УДК 343.9:004.6 DOI: 10.37025/1992-4437/2026-45-1-92

О. В. Пірог*,
кандидат технічних наук,
головний судовий експерт експертного сектору
(з дислокацією в м. Житомир),
Український науково-дослідний інститут
спеціальної техніки та судових експертиз
Служби безпеки України
вул. Миколи Василенка, 3, м. Київ, 03113, Україна
ORCID: https://orcid.org/0009-0001-6111-9676
email: pirogov@ztu.edu.ua
Т. М. Івасишин,
кандидат біологічних наук,
доцент кафедри кримінального процесу та криміналістики
навчально-наукового гуманітарного інституту,
Національна академія Служби безпеки України
вул. Михайла Максимовича, 22, м. Київ, 03066, Україна
ORCID: https://orcid.org/0009-0007-6604-0362

Історія статті
Отримано: 15.10.2025
Прийнято: 20.03.2026
Опубліковано: 28.05.2026

ВИЛУЧЕННЯ IP-КАМЕР: КРИМІНАЛІСТИЧНІ АСПЕКТИ

Анотація. У науковій статті, мету якої становить висвітлення підходів до розроблення та систематизації способів вилучення IP-камер під час проведення процесуальних дій як складника фіксування та збереження цифрових доказів, розглянуто криміналістичні аспекти вилучення IP-камер із особливою увагою до процедур відключення цих пристроїв від мережі, що унеможливлює втрату цінної інформації. У дослідженні застосовано спрямовані на теоретичне обґрунтування процесу вилучення IP-камер під час проведення процесуальних дій загальнонаукові методи наукового пізнання (формально-логічні методи – аналіз, синтез, індукція, дедукція, абстрагування, методи порівняння, моделювання, узагальнення) та спеціальні методи (криміналістичний, системно-структурний, техніко-правовий аналіз), послуговувалися типовими апаратними засобами цифрової криміналістики, зовнішніми накопичувачами, а також програмними інструментами Nmap, Wireshark, FTK Imager, ONVIF Device Manager. Наукова новизна дослідження полягає у формуванні системного бачення процесу вилучення IP-камер у криміналістичній практиці. До того ж висвітлено актуальність теми в умовах цифровізації, коли IP-камери є джерелом ключових цифрових доказів – відеозаписів, метаданих, журналів доступу та конфігураційних параметрів. Проаналізовано основні типи IP-камер: автономні, підключені до мережевих або цифрових відеореєстраторів (NVR/DVR), а також хмарні рішення з акцентом на особливості зберігання даних, рівень безпеки та вразливості. Детально розглянуто функціонування критичних мережевих протоколів (RTSP, HTTP, ONVIF, MQTT), використовуваних для передавання відео та команд, які можуть бути джерелом цифрових доказів. Особливу увагу приділено методам аналізу мережевого трафіку за допомогою Wireshark, що дає змогу встановити взаємодію камери з іншими пристроями в мережі, виявити потоки відео та визначити напрямок передавання даних, зокрема й хмарні сервіси. Розглянуто роль інструментів Nmap для пошуку активних камер і відеореєстраторів, аналізування відкритих портів і служб, що працюють на них. Описано труднощі, пов'язані з виявленням централізованих або хмарних сховищ відео: використання шифрування, нестандартних портів, самознищення даних або блокування доступу. Наведено практичні рекомендації щодо програмної (через фаєрволи, маршрутизатори) і фізичної (відключення мережі, екранування сигналів Faraday bag) ізоляції камери з одночасним збереженням запису на технічні носії, а також щодо створення резервних копій відео та конфігурацій, вилучення кешованих

*Відповідальний автор

даних, зчитування логів. Наголошено на важливості забезпечення допустимості зібраних матеріалів через використання хеш-функцій і детального документування всіх етапів вилучення та аналізування даних. Зазначено, що впровадження стандартизованих процедур відключення IP-камер і збереження цифрових доказів сприятиме підвищенню ефективності досудового розслідування та допустимості представлених у суді фактичних даних.

Ключові слова: цифрові докази; огляд; вилучення; процесуальні дії; Nmap; Wireshark; системи відеоспостереження.

Вступ

У сучасних умовах цифровізації суспільства (Khaustova, 2022a, 2022b) і широкого використання систем відеоспостереження (Kalbo et al., 2020; Korshenko et al., 2020; Haley, 2025; Holovin et al., 2025) особливої ваги набуває належна організація роботи правоохоронних органів у матеріальному середовищі, де функціонують IP-камери (мережеві відеокамери, що здійснюють цифровий відеозапис і передають дані через IP-мережі). Ці пристрої здатні фіксувати події в реальному часі, зберігати відеозаписи, метадані, мережеві журнали та іншу важливу інформацію, що може слугувати цифровими доказами (Ramadhan et al., 2019; Shevchuk, 2024). А втім, на практиці постають деякі проблеми, пов'язані із забезпеченням збереження таких даних під час вилучення обладнання або тимчасового припинення його роботи, а саме – ризик втрати цифрових слідів через некоректне вимкнення камер або несанкціоноване втручання в систему (Alshenai et al., 2024).

Під час проведення процесуальних дій незрідка постає потреба швидко відключити камери від мережі, щоб запобігти подальшому перезапису або видаленню даних (Horsman, 2021). Водночас це потрібно зробити без втрати інформації про конфігурацію, мережеві з'єднання, налаштування запису та інші цифрові артефакти, важливі для розслідування. Сьогодні в слідчій практиці бракує усталених алгоритмів безпечного вимкнення IP-камер, що створює ризики втрати доказової інформації та ускладнює подальший аналіз зібраних даних (Horsman, 2021; Bilous, & Latysh, 2022; Ivasishyn, & Piroh, 2025). Особливо загрозливою є ситуація, коли правопорушники навмисно знищують або вносять зміни у відеозаписи (Javed et al., 2021; Pogoretskyi, & Lysachenko, 2023; Petryk, 2025).

Через це постає нагальна потреба дослідити такі способи відключення IP-камер від мережі без втрати важливої інформації з огляду на технічні особливості систем спостереження та криміналістичні вимоги щодо забезпечення цілісності, автентичності й відтворюваності цифрових доказів. Упровадження таких процедур сприятиме (Pogoretskyi, & Lysachenko, 2023; Romaniuk, & Fomina, 2024; Petryk, 2025) підвищенню якості досудового розслідування, мінімізуватиме втрату доказів і забезпечуватиме їх допустимість (Hellwig, 2021; Mamatkulova, 2021; Lindeman et al., 2024) у суді.

Вилучення та аналізування IP-камер незрідка супроводжується технічними, правовими й організаційними труднощами (Horsman, 2021; Bratishko, 2023; Gehlot et al., 2022). Серед основних – фізичний доступ до пристроїв, які часто розміщені у важкодоступних місцях: на дахах, стовпах, у приміщеннях з обмеженим доступом. Іноді відеореєстратори зберігають у захищених серверних кімнатах або зачинених шафах, а власники або орендарі можуть відмовляти в доступі до них. Інша проблема – втрата або знищення відеозаписів, спричинені автоматичним перезаписом або навмисними діями правопорушників (Javed et al., 2021; Salem, & Hamarsheh, 2024). Додаткову складність становить захищеність камер від несанкціонованого доступу. Пристрої часто використовують шифрування, приватні мережі, VPN і засоби автентифікації, що ускладнює вилучення інформації без відповідних ключів (Bhardwaj et al., 2023; Stabili et al., 2024). Важливим викликом є різноманітність форматів відеозаписів. Виробники застосовують різні стандарти стиснення, а деякі пропрієтарні формати, що не підтримують загальнодоступні програвачі (Javed et al., 2021; Ruvinska, & Deviatkov, 2021). Не менш важлива проблема точності часових міток. Неправильно налаштований час або несинхронізовані камери ускладнюють встановлення хронології подій, а іноді часові позначки можуть бути навмисно змінені з метою фальсифікації фактичних даних (Van der Velden, 2015; Soni, 2025). Останні складнощі пов'язані з мережею: передача відео на хмарні сервери або злам камери ще до прибуття фахівців може призвести до втрати безпосереднього доступу до файлів (Ramakrishnan, & Haqanee, 2024; Salem, & Hamarsheh, 2024). Відсутність підключення до локальної мережі обмежує можливість отримання доступу до архівів (Gehlot et al., 2022).

