МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ (ЦИФРОВИХ) ДОКАЗІВ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ

Методичні рекомендації

Видання друге, доповнене

Київ – 2020

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ (ЦИФРОВИХ) ДОКАЗІВ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ

Методичні рекомендації

Видання друге, доповнене

Київ – 2020

УДК 343.16
В 43

Авторський колектив:

Гуцалюк М. В., кандидат юридичних наук, старший науковий співробітник (Міжвідомчий науково-дослідний центр боротьби з організованою злочинністю при Раді національної безпеки і оборони України);

Гавловський В. Д., кандидат юридичних наук, старший науковий співробітник (Міжвідомчий науково-дослідний центр боротьби з організованою злочинністю при Раді національної безпеки і оборони України);

Хахановський В. Г., доктор юридичних наук, професор (Національна академія внутрішніх справ);

Самойлов С. В., кандидат юридичних наук (Департамент кіберполіції Національної поліції України);

Киричок В.М. (Департамент кіберполіції Національної поліції України);

Степанець Д. С. (Державний науково-дослідний експертно-криміналістичного центр МВС України);

Одинокова О. А. (Головне слідче управління Національної поліції України);

Кагітін С. М. (Головне слідче управління Національної поліції України);

Школьніков В.І. (Національна академія внутрішніх справ).

Загальне упорядкування та редагування матеріалів видання:

Корнейко О. В., кандидат технічних наук, професор (Національна академія внутрішніх справ).

Рецензенти:

Ахтирська Н. М., кандидат юридичних наук, доцент (Київський національний університет імені Тараса Шевченка);

Звєрєв В. П., кандидат технічних наук, старший науковий співробітник (Апарат Ради національної безпеки і оборони України).

Рекомендації підготовлені за замовою Головного слідчого управління Національної поліції України (лист від 01.11.2019 за № 12494/05/24-2019).

Розглянуті, схвалені та рекомендовані до друку на засіданні науково-методичної ради Національної академії внутрішніх справ 20 травня 2020 року, протокол № 8.

В 43 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.

Розглянуто основні поняття, особливості та принципи роботи з електронними (цифровими) доказами, а також кримінально-процесуальні засади пошуку й вилучення комп'ютерної техніки та інформації з неї. Визначено особливості збирання електронних (цифрових) доказів, виявлення, огляду, фіксації, вилучення та упакування їх носіїв.

Зазначена друга редакція методичних рекомендацій декілька розширює матеріали, що були викладені за тією ж назвою авторами у першій редакції видання 2017 року, зокрема, в тому числі додатково наведені основні положення державного стандарту ДСТУ ISO/IEC 27037:2017 та новітні зміни в національному законодавстві.

Рекомендації розраховані на працівників слідчих, оперативних та інших практичних підрозділів правоохоронних органів, науковців, викладачів та здобувачів навчальних закладів юридичної освіти.

УДК 343.16

ЗМІСТ

ВСТУП

На даний час доказовою базою достатньої частки кримінальних правопорушень є електронні (цифрові) докази, так як сучасні правопорушення все більше здійснюється в кіберпросторі та за допомогою інформаційних технологій і систем.

Тому авторами розроблені зазначені методичні рекомендації щодо удосконалення процесуальних механізмів збирання, виявлення, огляду, фіксації та вилучення електронних (цифрових) доказів під час здійснення кримінального провадження. Рекомендації зорієнтовано на працівників правоохоронних органів, які не є експертами в роботі з комп'ютерними системами та мережами, проте мають знати основи отримання та аналізу такого виду доказів.

Мета цих рекомендацій — надання базових знань, які допоможуть правоохоронцям розуміти ключові положення електронних (цифрових) доказів, ставити правильно сформульовані конкретні питання експертам, операторам та провайдерам для отримання інформації, необхідної при розслідуванні відповідних кримінальних правопорушень, а також дотримуватися відповідних правил збирання та зберігання носіїв такої інформації. У рекомендаціях використано, зокрема, практичний досвід працівників Департаменту кіберполіції та Головного слідчого управління Національної поліції України, Державного науково-дослідного експертно-криміналістичного центру МВС України.

Зазначена редакція методичних рекомендацій декілька розширює матеріали, що були викладені за тією ж назвою авторами у першій редакції рекомендацій 2017 року.

