УДК 343.148:343.983 **DOI:** https://doi.org/10.32631/v.2025.1.36

Михайло Григорович Щербаковський,
доктор юридичних наук, професор,
Харківський національний університет внутрішніх справ,
навчально-науковий інститут № 5,
кафедра кримінального процесу,
криміналістики та експертології (завідувач);
https://orcid.org/0000-0003-1990-1231,
e-mail: shcherbakovskyi@gmail.com;

Сергій Олександрович Коломійцев,
Харківський національний університет внутрішніх справ,
навчально-науковий інститут № 4,
науково-дослідна лабораторія з проблем інформаційних технологій та протидії злочинності у кіберпросторі (науковий співробітник);
https://orcid.org/0009-0006-7070-9471,
e-mail :girbest@gmail.com

ЕКСПЕРТНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ЗБИРАННІ ТА ДОСЛІДЖЕННІ КОМП'ЮТЕРНИХ ДАНИХ

Доведено, що експертна інформаційна технологія – це система наукових положень, правових норм і заснованих на них методичних та організаційних рекомендацій щодо практичного використання технічних засобів, програм, систем, інформаційних масивів і баз даних, які застосовують у процесі проведення судових експертиз для підвищення ефективності вирішення завдань зі збирання та дослідження комп'ютерних даних.

Ключові слова: кримінальне провадження, криміналістичні технології, експертні інформаційні технології, комп'ютерні дані, судова експертиза, комп'ютерно-технічна експертиза.

Оригінальна стаття

Постановка проблеми

В умовах науково-технічного розвитку спостерігається постійний процес збільшення обсягу інформації в цілому, а також щодо відомостей про факти та обставини кримінальних правопорушень. Ця інформація у вигляді комп'ютерних даних міститься на матеріальних носіях – предметах, документах, в інформаційних мережах тощо, які потрапляють до орбіти кримінального провадження. Завдяки бурхливій інформатизації суспільства роль і значення комп'ютерних даних, що містяться на електронних носіях, у кримінальному судочинстві неухильно зростає. У зв'язку із цим теоретичною та практичною проблемою є необхідність упровадження у правозастосовну та судово-

експертну практику не лише вдосконалення наявних техніко-криміналістичних засобів, методів і прийомів дослідження джерел інформації, а й розроблення комплексу нових способів збирання інформації, яка має доказове значення для розслідування. Науковці активно обговорюють об'єднання різноманітних аспектів процесу розслідування кримінальних правопорушень в єдиний блок послідовних дій. Такий комплекс послідовних операцій та процедур у процесі слідчої діяльності визначений терміном «криміналістична технологія», а під час організації та проведення судових експертиз – «експертна технологія». Технологічний підхід розглядається у криміналістиці та судовій експертології як інноваційний спосіб збирання й отримання доказової інформації під час кримінального провадження. Проте визначення цих категорій та їх співвідношення залишаються дискусійними.

Стан дослідження проблеми

Проблеми впровадження технологій в окремих напрямах криміналістики та судових експертиз уже тривалий час перебувають у центрі уваги науковців. У працях вітчизняних учених розглядались проблеми використання криміналістичних та експертних технологій у кримінальному провадженні. Застосуванню технологічного підходу в розслідуванні кримінальних правопорушень приділяли увагу А. А. Барцицька, В. В. Білоус, І. В. Гора, Е. Б. Сімакова-Єфремян, Н. І. Клименко, В. А. Колесник, С. М. Корнійко, Н. В. Кисиль, О. М. Моїсєєв, А. М. Падалка, М. Я. Сегай, В. К. Стрінжа, В. В. Тіщенко, О. В. Фунікова, В. М. Шевчук, В. Ю. Шепітько, М. Г. Щербаковський, О. О. Юхно та ін. Однак унаслідок розвитку інформаційних технологій, глобальних мереж, стрімкого розроблення нових видів комп'ютерної техніки постає необхідність подальшого розвитку технологізації у сфері криміналістики та судових експертиз. Актуальності проблемі додає введення у кримінальний процесуальний закон нового виду доказової інформації – комп'ютерних даних (ст. 99 Кримінального процесуального кодексу України[1]). Комп'ютерні дані визначають як «будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою»[2], а дані – як «інформація, яка подана у

[1] Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 4651-VI // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 10.02.2025).

[2] Конвенція про кіберзлочинність : від 23.11.2001 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.02.2025).