Проблематика аналізу мережевого трафіку та криміналістичного дослідження систем відеоспостереження є актуальною в сучасній цифровій безпеці й криміналістиці. Науковці досліджують методи збирання, збереження та аналізування цифрових доказів із використанням сучасних інструментів і технологій (Salih et al., 2023). Вивчаючи питання вилучення даних з IoT-пристроїв, зокрема й із IP-камер (Gehlot et al. (Eds.), 2022), аналізують виклики, пов'язані з особливостями мережевого підключення і збереження цілісності

даних. Розглядають (Oettinger, 2024) мобільну криміналістику як необхідне доповнення під час огляду місця події, де можуть бути різноманітні пристрої. Розробляють практичні рекомендації з розслідування цифрових інцидентів за допомогою потужних інструментів, доступних у Kali Linux, що стосуються безпечного вилучення та аналізу IP-камер (Parasram, 2023). Обговорюючи методологію аналізу безпеки та ідентифікації вразливостей, що можна використовувати віддалено, фахівці (Stabili et al., 2024) пропонують власні підходи до виявлення вразливостей IP-камер, наголошують на необхідності обережного відключення пристроїв і недопущенні пошкоджень цифрових слідів. Ґрунтовно аналізують (Horsman, 2021; Lindeman et al., 2024) критерії допустимості цифрових доказів у контексті огляду місця події. Розглядають методи аналізу мережевого трафіку Wireshark та ідентифікації мережевих пристроїв через Nmap (Ndatinya et al., 2015; Ramakrishnan, & Haqanee, 2024). Висвітлюють нормативно-правові аспекти збирання цифрових доказів, ведення документації та забезпечення їхньої автентичності (Khakhanovskyi, & Hutsaliuk, 2019; Ivasyshyn, & Piroh, 2025; Petryk, 2025).

А втім, на часі оптимізація методів збирання, фіксування та надання цифрових доказів, особливо в умовах щораз більшої складності та масштабності цифрових систем відеоспостереження. Попри наявні напрацювання питання уніфікованих методик вилучення IP-камер під час проведення процесуальних дій недостатньо досліджені. Водночас актуалізується потреба формування алгоритмів роботи з мережевими пристроями відеоспостереження, які зважають на технічні, правові та процесуальні аспекти їх аналізу.

Мета статті полягає у висвітленні підходів до розроблення та систематизації способів вилучення IP-камер під час проведення процесуальних дій як складника фіксування та збереження цифрових доказів. Для досягнення цієї мети необхідно вирішити такі завдання: визначити основні принципи та вимоги до забезпечення цілісності цифрових даних під час роботи з мережевими пристроями; узагальнити наукові підходи до класифікації IP-камер та їх технічних характеристик; окреслити апаратні та програмні засоби, що застосовуються для їх виявлення в мережі, ізолювання та копіювання інформації; сформулювати основи для вдосконалення практики вилучення мережевих відеопристроїв під час проведення процесуальних дій.

Матеріали та методи

Методологічну основу цього дослідження становить система загальнонаукових і спеціальних методів наукового пізнання, спрямованих на теоретичне обґрунтування процесу вилучення IP-камер під час проведення процесуальних дій. Формально-логічні методи (аналіз, синтез, індукція, дедукція, абстрагування) застосовано для послідовного розкриття сутності поняття «вилучення IP-камери» як процесу криміналістичного забезпечення збереження цифрових доказів. За допомогою методу порівняння зіставлено підходи до вилучення IP-камер, описані у вітчизняній і зарубіжній криміналістичній літературі, та визначення спільних рис і відмінностей у процедурах забезпечення цілісності даних. Метод моделювання застосовано для теоретичного відтворення типових ситуацій виявлення та вилучення мережевих пристроїв із метою формування оптимальної послідовності дій працівників правоохоронних органів. Метод узагальнення дав змогу систематизувати наукові підходи до класифікації IP-камер і роботу з ними в процесі фіксування цифрових доказів. Серед спеціальних методів застосовано криміналістичний, системно-структурний і техніко-правовий аналіз, що забезпечив виявлення ключових аспектів доступу до пристроїв і носіїв інформації. Для опису технічного середовища послуговувалися типовими апаратними засобами цифрової криміналістики – портативними комп'ютерами з криміналістичним програмним забезпеченням, write-blocker, зовнішніми накопичувачами, Faraday-чохлами, а також програмними інструментами Nmap, Wireshark, FTK Imager, ONVIF Device Manager. Комплексне використання зазначених методів забезпечило наукову обґрунтованість висновків і сприяло формуванню системного бачення процесу вилучення IP-камер у криміналістичній практиці.

Результати та обговорення

Тип камери великою мірою визначає спосіб зберігання відеозаписів, методи доступу до даних, а також рівень захищеності самої інформації. Загалом можна виокремити три основні підходи до побудови системи спостереження на базі IP-камер: автономні камери, камери, підключені до NVR або DVR, а також хмарні рішення (див. табл. 1).

Отже, автономні IP-камери функціонують незалежно від зовнішніх систем збереження даних. Вони записують відео безпосередньо на вбудовані носії, як-от SD-карти або USB-накопичувачі. У деяких випадках такі камери можуть передавати дані за запитом на віддалений сервер через протоколи FTP, HTTP, RTSP або ONVIF. Завдяки вбудованим модулям штучного інтелекту вони здатні самостійно аналізувати потік, розпізнавати обличчя, фіксувати рух або звук, водночас не потребуючи підключення до зовнішнього відеореєстратора.

Таблиця 1

Порівняння параметрів різних типів IP-камер

Параметри	Автономні IP-камери	IP-камери з NVR/DVR	Хмарні IP-камери
Метод збереження інформації	SD-карта, USB	Жорсткий диск (HDD) у NVR/DVR	Хмарне сховище
Залежність від Інтернету	Немає	Частково	Потрібен
Доступ до записів	Локальний	Локальний + мережевий	Через Інтернет
Ризик порушення цілісності записів	Високий (крадіжка, пошкодження)	Середній (вихід із ладу HDD)	Низький (резервне копіювання)
Захищеність записів	Обмежена	Середня (шифрування, паролі)	Висока (хмарне шифрування)

Іншим типом є IP-камери, які функціонують у складі централізованих систем відеоспостереження, підключаючись до мережевих (NVR) або цифрових (DVR) відеореєстраторів. У цьому разі камери зв'язуються з реєстратором через Ethernet або через бездротове підключення. Уся інформація зберігається на жорстких дисках, підключених до відеореєстратора, що забезпечує більший обсяг пам'яті і триваліший період збереження архівів.

Хмарні IP-камери реалізують принципи сучасної цифрової інфраструктури, де всі відеозаписи передаються безпосередньо до віддалених сховищ, розміщених у хмарних середовищах, як-от Google Cloud, Amazon AWS, Dropbox або інші платформи, зокрема Hikvision Cloud чи Dahua Cloud. Камери підключаються до Інтернету через Wi-Fi або Ethernet, а всі дані автоматично шифруються, що забезпечує високий рівень захисту інформації. Хмарні камери часто забезпечують можливість дистанційного доступу до відеоархівів через мобільні додатки, а також підтримують функції аналітики на основі штучного інтелекту, що дає змогу автоматично виявляти підозрілі дії чи поведінкові аномалії в режимі реального часу.

