МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ ТА ДОСУДОВОМУ РОЗСЛІДУВАННІ

НАВЧАЛЬНИЙ ПОСІБНИК

за загальною редакцією
доктора філософії в галузі права
А. О. Волобоєва

УДК 343.1.85(477)

В43

Рекомендовано до друку Методичною радою
Донецького державного університету внутрішніх справ
(протокол № 12 від 26.08.2024 року)

Рецензенти:

Іваницький Сергій – професор кафедри економічної безпеки та фінансових розслідувань Національної академії внутрішніх справ, доктор юридичних наук, доцент

Яковенко Микола – заступник начальника сектору «Служба освітньої безпеки» Полтавського районного управління поліції Головного управління Національної поліції в Полтавській області, кандидат юридичних наук, доцент

В43 Використання сучасних інформаційних технологій в оперативно-розшуковій діяльності та досудовому розслідуванні : навчальний посібник / Волобоєв А. О., Габорець О. А., Тімошин А. С., Морозов Д. А., Пупинін О. М.; за заг. ред. А. О. Волобоєва. Кропивницький : ДонДУВС, 2024. – 128 с.

У навчальному посібнику розглянуто найактуальніші аспекти впровадження сучасних інформаційних технологій у сфері правоохоронної діяльності. Особливу увагу приділено питання використання електронних доказів, які є невід'ємною частиною сучасного кримінального процесу. Проаналізовано методи розвідки даних з відкритих джерел (OSINT), що дають змогу значно підвищити ефективність розслідувань за рахунок збору та аналізу доступної інформації. Окремо розглянуто функціонування єдиних інформаційних систем Міністерств внутрішніх справ, які забезпечують інтеграцію та координацію даних у межах правоохоронних органів. Виокремлено роль цифрової криміналістики, її інструментів та методів, що дозволяють на високому рівні проводити досудові розслідування, забезпечуючи надійність та достовірність зібраних цифрових доказів у судовому процесі.

Навчальний посібник призначений для практичних працівників Національної поліції України, викладачів, курсантів та слухачів закладів вищої освіти й усіх, хто цікавиться проблематикою безпеки.

УДК 343.1.85(477)

Відомості про авторів

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

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

Тімошин Анатолій Сергійович – доцент кафедри протидії кіберзлочинності факультету підготовки фахівців для підрозділів кіберполіції Харківського національного університету внутрішніх справ, кандидат фізико-математичних наук, доцент.

Морозов Демид Анатолійович – доцент кафедри правосуддя факультету підготовки фахівців для підрозділів поліції Луганського навчально-наукового інституту імені Е. О. Дідоренка Донецького державного університету внутрішніх справ, кандидат юридичних наук.

Пупинін Олександр Миколайович – аспірант Донецького державного університету внутрішніх справ.

ЗМІСТ

ВСТУП

У сучасних умовах оперативно-розшукова діяльність та досудове розслідування нерозривно пов'язані із застосуванням передових інформаційних технологій. Це особливо стосується процесів вилучення інформації з електронних інформаційних систем і проведення пошукових операцій в Інтернеті. Відповідно до чинних нормативно-правових актів України, перед оперативними підрозділами постають наступні завдання:

– виявлення, запобігання та припинення кримінальних правопорушень;

– встановлення осіб, які готують або вчиняють кримінальні правопорушення;

– розшук осіб, які ухиляються від органів досудового розслідування, слідчого судді, суду або відбування кримінального покарання;

– встановлення місцезнаходження та долі безвісти зниклих осіб.

Ефективне виконання зазначених завдань значною мірою залежить від застосування інтернет-ресурсів для пошуку доказів, спеціалізованих додатків для аналізу даних, а також використання функціональних підсистем єдиної інформаційної системи Міністерства внутрішніх справ України.

Перший розділ посібника присвячений аналізу електронних доказів та особливостям їх залучення до матеріалів справи. Значна увага приділяється забезпеченню цілісності електронних документів та проведенню експертизи електронних доказів, зокрема шляхом використання технологій хешування файлів. Описано методи документування вебконтенту, такі як створення скриншотів, фіксація вихідного коду вебсторінок та збереження змісту сайтів. Окремо розглянуто застосування протоколів Whois для отримання інформації про провайдера та власника сайту, а також методи виявлення IP-адреси комп'ютера в мережі з метою подальшого аналізу мережевого трафіку. Детально проаналізовано процес документування діяльності інтернет-наркомагазинів і представлено алгоритм встановлення осіб, причетних до незаконного обігу наркотичних засобів.

У другому розділі розглянуто роботу з пошуковими системами, зокрема з системою Google, з детальним аналізом використання пошукових операторів і методів розширеного пошуку. Висвітлено можливості використання потужних інструментів OSINT, таких як Maltego, та програмного забезпечення i2 Analysts Notebook, яке застосовується для аналізу великих масивів структурованих даних. Крім того, надано рекомендації щодо оптимізації робочого місця для проведення OSINT, включно з налаштуванням робочого комп'ютера та мережі.

Третій розділ присвячений єдиній інформаційній системі Міністерства внутрішніх справ України та її ключовим функціональним підсистемам, що є найбільш актуальними для оперативно-розшукової діяльності. Розглянуто такі підсистеми, як інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України», автоматизована інформаційна система оперативного призначення та «Оперативно-довідкова картотека».

У четвертому розділі досліджено основні аспекти функціонування Єдиного реєстру досудових розслідувань (ЄРДР). Описано його роль у процесі досудового розслідування, зокрема у забезпеченні централізованого збирання, зберігання та обліку інформації про кримінальні правопорушення. Визначено ключові функції та завдання ЄРДР, включаючи реєстрацію правопорушень, контроль за дотриманням законодавства під час досудового розслідування та забезпечення інформаційно-аналітичної підтримки діяльності правоохоронних органів.

У п'ятому розділі детально розглянуто поняття цифрової криміналістики, визначено її сутнісні характеристики та основні етапи, що включають збір, аналіз, збереження та представлення цифрових доказів. Проаналізовано різноманітні інструменти та методи, які використовуються в цифровій криміналістиці, включно зі спеціалізованим програмним забезпеченням для роботи з цифровими даними, що дозволяє ефективно проводити розслідування та збирати докази, які відповідають вимогам судових процесів.

Окрім того, у додатку А посібника наведені адреси сервісів і ресурсів, що можуть бути використані для пошуку або аналізу електронної пошти, зображень,

точок доступу Wi-Fi тощо. Додаток Б містить стислий опис інформаційних підсистем Інформаційного порталу Національної поліції України. Додатково в Додатку В зазначено витяги з нормативного документу стосовно загальних технічних вимог щодо технічних засобів для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій, а також Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів.

Матеріали посібника підготовлено з урахуванням робочих програм навчальних дисциплін, як: «Оперативно-розшукова діяльність», «Використання сучасних інформаційних технологій в оперативно-розшуковій діяльності», «Сучасні інформаційні технології в юридичній діяльності», «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції», які опановують здобувачі вищої освіти за спеціальностями 262 «Правоохоронна діяльність» та 081 «Право». Цей посібник буде корисним як для студентів, так і для практикуючих фахівців підрозділів Національної поліції, що здійснюють свою діяльність у сфері протидії організованій злочинності.

Розділ 1.
ЕЛЕКТРОННІ ДОКАЗИ

1.1 Загальні відомості.

Відповідно до частини першої статті 100 ЦПК України *електронними доказами* є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (у тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (у тому числі в мережі Інтернет).

Частиною другою статті 100 ЦПК України визначено, що електронні докази подаються в оригіналі або в електронній копії, засвідченій електронним підписом. Статтею 7 Закону України «Про електронні документи та електронний документообіг» визначено, що оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора.

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу. Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, у тому числі в паперовій копії.

Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму. Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму.

Електронний документ *не може бути застосовано як оригінал*, якщо це:

– свідоцтво про право на спадщину;

– документ, який, відповідно до законодавства, може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів;

– в інших випадках, передбачених законом.

Згідно зі статтею 12 Закону України «Про електронні документи та електронний документообіг», перевірка цілісності електронного документа може проводитися шляхом перевірки електронного цифрового підпису.

Для перевірки підписання документів електронним підписом можна скористатись онлайн-сервісом перевірки підпису на порталі «ДІЯ».

Огляд доказів за їх місцезнаходженням визначений статтею 85 ЦПК України. Письмові, речові та електронні докази, які не можна доставити до суду, оглядаються за їх місцезнаходженням.

Суд за заявою учасника справи чи з власної ініціативи може оглянути вебсайт, або сторінку сайту, інші місця збереження даних в мережі Інтернет з метою встановлення та фіксування їх змісту. У разі необхідності для проведення такого огляду суд може залучити спеціаліста.

Суд може призначити експертизу для встановлення та фіксування змісту вебсайту (сторінки), інших місць збереження даних у мережі Інтернет за умови, якщо це потребує спеціальних знань і не може бути здійснено судом самостійно або із залученням спеціаліста.

Про дату, час і місце огляду доказів за їх місцезнаходженням повідомляються учасники справи. Неявка цих осіб не є перешкодою для проведення огляду.

У разі необхідності, у тому числі за клопотанням учасника справи, для участі в огляді доказів за їх місцезнаходженням можуть бути залучені свідки, перекладачі, експерти, спеціалісти, а також здійснено фотографування, звуко- і відеозапис.

Суд забезпечує відеофіксацію огляду технічними засобами, якщо огляд здійснюється за відсутності хоча б однієї зі сторін, а також в інших випадках, коли суд визнає це за необхідне.

Про огляд доказів за їх місцезнаходженням складається протокол, що підписується всіма особами, які беруть участь в огляді. До протоколу додаються разом з описом усі складені або звірені під час огляду на місці плани, креслення, копії документів, а також зроблені під час огляду фотознімки, електронні копії доказів, відеозаписи тощо.

Суд під час розгляду справи повинен безпосередньо дослідити докази у справі: ознайомитися з письмовими та електронними доказами. Докази, що не були предметом дослідження в судовому засіданні, не можуть бути покладені судом в основу ухваленого судового рішення. Електронні докази оглядаються в судовому засіданні, за винятком випадків, передбачених ЦПК України, і пред'являються учасникам справи за їх клопотанням, а в разі необхідності – також свідкам, експертам, спеціалістам (частини перша–третя статті 229 ЦПК України).

Особи, яким пред'явлено для ознайомлення речові та електронні докази, можуть звернути увагу суду на ті чи інші обставини, пов'язані з оглядом. Ці заяви заносяться до протоколу судового засідання (частина перша статті 237 ЦПК України).

Протоколи огляду речових та електронних доказів, складені в порядку забезпечення доказів, виконання судового доручення або за результатами огляду доказів на місці, за клопотанням учасника справи оголошуються в судовому засіданні. Учасники справи можуть дати свої пояснення з приводу цих протоколів. Учасники справи можуть ставити питання з приводу речових та

електронних доказів свідкам, а також експертам, спеціалістам, які їх оглядали (стаття 237 ЦПК України).

Електронні письмові документи досліджуються в порядку, передбаченому для дослідження письмових доказів за статтею 235 ЦПК України.

Відтворення звукозапису, демонстрація відеозапису і їх дослідження проводяться в судовому засіданні або в іншому приміщенні, спеціально підготовленому для цього, з відображенням у протоколі судового засідання особливостей оголошуваних матеріалів і зазначенням часу демонстрації. Після цього суд заслуховує пояснення учасників справи (стаття 238 ЦПК України).

Відтворення звукозапису, демонстрації відеозапису, що мають приватний характер, а також їх дослідження проводиться за правилами щодо оголошення й дослідження змісту особистого листування і телеграфних повідомлень лише за згодою осіб, визначених Цивільним кодексом України (частина восьма статті 7, стаття 236, частина перша статті 238 ЦПК України).

Оригінали або копії електронних доказів зберігаються в суді в матеріалах справи. За клопотанням особи, яка надала суду оригінал електронного доказу на матеріальному носії, суд повертає такий матеріальний носій, на якому міститься оригінал доказу, цій особі після дослідження вказаного електронного доказу, якщо це можливо без шкоди для розгляду справи, або після набрання судовим рішенням законної сили. У матеріалах справи залишається засвідчена суддею копія електронного доказу або витяг із нього (стаття 101 ЦПК України).

Позиція Верховного Суду щодо визнання скриншотів електронного листування як електронного доказу є різною. Зокрема, Верховний Суд вважає, що роздруківка електронного листування не може вважатися електронним документом відповідно до положень ч. 1 ст. 5 Закону України «Про електронні документи та електронний документообіг», тобто не може вважатися доказом, адже не містить електронного підпису, який є обов'язковим реквізитом електронного документа, оскільки в такому випадку неможливо ідентифікувати відправника повідомлення, а зміст такого документа не захищений від внесення правок і викривлення.

До матеріалів справи можуть долучатися роздруківки електронних доказів: вебсторінок, листування у месенджерах та електронною поштою. Перед поданням до суду такі копії необхідно засвідчувати за правилами Державного стандарту України («Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів»).

Електронні докази є окремим засобом доказування, до яких так само висуваються вимоги щодо їх належності, допустимості, достовірності та достатності. Однак, у разі виникнення спору, інша сторона може змінити або ж видалити певну інформацію, що зафіксована або передавалася онлайн. Наприклад, сторінки та матеріали в мережі Інтернет, листування в месенджерах тощо можна видалити в будь-який момент. Для протидії цьому існують певні механізми фіксації змісту електронних доказів.

Проведення певної експертизи дозволяє встановити факт розміщення контенту в мережі Інтернет станом на конкретний момент часу для доказування:

– поширення недостовірної інформації;
– незаконного використання об’єктів права інтелектуальної власності;
– недобросовісного використання доменного імені;
– незаконного продажу фальсифікованої продукції;
– розміщення контенту, власником та/або автором якого є заінтересована особа.

Зазвичай висновок експерта є вагомим доказом під час вирішення справи. Судовий експерт – це особа, яка володіє спеціальними знаннями, які є необхідними для з’ясування певних обставин справи та повідомлена про кримінальну відповідальність за дачу завідомо неправдивого висновку. Однак тривалий час виготовлення висновку та висока вартість послуг експерта є тим фактором, що змушує сторін спору звертатися до інших способів фіксації інформації в мережі.

За експертним висновком можна звернутися до Центру компетенції адресного простору мережі Інтернет. Центр може підготувати звіт за

результатами фіксації змісту вебсторінки в мережі станом на певний момент часу та виготовити довідки щодо власників вебсайту. Зважаючи на практику, суди надають оцінку та враховують такі звіти та довідки під час вирішення спорів. Варто наголосити на швидкості виготовлення звіту (5 робочих днів з моменту оплати), а також можливість замовлення та отримання звіту онлайн.

Ще одна можливість – це використання ресурсів архівації мережі Інтернет (www.web.archive.org). Цей спосіб фіксації використовується для доведення наявності або відсутності змін тієї чи іншої сторінки в мережі. Відомості з такого ресурсу сторони можуть самостійно зафіксувати в протоколі. Експерти теж звертаються до цього ресурсу.

Як свідчить практика, суди враховують інформацію з указаного ресурсу. Наприклад, у справі № 910/13940/18 судовий експерт послався на відомості з цього сайту, які підтверджували зміну умов надання банківських послуг, що стало однією з підстав для відмови в позові.

1.2. Хеш файлу.

Переважна кількість електронних доказів може бути збережена у вигляді файлу, причому формат файлу може бути як текстовим, так й іншим (графічним, звуковим і т.ін.). Причому, ці цифрові джерела інформації також, як і звичайні джерела доказів, повинні відображати ті ж самі обставини і фактичну інформацію, які існували на момент вчинення правопорушення і, відповідно, потребують демонстрації того, що дані не піддавалися змінам, додаванню або видаленню і в них не вносилися (не можуть бути внесені) ніякі правки. Щоби бути впевненим, що файл не зазнав змін, використовують хеш-суму файлу.

Хеш файлу (хеш-сума) – це унікальний ідентифікатор файлу (рядок із букв і цифр), який обчислюється комп'ютером за допомогою певних математичних перетворень (алгоритмів) та спеціального програмного забезпечення.

Узагалі, кожен файл має певні ідентифікуючі властивості: формат, ім'я, розмір та ін. Але жодна з цих властивостей не є унікальним і не дозволяє однозначно ідентифікувати кожен файл. Наприклад, може існувати кілька файлів одного формату (наприклад, docx), однакового розміру та з однаковими іменами, що відрізняються при цьому за змістом. Проблему унікальної ідентифікації вирішує хеш-сума (контрольна сума, digest - дайджест) файлу.

Файли з однаковими хешами завжди є точними копіями один одного, навіть якщо в них різні імена та (або) розширення. Зміна вмісту файлу автоматично тягне зміну його хеша. Існує кілька загальноприйнятих алгоритмів (стандартів) розрахунку хешу. Найчастіше використовуються алгоритми: SHA-1, MD5, CRC. Хеші одного і того ж файлу, розраховані за різними алгоритмами, відрізнятимуться.

Розглянемо питання отримання контрольної (хеш) суми файлу. Найпростішим способом є використання контекстного меню Windows (Рис. 1).

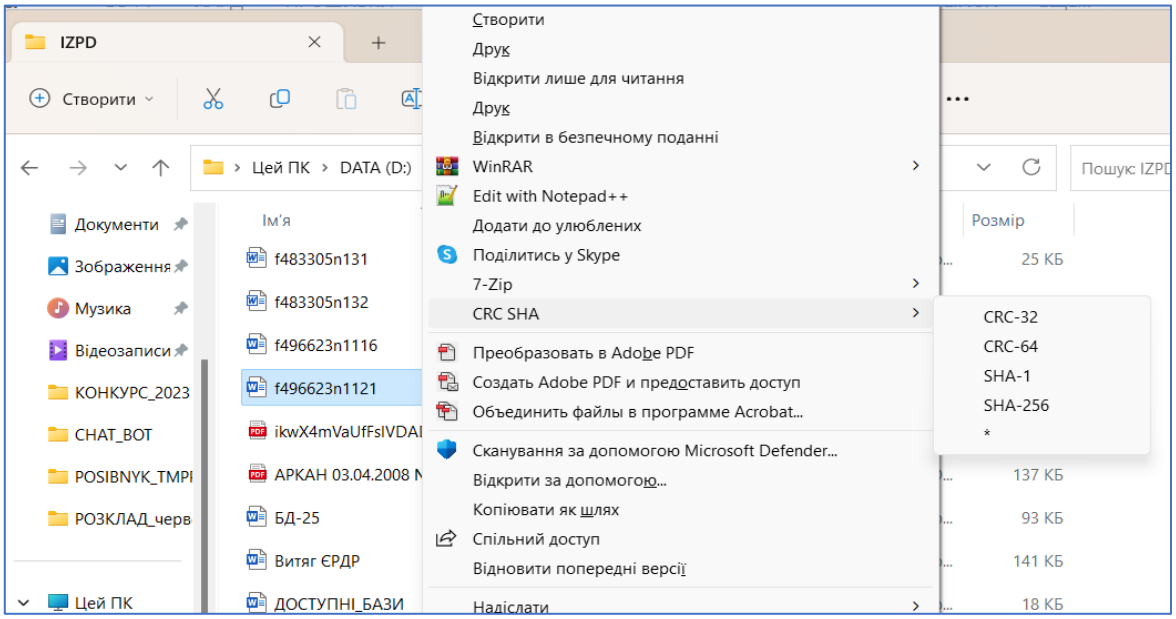

Рис. 1. Отримання контрольної (хеш) суми файлу за допомогою контекстного меню Windows.

Відкриваємо файловий провідник і встановлюємо курсор на відповідний файл. Затискаємо клавішу Shift та клацаємо правою кнопкою миші на файл. На Рис. 1 бачимо, що пропонується використати на вибір різні алгоритми – CRC-32,

CRC-64, SHA-1 і т.ін. Для прикладу виберемо алгоритм SHA-1. Отримаємо вікно з інформацією про контрольну суму файлу (Рис. 2).

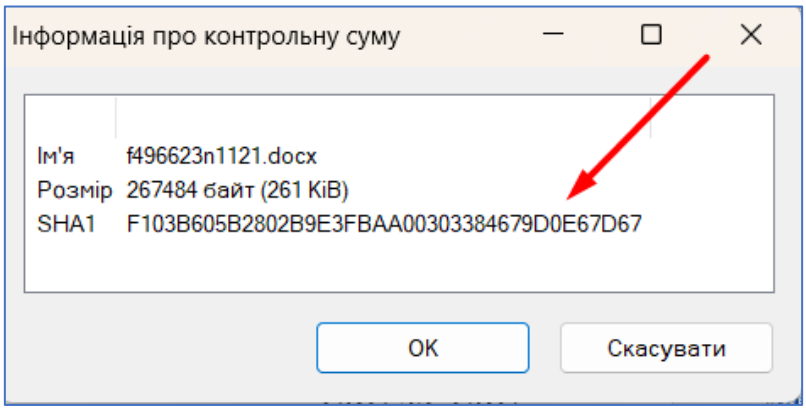

Рис. 2. Вікно з інформацією про контрольну суму файлу, згенерованою за допомогою алгоритму SHA-1.

Інший спосіб отримання хеш файлу – це використання командного рядка. Щоб зайти в командний рядок, тиснемо **Win + R**, у поле «Відкрити» пишемо cmd і тиснемо OK (Рис. 3).

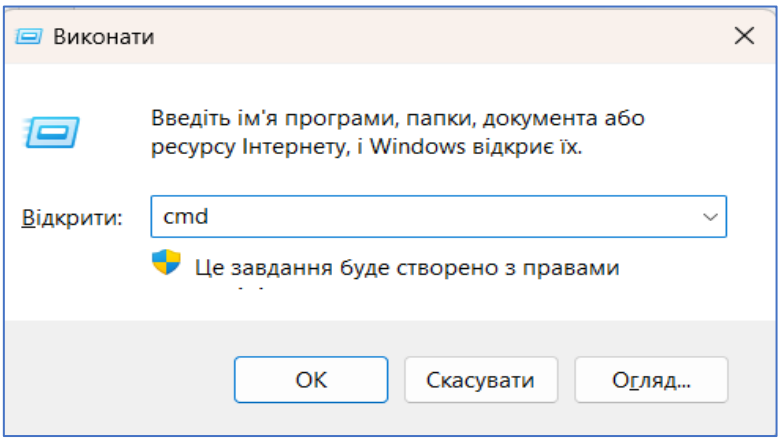

Рис. 3. Вікно команди "Виконати" для відкриття командного рядка (cmd) у Windows.

Відкриється вікно командного рядка (Рис. 4).

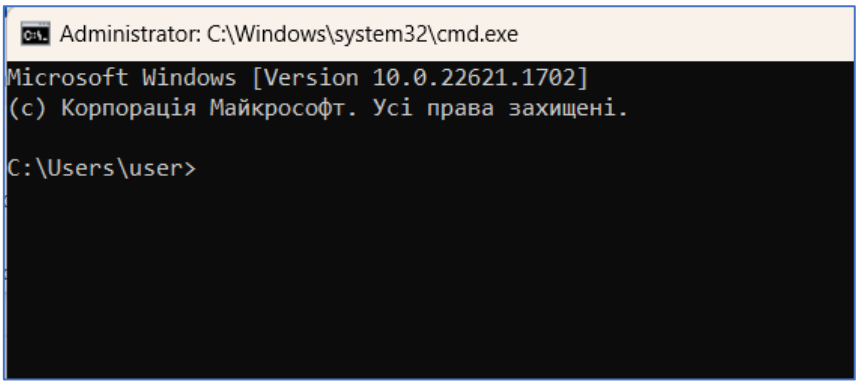

Рис. 4. Вікно командного рядка після запуску з використанням команди "cmd".

Далі звертаємося до вбудованої утиліти Certutil. Синтаксис утиліти:

CertUtil [Параметри] -hashfile InFile [HashAlgorithm]

На Рис. 5 бачимо приклад використання утиліти certutil. Команда дозволяє створити та відобразити криптографічний хеш файлу.

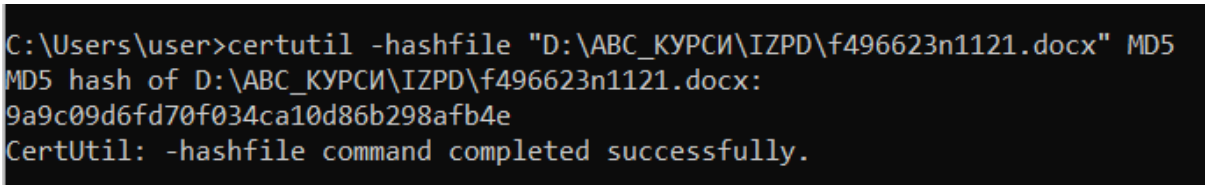

Рис. 5. Використання утиліти Certutil для створення та відображення криптографічного хешу файлу.

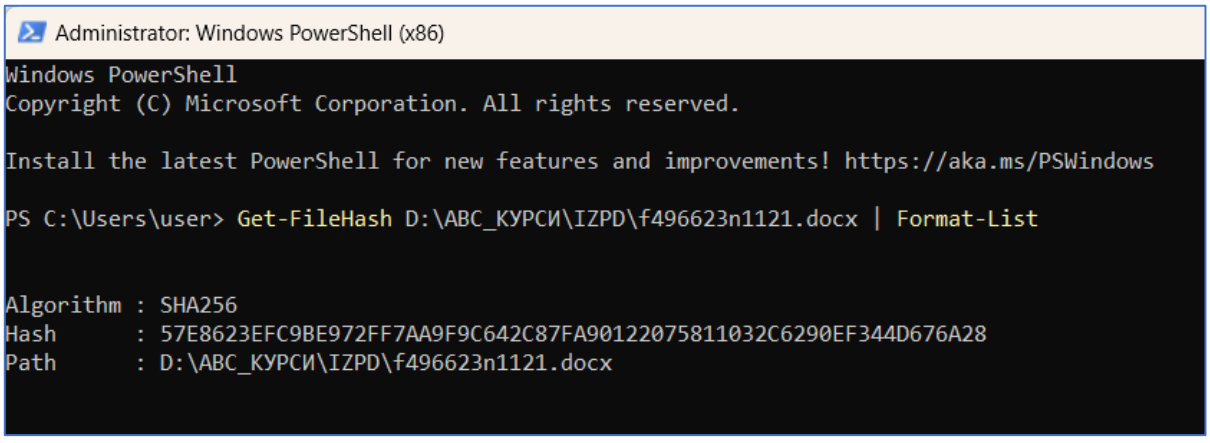

Рис. 6. Використання команди Get-FileHash в оболонці Windows PowerShell для отримання контрольної суми файлу з використанням алгоритму SHA-256.

