

**КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА;
ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ**

УДК 343.98:004.056.5

DOI <https://doi.org/10.32844/2618-1258.2026.3.42>

БУРЕНКО О.В.

**УЧАСТЬ СПЕЦІАЛІСТА У ЗБИРАННІ ТА ВИКОРИСТАННЯ ІНФОРМАЦІЇ
ІЗ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ ПІД ЧАС РОЗСЛІДУВАННЯ
КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ**

**PARTICIPATION OF A SPECIALIST IN THE COLLECTION
AND USE OF INFORMATION FROM VIDEO SURVEILLANCE SYSTEMS
DURING THE INVESTIGATION OF CRIMINAL OFFENSES**

У статті досліджено участь спеціаліста у збиранні і використанні інформації із систем відеоспостереження під час розслідування кримінальних правопорушень. Проаналізовано діюче законодавство України стосовно участі спеціаліста у процесі збирання, фіксації, дослідження та використання інформації із систем відеоспостереження під час розслідування кримінальних правопорушень. Визначено основні напрями діяльності спеціаліста під час проведення слідчих (розшукових) дій, пов'язаних із вилученням та аналізом цифрової відеоінформації. Приведено алгоритм дій спеціаліста під час вилучення інформації. Проаналізовано значення відеоспостереження як джерела доказової інформації у кримінальному провадженні. Окрему увагу приділено проблемам автентичності цифрових відеозаписів, забезпечення їх цілісності та процесуального оформлення. Наголошено на необхідності залучення спеціалістів у галузі цифрової криміналістики та інформаційних технологій під час розслідування кримінальних правопорушень.

Встановлено, що інформація, яку повідомляє спеціаліст, сама по собі не є самостійним джерелом доказів. На відміну від висновку експерта, який відповідно до статей 84 і 101 КПК України визнається процесуальним джерелом доказів, консультації, пояснення та технічна допомога спеціаліста мають допоміжний характер. Їх основне призначення полягає у забезпеченні законного та правильного отримання доказів. Юридична значущість інформації, наданої спеціалістом, зумовлюється не лише фактом надання консультації чи пояснень, а виключно її належним процесуальним оформленням. Відомості, отримані за участю спеціаліста, набувають доказового значення для кримінального провадження за умови їх фіксації у відповідних процесуальних документах.

Разом з тим, ефективне збирання та подальше використання інформації із систем відеоспостереження передбачає наявність спеціальних знань у сферах комп'ютерної техніки, цифрової криміналістики, телекомунікацій та сучасних технологій відеоаналізу. З огляду на це, залучення спеціаліста під час проведення слідчих (розшукових) дій, спрямованих на виявлення, вилучення, копіювання, аналіз та подальше використання цифрової відеоінформації, набуває особливої актуальності.

Ключові слова: кримінальне провадження, програмне забезпечення, цифрові докази, відеозапис, джерело доказів.

© БУРЕНКО О.В. – викладач кафедри кримінології та інформаційних технологій (Національна академія внутрішніх справ) <https://orcid.org/0000-0002-7583-7644>

Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)



The article examined the participation of a specialist in the collection and use of information from video surveillance systems during the investigation of criminal offenses. Analyzed the current legislation of Ukraine regarding the participation of a specialist in the process of collecting, recording, examining, and using information from video surveillance systems during the investigation of criminal offenses. Identified the main areas of activity of a specialist during investigative (search) actions related to the seizure and analysis of digital video information. Provided an algorithm of specialist actions during information retrieval. Analyzed the significance of video surveillance as a source of evidentiary information in criminal proceedings. Special attention was paid to the problems of authenticity of digital video recordings, ensuring their integrity, and procedural documentation. Emphasized the necessity of involving specialists in the field of digital forensics and information technologies during the investigation of criminal offenses.

It was established that the information provided by a specialist is not, by itself, an independent source of evidence. Unlike the expert's conclusion, which, according to Articles 84 and 101 of the Criminal Procedure Code of Ukraine, is recognized as a procedural source of evidence, the consultations, explanations, and technical assistance of a specialist are auxiliary in nature. Their main purpose is to ensure the lawful and proper collection of evidence. The legal significance of the information provided by a specialist is determined not only by the fact of giving consultations or explanations, but exclusively by its proper procedural documentation. The information obtained with the participation of a specialist acquires evidentiary value for criminal proceedings provided that it is recorded in the relevant procedural documents.