IP-камери відеоспостереження є мережевими пристроями, які для передавання відео, метаданих і команд управління використовують набір спеціалізованих мережевих протоколів. Розуміння цих протоколів надзвичайно важливе для фахівців із цифрової криміналістики (Javed et al., 2021; Gehlot et al., 2022; Bhardwaj et al., 2023).

Серед ключових протоколів IP-камер – RTSP (Real-Time Streaming Protocol), що, забезпечуючи передавання відеопотоків у реальному часі, дає змогу клієнтам керувати потоковими даними. Самі відео- та аудіофрагменти зазвичай передають через RTP (Real-Time Transport Protocol). У контексті криміналістики це означає можливість аналізування сесій RTSP, перехоплення даних або спроби відновлення фрагментів відеопотоку за наявності записаного трафіку. Стандартним портом для RTSP є 554, хоча деякі камери можуть використовувати альтернативні, зокрема 8554.

Інший широковживаний протокол HTTP IP-камер використовують для організування вебінтерфейсу та передавання статичних зображень або відеопотоків у форматі MJPEG. Користувач через HTTP керує пристроєм, змінює налаштування камери, отримує доступ до знімків, а то й запускає відеозапис. Також через вебзапити може надсилати команди. Доступ до вебінтерфейсу зазвичай через порт 80, а за захищеного з'єднання – через 443 (HTTPS).

Для забезпечення сумісності між камерами різних виробників використовують протокол ONVIF (Open Network Video Interface Forum). Він базується на SOAP (Simple Object Access Protocol) і дає змогу автоматично виявляти камери в локальній мережі. Підтримує передавання метаданих, віддалене налаштування параметрів пристрою та керування поворотними камерами. Завдяки цьому протоколу фахівці можуть отримати доступ до параметрів камери, також і з журналами подій, логами входів і списком активних підключень. Найчастіше працює через порт 8080, хоча можливі й інші – наприклад, 2020 або 8443.

В IP-камери з функціями розумного відеоспостереження дедалі активніше впроваджують протокол MQTT (Message Queuing Telemetry Transport), розроблений для IoT-середовища, що забезпечує швидке та надійне передавання невеликих повідомлень (Kostenko, 2021; Halahan et al., 2025; Yashchuk et al., 2025). Камера автоматично надсилає повідомлення про виявлення руху, зміну конфігурації чи спрацювання тривоги. Такі повідомлення можуть бути важливими в межах цифрової криміналістики (Horsman, 2021; Javed et al., 2021), адже уможливлюють відстеження хронології подій. За замовчуванням, MQTT працює на порту 1883, а захищене з'єднання через TLS (Transport Layer Security) – на порту 8883.

Метадані, що генерують і зберігають IP-камери, надзвичайно важливі в розслідуваннях, оскільки завдяки їм можна не лише підтвердити автентичність відеозаписів, а й установити джерело,

мережеву активність пристрою, його технічні характеристики та послідовність подій. Ці дані суттєво підвищують доказову цінність відео та дають змогу відновити повну картину подій навіть і тоді, коли саме відео було видалене або пошкоджене (Horsman, 2021; Javed et al., 2021).

До ключових категорій метаданих належать ідентифікаційні параметри пристрою, журнали доступу та мережевих підключень, а також часові мітки із супутніми механізмами синхронізації. Зокрема, MAC-адресу, унікальний ідентифікатор мережевого інтерфейсу, прив'язують до конкретного виробника, що й дає нагоду виявити камеру в мережі або простежити її переміщення між сегментами. Водночас завдяки IP-адресі можна встановити фізичне або логічне розміщення пристрою на момент знімання. Ідентифікатори камери, як-от серійний номер, ONVIF ID або UUID, часто використовують в автоматизованих системах управління відеоспостереженням для точного визначення пристрою серед багатьох інших.

Важливою складовою дослідження є аналіз логів доступу, які формуються в більшості сучасних IP-камер. Ці журнали фіксують також і підозрілі дії. Інформація про IP-адресу клієнта, час доступу, тип доступу (локальний чи віддалений), що зберігається, уможливлює виявлення фактів несанкціонованого втручання. Аналогічно журнали підключень дають змогу відстежити, які пристрої здійснювали з'єднання з камерою, які порти використовувалися, які протоколи були активні, що в разі дослідження витоку відео чи хакерської атаки може стати в пригоді. Журнали подій фіксують зміни конфігурації, запуск детектора руху, активацію тривоги або спроби перезаписування даних.

Окремої ваги набувають часові мітки, точність яких критично важлива для встановлення послідовності подій. Якщо камеру не синхронізовано із сервером часу (наприклад через NTP), її вбудований годинник може показувати неправильний час, що спричинить невідповідність між записом і фактичними подіями. Незрідка це використовують правопорушники для створення неправдивого алібі або зміщення хронології. Оскільки адміністратор може вручну змінити дату та час, необхідно звертати увагу на історію змін налаштувань годинника, збережену в логах.

Під час проведення процесуальних дій фахівці мають виявити всі активні камери. Для цього можуть використовуватися методи сканування портів, що дають змогу визначити IP-камери в локальній або глобальній мережі, а отже – виявити відкриті сервіси (RTSP, HTTP, ONVIF, SSH тощо) (див. табл. 2), ідентифікувати виробника пристрою, версію прошивки.

Таблиця 2

Основні порти IP-камер

Порт	Протокол	Використання
80, 8080	HTTP	Вебінтерфейс камери
443	HTTPS	Захищений вебдоступ
554	RTSP	Передавання відеопотоків
8000–9000	Виробники (Hikvision, Dahua)	Адмінпанелі
3702	ONVIF	Автоматичне виявлення камер
22	SSH	Доступ до системи камери
21	FTP	Завантаження відеофайлів

Nmap (Network Mapper) – один із найпотужніших сканерів мереж, що працює через командний рядок (використовують для пошуку пристроїв, виявлення відкритих портів, визначення ОС та сервісів; підтримує глибокий аналіз – версія прошивки, підтримання ONVIF тощо). Наприклад:

```
nmap -p 80,554,8000-9000 --open
-sV 192.168.1.0/24                    (1)
```

-p 80,554,8000-9000 – сканує порти, що часто використовуються камерами (HTTP, RTSP, адмінпанель);

--open – показує лише активні (відкриті) порти;

-sV – визначає версію сервісу, що працює на порту;

192.168.1.0/24 – перевіряє всі пристрої в підмережі.

Так, за допомогою мережевого сканування можна виявити IP-камери, підключені до мережі, та отримати важливу інформацію про доступні сервіси.

Якщо камера відповідає на порт 554 (RTSP) – вона передає відеопотік, навіть якщо вебінтерфейс вимкнено. Коли порт 3702 (ONVIF) відкритий, – можна отримати додаткові метадані про камеру.

Камери можуть бути доступні публічно через Shodan – пошукову систему для пристроїв.

Аналізування мережевого трафіку – надзвичайно важливий інструмент у розслідуванні інцидентів, пов'язаних із системами відеоспостереження. Використовуючи спеціалізоване програмне забезпечення, як-от Wireshark, можна відтворити повну картину взаємодії IP-камер з іншими пристроями в мережі, а отже – встановити, з якими ситемами і за допомогою яких протоколів здійснюється комунікація. Вивчення мережевого трафіку дає змогу з'ясувати, які саме дані передавалися, у який момент часу, куди саме вони спрямовувалися, що дає змогу відновити хронологію подій і знайти відеозаписи, які могли бути втрачені або пошкоджені.