Крім командного рядка, схожу операцію можна виконати і в оболонці Windows PowerShell за допомогою команди Get-FileHash (Рис. 6).

Синтаксис команди:

Get-FileHash шлях до файлу | Format-List, або можна вказати конкретний алгоритм створення контрольної суми:

Get-FileHash шлях до файлу -Algorithm MD5 | Format-List

Нарешті, для отримання контрольної суми файлу можна встановити програму HashTab. Фактично, це є розширенням для файлового провідника Windows. Тобто, у файловому менеджері ставимо курсор на файл, правою клавішою миші відкриваємо контекстне меню і вибираємо «Властивості». У вікні «Файл – властивості» (Рис. 7) після встановлення програми HashTab з'явиться нова вкладка «Хеши файлу». Можна бачити відразу декілька контрольних сум для цього файлу, які обчислені за різними алгоритмами. Навіть більше, на цій вкладці є можливість порівняти хеш взятого файлу з хешем іншого файлу. Якраз ця операція й потрібна для порівняння електронного доказу з оригіналом.

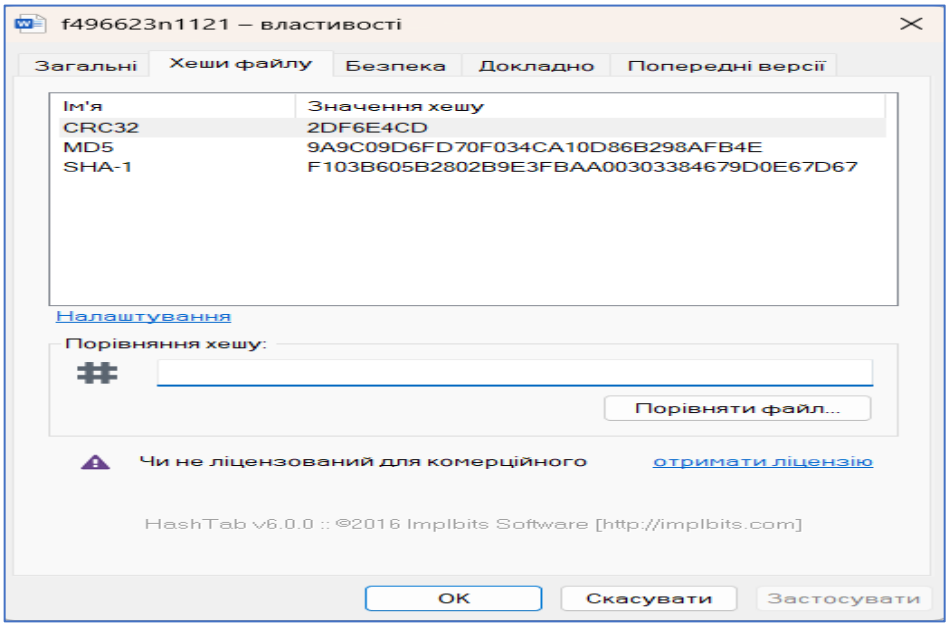

Рис. 7. Використання програми HashTab для отримання контрольних сум файлу в провіднику Windows.

1.3. Документування вебконтенту.

Нині вже напрацьована практика документування вебконтенту та використання одержаних доказів у кримінальному процесі. Під загальним поняттям вебконтенту будемо розуміти звичайні вебсайти, сайти соціальних мереж, сайти електронної пошти, однорангові (P2P) мережі. Документування вебконтенту може відбуватися в різних формах: можна створити звичайні скриншоти відкритих сторінок (сайтів, електронних листів, зображень і т.ін.), є можливість зберегти зміст усього сайту або зберегти вихідний код вебсторінок, який може мати потрібні коментарі користувача/розробника, (паролі, ідентифікатори, посилання на місце розташування, посилання на зовнішні сайти). Також можна відпрацювати доменне ім'я сайту, визначитись із метаданими сайту (коли створено, дані провайдера, дані замовника і т.ін.).

Фіксація вихідного коду вебсторінки. Вихідний код вебсторінок є не що інше, як набір HTML-тегів для розмітки тексту та інших елементів вебсторінки, і може містити різні корисні для доказів посилання (Рис. 8).

```
<!DOCTYPE html>
<!--[if !(IE 6) | !(IE 7) | !(IE 8)  ]><!-->
<html lang="uk" class="no-js">
<!--<![endif]-->
<head>
    <meta charset="UTF-8" />
        <meta name="viewport" content="width=device-width, initial-scale=1, maximum-sca
        <meta name="theme-color" content="#024f94"/>    <link rel="profile" href="https
    <meta name='robots' content='index, follow, max-image-preview:large, max-snippet:-1

    <!-- This site is optimized with the Yoast SEO plugin v20.11 - https://yoast.com/wo
    <title>Донецький державний університет внутрішніх справ (ДонДУВС)</title>
    <meta name="description" content="Донецький державний університет внутрішніх справ
    <link rel="canonical" href="https://dnuvs.ukr.education/" />
    <meta property="og:locale" content="uk_UA" />
    <meta property="og:type" content="website" />
    <meta property="og:title" content="Донецький державний університет внутрішніх справ
    <meta property="og:description" content="ДонДУВС - Донецький державний університет
    <meta property="og:url" content="https://dnuvs.ukr.education/" />
    <meta property="og:site_name" content="ДонДУВС" />
```

Рис. 8. Приклад вихідного коду вебсторінки з HTML-тегами й метаданими.

Щоб проглянути вихідний код вебсторінки, треба поставити курсор на вільному полі вебсторінки і клацнути праву клавішу миші. Відкриється діалогове вікно, де вибирають «Вихідний код сторінки». Після цього відкриється нова сторінка в браузері з HTML-кодом веб-сторінки. Можна скопіювати весь код у буфер пам’яті та зберегти в текстовому документі. Зберегти HTML-код можна й інакше: знаходячись на вебсторінці, відкриваємо вкладку «Файл» браузера та вибираємо «Зберегти як». Відкриється вікно «Збереження файлу» (Рис. 9). Вибираємо типфайлу – «Вебсторінка, тільки HTML» і зберігаємо.

Після збереження відповідних файлів потрібно обчислити їх геш-суму з метою подальшого контролю цілісності отриманої інформації.

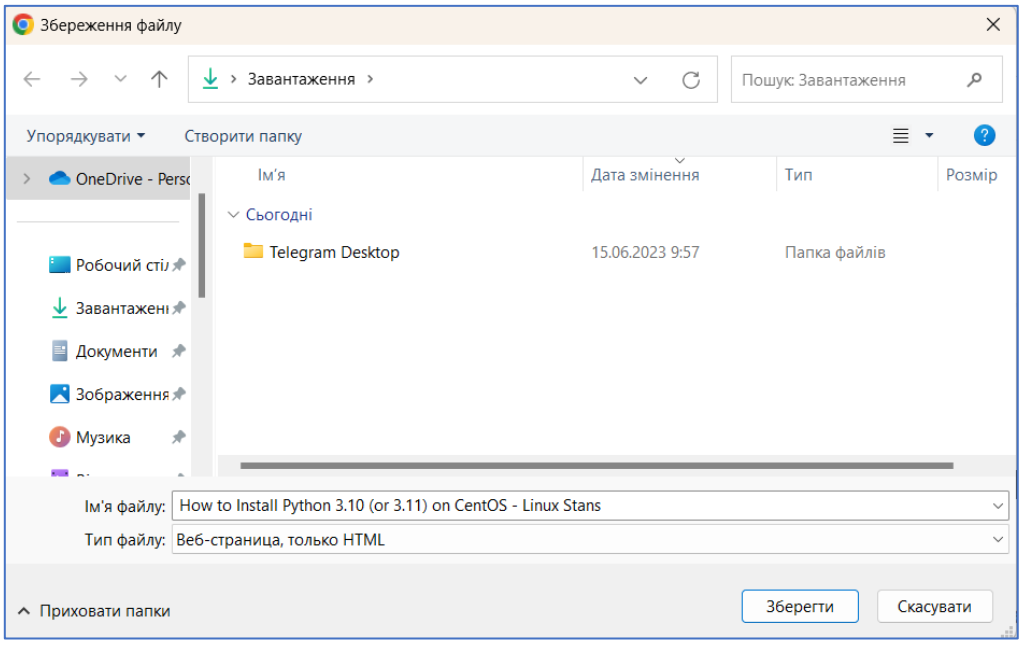

Рис. 9. Процес збереження HTML-коду вебсторінки.

Фіксація сайту. З метою фіксації вмісту всього вебсайту, а не окремої вебсторінки, можна створити копію сайту для перегляду в автономному режимі, наприклад, за допомогою програми HTTrack Website Copier, яка завантажує пов’язані вебоб’єкти за визначеною глибиною і дозволяє відкрити вебсайт з усіма зображеннями в автономному режимі (Рис. 10). Підтримується режим автоматичної перевірки та оновлення локальної копії, у цьому випадку вийде щось на зразок автономного дзеркала сайту.

Треба додати, що всі дії, які виконуються з приводу документування вебконтенту, можуть супроводжуватися зйомкою на відеокамеру (підробити відеозапис набагато складніше, ніж скриншот). Далі можна визначити геш відеофайлу та додати до цього характер аберації об'єктива (для підтвердження відзнятого матеріалу шляхом порівняння). Замість відеокамери, можна використати спеціальні додатки для відеозахоплення екрану (наприклад, CamStudio, OBS Studio, Bandicam).

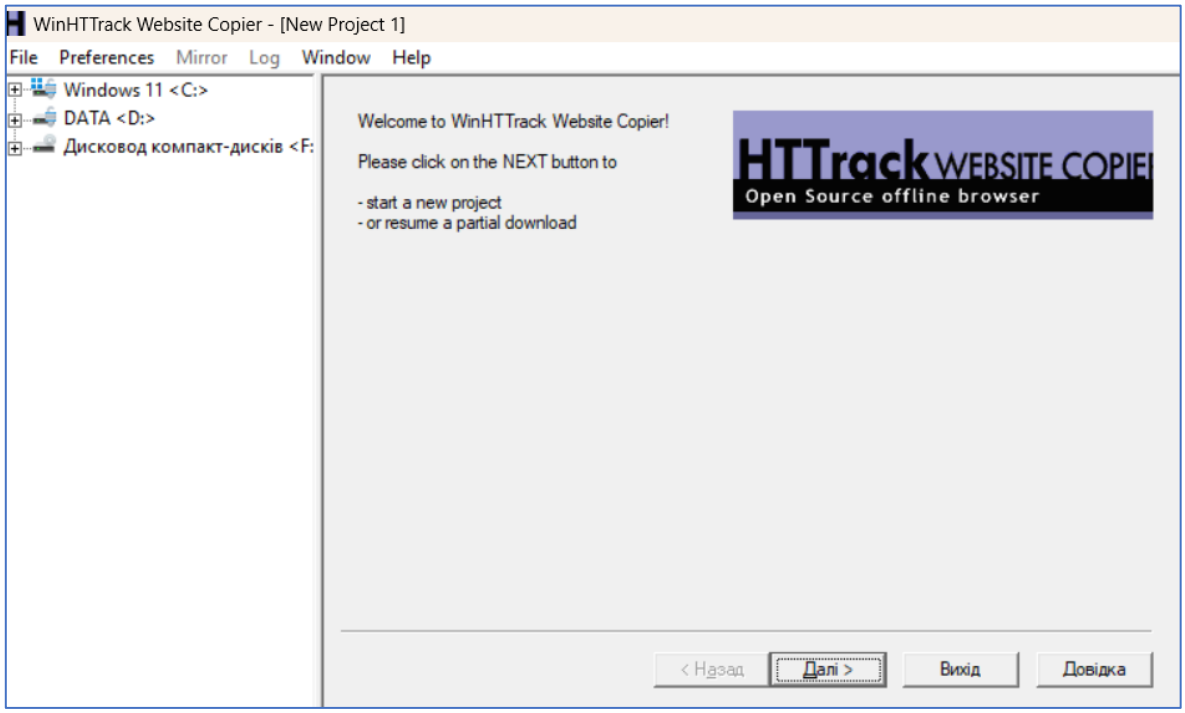

Рис. 10. Використання програми HTTrack Website Copier для створення копії вебсайту в автономному режимі.

1.4. Ідентифікація об’єктів в мережі Інтернет.

1.4.1. Протокол Whois.

Для встановлення осіб, які використовують вебсайти для протиправних дій, існують певні алгоритми дій і заходів. Основну увагу звертають на таке, як:

- конкретно, яка особа замовила виготовлення сайту;
- хто сплачує послуги адміністрування сайту;
- хто наповнює сайт відповідним контентом (фотографії, номера мобільних телефонів тощо);

Відповіді на ці питання можна знайти, якщо скористатися **сервісами Whois**. Whois (від англійської "who is" – "хто такий") – спеціальний мережевий протокол, який базується на протоколі TCP (використовується порт 43). Регулює службу Whois Міжнародна корпорація із присвоєння імен та номерів (ICANN). Його основне завдання – отримання реєстраційних даних про доменні імена та їх власників. Крім того, Whois-сервіс використовується для отримання інформації про мережеві блоки IP-адрес, а також інформації про організації або фізичні особи, які є власниками того чи іншого блоку IP.

Сервіс Whois дозволяє визначити належність IP-адресу тому чи іншому провайдеру, а також отримати інформацію про географію застосування шуканого IP, іншу технічну або контактну інформацію. Важливість цих даних дуже велика, оскільки вони дозволяють швидко визначити власника IP або, наприклад, отримати контакти провайдера для звернення в разі порушення з боку його абонентів.

Перевірка Whois (Check Whois) доменного імені зазвичай містить докладну інформацію щодо шуканого домену, яка включає: дату та час реєстрації, дату та час закінчення делегування доменного імені, поточні DNS-сервери домену, його статуси, а також інформацію про реєстранта – власника доменного імені. У випадку, якщо доменне ім'я не існує, то відповідь на Whios-запит міститиме відповідь про те, що доменне ім'я не знайдено. У деяких

випадках, якщо доменна зона не надає інформацію про власника доменного імені в результатах Whois-запитів, сервіс Whois може запитувати цю інформацію в реєстратора домену.

Серед сервісів Whois можна запропонувати DOMAINTOOLS.COM (Рис. 11).

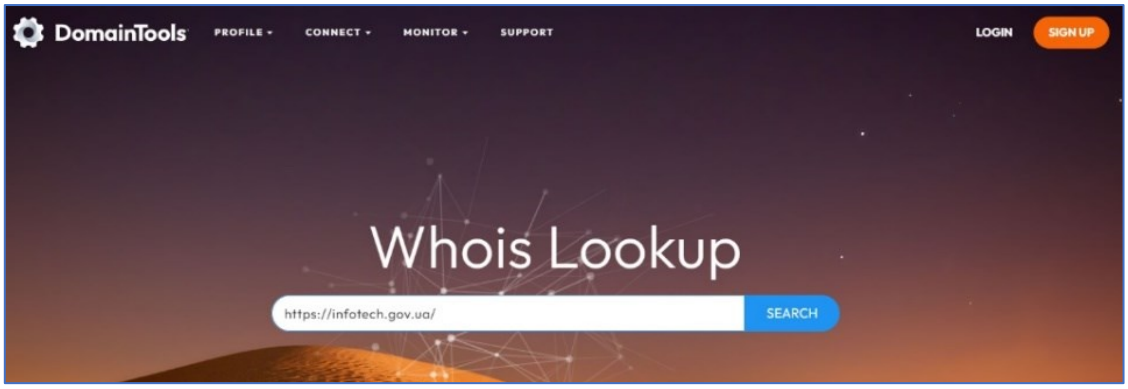

Рис. 11. Інтерфейс сервісу DOMAINTOOLS.COM для перевірки інформації за допомогою Whois Lookup

У полі пошуку ми вже добавили домен сайту, про який хочемо отримати інформацію. На Рис. 12 та Рис. 13 можна бачити надану сервісом відповідну інформацію, щодо дати створення сайту, терміну закінчення послуги, IP-адресу, місцезнаходження провайдера, власника доменного імені (на кого зареєстровано) та інше.

Whois Record for InfoTech.gov.ua

— Domain Profile

Registrar Status	OK-UNTIL
Dates	Created on 0-UANIC 20181009141533 Whois History Expires on 2023-10-09 Updated on UARR149-UANIC 20230414140357
Name Servers	ANIRBAN.NS.CLOUDFLARE.COM (has 25,240,801 domains) WANDA.NS.CLOUDFLARE.COM (has 25,240,801 domains)
Tech Contact	—
IP Address	91.197.4.10 is hosted on a dedicated server
IP Location	- Kyiv Misto - Kyiv - State Enterprise Infotech
ASN	AS201369 INFOTECH STATE ENTERPRISE "INFOTECH", UA (registered Apr 24, 2023)
IP History	1 change on 1 unique IP addresses over 0 years
Hosting History	2 changes on 3 unique name servers over 5 years

Whois Record (last updated on 2023-06-17)

Рис. 12. Результати запиту Whois для домену InfoTech.gov.ua

Рис. 13. Детальна інформація з бази даних Whois про домен InfoTech.gov.ua

Після встановлення з використанням сервісів Whois інформації про володільця сайту (або замовника для цього сайту послуги хостингу), відомості про правопорушника можна отримати, надіславши провайдеру (оператору) телекомунікацій відповідний запит. Паралельно в рамках відкритого кримінального провадження слід ініціювати одержання вказаних даних через процедуру тимчасового доступу до речей і документів.

1.4.2. Ідентифікація комп’ютера в Інтернеті.

Кожен комп'ютер або пристрій, що підключається до Інтернету, отримує унікальну IP-адресу. Якщо ми знаємо IP-адресу комп’ютера, то скориставшись протоколом Whois, ми зможемо отримати інформацію про провайдера, який надає послуги доступу до Інтернету особі, яка пов’язана з цим комп’ютером. А далі, звернувшись до провайдера, можемо отримати інформацію щодо самій особи.

Як можна дізнатись IP-адресу конкретного комп’ютера? Це питання вирішується по-різному, залежно від того, якою вихідною інформацією ми володіємо. Однак, який би метод отримання IP чужого комп’ютера ми не вибрали, у будь-якому випадку доведеться вступати в контакт з його власником або іншими людьми , які будуть в курсі наших намірів. По-перше, це може бути листування електронною поштою. Мейли, крім тексту відправника, містить метадані, серед яких є IP. У більшості випадків отримання IP відбувається за допомогою спеціально згенерованого лінка («гачка»), який і збере необхідні дані.

Існує декілька сервісів в Інтернеті, які дозволяють створювати лінк-гачок (лінк-логер). Ми розглянемо IP-Logger (Рис. 14). Серед різних інструментів, які пропонує вказаний сервіс, вибираємо Tracking Pixel > Create Pixel. Відкриється вікно (Рис. 14), у якому ми побачимо вже згенерований лінк-гачок (червоним шрифтом) і посилання на сторінку статистики.

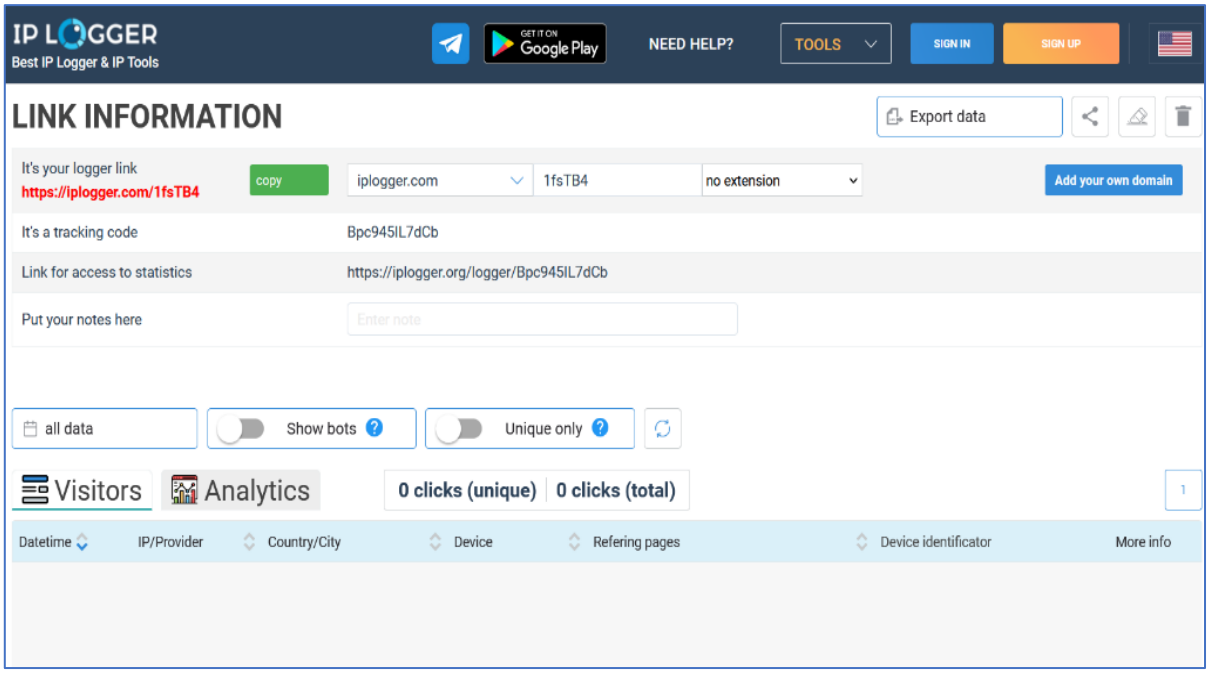

Рис. 14. Сторінка IP-логгера із відображенням статистики переходів за посиланням.

Для отримання IP-адреси іншого комп'ютера необхідно, щоб користувач цього комп'ютера перейшов за спеціальним посиланням-логером. Це посилання можна розмістити у повідомленнях у месенджерах, на сторінках соціальних

мереж, на певному вебсайті або надіслати електронною поштою. Також це посилання можна замаскувати під зображення або текст. Як тільки хтось переходить за цим посиланням, його IP-адреса реєструється в журналі статистики (Рис. 14, знизу). Крім IP-адреси, IP-логер визначає орієнтовне місцезнаходження комп'ютера. Важливо зазначити, що якщо користувач використовує VPN або подібну технологію, то визначити його справжнє місцезнаходження буде неможливо.

1.5. Аналізатори трафіка.

Після встановлення місцезнаходження потрібного комп'ютера (його IP-адреси та адреси провайдера) для збору необхідних доказів можна застосувати аналізатор трафіку.

Аналізатор трафіку (аналізатор мережевих пакетів) – це програмно-апаратний комплекс (прилад, або додаток), який уміє робити захоплення мережевого трафіку з подальшим його глибоким аналізом – DPI (Deep Packet Inspection), виконувати мережевий аналіз, проводити тестування пропускної спроможності та продуктивності мережі. Це спеціалізовані діагностичні утиліти, що дають можливість «слухати» мережевий трафік та аналізувати його на рівні одиниць передачі окремих протоколів. На професійному жаргоні їх називають сніфферами.

Одним із найпоширеніших і найпопулярніших аналізаторів трафіку сьогодні є Wireshark, що розповсюджується під ліцензією GNU GPL. Існують версії Wireshark для різних операційних систем: Linux, Windows, MacOS, FreeBSD, Solaris.

Перехопити трафік через сніффер можна наступними способами:

- шляхом прослуховування у звичайному режимі мережного інтерфейсу;
- підключенням до розриву каналу;
- перенаправленням трафіку;

- за допомогою аналізу побічних електромагнітних випромінювань;
- за допомогою атаки на рівень каналу та мережі, що призводить до зміни мережевих маршрутів.

Сніффер дозволяє перехопити будь-який зашифрований чи незашифрований трафік користувача (включаючи паролі та інші цінні дані). Отже, з одного боку, сніффер може бути використаний зловмисниками в незаконною метою. З іншого боку, це дуже корисний інструмент для отримання електронних доказів протиправної діяльності.

1.6. Документування «інтернет-магазинів», які використовуються в злочинних цілях.

Швидкий розвиток інформаційних технологій має суттєвий вплив на всі сфери життєдіяльності людей. Це відноситься і до поширення різноманітних інтернет-магазинів, які використовуються в злочинних цілях. Найчастіше злочинці створюють інтернет-магазини для незаконного збуту наркотичних засобів, психотропних речовин, прекурсорів.

Як приклад, розглянемо документування інтернет-магазинів по збуту наркотиків.

Продаж і просування наркотиків та психотропів, як правило, відбувається через мережу т.зв. «онлайн-магазинів». Мережа може складатися зі взаємопов’язаних ботів, чатів та каналів у месенджері Telegram, так званих «шопів». Оплата відбувається в криптовалюті або на анонімні електронні гаманці «ділка». Для цього використовуються такі платіжні системи, як GlobalMoney, EasyPay, з яких кошти виводяться на особисті банківські рахунки. Збут наркотичних засобів покупцям здійснюється безконтактно, шляхом схованок (так званих «закладок») або надсиланням через компанії, що надають послуги експрес-доставки: ТОВ «Нова Пошта», «Ін-тайм», «Делівері» тощо.

Спосіб розповсюдження наркотичних засобів та схема розрахунку проводиться наступним чином: у групі месенджера Telegram споживач наркотиків пише оператору або телеграм-боту, у якому місті він знаходиться, яку речовину планує придбати та її кількість. Після того споживач отримує повідомлення, у якому зазначається вартість вибраної речовини та номер електронного гаманця, на який необхідно здійснити переказ вказаної суми. Сплативши вказану суму на електронний гаманець, споживач відправляє оператору або телеграм-боту електрофотокопію квитанції про здійснення оплати. Перевіривши оплату, оператор або телеграм-бот, надсилає споживачу фотографію місця із зазначенням адреси та місця, де знаходиться схованка з речовиною.

