми відкриті, які сповіщення відображаються, який рівень заряду, чи вставлена SIM-карта, чи є карта пам'яті, чи підключені аксесуари. Фіксація може здійснюватися фото- та відеозйомкою з таким ракурсом, щоб були видимі ідентифікаційні ознаки пристрою, серійні номери, особливості корпусу, а також екран з інформацією, що відображається. У подальшому ці дані дозволяють відтворити контекст вилучення і зменшують ризик процесуальних сумнівів.

Важливо враховувати, що питання вимкнення чи залишення пристрою увімкненим має неоднозначний характер і залежить від ситуації. Якщо пристрій розблокований, залишення його увімкненим інколи дозволяє отримати доступ до даних, які після блокування будуть недоступними через шифрування. Якщо пристрій заблокований, вимкнення може призвести до переходу в стан, коли ключі шифрування очищуються з оперативної пам'яті, і подальше розблокування без пароля стане практично неможливим. У той же час тривале збереження увімкненого пристрою підвищує ризик дистанційного втручання і автоматичних змін. Отже, рішення має прийматися з урахуванням конкретних умов, рівня ризику віддаленого доступу і можливостей оперативного забезпечення ізоляції. Процесуально важливо документувати мотиви прийнятого рішення, щоб у подальшому пояснити його обґрунтованість.

Після вилучення пристрою ключовим завданням є організація коректного вилучення даних і створення копій для дослідження. Принциповим підходом сучасної цифрової криміналістики є мінімізація втручання в оригінальний носій та робота з перевіреними копіями. Це пов'язано з тим, що навіть відкриття файлів, перегляд повідомлень або запуск додатка може змінити часові мітки, стан кешу, журнали, а інколи й перезаписати частину даних. Тому у методологічному плані правильним є використання спеціалізованих інструментів і процедур, що забезпечують контрольоване зчитування інформації та фіксацію її цілісності [2]. На рівні загальних підходів розрізняють логічне, файлове та фізичне вилучення, а також комбіновані методи, орієнтовані на конкретні артефакти додатків і системні журнали. Вибір методу визначається моделлю пристрою, версією операційної системи, рівнем захисту, наявністю шифрування, умовами доступу, а також процесуальними строками й задачами провадження.

Логічне вилучення зазвичай дозволяє отримати найбільш очевидні дані, важливі для первинного аналізу: контакти, історію дзвінків, SMS, календар, фотографії, частину документів, а інколи й дані з популярних додатків та месенджерів. Воно є порівняно швидким і менш ризиковим щодо пошко-

дження даних, однак має суттєве обмеження: видалені дані, приховані елементи, фрагменти кешу, низькорівневі журнали і частина баз додатків можуть бути недоступними. Файлове вилучення, у свою чергу, дає можливість працювати зі структурою файлової системи і контейнерами додатків, отримувати бази даних месенджерів, файли конфігурацій, логи, токени, кешовані медіа, збережені сторінки браузера, історії пошуку і переходів, що є критично важливим саме для фішингових атак. Фізичне вилучення, якщо воно технічно можливе, дозволяє отримати повний знімок пам'яті на бітовому рівні і здійснювати відновлення видалених даних, аналіз залишкової інформації, фрагментів повідомлень, частин файлів та системних структур. Проте у випадку сучасних смартфонів фізичне вилучення часто обмежується через шифрування і захисні механізми виробників, а також може вимагати спеціальних умов і високої кваліфікації, що підвищує ризик помилок. У слідчій практиці важливим є не стільки формальне прагнення до найглибшого способу вилучення, скільки забезпечення відтворюваності, доказової чистоти і релевантності даних для конкретної події фішингу.

Для фішингових атак особливе значення мають цифрові сліди, пов'язані з комунікацією та взаємодією з підробленими ресурсами. Зокрема, на пристрої потерпілого можуть бути збережені повідомлення з посиланнями, копії листів, вкладення, скриншоти, історія дзвінків із номерами, що використовувалися для соціальної інженерії, а також записи про відкриття посилань у браузері чи вбудованому переглядачі месенджера. Артефакти браузера містять не лише історію відвідувань, але й кеш, cookies, сховище локальних даних, автозаповнення форм, збережені паролі, параметри редиректів і часові мітки. У фішингових схемах часто використовуються ланцюжки перенаправлень, скорочені посилання, проміжні сторінки, що імітують перевірку безпеки або підтвердження. Виявлення таких ланцюжків можливе шляхом аналізу історії переходів, мережевих журналів, даних DNS-кешу та слідів у додатках, які відкривали посилання. Додатково важливими є дані мобільного банкінгу: журнали входів, підтвердження операцій, push-сповіщення, SMS з одноразовими кодами, записи про зміну налаштувань, додавання нових пристроїв до довірених, а також повідомлення про підозрілу активність. У комплексі ці дані дозволяють встановити причинно-наслідковий зв'язок між фішинговим контактом і фактом заволодіння коштами або доступом [3].