Wireshark – один із найпопулярніших інструментів для глибокого аналізування мережевого трафіку, здатний детально досліджувати пакети, що проходять через мережу.

Для виділення трафіку, який проходить через IP-камери, використовують такі фільтри:

rtsp – фільтрує трафік RTSP-протоколу (передача відео);

http – фільтрує трафік HTTP-протоколу (вебінтерфейс);

ip.addr==192.168.1.10 – фільтрація за IP-адресою камери.

У системах відеоспостереження записи з IP-камер часто зберігаються в централізованих сховищах, як-от NVR (Network Video Recorder) або хмарних сервісах. Це дає можливість організувати зручний доступ до відеофайлів та їх довготривале зберігання. А втім, у контексті криміналістики важливо правильно виявити такі сховища.

NVR-системи зазвичай розміщують усередині корпоративної мережі або локального сервера, де приймають та обробляють відеодані від IP-камер. Натомість хмарні сервіси забезпечують зберігання відеозаписів на віддалених серверах із доступом до них через Інтернет і використанням різних платформ, як-от AWS, Google Cloud або спеціалізовані сервіси виробників камер.

Щоб визначити систему, яка виконує функції NVR, спеціаліст може скористатися кількома методами. Один із них – це сканування мережі та аналізування підключених пристроїв за допомогою інструментів на кшталт Nmap, що дає нагоду виявити активні вузли з характерними портами або службами, притаманними відеореєстраторам. Інший підхід полягає у вивченні мережевого трафіку між камерами та сервером за допомогою Wireshark, щоб виявити передавання потокових даних, зокрема за RTSP- чи ONVIF-протоколами, а також отримати метадані, які свідчать про централізоване зберігання відео. У деяких випадках допомагає аналіз MAC-адрес – унікальних ідентифікаторів пристроїв, за якими можна встановити виробника та модель системи.

Якщо йдеться про хмарні сховища, їх також можна виявити, аналізуючи вихідний мережевий трафік. Адже системи відеоспостереження, які використовують такі сервіси, регулярно передають відеодані до віддалених серверів. Вивчаючи цей трафік, зокрема HTTPS-з'єднання, можна виявити наявність комунікацій із хмарними платформами – наприклад Google Cloud, Azure або Dropbox. Крім того, багато хмарних систем використовують відкриті API для передавання даних. Тому перехоплення та аналізування таких запитів дає змогу підтвердити зв'язок між камерою та віддаленим сервісом. Додатково варто звернути увагу на доменні імена та IP-адреси, які фігурують у трафіку, – зіставляючи їх із відомими хостами хмарних сервісів, можна точно встановити напрямок передавання відео і тип задіяного сховища.

Виявлення централізованих сховищ відеозаписів у системах відеоспостереження супроводжується низкою викликів, які суттєво ускладнюють роботу спеціалістів (Horsman, 2021; Stoykova, 2024). Однією з ключових перешкод є використання шифрування даних. Більшість сучасних хмарних сервісів передають відео за допомогою захищених протоколів, як-от TLS або SSL, що повністю шифрують переданий трафік. У результаті стандартні інструменти моніторингу не можуть безпосередньо прочитати вміст переданої інформації або відстежити, чи є вона відео, що значно ускладнює встановлення цільових потоків та визначення напрямку передавання відеоданих.

Серед проблем можна виокремити і застосування нестандартних портів або протоколів. У сучасних камерах і відеореєстраторах нерідко навмисно переналаштовують значення портів, щоб ускладнити їх виявлення під час звичайного сканування.

Централізовані сховища відео важливі для відновлення записів, якщо їх пошкоджено на самій камері або в разі видалення даних. Перевірян ня центрального сховища дає змогу визначити, чи були втрачені або змінені дані. Коли є підозра в маніпулюванні відеофайлами, вивчаючи централізоване сховище, можна перевірити, чи зберігалися оригінальні файли до того, як вони були змінені або видалені.

У сучасних системах відеоспостереження для зручності та доступу до записів часто використовують технології віддаленого доступу, щоб підключати камери до сторонніх серверів або застосовувати їх через хмарні сервіси. Водночас це створює потенційні вразливості для системи, адже правопорушники можуть отримати доступ

до відеоархівів, маніпулювати даними або здійснювати зловмисне контролювання камер.

Системи відеоспостереження часто взаємодіють із зовнішніми серверами з низкою функціональних цілей, що мають важливе значення як для адміністрування, так і для убезпечення даних. Серед основних напрямів – підтримання постійного моніторингу та контролю: адміністратори отримують змогу в реальному часі підключатися до IP-камер, спостерігати за поточними подіями, а також здійснювати управління конфігурацією пристроїв. Такі можливості реалізуються як через мобільні застосунки, так і через вебінтерфейси.

Крім того, деякі IP-камери підтримують повноцінне віддалене адміністрування. Це робить можливим змінювання налаштувань, оновлення прошивки, керування потоками, а то й перезавантаження пристрою.

Системи виявлення вторгнень (IDS) або системи запобігання вторгненням (IPS), як-от Snort або Suricata, так само становлять ефективні інструменти для виявлення підключень до сторонніх серверів (Halahan et al., 2025), що дає змогу фахівцям встановити факти неавторизованого доступу або вторгнення в систему відеоспостереження, відновити журнали активності та проаналізувати передані дані, а також встановити, коли і в який спосіб відбувалися маніпулювання з відеозаписами чи камерами.

У сучасних системах відеоспостереження можуть бути вбудовані механізми самознищення даних, які слугують засобом захисту конфіденційної інформації. Їх, трапляється, також використовують і правопорушники для приховування слідів (Sokol et al., 2020; Horsman, 2021). Деякі камери та відеореєстратори реагують на втручання в систему або раптове відключення живлення автоматичним видаленням записів. Щоб забезпечити цілісність відеоданих і мінімізувати ризики втрати інформації, важливо ізолювати камери від стороннього втручання без утрати їх функціональності та зберегти архіви.

З-поміж ефективних підходів і програмне ізолювання, яке дає змогу відключити пристрій від Інтернету без припинення подавання живлення. Це досягається зміною в налаштуваннях камери або її мережевого оточення, завдяки чому зберігається запис на локальний носій, а доступ іззовні блокується. Такого ефекту можна досягти і через налаштування фаєрволів, здатних обмежити або повністю заблокувати вхідний і вихідний трафік, не зупиняючи сам процес відеозапису. Ще одним способом є переконфігурація маршрутизатора, коли через встановлення правил для пристрою блокується його вихід в Інтернет, зберігаючи водночас роботу у внутрішній мережі.

Через брак можливості здійснити програмну ізоляцію доцільно фізично відключити мережеве з'єднання, залишивши живлення камери. Якщо ж камера працює через бездротове з'єднання, її можна ізолювати за допомогою спеціального екранувального чохла Faraday bag, який блокує всі радіосигнали. Перед будь-яким відключенням варто створити резервну копію наявних відеозаписів. Це особливо важливо в ситуаціях, де є ризик втрати або знищення даних. Для створення повної копії носія можуть бути використані спеціалізовані інструменти, наприклад dd або FTK Imager.

Набуває ваги й такий захід, як безперервний моніторинг поведінки камери під час її відключення, щоб вчасно виявити можливу активацію функції самознищення або інші підозрілі дії.

Розслідуючи інциденти, пов'язані із системами відеоспостереження, серед ключових завдань – ретельне фіксування всіх цифрових слідів, які залишає камера. Це дає змогу не лише реконструювати хронологію подій, а й виявити можливі втручання в її роботу. Першим кроком є реєстрація всіх змін конфігурації камери до моменту її відключення. Необхідно зафіксувати параметри мережі, протоколи доступу, часові налаштування, облікові записи користувачів та будь-які інші модифікації.