У залежності від місця та масштабу злочинної діяльності інтернет-наркомагазини можна диференціювати: місцеві (які діють у межах одного міста чи району), регіональні (у межах міст області), міжрегіональні (які діють у межах країни) та міжнародні.

Окремими ознаками, що характеризують злочинну діяльність регіональних, міжрегіональних та міжнародних інтернет-наркомагазинів, є:

- значна кількість учасників;
- наявність самостійних структурних підрозділів, які територіально та функціонально відокремлені між собою, але ними керує єдиний керівник та вони реалізують спільні злочинні наміри в даній сфері;
- використання багатоплатформових месенджерів для смартфонів та інших пристроїв, що дозволяє обмінюватися текстовими повідомленнями та медіафайлами різних форматів (як правило, використовується месенджер Telegram);
- застосування комплексу заходів, що забезпечує високий рівень конспірації;
- чіткий розподіл функцій та обов’язків кожного учасника групи, систему заохочень та покарань;

- використання електронних грошей або криптовалют при здійсненні механізму злочинної діяльності.

За розподілом функцій учасників інтернет-наркомагазинів їх можна поділити на: організаторів, операторів, кур'єрів, зберігальників, фасувальників, закладників, пособників.

Так організатор здійснює підбір учасників групи, загальне керівництво, що проявляється в об'єднанні, спрямуванні та координації зусиль учасників на вчинення злочинів, плануванні та розподілі обов'язків між учасниками групи, встановлює систему заохочень та покарань, ціну на наркотичні засоби, розподіляє грошові кошти, отримані від збуту наркотичних засобів тощо. Керування членами групи організатор здійснює з дотриманням конспірації через месенджер, і, як правило, всіх членів групи знає лише організатор, інші учасники можуть не знати один одного.

Оператор через месенджер отримує інформацію від наркозалежних осіб про необхідну кількість наркотичного засобу, вказує покупцю електронний гаманець для оплати та після підтвердження отримання коштів від покупців на електронний гаманець відправляє повідомлення в Telegram про місцезнаходження «схованки» з наркотичним засобом. Функцію оператора може виконувати програма бот. За оренду програми бот організатор здійснює оплату або купує її.

Кур'єр, за вказівкою організатора, через компанії, що надають послуги експрес-доставки: ТОВ «Нова Пошта», «Ін-тайм», «Делівері», тощо – отримують або відправляють в інші міста наркотичні засоби, можуть доставляти наркотичні засоби до зберігальника, від зберігальника – до фасувальника, від фасувальника – до закладника. Як, правило, з метою конспірації, кур'єр передає наркотичні засоби іншим членам групи безконтактно – шляхом «схованок». Місце схованки відправляє повідомленням у месенджере Telegram.

Зберігальник. Його функція – це зберігання наркотичних засобів інтернет-наркомагазину. На кримінальному сленгу – «склад». Для організації безперебійного збуту наркотичних засобів організатори можуть створювати по

одному та декілька, так званих «складів», у кожному місті або районі, де здійснюється збут наркотичних засобів через інтернет-магазин.

Фасувальник. Його функція – це фасування наркотичних засобів у «закладки» для подальшого збуту за видом та масою, згідно прайсу інтернет-наркомагазину. Як правило, при фасуванні наркотичних засобів для дрібного збуту, використовуються поліетиленові пакетики з застібкою системи «Zipp-Lock», які замотуються в ізоляційну стрічку. Фасувальник фасує «закладки» та формує, так звані «майстер-клади» – дрібнооптові партії «закладок», які в подальшому отримує закладник. Щоб не переплутати вид та масу наркотичного засобу в «закладці», використовують різні кольори ізоляційних стрічок.

Закладник забирає дрібнооптові партії наркотичних засобів, так звані «майстер-клади», та кожну окрему «закладку» поміщає в окрему схованку. При тому він повинен дотримуватися правил обладнання схованок таким чином, щоб забезпечити надійність та якість «закладки» без пошкоджень до моменту безпосередньої реалізації. Зробивши схованку, закладник максимально повно, точно й доступно повинен описати її місце знаходження шляхом складання повідомлень, що містять достатню кількість друкованого тексту, використовуючи для цього встановлювані орієнтири, і докласти до них панорамну фотографію. Після здійснення схованки інформацію про схованку він спрямовує організатору або оператору.

Пособник. До цієї категорії належать особи, задіяні в рекламі інтернет-наркомагазину та вербуванні інших учасників. Для реклами своїх інтернет-наркомагазинів організатори використовують наступні способи: нанесення рекламних написів інтернет-адрес з продажу наркотичних засобів на парканах та стінах будинків, гаражів та інших споруд; розповсюдження серед споживачів наркотиків та молоді візиток із вказівкою інтернет-адрес з продажу наркотиків; наклеювання в під'їздах будинків, інших місцях масового перебування громадян постерів з рекламою інтернет-адрес з продажу наркотиків; викладення в YouTube або в чатах споживачів наркотиків роликів із рекламою інтернет-адрес з продажу наркотиків. За рекламу інтернет-наркомагазину в чатах споживачів наркотиків

організатор здійснює оплату адміністратору чату. Крім того, якщо раніше організатори інтернет-наркомагазину здійснювали вербовку інших учасників через власний інтернет-магазин, то останнім часом вони частіше звертаються до адміністраторів чатів споживачів наркотиків, де останні за плату в чаті викладають інформацію про наявність разової або постійної роботи в інтернет-наркомагазині та стикують бажаючих з організатором.

Кожний учасник інтернет-наркомагазину може виконувати декілька функцій, а якщо він дрібний місцевий, то всі функції може здійснити і сам організатор. Крім того, оскільки для збуту наркотичних засобів використовується Всесвітня мережа Інтернет, то з метою конспірації, деякі учасники групи, такі як організатор чи/та оператор, то під час збуту вони можуть перебувати в іншій країні від місця збуту.

Одним із шляхів встановлення таких осіб – це відпрацювання інформації по відомих номерах електронних гаманців системи прийому платежів (облікових записах користувача).

Як правило, інтернет-наркомагазини використовують декілька номерів електронних гаманців. Інформацію про номери електронних гаманців можна отримати від споживачів наркотиків, які купували наркотичні засоби в конкретному інтернет-наркомагазині, або зайти на сайт інтернет-магазина, або акаунт оператора наркомагазина в месенджері Telegram, та в переписці з оператором отримати інформацію про номер електронного гаманця без подальшої купівлі наркотичного засобу.

Якщо вже відкрито кримінальне провадження за незаконний збут наркотичних засобів, то інформацію про номер електронного гаманця можна отримати під час негласної слідчої (розшукової) дії передбаченої ст. 271 КПК України – контроль за вчиненням злочину, яка проводиться на підставі постанови прокурора.

Після отримання інформації про номери електронних гаманців, які використовуються для збуту наркотичних засобів, оперативним підрозділом на підставі п. 15 ч. 1 ст. 8, ч. 1 ст. 11 Закону України «Про оперативно-розшукову

діяльність» від 18 лютого 1992 року № 2135-XII, ч. 1 ст. 7 Закону України «Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними» від 15.02.1995 року, яка гласить: «На письмову вимогу державних органів (підрозділів), які мають право здійснювати оперативно-розшукову діяльність, банки, митні органи, а також кредитні, фінансові та інші установи, підприємства, організації (незалежно від форм власності) зобов'язані протягом трьох діб надіслати інформацію і документи про операції, рахунки, вклади, внутрішні та зовнішні економічні угоди юридичних осіб та громадян, відносно яких є оперативні та інші матеріали, що свідчать про їх причетність до незаконного обігу наркотичних засобів, психотропних речовин чи прекурсорів», робиться запит до фінансової установи про надання інформації по кожному електронному гаманцю про надання інформації щодо користувача, електронних адрес, номерів телефонів, банківських рахунків, IP-адрес, які було використано для авторизації та здійснення розрахунків за допомогою електронного гаманця (облікового запису користувача). У рамках порушеного кримінального провадження цю інформацію можна витребувати по запиту на підставі ч. 5 ст. 40 та ч. 2 ст. 93 Кримінально-процесуального кодексу України або на підставі ухвали слідчого судді про тимчасовий доступ до речей та документів (ст.ст. 40, 159, 160, 162-163 КПК України).

Так, наприклад, небанківська фінансова установа ТОВ Фінансова компанія «Контрактовий дім», що забезпечує роботу системи прийому платежів EasyPay, яку найбільш поширено використовують організатори інтернет-наркомагазинів в України, на запит правоохоронних органів надає у формі електронних таблиць наступну інформацію щодо облікового запису користувача (електронного гаманця):

- унікальний ідентифікатор користувача в системі (UserID). Реєстрація користувача здійснюється за номером телефону.
- номер гаманця (WalletNumber). Завжди пов'язаний із певним UserID та номером мобільного телефону (Phone). Один користувач може мати

будь-яку кількість гаманців, причому номера гаманців будуть різні, а UserID та Phone ті ж самі.

- анкетні дані користувача, якщо вони були вказані при реєстрації. Оскільки ця інформація при реєстрації не обов'язкова, то такої інформації може й не бути.
- номер мобільного телефону (Phone), за допомогою якого користувач зареєстрував електронний гаманець і за допомогою якого він буде підтверджувати фінансові операції через даний гаманець. Телефон веріфікується за допомогою смс-повідомлення з одноразовим паролем.
- грошові транзакції: час та суми грошей, які надійшли або переведені з гаманця;
- IP-адреси, з яких здійснювався вхід при реєстрації гаманця та здійснення фінансових операцій з вказівкою часу операції;
- частини номерів банківських карток (перші шість та останні чотири цифри номеру картки), на які виводились гроші з електронного гаманця та з яких він поповнявся, із вказівкою дати, часу та суми грошей. Оскільки банком-еквaєром, що обслуговує систему EasyPay є АТ «Альфа-Банк», то повну інформацію за номерами банківських карток можна отримати в АТ «Альфа-Банк» на підставі ухвали слідчого судді про тимчасовий доступ до речей та документів;
- номер телефону платника. Для зареєстрованих користувачів за замовчення підставляється номер, на який вони реєстрували свій акаунт;
- які операційні системи (Android, iOS, Windows тощо) використовувались при здійснені фінансових операцій;
- адреси платіжних терміналів, з яких поповнявся електронний гаманець, та номери мобільних телефонів, які використовувались при поповненні гаманця.

Отримана інформація від фінансової установи узагальнюється та аналізується та в подальшому використовується як доказ у кримінальній справі.

Отримавши інформацію про номер мобільного телефону, який використовується при здійсненні фінансових операцій за електронним гаманцем, для встановлення особи, яка ним користується, номер перевіряється за оперативним обліком.

Для встановлення IMEI мобільних терміналів, у які вставлялась SIM-карта за встановленим номером, спрямовується запит до підрозділу оперативно-технічних заходів. Для встановлення інших номерів мобільних телефонів, яким користується вказана особа, отримавши дані про IMEI, додатково робиться запит на історію IMEI. У відповіді буде вказано всі номери мобільних телефонів, які додавались у мобільний термінал. За необхідності робляться додаткові запити до підрозділу оперативно-технічних заходів за встановленими номерами мобільних телефонів та IMEI.

Для встановлення особи, що користується електронним гаманцем, на підставі ухвали слідчого судді про тимчасовий доступ до речей та документів, в операторів мобільного зв'язку робиться виїмка інформації про з'єднання, IMEI та прив'язка до базових станцій по встановлених номерах мобільних телефонів.

Крім того, для встановлення місцезнаходження мобільного терміналу із виявленим номером, на підставі ухвали слідчого судді проводиться негласна слідча (розшукова) дія, передбачена ст. 268 КПК України. Після цього оперативним шляхом, встановлюється особа, яка ним користується. Також відпрацьовується інформація про IP-адреси, з яких реєструвався електронний гаманець та здійснювались фінансові операції за ним. Для цього здійснюються запити до інтернет-провайдерів, за ким та за якою адресою зареєстровані встановлені IP-адреси. Отримана інформація, щодо адрес та власників перевіряється оперативним шляхом.

При встановленні номерів банківських карток, на які виводилися грошові кошти з електронного гаманця, на підставі ухвали слідчого судді про тимчасовий доступ до речей та документів, у банківських установах робиться виїмка

інформації про власників карток, транзакції за карткою, відео- та фотоматеріали з банківських терміналів, у які вставлялась картка, номери інших карток, з яких та на які переводились грошові кошти з цієї картки. За необхідності здійснити виїмку інформації по встановлених банківських картках.

У ході аналізу інформації про операційні системі, які використовувались при здійснені фінансових операцій, можна встановити з якого пристрою (мобільного телефону, планшету або комп'ютеру) проводить фінансові операції користувач гаманця. Цю інформацію можна використовувати при плануванні негласних слідчих (розшукових) дій, передбачених статтями 263, 264 КПК України.

Аналізуючи інформацію про номери платіжних карток та мобільних телефонів, з яких поповнювався електронний гаманець, можна встановити споживачів наркотиків, які купували наркотичні засоби в інтернет-наркомагазині.

Таким чином, аналізуючи всю отриману інформацію від фінансової установи по електронних гаманцях, інформацію від операторів мобільного зв'язку, інтернет-провайдерів, банківських установ та на основі проведення комплексу слідчо-оперативних заходів можна встановити осіб, причетних до збуту наркотичних засобів через інтернет-наркомагазини.

При встановленні осіб, які займаються збутом наркотичних засобів через інтернет-наркомагазини, для документування їх злочинної діяльності, необхідно використовувати комплекс негласних слідчих (розшукових) заходів, передбачених главою 21 КПК України, таки як: аудіо-, відеоконтроль особи (ст. 260 КПК); зняття інформації з електронних комунікаційних мереж (ст. 263 КПК); зняття інформації з електронних інформаційних систем (ст. 264 КПК); обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267 КПК); установлення місцезнаходження радіообладнання (радіоелектронного засобу) (ст. 268 КПК); спостереження за особою, річчю або місцем (ст. 269 КПК); аудіо-, відеоконтроль місця (ст. 270 КПК); контроль за вчиненням злочину (ст. 271 КПК), виконання спеціального завдання з розкриття

злочинної діяльності організованої групи чи злочинної організації (ст. 272 КПК), негласне отримання зразків, необхідних для порівняльного дослідження (ст. 274 КПК), використання конфіденційного співробітництва (ст. 275 КПК).

Аудіо-, відеоконтроль особи проводиться без її відома на підставі ухвали слідчого судді, для фіксації в місці перебування розмов цієї особи або інших звуків, рухів, дій, пов'язаних зі збутом наркотичних засобів (виготовлення наркотичних засобів, їх фасування тощо), для подальшого використання як джерело доказів злочинної діяльності. Даний вид НСРД проводиться стосовно особи, як у публічно доступних місцях, так і в публічно недоступних місцях, житлі чи іншому володінні особи (гаражі, автомобілі тощо). Для проведення цього виду НСРД у публічно недоступних місцях, житлі чи іншому володінні особи, необхідно отримати дозвіл слідчого судді на проведення негласної слідчої (розшукової) дії, передбаченої п. 5 ч. 1 ст. 267 КПК України, яка гласить: «Слідчий має право обстежити публічно недоступні місця, житло чи інше володіння особи шляхом таємного проникнення в них, у тому числі з використанням технічних засобів, з метою встановлення технічних засобів аудіо, відеоконтролю особи». Публічно недоступним є місце, до якого неможливо увійти або в якому неможливо перебувати на правових підставах без отримання на це згоди власника, користувача або уповноважених ними осіб.

Зняття інформації з електронних комунікаційних мереж (комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг) є різновидом втручання у приватне спілкування, що проводиться без відома осіб, які використовують засоби електронних комунікацій (телекомунікацій) для передавання інформації, на підставі ухвали слідчого судді, якщо під час його проведення можливо встановити обставини, які мають значення для кримінального провадження. При зверненні до слідчого судді на отримання дозволу на проведення цього виду НСРД повинні бути зазначені ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, транспортну комунікаційну мережу, таких, як IMEI мобільних терміналів, номери мобільних телефонів.

Зняття інформації з електронних інформаційних систем – це пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі (комп'ютері, ноутбуці, планшеті, телефоні тощо) або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача, який здійснюється на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування. При зверненні до слідчого судді на отримання дозволу на проведення цього виду НСРД повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, таки як MAC-адреси комп'ютера, ноутбука, планшета або серійні номери процесорів вказаних інформаційних систем.

Слід зауважити, що для встановлення ідентифікаційних ознак електронної інформаційної системи: MAC-адреси або серійного номеру процесора електронної інформаційної системи, якщо ці електронні інформаційні системи знаходяться в публічно недоступних місцях, житлі чи іншому володінні особи, необхідно проводити додаткову негласну слідчу (розшукову) дію, передбачених статтею 267 КПК України – «Обстеження публічно недоступних місць, житла чи іншого володіння особи», і після встановлення ідентифікаційних ознак електронної інформаційної системи, звертатись до слідчого судді на отримання дозволу на проведення НСРД передбаченого ст. 264 КПК України.

Відповідно до ч. 2 ст. 264 КПК України, не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту. Як приклад, це огляд сторінки в соцмережі, коментаря до публікації, перегляд відеороликів в YouTube тощо.

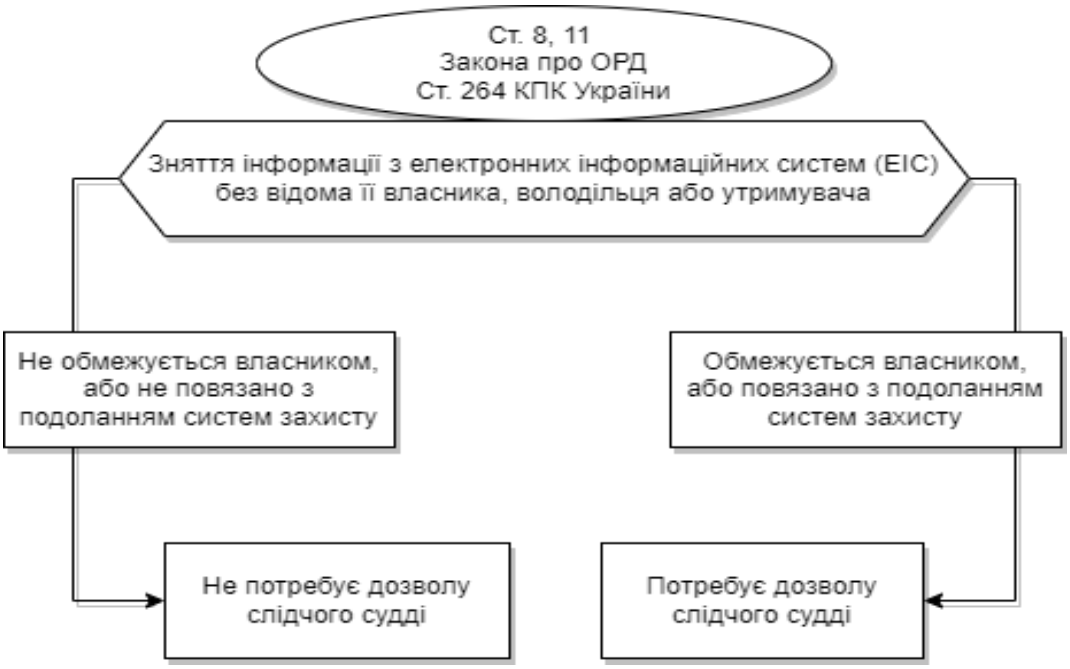

Рис. 15. Зняття інформації з електронних інформаційних систем (ЕІС) без відома її власника, володільця або утримувача

Обстеження публічно недоступних місць, житла чи іншого володіння особи при документуванні наркозбувальників проводиться з метою: встановлення технічних засобів аудіо-, відеоконтролю особи; встановлення МАС-адреси комп'ютера, ноутбука, планшета, для подальшого проведення НСРД, передбачених ст. 264 КПК України; виявленні та фіксації слідів вчинення злочинів, речей і документів, пов'язаних зі збутом наркотичних засобів; виготовлення копій чи зразків зазначених речей і документів; виявлення та вилучення зразків для дослідження.

Установлення місцезнаходження радіообладнання (радіоелектронного засобу) є негласною слідчою (розшуковою) дією, що полягає в застосуванні технічних засобів для отримання від мережевої інфраструктури або мобільного кінцевого (термінального) обладнання відомостей про місцезнаходження мобільного кінцевого (термінального) обладнання (точки його підключення до мережі), а в мережі фіксованого зв'язку – даних про фізичну адресу кінцевого пункту мережі, без розкриття змісту повідомлень, що передаються, якщо в результаті проведення такої негласної слідчої (розшукової) дії можливо

встановити обставини, які мають значення для кримінального провадження. При зверненні до слідчого судді на отримання дозволу на проведення цього виду НСРД повинні бути зазначені ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, транспортну телекомунікаційну мережу, таких як IMEI мобільних терміналів, номери мобільних телефонів. При проведенні цього виду НСРД можливо встановити місця перебування наркозбувальників, для подальшого встановлення їхнього місця мешкання, місць зберігання та фасування наркотиків.

Спостереження за особою, річчю або місцем проводиться для пошуку і фіксації дій особи та її поведінки або тих, з ким ця особа контактує, або певної речі чи місця в публічно доступних місцях шляхом проведення візуального спостереження за зазначеними об'єктами, при цьому може використовуватись відеозапис, фотографування, спеціальні технічні засоби для спостереження. Як приклад, фіксування отримання посилок із наркотиками в поштових відділеннях, фіксування здійснення «закладок» наркотиків, фіксування зняття грошей, отриманих за збут наркотиків із банківських карток тощо.

Аудіо-, відеоконтроль місця полягає в здійсненні прихованої фіксації відомостей за допомогою аудіо-, відеозапису всередині публічно доступних місць, без відома їх власника, володільця або присутніх у цьому місці осіб, за наявності відомостей про те, що розмови і поведінка осіб у цьому місці, а також інші події, що там відбуваються, можуть містити інформацію, яка має значення для кримінального провадження.

Важливим джерелом доказів при документуванні наркозбувальників є проведення негласної слідчої (розшукової) дії, передбаченої ст. 271 КПК України, а саме *контроль за вчиненням злочину.* Найбільш поширено для документування наркозбувальників використовується так форма контролю за вчиненням злочину, як *оперативна закупка* наркотичних засобів, яка проводиться на підставі постанови прокурора.

Вид наркотичного засобу, його кількість та на яку саме суму буде купувати наркотичний засіб особа, задіяна на проведення оперативної закупки,

попередньо обговорюється. Крім того, цю інформацію в постанові на проведення контролю за вчинення злочину вказує прокурор.

Під час проведення оперативної закупки, особі, яка проводить оперативну закупку наркотичних засобів, слідчий, у присутності понятих та оперативних працівників, вручає кошти для проведення оперативної закупки наркотиків. Далі покупець заходить на сайт Інтернет магазина або акаунт оператора наркомагазина в месенджері Telegram та в переписці з оператором вибирає вид та кількість наркотичного засобу, який буде купувати, отримує інформацію про номер електронного гаманця або банківської картки, куди треба перерахувати кошти за наркотичний засіб. Далі покупець слідує до терміналу та переводить необхідну суму на електронний гаманець або банківську картку. Після цього повідомляє про перерахунок грошей оператору, а той після підтвердження оплати, надає покупцю фото та координати місця, де знаходиться «закладка» з наркотичним засобом. Слідчий з покупцем та понятими направляються до місця «схованки», де вилучає куплений наркотичний засіб.

Усі дії покупця та його переписка з оператором фіксуються.

Далі відпрацьовується інформація за номером електронного гаманця або банківської картки, вилучений наркотичний засіб спрямовується на комплексну експертизу – молекулярно-генетичну, дактилоскопічну та експертизу наркотичних засобів. Отримана інформація використовується як доказ у кримінальному провадженні.

Іншим видом контролю за вчиненням злочину є *контрольована поставка*, яка проводиться з метою виявлення джерел і каналів незаконного обігу наркотичних засобів, осіб, які беруть участь у цьому. Контрольована поставка полягає в забезпеченні контрольованого переміщення (перевезення, пересилання) виявленої незаконної партії наркотичних засобів, з метою виявлення і подальшого викриття максимального числа учасників незаконного збуту наркотичних засобів, канали та маршрути транспортування наркотиків, способи їх маскування.

Негласне отримання зразків, необхідних для порівняльного дослідження проводиться на підставі ухвали слідчого судді, у який зазначаються відомості про конкретні зразки, які планується отримати. Під час цього виду негласних слідчих (розшукових) заходів негласно одбираються зразки ДНК-профіля наркозбувальників, наркотичних засобів тощо.

Виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації під час досудового розслідування тяжких або особливо тяжких злочинів можуть бути отримані відомості, речі й документи, які мають значення для досудового розслідування, особою, яка, відповідно до закону, виконує спеціальне завдання, беручи участь в організованій групі чи злочинній організації, або є учасником зазначеної групи чи організації, що на конфіденційній основі співпрацює з органами досудового розслідування. Виконання зазначеними особами такого спеціального завдання, як негласна слідча (розшукова) дія, здійснюється на підставі постанови слідчого, погодженої з керівником органу досудового розслідування або постанови прокурора зі збереженням у таємниці достовірних відомостей про особу. У постанові, крім відомостей, передбачених статтею 251 КПК, зазначається: 1) обґрунтування меж спеціального завдання; 2) використання спеціальних несправжніх (імітаційних) засобів.

Виконання спеціального завдання не може перевищувати шість місяців, а в разі необхідності строк його виконання продовжується слідчим за погодженням з керівником органу досудового розслідування або прокурором на строк, який не перевищує строку досудового розслідування.

При планування проведення кожного конкретного виду негласних слідчих (розшукових) дій треба враховувати доцільність та можливість їх проведення.

