МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ
Кафедра кримінального процесу, криміналістики та експертології
факультет № 6

ТЕКСТ ЛЕКЦІЇ

з навчальної дисципліни ***«Криміналістичні засоби та методи розкриття і розслідування кримінальних правопорушень»*** вибіркових компонент освітньої програми другого (магістерського) рівня вищої освіти
спеціальність: 262 "Правоохоронна діяльність"

за темою: КИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ ЦИФРОВИХ ДОКАЗІВ
(лекція № 1)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол № 7 від 30.08.2023 р.

СХВАЛЕНО
Вченою радою факультету № 6
Протокол № 7 від 25.08.2023 р.

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з юридичних дисциплін
Протокол № 7 від 29.08.2023 р.

Розглянуто на засіданні кафедри кримінального процесу, криміналістики та експертології факультету Протокол № 6 від 21.08.2023 року № 7

Розробник:
Доцент кафедри кримінального процесу, криміналістики та експертології факультету № 6 кандидат юридичних наук, доцент Заяць Д.Д.

Рецензенти:
Голова Київського районного суду м. Харкова, доктор юридичних наук, доцент Шаренко С.Л.
Професор кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, доктор юридичних наук, професор Степанюк Р.Л.

План лекції

1. Поняття цифрових (електронних) доказів, джерела таких доказів та принципи роботи з ними.
2. Процесуальні особливості роботи з електронними носіями інформації.
3. Збирання доказів в електронній формі під час проведення окремих слідчих (розшукових) дій.
4. Фіксація цифрових (електронних) доказів.

Рекомендована література:

Основна

1. Криміналістика : підручник : у 2 т. Т. 1 / [А. Ф. Волобуєв, М. В. Даньшин, А. В. Іщенко та ін.] ; за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової ; МВС України, Харків. нац. ун-т внутр. справ. – Харків, 2018. – 384 с. – ISBN 978-966-610-231-0 (Т. 1). URL: https://dspace.univd.edu.ua/xmlui/handle/123456789/6440
2. Криміналістика: Підручник / Кол. авт.: В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. / За ред. проф. В. Ю. Шепітька. — 4-е вид., перероб. і доп. — Х.: Право, 2008. — 464 с. URL: https://law.sspu.edu.ua/files/documents/books/library/17/shepitko.pdf
3. Криміналістика : підруч. для студ. вищ. навч. закл. / [К. О. Чаплинський, О. В. Лускатов, І. В. Пиріг, В. М. Плетенець, Ю. А. Чаплинська]. – 2-е вид, перероб. і доп. – Дніпро : Дніпроп. держ. ун-т внутр. справ ; Ліра ЛТД, 2017. – 480 с. URL: https://er.dduvs.in.ua/bitstream/123456789/1191/1/%D0%9B%D0%95%D0%9A%D0%A6%D0%86%D0%87%20%D0%B7%20%D0%BA%D1%80%D0%B8%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%D1%96%D1%81%D1%82%D0%B8%D0%BA%D0%B8%202016%2B.pdf
4. Криміналістика (криміналістична техніка): курс лекцій / П. Д. Біленчук, А. П. Гель, М. В. Салтевський, Г. С. Семаков. Київ : МАУП, 2001. 216 с. http://www.kul-lib.narod.ru/bibl.files/krim/book-710.htm

Додаткова

1. Використання електронних (цифрових) доказів у кримінальних провадженнях [Текст] : метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. — Вид. 2-ге, доп. — Київ : Вид-во Нац. акад. внутр. справ, 2020. — 104 с. http://elar.naiau.kiev.ua/bitstream/123456789/17605/1/%D0%92%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D1%85%20%28%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D1%85%29%20%D0%B4%D0%BE%D0%BA%D0%B0%D0%B7%D1%96%D0%B2.pdf

Інформаційні ресурси в Інтернеті

1. Експертна служба МВС України: URL://dndekc.mvs.gov.ua/
2. Харківський НДІ судових експертиз ім. Засл. проф. М.С. Бокаріуса: URL:// www.hniise.gov.ua/

ВСТУП

Сучасний аналіз судово-слідчої практики свідчить, що у значній кількості кримінальних проваджень доказовою базою правопорушень є електронні (цифрові) докази, оскільки на сьогодні все більше правопорушень вчиняється у кіберпросторі та за допомогою інформаційних технологій і систем.

ТЕКСТ ЛЕКЦІЇ

1. Поняття цифрових (електронних) доказів, джерела таких доказів та принципи роботи з ними.

Згідно з положеннями ст. 84 Кримінального процесуального кодексу (КПК) України, доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому законом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. *Процесуальними джерелами доказів* є показання, речові докази, документи, висновки експертів.