формі, придатній для її оброблення електронними засобами»[1]. Під час кримінального провадження збирання та дослідження комп'ютерної інформації здійснюються зазвичай шляхом проведення комп'ютерно-технічної експертизи, типовими завданнями якої є виявлення інформації, що міститься на речових доказах – комп'ютерних носіях[2].

Отже, потребує подальшого обговорення поняття «технології» у правозастосовній сфері в цілому, інформаційних технологій у криміналістиці й експертних інформаційних технологій, спрямованих на збирання та дослідження комп'ютерної інформації.

Мета і завдання дослідження

Метою статті є визначення поняття «експертна інформаційна технологія», її структури та зв'язку з криміналістичними технологіями.

Завданнями дослідження є аналіз наукових напрацювань щодо створення криміналістичних та експертних технологій, визначення поняття і складових експертних інформаційних технологій, демонстрація експериментального способу відбору програмного продукту для вирішення експертного завдання з відновлення знищених комп'ютерних даних.

Наукова новизна дослідження

Доведено, що експертна інформаційна технологія – це система наукових положень, правових норм і заснованих на них методичних та організаційних рекомендацій щодо практичного використання технічних засобів, програм, систем, інформаційних масивів і баз даних, які застосовують у процесі проведення судових експертиз для підвищення ефективності вирішення завдань зі збирання та дослідження комп'ютерних даних. Експертна інформаційна технологія складається з теоретичної, правової, методичної, організаційної, апаратної, програмної та інформаційної компонент. Доведено, що існують три способи впровадження апаратних, програмних, інформаційних складових в експертну технологію: застосування готових програмних і технічних засобів інформаційних технологій; модернізація, трансформація готових інформаційних технологій з урахуванням специфіки завдань, що вирішуються судовою експертизою; розроблення спеціальних експертних інформаційних технологій.

[1] Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 10.02.2025).

[2] Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень : наказ М-ва юстиції України від 08.10.1998 № 53/5 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (дата звернення: 10.02.2025).

Виклад основного матеріалу

Відповідно до етимологічного значення технологія визначається, з одного боку, як сукупність знань, відомостей про послідовність окремих виробничих операцій у процесі виробництва чого-небудь, а з іншого – як сукупність способів обробки або переробки матеріалів, виготовлення виробів, проведення різних виробничих операцій тощо [1, с. 321]. Завданням технології як науки є виявлення закономірностей із метою розроблення й використання на практиці найбільш ефективних та економічних виробничих процесів. Таким чином, поняття «технологія» є доволі широким і універсальним та стосується будь-якої цілеспрямованої продуктивної діяльності.

Первісними спробами розроблення технологічного підходу у криміналістиці до процесу розслідування вважається ідея запровадження схеми розслідування злочинів, порівняння процесу розслідування злочинів із виробничими процедурами, широке трактування криміналістичної техніки [2, с. 6]. Під криміналістичною технологією В. В. Тіщенко й А. А. Барцицька розуміють науково обґрунтовану систему практичних дій і процедур, методів і засобів їх здійснення, спрямованих на оптимізацію розслідування, шляхом поетапного та послідовного вирішення його тактичних і стратегічних завдань. До основних функцій криміналістичної технології, на їхню думку, належать: системоутворююча, пізнавальна, управлінська, прогностична [3, с. 40–45]. Запровадження криміналістичних технологій у практику розслідування передбачає впорядкування складного процесу комплексного використання технічних і тактичних засобів, що має велике значення для процесу розслідування в цілому. Зокрема, технологічний аспект застосування техніко-криміналістичних засобів полягає у безпосередньому взаємозв'язку техніки й тактики проведення окремих слідчих дій. Таким чином, у практичному аспекті криміналістична технологія реалізується через процес послідовного запровадження комплексу дій та процедур в інформаційно-пізнавальній та організаційно-управлінській сферах слідчої та експертної діяльності.

Різновидом криміналістичних технологій є експертні технології дослідження слідів кримінальних правопорушень. М. Я. Сегай і В. К. Стринжа вперше надали визначення експертної технології як: сукупності правил, прийомів і способів найбільш раціональної та ефективної організації проведення судових експертиз у державних судово-експертних установах; опису технологічних схем, процесів, карток; розроблення загальних та окремих положень з подальшого удосконалення зазначених правил, прийомів, способів, технологічних схем, процесів і карток [4, с. 3–4]. Один із авторів цієї статті розглядає експертну технологію більш широко як систему пізнавальних (дослідних),