Ще одним із джерел отримання доказів злочинної діяльності наркозбувальників, які займаються збутом наркотичних засобів безконтактним шляхом, це проведення експертиз вилучених наркотичних засобів, які вилучені при проведені слідчих дій або негласних слідчих (розшукових) дій (контролю за

вчиненням злочину). Як правило, наркозбувальники при збуті наркотичних засобів шляхом схованок, фасують наркотичні засобі для збуту, використовують поліетиленові пакетики із застібкою системи «Zipp-Lock», які замотують в ізоляційну стрічку. Тому важливо, для отримання доказів призначати не лише експертизу наркотичних засобів, а призначати комплексну експертизу, яка включає судову молекулярно-генетичну експертизу, судову дактилоскопічну експертизу та експертизу наркотичних засобів. Судова молекулярна-генетична експертиза проводиться для виявлення генетичних ознак (ДНК-профіля) наркозбувальників на упаковці, у яку поміщено наркотичній засіб, а судова дактилоскопічна експертиза проводиться на виявлення слідів пальців рук на упаковці. Якщо під час комплексної експертизи виявлено генетичні ознаки (ДНК-профіль) або сліди пальців рук, то ця інформація перевіряється за відповідними базами даних. У подальшому, при затриманні наркозбувальників, у них, на підставі постанови прокурора або ухвали слідчого судді, одбираються зразки букального епітелію для отримання генетичних ознак (ДНК-профілю), та вони дактилоскопируються. Після цього проводиться порівняльна молекулярно-генетична або дактилоскопічна експертиза. Результати експертиз використовуються як докази в рамках кримінального провадження.

Ще одним з основних джерел доказів злочинної діяльності наркозбувальників, що займаються збутом наркотичних засобів через інтернет-наркомагазини, є докази, отримані під час проведення обшуків та оглядів місця події при затриманні наркозбувальників. При цих слідчих діях важливо приділяти увагу не тільки вилученню наркотичних засобів, а і вилученню всіх наявних SIM-карток, банківських карток, записів, а також мобільних телефонів, планшетів, комп’ютерів тощо. Оскільки великий об’єм інформації щодо злочинної діяльності наркозбувальників може зберігатися в мобільних телефонах, планшетах, комп’ютерах, важливо при проведенні вказаних слідчих дій відразу залучати співробітників підрозділів по боротьбі з кіберзлочинністю та експертів за лінією комп’ютерно-технічних експертиз. Після огляду наявної інформації в мобільних телефонах, планшетах та комп’ютерах під час обшуку,

вони вилучаються та в подальшому спрямовуються для проведення комп'ютерно-технічної експертизи, з метою отримання вже видаленої з них інформації.

Отже, для документування груп наркозбувальників, які збувають наркотичні засоби через інтернет-наркомагазини, потрібен дуже великий об'єм оперативних, слідчих та негласних слідчих (розшукових) дій та необхідна взаємодія співробітників багатьох підрозділів.

Контрольні питання:

1. Що розуміють під електронним доказом?
2. Чи може бути заблокована юридична сила електронного документу?
3. У яких випадках електронний документ не може бути застосовано як оригінал?
4. Чи підтверджує електронний цифровий підпис цілісність електронного документу ?
5. Як відбувається огляд доказів за їх місцезнаходженням?
6. В якому випадку скриншоти вебсторінок (електронної пошти і т.ін.) можуть бути прийняті, як електронні докази?
7. Як правильно долучити до матеріалів справи роздруківки електронних доказів?
8. Як отримати експертний висновок щодо достовірності наданих до суду електронних доказів?
9. Що таке хеш-сума файлу?
10. Для чого використовують хеш файлу?
11. Які є способи обчислення хеш-суми файлу?
12. Які є форми документування вебконтенту?
13. Що таке вихідний код вебсторінки?
14. Як проглянути та зберегти вихідний код вебсторінки?

15. Як відбувається фіксація сайту?

16. Які дані збирає спеціальний мережевий протокол Whois?

17. Як скористуватися сервісом Whois?

18. Як можна дізнатись IP-адресу конкретного комп’ютера?

19. Як працює сервіс IP-Logger?

20. Що таке аналізатор трафіку?

21. Які способи перехоплення трафіку?

22. Яка схема розповсюдження наркотичних засобів та схема розрахунку?

23. Яку інформацію можна отримати від представника платіжної системи EasyPay щодо користувача електронного гаманця?

24. Які види негласних слідчих (розшукових) дій можуть бути використані для встановлення осіб, які займаються збутом наркотичних засобів через інтернет-наркомагазини?

Розділ 2.
РОЗВІДКА ДАНИХ З ВІДКРИТИХ ДЖЕРЕЛ (OSINT)

2.1. Пошукова система Google.

У попередньому розділі були розглянуті протокол Whois та створення лінка-логера в сервісі IP-Logger. Ці поняття можна впевнено віднести до OSINT. Проте, збирання даних у відкритих джерелах відбувається за допомогою значної кількості інструментів, котрі з яких розглянемо в цьому розділі.

Почнемо зі звичайного пошуку в Інтернеті. Коли ми складаємо деякий запит (з ключових слів або термінів), то отримуємо низку посилань на сайти, документи, зображення, які якнайкраще відповідають запиту. Ці результати надає нам пошукова система, де ми створювали запит. Найбільш відомою пошуковою системою є Google, яка охоплює більшу частину світового ринку: вона щодня реєструє десятки мільйонів запитів і працює на 117 мовах.

Рис. 16. Приклади пошукових систем для проведення OSINT

Прикладом інших підсистем є Yahoo!, Bing, META, DuckDuckGo, Yandex (Рис. 16). Питання вибору тієї або іншої пошукової системи для пошуку даних розглядається в площині таких властивостей системи, як обсяг індексної бази, регіони охоплення, принципи проведення пошуку, вхідна мова, швидкість відновлення інформації, здатність шукати «нестандартну» інформацію тощо.

Основний об'єкт індексації пошукової системи – тексти. Однак існують і такі системи, що дозволяють робити пошук за картинками, аудіо- та відеофайлами, архівами програм, новинами тощо. Наприклад, Google News Search здійснює тематичний пошук за новинами; Google Microsoft Search – за сайтами, присвяченими Microsoft; Nigma – пошук за картинками, книгами, музикою.

Варто враховувати також область дії пошукової системи. Серед них розрізняють локальні (обмежені національним доменом, певною мовою) і глобальні пошукові системи. Зазвичай глобальні системи добре покривають американський Інтернет і трохи гірше «знають» іншу частину. Тому якщо пошук свідомо обмежений країною або мовою, краще користуватися локальним пошуковиком (в Україні це пошукова система META).

Для отримання даних у пошуковій системі створюється (або формується) запит. Запити складаються так, щоб область пошуку була максимально конкретизована і звужена. Для створення запиту підбираються ключові слова та застосовуються оператори пошуку.

Спочатку на прикладі пошукової системи Google розглянемо оператори пошуку, які наявні в більшості пошукових систем. Водночас зауважимо, що пошукова система Google не є регістро залежною. Тобто, неважливо, малі, чи великі літери в ключових словах. Усі літери, які б не вводились, автоматично переводяться до нижнього регістру.

При пошуку, Google ігнорує дуже часто вживані слова і символи (наприклад, «де», «як», артиклі в англійській або німецькій мові, окремі цифри і літери і т.ін.), оскільки це уповільнює пошук. Якщо якесь слово запиту проігноровано, то це можна дізнатися одразу на сторінці результатів пошуку.

Для того щоб отримати сторінки, які обов’язково містять певне слово запиту, треба додати знак «+» перед цим словом, або після нього без пробілу. Якщо пошуковий термін має більше ніж одне значення і часто зустрічається у виразі з іншим словом (наприклад, слово «океан» може стосуватися географічних об’єктів, великого обсягу чогось або бути частиною виразу, наприклад, «океан почуттів»), то можна сфокусувати пошук, поставивши знак «-» перед словами, пов'язаними з тим значенням, яке нас не цікавить. Наприклад, «океан - почуттів». Це називають *винятком терміну* або фрази.

Якщо між ключовими словами додати оператори логіки AND, OR або NOT, то здійснюється пошук документів, що містять вказані слова разом (AND), або хоча б одне з них (OR), або зовсім відсутні (якщо слідують за оператором NOT). За замовчуванням, Google повертає сторінки, які включають усі пошукові терміни (ключові слова). Тому немає потреби вставляти AND між термінами, але цей оператор дуже корисний у поєднанні з іншими операторами. Порядок слів у запиті може впливати на результати пошуку.

Оператор NEAR допоможе знайти документи, у яких друге слово знаходиться на відстані від першого, яка не перевищує визначеного числа слів.

Оператор FOLLOWED BY дозволяє отримати документи, у яких ключові слова йдуть у заданому порядку;

За допомогою оператора lang отримаємо сторінки певною мовою. Після lang ставиться двокрапка і вказується параметр, який визначає потрібну мову документа (наприклад, українська – uk, білоруська – be, англійська – en, французька – fr).

Іноді потрібні результати, які включають деяку фразу повністю. Це називають *примусовим пошуком точного збігу*. У такому разі необхідно просто узяти фразу в лапки « ». Пошук по фразах є найбільш ефективним, якщо ви шукаєте власні імена.

Якщо при створенні запиту деякі слова невідомі (або забуті), то, замість цих слів, можна поставити знак зірочки «*».

Для контролю видачі результатів слід користуватись круглими дужками.

Крім указаних операторів, пошукова система Google містить спеціальні оператори, які дозволяють відшукати документи вказаного формату, сторінки з потрібними словами в домені сайту, у назві сайту або в тексті сторінки.

Базові правила використання операторів:

1) Пошукові оператори (крім операторів логіки) пишуться з двокрапкою.

2) В операторах усі літери мають бути маленькими (на відміну від ключових слів, які не чуттєві до величини символів). Винятки – оператори OR та AND.

3) Після оператора з двокрапкою та терміном не має бути жодних пробілів.

Далі розглянемо низку операторів, які найчастіше використовують при пошуку в Google.

link: – виведе перелік вебсторінок, які утримують посилання, на зазначену вебсторінку.

related: – виведе перелік вебсторінок, «подібних» до зазначеної вебсторінки.

info: – видасть інформацію, яку Google має стосовно зазначеної вебсторінки.

define: – поверне визначення слова, введеного після оператора, узяті з різних онлайн-джерел. По суті, це вбудований у Google словник.

site: – Google обмежить можливі результати пошуку сайтами в означеному домені. site:[домен] -inurl:https

allintitle: (intitle:) – Google обмежить результати пошуку тими, які будуть включати всі введені пошукові терміни (один термін) у заголовку сторінки.

allinurl: (inurl:) – результати пошуку будуть мати всі введені пошукові терміни (термін) в адресі (URL) сторінки. У поєднанні з оператором site дозволяє знаходити незахіщені сторінки. Пишуть: site:[домен] –inurl:https

allintext: (intext:) – знаходить сторінки, що містять вказані після оператора слова (слово) на сторінці сайту.

filetype: – знаходить конкретні типи документів по їх розширенню (pdf, docx, xlsx, pptx, txt та т.ін.). Наприклад, filetype:pdf (ключові слова).

Якщо треба обмежити пошук для певного діапазону числових даних (дати, виміри, ціни і т. ін.), пишуть два числа, розділених двома крапками без пробілів. Обов'язково вказати одиницю вимірювання або якийсь інший індикатор того, що саме являють собою ці числа. Наприклад, iPhone $300..$500.

Узагалі, за рахунок спеціальних операторів можна вирішити такі завдання:

- пошук помилок індексації;
- пошук незахищених сторінок (не https);
- пошук дублікатів контенту;
- пошук небажаних файлів і сторінок на сайті;
- пошук можливостей для гостьової публікації;
- пошук сторінок зі списками ресурсів;
- пошук сайтів для розміщення своїх посилань… і перевірки, наскільки вони підходять;
- пошук профілів у соціальних мережах;
- пошук можливостей для спонсорських постів;
- перевірка, як часто публікується новий контент на певному сайті;
- пошук сайтів з посиланнями на конкретні сайти.

У пошуковій системі Google є можливість сформувати складний запит за допомогою *розширеного пошуку* через *панель швидкого налаштування*.

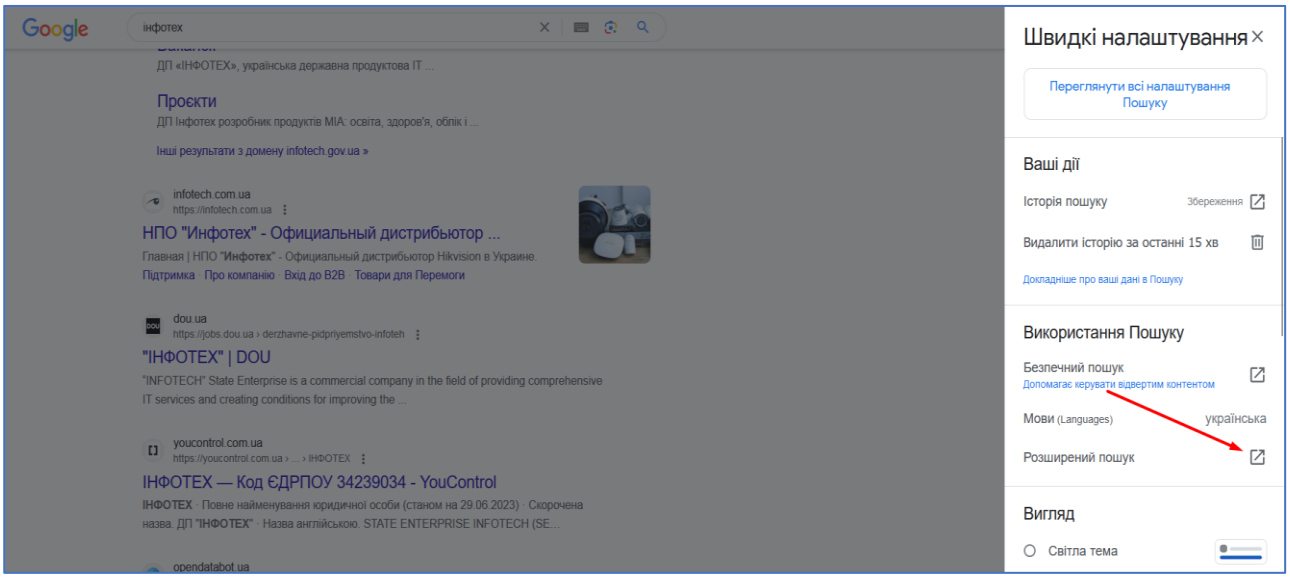

Рис. 17. Відкриття панелі швидкого налаштування

Щоб відкрити панель швидкого налаштування, спочатку на новій вкладці браузера в полі пошуку вкажемо декілька ключових слів і розпочнемо пошук. Потім, у правій стороні робочого вікна браузера знаходимо значок швидкого налаштування та тиснемо на нього. Справа відкриється вікно «Швидкі налаштування» (Рис. 17), на якому знаходимо «Розширений пошук» і тиснемо на значок.

Вікно розширеного пошуку (Рис. 18) поділяється на дві частини – «Знайти сторінки, що містять…» та «Додаткові налаштування…».

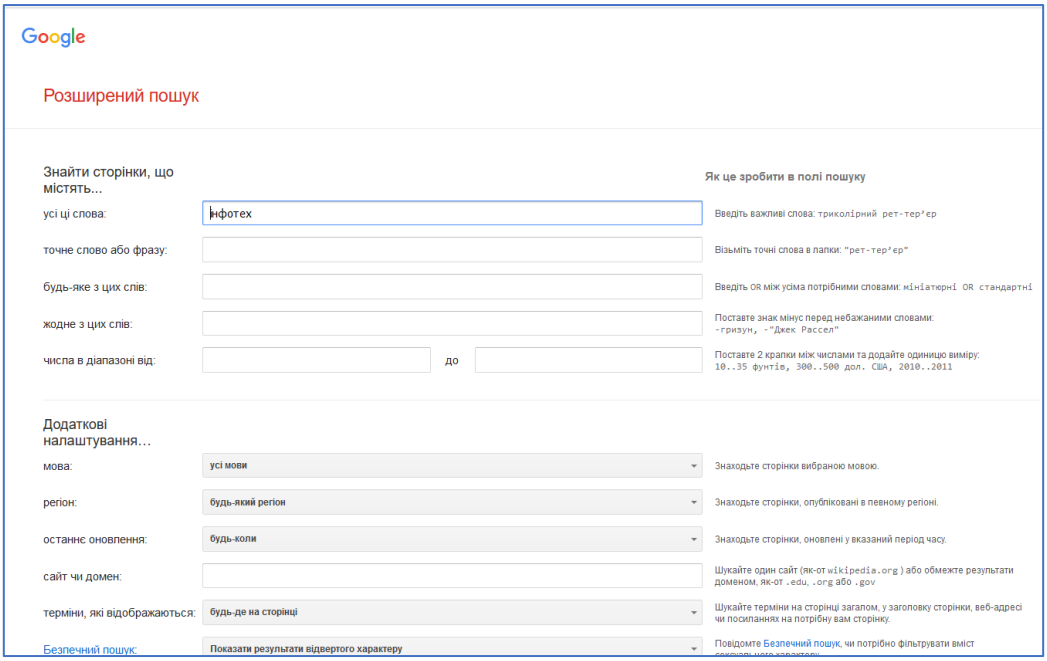

Рис. 18. Вікно розширеного пошуку Google з розділами для ключових слів і додаткових налаштувань

У частині «Знайти сторінки, що містять…» ми бачимо п'ять позицій для пошуку:

- поле для ключових слів;
- поле примусового пошуку точного збігу;
- поле можливого вибору одного з термінів;
- поле винятку терміна;
- два поля для пошуку сторінок з числовими даними заданого діапазону.

Праворуч від полів знаходиться довідкова інформація «Як це зробити в полі пошуку».

У частині «Додаткові налаштування…» бачимо вісім позицій:

- поле вибору мови;
- поле вибору країни;
- поле останнього оновлення сторінок;
- поле для уточнення домену;
- поле (Рис. 19) для уточнення розташування терміна (у заголовку сторінки, у тексті сторінки і т.ін.);
- поле безпечного пошуку (показати/сховати результати відвертого характеру);
- поле вибору типу файлу;
- поле права на користування.

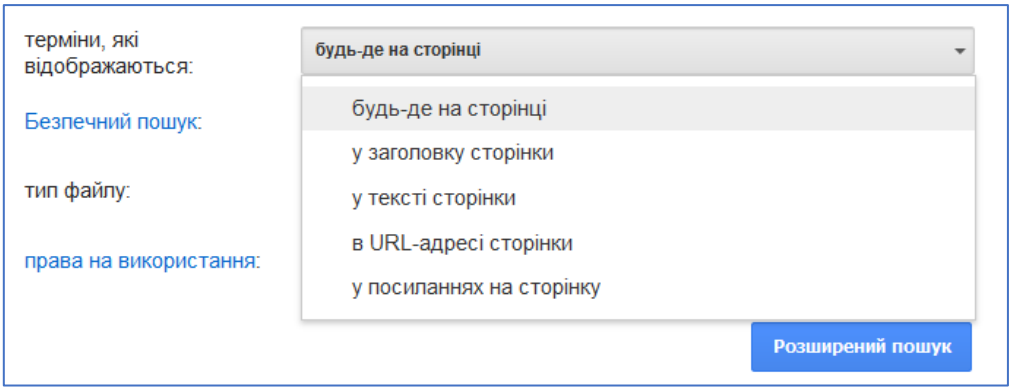

Рис. 19. Додаткові налаштування розширеного пошуку Google

Ми зробили детальний опис вікна розширеного пошуку і, як бачимо, цей додатковий сервіс пошукової системи Google практично повністю може замінити значну кількість пошукових операторів Google.

Треба зауважити, що при правильному використанні пошукових операторів ефект від пошуку даних може бути дуже значним.

2.2. Первинні дані для пошуку.

Якщо узагальнити набір даних, за якими, як правило, проводиться пошук, то ми отримаємо певні категорії ідентифікаторів. Розглянемо це більш детально.

Персональні дані особи. Ця категорія насичена великою кількістю ознак (атрибутів). По-перше, це ідентифікаційні дані особи:

- прізвище, ім’я, по батькові; дата народження; місце народження.

Загальні особисті дані:

- назва, серія, номер і дата видачі документу, який посвідчує особу;
- національний ідентифікаційний номер;
- стать;
- номер телефону;
- електронна пошта;
- посвідчення водія;
- номерний знак транспортного засобу;
- номери банківських карток;
- фінансова інформація (майновий стан і доходи);
- облікові записи в месенджерах;
- облікові записи в соціальних мережах;
- освіта;
- професія;
- сімейний стан, склад сім'ї;
- житлові умови;
- спосіб життя;
- життєві інтереси та захоплення;
- споживчі звички;
- особисті кабінети на сайтах;
- IP-адреса (у деяких випадках).

«Чутливі» особові дані:

- інформація про расове, етнічне походження та національність;
- відомості, що стосуються політичних, світоглядних та релігійних переконань;
- відомості про членство в політичних партіях, профспілках, релігійних або громадських організаціях;
- відомості про стан здоров'я і статеве життя;
- генетичні і біометричні дані, почерк;
- місце знаходження та шляхи пересування особи.

Ідентифікатори предметів. *Мобільний телефон* можна ідентифікувати за IMEI. Номер IMEI (International Mobile Equipment Identity) — унікальне 15-значне число, яке присвоюється кожному мобільному пристрою, що працює в мережах GSM, UMTS, LTE, 5G. Наявність IMEI дозволяє відстежувати переміщення мобільного пристрою і його місцезнаходження, коли він підключений до мережі. Таким чином можна шукати вкрадені телефони. Мобільний оператор може блокувати телефони за IMEI.

Точка доступу Wi-Fi. Якщо відома назва точки доступу або її MAC-адреса, то можна спробувати дізнатися її місце розташування з використанням певного сервісу.

Сучасні соціальні мережі є одним з найбільших джерел інформації для OSINT. Це пов’язано з тим, що навіть якщо шукана особа сама не зареєстрована в соціальних мережах, то там можуть бути її родичі, близькі особи, друзі, знайомі.

Електронна пошта поряд з номером телефону на сьогодні є ідентифікатором, що найбільш часто використовується для реєстрації на мережних ресурсах.

У додатку А можна знайти приклади мережевих ресурсів для пошуку та аналізу таких об’єктів, як мобільний телефон, електронна пошта, фотозображення тощо.

2.3. Програми пошуку і аналізу даних.

Крім наведених інструментів, вельми корисними програмами як для пошуку, так і для аналізу даних є платформи Gephi (gephi.org), Maltego (maltego.com), IBM i2 ANB (ibm.com/products/i2-analysts-notebook).

Maltego – це комерційна програма із вбудованим штучним інтелектом для збору інформації про об'єкти, людей, сайти тощо. Вона автоматично аналізує дані з усіх відкритих джерел інформації, зіставляє їх, виводить результат аналізу у вигляді зручної схеми. Аналіз здійснюється за допомогою запиту записів DNS, Whois, пошукових систем, різноманітних API, отриманням метаданих.

Програма створена компанією PATERVA (Німеччина) у 2017 році. Точний алгоритм, за яким вона працює, не відомий (є комерційною таємницею розробника). Переважно, Maltego використовується комерційними організаціями для забезпечення захисту внутрішньої інформації від зовнішнього доступу. Програма показує, через які канали конкуренти можуть отримати дані. Очевидно, наявність таких каналів і дає можливість виконувати OSINT.

Автори Maltego пропонують п’ять релізів: Maltego Case File, Maltego Common Edition, Maltego Classic, Maltego XL, Maltego One.

Щоб зрозуміти різницю між цими релізами, треба вказати, що програма будує схему зв’язків між певними об’єктами, використовуючи 3 елементи: Entities, Transforms и Links.

Entities (об'єкти) – це може бути Person (людина), Company (компанія), Phone number (телефон), Domain (домен), DNS name (ім'я DNS-серверу), Technology (вебтехнологія, наприклад, Google Ads). Об’єкти розміщуються у робочій області програми у вигляді піктограм (Рис. 20).

Links (зв'язки) між об'єктами (наприклад, людині відповідає e-mail або номер телефону) встановлюються вручну або автоматично після запуску трансформів.

Transforms (трансформи, процеси) – процедури, які отримують інформацію з відкритих джерел, пов'язану з об'єктом, вказуючи зв’язки і розширюючи схему. Можна вважати, що це найбільш важливий і потужний елемент програми.

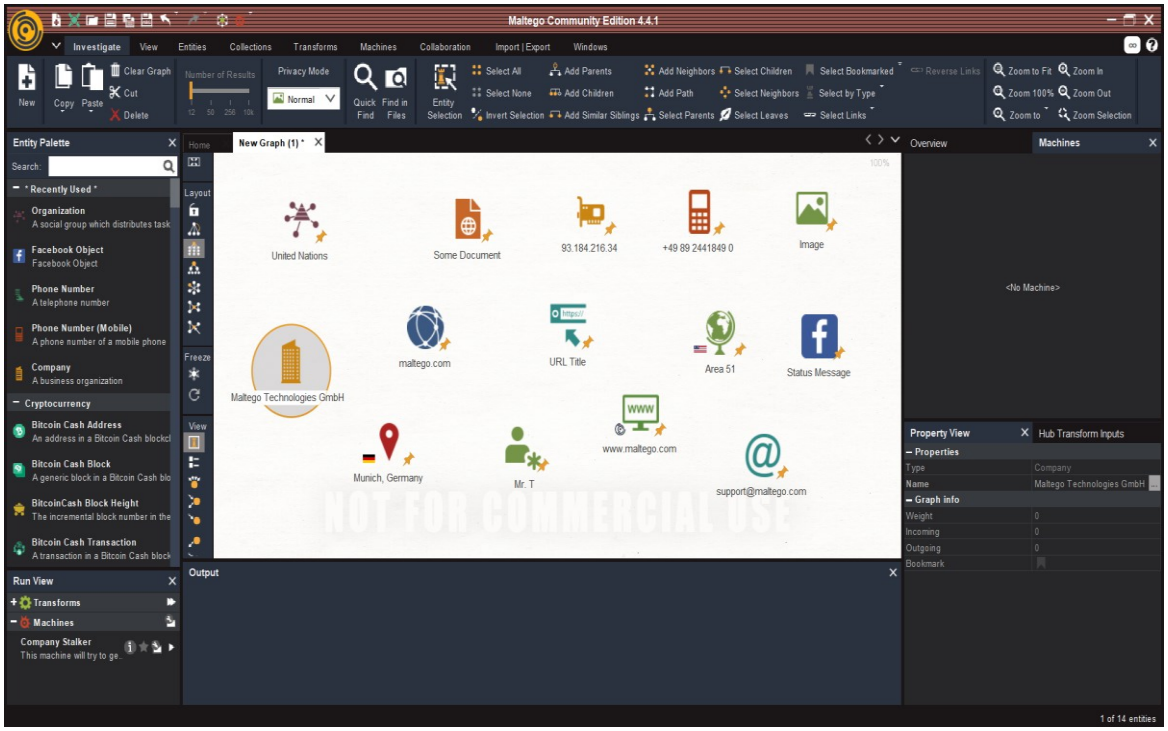

Рис. 20. Об’єкти розміщуються у робочій області програми у вигляді піктограм.

