УДК 343.132.1 doi: https://doi.org/10.33270/01201152.58

Черняховський Б. В. – ад'юнкт кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2 Національної академії внутрішніх справ, м. Київ
ORCID: https://orcid.org/0000-0002-7289-3034

Особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

Метою *дослідження є визначення особливостей проведення слідчого огляду під час досудового розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.* ***Методологія.*** *У статті застосовано емпіричні й теоретичні методи дослідження. Серед емпіричних – аналіз результатів опитування працівників оперативних підрозділів кіберполіції та судових експертів системи Міністерства внутрішніх справ, даних відкритої частини Єдиного державного реєстру судових рішень; з-поміж теоретичних – аналіз і синтез, аналогія, порівняння, узагальнення.* ***Наукова новизна.*** *Запропоновано прийоми виявлення, фіксації та вилучення нематеріальних цифрових (електронних) доказів. Обґрунтовано необхідність розроблення нормативних актів для систематизації методів проведення слідчого огляду доказових джерел у цифровій (електронній) формі.* ***Висновки.*** *1. Слідчий огляд інформації в цифровій (електронній) формі є основою системи доказування вчинення несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. 2. Застосування спеціальних знань під час слідчого огляду в досудовому розслідуванні комп'ютерних злочинів є обов'язковим. Залучення спеціаліста надає можливість мінімізувати й ліквідувати ризики втрати або знищення цифрових (електронних) доказів, забезпечує ефективну організацію дій учасників слідчого огляду. 3. Методика роботи слідчого з інформацією в цифровій (електронній) формі підлягає законодавчому врегулюванню. Закріплення базових алгоритмів організації роботи слідчої (слідчо-оперативної) групи під час проведення огляду забезпечує належний процесуальний контроль за дотриманням законності в досудовому розслідуванні й обумовлює системне вдосконалення методики розслідування кіберзлочинів.*

Ключові слова: слідчий огляд; огляд місця події; огляд комп'ютерного обладнання; огляд комп'ютерної мережі; огляд документів; огляд цифрових (електронних) доказів; комп'ютер; комп'ютерна мережа; несанкціоноване втручання в роботу комп'ютерів; комп'ютерний злочин.

Вступ

В умовах сьогодення роботу державних установ, організацій та підприємств організовують за допомогою комп'ютерів, комп'ютерних систем, комп'ютерних мереж і мереж електрозв'язку, унаслідок чого несанкціоноване втручання в їхню роботу є впливовим фактором для становлення України як сучасної, демократичної, правової держави. Саме кіберінциденти у сфері інформаційної інфраструктури позначаються на геополітичному іміджі держави, її економіці, обороні й безпеці.

Питання якості проведення в межах кримінального провадження слідчого огляду об'єктів сфери інформаційних технологій є важливим елементом стратегічних, тактичних й оперативних методів реагування держави на кіберзагрози, що зумовлює актуальність розроблення нових і вдосконалення наявних криміналістичних прийомів, методів, засобів розслідування, які відповідають умовам сьогодення.

Аспекти розслідування злочинів у сфері комп'ютерних технологій були і залишаються предметом дослідження знаних учених-криміналістів, зокрема: Т. В. Авер'янової, К. І. Бєлякова, П. Д. Біленчука, В. В. Бірюкова, В. Б. Вєхова, В. В. Крилова, В. О. Мєщєрякова, І. Ю. Михайлова, О. І. Мотляха, О. В. Орлова, О. Р. Росинської, М. В. Салтевського, В. Г. Хахановського, С. С. Чернявського та ін. Водночас потреби слідчих зумовлені стрімким розвитком сфери інформаційних технологій, засвідчують важливість системного імплементування в практичну діяльність наукових розробок щодо методології виявлення, огляду й збору доказів, зокрема в цифровій (електронній) формі дасть змогу сформувати стале емпіричне підґрунтя для їх закріплення в кримінальному процесуальному законодавстві України.

Мета і завдання дослідження

Метою статті є висвітлення організаційних, тактичних, криміналістичних методів і прийомів слідчого огляду в кримінальних провадженнях щодо несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

Досягнення мети дослідження передбачало такі завдання:

– здійснити криміналістичну характеристику слідчого огляду в умовах розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

– визначити сутність й особливості слідчого огляду нематеріальної складової доказової бази – роботи із цифровими (електронними) доказами;

– на підставі аналізу наявної практики сформулювати рекомендації щодо оптимізації та підвищення якості досліджуваної слідчої дії.

Виклад основного матеріалу

Розслідування злочинів у сфері використання інформаційних технологій потребує безперервного вдосконалення криміналістичних способів, методів і засобів для забезпечення швидкого, повного й неупередженого розслідування. Ефективність протидії несанкціонованому втручанню в роботу комп'ютерів, комп'ютерних систем і комп'ютерних мереж залежить від стану готовності слідчих до роботи з віртуальною інформацією в електронному (цифровому) середовищі, її виявлення та документування (фіксації), що становить сукупність факторів організаційно-правового характеру та потребує відповідного матеріально-технічного оснащення.

На підставі результатів порівняльного аналізу міжнародного досвіду використання цифрової (електронної) інформації в кримінальному судочинстві обґрунтовують доцільність, з огляду на прийняті в Україні нормативні акти, розширити поняття доказів, а також сформулювати дефініцію електронного доказу, критерії їх допустимості й достовірності (Akhtyrska, 2019, p. 221-224).

Згідно зі статистичними відомостями, упродовж останніх п'яти років в Україні внаслідок несанкціонованого втручання в роботу комп'ютерів, комп'ютерних мереж, мереж електрозв'язку постраждало понад 100 тисяч осіб. Крім того, об'єктами посягання були об'єкти критичної інфраструктури й низка інших об'єктів інформаційної інфраструктури. Відповідно до офіційних даних правоохоронних органів, 2019 року зареєстровано 1289 фактів з кваліфікацією за ст. 361 КК України, що на 185 фактів більше, ніж 2018 року ("Opryliudnennia publichnoi informatsii", 2020).

Тому для слідчих Національної поліції та органів безпеки як суб'єктів здійснення досудового розслідування у сфері національної кібербезпеки ("Ukaz Prezydenta", 2016) практичне значення мають криміналістичні розробки, пов'язані зі слідчим оглядом, адже для кримінального провадження вагоме значення має якість фіксації слідів злочинних посягань на роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, здійснених шляхом несанкціонованого втручання.