Статтею 98 КПК України чітко визначено, що *речовими доказами* є матеріальні об’єкти, які були знаряддям вчинення кримінального правопорушення, зберегли на собі його сліди або містять інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження, в тому числі предмети, що були об’єктом кримінально протиправних дій, гроші, цінності та інші речі, набуті кримінально протиправним шляхом.

Відповідно до ст. 99 КПК України документи є речовими доказами, якщо вони містять відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. *До документів можуть належати*: матеріали фотозйомки, звукозапису, відеозапису та *інші носії інформації* (у тому числі *електронні*), а *також носії інформації,* на яких за допомогою технічних засобів зафіксовано процесуальні дії. Як ви вже знаєте з курсу криміналістики, у деяких випадках, а саме тоді,

коли документ незмінний, він може бути одночасно письмовим і речовим доказом.

На підставі вище зазначеного, можна сказати, що **електронні докази** — це докази у кримінальних провадженнях, які можна отримати в електронній формі. Електронні докази отримують за допомогою електронних пристроїв, комп'ютерних носіїв інформації, а також комп'ютерних мереж, у тому числі через мережу Інтернет. Вони стають доступними для сприйняття людиною після обробки засобами комп'ютерної техніки.

Разом із поняттям ***«електронні докази»*** (electronic evidence), часто застосовують поняття ***«цифрові докази»*** (digital evidence). Оскільки на законодавчому рівні ці поняття ще не регламентовані, їх використовують паралельно. Інформація, подана у формі, придатній для її оброблення електронними засобами, відповідно до Закону України «Про електронні документи та електронний документообіг» називається **даними.** До таких даних, згідно «Конвенції про кіберзлочинність» 2001 року відносяться:

- «*комп'ютерні дані*» — будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, 6 включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою;
- «*комп'ютерна система»* — будь-який пристрій або групу взаємно поєднаних або пов'язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних.

Окремі положення Закону України «Про основні засади забезпечення кібербезпеки України» визначають ***кіберзлочин*** (*комп'ютерний злочин*) як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

В Україні електронні докази, як правову категорію, визначено в 2017 році у Цивільному процесуальному кодексі (ЦПК) України, Господарському процесуальному кодексі (ГПК) України та Кодексі адміністративного

судочинства (КАС) України. На цей час існує певна судова практика їх використання. Так, згідно зі ст. 100 ЦПК України, ст. 96 ГПК України та ст. 99 КАС України електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, які мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (у тому числі в мережі Інтернет).

Зараз ведеться робота щодо впровадження поняття «електронні (цифрові) докази» в законодавство України, зокрема в КПК України.

Електронні дані набагато легше змінити чи підробити, ніж традиційні форми доказів, тому правоохоронцям потрібно дотримуватися таких правил поводження з даними, які нададуть можливість забезпечити допустимість доказів.

На відміну від звичайних паперових документів, характеристики та просторові межі яких ми звикли бачити, електронні документи мають іншу природу і вирізняються такими характеристиками:

– електронний документ не може існувати без носія інформації. При цьому набувають значення ідентифікаційні ознаки носія інформації (зокрема найменування типу, марки моделі, індивідуального машинного носія, на якому записаний документ);

– електронні докази невидимі «неозброєним оком» (без спеціального інструментарію) і для їх сприймання та дослідження використовують програмно-технічні засоби;

– вони можуть бути змінені, пошкоджені або знищені в процесі експлуатації пристрою користувачем чи під впливом фізичних чинників (високий рівень вологості, висока температура, електромагнітні випромінювання тощо);

– за стадіями виготовлення документи, в тому числі й електронні, поділяють на оригінали, дублікати, копії й виписки. У ч.3 ст. 99 КПК України визначено, що оригіналом документа є сам документ, а оригіналом електронного документа — його відображення, якому надається таке саме значення, як і документу. Разом із тим, для електронного документа такі поняття, як «оригінал», «дублікат», «копія» є умовними, оскільки у всіх цих випадках електронний документ залишається оригіналом. У ст. 7 Закону України від 22 травня 2003 року № 851-IV «Про електронні документи та електронний документообіг» передбачено, що електронна копія та копія електронного документа на папері засвідчуються в порядку, передбаченому законом, але відповідний нормативний акт до цього часу не ухвалено. Навіть нотаріуси не вповноважені державою засвідчувати такі копії.

У кримінальному процесі докази мають відповідати двом вимогам, які висуваються до його змісту та форми, — належності (ст. 85 КПК України) і допустимості (ст. 86 КПК України). Закономірно, що такі ознаки повинен мати й електронний доказ, що може забезпечуватися коректністю фіксації та подальшою незмінністю комп'ютерних даних.