Наведемо деякі приклади трансформів. Так якщо об'єкт – Website, то трансформ «To IP Address» знаходить IP-адресу сайту, створює новий об'єкт IPv4 Address і новий зв'язок між сайтом і IP-адресою. Якщо об'єкт – Domain, трансформ «To Entities from WHOIS» знаходить інформацію про реєстранта або реєстратора в WHOIS-каталозі, створює об'єкти Company, Person, Email Address, Phone Number, Location і їхні зв'язки з об'єктом Domain. Трансформи «CipherTrace» відстежують адреси і транзакції у категоріях ризику: чорні ринки, ransomware, gambling, криптовалютні міксери. Трансформи «VirusTotal» шукають домени, пов'язані зі зловмисними, фішинговими кампаніями, розсиланням спама. Транформи «Social Links» пов’язані з технологією розпізнавання облич.

Тепер щодо характеристик релізів. У Maltego CF (CaseFile Free) можна створювати схеми лише вручну, жодні трансформи не працюють. Побудовану схему можна вивантажити тільки в комерційну версію (фактично, експорт результату аналізу в якісь відомі формати відсутній).

Maltego CE (Community Edition Free) – публічна версія, для навчальних цілей. Цей реліз не допускає використання в комерційних цілях (на що вказує водяний знак на робочому вікні програми). Програмі надається доступ до Free Transformation Hub (пробники трансформів). Це означає, що можна встановити трансформи, але їх функції будуть обмежені. Зокрема, максимальний розмір виводу з однієї Transforms обмежений 12 Entities (перші 12 варіантів аналізу). Взагалі, можна візуалізувати до 10 000 об'єктів на схемі. Також можливо робити експорт у будь-якому доступному вигляді, у тому числі і у вигляді OSINT звіту у PDF із додатком схеми. Використання Maltego CE передбачає реєстрацію та створення облікового запису.

Maltego Classic – це комерційна версія Maltego, яка дозволяє користувачам візуалізувати до 10 000 об'єктів на схемі. Максимальний розмір вивантаження за одним запитом складає до 10 000 Entities. Є доступ до пакету базових Transforms та Commercial Transform Hub. За окрему плату можна отримати додаткові набори Transforms та Entities для проведення OSINT.

Maltego XL (eXtra Large) – преміум-клас для візуалізації великих наборів даних, відображає понад 1 000 000 об'єктів на одній схемі. Розмір вивантаження від одного Transform складає 64 000 результатів. Пакет процесів (трансформів) такий ж, як і в Maltego Classic.

Maltego One – нове уніфіковане рішення для професіоналів і великих підприємств.

i2 Analyst's Notebook. Для аналізу структурованих даних великих розмірів може бути застосоване програмне забезпечення i2 Analyst's Notebook, або скорочено – i2 ANB. Це аналітичне середовище, після отримання даних, надає схему зв'язків між об'єктами (Рис. 21).

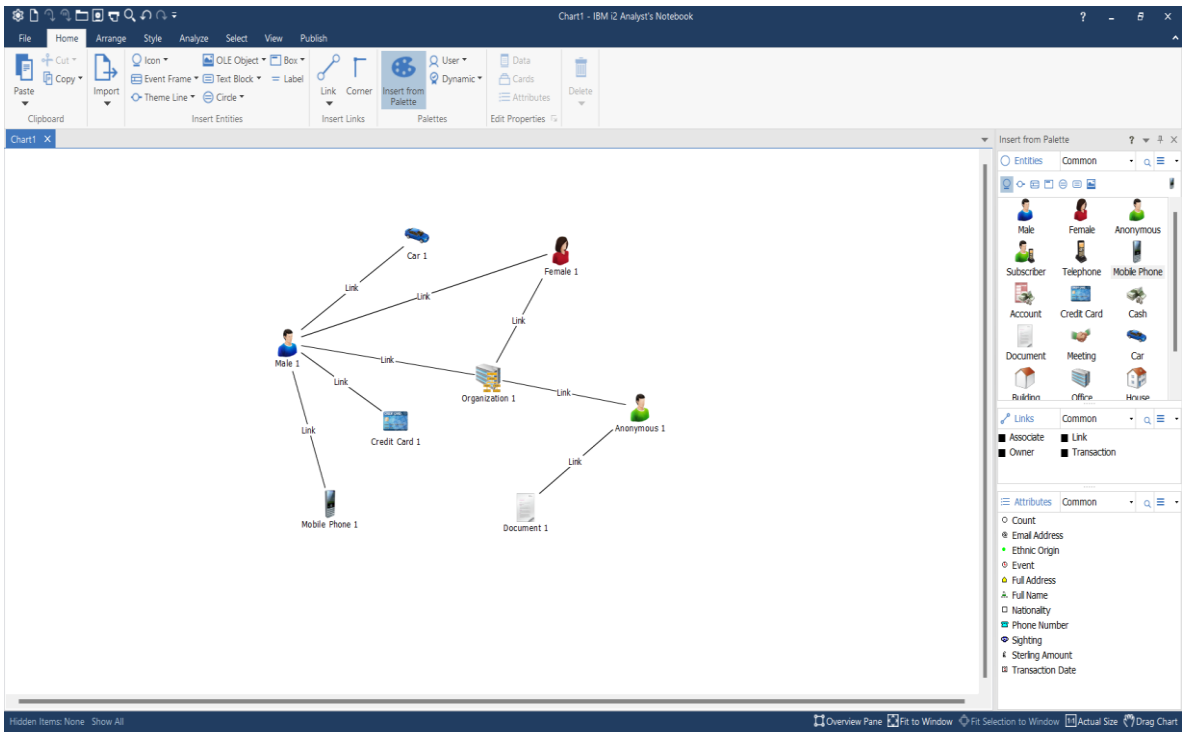

Рис. 21. Аналіз зв'язків між об'єктами за допомогою програмного забезпечення i2 Analyst's Notebook (i2 ANB)

Таким чином, відбувається:

- швидка систематизація розрізнених даних у єдиному узгодженому поданні;
- визначення ключових осіб, подій, зв'язків і закономірностей, які не завжди можна виявити іншими засобами;
- поліпшення розуміння структури, ієрархії та способів дій кримінальних та шахрайських угруповань.

Прикладом великих обсягів структурованих даних, для яких доцільно використовувати i2 ANB, є таблиці банківських транзакцій та телефонних з’єднань. Зазвичай ці дані представлені у форматі xlsx. Додаток i2 ANB дозволяє імпортувати файли Excel і в декілька кроків створювати схему зв’язків між об'єктами, такими як банківські рахунки або мобільні номери. Крім того, кожен об'єкт на схемі може бути детально охарактеризований, наприклад, через зазначення дати або обсягу транзакції, типу і напрямку з'єднання тощо.

2.4. Підготовка робочого середовища

Використання OSINT (Open Source Intelligence) вимагає ретельної підготовки робочого середовища, включаючи налаштування комп'ютера, операційної системи, відповідного програмного забезпечення та реєстрації на необхідних ресурсах. Перелічимо основні вимоги та рекомендації:

- параметри оперативної пам'яті та процесора повинні забезпечувати можливість одночасного запуску кількох операційних систем;
- рекомендується створити кілька віртуальних операційних систем (переважно на базі Linux та Android), які будуть використовуватись для пошуку інформації та реєстрації на мережевих ресурса;
- необхідно встановити інтерпретатор високорівневої мови програмування Python (або програмний пакет Anaconda);
- встановити декілька класичних браузерів та браузер Tor для забезпечення анонімності в Інтернеті;
- використовувати vpn для захисту мережевих з'єднань;
- встановити програми для візуалізації та аналізу зв'язків між об'єктами, такі як Maltego, ibm i2 analysts notebook, Gephi тощо;
- використовувати популярні месенджери для комунікації;
- рекомендується створити власний vpn-сервер на віддаленій віртуальній машині для забезпечення додаткового рівня безпеки;
- мати декілька sim-карт для реєстрації на відповідних онлайн-ресурсах.

Контрольні питання:

1. Чим різняться пошукові системи?
2. Як зобов’язати пошукову систему надати посилання на джерела з певним ключовим словом?
3. Як реалізувати при пошуку виняток терміна?
4. Поясніть призначення операторів логіки.
5. Як реалізувати примусовий пошук точного збігу певної фрази?
6. Поясніть базові правила використання пошукових операторів.
7. За рахунок якого оператора можна отримати сайти в означеному домені?
8. Як здійснити пошук незахищених сторінок (не https)?
9. Як обмежити результати пошуку тільки тими сторінками, які містять певне слово в тексті сторінки (у заголовку сторінки, в адресі сторінки)?
10. Які можливості пошуку надаються у вікні розширеного пошуку?
11. За якою ознакою можна ідентифікувати мобільний телефон?
12. Яке призначення програми Maltego?
13. Які типи об’єктів передбачені в Maltego?
14. Що таке трансформи в програмі Maltego?
15. Наведіть приклади трансформів.
16. За якими параметрами відрізняються релізи maltego?
17. Яке призначення програми i2 ANB?
18. Укажіть приклади структурованих даних, для яких доцільно використовувати i2 ANB.
19. Які параметри комп’ютера необхідні для здійснення OSINT?
20. Яке програмне забезпечення доцільно встановити на комп’ютері для забезпечення якісного пошуку в Інтернеті та аналізу отриманих даних?
21. Які налаштування мережі забезпечать безпечний пошук в Інтернеті?

Розділ 3.
ЄДИНА ІНФОРМАЦІЙНА СИСТЕМА МВС

Сучасні інформаційні технології опрацювання даних у правоохоронній сфері є сукупністю методів і програмно-технічних засобів для збирання, обробки, зберігання, розповсюдження, відтворення і використання інформації, яка може суттєво забезпечити підвищення рівня боротьби зі злочинністю.

Основними тенденціями розвитку інформаційних технологій є:

- удосконалення форм та методів управління системами інформаційного забезпечення;
- централізація та інтеграція комп'ютерних банків даних;
- впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків;
- розбудова та широке використання ефективних та потужних комп'ютерних мереж;
- застосування спеціалізованих засобів захисту інформації;
- налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні.

Отже, інформаційні технології забезпечують функціонування та удосконалення інтегрованих автоматизованих систем, що створюються для діяльності поліції. На даний час такою системою є єдина інформаційна система МВС (далі – ЕІС МВС).

Положення про ЕІС МВС та переліку її пріоритетних інформаційних ресурсів затверджено Постановою Кабінету Міністрів України від 14 листопада 2018 р. № 1024.

Згідно Положенням, ЕІС МВС становить сукупність взаємозв'язаних функціональних підсистем, програмно-інформаційних комплексів, програмно-технічних та технічних засобів телекомунікації, які забезпечують логічне поєднання визначених інформаційних ресурсів, обробку та захист інформації, внутрішню та зовнішню інформаційну взаємодію. Інтеграція інформаційних

ресурсів ЕІС МВС – комплекс методів та процедур, спрямованих на логічне функціональне об’єднання інформаційних ресурсів ЕІС МВС у визначених форматах, за узгодженими показниками, для їх автоматизованої обробки, використання та надання користувачам в уніфікованому вигляді.

Функціональними підсистемами ЕІС МВС є (див. Рис. 22):

- національна система біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства;
- «Інформаційний портал Національної поліції України»;
- автоматизована інформаційна система оперативного призначення;
- Єдиний державний реєстр транспортних засобів;
- Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху;
- система фіксації адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху в автоматичному режимі;
- система екстреної допомоги населенню за єдиним телефонним номером 112;
- інтегрована міжвідомча інформаційно-телекомунікаційна система щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон;
- інформаційно-телекомунікаційна система прикордонного контролю “Гарт-1”;
- інші системи, реєстри та бази (банки) даних, створені суб’єктами єдиної інформаційної системи МВС в межах реалізації владних повноважень.

Структура та порядок роботи функціональних підсистем ЕІС МВС визначаються положеннями про ці підсистеми, які розробляються суб’єктами ЕІС МВС з урахуванням затвердженого МВС Типового положення про функціональну підсистему єдиної інформаційної системи МВС та затверджуються в установленому законодавством порядку.

Рис. 22. Функціональні підсистеми Єдиної інформаційної системи МВС України

В оперативно-розшуковій діяльності інформаційні (функціональні) підсистеми використовуються для з'ясування певної інформації щодо наявності в підозрюваного автотранспорту, зареєстрованої зброї, кримінальних зв'язків тощо. У зв'язку з цим будь-яка функціональна підсистема або реєстр ЕІС МВС можуть бути корисними для отримання певної інформації. Розглянемо більш уважно такі підсистеми, як «Інформаційний портал Національної поліції» та автоматизовану інформаційну систему оперативного призначення.

З метою організації інформаційно-аналітичного забезпечення поліції, згідно з Наказом МВС України від 03.08.2017 р. № 676, затверджено Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» (далі – ІТС ІПНП). Це Положення визначає

основні завдання, призначення, суб’єктів та структуру ІТС ІПНП, а також умови її функціонування.

На Рис. 23 бачимо стартову сторінку ІТС ІПНП.

Рис. 23. Стартова сторінка ІТС ІПНП.

Протягом останніх років було сформовано значну кількість інформаційних підсистем ІТС ІПНП. Наприклад,

- «Гарпун» (наказ № 497 від 13.06.2018 р.);
- «Єдиний облік» (наказ № 508 від 14.06.2019 р.);
- «Слід» (наказ № 257 від 16.03.2020 р.);
- «Дорожньо-транспортна пригода» (наказ № 533 від 15.07.2020 р.);
- «Custody Records» (наказ № 311 від 24.05.2022 р.);
- «Електронний кабінет ювенального поліцейського» (наказ № 855 від 27.12.2022 р.);
- «Облік кривдника» (наказ № 8 від 16.01.2023 р.);
- «Адміністративна практика» (наказ № 180 від 13.03.2023 р.).

На Рис. 24 маємо скриншот робочого вікна ІТС ІПНП.

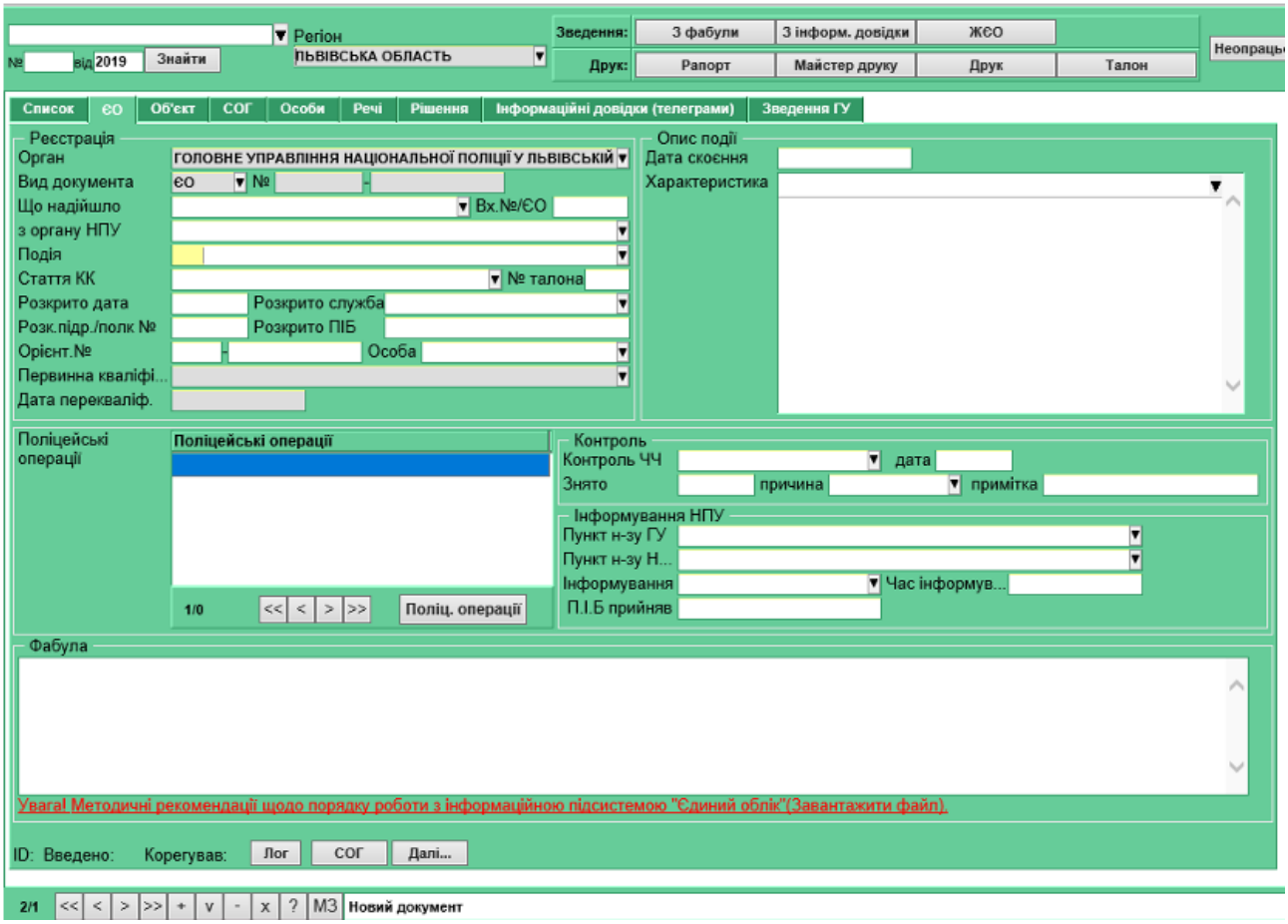

Рис. 24. Робоче вікно ІТС ІПНП.

Під час введення військового стану додалися нові вкладки в ІТС ІПНП як «Блокпост» та «Особа (розшук у зв'язку з державною зрадою)».

Більш детальну інформацію з інформаційних підсистем ІТС ІПНП можна проглянути в Додатку Б.

Наказом № 870 від 20.10.2017 р. було затверджено Положення про автоматизовану інформаційну систему оперативного призначення ЄІС МВС (далі – АІС ОП).

АІС ОП є сукупністю програмно-технічних та технічних засобів електронних комунікацій і призначена для накопичення й обробки відомостей, що утворюються в процесі оперативно-розшукової діяльності та діяльності з проведення кримінального аналізу Національної поліції України, крім

інформації, яка обробляється в інформаційно-пошуковій системі «Філін» Національної поліції України.

Основним завданням АІС ОП є об’єднання отриманої в процесі оперативно-розшукової діяльності Національної поліції України інформації в єдиному інформаційному просторі з використанням сучасних інформаційних технологій, комп'ютерного та електронного комунікаційного обладнання.

У межах досудового розслідування та проведення оперативно-розшукових заходів за оперативно-розшуковими справами здійснюється отримання відомостей з персонально-довідкового обліку. Відомості надаються з інформаційної підсистеми «Оперативно-довідкова картотека» (далі – ОДК) єдиної інформаційної системи Міністерства внутрішніх справ України.

ОДК містить відомості стосовно осіб, яким повідомлено про підозру в учиненні кримінального правопорушення, та осіб, яких засуджено за вчинення кримінального правопорушення. Порядок доступу до відомостей персонально-довідкового обліку єдиної інформаційної системи Міністерства внутрішніх справ України затверджено наказом МВС України № 1256 від 29.11.2016 р.

Треба додати, що співробітники чергових частин, слідчі, працівники оперативних підрозділів карного розшуку, експерти-криміналісти, дільничні інспектора поліції у процесі своєї роботи накопичують величезні бази даних оперативно-довідкового і оперативно-розшукового призначення. У цих базах зазвичай міститься інформація, яка стосується:

- Обліково-реєстраційних даних громадян.
- Правопорушень і кримінальних подій.
- Правопорушників і злочинців.
- Викрадених і вилучених речей, а також предметів антикваріату.
- Власників автомототранспортних засобів.
- Власників вогнепальної зброї.
- Громадян, що перебувають у розшуку та безвісти зниклих громадян.

Контрольні питання:

1. Що таке Єдина інформаційна система МВС України?
2. За якими напрямами працюють функціональні підсистеми ЕІС МВС?
3. З якою метою створено інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»?
4. Укажіть приклади інформаційних підсистем ІТС ІПНП, які були нещодавно введені в дію.
5. Для накопичення якої інформації утворено автоматизовану інформаційну систему оперативного призначення?
6. Які відомості містить «Оперативно-довідкова картотека»?
7. Які основні функції виконує система екстреної допомоги населенню за єдиним телефонним номером 112?
8. Яким чином забезпечується захист інформації в Єдиній інформаційній системі МВС?
9. Назвіть приклади міжнародного співробітництва у рамках функціонування ЕІС МВС.
10. Яка роль Єдиного державного реєстру транспортних засобів у забезпеченні безпеки дорожнього руху?

Розділ 4.
ЄДИНИЙ РЕЄСТР ДОСУДОВИХ РОЗСЛІДУВАНЬ

Єдиний реєстр досудових розслідувань (ЄРДР) – це створена за допомогою автоматизованої системи електронна база даних, яка забезпечує централізоване збирання, зберігання, захист, облік, пошук і узагальнення інформації про кримінальні провадження. ЄРДР також використовується для формування звітності та надання відповідних даних згідно з вимогами Кримінального процесуального кодексу (КПК) України, з дотриманням законодавства щодо захисту персональних даних та інформації з обмеженим доступом.

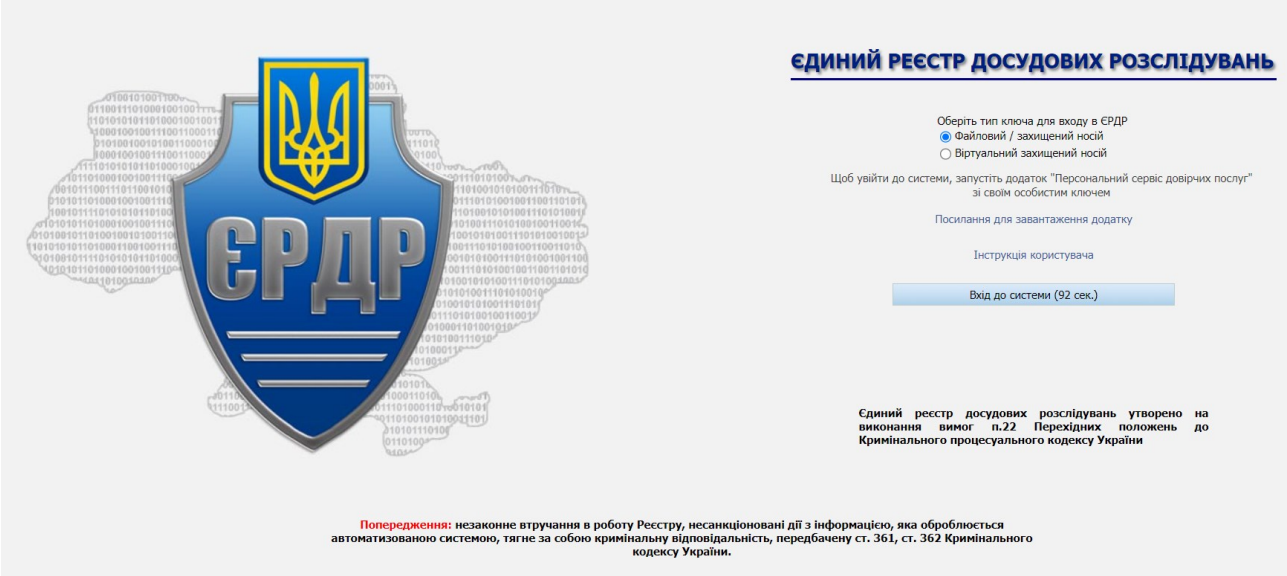

Рис. 25. Головна сторінка Єдиного реєстру досудових розслідувань (ЄРДР)

Ця система створена відповідно до положень КПК з метою:

- реєстрації кримінальних правопорушень та обліку рішень, прийнятих у ході досудового розслідування, включаючи дані про осіб, які скоїли правопорушення, та результати судового розгляду;
- забезпечення оперативного контролю за дотриманням законодавства під час досудового розслідування;

- аналізу стану та структури кримінальних правопорушень, що відбуваються в країні;
- інформаційно-аналітичної підтримки діяльності правоохоронних органів.

Оператором і адміністратором ЄРДР виступає *Генеральна прокуратура України*, яка відповідає за ведення та функціонування цієї бази даних, забезпечуючи її належне використання у межах чинного законодавства. Крім цього, ЄРДР сприяє підвищенню прозорості та підзвітності у діяльності правоохоронних органів, що є важливим аспектом забезпечення верховенства права в Україні.

Держатель Єдиного реєстру досудових розслідувань виконує наступні функції:

- розробка організаційних, методологічних та програмно-технічних засобів для ведення ЄРДР. Це включає технічне та технологічне створення, підтримку програмного забезпечення реєстру, адміністрування бази даних, моніторинг використання системи, забезпечення зберігання та захисту даних, а також контроль доступу до інформації.
- організація взаємодії з базами даних Міністерства внутрішніх справ України та Державної судової адміністрації України, забезпечуючи ефективний обмін даними.
- розробка та вдосконалення нормативно-правових документів, що регулюють створення, ведення та використання ЄРДР.

Користувачами ЄРДР є:

- керівники прокуратур та органів досудового розслідування;
- прокурори;
- слідчі органів поліції, Служби безпеки України, органів, що здійснюють контроль за дотриманням податкового законодавства, органів Державної кримінально-виконавчої служби України та

Державного бюро розслідувань, детективи Національного антикорупційного бюро;

- інші уповноважені особи органів прокуратури та досудового розслідування, які виконують функції інформаційно-аналітичного забезпечення правоохоронних органів і ведення спеціальних обліків (оперативних, оперативно-облікових, дактилоскопічних тощо).