Якість слідчого огляду залежить від виконання таких завдань: вивчення обстановки на місці для з'ясування суті й обставин події, що дають підстави для здійснення досудового розслідування; отримання первинної інформації для висунення версій про механізм здійснення несанкціонованого втручання в електронну (цифрову) інформаційну систему, особу злочинця, наявність співучасників учинення злочину, дії кожного з них, час учинення злочину й інші обставини, які мають значення для розкриття та розслідування злочину; збір відомостей для організації розшуку злочинця за гарячими слідами, проведення оперативно-розшукових заходів (за його антропологічними ознаками, трасологічними слідами, характерними ознаками на підставі профайлу тощо) для його встановлення і затримання; встановлення слідів злочину, предметів, залишених злочинцем, та інших об'єктів, які можуть мати доказове значення; фіксація всього виявленого під час огляду, вилучення об'єктів, які можуть мати доказове значення для слідства; встановлення обставин, що сприяли вчиненню злочину.

Під час розслідування комп'ютерного злочину слідчий огляд проводять у місцях збереження й обробки комп'ютерної інформації, що зазнала злочинного впливу (знищення, перекручення, блокування чи шифрування), знаходження комп'ютерного обладнання, яке використовували під час учинення злочину (наприклад, у разі розповсюдження комп'ютерного вірусу після незаконного проникнення в комп'ютерну мережу), місцях збереження інформації, отриманої злочинним шляхом (у разі несанкціонованого заволодіння інформацією в електронній (цифровій) формі), місцях порушення правил експлуатації комп'ютерів, комп'ютерних систем або мереж, за місцем виявлення шкідливих наслідків (знищення, блокування, модифікації, копіювання інформації, порушення алгоритму роботи комп'ютерів, комп'ютерної системи або мережі) (Polyvaniuk, 2011, p. 243-248). Середовище вчинення комп'ютерного злочину умовно можна поділити на матеріальне (комп'ютерно-технічне устаткування, приміщення, у якому воно знаходиться) і нематеріальне інформаційне середовище в цифровій (електронній) формі.

Особливість огляду нематеріального (цифрового) середовища полягає в тому, що предметом цього злочину є інформація, яку зберігають в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації та передають через комп'ютерні мережі чи мережі електрозв'язку.

Криміналістична наука визначає, що саме збір даних й інформації відіграє вирішальну роль у розслідуванні комп'ютерних злочинів. Саме цифрові (електронні) докази підтримують

або спростовують теорію про те, як сталося правопорушення, указують на наявність елементів складу злочину, таких як умисел чи алібі. Такі докази здебільшого невидимі, залежні від часу, потребують дотримання умов допустимості (Parkavi, Divyam, & Sherry, 2020, p. 28).

Процес здійснення слідчого огляду умовно поділяють на три етапи: підготовчий, робочий та заключний.

Перший етап – підготовчий (організаційний) – розпочинається з моменту прийняття рішення про його проведення та підготовки до наступного (робочого) етапу.

До прибуття на місце проведення огляду для слідчого важливо вирішити такі організаційні питання: 1) забезпечення охорони місця події (об'єктів огляду) до прибуття слідчої (слідчо-оперативної) групи, недопущення сторонніх осіб, збереження цілісності обстановки та слідів кримінального правопорушення; 2) з'ясування характеристики можливого місця вчинення злочину (тип будівлі/приміщення, входи, виходи, наявність персоналу охорони, наявність і тип сигналізаційної системи, системи відеоспостереження); 3) з'ясування загальної характеристики потенційних об'єктів огляду (орієнтовна кількість і фактичне розташування комп'ютерів, серверів, комп'ютерних систем, інших пристроїв, тип програмного забезпечення, систем електрозв'язку, шляхи підведення електропостачання, комунікаційних і мережевих кабелів провайдера, тип підключення до глобальної мережі Інтернет, використання на об'єкті сервісів хмарних сховищ); 4) запобігання або ослаблення шкідливих наслідків кримінального правопорушення; 5) присутність на місці осіб, які можуть надати необхідну інформацію (власник приміщення/будови, керівник установи/організації, у якій планують проведення слідчої дії; особи, відповідальні за обслуговування комп'ютерного обладнання, інформаційну безпеку; інші працівники установи, які перебувають на місці, їх чисельність); 6) на підставі викладеної інформації визначити склад слідчої (слідчо-оперативної) групи, учасники якої забезпечать належний супровід і технічну підтримку огляду для слідчого, а саме: інспектор-криміналіст, оперативні працівники підрозділу боротьби з кіберзлочинністю, кількість яких визначають залежно від масштабів проведення огляду, інші спеціалісти, які забезпечать пошук, фіксацію, вилучення, опис й інтерпретацію слідів за допомогою спеціальних знань (згідно зі ст. 71 КПК України); працівники інших підрозділів (для забезпечення безпеки й недопущення сторонніх осіб до місця проведення огляду до його завершення, опитування осіб, які перебувають на місці злочину, надання іншої допомоги), а також особа, що забезпечить безперервну відеофіксацію процесу огляду; 7) перевірка готовності криміналістичної валізи для фіксації та вилучення матеріальних слідів злочину, а також криміналістичного технічного та програмного забезпечення спеціаліста, який супроводжує слідчий огляд (ноутбук зі спеціальним програмним забезпеченням (ліцензійним), криміналістичні завантажувальні диски, мобільні носії інформації, на які безпосередньо копіюватимуть дані (жорсткі диски, зовнішні пристрої з накопичувачами та для роботи з оптичними носіями інформації), інструменти для демонтажу обладнання (викрутки, кусачки, пінцет тощо), фото- та відеокамера для документування огляду із запасними акумуляторами й додатковими флеш-носіями, бирки для нумерації доказів, упаковки для транспортування вилучених об'єктів (антистатичні пакети, кабельна стяжка, коробки для DVD-дисків та інших вилучених об'єктів) (Hrebeniuk, 2017, p. 15); 8) якщо на комп'ютерних засобах, у комп'ютерній системі чи мережі, яка підлягає огляду, здійснюють обробку та зберігання інформації з обмеженим доступом, або ж використовують персональні дані осіб відповідно до Закону України «Про захист персональних даних» і така інформація, на думку слідчого, прокурора обґрунтовано може бути використана для встановлення обставин злочину та бути джерелом доказової інформації, необхідно зважати на стандарт допустимості доказів, згідно з яким порядок доступу до такої інформації в межах кримінального провадження регламентований положеннями ст. 159, 160 КПК України з подальшим винесенням ухвали суду про надання дозволу на тимчасовий доступ до такої інформації з метою її огляду та, за необхідності копіювання (така обставина типова для проведення слідчого огляду комп'ютерів і комп'ютерних мереж у юридичних осіб, відомств, установ виконавчої влади, кредитних і банківських установ, а також з надання послуг електрозв'язку, приватної охоронної тощо).