Джерелами доказів в електронній формі можуть бути: різноманітні носії інформації; моноблоки; мобільні пристрої; (мобільні телефони, планшетні комп'ютери), цифрові камери; роутери; маршрутизатори; комп'ютерні мережі; глобальна мережа Інтернет; звуко- та відеозаписи тощо, тобто джерелом доказів може бути будь-який електронний пристрій, який знаходиться на місці події, місці обшуку. Слід також зазначити, що постійно з'являються нові види електронних пристроїв, які можуть містити електронні докази. Натепер, у ході розслідування будь-якого злочину, слідчі крім основних «традиційних» доказів, повинні виявляти, фіксувати та вилучати й електронні докази. Тому під час досудового розслідування, наприклад, крадіжки з'ясовують, чи мав потерпілий комп'ютер, чи підтримує він інтернет-контакти тощо.

<u>Докази вчинення злочину можуть бути виявлені:</u>

− у комп'ютері потерпілого;

− у інтернет-провайдера, послугами якого користувався потерпілий;

− у комп’ютері підозрюваного;

− у інтернет-провайдера, послугами якого користувався підозрюваний;

− у іншому місці кіберпростору.

Важливим джерелом доказів є комп’ютерна система, яка складається з корпусу, де розміщені мікропроцесор, плати, накопичувачі інформації та порти для зовнішніх пристроїв; монітора; периферійних пристроїв (принтер, сканер тощо), програмного забезпечення, зокрема:

– системне програмне забезпечення;

– прикладне програмне забезпечення (текстові і графічні редактори, системи управління базами даних, електронні таблиці, системи презентацій та ін.).

До інформаційних об’єктів (даних) відносяться:

– текстові і графічні документи;

– дані у форматах мультимедіа;

– інформація у форматах баз даних та інші додатки прикладного характеру.

Важлива інформація може міститись й у тимчасових файлах. Більшість текстових редакторів і систем управління базами даних створюють тимчасові файли як побічний продукт нормальної роботи програмного забезпечення. Користувачі комп’ютерів зазвичай не усвідомлюють важливості створення цих файлів тому, що вони, як правило, знищуються програмою наприкінці сеансу роботи. Але дані, які містять ці знищені файли, можуть виявитися найціннішими. Особливо, якщо вихідний файл був зашифрований чи документ із текстом був надрукований без збереження на диску, такі файли можуть бути відновлені.

Існують зовнішні та внутрішні накопичувачі інформації, а також змінні носії (CD, DVD-диски) та різноманітні USB-накопичувачі. У цифрових камерах та мобільних телефонах широко використовуються невеликі за розмірами карти пам’яті (SD, micro SD, compact Flash CF тощо), які можуть містити значний обсяг інформації. Наприклад, карта Western Digital SanDisk Ultra microSDXC має обсяг пам'яті 400 ГБ.

Дуже багато різноманітної інформації містять сучасні мобільні пристрої — *смартфони, планшети та різноманітні плеєри*. Крім того, інформація про факти та обставини, що мають значення для кримінального провадження, може міститись у *системі відеоспостереження*. Слід зазначити, що в багатьох IP-камерах можуть бути накопичувачі інформації, що дають змогу здійснювати відеофіксацію та зберігати відеоматеріал без підключення до реєстратора.

Багато електронних пристроїв можуть здійснювати обмін інформацією через локальні комп'ютерні мережі або глобальну мережу Інтернет. Тому для дослідження спеціалізованих пристроїв (концентраторів, маршрутизаторів, комутаторів тощо) необхідні знання фахівця.

Слід зауважити, що сьогодні великий обсяг інформації зберігається у «хмарних технологіях», тобто поза місцезнаходженням фізичної чи юридичної особи. На цей час, для перевірки цілісності даних використовується механізм розрахунку контрольної суми або хеш-суми. ***Контрольна сума*** **—** це певне значення, обчислене на основі набору даних із застосуванням одного із математичних (криптографічних) алгоритмів (наприклад, CRC32, MD5, SHA-1, SHA-2, SHA-3 або ін.), які використовується для перевірки цілісності даних при їх передачі або збереженні. Зазначені контрольні суми можна отримати, використовуючи, наприклад, таку програму, як HashTab. Вона відкрито розповсюджена в мережі Інтернет і вважається найбільш ефективною для такого роду обчислень.

Будь яка діяльність, як і робота з електронними доказами, вимагає ***дотримування певних принципів***, до яких відносяться:

1. *Законність.* Слідчі, прокурори, дізнавачі, що провадять розслідування і досліджують докази в електронній формі, зобов'язані дотримуватися чинного законодавства, загальних процесуальних та криміналістичних принципів.

2. *Цілісність даних*. Дії фахівця не повинні призводити до матеріальних змін даних, електронних пристроїв чи носіїв інформації, які можуть використовуватись як докази.

3. *Документування процесу*. Документуванню підлягають будь-які дії, що здійснюються стосовно електронних доказів, і зберігають ці документи на

випадок перевірки, щоб незалежна третя сторона могла повторити ці дії та отримати аналогічний результат.