Внесення відомостей до ЄРДР здійснюється Реєстратором через фіксацію інформації та вибір даних із довідників для заповнення документів первинного обліку щодо:

- кримінальних правопорушень;
- наслідків досудового розслідування;
- заподіяних збитків, результатів їх відшкодування та вилучення предметів злочинної діяльності;
- осіб, які вчинили кримінальне правопорушення, або підозрюваних у його вчиненні;
- руху кримінального провадження.

Форми документів первинного обліку та довідників є єдиними для Реєстраторів усіх правоохоронних органів, що забезпечує стандартизацію обліку.

Облік кримінальних правопорушень та осіб, які їх вчинили, ведеться відповідно до територіального принципу (за місцем вчинення правопорушення) або визначенням прокурора відповідного рівня згідно зі статтею 218 КПК України.

Обмін інформацією між ЄРДР та базами даних Міністерства внутрішніх справ здійснюється відповідно до чинного законодавства. Крім того, обмін даними щодо осіб у кримінальних провадженнях, інформація про яких міститься в ЄРДР та автоматизованій системі документообігу суду, а також облік та використання даних про результати судового провадження здійснюються з дотриманням законодавчих вимог.

Ці функції забезпечують єдність і ефективність роботи правоохоронних органів, сприяють захисту прав людини та зміцнюють верховенство права в державі.

Відомості з ЄРДР надаються у вигляді витягу відповідно до порядку, встановленого КПК України. Витяг з ЄРДР є документом, який підтверджує факт внесення до ЄРДР відомостей про кримінальне правопорушення.

Право доступу до відомостей, внесених до ЄРДР, мають:

- держатель у повному обсязі, з урахуванням повноважень, наданих прокурорам та керівникам підрозділів Генеральної прокуратури України;
- директор Національного бюро, його перший заступник, керівник Підрозділу детективів та керівник Управління внутрішнього контролю Національного бюро в межах, визначених статтею 17 Закону України «Про Національне антикорупційне бюро України»;
- прокурори та керівники регіональних, місцевих і військових прокуратур у межах кримінальних правопорушень, розслідування яких здійснюється слідчими прокуратури та слідчими піднаглядних їм органів;
- керівники органів прокуратури та досудового розслідування, слідчі органів прокуратури, поліції, безпеки, податкових органів, органів Державної кримінально-виконавчої служби України, Державного бюро розслідувань, Національного бюро в межах кримінальних правопорушень, які вони розслідують та за дотриманням вимог кримінального процесуального законодавства;
- користувачі в межах наданих адміністратором прав доступу для отримання інформації про розпочаті досудові розслідування, прийняті під час досудового розслідування рішення, ведення спеціальних обліків, проведення аналізу результатів діяльності правоохоронних органів.

На основі даних, внесених реєстраторами про кримінальні правопорушення та результати досудового розслідування, Адміністратори ЄРДР формують єдину звітність про кримінальні правопорушення, осіб, які їх вчинили, та рух кримінальних проваджень. Форма, періодичність подання звітності та правила її формування визначаються нормативними актами, погодженими з центральним органом виконавчої влади у галузі статистики.

Прокурори та керівники органів досудового розслідування на всіх рівнях забезпечують контроль у своїх відомствах за своєчасним, повним та достовірним внесенням інформації до ЄРДР у встановлені КПК України строки.

Реєстратор є відповідальною особою за своєчасність, повноту та об’єктивність внесених до Реєстру відомостей відповідно до чинного законодавства. Реєстратори та користувачі несуть відповідальність за порушення вимог Положення про ЄРДР, втрату, пошкодження електронних ключів доступу та незаконне втручання в роботу ЄРДР згідно з чинним законодавством.

Контрольні питання:

1. Що таке Єдиний реєстр досудових розслідувань (ЄРДР) і які його основні функції?
2. Які основні завдання ЄРДР у контексті досудового розслідування?
3. Хто є оператором і адміністратором ЄРДР, і які їхні функції?
4. Які органи мають право доступу до відомостей, внесених до ЄРДР, і в яких межах?
5. Які дії здійснює реєстратор під час внесення інформації до ЄРДР?
6. Як забезпечується обмін інформацією між ЄРДР та іншими базами даних, зокрема базами даних Міністерства внутрішніх справ?
7. Які права та обов'язки мають користувачі ЄРДР?
8. Яка відповідальність покладається на реєстраторів та користувачів ЄРДР за порушення вимог Положення про ЄРДР?

9. Як забезпечується стандартизація обліку кримінальних правопорушень у ЄРДР?

10. В яких випадках надається витяг з ЄРДР і що він підтверджує?

Розділ 5.
ЗАСТОСУВАННЯ ЦИФРОВОЇ КРИМІНАЛІСТИКИ В ДОСУДОВОМУ РОЗСЛІДУВАННІ

5.1. Поняття та сутність цифрової криміналістики.

Цифрова криміналістика, або *комп'ютерна криміналістика*, є міждисциплінарною галуззю знань, яка поєднує в собі принципи та методи інформаційних технологій, права, судової експертизи та кримінального розслідування. Вона спрямована на виявлення, збереження, аналіз та презентацію цифрових доказів у межах правової системи. Основна мета цифрової криміналістики полягає у виявленні істини у випадках, де цифрова інформація може бути ключовим елементом у розслідуванні злочинів або вирішенні юридичних суперечок.

Цифрова криміналістика включає процеси виявлення, вилучення, аналізу та інтерпретації електронних даних, які можуть слугувати доказами у кримінальних, цивільних або адміністративних справах. До основних об'єктів дослідження цифрової криміналістики належать комп'ютери, мобільні телефони, сервери, мережеві пристрої, хмарні сховища, електронна пошта, соціальні мережі та інші джерела цифрових даних.

Цифрові докази, на відміну від традиційних фізичних доказів, мають низку унікальних характеристик. По-перше, цифрові дані можуть бути легко скопійовані та передані без втрати якості. По-друге, цифрові докази можуть бути змінені або видалені, не залишаючи видимих слідів, що робить їх вразливими до маніпуляцій. По-третє, цифрові докази можуть бути збережені в різних форматах та на різних носіях, що вимагає використання спеціалізованих інструментів для їх вилучення та аналізу.

Сутність цифрової криміналістики полягає у систематичному та науково обґрунтованому підході до обробки цифрових доказів. Це включає:

– виявлення цифрових доказів: цей етап включає ідентифікацію потенційних джерел цифрових доказів у межах конкретного розслідування. Наприклад, це може бути комп'ютер підозрюваного, мобільний телефон жертви або сервер, який використовувався для передачі незаконної інформації;

– захоплення та збереження доказів: після виявлення цифрових доказів важливо їх правильно захопити та зберегти, щоб запобігти їх модифікації або видаленню. Цей процес включає створення точних копій (образів) цифрових носіїв, використовуючи спеціалізоване програмне забезпечення та апаратні засоби, які забезпечують цілісність даних;

– аналіз цифрових доказів: на цьому етапі експерти з цифрової криміналістики здійснюють детальний аналіз зібраних даних з метою виявлення релевантної інформації, яка може підтвердити або спростувати певні факти у справі. Аналіз може включати відновлення видалених файлів, розшифровку зашифрованих даних, дослідження метаданих, аналіз мережевої активності тощо;

– документування та презентація результатів: завершальним етапом є підготовка звіту, в якому представлені результати аналізу. Звіт має бути складений так, щоб його могли зрозуміти не тільки фахівці, але й представники судової системи, адвокати та інші зацікавлені сторони. Документування також включає підготовку до можливого свідчення в суді, де експерт має бути готовий пояснити свої висновки та методи, що були використані для їх досягнення.

5.2. Основні етапи процесу цифрової криміналістики.

Цифрова криміналістика, як наукова дисципліна, передбачає систематичний підхід до виявлення, збору, аналізу та документування цифрових доказів, що можуть бути використані в судових процесах. Процес цифрової криміналістики базується на суворих методологічних принципах і складається з кількох основних етапів, які забезпечують надійність і достовірність отриманих

доказів. Кожен етап має важливе значення для досягнення кінцевої мети – отримання та збереження доказів, які можуть бути використані у правовому контексті.

1. Ідентифікація та виявлення

Першим етапом є ідентифікація джерел потенційних цифрових доказів. Цей етап включає виявлення об'єктів, які можуть містити релевантну інформацію для розслідування. Цифрові пристрої, такі як комп'ютери, мобільні телефони, сервери, а також хмарні сервіси, є основними джерелами таких доказів. Важливо провести попередній аналіз для виявлення всіх можливих джерел інформації, включаючи нетрадиційні носії, такі як IoT-пристрої або блокчейн-технології.

Цей етап також передбачає розробку плану дослідження, який визначає, які саме дані потрібно виявити, де їх шукати та які методи будуть використані для їх вилучення. Успіх цього етапу залежить від точного визначення джерел даних, їхнього місцезнаходження та правового статусу, що дозволяє уникнути втрати потенційно важливих доказів.

2. Захоплення та збирання

На етапі захоплення відбувається фізичне або логічне вилучення цифрових доказів з їх джерел. Це може включати створення образів жорстких дисків, вилучення даних з оперативної пам'яті, збереження вмісту мобільних пристроїв або вилучення даних з хмарних сховищ. Основним завданням цього етапу є забезпечення цілісності та автентичності даних.

Збирання доказів має бути проведене з урахуванням принципу беззмінності, тобто дані мають бути зібрані таким чином, щоб виключити можливість їх зміни під час вилучення. Для цього використовуються спеціалізовані інструменти та методи, такі як write-blockers, які запобігають запису на носій під час його дослідження.

3. Збереження та консервація

Після збирання цифрових доказів важливо забезпечити їхнє збереження в умовах, що гарантують їх цілісність та захист від несанкціонованого доступу.

Консервація даних включає створення резервних копій, шифрування даних та їх фізичний захист.

На цьому етапі важливо також забезпечити документування всіх дій, пов'язаних зі збереженням доказів, включаючи створення детальних журналів доступу, які дозволять відстежувати всі зміни та доступ до даних. Це забезпечує ланцюжок збереження (chain of custody), який гарантує, що дані залишаються незмінними від моменту їх вилучення до подання в суді.

4. Аналіз та інтерпретація

Аналіз є одним із найскладніших і найбільш відповідальних етапів процесу цифрової криміналістики. Він включає систематичне дослідження зібраних даних з метою виявлення доказів, які можуть підтвердити або спростувати певні гіпотези в рамках розслідування. Аналіз може включати різні методи, такі як:

Форензічний аналіз даних: відновлення видалених файлів, аналіз метаданих, дослідження структури файлів.

Мережевий аналіз: аналіз трафіку, дослідження логів мережевої активності, виявлення підозрілої активності.

Аналіз мобільних пристроїв: вилучення даних з мобільних телефонів, включаючи текстові повідомлення, дзвінки, дані додатків.

Криптографічний аналіз: розшифровка зашифрованих даних, виявлення прихованих інформаційних потоків.

Цей етап вимагає використання сучасних інструментів та методик, які дозволяють автоматизувати процеси аналізу та забезпечують високу точність результатів. Важливо, щоб результати аналізу були документовані з використанням детальної методології, що дозволяє відтворити отримані висновки в суді.

5. Документування та презентація

Документування всіх етапів процесу цифрової криміналістики є ключовим для забезпечення прийнятності доказів у суді. Документування включає створення детальних звітів, які описують всі дії, що були виконані під час розслідування, методи, що використовувалися, та результати, які були досягнуті.

Презентація результатів має бути чіткою, зрозумілою та орієнтованою на потреби суду. Важливо, щоб експерт міг не тільки представити результати аналізу, але й пояснити використані методи та їх відповідність встановленим стандартам.

Звіт повинен містити чіткі висновки, засновані на отриманих даних, і бути підкріплений відповідними доказами, які можуть бути перевірені та підтверджені іншими фахівцями в галузі. У разі необхідності експерт повинен бути готовим надати додаткові пояснення або відповісти на питання, пов'язані з методологією або отриманими результатами.

Отже, основні етапи процесу цифрової криміналістики є взаємопов'язаними і спрямованими на досягнення максимальної достовірності та надійності отриманих доказів. Дотримання всіх етапів процесу є критично важливим для забезпечення законності та прийнятності цифрових доказів у судовому процесі. В умовах стрімкого розвитку інформаційних технологій цифрова криміналістика стає невід'ємною частиною сучасної системи правосуддя, що забезпечує ефективне розслідування та справедливий судовий розгляд.

5.3. Інструменти та методи цифрової криміналістики.

Програмне забезпечення для цифрової криміналістики відіграє ключову роль у процесі збору, аналізу та документування цифрових доказів. У сучасній практиці використовуються різноманітні інструменти та платформи, які забезпечують всебічну підтримку всіх етапів розслідування. Ці інструменти допомагають експертам ефективно обробляти великі обсяги даних, автоматизувати рутинні процеси та забезпечувати високу точність результатів. Програмне забезпечення для цифрової криміналістики можна поділити на кілька категорій залежно від його функціонального призначення.

Інструменти для створення образів дисків (Disk Imaging Tools).

Одним із перших і найбільш важливих кроків у цифровій криміналістиці є створення образів дисків, тобто копій усіх даних, що зберігаються на цифровому носії. Цей процес має бути виконаний таким чином, щоб забезпечити точність і цілісність копії, яка буде використовуватися для подальшого аналізу.

Популярні інструменти:

FTK Imager: відомий інструмент для створення образів дисків, який дозволяє здійснювати детальний попередній перегляд даних перед їх копіюванням. FTK Imager підтримує різні формати збереження та забезпечує високу швидкість роботи.

dd: це утиліта командного рядка, доступна в UNIX-подібних операційних системах, яка використовується для копіювання і створення образів дисків на низькому рівні. Вона є потужним інструментом, хоча потребує певних навичок для ефективного використання.

EnCase: програмний комплекс, який окрім створення образів дисків, включає широкий спектр функцій для аналізу та управління цифровими доказами.

Інструменти для аналізу файлів та даних (File and Data Analysis Tools).

Аналіз файлів та даних є одним із найбільш ресурсоємних етапів цифрової криміналістики. Для його виконання використовуються інструменти, які дозволяють досліджувати файлові системи, відновлювати видалені файли, аналізувати метадані, а також досліджувати приховані або зашифровані файли.

Популярні інструменти:

Autopsy: Це потужна платформа з відкритим кодом для аналізу файлових систем і дисків, яка дозволяє відновлювати видалені файли, досліджувати хронологію подій та аналізувати різні типи медіафайлів.

X-Ways Forensics: Програмне забезпечення, що забезпечує глибокий аналіз файлових систем, пошук за сигнатурами файлів, відновлення даних і багатозадачну роботу з великими обсягами інформації.

The Sleuth Kit (TSK): Набір утиліт для аналізу файлових систем, який підтримує роботу з різними файловими системами, включаючи FAT, NTFS, exFAT та інші.

Інструменти для аналізу мобільних пристроїв (Mobile Device Forensics Tools).

Мобільні пристрої, такі як смартфони та планшети, часто містять велику кількість важливих даних, включаючи текстові повідомлення, дзвінки, дані з додатків та геолокаційні дані. Аналіз мобільних пристроїв вимагає спеціалізованих інструментів, здатних працювати з різними операційними системами та типами даних.

Популярні інструменти:

Cellebrite UFED: Один із найбільш відомих інструментів для аналізу мобільних пристроїв, який підтримує роботу з багатьма моделями телефонів і планшетів. UFED дозволяє вилучати дані з різних джерел, включаючи повідомлення, журнали дзвінків, мультимедійні файли та інше.

MOBILedit Forensic: Програма, що дозволяє проводити глибокий аналіз мобільних пристроїв, включаючи доступ до видалених даних, копіювання інформації з SIM-карт і аналіз даних з різних мобільних додатків.

Oxygen Forensic Detective: Це комплексне рішення для вилучення, аналізу та інтерпретації даних з мобільних пристроїв, яке підтримує широкий спектр пристроїв та типів даних.

Інструменти для мережевої криміналістики (Network Forensics Tools).

Мережеві криміналістичні інструменти використовуються для збору, моніторингу та аналізу мережевого трафіку з метою виявлення шкідливої активності, аналізу атак і збору цифрових доказів. Ці інструменти дозволяють відстежувати комунікації, виявляти зловмисників і відновлювати події, що відбувалися в мережі.

Популярні інструменти:

Wireshark: Один із найбільш поширених інструментів для аналізу мережевого трафіку. Wireshark дозволяє захоплювати пакети даних у реальному часі, аналізувати їх вміст і визначати аномалії або підозрілу активність.

NetworkMiner: Це інструмент для пасивного аналізу мережевого трафіку, який дозволяє збирати та аналізувати дані про сесію, файли, сертифікати та іншу інформацію, що передається мережею.

tcpdump: Утиліта командного рядка для захоплення мережевих пакетів і аналізу трафіку, яка є потужним інструментом для розслідування інцидентів, пов'язаних із мережевою активністю.

Інструменти для аналізу шкідливого ПЗ (Malware Analysis Tools).

Аналіз шкідливого програмного забезпечення (Malware) є важливим аспектом цифрової криміналістики, особливо у випадках, пов'язаних з кіберзлочинністю. Інструменти для аналізу шкідливого ПЗ дозволяють досліджувати поведінку шкідливих програм, ідентифікувати їх джерела та розробляти методи захисту.

Популярні інструменти:

IDA Pro: це інтерактивний дизасемблер і відладчик, який дозволяє проводити статичний та динамічний аналіз шкідливого ПЗ, досліджуючи його внутрішню структуру та функції.

Cuckoo Sandbox: платформа для динамічного аналізу шкідливого ПЗ, яка автоматично запускає підозріле програмне забезпечення в ізольованому середовищі та спостерігає за його поведінкою.

VirusTotal: онлайн-сервіс, який дозволяє перевірити файли та URL-адреси на наявність шкідливого ПЗ за допомогою багатьох антивірусних двигунів і отримати детальну інформацію про знайдені загрози.

Методи захоплення та аналізу даних з цифрових носіїв є ключовими компонентами процесу цифрової криміналістики, що дозволяють забезпечити збереження, дослідження та використання цифрових доказів у розслідуванні кримінальних правопорушень. Взаємодія цих методів із програмним забезпеченням, забезпечує комплексний підхід до збирання та аналізу

інформації, яка може мати критичне значення в контексті правового розслідування.

Процес захоплення даних полягає у створенні точних копій інформації з цифрових носіїв, таких як жорсткі диски, мобільні пристрої, флеш-накопичувачі та інші носії даних. Цей процес є надзвичайно важливим, оскільки дозволяє зберегти оригінальні дані в їхньому первісному вигляді, що є необхідною умовою для їх подальшого використання як доказів у судовому процесі.

Рис. 26. Основні методи комп’ютерної криміналістики

Інтеграція методів захоплення та аналізу даних є ключовою для забезпечення надійності й достовірності цифрових доказів. Використання програмних інструментів, таких як EnCase, Autopsy або X-Ways Forensics, дозволяє не лише захоплювати дані, але й проводити їх комплексний аналіз, що дає змогу отримувати повну картину того, що відбувалося на цифровому носії.

Ці інструменти забезпечують високий рівень автоматизації, що дозволяє значно скоротити час обробки даних та підвищити точність результатів.

Таким чином, ефективне захоплення та аналіз даних з цифрових носіїв є основою для успішного проведення цифрової криміналістики. Ці методи не тільки забезпечують збереження цифрових доказів, але й дозволяють отримати важливу інформацію для розслідування, яка може бути використана в суді для підтримки або спростування певних версій подій. Інтеграція передових програмних інструментів і дотримання кращих практик захоплення й аналізу даних є ключовими для досягнення високої ефективності та точності в цифровій криміналістиці.

Контрольні питання:

1. Що таке цифрова криміналістика, і які міждисциплінарні галузі знань вона поєднує?
2. Яка основна мета цифрової криміналістики?
3. Які об'єкти дослідження включає цифрова криміналістика?
4. Які особливості мають цифрові докази порівняно з традиційними фізичними доказами?
5. У чому полягає сутність цифрової криміналістики?
6. Які етапи включає процес цифрової криміналістики?
7. Які джерела потенційних цифрових доказів необхідно виявити на етапі ідентифікації?
8. Як забезпечується цілісність і автентичність даних на етапі захоплення та збирання цифрових доказів?
9. Які дії входять до етапу збереження та консервації цифрових доказів?
10. Які методи використовуються на етапі аналізу та інтерпретації цифрових доказів?
11. Чому важливе документування та презентація результатів у цифровій криміналістиці?

12. Які програмні інструменти використовуються для створення образів дисків у цифровій криміналістиці?

13. Які інструменти застосовуються для аналізу файлів та даних?

14. Які можливості надають інструменти для аналізу мобільних пристроїв?

15. Як мережеві криміналістичні інструменти допомагають у виявленні та аналізі шкідливої активності в мережах?

16. Які інструменти використовуються для аналізу шкідливого ПЗ, і в чому їхні переваги?

Додаток А

Об’єкт	**Сервіси та ресурси для пошуку або аналізу об’єкта**
Точка доступу Wi-Fi	wigle.net, alexell.ru/network/mac-geo/
Банківська платіжна картка	binbase.com/search.html, bindb.com/bin-database.html, bincodes.com/bin-checker/ (встановлення банку-емітента за номером картки)
Мобільний телефон	truecaller.com, sync.me, findnumberapp.com, phonenumber-lookup.info,github.com/sundowndev/ PhoneInfoga, застосунки: Getcontact, Eyecon, Telegram-боти @get_kontakt_bot, @getfb_bot
Електронна пошта	github.com/alpkeskin/mosint, github.com/megadose/holehe
Фотознімки	exif.regex.info/exif.cgi, imageforensic.org, fotoforensics.com, jimpl.com, play.google.com/store/ apps/details?id=com.exiftool.free
Зображення	/github.com/adamian98/pulse/, покращення якості зображень /github.com/DmitryUlyanov/deep-image-prior, demos.algorithmia.com/colorize-photos, myheritage.nl/photo-enhancer, letsenhance.io, improvephoto.net, pinkmirror.com

Додаток Б

Загальний перелік інформаційних ресурсів, що функціонують у системі «Інформаційний портал Національної поліції»

№ з/п	Назва інформаційної підсистеми ІПНП НПУ	Призначення інформаційної підсистеми	Нормативно-правова база функціонування інформаційної підсистеми
1	ІТС ІПНП	Інформаційно-комунікаційна система «Інформаційний портал Національної поліції України» - сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення.	Наказ МВС України від 03.08.2017 № 676 «Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» (зареєстровано в Міністерстві юстиції України 28.08.2017 за №1059/30927).
2	ЦУНАМІ	Інформаційно-програмний комплекс призначений для управління силами й засобами органів (підрозділів) поліції. Дозволяє управляти нарядами поліції для реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події у режимі реального часу.	Наказ МВС України від 16.02.2018 № 111 «Про затвердження Інструкції з організації реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України».

3	HotLine	Гаряча лінія НПУ (повідомлення про неправомірні дії працівників поліції, отримання інформації про первинну реєстрацію у органах (підрозділах) поліції звернень, поданих до гарячої лінії (call-centre), отримання довідкової інформації)	Нормативні підстави щодо функціонування системи відсутні.
4	АРМ 102	Облік повідомлень на лінію «102» за допомогою телекомунікаційних мереж. Забезпечує прийняття, фіксацію, оброблення та реєстрацію повідомлень про правопорушення та інші події, передачу інформації про них відповідним оперативно-диспетчерським службам для організації реагування на такі повідомлення.	Наказ МВС України від 16.02.2018 № 111 «Про затвердження Інструкції з організації реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України».
5	Єдиний облік	Облік заяв і повідомлень про вчинені кримінальні правопорушення та інші події, які прийняти та зареєстровані органами поліції. В зазначеній підсистемі накопичується	Наказ МВС України від 08.09.2019 № 100 «Про затвердження Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події» Наказ МВС України № 508 від 14.06.2019 «Про затвердження Інструкції з формування та

		інформація щодо обставин скоєння правопорушення, опису правопорушника, місця скоєння злочину, у тому числі географічних координат, способу скоєння, відомостей стосовно осіб, предметів посягання.	ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».
6	Кримінальні провад-ження	Облік відомостей про кримінальні правопорушення, осіб, які їх вчинили або підозрюються в їх вчиненні, досудове розслідування за якими здійснюється слідчими органів поліції.	пункт 2 частини першої статті 26 Закону України «Про Національну поліцію»; Наказ Генпрокуратури України, МВС України від 17.11.2012 № 115/1046 «Про затвердження Порядку взаємодії Генеральної прокуратури України та Міністерства внутрішніх справ України щодо обміну інформацією з Єдиного реєстру досудових розслідувань та інформаційних систем органів внутрішніх справ» Наказ ГПУ від 06.04.2016 №139 «Про затвердження Положення про порядок ведення Єдиного реєстру досудових розслідувань».
7	Корупція	Облік відомостей щодо зареєстрованих кримінальних та адміністративних корупційних правопорушень, осіб, які їх вчинили, та результатів розгляду цих правопорушень у судах.	Наказ ГПУ, МВСУ, СБУ, МДЗУ, МОУ, ДСАУ від 22.04.2013 № 52/394/172/71/ 268/60 «Про затвердження Інструкції про порядок обліку кримінальних та адміністративних корупційних правопорушень».