Важливим етапом також вважають вилучення кешованих даних із пам'яті пристрою. Багато моделей камер тимчасово зберігають відео, конфігураційні дані або інші метадані у внутрішньому кеші або на знімних носіях, як-от SD-карти. Ці дані можуть бути втрачені після перезавантаження або відключення камери, тому їх необхідно зібрати якнайшвидше. Використовують програмне забезпечення на кшталт FTK Imager для створення точного образу носія, а також інструменти аналізу оперативної пам'яті, наприклад Volatility.

Певну увагу слід приділити залишковим слідам у журналах підключень. Журнали містять цінну інформацію про кожну спробу доступу до камери, включно з IP-адресами, типами операцій і часовими мітками.

У масштабних системах спостереження, де використовується централізоване управління, важливо додатково опрацювати логи із SIEM-систем. Такі системи реєструють події в реальному часі, фіксують спроби віддаленого доступу та зберігають інформацію про взаємодію між пристроями, даючи змогу побудувати цілісну картину інциденту.

Після відключення IP-камери невідкладно проводять криміналістичний аналіз, щоб виявити залишкові цифрові артефакти, які можуть містити цінні докази. Серед ключових напрямів – робота з локальними носіями, зокрема SD-картами, які часто використовують для зберігання відео. Якщо відеозаписи видалені, а носій ще не перезаписа-

ний, є висока ймовірність їх часткового або повного відновлення. У такому разі можна знайти не лише самі відеофайли, а й фрагменти, що містять ключові епізоди, а також супутні метадані, які вказують на час створення запису, модель камери та інші технічні характеристики.

Крім відео джерелом доказів можуть стати резервні копії конфігурації та прошивки, що деякі IP-камери зберігають автоматично. Аналізуючи ці резервні копії, з'ясовують, як саме була налаштована камера, до яких систем вона підключалась і хто мав до неї доступ.

Важливим джерелом інформації є й метадані відеофайлів, які залишаються навіть після спроб їх видалення або приховування. Такі метадані можуть містити часові мітки, що засвідчують точний момент запису, технічну інформацію про пристрій, зокрема й виробника, модель, а також, за наявності GPS-модуля, й координати місця зйомки. Усе це дає змогу не лише підтвердити автентичність відео, а й зіставити його з іншими подіями і технічними даними в межах розслідування.

Юридична цінність цифрових доказів безпосередньо залежить від збереження цілісності та достовірності інформації. Вкрай важливо гарантувати, що відеозаписи не були змінені чи підроблені на жодному етапі – від вилучення до передавання і подальшого аналізування. Для цього застосовують кілька основних методів. Серед найважливіших є використання хеш-функцій, які формують унікальний цифровий підпис для кожного файлу. Будь-яка, навіть найменша, зміна вмісту відеозапису призводить до зміни хеш-суми, що дає змогу виявити спроби підроблення або модифікації.

Додатково дуже важливим є докладне протоколювання усіх етапів роботи з цифровими доказами. Це передбачає фіксування часу, місця і способу отримання даних, опис використовуваного обладнання, а також детальний перелік усіх виконаних дій із даними. У звітах також обов'язково наводять хеш-суми для підтвердження цілісності даних. Така деталізація забезпечує юридичну значущість зібраних доказів.

Висновки

Ґрунтуючись на досвіді вітчизняних і зарубіжних науковців і практиків у контексті проблематики аналізування мережевого трафіку та криміналістичного дослідження систем відеоспостереження, що актуалізується в сучасній цифровій безпеці й криміналістиці, а також на результатах опрацювання матеріалів експертних проваджень за період 2020 – перше півріччя 2025 р., узагальненні матаріалів проведення відповідних судових експертиз та експертних досліджень, з'ясовано, що криміналістичні основи вилучення IP-камер становлять низку важливих кроків, що дають змогу зберегти цілісність даних і мінімізувати ризики їх втрати. Спочатку варто використовувати сканери портів, як-от Nmap, для визначення активних з'єднань камери з мережею, а також аналізування мережевого трафіку за допомогою Wireshark для встановлення відеопотоків і команд управління. Перед вилученням необхідно ретельно проаналізувати логи та записи підключень, щоб зафіксувати всю цифрову активність пристрою. Для збереження доказів слід створити резервні копії даних, зберегти хеш-суми та журнали, що підтверджують цілісність даних. Камеру можна відключити від мережі як програмно, так і фізично залежно від обставин, а для додаткового захисту від бездротових сигналів варто використовувати Faraday bags, які блокують передавання даних радіоканалами. Весь процес вилучення має бути детально зафіксований для забезпечення прозорості та юридичної значущості зібраних доказів.

Подяки

Немає.

Фінансування

Дослідження не отримувало фінансування.

Конфлікт інтересів

Немає.

References

[1] Alshenai, I. M., Alharbi, L. A., Ramachandran, S., & Kim, K. (2024). Cybersecurity and Forensic Analysis of IP-Cameras Used in Saudi Arabia. *Journal of Information Security and Cybercrimes Research, 7*(1), 67–84. DOI: https://doi.org/10.26735/LLFQ4473

[2] Bhardwaj, A., Kaushik, K., Bharany, S., & Kim, S. (2023). Forensic analysis and security assessment of IoT camera firmware for smart homes. *Egyptian Informatics Journal, 24*(4), 100409. DOI: https://doi.org/10.1016/j.eij.2023.100409

[3] Bilous, V., & Latysh, K. (2022). Sudovi ekspertyzy radioelektronnykh zasobiv ta pytannia zabezpechennia dopustymosti tsyfrovykh dokaziv, zokrema yikh tsilisnosti [Forensic examination of radio electronic devices as a form of using special knowledge during investigation of corruption criminal offenses]. *Naukovi Pratsi Mizhrehionalnoi akademii upravlinnia personalom. Yurydychni Nauky, 1*(61), 5–11 [in Ukrainian]. DOI: https://doi.org/10.32689/2522-4603.2022.1

[4] Bratishko, N. (2023). Napriamy vykorystannia tsyfrovoi kryminalistyky v umovakh voiennoho stanu [Directions of digital forensics under martial law]. *Naukovyi visnyk Dniprovskoho derzhavnoho universytetu vnutrishnikh sprav*,

2(Spetsvyp.), 282–288 [in Ukrainian].
DOI: https://doi.org/10.31733/2078-3566-2023-6-282-288

[5] Gehlot, A., Singh, R., Singh, J., & Sharma, N. R. (Eds.). (2022). *Digital Forensics and Internet of Things*. Scrivener Publishing LLC.
DOI: https://doi.org/10.1002/9781119769057

[6] Halahan, N., Borysenko, I., Khab'iuk, N., Starodubtsev, Ya., & Kovalchuk, N. (2025). Kontseptualna model orhanizatsiino-tekhnichnoi systemy kiberzakhystu IoT-platform. [Conceptual model of organizational and technical system for cyber security of IoT platform]. *Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh, 82*(2), 226–231 [in Ukrainian].
DOI: https://doi.org/10.31891/2219-9365-2025-82-31

[7] Haley, P. (2025). The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent. *Sensors (Basel, Switzerland), 25*(10), 3160.
DOI: https://doi.org/10.3390/s25103160

[8] Hellwig, K. (2021). The Potential and the Challenges of Digital Evidence in International Criminal Proceedings. *International Criminal Law Review,* (22), 965–988.
DOI: https://doi.org/10.1163/15718123-bja10110

[9] Holovin, O. M., & Sapunova, N. O. (2025). Evoliutsiia system videosposterezhennia: vid analohovykh kamer do intelektualnykh system videoanalityky na osnovi hranychnykh obchyslen [Evolution of video surveillance systems: from analog cameras to intelligent video analytics systems based on edge computing]. *Informatsiini tekhnolohii ta systemy*, (3), 56–75 [in Ukrainian].
DOI: https://doi.org/10.15407/intechsys.2025.03.056