4. *Експертна підтримка*. Якщо передбачається, що при огляді (обшуку) можуть бути виявлені електронні докази, необхідно залучити фахівців (спеціалістів), забезпечивши, за можливості, їх присутність на місці події, тим самим отримати їхню підтримку.

5. *Фахова підготовка*. Якщо при огляді (обшуку) відсутні фахівці з роботи з електронними доказами, то першочергові дії на місці події здійснюють особи, які мають необхідні знання та навички для виявлення і збирання доказів.

6. *Розумна обережність*. Слід уникати будь-яких навмисних або ненавмисних дій, які можуть призвести до пошкодження потенційних доказів, представлених у цифровій формі. Задля цього співробітники правоохоронних органів не повинні мати доступ до цифрових пристроїв, якщо їм бракує компетентності і вони не обізнані з відповідними процесами. Зокрема, якщо фізичний обсяг цифрового пристрою занадто великий, наприклад, сервер в інформаційному центрі; чи це критично для безпеки цифрового пристрою, зупинка якого загрожуватиме життю людей, або коли необхідно зафіксувати спосіб роботи підозрюваного під час зловживання системою.

2. Процесуальні особливості роботи з електронними носіями інформації.

Відповідно до вимог КПК України в процесі досудового розслідування у кримінальних провадженнях слідчий, прокурор на підставі відповідного процесуального рішення, у тому числі постанови або ухвали суду, зобов’язані вилучати:

– речові докази;

– предмети і документи, обіг яких заборонено (якщо у власника немає дозволу на їх придбання і зберігання);

– документи, що засвідчують особу заарештованого, підозрюваного, обвинуваченого (підсудного);

– інші документи, що мають значення у справі.

Дії, пов’язані з вилученням і дослідженням комп’ютерного обладнання,

мають відповідати вимогам законодавства, а саме: Конституції України, законів України: «Про інформацію», «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про судову експертизу», «Про телекомунікації», Кримінального та Кримінального процесуального кодексу України, Конвенції про кіберзлочинність та інших нормативно-правових актів.

Вимоги до проведення слідчих (розшукових) дій чітко визначені у ст. 223 КПК України. Пошук та вилучення доказів в електронній формі можуть здійснюватися під час кримінального провадження відповідно до Кримінального процесуального кодексу України шляхом здійснення таких слідчих (розшукових) дій:

– обшуку (ст. 234 КПК України) на підставі ухвали слідчого судді (ст. 235 КПК України);

– огляду (ст. 237 КПК України).

Крім того, пошук та вилучення доказів в електронній формі можуть здійснюватися шляхом:

– проведення негласних слідчих (розшукових) дій відповідно до глави 21 КПК України та зважаючи на Інструкцію про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затвердженої Спільним Наказом Генеральної прокуратури України, МВС, СБУ, Адміністрації Державної прикордонної служби України, Міністерства юстиції України та Міністерства фінансів України від 16.11.2012 № 114/1042/516/1199/936/1687/5;

– здійснення такого заходу забезпечення кримінального провадження, як тимчасовий доступ до речей і документів (ст. 159 КПК України) на підставі ухвали слідчого судді, суду;

– зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України);

– зняття інформації з електронних інформаційних систем (ст. 264 КПК України); – дослідження інформації, отриманої при застосуванні технічних засобів (ст. 266 КПК України);

– встановлення місцезнаходження радіоелектронного засобу (ст. 268 КПК

України).

Відповідно до вимог ст. 168 КПК України тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, здійснюється лише у разі, якщо вони безпосередньо зазначені в ухвалі суду.

Забороняється тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків, коли їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження, або якщо такі об'єкти отримані в результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення, а також якщо доступ до них обмежується їх власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту.

Слід зазначити, що відповідно до п. 4 ст. 99 КПК України копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа. Тому, на підставі ст. 168 КПК України, у разі необхідності, слідчий чи прокурор здійснює копіювання інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста.

З метою організації належного техніко-криміналістичного забезпечення огляду місця події та порядку залучення працівників органів досудового розслідування поліції та Експертної служби МВС України на спеціалізованій пересувній лабораторії на стадії досудового розслідування визначаються Інструкцією «Про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події»,

затвердженою наказом Міністерства внутрішніх справ України від 03.11.2015 № 1339 у якій визначені обов'язки та повноваження працівників як спеціалістів під час проведення огляду місця події.

Водночас, у разі отримання слідчим ініціативного рапорту від оперативного підрозділу щодо проведення відповідних негласних слідчих (розшукових) дій (НСРД) в рамках супроводження зазначеного кримінального провадження, слідчий зобов'язаний у триденний термін звернутися до суду з відповідним клопотанням або, у разі якщо слідчий вважає проведення НСРД, описаного в ініціативному рапорті недоцільним, у триденний термін письмово повідомити про це підрозділ-ініціатор.