Слідчий як процесуальна особа зобов'язаний встановити й документально зафіксувати підстави та законність проведення процесуальної дії – слідчого огляду. Із цього приводу Верховний Суд на офіційному вебсайті надав роз'яснення від 3 січня 2019 року з посиланням на постанову Верховного Суду України, ухвалену колегією суддів Другої судової палати Касаційного кримінального суду 8 листопада 2018 року у справі № 536/1048/16-к, провадження № 51-4088км18, у якому зазначено, що законодавець, окрім можливості проникнення до житла чи іншого володіння особи на підставі судового рішення, передбачив іншу процесуальну гарантію захисту прав особи, а саме −

можливість проникнути до житла чи іншого володіння особи за добровільною згодою особи, яка ним володіє ("Ohliad zhytla", 2020).

Підготовчий етап завершується після прибуття на місце події та виконання таких дій: фіксація часу прибуття на місце проведення огляду, час початку слідчої дії; під час проведення огляду у власності заявника/потерпілого, отримання в присутності понятих добровільної письмової згоди на огляд місцевості, приміщення та іншого майна; встановлення місць зовнішнього підключення до будівлі електропостачання, комунікаційних і мережевих кабелів, організація їх охорони на час проведення огляду; збір попередніх відомостей (опитування) від осіб, які перебувають на місці події, для врахування обставин, що можуть мати значення для проведення огляду, встановлення змін на місці події, осіб, які їх учинили, і з якою метою; усунення з місця події всіх сторонніх осіб; пошук та залучення понятих (не менше ніж дві особи) з розрахунку кількості приміщень, у яких розташовані окремі елементи комп'ютерної системи (важливою є обізнаність понятих у комп'ютерній техніці та процесах роботи з електронною (цифровою інформацією), щонайменше – на рівні впевнених користувачів, для забезпечення факту усвідомлення та підтвердження останніми суті дій учасників слідчої групи); остаточне визначення кола інших учасників огляду (коригування складу слідчої групи); інструктаж учасників огляду, повідомлення та за потреби роз'яснення їхніх прав та обов'язків; проведення інших невідкладних дій і вжиття заходів, спрямованих на покращення умов огляду (забезпечення штучного освітлення, наявність автономних пристроїв живлення для технічних засобів тощо) (Antoshchuk et al., 2016).

На початковому етапі організовують інші пошукові заходи, а також вирішують питання щодо витребування необхідної інформації від провайдерів, інших установ, що обслуговують об'єкт, і визначають доцільність застосування службово-розшукового собаки (залежно від способу здійснення доступу до комп'ютерних пристроїв).

Робочий етап полягає в безпосередньому проведенні огляду, який з метою охоплення всіх можливих слідчих версій вчинення злочину передбачає огляд місцевості, приміщень, предметів (комп'ютерної техніки) і документів, зокрема електронних.

Передусім проводять загальний огляд місця події, який полягає у визначенні територіальних меж місця проведення огляду, складанні плану-схеми (розташування об'єктів огляду, мережевих з'єднань комп'ютерів, серверів між собою, із засобами й каналами електрозв'язку, іншим периферійним обладнанням), встановленні вихідної точки та способу огляду (його послідовності), визначенні точок орієнтирів і виборі позиції для орієнтуючої та оглядової фото- й відеозйомки (Polyvaniuk, 2011, p. 243-248).

Наступним кроком є статична фіксація технічних (комп'ютерних) пристроїв та інших матеріальних об'єктів, наявних мережевих підключень (спосіб підключення: за допомогою технологій Wi-Fi чи кабелю), кількість роз'ємів підключення в кожного пристрою, їх види, схема взаємного розташування пристроїв, порядок з'єднань у мережі, вид використовуваних кабелів, їх кількість, зовнішній вигляд пристроїв (номер, модель, форма, колір), стан (увімкнений/вимкнений) на момент проведення огляду. Усі ці дії супроводжують криміналістичною фото- та відеозйомкою, складають план приміщення та схему розташування комп'ютерного обладнання, локальних мереж, інших точок підключення до системи, локальної мережі чи мережі Інтернет. Також важливо унеможливити фізичний доступ до комп'ютерної техніки осіб, які з нею працюють, урахувати й ужити спеціальних заходів для блокування спроб здійснення віддаленого доступу до такої техніки. Зазначені дії рекомендовано попередньо узгодити зі спеціалістом до початку проведення огляду для оперативної координації дій учасників слідчої групи.

Після завершення процедури загального огляду слідчий переходить до динамічної стадії – детального огляду. Динаміка зумовлена тим, що предмети, визначені як окремі об'єкти огляду, можуть зрушуватися з місця. Об'єкти огляду за вказівкою слідчого детально опрацьовує спеціаліст-криміналіст на предмет слідів пальців рук, нігтів, слідів фізичного контакту з іншими твердими поверхнями, зокрема тими, якими спричинено механічні пошкодження, для їх фіксації та вилучення. Цей підхід є типовим для фіксації слідів злочину (відомий для слідчих), однак слід ураховувати можливість виявлення відшарування чи нашарування речовин, порошків, фарби, інших мікроелементів на поверхнях комп'ютерного устаткування, зокрема біологічних слідів ДНК-профілю чи одорологічних слідів.

Під час розгляду версії несанкціонованого втручання шляхом фізичного підключення до комп'ютерного устаткування чи комп'ютерної мережі доцільно зосереджувати увагу на наявності нашарувань пилу на поверхнях, що можуть свідчити про пересування чи зрушення з місця окремих пристроїв. Крім того, слід оглянути внутрішній вміст комп'ютерного устаткування, який не є легкодоступним, його переважно не перевіряє безпосередній користувач (співробітник). Встановлюють наявність змін у конструкції комп'ютерного

устаткування (не передбачене для роботи обладнання, сторонні пристрої розширення пам'яті, замінені або ж видалені мікросхеми), інші комплектуючі (Starushkevych, 2003, p. 77-78). Доцільно за участю працівника оперативно-технічного забезпечення оглянути точки мережевого підключення та електропостачання на предмет втиснення, перевірити стан кабелів щодо можливих слідів припаювання, надрізання ізоляційного покриття тощо. Для огляду дрібних предметів рекомендують використовувати пінцет, якщо ж ідеться про габаритні предмети – спеціаліст повинен працювати в рукавичках. Після вилучення дрібних предметів для судового експертного дослідження їх поміщують в окремий поліетиленовий пакет, який герметично закривають й опечатують з відповідною биркою.