[10] Horsman, G. (2021). Digital evidence and the crime scene. *Science & justice: journal of the Forensic Science Society*, *61*(6), 761–770.
DOI: https://doi.org/10.1016/j.scijus.2021.10.003

[11] Ivasyshyn, T. M., & Piroh, O. V. (2025). Poriadok zbyrannia tsyfrovykh dokaziv [The procedure for collecting digital evidence]. *Kryminalistyka i sudova ekspertyza*, (70), 371–381 [in Ukrainian].
DOI: https://doi.org/10.33994/kndise.2025.70.28

[12] Javed, A. R., Jalil, Z., Zehra, W., Gadekallu, T. R., Suh, D. Y., & Piran, Md. J. (2021). A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions. *Engineering Applications of Artificial Intelligence*, (106), 104456.
DOI: https://doi.org/10.1016/j.engappai.2021.104456

[13] Kalbo, N., Mirsky, Y., Shabtai, A., & Elovici, Y. (2020). The Security of IP-Based Video Surveillance Systems. *Sensors (Basel, Switzerland), 20*(17), 4806.
DOI: https://doi.org/10.3390/s20174806

[14] Khakhanovskyi, V. H., & Hutsaliuk, M. V. (2019). Osoblyvosti vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh [The peculiarities of digital evidence use in criminal proceedings]. *Kryminalistychnyi visnyk, 31*(1), 14–20 [in Ukrainian].
DOI: https://doi.org/10.37025/1992-4437/2019-31-1-13

[15] Khaustova, M. H. (2022a). Derzhavna polityka v umovakh tsyfrovizatsii suspilstva. Mizhnarodnyi dosvid realizatsii prohram ta stratehii tsyfrovizatsii [Public policy in the context of digitalization of society. International experience in implementing programs and digitization strategies]. *Analitychno-porivnialne pravoznavstvo*, (2), 209–216 [in Ukrainian].
DOI: https://doi.org/10.24144/2788-6018.2022.02.40

[16] Khaustova, M. H. (2022b). Poniattia tsyfrovizatsii: natsionalni ta mizhnarodni pidkhody [The concept of digitalization: national and international approaches]. *Pravo ta innovatsii, 2*(38), 7–18 [in Ukrainian].
DOI: https://doi.org/10.37772/2518-1718-2022-2(38)-1

[17] Korshenko, V. A., Chumak, V. V., Mordvyntsev, M. V., & Pashniev, D. V. (2020). Stan system bezpeky z vykorystanniam tekhnichnykh zasobiv videozapysu ta videosposterezhennia: zarubizhnyi dosvid, perspektyvy vprovadzhennia v diialnist Natsionalnoi politsii Ukrainy [Security systems status with the use of technical means of video recording and video surveillance: international experience, perspectives for implementation in the activities of the National police of Ukraine]. *Pravo i bezpeka, 2*(77), 86–92 [in Ukrainian].
DOI: https://doi.org/10.32631/pb.2020.2.12

[18] Kostenko, O. V. (2021). Napriamy rozvytku prava u sferi internet rechei (IoT) ta shtuchnoho intelektu [Directions of development of law in the field of internet of things (IoT) and artificial intelligence]. *Aktualni problemy vitchyznianoi yurysprudentsii*, (3), 130–136 [in Ukrainian].
DOI: https://doi.org/10.15421/392161

[19] Lindeman, J., Luchtman, M., & Van Toor, D. (2024). Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair-Trial Rights in the Netherlands. *Admissibility of Evidence in EU Cross-Border Criminal Proceedings*, 103–126.
DOI: https://doi.org/10.5040/9781509972029.ch-007

[20] Mamatkulova, K. (2021). Admissibility Of Electronic Evidence In Criminal Proceedings. *The American Journal of Political Science Law and Criminology, 3*(2), 144–152.
DOI: https://doi.org/10.37547/tajpslc/volume03issue02-21

[21] Ndatinya, V., Xiao, Z., Manepalli, V. R., Meng, K., & Xiao, Y. (2015). Network forensics analysis using Wireshark. *International Journal of Security and Networks, 10*(2), 91–106.
DOI: https://doi.org/10.1504/ijsn.2015.070421

[22] Oettinger, W. (2024). *Learn Mobile Forensics: The Complete Guide from Extraction to Courtroom Testimony*. Packt Publishing.
https://learning.oreilly.com/library/view/learn-mobile-forensics/9781835889602/
[23] Parasram, S. V. N. (2023). *Digital Forensics with Kali Linux* (3rd ed.). Packt Publishing.
https://learning.oreilly.com/library/view/digital-forensics-with/9781837635153/
[24] Petryk, V. V. (2025). Vykorystannia elektronnykh dokaziv u kryminalnomu provadzhenni: problemy yikh zboru, perevirky ta otsinky [The use of electronic evidence in criminal proceedings: issues of collection, verification, and evaluation]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo, 87*(4), 119–123 [in Ukrainian].
DOI: https://doi.org/10.24144/2307-3322.2025.87.4.17
[25] Pogoretskyi, M. A., & Lysachenko, E. I. (2023). Vstanovlennia dostovirnosti tsyfrovykh dokaziv Mizhnarodnym kryminalnym sudom: okremi problemni pytannia ta shliakhy yikh vyrishennia [Establishing the reliability of digital evidence by the International criminal court: some problematic issues and ways to solve them]. *Visnyk kryminalnoho sudochynstva*, (1–2), 54–73 [in Ukrainian].
DOI: https://doi.org/10.17721/2413-5372.2023.1-2/54-73
[26] Ramadhan, R., Mualfah, D., & Hariyadi, D. (2019). Digital Forensics: Acquisition and Analysis on CCTV Digital Evidence using Static Forensic Method based on ISO /IEC 27037:2014. In *Proceedings of the Second International Conference on Science, Engineering and Technology (ICoSET 2019)* (pp. 85–89).
DOI: https://doi.org/10.5220/0009120400850089
[27] Ramakrishnan, G., & Haqanee, M. (2024). *Cloud Forensics Demystified*. Packt Publishing.
https://learning.oreilly.com/library/view/cloud-forensics-demystified/9781800564411/
[28] Romaniuk, V. V., & Fomina, T. H. (2024). Poriadok zbyrannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh pro kolaboratsiinu diialnist. *Visnyk kryminolohichnoi asotsiatsii Ukrainy*, *2*(32), 344–353 [in Ukrainian].
DOI: https://doi.org/10.32631/vca.2024.2.25
[29] Ruvinska, V. M., & Deviatkov, V. V. (2021). Videosposterezhennia dlia system bezpeky: modeli, metody ta zaproponovani rishennia [Video surveillance for security systems: models, methods and proposed solutions]. *Informatyka ta matemanychni metody v modeliuvanni*, *11*(4), 331–342 [in Ukrainian].
DOI: https://doi.org/10.15276/imms.v11.no4.331
[30] Salem, Y., & Hamarsheh, M. M. N. (2024). Forensically analyzing IoT smart camera using MAoIDFF-IoT framework. *Forensic Science International: Digital Investigation*, (51), 301829.
DOI: https://doi.org/10.1016/j.fsidi.2024.301829
[31] Salih, K., & Dabagh, N. (2023). Digital Forensic Tools: A Literature Review. *Journal of Education and Science, 32*(1), 109–124.
DOI: https://doi.org/10.33899/edusj.2023.137420.1304
[32] Shevchuk, V. M. (2024). Rol tekhnolohii shtuchnoho intelektu u pravookhoronnii diialnosti ta zabezpechenni bezpeky ta oboronozdatnosti Ukrainy [The role of artificial intelligence technologies in law enforcement activities and ensuring the security and defense capacity of Ukraine]. *Yurydychnyi naukovyi elektronnyi zhurnal*, (6), 356–361 [in Ukrainian].
DOI: https://doi.org/10.32782/2524-0374/2024-6/88
[33] Sokol, P., Rozenfeldov, L., Lucivjanska, K., & Harasta, J. (2020). IP Addresses in the Context of Digital Evidence in the Criminal and Civil Case Law of the Slovak Republic. *Forensic Science International: Digital Investigation*, (32), 51–58.
DOI: https://doi.org/10.1016/j.fsidi.2020.300918
[34] Soni, N. (2025). Forensic Value of Exif Data: An Analytical Evaluation of Metadata Integrity across Image Transfer Methods. *Perspectives in Legal and Forensic Sciences*, *2*(2), 10006-10006.
DOI: https://doi.org/10.70322/plfs.2025.10006
[35] Stabili, D., Bocchi, T., Valgimigli, F., & Marchetti, M. (2024). Finding (and exploiting) vulnerabilities on IP Cameras: the Tenda CP3 case study. *International Workshop on Security*.
DOI: https://doi.org/10.48550/arXiv.2406.15103
[36] Van der Velden, L. (2015). Forensic devices for activism: Metadata tracking and public proof. *Big Data & Society*, *2*(2).
DOI: https://doi.org/10.1177/2053951715612823
[37] Yashchuk, V. I., Panovyk, U. P., Cherkas, S. A., Ivanusa, A. I., & Tkachuk, R. L. (2025). Kompleksna model zakhystu IoT-prystroiv u pobutovomu seredovyshchi: zahrozy, vrazlyvosti ta metody neitralizatsii [Comprehensive protection model of IoT devices in the home environment: threats, vulnerabilities and methods of neutralization] *Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti*, (32), 125–140 [in Ukrainian].
DOI: https://doi.org/10.32447/20784643.32.2025.10