3. Збирання доказів в електронній формі під час проведення окремих слідчих (розшукових) дій.

Збирання доказів в електронній формі є нелегким процесом, оскільки це зумовлено складністю об'єктів. Проте, не кожний слідчий володіє спеціальними знаннями у сфері сучасних інформаційно-комунікаційних технологій у достатній мірі, щоб успішно організувати розслідування. У зв'язку з цим бажана допомога відповідного фахівця, який є достатньо підготовленим у цій сфері, оскільки навіть незначна некваліфікована дія з доказами в електронній формі може спричинити незворотну втрату цінної інформації. Тому вилучення та дослідження об'єктів в електронній формі за можливості має проводити фахівець.

Підготовка до проведення слідчих (розшукових) дій.

Перед обшуком необхідно з'ясувати такі питання:

– Яке комп'ютерне обладнання та програмне забезпечення може бути на місці обшуку?

– Хто відповідає за обладнання (системний адміністратор)?

– Яка кількість обладнання може бути виявлена?

– Який обсяг даних потрібно буде скопіювати?

– Чи існують резервні копії даних та де вони зберігаються?

Плануючи обшук необхідно:

– отримати ухвалу слідчого судді (ст. 233 КПК України) для проникнення в приміщення та вилучення відповідних доказів;

– створити слідчо-оперативну групу (СОГ) до складу якої включаються слідчий (він є старшим СОГ), працівник оперативного підрозділу, інспектор-криміналіст та інші учасники відповідно до наказів МВС України від 07.07.2017 № 575 «Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні» та від 03.11.2015 № 1339 «Про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події»;

– створити групу спеціалістів з числа працівників кіберполіції та інших підрозділів для виїзду на місце події з метою виявлення слідів, їх фіксації, вилучення, опису та інтерпретації з урахуванням спеціальних знань (ст. 128 КПК України);

– проінструктувати членів слідчо-оперативної групи щодо порядку роботи;

– забезпечити групу необхідними інструментами та обладнанням;

– забезпечити швидкий та безпечний шлях для проникнення в приміщення.

***З метою збирання електронних (цифрових) доказів використовують такі техніко-криміналістичні засоби*:**

1. *Носії інформації, на які безпосередньо копіюватимуться дані*:

– жорсткі диски (вінчестери);

– змінні носії (CD-DVD-диски);

– зовнішні пристрої з накопичувачами та для роботи з оптичними носіями інформації тощо.

2. *Інструменти для демонтажу обладнання*:

– викрутки (плоскі та фігурні);

– кусачки;

– плоскогубці;

– пінцет тощо.

3. Інструменти для документування процесу:

– фото- та відеокамера;

– бірки для нумерації доказів.

4. Матеріали для упаковки та транспортування вилучених об'єктів:

– антистатичні пакети;

– кабельна стяжка;

– коробки для DVD-дисків;

– коробки різноманітних розмірів для інших вилучених об'єктів.

5. Інші засоби та матеріали:

– транспорт для перевезення слідчо-оперативної групи, інструментів та вилучених матеріалів;

– папір для друку;

– роздруковані тексти із правами та обов'язками учасників слідчих дій;

– ноутбук зі стандартним програмним забезпеченням;

– спеціалізовані програмно-апаратні пристрої цифрової криміналістики (форензіки), криміналістичні загрузочні диски тощо.

Особливості проведення обшуку.

Враховуючи всі тактичні особливості підготовки та проведення обшуку (які розглядались у основному курсі криміналістики) та вживши першочергових заходів, слідчому необхідно в присутності понятих попередньо оглянути всі приміщення та/або їх частини, де планується проведення обшуку, на предмет наявності в них будь-яких інших осіб з метою недопущення видалення останніми будь-якої інформації з пам'яті комп'ютера, знищення ними з'ємних носіїв інформації, знищення будь-яких інших предметів або документів, які планується відшукати. Потрібно також зважати на те, що існує можливість включити до складу програмного забезпечення комп'ютера програму, яка періодично вимагає введення паролю, і, якщо декілька секунд правильний пароль не буде введений, дані в комп'ютері можуть автоматично знищуватись або зашифровуватись. Тому, доцільно запропонувати всім