Важливим елементом слідчого огляду на підприємствах, в організаціях, установах є огляд паперових документів – журналів обліку роботи з комп'ютерним устаткуванням (якщо такі ведуть), лістингів (роздруківок текстів комп'ютерних програм), технічної, технологічної та іншої документації. Увагу слід акцентувати на наявності підчищень, виправлень, додаткових записів, порядку нумерації сторінок, вкладень, розпоряджень на виконання певних програмно-технічних робіт з комп'ютерним устаткуванням чи заміні програмного забезпечення, введенні додаткової інформації, не передбаченої технологічним процесом, відповідності форм запису такої інформації встановленим правилам тощо (Eminov, & Ishenko, 2015, p. 208).

Під час пошуку та фіксації слідів злочинця сліди пальців рук доцільно шукати також на поверхнях жорстких дисків, оптичних дисків, флеш-карт, паперових документів, які створено за допомогою оглядуваного пристрою та знаходяться поряд з ним. Однак під час пошуку дактилоскопічних слідів на поверхнях комп'ютерного обладнання важливо не обробляти пристрої (технічні складові) магнітними порошками, оскільки використання їх і магнітних пензлів може пошкодити електронні складові та знищити ті сліди, які доцільно й ефективніше було б виявляти в лабораторних умовах (Amelin, & Sokolova, 2017, p. 66). Як альтернативу в таких випадках для зняття слідів пальців рук використовують хімічні засоби, які не мають магнітовмісних сполук (сажа, порошок оксиду цинку тощо). Під час пошуку інших слідів фізичного походження необхідно узгоджувати зі спеціалістом застосування магнітних шукачів, ультрафіолетових освітлювачів та інших пристроїв аналогічного принципу дії для запобігання ризикам негативного впливу на носії інформації, мікросхеми пам'яті тощо.

Під час документування несанкціонованого втручання на об'єкти інформаційної інфраструктури або підприємства, установи, які використовують у своїй діяльності інформацію з обмеженим доступом чи персональні дані осіб, додатково слід урахувати таке. Для повноцінного об'єктивного огляду, який надасть можливість сформулювати всі можливі слідчі версії злочину, необхідно встановити, які способи протидії витоку та несанкціонованому доступу до інформації застосував власник чи керівник підприємства/установи, зокрема: спосіб екранізації (екранізація комп'ютерної та електричної техніки чи приміщення, у якому вона знаходиться); особливості перемонтування окремих ланок, ліній, кабелів; використання прихованих спеціальних пристроїв пасивного й активного захисту інформації; наявність спеціальної системи заземлення для технічних засобів передання інформації та мережевих фільтрів тощо.

За результатами огляду й аналізу матеріальної складової місця злочину слід концентруватися на роботі з інформацією в електронній формі. Участь спеціаліста у сфері комп'ютерних технологій за відповідним напрямом є одним із ключових моментів, який необхідно врахувати й забезпечити під час огляду комп'ютерів, що забезпечують функціонування інформаційної системи. Адже з програмно-технічної позиції елементи, які належать до складу комп'ютерної системи, під час дослідження на місці потребують максимально обережного поводження, з огляду на такі фактори, як великий масив інформації в електронній формі, наявність права інтелектуальної власності на окрему частину інформації, яку оглядають, наявність прихованих даних, доступ до якої базовий користувач комп'ютера не спроможний отримати й, що найсуттєвіше, ризики втрати інформації через необережні дії та можливий запрограмований автоматичний запуск алгоритму її знищення. Здійснений нами аналіз слідчої практики засвідчує, що непоодинокими є випадки інсталяції причетними до вчинення злочину особами програмних засобів, налаштованих на деінсталяцію (видалення) з електронного журналу дій інформації про виконання певних команд, мережевих з'єднань, видалення конкретної інформації (файлів) або ж форматування чи пошкодження пристрою збереження інформації.

Деякі вчені розділяють учасників слідчої/-слідчо-оперативної групи на дві категорії: обов'язкові учасники й факультативні, а спеціалістів, які є фахівцями в збиранні специфічних слідів злочинів аналізованої категорії, відносять до другої (факультативної) групи (Polyvaniuk, 2011, p. 243-248).

Ми категорично не поділяємо таке твердження, оскільки віднесення спеціаліста у сфері інформаційних технологій до категорії необов'язкового (факультативного) учасника цієї слідчої дії формалізації позиції слідчого щодо необхідності залучення спеціаліста, він допускає можливість залучення до огляду, роботи з інформаційними технологіями особи (з навичками звичайного користувача), яка не може цілком обґрунтувати способи виконання певних дій/маніпуляцій з комп'ютерною технікою, підтвердити їхню доцільність і правильність, що своєю чергою не відповідає стандарту належності зібраних доказів у кримінальному провадженні.

Такий підхід схвалюють представники наукового кола криміналістів Сполучених Штатів Америки, які виокремлюють напрям цифрової криміналістики як нової науки, що набуває дедалі важливішого значення з огляду на збільшення кількості фактів використання злочинним елементом комп'ютерів і комп'ютерних мереж у протиправній діяльності. На думку відомого в США науковця Джона Філіпа Крейгера, компетентність у сфері цифрової криміналістики потребує ґрунтовного набору знань і навичок, що передбачають глибоке розуміння комп'ютерного обладнання, програмного забезпечення, комп'ютерних мереж, криміналістики, а також національних законів, які регламентують процедуру доказування (Craiger, 2007). Представник наукової спільноти у сфері цифрової криміналістики Йоган Кейсі зазначає про посилення залежності від цифрових доказів у всіх видах юридичних справ, тому ризики неправильного поводження, неправильного тлумачення призводять до нерозуміння специфіки та правових маніпуляцій у суді. Вагому роль у цьому відіграють практична готовність і наукова обізнаність фахівця. Непрофесійне поводження із цифровими доказами може призвести не лише до відповідальності особи, яка з ними працює, а й до ускладнення встановлення достовірності та цілісності даних, достовірності результатів судової оцінки зібраних відомостей. Значущою є інтерпретації інформації в цифровій формі та застосованого способу її отримання (Casey, 2019).

З огляду на зазначене, під час проведення слідчого огляду за фактом несанкціонованого втручання для виявлення, фіксації та збереження доказів в електронній (цифровій) формі участь спеціаліста є обов'язковою.

Специфіка злочину, передбаченого ст. 361 КК України, визначає, що для реалізації завдань кримінального провадження лише речових доказів недостатньо, тому важливою є процесуально грамотна й технічно правильна фіксація інформації в комп'ютерах, комп'ютерних мережах і системах.