організаційних (управлінських) операцій, слідчих, судових, оперативно-розшукових та інших прийомів та способів, що застосовуються відповідними суб'єктами, згідно з чинним законодавством, для вирішення слідчо-, судово-експертних ситуацій з метою отримання доказової інформації у справі [5, с. 20]. Н. І. Клименко експертною технологією вважає сукупність операцій, що здійснюються в певній послідовності, виконуються на основі певних знань у зв'язку із проведенням дослідження яких-небудь об'єктів, речових доказів із метою пошуку відповідей на поставлені перед експертом питання [6, с. 143]. У цьому визначенні поняття «технологія» збігається з поняттям «експертна методика». О. М. Моїсєєв уважає, що експертна технологія – це система робочих операцій, які становлять раціональні дії з оптимального використання судовим експертом наявних ресурсів (матеріальних, технічних, фінансових, трудових, інтелектуальних, нормативно-правових) для забезпечення результативного проведення судових експертиз [7, с. 18]. А. М. Падалка та І. В. Пашинська відносять до експертних технологій використання техніко-криміналістичних засобів, апаратно-програмних комплексів, програмного забезпечення, організаційних рішень і методичних прийомів для вирішення завдань як інструменту створення проміжного або підсумкового матеріального чи нематеріального продукту [8, с. 567].

Підсумовуючи надані визначення, можна дійти висновку, що вчені застосовують діяльнісний підхід до розуміння експертної технології, застосування якої відбувається шляхом комплексного цілеспрямованого послідовного проведення різного роду дій і процедур із метою ефективного вирішення експертних завдань. Експертна технологія – це цілісна структура практичного вирішення експертних завдань, що охоплює матеріально-технічне забезпечення та застосування експертно-методичного й організаційно-управлінського комплексів. Основна мета експертної технології – оптимальне поєднання всіх структурних елементів експертної діяльності, що впорядковує процес їх практичної реалізації [3, с. 106].

В. Ю. Шепітько вказує, що нині зростання обсягів інформаційних ресурсів, швидкості і гнучкості інформаційних процесів, а також широкомасштабне впровадження інформаційних технологій в усі сфери життєдіяльності як невід'ємного складника інформаційної епохи створили підґрунтя для застосування інформаційних технологій у сучасних умовах проведення судових експертиз [9, с. 25]. І. В. Пиріг звертає увагу на особливості сучасного етапу розвитку судових експертиз, які ґрунтуються на теоретичній основі судової експертології, новітніх досягненнях науки, техніки та інформаційних технологіях [10, с. 48]. Сучасні процеси експертної діяльності зумовлені практичною необхідністю створення узагальнюючої структури, яка б об'єднувала

технологічний комплекс інформаційно-пізнавальних, організаційно-управлінських процедур і технічних засобів. Тому, як слушно зазначає О. О. Юхно, застосування інновацій зумовлює кардинальні зміни наукової парадигми криміналістики, експертології та досудового розслідування в цілому [11, с. 46].

У період глобальної інформатизації актуальним є інноваційний підхід до розуміння поняття «технологія», що пов'язане із запровадженням новітніх інформаційних розробок у практику боротьби зі злочинністю, зокрема щодо сучасних можливостей комп'ютерних засобів, інформаційно-обчислювальних систем, засобів телекомунікації та систем зв'язку. З урахуванням кількісних і структурних змін у складі злочинності та загального зростання її технологічного рівня мають бути переглянуті заходи щодо її подолання, насамперед розвиток експертних технологій на базі сучасної комп'ютерної техніки і програмних продуктів. Указане стосується передусім такого найсучаснішого роду судових експерти, як комп'ютерно-технічної. Тому в літературі наголошується, що зараз актуальним і необхідним є розроблення уніфікованих методик проведення судової комп'ютерно-технічної експертизи, яка б відповідала вимогам законодавства та сьогодення й ураховувала досягнення вітчизняних і зарубіжних науковців [12, с. 61].

Сьогодні одним із головних критеріїв результативності судово-експертної діяльності є впровадження досягнень науки у практику, що вимагає переходу до використання різноманітних інноваційних технологій. Провідне місце в цьому контексті належить дослідженням інформаційних технологій, що забезпечують процес розслідування та розкриття злочинів.

Згідно зі ст. 1 Закону України «Про Національну програму інформатизації» інформаційно-комунікаційні технології – це результат інтелектуальної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік та послідовність виконання операцій для збирання, обробки, накопичення та використання інформаційної продукції, надання інформаційних послуг. Задля реалізації інформаційно-комунікаційних технологій застосовуються засоби інформатизації, якими є комп'ютери, електронно-обчислювальна техніка, програмні продукти, інформаційні системи або їхні окремі елементи, електронні комунікаційні мережі, що використовуються для реалізації інформаційно-комунікаційних технологій[1].