присутнім особам зайняти будь-яке одне приміщення або його частину, для того, щоб вони постійно знаходилися в полі зору працівників оперативного підрозділу, слідчих та понятих. Відповідно до ч. 3 ст. 236 КПК України слідчий, прокурор має право заборонити будь-якій особі залишити місце обшуку до його закінчення та вчиняти будь-які дії, що заважають проведенню обшуку. Невиконання цих вимог тягне за собою передбачену законом відповідальність. Необхідно обов'язково унеможливити відключення працюючого обладнання чи навіть закривання кришки ноутбука. Для цього слід відразу відсторонити операторів (користувачів) від обладнання. Сьогодні значна кількість інформації зберігається у «хмарних сховищах», тобто розміщена поза місцезнаходженням фізичної чи юридичної особи. Тому присутні під час обшуку особи можуть використати наявні в них різноманітні гаджети, у тому числі мобільні телефони, для вчинення будь-яких дій з метою пошкодження, знищення, перетворення інформації, яка фактично може перебувати на відстані (навіть у межах приміщення, де відбувається обшук, тощо). З огляду на це доцільно усім присутнім при обшуку особам, на початку обшуку повідомити про заборону використання мобільних телефонів чи інших електронних пристроїв, які знаходять у них, та покласти їх на місце, доступне для поля зору слідчого, оперативного працівника, понятих, для здійснення контролю за невикористанням зазначених речей під час проведення обшуку. Також, ч. 5 ст. 236 КПК України визначено, що за рішенням слідчого чи прокурора може бути проведено обшук осіб, які перебувають в житлі чи іншому володінні, якщо є достатні підстави вважати, що вони переховують при собі предмети або документи, які мають значення для кримінального провадження. Обшук особи повинен бути здійснений особами тієї ж статі. Беручи до уваги зазначену вище норму КПК України, у разі, якщо особи відмовляються виконувати вимоги слідчого щодо невикористання мобільних телефонів чи інших електронних пристроїв, які знаходяться при них, можливе проведення обшуку особи та вирішення питання щодо доцільності вилучення мобільного телефону чи електронного пристрою, попередньо оглянувши останній, за участю відповідних спеціалістів, на наявність у них електронних документів, що мають

значення у кримінальному провадженні. Крім того, залежно від поверху, на якому знаходиться приміщення, до початку проведення обшуку за можливості необхідно залучити працівників оперативного підрозділу та інших окремих понятих для спостереження за вікнами приміщення, в якому проводиться обшук, з метою своєчасного виявлення будь-якого викидання предметів з приміщення, що потрібно вчасно виявити та задокументувати.

Після цього залежно від виду приміщення, в якому проводиться обшук, слідчий розподіляє учасників слідчої дії у приміщенні залежно від їх кількості на групи, до якої крім СОГ можуть входити:

– спеціаліст експертної служби (ДНДЕКЦ або територіальних підрозділів експертної служби МВС України) чи іншої установи;

– особа — власник приміщення або його частини (представник цієї особи), та/або особа, яка займає приміщення чи його частину;

– поняті.

До протоколу обшуку вносяться відомості про найменування приміщень або їх частин, а також про слідчих, які проводитимуть обшук у таких приміщеннях або їх частинах, працівників ДКП НП України, власників цих приміщень, їх представників, осіб, які займають ці приміщення, понятих.

У разі застосування технічних засобів фіксації під час обшуку в окремому приміщенні чи його частині, відповідні відомості зазначаються в конкретному додатку до протоколу обшуку. Якщо технічні засоби фіксації не застосовуються, в додатку до протоколу обшуку та в протоколі обшуку має бути запис про роз’яснення порядку застосування технічних засобів фіксації, а також відомості про те, що від учасників та присутніх клопотання про їх застосування не надходили. Слідчий кожної такої групи є відповідальним за проведення обшуку виділеної йому частини приміщення та за оформлення відповідного додатка до протоколу обшуку. Вимоги слідчого слідчої групи щодо проведення обшуку виділеної частини приміщення є обов’язковими для виконання працівниками кіберполіції. З метою забезпечення збереження слідів учиненого кримінального правопорушення (залежно від його виду) під час виявлення предметів комп’ютерної техніки, інших предметів чи документів

працівники кіберполіції за дорученням слідчого мають здійснювати їх огляд у спеціальних рукавицях, про що вносяться відомості до протоколу. Усі вилучені предмети, цінності і документи пред'являються для ознайомлення понятим та іншим учасникам слідчої дії. У необхідних випадках зазначені об’єкти упаковуються для уникнення їх пошкодження, неконтрольованого доступу до них та забезпечення зберігання слідів (мікрослідів), які є на них, з оформленням бірок із відповідними написами, засвідченими підписами особи, в якої вилучено речі, понятих, слідчого, працівника оперативного підрозділу, спеціаліста, які скріплюються печаткою відповідного органу, відомості про що вносяться до протоколу. Усі вилучені предмети, цінності і документи пред'являються понятим та іншим учасникам слідчої дії. Після завершення складання протоколу обшуку та всіх його додатків учасники обшуку, в тому числі й працівники оперативного підрозділу, присутні особи, поняті мають почергово ознайомитись зі змістом протоколу обшуку та всіх його додатків та поставити свої підписи у відведених в протоколі та додатках місцях.

Дослідження джерел електронних (цифрових) доказів.