At the same time, the effective collection and subsequent use of information from video surveillance systems requires specialized knowledge in the fields of computer technology, digital forensics, telecommunications, and modern video analysis technologies. In view of this, the involvement of a specialist during investigative (search) actions aimed at detecting, seizing, copying, analyzing, and further using digital video information becomes particularly relevant.

Key words: *criminal proceedings, software, digital evidence, video recording, source of evidence.*

Вступ. Стрімкий розвиток інформаційних технологій зумовив широке впровадження систем відеоспостереження у громадських місцях, на об'єктах транспортної інфраструктури, в установах, на підприємствах та в приватному секторі. Як наслідок, відеоінформація набуває дедалі більшого значення як джерело доказів у кримінальному провадженні. Відеоматеріали забезпечують об'єктивну фіксацію обстановки місця події, механізму вчинення кримінального правопорушення, зовнішніх ознак осіб, які причетні до діяння, транспортних засобів, маршрутів їх пересування та інших обставин, що мають суттєве значення для встановлення істини у справі та мають доказове значення.

Тему участі спеціаліста у збиранні та використанні інформації із систем відеоспостереження під час розслідування кримінальних правопорушень, вивчали такі вчені, як В. Ю. Шепітько, Р. Л. Степанюк, Г. К. Авдєєва, Т. Г. Фоміна.

Питання залучення спеціалістів до кримінального провадження останнім часом перебувають у фокусі наукових досліджень І. М. Вигівського, В. В. Юсупова, А. В. Коваленка, О. А. Кравченка, О. Д. Кувшинова, Є. Д. Лук'янчикова, Д. Б. Сергєєвої, В. О. Яремчука та інших науковців. У межах зазначених праць здійснюється розроблення та вдосконалення тактичних аспектів окремих слідчих (розшукових) дій, де значна увага приділяється визначенню специфіки залучення спеціалістів, аналізу їхнього процесуального статусу, а також обґрунтуванню організаційних і тактичних засад їхньої участі у кримінальному процесі.

Постановка завдання. Метою статті є визначення особливостей участі спеціаліста у збиранні і використанні інформації із систем відеоспостереження під час розслідування кримінальних правопорушень.

Результати дослідження. Сучасні цифрові системи відеофіксації мають складну архітектуру, яка передбачає використання різних форматів запису, алгоритмів стиснення відео, мережевих протоколів передачі даних та спеціалізоване програмне забезпечення. Як засвідчує слідча

практика, ефективність використання інформації із систем відеоспостереження значною мірою залежить від своєчасного залучення спеціаліста. Відсутність спеціальних знань у цій сфері створює високі ризики втрати важливої доказової інформації, пошкодження носіїв даних або порушення процесуального порядку їх вилучення. З огляду на це, залучення спеціаліста є одним із ключових чинників забезпечення належного збирання та використання цифрових доказів у кримінальному провадженні.

Під час розслідування кримінальних правопорушень фахівці, володіючи спеціальними знаннями, необхідними для належної фіксації, аналізу та оцінки складних і нестандартних обставин, відіграють ключову роль у документуванні фактів протиправної діяльності. Згідно з ч. 1 ст. 71 КПК України, спеціалістом є особа, яка володіє спеціальними знаннями та навичками і залучається до процесуальних дій під час досудового розслідування або судового розгляду для надання консультацій, пояснень, довідок чи висновків із питань, що потребують відповідної фахової компетенції [1].

Спеціаліст може бути залучений для надання безпосередньої технічної допомоги (фотографування, складення схем, планів, креслень, відбір зразків для проведення експертизи тощо) сторонами кримінального провадження під час досудового розслідування і судом під час судового розгляду, а також для надання довідок, висновків та інших документів (довідки, висновки з питань, що належать до сфери його знань, щодо ідентифікації особи, зброї, бойових припасів, вибухових речовин, вибухових пристроїв, слідів вибуху або пострілу, наркотичних засобів, психотропних речовин, їх аналогів і прекурсорів, сильнодіючих лікарських засобів) (ч. 2 ст. 71 КПК України) [1].

Разом із тим, інформація, яку повідомляє спеціаліст, сама по собі не є самостійним джерелом доказів. На відміну від висновку експерта, який відповідно до статей 84 і 101 КПК України визнається процесуальним джерелом доказів, консультації, пояснення та технічна допомога спеціаліста мають допоміжний характер. Їх основне призначення полягає у забезпеченні законного та правильного отримання доказів [1].