Істотним елементом експертної технології визначено технічні засоби та методи дослідження, що відіграють роль інструментарію

[1] Про Національну програму інформатизації : Закон України від 01.12.2022 № 2807-IX // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2807-20 (дата звернення: 10.02.2025).

експерта. В аспекті комп'ютерно-технічної експертизи таким компонентом є апаратне та програмне забезпечення судово-експертного дослідження. *Апаратне (технічне) забезпечення* – це фізичні компоненти інформаційної технології: портативні та стаціонарні комп'ютери, планшети, мобільні телефони, пристрої введення, запам'ятовувальні пристрої, пристрої виведення та ін. Через апаратне забезпечення здійснюється доступ до більшості програм та інформаційних даних. *Програмне забезпечення* існує та будується безпосередньо на апаратному забезпеченні, носіях інформації, які без нього не функціонують. Програмне забезпечення можна умовно розділити на дві категорії: операційні системи та прикладне програмне забезпечення. Програмне забезпечення операційної системи керує апаратним забезпеченням, створює інтерфейс між апаратним забезпеченням і користувачем, надає платформи розробникам програмного забезпечення для написання програм.

Отже, поняття експертної інформаційної технології можна сформулювати як систему наукових положень, правових норм і заснованих на них методичних та організаційних рекомендацій щодо практичного використання технічних засобів, програм, систем, інформаційних масивів і баз даних, які застосовують у процесі проведення судових експертиз для підвищення ефективності рішення поставлених завдань зі збирання та дослідження комп'ютерних даних. У наведеному визначені можна виокремити такі складові експертної інформаційної технології: теоретичну, правову, методичну, організаційну, апаратну, програмну та інформаційну.

Упровадження апаратних, програмних та інформаційних складових в експертну технологію може здійснюватися трьома способами: 1) застосуванням готових програмних засобів інформаційних технологій; 2) модернізацією і трансформацією готових інформаційних технологій з урахуванням специфіки завдань, які вирішує судова експертиза; 3) розробленням спеціальних інформаційних експертних технологій.

Застосування готових засобів для вирішення експертного завдання з відновлення знищених комп'ютерних даних проілюструємо на прикладі наявних у вільному доступі програм.

Відновлення видалених комп'ютерних даних відіграє критично важливу роль у кримінальному провадженні. Інформація, яка здається втраченою, може стати ключовим доказом у розслідуванні злочинів. Ефективність програмного забезпечення для пошуку та відновлення даних є одним із ключових чинників забезпечення якісного збору цифрових доказів. У кримінальному провадженні цифрові дані можуть виступати доказами злочинної діяльності або слугувати підтвердженням невинуватості підозрюваних. У багатьох випадках

такі дані можуть бути видалені або пошкоджені зловмисниками з метою приховування слідів злочину. Завдання експертів полягає у відновлені цих даних, збереженні їхньої цілісності та допустимості як доказів у суді. Різноманіття наявних у вільному доступі програм, які можуть бути застосовані для відновлення даних, ускладнює вибір оптимального інструмента для експертних цілей. Ці програми мають різні рівні функціональності, алгоритми відновлення та певні обмеження.

Мета проведеного експериментального дослідження полягала в порівнянні сучасних програм відновлення даних, перевірці швидкості їхньої роботи і здатності відновлювати файли рідкісних, специфічних форматів. Експеримент проводився за допомогою комп'ютера з операційною системою Windows 11, 64-bit, центральним процесором – AMD Ryzen 3 5300U, оперативною пам'яттю – 20 ГБ, USB-флешнакопичувачем – 2 ГБ. Програмне забезпечення відбиралось за такими критеріями: доступність, популярність і кількість позитивних відгуків користувачів. Використовувалися такі програми: Recuva, Tenorshare 4DDiG, Wise Data Recovery, MiniTool Power Data Recovery, Stellar Data Recovery.