8	Адмінпрак-тика	Облік відомостей щодо виявлених адміністративних правопорушень, осіб, які їх вчинили, та результатів розгляду цих правопорушень компетентними органами	пункт 2 частини першої статті 26 Закону України «Про Національну поліцію»; Наказ МВС України № 595 від 04.07.2016 «Про затвердження Інструкції з автоматизованого обліку адміністративних правопорушень».
9	Адмінпрак-тика -штрафи	Дані про сплату штрафів за вчинені адміністративні правопорушення у сфері безпеки дорожнього руху в автоматичному режимі.	Наказ МВС України від 20.06.2013 № 606 «Про вдосконалення процедури сплати штрафів за порушення Правил дорожнього руху та застосування механізму автоматичного заліку таких штрафів під час оформлення коштів» (зареєстровано в Міністерстві юстиції України 27.06.2013 за № 1093/23625). Доручення НПУ від 20.07.2016 № 7914/01/46-2016 «Про впорядкування автоматизованого обліку адміністративних правопорушень, у тому числі бланкової продукції, протоколів та постанов, та дорожньо-транспортних пригод».
10	Склад (облік бланкової продукції)	Облік бланкової продукції НПУ	Доручення НПУ від 20.07.2016 № 7914/01/46-2016 «Про впорядкування автоматизованого обліку адміністративних правопорушень, у тому числі бланкової продукції, протоколів та постанов, та дорожньо-транспортних пригод».
11	ДТП	Облік відомостей про дорожньо-транспортні пригоди, що сталися на території України, осіб,	Наказ НПУ № 533 від 15.07.2020 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми

		які скоїли ДТП, транспортні засоби, та місце зіткнення	«Дорожньо-транспортна пригода» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» (зареєстровано в Міністерстві юстиції України 31.07.2020 за №726/35009).
12	Розшук	Облік відомостей щодо підозрюваних, обвинувачених (підсудних), осіб, які ухиляються від відбування покарання або вироку суду, та безвісно зниклих осіб	пункти 3 та 4 частини першої статті 26 Закону України «Про Національну поліцію"; Наказ МВС України від 05.01.2005 №3дск (зареєстровано в Міністерстві юстиції України 01.02.2005 за № 132/10412), зі змінами затвердженими наказом МВС від 26.11.2012 № 1084/дск (зареєстровано в Міністерстві юстиції України 27.12.2012 за № 2199/22511) «Про затвердження Інструкції з організації розшуку підозрюваних, обвинувачених (підсудних), осіб, які ухиляються від відбування кримінального покарання, безвісно зниклих осіб та встановлення особи невпізнаних трупів».
13	Пізнання	Облік відомостей щодо підозрюваних, обвинувачених (підсудних), осіб, які ухиляються від відбування покарання або вироку суду, зниклих безвісти, невпізнаних трупів та осіб, які не здатні через стан здоров’я або вік повідомити	пункти 3 та 4 частини першої статті 26 Закону України «Про Національну поліцію»; Наказ МВС України від 05.01.2005 № 3дск (зареєстровано в Міністерстві юстиції України 01.02.2005 за № 132/10412), зі змінами затвердженими наказом МВС від 26.11.2012 № 1084/дск (зареєстровано в Міністерстві юстиції України 27.12.2012 за № 2199/22511)

		інформацію про себе. Проведення в автоматизованому режимі пошукових і пізнавальних заходів з метою розшуку та ідентифікації осіб (трупів).	«Про затвердження Інструкції з організації розшуку підозрюваних, обвинувачених (підсудних), осіб, які ухиляються від відбування кримінального покарання, безвісно зниклих осіб та встановлення особи невпізнаних трупів».
14	Гарпун	Облік відомостей про транспортні засоби та номерні знаки транспортних засобів, що розшукуються у рамках кримінального, виконавчого проваджень, проваджень в справах про адміністративні правопорушення, оперативно-розшукової діяльності, а також за ухвалою слідчого судді, суду.	пункт 14 частини першої статті 26 Закону України «Про Національну поліцію»; наказ МВС України від 13.06.2018 № 497 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», зареєстрованої в Мін'юсті 06.07.2018 за №787/32239; наказ НПУ від 11.03.2019 № 217 «Про введення в експлуатацію інформаційної підсистеми «Гарпун»; доручення НПУ від 19.04.2019 № 4624/01/27-2019 «Про запровадження в експлуатацію програмного модуля аналітичної обробки інформації про розшук транспортного засобу»; Робочий проект «Інформаційна підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».
15	Особа	Облік відомостей щодо осіб, які вчинили правопорушення, у тому числі тих	пункт 1 частини першої статті 26 Закону України «Про Національну поліцію»; наказ МВС України від 28.07.2017

		відносно яких поліцейські здійснюють профілактичну роботу.	№ 650 «Про затвердження Інструкції з організації діяльності дільничних офіцерів поліції», зареєстрованої в Мін'юсті 21.08.2017 за №1041/30909; наказ МВС України від 19.12.2017 № 1044 «Про затвердження Інструкції з організації роботи підрозділів ювенальної превенції Національної поліції України», зареєстрованої в Мін'юсті 07.06.2018 за № 686/32138.
16	Зареєстрована зброя	Облік зброї, що перебуває в користуванні фізичних та юридичних осіб та яка обліковується підрозділами дозвільної системи.	пункт 16 частини першої статті 26 Закону України «Про Національну поліцію»; наказ МВС України від 21.08.1998 № 622 (зі змінами) «Про затвердження Інструкції про порядок виготовлення, придбання, зберігання, обліку, перевезення та використання вогнепальної, пневматичної, холодної і охолощеної зброї, пристроїв вітчизняного виробництва для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями метальними снарядами несмертельної дії, та патронів до них, а також боєприпасів до зброї, основних частин зброї та вибухових матеріалів», зареєстрованої в Мін'юсті 07.10.1998 за № 637/3077.
17	Криміналь-на зброя	Облік викраденої, втраченої, вилученої, знайденої та добровільно зданої із числа тієї, що	Наказ МВС України від 31.05.1993 № 314 «Про затвердження Інструкції про порядок приймання, зберігання, обліку, знищення чи реалізації

		незаконно зберігалася зброї та деталей зброї.	вилученої, добровільно зданої, знайденої зброї та боєприпасів до неї», зареєстрованої в Мін'юсті 12.08.1993 за № 106.
18	Custody Records	Процес фіксації, формування, накопичення, обліку та пошуку інформації про факти затримання, доставлення, ідентифікації, документування, опитування затриманої особи в органі (підрозділі) поліції, ізоляторі тимчасового тримання.	пункт 7 частини першої статті 26 Закону України «Про Національну поліцію»; наказ НПУ від 28.12.2020 № 1041 «Про впровадження пілотного проекту «Інформаційна підсистема «CustodyRecords» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».
19	ІТТ-Custody Records	Облік відомостей про роботу ІТТ та осіб, які в них утримуються.	Меморандум про співпрацю між Національною поліцією України та Міністерством юстиції України у сфері надання безоплатної правової допомоги від 12 лютого 2016 року стосовно недопущення порушень прав людини на захист під час затримання, тортур, нелюдського поводження із затриманими, запобігання випадків засудження невинних людей та порушення гарантій адвокатської діяльності. Доручення НПУ від 25.03.2016 № 3173/01/37-2016 «Про випробовування та впровадження в тестову експлуатацію інформаційної підсистеми «ІТТ» у складі інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».

20	Затримані і доставлені	Облік осіб затриманих і доставлених до органу (підрозділу) поліції за підозрою у вчиненні правопорушень та надання таким особам безоплатної вторинної правової допомоги.	пункт 7 частини першої статті 26 Закону України «Про Національну поліцію»; Наказ МВС України 23.05.2017 № 440 «Про затвердження Інструкції з організації діяльності чергової служби органів (підрозділів) Національної поліції України», зареєстровано в Міністерстві юстиції України 15 червня 2017 р. за №750/30618.
21	Втрачені документи	Облік викрадених (втрачених) документів за зверненням громадян, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери.	пункт 12 частини першої статті 26 Закону України «Про Національну поліцію» Наказ МВС України від 12.10.2009 №436 «Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України» (зареєстровано в Міністерстві юстиції України 28.12.2009 за №1256/17272).
22	Річ	Облік викрадених, вилучених речей, цінностей та іншого майна, що має характерні ознаки для ідентифікації.	пункт 12 частини першої статті 26 Закону України «Про Національну поліцію»; наказ МВС України від 14.06.2019 № 508 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», зареєстрованої в Мін’юсті 04.07.2019 за №739/33710.
23	Антикваріат	Облік викрадених, вилучених культурних цінностей, що належать до об’єктів	Наказ МВС України від 12.10.2009 № 436 «Про затвердження Положення про Інтегровану інформаційно-

		матеріальної і духовної культури та мають художнє, історичне, етнографічне та наукове значення.	пошукову систему органів внутрішніх справ України» (зареєстровано в Міністерстві юстиції України 28.12.2009 за № 1256/17272).
24	Виконавче проваджен-ня	Облік постанов державних та приватних виконавців про розшук/припинення транспортного засобу боржника, встановлення/скасування тимчасового обмеження боржника в праві користування зброєю та керуванні транспортними засобами.	Наказ МВС та Мін'юсту від 30.01.2018 № 64/261/5 «Про затвердження Порядку взаємодії Міністерства внутрішніх справ України, Національної поліції України та органів і осіб, які здійснюють примусове виконання судових рішень і рішень інших органів», зареєстровано в Мін'юсті від 05.02.2018 за №140/31592.
25	Домашній арешт	Облік підозрюваних, обвинувачених, які перебувають під домашнім арештом.	пункт 7 частини першої статті 26 Закону України «Про Національну поліцію»; наказ МВС України від 13.07.2016 № 654 «Про затвердження Інструкції про порядок виконання органами Національної поліції ухвал слідчого судді, суду про обрання запобіжного заходу у вигляді домашнього арешту та про зміну раніше обраного запобіжного заходу на запобіжний захід у вигляді домашнього арешту», зареєстрованої в Мін'юсті 03.08.2016 за №1087/29217.
26	Тимчасовий заборонний припис	Облік термінових заборонних приписів стосовно кривдників для запобігання та протидії домашньому	Закон України «Про запобігання та протидію домашньому насильству», Наказ МВС України від 01.08.2018 №654 «Про затвердження Порядку

		насильству, забезпечення вжиття заходів з негайного його припинення, недопущення продовження чи повторного вчинення.	винесення уповноваженими підрозділами органів Національної поліції України термінового заборонного припису стосовно кривдника. Доручення НПУ від 04.02.2020 №1455 «Про внесення інформації до ІП «Терміновий заборонній припис стосовно кривдника».
27	Драгер	Облік спеціальних технічних засобів, якими здійснюється проведення огляду водіїв транспортних засобів на стан алкогольного сп'яніння (Drager) та облік інформації про осіб, які тестуються із зазначенням результатів тестування.	Наказ МВС України та Міністерство охорони здоров'я від 09.11.2015 №1452/7354 «Про затвердження Інструкції про порядок виявлення у водіїв транспортних засобів ознак алкогольного, наркотичного чи іншого сп'яніння або перебування під впливом лікарських препаратів, що знижують увагу та швидкість реакції, зареєстровано в Мінюсті. 11.11.2015 №1413/27858.
28	Дозвіл БДР	Облік дозволів на рух окремих категорій транспортних засобів, у тому числі небезпечних та негабаритних вантажів.	пункт 15 статті 26 Закону «Про Національну поліцію»; Наказ МВС України від 04.08.2018 № 656 «Про затвердження деяких нормативно-правових актів з питань дорожнього перевезення небезпечних вантажів» (Зареєстровано в Міністерстві юстиції України 11 вересня 2018 р. за №1041/32493). Доручення НПУ №14342 від 28.12.2016 «Про організацію роботи щодо використання інформаційної підсистеми «Дозвіл ДБР».
29	Протидія ОГ та ЗО	Облік результатів розгляду у судах	Доручення НПУ № 6667/01/15-2019 від 06.06.2019

		кримінальних проваджень, розпочатих стосовно організованих злочинних груп і злочинних організацій	«Про розробку та впровадження в органах та підрозділах поліції інформаційної підсистеми «Протидія ОГ та ЗО».
30	Розслідування	Облік інформації про розбої, що вчинено на території України.	Доручення НПУ № 1713/01/14-2019 від 11.02.2019 «Про порядок обліку в інформаційно-комунікаційній системі ІПНП відомостей про розбої».
31	Паспорт поліцейської дільниці	Облік інформації щодо поліцейських дільниць, їх характеристик та закріплених працівників, з відображенням на мапі України.	Доручення НПУ від 25.09.2019 № 10954/02/20-2019 «Про впорядкування діяльності поліцейських дільниць та запровадження інформаційної підсистеми «Паспорт поліцейської дільниці».
32	УЗПЛ Huamn rights	Облік порушень прав людини працівниками органів (підрозділів) поліції, у т.ч. працівниками ІТТ щодо утримуваних в них осіб.	пункт 2.2 Плану основних заходів Національної поліції України на 2017 рік (ДДЗ НП від 28.12.2016 № 14257/02/25-2016).
33	Облік GPS - пристроїв	Облік GPS - пристроїв, які встановлено на службовий транспорт Національної поліції України.	Доручення НПУ від 18.10.2019 № 11788/01/27-2019 «Про проведення в Національній поліції пілотного проекту GPS - моніторингу».
34	Облік SIM карток	Облік СІМ-карток, які використовуються в планшетних пристроях поліцейських.	Наказ НПУ № 244 від 14.03.2018 Про затвердження Порядку контролю за використанням SIM-карток для пристроїв рухомого (мобільного) зв'язку, які використовуються для роботи з інформаційними ресурсами НПУ.

35	Об'єкт дозвільної системи	Облік дозволів на відкриття об’єктів дозвільної системи та отримання інформації щодо наданих дозволів територіальними підрозділами Національної поліції при отриманні ліцензій в МВС.	Доручення НПУ від 03.01.2020 № 102 «Про порядок обліку в інформаційно-телекомунікаційній системі «Інформаційний портал Національної поліції України» відомостей про дозволи на відкриття об’єктів дозвільної системи».
36	Службовий транспорт	Облік службового транспорту.	Наказ НПУ від 27.04.2018 № 439 «Про впровадження в органх і підрозділах поліції інформаційної підсистеми Службовий транспорт . Наказ МВС України від 07.09.2017 №757 «Про затвердження Порядку використання і зберігання транспортних засобів Національної поліції України».
37	Комп`ютер-на техніка	Облік комп'ютерної техніки.	Наказ НПУ від 22.05.2018 № 509 «Про організацію інформаційного обліку комп’ютерної техніки та комп’ютерних програм, що використовуються в органах та підрозділах поліції».
38	Затримані ТЗ	Облік відомостей про ТЗ, що евакуйовано до спеціального майданчика чи стоянки на підставі акту огляду та тимчасового затримання ТЗ, що складено поліцейським.	наказ МВС України від 13.06.2018 № 497 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», зареєстрованої в Мін’юсті 06.07.2018 за № 787/32239; постанова КМУ від 17.12.2008 № 1102 «Про затвердження Порядку тимчасового затримання

			та зберігання транспортних засобів на спеціальних майданчиках і стоянках»; наказ МВС від 07.11.2015 № 1395 «Про затвердження Інструкції з оформлення поліцейськими матеріалів про адміністративні правопорушення у сфері забезпечення безпеки дорожнього руху, зафіксовані не в автоматичному режимі», зареєстрованої в Мін'юсті 10.11.2015 за № 1408/27853.
39	Службове завдання	Інформаційно-програмний комплекс призначений для формування переліку додаткових завдань для ГРПП.	Доручення НПУ від 22.08.2019 № 9796/04/20-2019 «Про організацію превентивних заходів з використанням інформаційної підсистеми «Службове завдання».
40	Дорожній лист	Облік видачі дорожніх листів службового транспорту.	Наказ НПУ від 28.12.2018 № 1231 «Про впровадження в органах та підрозділах поліції інформаційної підсистеми «Дорожній лист».
41	Коронавірус	Облік осіб, у яких є підтвердження або підозра у зараженні коронавірусної хворобою COVID-19, та місць їх обсервації.	Доручення НПУ від 24.03.2020 № 3804/01/25-2020 «Про запобігання поширенню на території України коронавірусної хвороби (COVID-19)».
42	Атріум	Інформаційно-програмний комплекс призначений для: - формування та наповнення електронного журналу контролю за прибуттям та поставленням на облік раніше судимих осіб за формою,	Наказ МВС України від 11 грудня 2019 року № 1032 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Атріум» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», зареєстрований в Міністерстві

		визначеною в додатку 26 до Порядку взаємодії установ виконання покарань, уповноважених органів з питань пробації та суб'єктів соціального патронажу під час підготовки до звільнення осіб, які відбувають покарання у вигляді обмеження волі або позбавлення волі на певний строк, затвердженого наказом міністерства соціальної політики України, міністерства охорони здоров'я України, міністерства внутрішніх справ України від 03 квітня 2018 року № 974/5/467/609/280, зареєстрованого в Міністерстві юстиції України 05 квітня 2018 року за № 408/31860, а також контролю за поведінкою осіб, щодо яких встановлено адміністративний нагляд;- інформаційно-аналітичного забезпечення діяльності поліції, у тому числі з використанням геоінформаційних підсистем для	юстиції України 27 лютого 2020 р. за №217/34500.

		візуалізації інформації у вигляді електронних карт, при проведенні аналізу та встановлення зв'язків між даними, що мають значення під час розслідування кримінальних правопорушень;- установлення місцезнаходження осіб, що яких встановлено адміністративний нагляд та які ухиляються від обліку.	
43	Доручення слідчого	Облік доручень винесених слідчими підрозділами НПУ.	Доручення МВС України від 26.11.2014 № 24984/Ск «Про забезпечення підключення міськрайлінорганів до ІП «Слідство: доручення» ІІПС ОВС». Доручення МВС України від 03.12.2014 № 25621/Ск «Про організацію обліку доручень слідчих щодо проведення слідчих (розшукових) дій».
44	Інспектор	Облік порушень законності, допущеної працівниками поліції під час реєстрації та розгляду заяв і повідомлень про вчинені кримінальні правопорушення та інші події.	Наказ НПУ від 22.02.2016 № 157 «Про затвердження інструкції про порядок складання звіту 1-ЄО».
45	Масові заходи	Облік масових заходів.	Наказ НПУ від 17.02.2017 № 131 «Про організацію моніторингу оперативної обстановки в державі стосовно забезпечення публічної

			(громадської) безпеки та порядку в публічних (громадських) місцях у зв'язку з проведенням масових заходів».
46	Органи	Інструмент формування відомостей про назву органа та керівника у електронного рапорту при спрощеному порядку розгляду заяв і повідомлень без ознак кримінальних правопорушень.	Наказ НПУ від 03.04.2017 № 311 «Про запровадження експерименту зі спрощеного порядку розгляду заяв і повідомлень без ознак кримінальних правопорушень». Доручення НПУ від 04.05.2017 № 4592/01/26-2017 «Про актуалізацію автоматизованого обліку «Орган».
47	Облік відеокамер	Облік встановлених відеокамер.	Наказ НПУ від 08.06.2021 № 487 «Про введення у тестову експлуатацію ІП «Облік відеокамер» системи ІПНП» Алгоритм дій працівників поліції під час збору та внесення даних до інформаційної підсистеми «Облік відеокамер».
48	Облік порушень ІОС	Облік надзвичайних подій серед особового складу.	Відповідальний підрозділ ДКЗ.
49	Особові справи звільнених	Облік особових справ звільнених поліцейських.	Відповідальний підрозділ ДКЗ.
50	Облік дисциплінарних стягнень	Облік дисциплінарних стягнень.	Відповідальний підрозділ ДКЗ; Методичні рекомендації щодо порядку формування ІП «Облік дисциплінарних стягнень».
51	Облік тимчасово відсутніх працівників	Облік тимчасово відсутніх працівників.	Відповідальний підрозділ ДКЗ.

52	Відряджен-ня	Облік відряджень поліцейських.	Наказ МВС України від 02.08.2017 № 672 «Про затвердження Інструкції про службові відрядження у межах України», зареєстрованого в Мін'юсті 22.08.2017 за № 1042/30910; Наказ МВС України від 08.08.2018 № 755 «Про впровадження автоматизованої інформаційної системи обліку службових відряджень поліцейських».
53	Поліцейські операції	Автоматизований облік початку, закінчення та результатів проведення поліцейських операцій.	Наказ НПУ від 09.10.2018 № 841 ДСК «Про затвердження інструкції про організацію та порядок проведення поліцейських операцій по розшуку і затриманню озброєних та інших осіб, які вчинили суспільно небезпечні діяння».
54	Слід	Облік слідової інформації та інших об'єктів що були вилучені під час проведення слідчих (розшукових) дій відповідальними особами органів досудового розслідування поліції, підрозділу криміналістичного забезпечення органу досудового розслідування поліції для зберігання, знищення, пересилання, схоронності тимчасово	Наказ МВС України № 257 від 16.03.2020 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «СЛІД» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», зареєстрований в Мінюсті за № 319/34602 від 31.03.2020. Доручення №1885/05/24-2021 від 17.02.2021 «Про впровадження в тестову експлуатацію інформаційної підсистеми «Слід» ІТС ІПНП».

		вилученого майна під час кримінального провадження.	
55	Точки POI	Облік інформації на мапі щодо розміщення об’єктів інтересів НПУ	Наказ НПУ від 08.06.2021 № 486 «Про введення у тестову експлуатацію ІП «Точки інтересів» системи ІПНП». Алгоритм дій працівників поліції під час збору та внесення даних до інформаційної підсистеми «Точки інтересів».
56	Облік кривдників	Узагальнення відомостей про взяття на проф. облік, проведення профілактичної роботи та зняття з обліку кривдника працівниками уповноважених підрозділів органів Національної поліції України.	Наказ Національної поліції України від 28.12.2021 № 1081 «Про організацію впровадження пілотного проекту функціонування інформаційної підсистеми «Облік кривдників».
57	РЕЗ та ВП	Внесення інформації про радіочастотний діапазон радіозв’язку в Національній поліції України.	Службовий лист НПУ від 19.11.2020 № 7905/27/01/4-2020 «Про розробку підсистем в ІТС ІПНП».
58	ЕЗК	Внесення інформації про електронні засоби контролю та облік засобів зв'язку в Національній поліції України.	Службовий лист НПУ від 19.11.2020 № 7905/27/01/4-2020 «Про розробку підсистем в ІТС ІПНП».
59	Облік відео пристроїв НПУ	Облік відеопристроїв (відеокамер та відеореєстраторів), які використовуються Національною поліцією України.	Службовий лист НПУ від 19.11.2020 № 7905/27/01/4-2020 «Про розробку підсистем в ІТС ІПНП».

60	Облік ППОК	Відомості щодо обліку поліцейських, державних службовців та інших працівників НПУ, які загинули, отримали тілесні ушкодження (травми, контузії тощо) та (або) інвалідність внаслідок поранення.	
61	Патруль	Відомості про облік інформації про розстановку сил і засобів Національної поліції України.	
62	Погодження руху ТЗ	Відомості про погодження руху транспортних засобів.	Доручення Національної поліції України від 28.12.2016 № 14342/02/20-2016 «Про організацію роботи щодо використання інформаційної системи «Дозвіл БДР»».
63	Гарпун-трафік	Відомості про моніторинг транспортних засобів за державними номерними знаками, пошук адрес.	Доручення НПУ від 25.03.2019 № 3465/01/27-2019 «Про використання інформаційних ресурсів інформаційної підсистеми «Гарпун» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»».
64	Поліцейське піклування	Відомості про облік відомості про осіб, щодо яких застосовано поліцейське піклування.	Наказ МВС України від 12.10.2020 № 724 «Про затвердження Інструкції з оформлення матеріалів про застосування поліцейського піклування».
65	Інтерпол-викрадені ТЗ	Банк даних викрадених транспортних засобів Генерального секретаріату Інтерполу.	Доручення Національної поліції України від 06 жовтня 2017 року № 10807/03/27-2017

			«Про організацію доступу до баз даних Інтерполу».
66	Інтерпол-викрадені документи	Банк даних викрадених, втрачених та загублених проїзних документів Генерального секретаріату Інтерполу.	Наказ Національної поліції України від 17.08.2018 № 786 «Про організацію впровадження інформаційної підсистеми доступу до банку даних Інтерполу «Викрадені/втрачені/загублені проїзні документи».
67	Пошук НАІС (ТЗ посвід-чення)		Доручення Національної поліції України від 23.11.2018 № 14242/01/27-2018 «Про впровадження в органах (підрозділах) поліції в дослідну експлуатацію інформаційної підсистеми «Гарпун»».
68	Зареєстрована зброя-Арсенал	Відомості про зброю та боєприпаси до неї, що видано працівникам органів (підрозділів) поліції та цивільним особам, які беруть участь у відсічі та стримуванні збройної агресії росії.	Доручення Національної поліції України від 18.04.2022 № 2519/01/27-2022 «Про тимчасовий облік вогнепальної зброї та боєприпасів до неї в системі ІПНП».
69	Блокпост	Відомості про підозрілих осіб, причетних до діяльності диверсійно-розвідувальних груп противника на території України.	Доручення Національної поліції України від 13.05.2022 № 3141/01/27-2022 «Про введення в тестову експлуатацію інформаційної підсистеми «Блокпост» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»».
70	ТЗ - військовий стан	Відомості про транспортні засоби, які надійшли на територію України в якості гуманітарної допомоги, вилучені або відчужені	Доручення НПУ № 3/39/01/37-2022 від 13.05.2022 «Про введення в тестову експлуатацію інформаційної підсистеми «ТЗ – військовий стан» інформаційно-комунікаційної системи

		на потреби Збройних сил України, територіальної оборони, правоохоронних органів, волонтерів	«Інформаційний портал Національної поліції України»».
71	Внутрішньо переміщені особи	Відомості щодо внутрішньо переміщених осіб, які залишили своє місце проживання в результаті збройної агресії росії проти України.	Доручення Національної поліції України від 23.06.2022 № 4294/01/25-2022 «Про введення в тестову експлуатацію інформаційної підсистеми «ВПО» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»».
72	Добровольчі формування територіальних громад	Відомості щодо добровольчих формувань територіальних громад та їх членів.	Доручення Національної поліції України від 19.08.2022 № 5779/01/27-2022 «Про введення в тестову експлуатацію інформаційної підсистеми «Добровольчі формування територіальних громад» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»».
73	Воєнний злочинець	Облік осіб, які причетні до військової агресії (військовослужбовці збройних сил російської федерації, члени незаконних збройних формувань, приватних військових компаній, колаборантів тощо).	Доручення Національної поліції України від 26.07.2022 № 5153/01/24-2022 «Про введення в тестову експлуатацію ІП «Воєнний стан» системи ІПНП».

Додаток В

ВИТЯГ

з нормативного документу «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у комунікаційних мережах загального користування України», затвердженого наказом Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України 04.09.2018 № 1519/533

……

Розроблення загальних технічних вимог обумовлена розвитком системи електронних комунікацій, які використовують нові сучасні комунікаційні технології.