Список використаних джерел

[1] Alshenai I. M., Alharbi L. A., Ramachandran S., Kim K. Cybersecurity and Forensic Analysis of IP-Cameras Used in Saudi Arabia. *Journal of Information Security and Cybercrimes Research.* 2024. No 7(1). P. 67–84.
DOI: https://doi.org/10.26735/LLFQ4473
[2] Bhardwaj A., Kaushik K., Bharany S., Kim S. Forensic analysis and security assessment of IoT camera firmware for smart homes. *Egyptian Informatics Journal.* 2023. No 24(4). Art. 100409.
DOI: https://doi.org/10.1016/j.eij.2023.100409
[3] Білоус В., Латиш К. Судові експертизи радіоелектронних засобів та питання забезпечення допустимості цифрових доказів, зокрема їх цілісності. *Наукові Праці Міжрегіональної академії управління персоналом. Юридичні науки*. 2022. № 1(61). С. 5–11.
DOI: https://doi.org/10.32689/2522-4603.2022.1.1

[4] Братішко Н. Напрями використання цифрової криміналістики в умовах воєнного стану. *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2023. № 2 (Спецвип.). С. 282–288.
DOI: https://doi.org/10.31733/2078-3566-2023-6-282-288
[5] Gehlot A., Singh R., Singh J., Sharma N. R. (Eds.). Digital Forensics and Internet of Things. Scrivener Publishing LLC, 2022.
DOI: https://doi.org/10.1002/9781119769057
[6] Галаган Н., Борисенко І., Хаб'юк Н., Стародубцев Я., Ковальчук Н. Концептуальна модель організаційно-технічної системи кіберзахисту IoT-платформ. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2025. № 82(2). С. 226–231.
DOI: https://doi.org/10.31891/2219-9365-2025-82-31
[7] Haley P. The Impact of Biometric Surveillance on Reducing Violent Crime: Strategies for Apprehending Criminals While Protecting the Innocent. *Sensors (Basel, Switzerland)*. 2025. No 25(10). Art. 3160.
DOI: https://doi.org/10.3390/s25103160
[8] Hellwig K. The Potential and the Challenges of Digital Evidence in International Criminal Proceedings. *International Criminal Law Review*. 2021. No 22. P. 965–988.
DOI: https://doi.org/10.1163/15718123-bja10110
[9] Головін О. М., Сапунова Н. О. Еволюція систем відеоспостереження: від аналогових камер до інтелектуальних систем відеоаналітики на основі граничних обчислень. *Інформаційні технології та системи*. 2025. № 3. С. 56–75.
DOI: https://doi.org/10.15407/intechsys.2025.03.056
[10] Horsman G. Digital evidence and the crime scene. *Science & justice: journal of the Forensic Science Society*. 2021. No 61(6). P. 761–770.
DOI: https://doi.org/10.1016/j.scijus.2021.10.003
[11] Івасишин Т. М., Пірог О. В. Порядок збирання цифрових доказів. *Криміналістика і судова експертиза*. 2025. Вип. 70. С. 371–381.
DOI: https://doi.org/10.33994/kndise.2025.70.28
[12] Javed A. R., Jalil Z., Zehra W., Gadekallu T. R., Suh D. Y., Piran Md. J. A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions. *Engineering Applications of Artificial Intelligence*. 2021. No 106. Art. 104456.
DOI: https://doi.org/10.1016/j.engappai.2021.104456
[13] Kalbo N., Mirsky Y., Shabtai A., Elovici Y. The Security of IP-Based Video Surveillance Systems. *Sensors (Basel, Switzerland)*. 2020. No 20(17). Art. 4806.
DOI: https://doi.org/10.3390/s20174806
[14] Хахановський В. Г., Гуцалюк М. В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник*. 2019. № 31(1). С. 14–20.
DOI: https://doi.org/10.37025/1992-4437/2019-31-1-13
[15] Хаустова М. Г. Державна політика в умовах цифровізації суспільства. Міжнародний досвід реалізації програм та стратегії цифровізації. *Аналітично-порівняльне правознавство*. 2022. № 2. С. 209–216.
DOI: https://doi.org/10.24144/2788-6018.2022.02.40
[16] Хаустова М. Г. Поняття цифровізації: національні та міжнародні підходи. *Право та інновації*. 2022. № 2(38). С. 7–18.
DOI: https://doi.org/10.37772/2518-1718-2022-2(38)-1
[17] Коршенко В. А., Чумак В. В., Мордвинцев М. В., Пашнєв Д. В. Стан систем безпеки з використанням технічних засобів відеозапису та відеоспостереження: зарубіжний досвід, перспективи впровадження в діяльність Національної поліції України. *Право і безпека*. 2020. № 2(77). С. 86–92.
DOI: https://doi.org/10.32631/pb.2020.2.12
[18] Костенко О. В. Напрями розвитку права у сфері інтернет речей (IoT) та штучного інтелекту [Directions of development of law in the field of internet of things (IoT) and artificial intelligence]. *Актуальні проблеми вітчизняної юриспруденції*. 2021. № 3. С. 130–136.
DOI: https://doi.org/10.15421/392161
[19] Lindeman J., Luchtman M., Van Toor D. Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair-Trial Rights in the Netherlands. *Admissibility of Evidence in EU Cross-Border Criminal Proceedings*. 2024. С. 103–126.
DOI: https://doi.org/10.5040/9781509972029.ch-007
[20] Mamatkulova K. Admissibility Of Electronic Evidence In Criminal Proceedings. *The American Journal of Political Science Law and Criminology*. 2021. No 3(2). P. 144–152.
DOI: https://doi.org/10.37547/tajpslc/volume03issue02-21
[21] Ndatinya V., Xiao Z., Manepalli V. R., Meng K., Xiao Y. Network forensics analysis using Wireshark. *International Journal of Security and Networks*. 2015. No 10(2). P. 91–106.
DOI: https://doi.org/10.1504/ijsn.2015.070421
[22] Oettinger W. Learn Mobile Forensics: The Complete Guide from Extraction to Courtroom Testimony. Packt Publishing, 2024. 295 p.
URL: https://learning.oreilly.com/library/view/learn-mobile-forensics/9781835889602
[23] Parasram S. V. N. Digital Forensics with Kali Linux (3rd ed.). Packt Publishing, 2023. 414 p.
URL: https://learning.oreilly.com/library/view/digital-forensics-with/9781837635153/
[24] Петрик В. В. Використання електронних доказів у кримінальному провадженні: проблеми їх збору, перевірки та оцінки. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2025. Вип. 87(4).