Також вважаємо за доцільне дотримання слідчим принципу Міжнародного кримінального суду – «правила найкращого доказу» (best evidence rule). Його суть полягає в наданні привілейованого статусу саме оригіналу документа, порівняно з його копією чи відображенням ("Posibnyk zi zboru dokaziv", 2019). Дотримання такого принципу залежить від використання спеціальних знань під час збирання доказів в електронній (цифровій) формі, якими володіє спеціаліст. Ця умова убезпечить від ненавмисного видалення чи пошкодження електронних (цифрових) файлів, а також уникнення випадків запрограмованого самознищення електронних (цифрових) файлів у разі введення неправильного пароля.

Зазначені рекомендації не є вичерпними, однак, на наш погляд, достатньо обґрунтовують обов'язковий характер залучення спеціаліста з відповідними фаховими знаннями, що забезпечить повноцінний, комплексний пошук електронних (цифрових) доказів (анг. digital evidences) і належне збереження доказової інформації.

Наступний крок робочого етапу огляду полягає у фіксації так званих внутрішніх слідів злочину, тобто слідів, залишених в електронній формі, які може бути виявлено, оглянуто та зафіксовано за допомогою відповідного програмного забезпечення на комп'ютерному носії.

Змістовним, на наш погляд, є визначення Т. Е. Кукарнікової (Kukarnikova, 2003), яка вважає, що слід комп'ютерного злочину – це будь-яка зміна середовища (файлової системи), пов'язана з подією злочину. Оскільки файлова система є сукупністю особливих інформаційних одиниць-файлів, спеціальних службових таблиць (каталогів, таблиць розділів, завантажувальних записів, таблиць розміщення файлів) і кластерів, ці зміни можуть полягати в зміні місця розташування та вмісту файлів; зміні формату або характеристик файлів; створенні чи вилученні файлів; зміні вмісту спеціальних службових таблиць, стану кластерів. Дія одного інформаційного об'єкта на інший може бути виявлена між двома відомими станами інформаційного об'єкта – за ознаками зміни змісту формату файлових характеристик і за зміною алгоритму роботи програми (p. 16).

Слушним видається твердження, що участь спеціаліста на цьому етапі огляду є ключовою та обов'язковою. Саме взаємодія слідчого, прокурора зі спеціалістом, повноваження та спеціалізація якого процесуально підтверджені, забезпечує правову платформу для принципів належності й допустимості всіх виявлених і

зафіксованих електронних (цифрових) доказів у кримінальному провадженні.

Отже, увагу слідчого, прокурора та спеціаліста слід зосередити на таких слідах злочину, як: інформація, що зберігається на комп'ютерних носіях (зміни у файловій системі; шкідливі програмні засоби, небезпечні файлові програми); програми-файли з прямими посиланнями на веб-сторінки в мережі Інтернет; програми, які автономно здійснюють копіювання, блокування, модифікацію чи знищення інформації; файлове програмне забезпечення для підбору паролів доступу тощо.

У контексті документування несанкціонованого втручання в комп'ютери, автоматизовані системи та комп'ютерні мережі спеціаліст виконує такі завдання:

– діагностування апаратних засобів (комп'ютери, ноутбуки, планшети, жорсткі диски, флеш-накопичувачі, картки пам'яті, мобільні пристрої тощо);

– визначення функціонального призначення, характеристик, алгоритму роботи й структурних особливостей, стану виявленого програмного, системного та прикладного забезпечення;

– пошук, виявлення, аналіз та оцінювання цифрових даних, виготовлених користувачем або створених прикладними програмами для організації інформаційних процесів у комп'ютерній системі;

– ідентифікація електронних (цифрових) файлів/каталогів, їх ототожнення з файлами/каталогами на інших носіях інформації (Teplytskyi, Sharai, Kovalov, & Kuzmin, 2019).

Постійний розвиток й удосконалення електронних, інформаційних систем сприяє розширенню кола окреслених завдань, тому в кожному конкретному випадку їх слід визначати індивідуально. Реалізація завдань слідчого огляду є лише попереднім етапом у документуванні цього злочину, оскільки належним підтвердженням результатів фіксації даних, що можуть слугувати доказом у судовому провадженні, є висновок експерта. Тому для слідчого важливо, щоб поставлені перед спеціалістом завдання під час проведення огляду відповідали методиці й вимогам, на яких ґрунтуються питання для судових експертних досліджень комп'ютерної техніки та програмних продуктів чи досліджень телекомунікаційних систем і засобів.

З позицій криміналістичної тактики увагу слідчого необхідно зосередити на огляді та, за необхідності, вилученні комп'ютерного обладнання, периферійних мобільних пристроїв, якими безпосередньо користуються особи, щодо яких є достатні підстави вважати їх причетними до вчинення кримінального правопорушення. У випадках використання останніми систем «віддаленого доступу» увагу слід акцентувати саме роботі із сервером.

Під час огляду локальних комп'ютерів, комп'ютерної мережі та її віддалених ресурсів рекомендовано дотримуватися такого алгоритму дій: 1) зафіксувати інформацію, яка відображається на моніторі (відкриті файли, програми, процеси, завантаження, мережеві з'єднання та їх активність), зберегти її; 2) перевірити налаштування BIOS і завантажити операційну систему з робочого примірника (флеш-накопичувача чи з оптичного диска, заздалегідь підготовленого спеціалістом); 3) приєднати зовнішній носій інформації (жорсткий диск/флеш-накопичувач), на який здійснюватимуть копіювання криміналістично значущої інформації для досудового розслідування, – контрольний носій; 4) запустити програму запису зображення екрана монітора для додаткової фіксації процесу огляду (зокрема під час перегляду відеофайлів), після чого створені в процесі огляду відеограму та зафіксовані зображення екрана монітора після завершення огляду зберегти на приєднаний зовнішній носій в окремому каталозі; 5) вивести на екран монітора інформацію про апаратне та програмне забезпечення комп'ютера, які його ідентифікують, зафіксувати її в протоколі огляду та зберегти на зовнішньому носії інформації в окремому файлі; 6) вивести на екран монітора налаштування мережевого адаптера, зафіксувати, як і в попередньому випадку; 7) створити файл-образ (еталон) для перевірки правильності підрахунку контрольних сум за допомогою призначеної для цього програми, перевірити та продемонструвати учасникам слідчої дії результати, після чого зберегти файл-еталон та файл із його контрольною сумою на носієві, призначений для запису й зберігання доказової інформації (Hrebeniuk et al., 2017); 8) провести детальний огляд інформації, що збережена на комп'ютері. Слід акцентувати увагу учасників огляду (понятих) на змісті, місці розміщення виявленої та значущої для слідства інформації; 9) запустити браузер і ввести ідентифікаційні дані (доменне ім'я, паролі за їх наявності) віддаленого ресурсу, провести огляд зовнішнього інформаційного ресурсу (сайту), його наповнення. Важливо продемонструвати учасникам слідчої дії (понятим) зміст і місце розміщення файлів на віддаленому ресурсі, які можуть мати значення для кримінального провадження; 10) за допомогою криміналістичного програмного забезпечення установити IP-адресу (ping) сайту, шляхи проходження в процесі обміну інформацією між сайтом і відповідним комп'ютером (для встановлення провайдера скористатися відповідним веб-ресурсом, що ідентифікує приналежність