……

1. Сфера застосування

……

Загальні технічні вимоги можуть використовуватись:

- операторами, провайдерами електронних комунікацій;
- проектувальниками та виробниками технічних засобів;
- проектувальниками електронних комунікаційних мереж та виробниками обладнання комунікацій;
- органами, уповноваженими на здійснення оперативно-розшукових заходів та негласних слідчих (розшукових) дій;
- органами з оцінки відповідності, випробувальними центрами (лабораторіями), що здійснюють діяльність з підтвердження відповідності технічних засобів;
- адміністратором Автоматизованої інформаційної системи «Централізована база даних перенесених номерів».

……

3. Терміни, визначення понять та скорочення

……

3.2. Скорочення

ЗІП	-	Запасні частини, інструмент та приладдя
ЗЗТМ	-	Засоби захищеної транспортної мережі
ЗУСП	-	Засоби управління системою перехоплення
МК	-	Мережний комплект для здійснення перехоплення комунікацій
ОВОП	-	Обладнання відбору об'єкта перехоплення
ПЗ	-	Програмне забезпечення
СПТ	-	Система законного перехоплення комунікацій
HLR	-	Home location register (опорний регістр місцезнаходження)
HSS	-	Home Subscriber Server (сервер власних абонентів)
IMS-CSCF	-	Internet Protocol Multimedia Core Network Subsystem - Call Session Control Function (мультимедійна підсистема базової мережі на основі Інтернет-протоколу з функцією управління сеансами зв'язку)

……

4. Загальні вимоги

4.1. Склад технічних засобів

4.1.1. До складу технічних засобів для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у комунікаційних мережах загального користування України відносяться (див. рисунки 1.1 та 1.2):

- мережний комплект (МК) для здійснення перехоплення комунікацій;
- засоби управління системою перехоплення комунікацій (сервери, станції, термінали та інші - ЗУСП);
- засоби захищеної транспортної мережі (ЗЗТМ);

- програмне забезпечення (ПЗ) технічних засобів;
- експлуатаційна та програмна документація технічних засобів;
- комплект запасних частин, інструменту та приладдя (ЗІП).

4.1.2. Функціональне поєднання цих засобів утворює систему перехоплення комунікацій (СПТ).

5. Вимоги за призначенням

5.1. Призначення системи перехоплення комунікацій

СПТ призначена для оперативного отримання інформації стосовно об'єкта перехоплення та має забезпечувати:

а) можливість доступу до будь-якого об'єкту перехоплення без зниження якості комунікаційних послуг, що надаються абонентам спостереження, та/або без внесення змін і завад до роботи комунікаційної мережі;

б) відповідність функціональних можливостей СПТ рівню розвитку комунікаційних технологій, які використовуються у комунікаційних мережах;

в) можливість здійснення модернізації СПТ відповідно до розвитку комунікаційної мережі, яка зумовлена впровадженням нових комунікаційних технологій і послуг;

г) можливість ініціювання перехоплення комунікацій і незалежного використання отриманої інформації кожним з суб'єктів перехоплення;

д) технічні можливості контролю використання СПТ за призначенням згідно із законодавством України.

5.2. Призначення МК та їх склад

5.2.1. МК для здійснення перехоплення комунікацій призначені для розпізнавання і відгалуження об'єктів перехоплення, відбору та передачі даних до ЗУСП (див. рисунки 1.1 та 1.2).

5.2.2. До складу МК має входити обладнання відбору об'єкта перехоплення (ОВОП) та шлюз, які встановлюються на сегменті комунікаційної мережі загального користування України.

5.2.3. Організація взаємодії ОВОП та шлюзу здійснюється по інтерфейсу перехоплення.

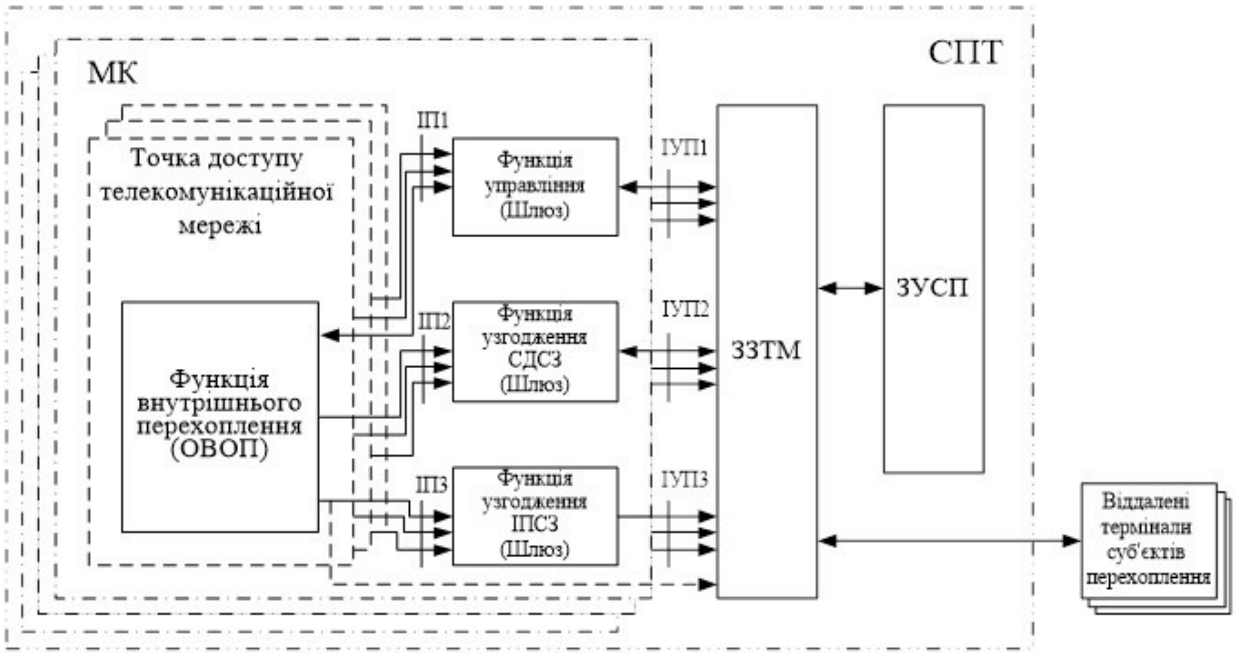

Рисунок 1.1. Схема функціонування інтерфейсів (у загальному випадку)

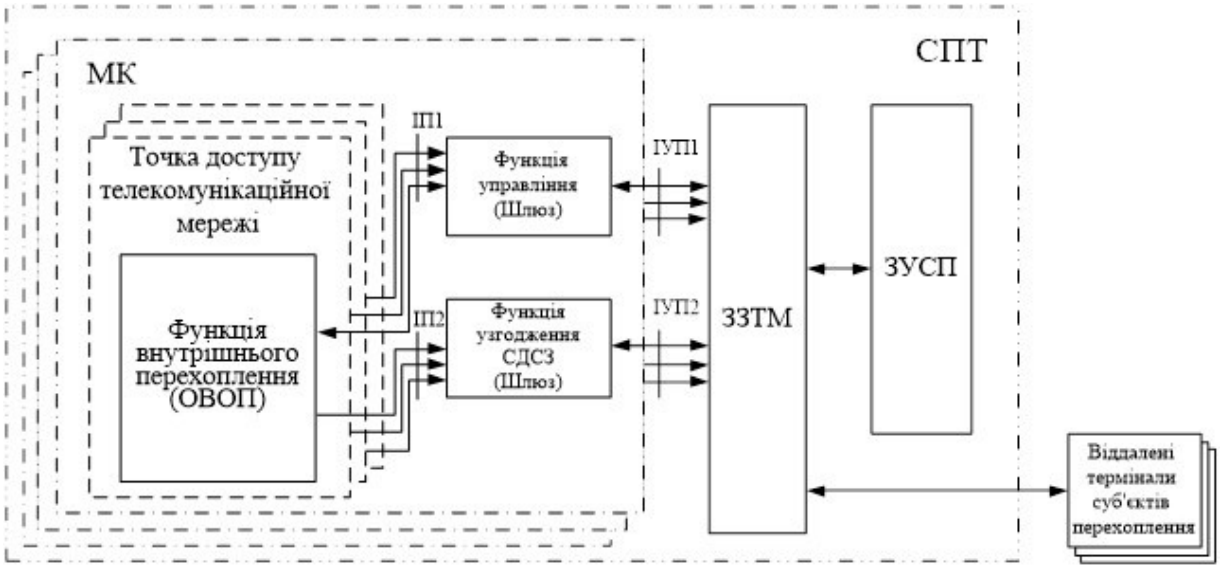

Рисунок 1.2. Схема функціонування інтерфейсів при перехопленні комунікацій з опорного регістру місцезнаходження (HLR), серверу власних абонентів (HSS) або з мультимедійної підсистеми базової мережі на основі Інтернет-протоколу з функцією управління сеансами зв'язку (IMS-CSCF)

5.2.4. Шлюз має здійснювати взаємодію із ЗУСП по інтерфейсу управління та передачі.

5.2.5. Для організації доступу до будь-яких об'єктів перехоплення з урахуванням технічних характеристик та особливостей побудови комунікаційної мережі можуть використовуватися технологічні можливості мережі при відгалуженні об'єктів перехоплення.

5.2.6. МК при здійсненні перехоплення комунікацій не повинні погіршувати якість послуг, що надаються абонентам комунікаційної мережі.

5.2.7. Відповідність МК у складі комунікаційного обладнання стандартам та цим ЗТВ має бути підтверджена у встановленому законодавством порядку.

5.3. Призначення ЗУСП

ЗУСП повинні здійснювати управління МК з метою забезпечення гарантованого перехоплення об'єктів перехоплення, прийому даних від МК та їх обробки, підготовки копій об'єктів перехоплення, а також для організації незалежного використання отриманої інформації кожним з суб'єктів перехоплення.

5.4. Призначення ЗЗТМ

ЗЗТМ повинні забезпечувати взаємодію технічних засобів СПТ між собою, а також між ЗУСП та віддаленими терміналами суб'єктів перехоплення по захищених каналах електрозв'язку.

5.5. Призначення ПЗ СПТ

ПЗ повинне забезпечувати функціонування технічних засобів СПТ відповідно до цих ЗТВ.

5.6. Призначення ЗІП

ЗІП повинні забезпечувати підтримання та відновлення працездатності, справності складових частин СПТ при технічному обслуговуванні.

……

7. Вимоги до документації СПТ

7.1. Вимоги до експлуатаційної документації СПТ

Комплект експлуатаційної документації, призначений для вивчення конструкції технічних засобів і правил їх експлуатування, має містити:

а) паспорти або формуляри на технічні засоби СПТ;

б) настанову щодо експлуатування технічних засобів СПТ;

в) відомості ЗІП для технічних засобів СПТ;

г) настанову операторів робочих місць технічних засобів СПТ.

7.2. Вимоги до програмної документації СПТ

До складу програмної документації обов'язково має входити сукупність програмних документів, що містять дані, необхідні для експлуатування та супроводження ПЗ. До складу програмної документації обладнання вітчизняного виробництва додатково мають входити документи з даними для створення ПЗ та з описом програм.

……

11. Вимоги до захищених каналів електрозв'язку СПТ

11.1. Захищені канали електрозв'язку повинні:

а) забезпечувати гарантовану передачу об'єктів перехоплення з визначеними показниками надійності, необхідної пропускної спроможності та рівнем якості;

б) відповідати вимогам нормативних документів сфери комунікацій;

в) використовувати стандартні протоколи зв'язку та методи кодування інформації.

11.2. Надійність захищених каналів ЗЗТМ має досягатися резервуванням, побудовою кільцевих і багатозв'язаних з'єднань.

……

ВИТЯГ

з Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису, затвердженої наказом Міністерства внутрішніх справ України 18.12.2018 № 1026

І. Загальні положення

……

2. Застосування працівниками поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, здійснюється з метою:

1) попередження, виявлення або фіксування правопорушення;

2) охорони громадської безпеки та власності;

3) забезпечення безпеки осіб;

4) забезпечення публічної безпеки і порядку.

……

ІІІ. Порядок застосування відеореєстраторів, встановлених на службових транспортних засобах

1. Відеореєстратор може бути встановлений усередині салону службового транспортного засобу та/або зовні для максимальної фіксації навколишньої обстановки та/або внутрішньої частини салону в спосіб, що не заважає огляду водія.

2. Включення відеореєстратора здійснюється з моменту початку виконання службових обов’язків або спеціальної поліцейської операції, а відеозапис ведеться безперервно до її завершення, при цьому в процесі включення відеореєстратора поліцейський переконується в точності встановлених на пристрої дати та часу. Залежно від наявних режимів відеореєстратора та освітлення відеозапис здійснюється у відповідному режимі денної або нічної зйомки.

IV. Порядок застосування автомобільних систем

1. Автомобільні системи встановлюються на службових транспортних засобах ситуаційних центрів, командно-штабних автомобілях, спеціальному автотранспорті для перевезення затриманих та взятих під варту осіб.

2. У спеціальному автотранспорті, призначеному для перевезення затриманих та взятих під варту осіб, кількість відеокамер автомобільної системи визначається відповідно до технічних завдань та норм належності, затверджених у встановленому порядку.

3. Автомобільні системи спеціального автотранспорту включаються під час здійснення конвоювання з моменту поміщення затриманих та взятих під варту осіб до його камер.

V. Порядок застосування стаціонарних систем

1. Стаціонарні системи органів, підрозділів поліції працюють у цілодобовому режимі.

2. Наказом керівника органу, підрозділу поліції призначається відповідальна особа, на яку покладаються:

контроль за функціонуванням стаціонарної системи органу, підрозділу поліції;

перегляд відеозаписів;

копіювання та видача відеозаписів.

3. Копіювання та видача інформації із стаціонарної системи проводяться відповідальною особою на підставі письмового доручення керівника органу, підрозділу поліції або особи, яка виконує його обов’язки, про що робиться відмітка в Журналі обліку копіювання та видачі відеозаписів зі стаціонарної системи технічних приладів і технічних засобів фото- і кінозйомки, відеозапису.

4. У разі виявлення непрацездатності елементів стаціонарної системи користувач або черговий повідомляє відповідальну особу.

5. Під час ведення відеоспостереження з використанням стаціонарних систем у громадських місцях, окремих службових приміщеннях органів і

підрозділів поліції, у тому числі спеціальних приміщеннях, призначених для утримання затриманих та взятих під варту осіб, на видному місці встановлюється попереджувальний знак про проведення відеоспостереження.

VI. Порядок застосування засобів фото- та відеозапису на БпЛА

1. Польоти БпЛА здійснюються відповідно до законодавства у галузі державної авіації України.

2. БпЛА можуть бути обладнані системами (однією або декількома) фото- і відеозапису залежно від технічних характеристик повітряного судна.

3. Кількість відеокамер та порядок їх використання на БпЛА (умови польотів, погодні умови, час доби тощо) визначаються згідно з керівництвом з льотної експлуатації БпЛА та/або згідно з інструкцією виробника.

4. Підготовка та розробка польотного завдання, у якому визначається початок та кінець роботи систем фото- і відеозапису, розміщених на БпЛА, здійснюються у порядку, визначеному законодавством, із дотриманням відповідних вимог, польотне завдання затверджує керівник органу підрозділу поліції.

5. Після виконання польотного завдання інформація з карти пам’яті або флеш-карти БпЛА експортується (переноситься) на носій інформації (карту пам’яті або флеш-карту) працівника поліції, який ставив завдання, про що робиться відмітка в польотному завданні.

……

VIII. Загальний порядок зберігання та видачі відеозаписів

1. Вивантаження відеозаписів з карт пам’яті портативних відеореєстраторів та відеореєстраторів, установлених на службових транспортних засобах, БпЛА, на сервер зберігання відеозаписів здійснюється шляхом приєднання карти пам’яті до спеціального обладнання в автоматичному режимі за допомогою спеціального програмного забезпечення або в інший спосіб, визначений виробником до такого сервера.

2. Відеозаписи автомобільних та стаціонарних систем зберігаються на сервері у визначений виробником спосіб.

3. Строк зберігання відеозаписів становить:

1) з портативних та відеореєстраторів, установлених у службових транспортних засобах, БпЛА,- 30 діб;

2) з автомобільної або стаціонарної системи залежно від технічних характеристик - не менше 30 діб;

3) у стаціонарних системах, які використовуються під час відбору кандидатів на службу до поліції,- 60 діб;

4) під час проведення поліцейськими навчальних занять та навчальних зборів зі службової підготовки - встановлюється керівником навчань.

4. Строк зберігання відеозаписів за рішенням керівника органу, підрозділу поліції може бути збільшено у разі використання їх у процесі здійснення оперативно-розшукової діяльності, у рамках розслідування кримінального провадження та/або в провадженнях у справах про адміністративні правопорушення, у разі фіксації надзвичайних подій за участю особового складу поліції, інших подій, якщо вони можуть бути використані в процесі службової діяльності органів, підрозділів поліції, під час проведення службових розслідувань.

5. Контроль за використанням технічних приладів і технічних засобів, що мають функцію фото- і кінозйомки, відеозапису, здійснює відповідальна особа, за інформацією, отриманою з їх допомогою,- безпосередньо керівник органу, підрозділу поліції.

6. Дозвіл на копіювання та видачу відеозаписів надається відповідальній особі виключно за рішенням керівника цього органу, підрозділу поліції.

Копіювання та видача відеозапису проводяться відповідальною особою на підставі відповідного письмового доручення керівника органу, підрозділу поліції або особи, яка виконує його обов’язки.

У разі копіювання та видачі відеозапису робиться відмітка в Журналі обліку копіювання та видачі відеозаписів зі стаціонарної системи або в Журналі обліку.

7. Відеозаписи або копії з них можуть бути надані за вмотивованими запитами органів державної влади, органів досудового розслідування, прокуратури, слідчого судді та суду, поліцейського та інших осіб у порядку, передбаченому законодавством України.

8. Передавання відеозаписів, отриманих з портативних та відеореєстраторів, установлених на службових транспортних засобах, БпЛА, автомобільних та стаціонарних систем для використання засобами масової інформації, а також поширення в мережі Інтернет, здійснюється з дозволу керівника органу, підрозділу поліції з дотриманням Закону України «Про захист персональних даних». Таке передавання здійснюється виключно з метою забезпечення безпеки та захисту інтересів громадян, суспільства і держави, а також з метою захисту гідності та честі працівника поліції.

9. Відеозаписи працівникам органу, підрозділу поліції видаються в тому вигляді, в якому вони були збережені на док-станції,- без коригування. Перегляд, аналіз відеозапису здійснюються працівником поліції, якому він виданий у встановленому цією Інструкцією порядку для виконання покладених на нього завдань в межах його повноважень.

СПИСОК ВИКОРИСТАНИХ ТА РЕКОМЕНДОВАНИХ ДЖЕРЕЛ:

1. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: Львівський державний університет внутрішніх справ, 2020. 256 с.

2. Вишня В. Б., Мирошниченко В. О., Комісаров О. Г., Прокопов С. О. «Інформаційне забезпечення діяльності Національної поліції України». Збірник законодавчих та нормативних документів. Дніпро: Дніпровський державний університет внутрішніх справ, 2016. 476 с.

3. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов. Київ, 2017. 148 с.

4. Волобоєв А. О., Лунгол О. М., Габорець О. А. Розвиток цифрової компетентності майбутніх фахівців юридичного спрямування: практичні аспекти. *Вісник науки та освіти: журнал.* 2022. С. 193–204. DOI: https://doi.org/10.52058/2786-6165-2022-5(5)

5. Волобоєв А. О., Пекарський С. П. Концепція діяльності підрозділів кримінальної поліції в період збройної агресії. *Електронний журнал «Успіхи і досягнення у науці». Серія «Право».* Вип. № 3 (3), Том 2. Київ: Наукові перспективи, 2024. С. 58–69 DOI: https://doi.org/10.52058/3041-1254-2024-3(3)-58-69.

6. Габорець О. А., Лунгол О. М. Основи кібербезпеки: методичні рекомендації до практичних занять. Кропивницький: Book Creator, 2023. 76 с. URL: https://read.bookcreator.com/fQ6a2RCUdGO8pRylJCh2iAlj1bt2/v0qCTrYoRnGfe3g3qIgfHQ/axo1DK1pTdutlxaUM4L81Q

7. Інструкція з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України»: затв. наказом МВС України від 13.06.2018

№ 497. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0787-18#Text.

8. Інструкція про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол: затв. наказом МВС, ОГП, НАБУ, СБУ, ДБР, МФУ, МФУ від 17.08.2020 № 613/380/93/228/414/510/2801/5. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0849-20#Text.

9. Інформаційне забезпечення професійної діяльності: навчальний посібник / І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро: Дніпровський державний університет внутрішніх справ, 2018. 220 с.

10. Конституція України від 28 червня 1996 року. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/254 k/96-вр #Text.

11. Користін О. Є., Тімошин А. С. Інформаційні технології в кримінальному аналізі (практична частина) : навчальний посібник. 2023, 112 с.

12. Кримінальний процесуальний кодекс України від 13 квітня 2012 року № 4651-VI. *Відомості Верховної ради України.* URL: https://zakon.rada.gov.ua/laws/show/4651-17/conv#n2409.

13. Кулешник Я. Ф., Сеник В. В., Сорокач О. В. Застосування інформаційних технологій для автоматизованої ідентифікації осіб : навчально-методичний посібник. Львів: Львівський державний університет внутрішніх справ, 2019. 122 с.

14. Лунгол О. М., Габорець О. А. OSINT-технології в правоохоронній діяльності: навчальний посібник. Мультимедійне видання. Кропивницький: Book Creator, 2023. 107 с. URL: https://read.bookcreator.com/fQ6a2RCUdGO8pRylJCh2iAlj1bt2/sWY11xVJRKymMSKpkHe4TQ/izsvJPMuS4uLPTsQxI8LvQ

15. Методичні рекомендації по захисту інформації у мережі Інтернет / О. С. Гавриш, Е. В. Рижков. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2017. 17 с.

16. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник. Львів: Львівський державний університет внутрішніх справ, 2017. 244 с.

17. Никифорчук Д. Й., Греченко С. Ю. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності. *Оперативно-розшукова діяльність органів внутрішніх справ: проблеми теорії та практики: матеріали Всеукраїнської науково-практичної конференції* (15-16 жовтня 2015 р., м. Дніпропетровськ). Дніпропетровськ: ДДУВС, 2015. С. 23-26.

18. Оперативно-розшукова діяльність у виявленні та розслідуванні злочинів: теорія, історія і сучасна практика : навч.-метод. посібник / О. О. Подобний. Одеса : Видавничий дім «Гельветика», 2021. 258 с.

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

20. Особливості виявлення фактів, пов’язаних із незаконним розповсюдженням медійного контенту в мережах провайдерів програмної послуги та Інтернет провайдерів, мережі Інтернет: методичні рекомендації / [Гавриш О. С., Краснобрижий І. В., Мирошниченко В. О., Прокопов С. О., Рижков Е. В.]. Дніпро: Дніпроп. держ. ун-т. внутр. справ, 2017. 49 с.

21. Подобний О. О. Оперативно-розшукова діяльність у виявленні та розслідуванні злочинів: теорія, історія і сучасна практика: навч.-метод. посібник. Одеса: Видавничий дім «Гельветика», 2021. 200 с.

22. Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС: затв. наказом МВС України від 20.10.2017 № 870. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z1433-17#n13.

23. Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів: затв. Постановою Кабінету Міністрів України від 14 листопада 2018 р. № 1024. *Відомості*

Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF#Text.

24. Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України»: затв. наказом МВС України від 03.08.2017 № 676. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

25. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2939-17#n57.

26. Про електронні комунікації. Закон України від 16.12.2020 № 1089-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

27. Про електронну ідентифікацію та електронні довірчі послуги. Закон України від 05.10.2017 № 2155-VIII. *Відомості Верховної ради України.* URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

28. Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису. Наказ Міністерства внутрішніх справ від 18.12.2018 № 1026. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0028-19#Text.

29. Про затвердження нормативного документа «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у комунікаційних мережах загального користування України. Загальні технічні вимоги. Наказ Служби безпеки України, Адміністрації державної служби спеціального зв'язку та захисту інформації України від 04.09.2018 № 1519/533. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/rada/show/v1519950-18#Text.

30. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

31. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

32. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-XII. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2657-12# Text.

33. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

34. Про Національну поліцію: Закон України від 2 липня 2015 року № 580-VIII. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

35. Про Національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/74/98-вр#Text.

36. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2135-12/conv#n49.

37. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30 червня 1993 року № 3341-XII. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/3341-12#Text.

38. Про розвідку: Закон України від 17 вересня 2020 року № 912-IX. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/912-20#Text.

39. Розвідка з відкритих джерел (OSINT) / Науково-методичні рекомендації. Розробники Манжай О. В., Потильчак А. О. / ХНУВС. Харків, 2021. 30 с.

40. Цивільний процесуальний кодекс України від 18 березня 2004 року № 1618-IV. *Відомості Верховної ради України.* URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text.

Information about the authors

Artur Olehovych Voloboiev – Head of the Department of Operational Investigation and Information Security of the Faculty of Specialist Training for Criminal Police Units of the Donetsk State University of Internal Affairs, PhD in Law.

Olha Andriivna Haborets – Associate Professor of the Department of Operative and Investigative Activities and Information Security of the Faculty of Specialist Training for Criminal Police Units of the Donetsk State University of Internal Affairs, PhD in Pedagogy.

Anatoliy Serhiyovych Timoshin – Associate Professor of the Department of Cybercrime Counteraction at the Faculty of Training Specialists for Cyberpolice Units of Kharkiv National University of Internal Affairs, Candidate of Physical and Mathematical Sciences, Associate Professor.

Demid Anatoliyovych Morozov – Associate Professor of the Department of Justice at the Faculty of Training Specialists for Police Units of the E. O. Didorenko Luhansk Educational and Scientific Institute of Donetsk State University of Internal Affairs, Candidate of Legal Sciences, Associate Professor.

Oleksandr Mykolayovych Pupinin – Postgraduate Student at Donetsk State University of Internal Affairs.

Для нотаток

Для нотаток

Для нотаток

Для нотаток

Навчальне видання

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ ТА ДОСУДОВОМУ РОЗСЛІДУВАННІ

НАВЧАЛЬНИЙ ПОСІБНИК

за загальною редакцією
доктора філософії в галузі права
А. О. Волобоєва