У випадках, коли фішинг супроводжується встановленням шкідливого програмного забезпечення або підробленого додатка, на мобільному пристрої можуть бути сліди інсталяції, запити дозволів, записи про доступ до служби спеціальних можливостей, зміни в налаштуваннях безпеки, появу профілів керування, встановлення сертифікатів, а також нетипова мережна активність. Зловмисники можуть прагнути отримати доступ до SMS для перехоплення кодів, до контактів для подальшого розповсюдження фішингових повідомлень, до сповіщень для зчитування одноразових паролів, а також до екрану для зняття даних із банківських додатків. Тому важливо фіксувати перелік встановлених програм, їх походження, час інсталяції, запитані й надані дозволи, а також ознаки підроблення. Встановлення факту, що застосунок був завантажений не з офіційного магазину або що користувач надавав нетипові дозволи незадовго до інциденту, може істотно посилити доказову конструкцію щодо механізму атаки і необережної поведінки потерпілого, а також підтвердити умисні дії підозрюваного, якщо йдеться про пристрій злочинця або посередника.

Окрема група доказових даних у провадженнях пов'язаних із розслідуванням фішингових атак пов'язана з метаданими та ідентифікаторами. Метадані включають часові мітки створення і зміни файлів, геолокаційні координати фотографій або знімків екрану, ідентифікатори пристрою, версії операційної системи, дані про SIM-карту, мережеві ідентифікатори, а також технічні параметри підключень. У практиці розслідування це дозволяє вирішувати як мінімум три важливі задачі. По-перше, уточнення хронології подій: коли отримано фішингове повідомлення, коли відкрито посилання, коли введено дані, коли здійснено транзакцію, коли відбувся дзвінок псевдопрацівника банку, коли створено скриншот або збережено документ. По-друге, кореляція подій між різними джерелами: зіставлення часу на пристрої з часом у банківських логах, у системах провайдерів, у сервісах пошти чи месенджерів. По-третє, атрибуція пристрою і його зв'язок із конкретною особою: встановлення належності номерів, акаунтів, карт і пристроїв, що використовувалися для входу, а також виявлення зв'язків між фігурантами через контакти, групи, канали, спільні платежі чи спільні мережеві параметри.

Проте метадані не є безумовно надійним джерелом істини: часові мітки можуть змінюватися при копіюванні, синхронізації, відновленні з резервної копії, а також при зміні часу

на пристрої. Геолокаційні дані можуть бути відсутніми або спотвореними через налаштування конфіденційності. Зловмисники можуть використовувати підроблені профілі, анонімізацію, VPN, проксі, віртуальні SIM або тимчасові номери. Тому метадані мають оцінюватися критично і в сукупності з іншими доказами, а їх автентичність повинна підтверджуватися процедурою вилучення і верифікації.

Автентифікація цифрових доказів у контексті мобільних пристроїв передбачає доведення трьох ключових параметрів: що саме ці дані були отримані з конкретного пристрою, що вони не були змінені після вилучення, і що їх інтерпретація відповідає реальному функціонуванню системи. Практичним інструментом підтвердження цілісності є використання криптографічних контрольних сум, які обчислюються для створеної копії або для конкретних файлів і вносяться до процесуальних документів [4]. Якщо в подальшому виникає потреба у повторному дослідженні, експерт може знову обчислити контрольні суми і підтвердити, що об'єкт дослідження є тим самим, що і на момент первинного вилучення. Це має не лише технічне, а й процесуальне значення: підтверджує незмінність доказу і підтримує його допустимість.

Не менш важливим є забезпечення ланцюга збереження. Йдеться про детальне документування руху носія і копій: хто вилучив, хто транспортував, де і як зберігалося, хто створював копії, хто мав доступ, які дії виконувалися, у який час, у яких умовах, із застосуванням яких інструментів. У випадку мобільних пристроїв ланцюг збереження ускладнюється тим, що інколи виникає потреба у проміжних діях до створення повної копії, наприклад у стабілізації пристрою, заряджанні, тимчасовому екрануванні, підключенні до спеціального обладнання. Кожна така дія потенційно може вплинути на дані або породити сумніви, отже повинна бути мотивована і зафіксована. У судовій перспективі саме дотримання ланцюга збереження часто є вирішальним аргументом на користь достовірності цифрових доказів.