С. 119–123.
DOI: https://doi.org/10.24144/2307-3322.2025.87.4.17
[25] Погорецький М. А., Лисаченко Є. І. Встановлення достовірності цифрових доказів Міжнародним кримінальним судом: окремі проблемні питання та шляхи їх вирішення. *Вісник кримінального судочинства*. 2023. № 1–2. С. 54–73.
DOI: https://doi.org/10.17721/2413-5372.2023.1-2/54-73
[26] Ramadhan R., Mualfah D., Hariyadi D. Digital Forensics: Acquisition and Analysis on CCTV Digital Evidence using Static Forensic Method based on ISO /IEC 27037:2014. *Proceedings of the Second International Conference on Science, Engineering and Technology (ICoSET 2019)*. 2019. P. 85–89.
DOI: https://doi.org/10.5220/0009120400850089
[27] Ramakrishnan G., Haqanee M. Cloud Forensics Demystified. Packt Publishing, 2024. 348 p.
URL: https://learning.oreilly.com/library/view/cloud-forensics-demystified/9781800564411/
[28] Романюк В. В., Фоміна Т. Г. Порядок збирання електронних (цифрових) доказів у кримінальних провадженнях про колабораційну діяльність. *Вісник кримінологічної асоціації України*. 2024. № 2(32). С. 344–353.
DOI: https://doi.org/10.32631/vca.2024.2.25
[29] Рувінська В. М., Девятков В. В. Відеоспостереження для систем безпеки: моделі, методи та запропоновані рішення. *Інформатика та математичні методи в моделюванні*. 2021. № 11(4). С. 331–342.
DOI: https://doi.org/10.15276/imms.v11.no4.331
[30] Salem Y., Hamarsheh M. M. N. Forensically analyzing IoT smart camera using MAoIDFF-IoT framework. *Forensic Science International: Digital Investigation*. 2024. No 51. Art. 301829.
DOI: https://doi.org/10.1016/j.fsidi.2024.301829
[31] Salih K., Dabagh N. Digital Forensic Tools: A Literature Review. *Journal of Education and Science*. 2023. No 32(1). P. 109–124.
DOI: https://doi.org/10.33899/edusj.2023.137420.1304
[32] Шевчук В. М. Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки та обороноздатності України. *Юридичний науковий електронний журнал*. 2024. № 6. С. 356–361.
DOI: https://doi.org/10.32782/2524-0374/2024-6/88
[33] Sokol P., Rozenfeldov L., Lucivjanska K., Harasta J. IP Addresses in the Context of Digital Evidence in the Criminal and Civil Case Law of the Slovak Republic. *Forensic Science International: Digital Investigation*. 2020. No 32. P. 51–58.
DOI: https://doi.org/10.1016/j.fsidi.2020.300918
[34] Soni N. Forensic value of Exif data: An analytical evaluation of metadata integrity across image transfer methods. *Perspectives in Legal and Forensic Sciences*. 2025. No 2(2). Art. 10006–10006.
DOI: https://doi.org/10.70322/plfs.2025.10006
[35] Stabili D., Bocchi T., Valgimigli F., Marchetti M. Finding (and exploiting) vulnerabilities on IP Cameras: the Tenda CP3 case study. *International Workshop on Security*. 2024.
DOI: https://doi.org/10.48550/arXiv.2406.15103
[36] Van der Velden L. Forensic devices for activism: Metadata tracking and public proof. *Big Data & Society*. 2015. No 2(2).
DOI: https://doi.org/10.1177/2053951715612823
[37] Ящук В. І., Пановик У. П., Черкас С. А., Івануса А. І., Ткачук Р. Л. Комплексна модель захисту IoT-пристроїв у побутовому середовищі: загрози, вразливості та методи нейтралізації. *Вісник Львівського державного університету безпеки життєдіяльності*. 2025. № 32. С. 125–140.
DOI: https://doi.org/10.32447/20784643.32.2025.10

O. Piroh,
Cand. Sc. (Technical)
Chief Forensic Expert of the Expert Sector (based in Zhytomyr),
Ukrainian Scientific Research Institute of Special Equipment
and Forensic Expertise,
Security Service of Ukraine
3 Mykoly Vasylenka St., Kyiv, 03113, Ukraine
ORCID: https://orcid.org/0009-0001-6111-9676
email: pirogov@ztu.edu.ua
T. Ivasyshyn,
Cand. Sc. (Biological),
Associate Professor of the Department of Criminal Procedure
and Criminalistics, Educational and Scientific Humanitarian Institute,
National Academy of the Security Service of Ukraine
22 Mykhaila Maksymovycha St., Kyiv, 03066, Ukraine
ORCID: https://orcid.org/0009-0007-6604-0362

IP CAMERAS SEIZURE: FORENSIC ASPECTS

Abstract. The article examines aspects of a forensic procedural actions involving the use of IP camera-based video surveillance systems, with particular attention to procedures for disconnecting such devices from the network without losing critical data. The study employs general scientific methods of cognition aimed at the theoretical substantiation of the process of IP camera seizure during the conduct of procedural actions, including formal-logical methods (analysis, synthesis, induction, deduction, abstraction), as well as methods of comparison, modeling, and generalization, along with special methods (forensic, system-structural, and technical-legal analysis). The research relied on standard digital forensic hardware tools, external storage devices, and software instruments such as Nmap, Wireshark, FTK Imager, and ONVIF Device Manager. The scientific novelty of the study lies in the formation of a systematic vision of the process of IP camera seizure in forensic practice. Furthermore, the relevance of the topic is highlighted in the context of digitalization, where IP cameras serve as sources of key digital evidence-video recordings, metadata, access logs, and configuration parameters. The main types of IP cameras are categorized and analyzed: standalone devices, those connected to network or digital video recorders (NVR/DVR), and cloud-based solutions, with emphasis on data storage features, security levels, and vulnerabilities. The study examines the operation of key network protocols (RTSP, HTTP, ONVIF, MQTT) used for video and command transmission. These protocols can serve as important sources of digital evidence. Special attention is given to network traffic analysis using Wireshark, which enables investigators to identify interactions between cameras and other network devices, detect video streams, and determine data transmission paths, including those involving cloud services. The role of Nmap in searching for active cameras and video recorders, analyzing open ports, and identifying active services is also discussed. The study highlights challenges in detecting centralized or cloud-based video storage, such as the use of encryption, non-standard ports, self-erasing data mechanisms, or restricted access. Practical recommendations are provided for both software-based (via firewalls and routers) and physical (network disconnection or signal shielding with a Faraday bag) isolation of cameras while maintaining the integrity of technical recordings. The authors also offer guidelines for creating video and configuration backups, retrieving cached data, and analyzing log files. The importance of ensuring the admissibility of collected data through cryptographic hash verification and detailed documentation of all stages of data collection and analysis is emphasized. The study concludes that implementing standardized procedures for disconnection of IP cameras and the preservation of digital evidence significantly enhances the effectiveness of pre-trial investigations and the admissibility of factual data presented in court.

Keywords: digital evidence; inspection; seizure; procedural actions; Nmap; Wireshark; video surveillance systems.