IP-адреси); 11) для кваліфікованого збереження (вилучення) виявленої інформації здійснювати побітове копіювання на під'єднаний спеціалістом зовнішній носій зберігання інформації, демонструючи ці дії понятим; 12) використовуючи криміналістичне програмне забезпечення, вивести на екран монітора інформацію про контрольну суму кожного файлу, значущого для слідства, що зафіксований на зовнішньому носії, зберегти її у відповідному окремому файлі; 13) після копіювання всієї виявленої, значущої для кримінального провадження інформації підключити другий відформатований зовнішній носій зберігання інформації та скопіювати на нього всю інформацію з контрольного носія; 14) відключити контрольний та робочий носії із зібраною (збереженою) інформацією, вилучити диск з робочим примірником криміналістичного програмного забезпечення, здійснити пакування контрольного примірника носія з доказовою інформацією в спосіб, який унеможливить доступ до нього, опечатати й засвідчити на бирці з печаткою та підписами учасників слідчої дії, понятих; 15) зафіксувати порядок і зміст зазначених вище дій у протоколі огляду, обов'язково зазначивши контрольну суму інформації, зауваження, клопотання і доповнення від учасників слідчої дії.

За результатами проведення огляду комп'ютера, комп'ютерної мережі, віддаленого інформаційного ресурсу до протоколу огляду долучають: робочі та контрольні примірники криміналістичних програмних засобів, застосовані для виявлення, копіювання та збереження інформації на інший носій; контрольний примірник файлу – еталону; контрольний примірник носія зі збереженими файлами, інформацією, що мають доказове значення; за наявності фізичних слідів втручання чи стороннього застосування комп'ютерного обладнання, що потребують судово-експертного дослідження, носій, що був об'єктом огляду.

Заключний етап проведення слідчого огляду визначає успішність проведення слідчого огляду, що потребує урахування вимог, дотримання яких забезпечить належне судове експертне дослідження вилучених об'єктів у межах комп'ютерно-технічної експертизи чи експертизи програмного забезпечення. Слід ураховувати необхідність коректного завершення усіх програмних засобів, які працюють, що убезпечить від потенційної можливості втрати важливої інформації (доказів) чи її псування.

За рекомендаціями фахівців Державного науково-дослідного експертно-криміналістичного центру МВС України (Teplytskyi, Sharai, Kovalov, & Kuzmin, 2019), під час проведення слідчого огляду після вилучення комп'ютерної техніки та пристроїв інформаційно-телекомунікаційного зв'язку, складових мереж електрозв'язку категорично заборонено їх умикати й проводити на них будь-які операції (завантажувати операційну систему, створювати, видаляти файли тощо). Слід ураховувати, що вилучені об'єкти є потенційним джерелом доказів, а будь-які непрофесійні дії з ними згодом можуть бути підставою для визнання доказів недопустимими. Крім цього, такі дії можуть призвести до фактичного видалення або зміни доказової чи важливої оперативної інформації.

Аналіз слідчої практики засвідчує, що фахівці у сфері інформаційних технологій часто за завданням власника техніки інсталюють на комп'ютерні та мобільні пристрої спеціальні програмні продукти, які забезпечують автоматичне знищення інформації, що на них міститься, за умов неавторизованого чи неідентифікованого доступу. Будь-які некваліфіковані дії, маніпуляції із вилученою технікою, програмним забезпеченням без участі відповідного фахівця є недопустимими.

Упакуванню підлягають усі вилучені об'єкти огляду. Їх слід упаковувати окремо, що надасть можливість надалі повторно проаналізувати отриману під час огляду інформацію та визначити порядок призначення і проведення судово-експертних досліджень, додаткових слідчого огляду, обшуку чи слідчого експерименту без необхідності переупакування окремих елементів, які потрібно використати для окремих слідчих дій. Спосіб упакування має гарантувати неможливість будь-яких змін об'єктів дослідження або їх складових (вмісту), носіїв з об'єктами дослідження, уберігати їх від пошкоджень, погіршення властивостей унаслідок стороннього впливу. У разі пакування об'єктів у картонні короби місця з'єднання їх сторін необхідно обклеювати клейкою стрічкою з проставленням печатки (передусім – у місцях згину клейкої стрічки). Пакування вилучених речей до пакетів передбачає дотримання правил криміналістичного забезпечення проведення огляду: обв'язування шовковою (капроновою) ниткою, фіксація двома подвійними простими вузлами на протилежних сторонах тощо. Кожну окрему упаковку з вилученими речовими доказами опечатують биркою, зазначаючи назву та характеристики предмета (номер, марку, серію, тип), номер кримінального провадження, фабулу події, прізвище особи, у якої вилучено предмет, місце (адресу), дату й час вилучення, посаду, П.І.Б., особистий підпис слідчого, спеціаліста та понятих, присутніх під час вилучення і пакування. Обов'язковим є скріплення бирки печаткою. Важливо, що застосування стрейч-плівок і клейких стрічок для

закріплення паперових бирок є недопустимими (Teplytskyi, Sharai, Kovalov, & Kuzmin, 2019).

Для запобігання маніпуляціям захисників у судовому засіданні, висунення останніми оцінних суджень тощо, під час складання (заповнення) протоколу огляду рекомендовано не вживати «сленгову риторику». Крім того, під час вилучення комп'ютерного устаткування в протоколі огляду слід окремо фіксувати конфігурації підключень кабелів до USB-портів й інших елементів з'єднань, під'єднаних периферійних пристроїв, детально описуючи їх (назва, модель і серійний та інвентарний номери кожного окремого пристрою). Такий підхід спрощує подальші процесуальні дії з вилученою технікою та забезпечує об'єктивність і повноту в наданні судових експертних висновків.