Суттєвою проблемою у вилученні та автентифікації є шифрування, яке стало стандартом для сучасних мобільних платформ. Доступ до даних часто пов'язаний із введенням пароля або використанням біометрії, а після перезавантаження пристрою значна частина даних залишається недоступною до моменту первинного розблокування. Це зумовлює практичні дилеми: з одного боку, слідству необхідно забезпечити недоторканність даних, з іншого потрібно зберегти можливість доступу. У межах правових процедур можуть застосовуватися процесуальні механізми отримання інформації від власника, а також залучення спеціаліста або експерта, який, дотримуючись методик, здійснює технічні дії. Однак будь-яке примусове втручання в систему захисту може бути піддане критиці, якщо воно не має належного процесуального оформлення або виходить за межі дозволених дій. Тому пріоритетом має бути використання законних способів доступу, а у разі неможливості їх застосування слід максимально фокусуватися на альтернативних джерелах: даних від операторів зв'язку, банків, сервісів електронної пошти, месенджерів, логів веб-серверів, доменних реєстраторів, а також цифрових слідів, що зберігаються в хмарі і можуть бути отримані процесуальними засобами співпраці.

У кримінальних провадженнях про фішингові атаки важливо не зводити цифрове дослідження до пошуку лише тексту повідомлення або посилання. Професійний підхід передбачає побудову цифрової картини події, тобто реконструкцію ланцюга взаємодій користувача з інформаційним середовищем. Така реконструкція включає встановлення каналу первинного контакту, ідентифікацію доменів і ресурсів, з якими взаємодіяв пристрій, фіксацію мережевих з'єднань, аналіз поведінкових артефактів у додатках, перевірку змін у налаштуваннях безпеки, встановлення часу і способу підтвердження транзакцій, а також визначення ознак компрометації облікових записів. Наприклад, для SMS-фішингу важливими будуть не лише текст і номер відправника, але й дані про доставку, часові мітки, можливі підміни імені відправника, ознаки використання масових розсилок, подальші переходи за посиланням, а також співвідношення часу з банківськими діями. Для фішингу через месенджер важливим стане встановлення, чи є повідомлення результатом компрометації акаунта знайомої особи, чи це був підроблений профіль, які метадані профілю, коли створений акаунт, чи змінювався аватар і ім'я, чи були попередні контакти. Для фішингу через підроблену сторінку критично визначити, чи збереглися у браузері дані автозаповнення або збережені паролі, чи були введені логіни, чи створювалися скриншоти, чи зберігалася сторінка в кеші. Для схем з псевдопідтримкою і телефонним впливом важливими є журнали дзвінків, записи у месенджерах, а також можливі записи екрану чи голосових нотаток [5].

Встановлення технічних характеристик фішингової інфраструктури є окремим блоком роботи, який тісно пов'язаний із мобільним пристроєм. На ньому можуть бути збережені доменні імена, параметри URL, реферери переходів, дані про сертифікати безпеки, вміст сторінки в кеші, а інколи й фрагменти форм, що заповнювалися. Навіть якщо сторінка вже недоступна, кеш або збережені дані можуть дозволити довести факт її відвідування і зміст. У деяких випадках корисними є дані про встановлені профілі VPN, проксі, нетипові налаштування DNS, що могло бути використано для перенаправлення трафіку. Також важливими є ознаки фішингових додатків: наявність невідомих сертифікатів, профілів керування, нетипових дозволів, а також системних служб, що працюють у фоні.

Проблемою, яка часто виникає у судовій перспективі, є доведення того, що конкретна особа здійснювала дії на пристрої. Оскільки смартфон може використовуватися кількома особами, а в деяких випадках доступ до пристрою може бути отриманий дистанційно через шкідливе ПЗ, необхідно будувати доказування не лише на наявності артефактів, але й на сукупності обставин. Для потерпілого ключовим є встановлення факту введення даних і причинного зв'язку між цим фактом і наслідками. Для підозрюваного важливо показати контроль над інфраструктурою або участь у комунікаціях, наявність відповідних акаунтів, токенів, листування щодо обміну реквізитами, інструкцій, розподілу ролей, а також сліди доступу до викрадених коштів. У цьому сенсі мобільні пристрої підозрюваних можуть містити дані про створення фішингових сторінок, адміністрування доменів, використання панелей керування, отримання повідомлень із введеними жертвами даними, листування в групах, де координується діяльність, а також логістику виведення коштів через підставні рахунки. Автентифікація таких даних має поєднувати технічну перевірку цілісності з процесуальним доведенням їх походження та контексту використання.