Юридична значущість інформації, наданої спеціалістом, зумовлюється не лише фактом надання консультацій чи пояснень, а виключно її належним процесуальним оформленням. Відомості, отримані за участю спеціаліста, набувають доказового значення для кримінального провадження за умови їх фіксації у відповідних процесуальних документах:

- протоколи огляду місця події;
- протоколи обшуку;
- протоколи тимчасового доступу до речей і документів;
- протоколи огляду предметів та документів;
- протоколи проведення слідчого експерименту;
- додатках до протоколів (фототаблицях, схемах, планах, відеозаписах, цифрових копіях, журналах хешування тощо).

Якщо спеціаліст для наприкладу, здійснює форензичне копіювання жорсткого диска відеореєстратора, то саме протокол слідчої (розшукової) дії повинен містити відомості про використання обладнання, програмне забезпечення, метод копіювання, обчислені хеш-значення та інші технічні параметри. У такому випадку ці відомості стають частиною процесуального документа, який відповідно до КПК може використовуватися як джерело доказової інформації. Також письмові пояснення спеціалістів можуть бути додатками до протоколу процесуальної дії, у проведенні якої відповідні спеціалісти брали участь (ст. 105 КПК України).

Під час розслідування кримінальних правопорушень, для збирання інформації із систем відеоспостереження зазвичай залучають спеціаліста з інформаційних технологій (у галузі захисту інформації, інформаційно-аналітичного забезпечення або у сфері протидії кіберзлочинності) [2, с. 143].

Залучення спеціаліста позитивно впливає й на оперативність розслідування. Завдяки використанню сучасних технічних засобів і спеціалізованого програмного забезпечення значна частина інформації може бути отримана та попередньо проаналізована безпосередньо під час проведення слідчої (розшукової) дії. Це дозволяє швидше встановити коло осіб, причетних до кримінального правопорушення, визначити маршрути їх пересування, ідентифікувати транспортні засоби, уточнити час окремих подій та сформувати версії щодо механізму вчинення злочину. В свою чергу оперативне отримання такої інформації дає можливість своєчасно організувати подальші слідчі (розшукові) та процесуальні дії, призначити необхідні судові експертизи, провести обшуки чи тимчасовий доступ до речей і документів, а також запобігти втраті інших доказів.

Згідно з нормами Кримінального процесуального кодексу України, залучення спеціаліста є необхідним для надання технічної допомоги під час проведення слідчих (розшукових) дій, зокрема для застосування технічних засобів, а також виявлення, фіксації та вилучення доказів. Зазначена практика набуває особливої значущості під час опрацювання цифрових носіїв інформації та систем відеоспостереження.

На сьогодні у чинному законодавстві України відсутнє нормативне визначення поняття «цифровий доказ», а також не встановлено чіткого порядку фіксації цифрової інформації, зокрема переліку відомостей, що підлягають обов'язковому відображенню у протоколі процесуальної дії та додатках до нього. Неналежне або неповне документування цифрових даних створює ризик їх визнання недопустимими як джерел доказів у кримінальному провадженні. Наразі в Україні відсутній уніфікований підхід до оцінки достовірності цифрових доказів, отриманих як із матеріальних носіїв інформації, так і з мережі Інтернет [3, с. 171].

В той же час в діючому кримінальному процесуальному законодавстві України вказано на можливість роботи з цифровою інформацією (цифровими доказами). Зокрема, у ч. 2 ст. 99 КПК України зазначено, що до документів, зокрема, можуть належати «матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні)» [1].

Науковці в галузі кримінально-правових наук вважають, що сьогодні рівень підготовки слідчих у роботі із програмно-технічними комплексами та складними програмними оболонками є низьким. У зв'язку з цим потрібно обов'язково залучати спеціаліста під час роботи з «цифровими доказами», оскільки найменша некваліфікована дія може призвести до втрати важливої доказової чи орієнтуючої інформації [4, с. 135].

На сьогодні участь спеціаліста необхідна під час огляду місця події; тимчасового доступу до речей і документів; обшуку, вилучення серверів, відеореєстраторів, жорстких дисків; копіювання цифрової інформації; проведення комп'ютерно-технічних досліджень. Саме спеціаліст може забезпечити правильне відключення обладнання, недопущення втрати інформації, копіювання відеозаписів без зміни їх структури, а також документування технічних параметрів системи відеоспостереження.