Наукова новизна

Наукова новизна дослідження зумовлена результатами аналізу проблематики й особливостей проведення слідчого огляду в межах досудового розслідування за ст. 361 КК України, що охоплює безпосередній огляд комп'ютерів, комп'ютерного та мережевого устаткування, інформації в цифровій (електронній) формі, яка в них зберігається, обробляється та має доказове значення для кримінального провадження. Визначено особливості кожного етапу проведення слідчого огляду залежно від специфіки слідової картини комп'ютерного злочину. Виокремлено питання взаємодії слідчого зі спеціалістом під час огляду, спрямованого на пошук, дослідження та вилучення (збереження) цифрових (електронних) доказів. Аргументовано обов'язковість залучення спеціаліста у сфері інформаційних (комп'ютерних) технологій для проведення слідчого огляду. Задля ілюстрації такої позиції розглянуто базові особливості взаємодії учасників слідчої (слідчо-оперативної) групи на кожному етапі проведення слідчого огляду, що забезпечують дотримання вимог належності й допустимості доказів у кримінальному провадженні щодо комп'ютерного злочину.

Висновки

Проведення слідчого огляду під час розслідування фактів несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку потребує належної нормативної і технічної готовності слідчих до роботи з інформацією в електронній (цифровій) формі. Важливо, щоб нормативно-правове забезпечення діяльності правоохоронних органів відповідало умовам сьогодення, зокрема в частині науково-дослідної роботи й розроблення відомчих (розпорядчих) актів, інструкцій методичного характеру, які регламентують проведення різних видів слідчого огляду в межах розслідування комп'ютерних злочинів.

REFERENCES

Akhtyrska, N.M. (2019). Mizhnarodnyi dosvid vykorystannia tsyfrovoi informatsii u kryminalnomu sudochynstvi [International experience in the use of digital information in criminal proceedings]. *Yurydychnyi naukovyi elektronnyi zhurnal, Legal scientific electronic journal, 4,* 221-224. doi: https://doi.org/10.32782/2524-0374/2019-4/59 [in Ukrainian].

Amelin, O.V., & Sokolova, Ya.A. (2017). *Rekomendatsii shchodo osoblyvostei dosudovoho rozsliduvannia ta protsesualnoho kerivnytstva u kryminalnykh provadzhenniakh pro zlochyny, vchyneni z vykorystanniam elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku [Recommendations on the peculiarities of pre-trial investigation and procedural guidance in criminal proceedings on crimes committed with the use of electronic computers (computers), systems and computer networks and telecommunication networks]: rishennia nauk.-metod. rady NAPU vid 20 kvit. 2017 r. protokol No. 3).* Kyiv: NAPU [in Ukrainian].

Antoshchuk, A.O., Atamanchuk, V.M., & Komarynska, Yu.B. (et al.). (2016). *Osoblyvosti rozsliduvannia okremykh vydiv zlochyniv [Features of the investigation of certain types of crimes].* Kyiv: NAVS. Retrieved from https://arm.naiau.kiev.ua/books/orovz/lections/lection8.html [in Ukrainian].

Casey, E. (2019). Trust in digital evidence. *Forensic Science Internationanl: Digital investigation, 31.* doi: https://doi.org/10.1016/j.fsidi.2019.200898.

Craiger, P. (2007). Training and Education in Digital Evidence. *Handbook of Digital and Multimedia Forensic Evidence.* J.J. Barbara (Eds.). Humana Press Inc., Totowa. doi: https://doi.org/10.1007/978-1-59745-577-0_2.

Eminov, V.E., & Ishenko, E.P. (2015). *Sledstvennye deystviia - osnova raskrytiia prestupleniy: psikhologo-kriminalisticheskiy analiz [Investigative actions - the basis of crime detection: psychological and forensic analysis].* Moscow: Norma; Infra-M [in Russian].

Hrebeniuk, M.V., Havlovskyi, V.D., & Hutsaliuk, M.V. (et al.). (2017). *Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh [The use of electronic (digital) evidence in criminal proceedings].* M.V. Hrebeniuk (Eds). Kyiv: MNDTs pry RNBO Ukrainy [in Ukrainian].

Kukarnikova, T.E. (2003). Elektronnyy dokument v ugolovnom protsesse i kriminalistike [Electronic document in criminal proceedings and forensics]. *Extended abstract of candidate's thesis.* Voronezn [in Russian].

Ohliad zhytla chy inshoho volodinnia osoby mozhe buty provedeno za dobrovilnoiu zhodoiu osoby, yaka nym volodiie, za umovy naiavnosti protsesualnykh harantii zakhystu [An inspection of a person's home or other property may be conducted with the voluntary consent of the person who owns it, provided that there are procedural guarantees of protection]. (2019). *Sait "Verkhovnyi Sud", Site "Supreme Court".* Retrieved from https://supreme.court.gov.ua/supreme/pres-centr/news/615161 [in Ukrainian].

Opryliudnennia publichnoi informatsii [Disclosure of public information]. *Sait "Natsionalna politsiia", Site "National Police".* (2020). Retrieved from https://www.npu.gov.ua/activity/zviti/oprilyudnennya-publichnoji-informacziji.html [in Ukrainian].

Parkavi, R., Divyam, K., & Sherry, R.V. (2020). Digital Crime Evidence. *Critical Concepts, Standards, and Techniques in Cyber Forensics, IGI Global.* Thiagarajar College of Engineering India. doi: https://doi.org/10.4018/978-1-7998-1558-7.ch008.

Polyvaniuk, V. D. (2011). Taktychni osoblyvosti provedennia ohliadu mistsia podii pry rozsliduvanni zlochyniv, vchynenykh u bankivskii systemi Ukrainy z vykorystanniam suchasnykh informatsiinykh tekhnolohii [Tactical features of the location review on the detection of criminals, participation in the Ukrainian authorities of Ukraine with modern information technology]. *Visnyk Zaporizkoho natsionalnoho universytetu, Bulletin of Zaporizhia National University, 1,* 243-248 [in Ukrainian].

Posibnyk zi zboru dokaziv dlia Mizhnarodnoho kryminalnoho sudu [Evidence Collection Guide for the International Criminal Court]. (2019). Kyiv: M-vo z pytan tymchasovo okupovanykh terytorii ta vnutrishno peremishchenykh osib Ukrainy [in Ukrainian].