Суттєвого значення набуває участь спеціаліста або експерта. У багатьох випадках слідчі дії з мобільними пристроями потребують спеціальних знань, оскільки неправильні дії можуть не лише знищити докази, а й створити процесуальні ризики. Експертне дослідження забезпечує методичну дисципліну: вибір адекватного способу вилучення, документування параметрів, створення копій, обчислення контрольних сум, ведення журналів операцій, пояснення результатів суду мовою, зрозумілою без спеціальних знань. Важливо, щоб експерт у висновку не лише перераховував знайдені об'єкти, а й пояснював їх значення в системі доказування, вказував на можливі альтернативні пояснення і межі достовірності. Для фішингових атак це особливо актуально, оскільки одна і та сама ознака може мати різні причини: наприклад, поява певного домену в історії браузера може бути як результатом переходу за посиланням, так і автоматичним завантаженням ресурсу через рекламу; наявність одноразового коду в SMS може свідчити як про ініціювання входу жертвою, так і про спробу входу зловмисником; зміна налаштувань безпеки може бути наслідком втручання шкідливого ПЗ або самостійних дій користувача. Тому експертне тлумачення повинно бути обережним, верифікованим і підкріпленим сукупністю слідів.

Окремо слід акцентувати увагу на проблемі синхронізації даних з хмарою і взаємодії мобільного пристрою з онлайн-акаунтами. У сучасних екосистемах значна частина цифрових слідів живе в сервісах: історія листування може зберігатися на серверах месенджера, електронні листи у поштових провайдерах, резервні копії у хмарних сховищах, журнали входів у сервісах автентифікації, а банківські події у системах фінансових установ. Мобільний пристрій у такому випадку є інтерфейсом доступу, а не єдиним місцем зберігання інформації. Це означає, що стратегія розслідування повинна бути комплексною: вилучення даних з пристрою має поєднуватися з отриманням даних від сервісів і провайдерів. При цьому мобільний пристрій часто містить ключі до такого доступу: токени сесій, ідентифікатори акаунтів, адреси електронної пошти, прив'язані номери, а також підтвердження факту використання конкретного сервісу. Належна автентифікація передбачає узгодження локальних даних із серверними журналами, що підвищує доказову силу і зменшує ризик оспорювання.

У практиці розслідування фішингових атак виникають специфічні ситуації, що потребують окремої тактики. Якщо пристрій потерпілого залишається в користуванні, а вилучення неможливе або недоцільне, слід забезпечити швидке і коректне копіювання релевантних даних з мінімальним втручанням: створення скриншотів, експорт листування, збереження повідомлень, фіксація сторінок у браузері, запис екрану, документування налаштувань [6]. Однак такі дії мають обмежену доказову силу порівняно зі спеціалізованим вилученням і можуть бути піддані сумніву через можливість редагування. Тому, якщо обставини дозволяють, перевагу слід надавати проце-

дурі, що забезпечує контрольні суми, належну фіксацію та участь спеціаліста. Інша ситуація виникає, коли пристрій підозрюваного містить дані, що швидко знищуються, наприклад тимчасові чати, повідомлення з авто-видаленням, або коли використано додатки з підвищеним рівнем приватності. У таких випадках першочерговими стають заходи з негайного блокування доступу до мережі і швидкого створення копії з урахуванням ризику перезапису даних. Тактика повинна бути законною і обґрунтованою, а всі дії мають бути процесуально задокументовані.

Особливу увагу слід приділяти перевірці достовірності отриманих даних та виявленню ознак підроблення. У цифровому середовищі можлива фальсифікація скриншотів, редагування листування, підміна контактів, а також створення штучних артефактів для введення слідства в оману. Тому важливо працювати не лише з візуальними відображеннями інформації, а й з первинними даними, базами, журналами і метаданими. Наприклад, скріншот фішингового повідомлення має меншу доказову цінність, якщо не підтверджено наявність такого повідомлення у базі даних месенджера або в системних журналах. Відповідно, автентифікація повинна охоплювати порівняння різних джерел: бази даних додатків, журнали повідомлень, журнали сповіщень, а також серверні дані за можливості. Для браузерних артефактів важливо співставляти історію з кешем, cookies і локальним сховищем, а для банківських операцій узгоджувати дані з виписками і журналами входів. Такий підхід забезпечує стійкість доказування навіть у разі спроб протидії.