Під час розслідування кримінальних правопорушень джерелами відеоінформації можуть виступати камери зовнішнього спостереження; інтегровані системи громадської безпеки «Безпечне місто»; приватні системи відеонагляду; автомобільні відеореєстратори; персональні нагрудні відеокамери працівників поліції та мобільні пристрої громадян [5, с. 37].

Ключовим завданням спеціаліста є встановлення місць розташування засобів відеофіксації, визначення секторів огляду, а також перевірка технічного стану обладнання та відповідності часових параметрів запису. Необхідно враховувати, що розбіжність між системним часом відеореєстраторів та фактичним часом може суттєво впливати на коректність відтворення хронології подій.

Під час вилучення інформації спеціаліст зобов'язаний дотримуватися наступного алгоритму дій:

1. Ідентифікація типу обладнання та формату запису (встановлення типу DVR/NVR; моделі; операційної системи; файлової системи; формату відеозапису; способу збереження відео).

2. Визначення оптимального методу копіювання даних. Взагалі вибір конкретного методу залежить від типу обладнання, його технічного стану, особливостей файлової системи, способу зберігання інформації та процесуальної ситуації. На сьогодні використовують наступні методи:

- Форензичне копіювання (forensic imaging або forensic acquisition) є найбільш надійним способом вилучення цифрової інформації. Процес полягає у створенні побітової копії (bit-by-bit image) носія інформації, що гарантує повну цілісність оригінальних даних без будь-яких змін. Окрім видимих файлів, процедура передбачає копіювання службової інформації файлової системи, прихованих розділів диска, незайнятих секторів, видалених даних, журналів файлової системи, метаданих та інших цифрових артефактів, які можуть становити доказову цінність.

- Logical acquisition (логічне копіювання) полягає у вилученні лише тих файлів і каталогів, до яких забезпечується доступ через операційну систему або програмне забезпечення пристрою. На відміну від форензичного копіювання, при логічному вилученні не копіюються незайняті сектори носія, службові структури файлової системи, видалені файли чи інші приховані області.

- Physical acquisition (фізичне копіювання) передбачає отримання повного вмісту фізичної пам'яті пристрою незалежно від структури файлової системи чи можливостей операційної системи. Цей метод дозволяє отримати інформацію навіть із пошкоджених або заблокованих носіїв. Під час розслідування кримінальних правопорушень фізичне копіювання

використовується у випадках пошкодження файлової системи відеореєстратора; відсутності доступу через стандартний інтерфейс; використання нестандартних файлових систем виробника; необхідності відновлення видалених відеозаписів; дослідження накопичувачів із серйозними програмними збоями.

– Live acquisition (отримання інформації із працюючої системи) застосовується тоді, коли цифровий пристрій перебуває у ввімкненому стані, а його вимкнення може призвести до втрати важливої інформації. Для систем відеоспостереження цей метод є особливо актуальним, оскільки сучасні мережеві відеореєстратори та сервери можуть безперервно записувати відео; зберігати дані лише в оперативній пам'яті; автоматично видаляти записи після вимкнення; використовувати шифрування, ключі якого доступні лише під час роботи системи.

3. Забезпечення повної незмінності оригінального цифрового носія інформації. Це один із базових принципів цифрової криміналістики. Для цього застосовують спеціалізовані апаратні або програмні засоби блокування запису (write blocker). Write blocker є пристроєм або програмним модулем, який забезпечує односторонній доступ до носія інформації: спеціаліст може читати всі дані, але фізично не має можливості записувати або змінювати будь-яку інформацію на оригінальному накопичувачі. Таким чином виключається ризик випадкової модифікації цифрових доказів під час їх копіювання чи дослідження. увагу на необхідність детального документування всіх виконаних дій. У процесуальних документах повинні бути відображені дата і час вилучення цифрового носія, модель та серійний номер обладнання, характеристики носія інформації, спосіб підключення, тип використаного write blocker, програмне забезпечення, за допомогою якого здійснювалося копіювання, алгоритм хешування та отримані контрольні значення.