Якщо на місці обшуку виявлено *ввімкнений комп'ютер* або інші електронні пристрої, необхідно провести огляд (виїмку) комп'ютерних даних у режимі реального часу. Перш за все потрібно не дати можливості його заблокувати або вимкнути чи зашифрувати.

У ввімкнених пристроях є дуже нестійкі «*енергозалежні дані*». І якщо їх не зберегти правильно і швидко, вони можуть бути втрачені.

Оперативна пам'ять сучасних комп'ютерних систем може вміщати понад 16 ГБ інформації і більше (це майже 55 тис. зображень). У сучасних комп'ютерних системах дані часто зберігаються і обробляються не на самому пристрої, а, наприклад, у «хмарних сховищах». Таку інформацію теж можна втратити.

Слід зазначити, що порядок доступу до таких даних регулюється законодавством тієї країни, де вони перебувають фізично. У деяких країнах закон може забороняти виїмку такої інформації і доступ до неї навіть у режимі реального часу.

В оперативній пам’яті може знаходитися:

– інформація про виконувані у комп’ютері процеси;

– інформація про виконувані сервіси;

– системна інформація;

– дані про користувачів, які перебувають в системі;

– про відкриті порти;

– кеш ARP (протоколу визначення адреси);

– кеш DNS (доменної системи імен);

– інформація про автоматично завантажені додатки;

– незбережені документи;

– бінарні процеси і сервіси, в тому числі шкідливі програми, які зберігаються тільки в оперативній пам'яті.

Для збереження «енергозалежних даних» у процесі обшуку необхідно:

– визначити, вилучити, описати і сфотографувати кожен пристрій, що містить «енергозалежні дані»;

– ізолювати підозрюваних та інших сторонніх осіб від комп'ютерного обладнання і не допустити, щоб вони змінили або знищили докази;

– спостерігати за складовими комп'ютерної системи і запобігати будь-якій автоматичній зміні або знищенню доказів.

Отримання електронних доказів у ввімкнених пристроях повинен здійснювати відповідний спеціаліст, наприклад, працівник кіберполіції зі застосуванням спеціальних знань, засобів та програм. Він повинен у присутності понятих та учасників обшуку оглянути пристрій, оголосити всім присутнім назву (ім’я) пристрою (користувача), операційну систему, її версію, розрядність, MAC-адресу та пояснення — яке доказове значення вони матимуть у подальшому. Ця інформація обов’язково вноситься до протоколу.

Особливості огляду локального комп’ютерного засобу.

1. Після вмикання комп’ютера необхідно пересвідчитись у налаштуванні BIOS на завантаження з приводу оптичних дисків або з флеш-накопичувача (при загрузці натиснути клавішу Del, Esc або F2 — при включенні комп’ютера на моніторі з’являється повідомлення, наприклад, Press DEL to enter SETUP), у

разі потреби внести необхідні зміни та перезавантажити.

2. Завантажити операційну систему з робочого примірника спеціаліста (оптичного диска з дистрибутивом або з зовнішнього носія інформації).

3. Підключити принтер, роздрукувати текст із правами й обов'язками учасників слідчої дії, ознайомити їх із цими документами під підпис.

4. Приєднати носій, на який здійснюватиметься запис і на якому зберігатиметься інформація, отримана під час огляду, після чого його відформатувати.

5. За допомогою відповідної програми вивести на екран монітора інформацію про апаратне та програмне забезпечення комп'ютера, необхідну для його ідентифікації, зберегти її як окремий файл.

6. 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 файлеталон та файл із його контрольною сумою на носієві, призначений для запису та зберігання доказової інформації.

7. У разі потреби в перегляді файлів із відеограмами запустити програму запису зображення екрана монітора.

8. Здійснити огляд вмісту носіїв інформації, демонструючи учасникам зміст та місцезнаходження (шлях розташування) файлів, які слідчий вважає такими, що стосуються справи, скопіювавши їх на носій, призначений для запису та зберігання доказової інформації.

9. У разі потреби та наявності ресурсів здійснити побітове копіювання, створивши файл-образ носія, який оглядається, та зберегти його на носій, призначений для запису та зберігання доказової інформації.

10. Скопіювати файли з відеограмою та скриншотами зображення екрана монітора, створеними під час огляду, та зберегти їх на носій, призначений для запису та збереження доказової інформації, в окремому каталозі.

11. За допомогою відповідної програми вивести на екран монітора інформацію про контрольну суму кожного файла (з інформацією, що стосується справи), зафіксованого раніше на носієві, призначеному для запису

та зберігання доказової інформації, зберігаючи при цьому дані про контрольну суму в окремі файли.

12. Приєднати та відформатувати другий носій, після цього скопіювати на нього всю інформацію з контрольного носія.