Об'єктами дослідження у процесі експерименту стали 24 спеціально створені файли різних специфічних форматів:

– формати документів і текстових даних: .rtf (використовується в таких текстових редакторах, як WordPad, Microsoft Word); .txt (застосовується для нотаток, скриптів, конфігурацій); .md (використовується для документації, README-файлів у проєктах); .tex (застосовується в академічній та науковій сферах);

– формати архівів: .zip (для упакування та стиснення файлів); .tar.gz (резервне копіювання даних у Linux); .7z (для зменшення розміру великих файлів); .zpaq (резервне копіювання); .arj (старий формат архівів, популярний у DOS-системах); .cab (використовується для встановлення програм і оновлень);

– конфігураційні файли: .ini (застосовується у програмах для Windows); .yaml (використовується в DevOps, наприклад Kubernetes, Ansible); .toml (для проєктів на Python та Rust);

– криптографічні та ключові файли: .key (використовується у сертифікатах SSL/TLS та криптографії); .pem (для захисту даних SSL/TLS);

– графічні формати: .png (для графічних елементів); .bmp (для високоякісної графіки);

– бази даних і структуровані дані: .db (використовується у месенджерах та додатках для збереження даних); .csv (для імпорту/експорту даних у таблицях); .json (для API та конфігурацій додатків);

– спеціальні та системні файли: .bin (прошивки, образи пам'яті); .myownformat (власний користувацький формат); .izh (специфічний

для окремих програм або систем, часто використовується у пропрієтарних рішеннях для резервного копіювання чи передачі даних); .log (формат текстових файлів для запису подій або процесів під час роботи програм чи систем).

У межах дослідження для повного заповнення обсягу пам'яті USB-флешнакопичувача, крім наведених файлів, було записано різноманітні дані для штучного створення стороннього «шуму».

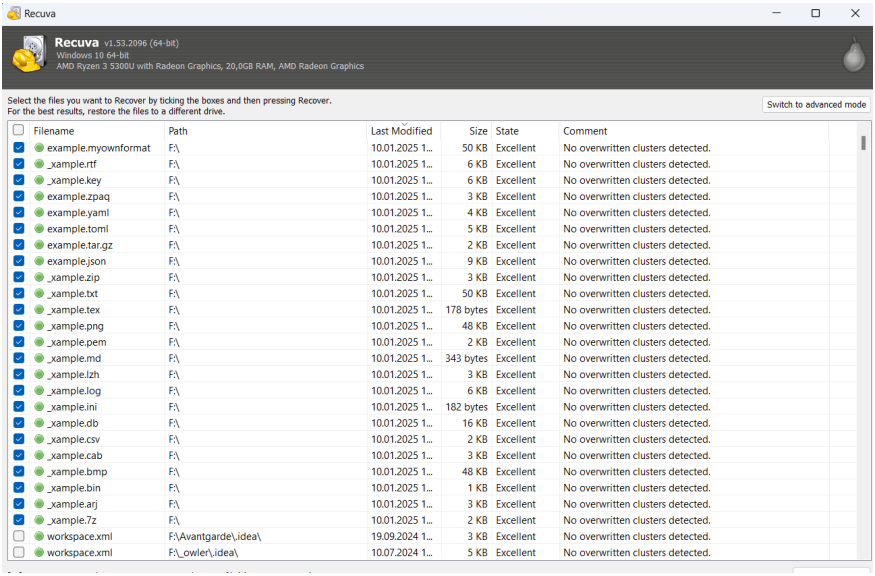
Можливість відновлення знищених файлів залежить від того, яким саме способом вони були видалені на носії. Видалення файлів може здійснюватися трьома способами:

1) звичайне видалення використанням команди «Видалити». Під час такого видалення операційна система безпосередньо файл не знищує, а лише позначає простір, який він займав, як вільний. Одночасно видаляється запис про файл у файловій таблиці, і файл фактично стає невидимим для користувача. На дисковому накопичувачі файл залишається доти, доки на його місце на диску не буде записано нові дані. У разі такого видалення ймовірність відновлення є найвищою;

2) швидке форматування накопичувача (диска). Під час швидкого форматування видаляється вся файлова таблиця, а файлова система повністю переініціалізується. Самі файли не знищуються, але видалення файлової таблиці суттєво ускладнює їхнє відновлення;

3) повне форматування накопичувача (диска). Під час такого видалення операційна система повністю очищує носій даних, стираючи не лише файлову таблицю, а й самі дані. Виконується перезапис кожного сектора на диску (зазвичай нулями або іншими символами). Вказаний спосіб видалення унеможливлює подальше відновлення даних звичайними доступними програмами. Лише складними апаратними методами, що використовуються у спеціалізованих лабораторіях, можуть бути частково відновлено деякі дані. Однак це дуже дорогі малодоступні технології, а їх застосування вимагає багато часу [13, pp. 210–211].