4. Верифікація цілісності цифрових даних (integrity verification). Досить важливий етап роботи спеціаліста під час вилучення інформації із систем відеоспостереження. Її метою є підтвердження того, що після копіювання, транспортування, зберігання чи дослідження цифрова інформація не була змінена. Саме забезпечення цілісності є однією з ключових вимог цифрової криміналістики, оскільки навіть незначна модифікація одного біта інформації призводить до зміни цифрового відбитка (хеш-значення) файлу.

5. Обов'язкова фіксація криптографічних хеш-значень (hash values) цифрових доказів є фундаментальним принципом цифрової криміналістики. Найбільш надійним способом підтвердження незмінності цифрової інформації є використання криптографічних хеш-функцій. Контрольні хеш-значення є своєрідним «цифровим відбитком» файлу або носія інформації. Воно формується шляхом математичного перетворення всього масиву даних і є унікальним для конкретного цифрового об'єкта. Навіть зміна одного біта інформації призводить до формування абсолютно іншого хеш-значення. Завдяки цій властивості хешування дозволяє швидко та об'єктивно встановити, чи зазнали цифрові дані будь-яких змін після їх вилучення [6].

Суворе дотримання методології цифрової криміналістики є критично важливим, оскільки будь-яке несанкціоноване втручання у структуру відеофайлів може стати підставою для визнання доказу недопустимим у судовому процесі.

У 2020 р. Центром прав людини Університету Берклі в Каліфорнії та Офісом Верховного комісара ООН з прав людини представлений «Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права» (Протокол Берклі). Він містить стандарти і методологічні підходи до збирання, збереження та аналізу інформації у відкритому доступі, яка може слугувати доказом у кримінальному провадженні. У Протоколі Берклі викладені алгоритми пошуку, накопичення, аналізу та збереження цифрової інформації з відкритих джерел із дотриманням принципів об'єктивності, компетентності, підзвітності, відповідності законодавству, безпеки, точності, незалежності, прозорості, дотримання прав людини [7, с. 15].

Висновки. Таким чином, правильне відключення обладнання, недопущення втрати інформації, копіювання відеозаписів без зміни їх структури, документування технічних параметрів системи відеоспостереження, вилучення серверів, відеореєстраторів, жорстких дисків в подальшому сприяє успішності розслідування кримінальних правопорушень. Саме участь спеціаліста і дозволяє вирішити вищезазначені завдання. Вони інколи виступають ключовими учасниками кримінального провадження в частині технічного та аналітичного супроводу слідчих (розшукових) дій. В той же час інформація, яку повідомляє спеціаліст, сама по собі не є самостійним джерелом доказів. Тому виключно належне процесуальне оформлення консультацій чи пояснень, наданих спеціалістом і зафіксоване у відповідних процесуальних документах, надає їй юридичної значущості.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України від 13 квіт. 2012 р. No 4651-VI. URL : <http://zakon3.rada.gov.ua/laws/show/4651-17/print> (дата звернення: 02.08.2026).
2. Калганова О. А., Котух Є. В. Особливості залучення спеціаліста під час розслідування кримінальних правопорушень, учинених у кіберпросторі. *Ірпінський юридичний часопис*. 2023. Вип. 4(13). С. 141–147. DOI: 10.33244/2617-4154.4(13).2023.141-147.
3. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : монографія / [В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін.] ; за заг. ред. В. Ю. Шепітька ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 208 с.
4. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.
5. Матулене С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: український та європейський досвід. *Теорія та практика судової експертизи і криміналістики*. Вип. 4 (29). 2022. С. 37. URL: <https://khrife-journal.org/index.php/journal/issue/view/18/4-22>.
6. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Amsterdam ; Boston ; Heidelberg ; London ; New York ; Oxford ; Paris ; San Diego ; San Francisco ; Singapore ; Sydney ; Tokyo : Academic Press, 2011. 868 p.
7. Авдєєва Г. К. Цифрова інформація як доказ у кримінальному провадженні. *Актуальні питання теорії та практики в галузі права, освіти, соціально-гуманітарних та поведінкових наук в умовах воєнного стану* : матеріали міжнар. наук.-практ. конф. (м. Чернігів, 25–26 квітня 2023 р.) : у двох томах. Том 1 / голов. ред. В. Ф. Пузирний ; Академія Державної пенітенціарної служби. Чернігів : Академія ДПіТс, 2023. С. 15.

Дата першого надходження статті до видання: 07.05.2026

Дата прийняття статті до друку після рецензування: 29.05.2026

Дата публікації (оприлюднення) статті: 15.06.2026