13. Інформацію про здійснений огляд (а також зауваження, клопотання чи доповнення учасників, за наявності) внести до протоколу та роздрукувати його, після чого обрахувати його контрольну суму й обидва файли (протокол і файл з його контрольною сумою) зберегти на контрольному і робочому примірниках носіїв разом з каталогом із доказовою інформацією. У разі необхідності або клопотання учасників слідчої дії продемонструвати їм текст протоколу для порівняння з тим, що роздрукований, відтворити збережені відеограми чи інші файли з доказовою інформацією.

14. Від'єднати контрольний та робочий носії з доказовою інформацією, диск з робочим примірником дистрибутиву, упакувати контрольний примірник носія з доказовою інформацією так, щоб унеможливити доступ до нього, та здійснити його опечатування стандартним способом, про що також зазначити у протоколі, після чого надати його учасникам на засвідчення підписами.

Особливості огляду віддаленого ресурсу комп'ютерної мережі.

1. Після вмикання комп'ютера необхідно пересвідчитись у налаштуванні BIOS на завантаження з приводу оптичних дисків, у разі потреби внести необхідні зміни та перезавантажити.

2. Здійснити завантаження операційної системи з робочого примірника спеціаліста (оптичного диска з дистрибутивом).

3. Підключити принтер, роздрукувати текст із правами й обов'язками учасників, ознайомити їх під підпис.

4. Приєднати носій, на який здійснюватиметься запис і на якому зберігатимуться електронні докази, отримані під час огляду, відформатувати його.

5. За допомогою відповідної програми отримати на екран монітора інформацію про апаратне та програмне забезпечення комп'ютера, необхідну для його ідентифікації, зберегти її як окремий файл.

6. Створити файл-еталон для перевірки правильності підрахунку контрольних сум за допомогою призначеної для цього програми, перевірити та продемонструвати учасникам результати, зберегти файл-еталон та файл з його контрольною сумою на носієві, призначеному для запису та зберігання доказової інформації.

7. У разі потреби перегляду файлів із відеограмами запустити програму запису зображення екрана монітора.

8. За допомогою відповідної програми вивести на екран монітора налаштування мережевого адаптера, зафіксувати ці дані скріншотом та зберегти їх під окремою назвою.

9. Запустити браузер та ввести доменне ім’я (інший прийнятний ідентифікатор) віддаленого ресурсу, здійснити огляд умісту сайту чи іншого ресурсу, демонструючи учасникам слідчої дії зміст та місцезнаходження (шлях розміщення) файлів на віддаленому ресурсі, які слідчий (оперуповноважений) уважає такими, що стосуються справи, скопіювати на носій, призначений для запису та зберігання доказової інформації.

10. У разі потреби застосувати відповідні програмні засоби для встановлення IP-адреси сайту (ping), шляху проходження пакетів при обміні інформацією з ним, скопіювати їх на носій, призначений для запису та зберігання доказової інформації.

11. За необхідності встановлення провайдера, якому належить IP-адреса сайту, або реєстратора доменного імені скористатись відповідними веб-сервісами мережі Інтернет.

12. Скопіювати файли з відеограмою та скриншотами зображення екрана монітора, створеними під час огляду, та зберегти їх на носієві, призначеному для запису та зберігання доказової інформації, в окремому каталозі.

13. За допомогою відповідної програми вивести на екран монітора інформацію про контрольну суму кожного файла (з інформацією, що стосується справи), зафіксованого на носієві, призначеному для запису та зберігання доказової інформації, зберігаючи при цьому дані про контрольну суму в окремих файлах.

14. Приєднати та відформатувати другий носій, після цього скопіювати на нього всю інформацію з контрольного носія.

15. Інформацію про здійснений огляд (а також зауваження, клопотання чи доповнення учасників слідчої дії, за наявності) внести до протоколу та роздрукувати, підрахувати його контрольну суму й обидва файли (протокол і файл з його контрольною сумою) зберегти на контрольному і робочому примірниках носіїв разом з каталогом із доказовою інформацією. У разі необхідності або клопотання учасників продемонструвати їм текст протоколу для порівняння з тим, що роздрукований, відтворити збережені відеограми чи інші файли з доказовою інформацією.

16. Від'єднати контрольний та робочий носії з доказовою інформацією, диск з робочим примірником дистрибутиву, упакувати контрольний примірник носія з доказовою інформацією так, щоб унеможливити доступ до нього, та здійснити його опечатування стандартним способом, про що також зазначити у протоколі, після чого надати його учасникам на засвідчення підписами. При цьому слід мати на увазі, що для проведення огляду акаунтів у соціальних мережах, месенджерів, поштових клієнтів тощо, які зберігаються на вилученій комп'ютерній техніці та потребують здійснення обходу логічного захисту, а особа, яка нею володіє, не дала добровільної згоди на ці дії, то слідчий зобов'язаний звернутись до суду з відповідним клопотанням щодо отримання дозволу на проведення такого огляду.