Перший етап експерименту полягав у встановлені можливості пошуку та відновлення видалених звичайним способом файлів з USB-флешнакопичувача об'ємом 2 ГБ і порівнянні швидкості цієї процедури. На цьому етапі експерименту встановлено, що вибрані програми успішно знайшли всі 24 тестові файли після їх видалення: Recuva – 50 с; Wise Data Recovery – 2 хв 5 с; Tenorshare 4DDiG – 2 хв 18 с; Stellar Data Recovery – 2 хв 45 с; MiniTool Power Data Recovery – 3 хв 45 с. На рис. 1 показано файли, відновлені програмою Recuva.



Filename	Path	Last Modified	Size	State	Comment
example.myownformat	F:\	10.01.2025 1...	50 KB	Excellent	No overwritten clusters detected.
_xample.rtf	F:\	10.01.2025 1...	6 KB	Excellent	No overwritten clusters detected.
_xample.key	F:\	10.01.2025 1...	6 KB	Excellent	No overwritten clusters detected.
example.zpaq	F:\	10.01.2025 1...	3 KB	Excellent	No overwritten clusters detected.
example.yaml	F:\	10.01.2025 1...	4 KB	Excellent	No overwritten clusters detected.
example.toml	F:\	10.01.2025 1...	5 KB	Excellent	No overwritten clusters detected.
example.tar.gz	F:\	10.01.2025 1...	2 KB	Excellent	No overwritten clusters detected.
example.json	F:\	10.01.2025 1...	9 KB	Excellent	No overwritten clusters detected.
_xample.zip	F:\	10.01.2025 1...	3 KB	Excellent	No overwritten clusters detected.
_xample.txt	F:\	10.01.2025 1...	50 KB	Excellent	No overwritten clusters detected.
_xample.tex	F:\	10.01.2025 1...	178 bytes	Excellent	No overwritten clusters detected.
_xample.png	F:\	10.01.2025 1...	48 KB	Excellent	No overwritten clusters detected.
_xample.pem	F:\	10.01.2025 1...	2 KB	Excellent	No overwritten clusters detected.
_xample.md	F:\	10.01.2025 1...	343 bytes	Excellent	No overwritten clusters detected.
_xample.lzh	F:\	10.01.2025 1...	3 KB	Excellent	No overwritten clusters detected.
_xample.log	F:\	10.01.2025 1...	6 KB	Excellent	No overwritten clusters detected.
_xample.ini	F:\	10.01.2025 1...	182 bytes	Excellent	No overwritten clusters detected.
_xample.db	F:\	10.01.2025 1...	16 KB	Excellent	No overwritten clusters detected.
_xample.csv	F:\	10.01.2025 1...	2 KB	Excellent	No overwritten clusters detected.
_xample.cab	F:\	10.01.2025 1...	3 KB	Excellent	No overwritten clusters detected.
_xample.bmp	F:\	10.01.2025 1...	48 KB	Excellent	No overwritten clusters detected.
_xample.bin	F:\	10.01.2025 1...	1 KB	Excellent	No overwritten clusters detected.
_xample.arj	F:\	10.01.2025 1...	3 KB	Excellent	No overwritten clusters detected.
_xample.7z	F:\	10.01.2025 1...	2 KB	Excellent	No overwritten clusters detected.
workspace.xml	F:\Avantgarde\.idea\	19.09.2024 1...	3 KB	Excellent	No overwritten clusters detected.
workspace.xml	F:_owler\.idea\	10.07.2024 1...	5 KB	Excellent	No overwritten clusters detected.

Рис 1. Файли, відновлені програмою Recuva

На другому етапі експерименту пошук файлів здійснювався на USB-флешнакопичувачі, який був відформатований у швидкому режимі. Результати експерименту показали, що застосованими програмами відновлено: Tenorshare 4DDiG – 10 файлів (2 хв), Stellar Data Recovery – 9 файлів (7 хв 5 с); Wise Data Recovery – 7 файлів (2 хв 5 с), Recuva – 7 файлів (8 хв), MiniTool Power Data Recovery – 2 файли (3 хв 40 с). На цьому етапі експерименту час пошуку не відігравав суттєвої ролі, оскільки відсоток знайдених файлів значно зменшився. Найбільш корисним є показник кількості виявлених файлів. Після видалення файлової таблиці інформація про файли переплуталася, що ускладнило процес їхньої ідентифікації та відновлення. Хоча після швидкого форматування файли все ще не були остаточно видалені з USB-флешнакопичувача, застосовані для їхнього пошуку та відновлення програми не змогли впоратися із завданням повністю. Причиною такого негативного результату є видалення інформації про закінчення одного файлу і початок іншого. У такому разі розпізнати файли серед «шуму» можна за їхньою сигнатурою, тобто унікальним набором байтів, розміщеним на початку або, у деяких випадках, наприкінці файлу. У підсумку найкращий результат показала програма Tenorshare 4DDiG, яка змогла ідентифікувати 10 із 24 файлів і зробила це за найкоротший час. Найгірший результат – лише 2 із 24 файлів –

продемонструвала програма MiniTool Power Data Recovery. На рисунку 2 показано файли, знайдені програмою Tenorshare 4DDiG.