Під час розслідування фішингових атак, у яких заволодіння коштами відбувається через подальше виведення на підставні рахунки або через ланцюжок транзакцій, мобільний пристрій може містити докази фінансової логістики. Це можуть бути повідомлення з реквізитами, фото банківських карт, дані про додані отримувачі, підтвердження платежів, переписка про розподіл коштів, використання криптогаманців, обмінники або інші інструменти [7]. Автентифікація таких даних потребує поєднання цифрових слідів на пристрої з документальними даними фінансових установ і, за необхідності, з результатами інших експертиз. У підсумку формується доказовий ланцюг від фішингового контакту до наслідків у вигляді списання коштів і їх подальшого руху.

У системному вимірі ефективність вилучення та автентифікації цифрових доказів залежить від організації роботи органів досудового розслідування, технічного оснащення та рівня компетентності. Практика вимагає уніфікованих алгоритмів дій під час вилучення мобільних пристроїв, наявності засобів ізоляції від мережі, доступу до сертифікованих або принаймні перевірених інструментів мобільної криміналістики, а також підготовки кадрів. В умовах швидкої еволюції мобільних платформ методики повинні регулярно оновлюватися, а слідчі та експерти мають підтримувати кваліфікацію через навчання і практичні тренування. Важливо також вибудовувати співпрацю з банками, операторами зв'язку та провайдерами сервісів для оперативного отримання логів, блокування транзакцій і збереження даних, які можуть бути втрачені через короткі строки зберігання.

Висновки. Узагальнюючи, мобільні пристрої при розслідуванні фішингових атак є джерелом багаторівневої доказової інформації, що охоплює комунікаційні артефакти, дані веб-взаємодії, сліди роботи банківських ідентифікаційних механізмів, метадані, системні журнали, а також ознаки шкідливого впливу. Вилучення таких даних повинно здійснюватися з урахуванням ризику їх миттєвої зміни або знищення, що зумовлює потребу в ізоляції від мережі, правильній фіксації первинного стану, створенні контрольованих копій і застосуванні криптографічних механізмів підтвердження цілісності. Автентифікація цифрових доказів має базуватися на контрольних сумах, документованому ланцюзі збереження, коректній інтерпретації артефактів та зіставленні локальних даних з серверними джерелами. Лише сукупність цих умов забезпечує допустимість, належність і достовірність цифрових доказів у кримінальному провадженні та створює підґрунтя для ефективної протидії фішинговим атакам у сучасному цифровому середовищі.

Література:

1. Використання електронних (цифрових) доказів у кримінальних провадженнях. метод. реком. М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін. ; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ. Вид-во Нац. акад. внутр. справ. 2020. 104 с.

2. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.

3. Пічієнко М. Г. Методики розслідування фішингових атак з використанням інструментів OSINT. Проблеми електромагнітної сумісності перспективних безпроводових мереж зв›язку (ЕМС-2021) : матеріали VII Міжнародної науково-технічної конференції, Харків, 25–26 листопада 2021 р. Харків. 2021. С. 101–103.

4. Сабадаш В.П. Фішинг як найбільш розвинений вид шахрайства в Інтернеті. *Університетські наукові записки*. 2006. № 1(17). С. 228–233.

5. Цифрова криміналістика та її роль у формуванні доказової інформації в умовах воєнних дій : монографія / В. Ю. Шепітько, М. В. Шепітько, К. В. Латиш, М. В. Капустіна, Є. Є. Демидова; за ред. В. Ю. Шепітька ; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2025. 200 с.

6. Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посіб. Київ. Юрінком Інтер, 2025. 236 с.

7. Buchyk S., Shutenko D., Toliupa S. Phishing Attacks Detection.Information Technology and Implementation. (IT&I-2022), November 30 -December 02, 2022, Kyiv, Ukraine. pp.193–201.

Дата першого надходження статті до видання: 24.02.2026
Дата надходження виправленої версії статті: 20.03.2026
Дата прийняття статті: 27.03.2026
Дата публікації статті: 12.06.2026