Starushkevych, A. (2003). Orhanizatsiia ohliadu mistsia podii. Analiz kryminalistychno-znachymoi informatsii pry rozsliduvanni zlochyniv u sferi kompiuternoi informatsii [Organization of site inspection. Analysis of forensically significant information in the investigation of crimes in the field of computer information]. *Visnyk prokuratury, Bulletin of the Prosecutor's Office, 12,* 77-78 [in Ukrainian].

Teplytskyi, B.B., Sharai, L.H., Kovalov, K.M., & Kuzmin, S.A. (2019). *Zlochyny u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku: spetsialni pytannia kvalifikatsii, provedennia slidchykh (rozshukovykh) dii, pryznachennia kompiuterno-tekhnichnykh sudovykh ekspertyz [Crimes in the field of use of electronic computers (computers), systems and computer networks and telecommunication networks: special issues of qualification, conducting investigative (search) actions, appointment of computer-technical forensic examinations].* Kyiv: Palyvoda A.V. [in Ukrainian].

Ukaz Prezydenta Ukrainy "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy": vid 15 berez. 2016 r. No. 96/2016 [Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine" from March 15, 2016, No. 96/2016]. *Uriadovyi kurier, Government courier, 52* [in Ukrainian].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Ахтирська Н. М. Міжнародний досвід використання цифрової інформації у кримінальному судочинстві. *Юридичний науковий електронний журнал.* 2019. № 4. С. 221–224. doi: https://doi.org/10.32782/2524-0374/2019-4/59.

Амелін О. В., Соколова Я. А. Рекомендації щодо особливостей досудового розслідування та процесуального керівництва у кримінальних провадженнях про злочини, вчинені з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : рішення наук.-метод. ради НАПУ (від 20 квіт. 2017 р. протокол № 3). Київ: НАПУ, 2017. 66 с.

Особливості розслідування окремих видів злочинів : мультимед. навч. посіб. / [А. О. Антощук, В. М. Атаманчук, Ю. Б. Комаринська та ін.]. Київ : НАВС, 2016. URL: https://arm.naiau.kiev.ua/books/orovz/lections/lection8.html.

Casey E. Trust in digital evidence. *Forensic Science Internationanl: Digital investigation.* 2019. No. 31. doi: https://doi.org/10.1016/j.fsidi.2019.200898.

Craiger P. Training and Education in Digital Evidence. *Handbook of Digital and Multimedia Forensic Evidence* / Edited by: J. J. Barbara. Humana Press Inc., Totowa, 2007. doi: https://doi.org/10.1007/978-1-59745-577-0_2.

Еминов В. Е., Ішенко Е. П. Следственные действия – основа раскрытия преступлений: психолого-криминалистический анализ : практ. пособие. М. : Норма ; Инфра-М, 2015. 208 с.

Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М. В. Гребенюк, В. Д. Гавловський М. В. Гуцалюк та ін.] ; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 76 с.

Кукарникова Т. Э. Электронный документ в уголовном процессе и криминалистике : автореф. дис. ... канд. юрид. наук : 12.00.09. Воронеж, 2003. 28 с.

Огляд житла чи іншого володіння особи може бути проведено за добровільною згодою особи, яка ним володіє, за умови наявності процесуальних гарантій захисту. *Верховний Суд :* [офіц. сайт]. 2019. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/615161.

Оприлюднення публічної інформації. *Національна поліція :* [офіц. сайт]. 2020. URL: https://www.npu.gov.ua/activity/zviti/oprilyudnennya-publichnoji-informacziji.html.

Parkavi R., Divya K., Sherry R. V. Digital Crime Evidence. *Critical Concepts, Standards, and Techniques in Cyber Forensics, IGI Global.* Thiagarajar College of Engineering India, 2020. 28 p. doi: https://doi.org/10.4018/978-1-7998-1558-7.ch008.

Поливанюк В. Д. Тактичні особливості проведення огляду місця події при розслідуванні злочинів, вчинених у банківській системі України з використанням сучасних інформаційних технологій. *Вісник Запорізького національного університету.* 2011. № 1. С. 243–248.

Посібник зі збору доказів для Міжнародного кримінального суду. Київ : М-во з питань тимчасово окупованих територій та внутрішньо переміщених осіб України, 2019. 43 с.

Старушкевич А. Організація огляду місця події. Аналіз криміналістично-значимої інформації при розслідуванні злочинів у сфері комп'ютерної інформації. *Вісник прокуратури.* 2003. № 12. С. 77–78.

Теплицький Б. Б., Шарай Л. Г., Ковальов К. М., Кузьмін С. А. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз : наук.-практ. посіб. Київ : Паливода А. В., 2019. 168 с.

Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 берез. 2016 р. № 96/2016. *Урядовий кур'єр*. 2016. № 52.

Стаття надійшла до редколегії 06.04.2020

Cherniakhovskyi B. – Postgraduate Student of the Department of Forensic Support and Forensic Science of the Educational and Scientific Institute No. 2 of the National Academy of Internal Affairs, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-7289-3034

Peculiarities of Conducting an Investigative Review during the Investigation of Unauthorized Interference in the Operation of Computers, Automated Systems, Computer Networks or Telecommunication Networks

*The **purpose** of the study is to determine the specifics of the investigative review during the pre-trial investigation of unauthorized interference with computers, automated systems, computer networks or telecommunications networks. **Methodology.** The article uses empirical and theoretical research methods. Among the empirical methods used were employees of operational units of cyberpolice and forensic experts of the Ministry of Internal Affairs, data analysis of the open part of the Unified State Register of Judgments. Theoretical methods were analysis and synthesis, analogy, comparison, generalization. **Scientific novelty.** Methods of detection, fixation and seizure of intangible digital (electronic) evidence are proposed. The necessity of development of normative acts for systematization of methods of conducting investigative review of evidence sources in digital (electronic) form is substantiated. **Conclusions.** 1. Investigative review of information in digital (electronic) form is the basis of the system of proving the unauthorized interference in the work of computers, automated systems, computer networks or telecommunications networks. 2. The use of special knowledge during the investigative examination in the pre-trial investigation of computer crimes is mandatory. Involvement of a specialist allows minimizing and eliminating the risks of loss or destruction of digital (electronic) evidence and ensures effective organization of actions of participants in the investigative review. 3. The method of work of the investigator with information in digital (electronic) form is subject to legislative regulation. Consolidation of basic algorithms for organizing the work of the investigative (investigative-operational) group during the investigative review provides proper procedural control over compliance with the law in the pre-trial investigation and determines the systematic improvement of cybercrime investigation methods.*

Keywords: investigative review; review of the scene; inspection of computer equipment; computer network overview; review of documents; review of digital (electronic) evidence; computer; computer network; unauthorized interference with computers; computer crime.