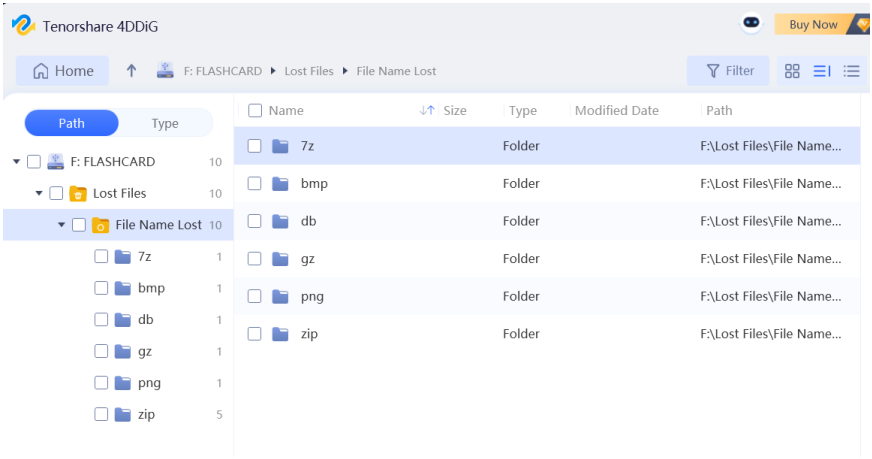


Рис. 2. Файли, знайдені програмою Tenorshare 4DDiG

Виходячи з отриманих результатів, можна зробити висновок, що застосовані програми розпізнають лише сигнатури популярних форматів. Більшість програм успішно впоралися лише з розпізнаванням форматів архівів і графічних файлів. Відновлення менш поширених або специфічних форматів після швидкого форматування виявилося неможливим.

Отримані результати свідчать про те, що більшість вільно доступних програм здатні відновлювати лише файли з відомими сигнатурами, що підтверджує важливість правильного вибору програмного забезпечення залежно від типу даних, які потрібно відновити. Для відновлення рідкісних або специфічних форматів файлів під час проведення експертиз доцільніше використовувати більш спеціалізовані інструменти, такі як X-Ways Forensics[1] та EnCase Forensic[2], або апаратні методи, зокрема PC-3000[3] та DeepSpar Disk[4].

[1] X-Ways Forensics: Integrated Computer Forensics Software // X-Ways : сайт. URL: https://www.x-ways.net/forensics (дата звернення: 10.02.2025).

[2] OpenText Forensic (EnCase) // Openteext : сайт. URL: https://www.opentext.com/products/forensic (дата звернення: 10.02.2025).

[3] PC-3000 // ACELab : сайт. URL: https://www.acelab.eu.com/catalog (дата звернення: 10.02.2025).

[4] DeepSpar Disk : сайт. URL: https://www.deepspar.com (дата звернення: 10.02.2025).

Висновки

У сучасний період інформатизація всіх сфер суспільства, зростання обсягів різнорідних інформаційних ресурсів, розвиток інформаційних технологій та існування слідів правопорушень у вигляді комп'ютерних даних слугують підставою для формування експертних інформаційних технологій. Експертні технології дослідження слідів кримінальних правопорушень є різновидом криміналістичних технологій, що застосовуються під час кримінальних проваджень.

Експертна інформаційна технологія – це система наукових положень, правових норм і заснованих на них методичних та організаційних рекомендацій щодо практичного використання технічних засобів, програм, систем, інформаційних масивів і баз даних, які застосовують у процесі проведення судових експертиз для підвищення ефективності вирішення завдань зі збирання та дослідження комп'ютерних даних. Експертна інформаційна технологія складається з теоретичної, правової, методичної, організаційної, апаратної, програмної та інформаційної компонент. Існують три способи впровадження апаратних, програмних, інформаційних складових в експертну технологію: застосування готових програмних і технічних засобів інформаційних технологій; модернізація, трансформація готових інформаційних технологій з урахуванням специфіки завдань, що вирішуються судовою експертизою; розроблення спеціальних експертних інформаційних технологій.

Список бібліографічних посилань: 1. Словник української мови : в 11 т. / АН Української РСР, Ін-т мовознав. ім. О. О. Потебні ; редкол.: І. К. Білодід (голова) та ін. Київ : Наук. думка, 1979. Т. 9. 658 с. **2.** Барцицька А. А. Криміналістичні технології: сутність та місце в системі криміналістичної науки : автореф. … канд. юрид. наук : 12.00.09. Одеса, 2011. 20 с. **3.** Тіщенко В. В., Барцицька А. А. Теоретичні засади формування технологічного підходу в криміналістиці : монографія. Одеса : Фенікс, 2012. 198 с. **4.** Сегай М. Я., Стринжа В. К. Актуальные проблемы экспертной технологии в условиях НТР. *Криминалистика и судебная экспертиза.* 1984. Вип. 29. С. 3–7. **5.** Щербаковский М. Г. Содержание, свойства и функции экспертных технологий // Сучасні судово-експертні технології в кримінальному і цивільному судочинстві : матеріали Міжнар. наук.-практ. конф. (м. Харків, 14–15 берез. 2003 р.) / МВС України, Нац. ун-т внутр. справ. Харків, 2003. С. 16–21. **6.** Клименко Н. І. Судова експертологія : курс лекцій. Київ : Ін Юре, 2007. 528 с. **7.** Моїсєєв О. М. Експертні технології: теорія формування і практика застосування : монографія. Харків : Апостіль, 2011. 424 с. **8.** Падалка А. М., Пашинська І. В. Застосування технологій у судово-експертній діяльності. *Юридичний науковий електронний журнал.* 2023. № 11. С. 565–567. DOI: https://doi.org/10.32782/2524-0374/2023-11/139. **9.** Шепітько В. Ю. Інновації в

судово-експертній діяльності // Інноваційні методи, засоби та технології в криміналістиці та судовій експертизі : наук.-практ. посіб. / за ред. В. Ю. Шепітька. Харків : Право, 2023. 116 с. **10.** Пиріг І. В. Теоретико-прикладні проблеми експертного забезпечення досудового розслідування : монографія. Дніпропетровськ : Дніпропетров. держ. ун-т внутр. справ ; Ліра ЛТД, 2015. 432 с. **11.** Юхно О. Генезис і проблемні питання використання новітніх технологій та штучного інтелекту в криміналістиці, експертній діяльності та досудовому розслідуванні. *Теорія та практика судової експертизи і криміналістики.* 2021. Вип. 3 (25). С. 40–59. DOI: https://doi.org/10.32353/khrife.3.2021.04. **12.** Климчук М. П., Комісарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посіб. Львів : Львів. держ. ун-т внутр. справ, 2022. 112 с. **13.** Tanenbaum A. S., Bos H. Modern Operating Systems. New Jersey : Prentice Hall, 2001. 1137 p.

Надійшла до редколегії 11.02.2025

Прийнята до опублікування 13.03.2025

Shcherbakovskyi M. H., Kolomiitsev S. O. Expert information technology in the collection and analysis of computer data

In the modern period of society's informatisation, the growth of heterogeneous information resources, the development of information technology and the existence of traces of offences in the form of computer data serve as the basis for the formation of expert information technologies. Expert technologies for investigating traces of criminal offences are a type of forensic technologies used in criminal proceedings and represent a set of consistent procedures, operations, techniques and methods of using technical means to solve a task.

Expert technology as an embodiment of an innovative approach to the practice of combating crime is considered to be a holistic structure of practical solution of expert tasks, including logistics, application of expert methodological, organisational and managerial measures. The main purpose of expert technology is the optimal combination of all structural elements of expert activity, which streamlines the process of their practical implementation. Expert information technology as a complex category includes theoretical, legal, methodological, organisational, hardware, software and information components.

The article defines expert information technology as a system of scientific provisions, legal norms and methodological and organisational recommendations based on them regarding the practical use of technical means, programs, systems, information arrays and databases used in the process of conducting forensic examinations, with a view to improving the efficiency of solving the tasks of collecting and researching computer data.

It is shown that there are three ways of implementing hardware, software and information components into expert technology: a) use of ready-made software and hardware information technologies; b) modernisation and transformation of existing information technologies with due regard for the specifics of the tasks performed by forensic examination; c) development of special expert information technologies. On the example of existing computer programs, the

author demonstrates an experimental method of selecting a software product for solving the expert task of restoring destroyed computer data.

Keywords: criminal proceedings, forensic technologies, expert information technologies, computer data, forensic examination, computer-technical examination.