Крім того, у додатку до основного матеріалу методичних рекомендацій наведені основні положення державного стандарту ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», що набув чинності з 1 січня 2019 року і представлений у виданні не як офіційне представлення цього стандарту. Зазначений національний стандарт гармонізований методом перекладу з відповідним міжнародним стандартом, що розроблений спільним технічним комітетом Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC) і де наведений сталий зарубіжний досвід щодо ідентифікації, збирання, здобуття та збереження потенційних електронних (цифрових) доказів. Але читачі повинні розуміти, що зазначений стандарт не повною мірою відповідає специфічним вимогам існуючої редакції Кримінального процесуального кодексу України.

1. ПОНЯТТЯ, ОСОБЛИВОСТІ ТА ПРИНЦИПИ РОБОТИ З ДОКАЗАМИ В ЕЛЕКТРОННІЙ (ЦИФРОВІЙ) ФОРМІ

Відповідно до 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.

Згідно ст. 98 КПК України **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. У деяких випадках, а саме тоді, коли документ незмінний, він може мати одночасно ознаки і документа, і речового доказу.

Отже**, 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 окреслені, 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.**

Відповідно до «Конвенції про кіберзлочинність» 2001 року:

«**комп'ютерні дані**» **—** будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі,

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.

Згідно із Законом України «Про основні засади забезпечення кібербезпеки України»: кіберзлочин **(комп'ютерний злочин) —** 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 як юридичну категорію електронні докази започатковано в 2017 році у Цивільному процесуальному кодексі (ЦПК) України, Господарському процесуальному кодексі (ГПК) України та Кодексі адміністративного судочинства (КАС) України. Натепер накопичено певну судову практику 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).

На даний час йде 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 само 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 обшуку. Варто також зазначити, що постійно з'являються нові види електронних пристроїв, які можуть містити електронні докази.

Сьогодні, і це вже очевидно, коли розглядають традиційні злочини, варто брати до уваги ймовірність наявності й електронних доказів. Тому під час досудового розслідування з'ясовують, чи має потерпілий від злочину комп'ютер, чи підтримує він інтернет-контакти тощо.

Докази вчинення злочину можуть знаходитися в:

- *комп'ютері потерпілого;*
- *інтернет-провайдера, послугами якого користувався потерпілий;*
- *комп'ютері підозрюваного;*
- *інтернет-провайдера, послугами якого користувався підозрюваний;*
- *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) віднесені: текстові і графічні документи; дані у форматах мультимедіа; інформація у форматах баз даних та інші додатки прикладного характеру.

Важливу інформацію можуть містити й тимчасові файли. 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. Проте дані, які містять ці знищені файли, можуть виявитися найціннішими. Особливо, якщо вихідний файл був зашифрований чи документ із текстом був надрукований без збереження на диска, 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.

Надзвичайно багато різноманітної інформації містять сучасні мобільні пристрої — *смартфони, планшети та різноманітні плеєра.*

Крім того, інформацію про факти та обставини, що мають значення для кримінального провадження, можуть містити системи 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.

Варто також зважати на те, що сьогодні значний обсяг інформації зберігається у «хмарних технологіях», тобто поза місцезнаходженням фізичної чи юридичної особи.

Нині для перевірки цілісності даних використовується механізм розрахунку контрольної суми або хеш-суми. **Контрольна сума —** 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.

Означені контрольні суми можна отримати, послуговуючись, наприклад, такою програмою, як **HashTab** (відкрито розповсюджена в мережі Інтернет), яку вважають найбільш ефективною для цього.

Під час роботи з електронними доказами слід дотримуватися таких принципів:

1. *Законність.* Працівники та підрозділів, 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.* Документують будь-які дії, виконувані 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, отримують підтримку фахівців (спеціалістів), забезпечивши, за можливості, їх присутність на місці події.

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

6. *Розумна обережність*. Уникають будь-яких навмисних або ненавмисних дій, які можуть призвести до пошкодження потенційних доказів, представлених у цифровій формі.

До прикладу, правоохоронці 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, приміром, 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. КРИМІНАЛЬНО-ПРОЦЕСУАЛЬНІ ЗАСАДИ ПОШУКУ, ВИЛУЧЕННЯ КОМП'ЮТЕРНОЇ ТЕХНІКИ ТА ІНФОРМАЦІЇ З НЕЇ

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 — 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);

– установлення 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 відповідно до вимог ст. 168 КПК України в 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.

Крім того, слід пам'ятати, що 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 ЕЛЕКТРОННИХ (ЦИФРОВИХ) ДОКАЗІВ (ВИЯВЛЕННЯ, ОГЛЯД, ФІКСАЦІЯ, ВИЛУЧЕННЯ ТА УПАКУВАННЯ НОСІЇВ)

Збирання доказів в електронній формі є достатньо нелегким процесом, що 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.

3.1. 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.

3.2. Інструментарій для збирання електронних (цифрових) доказів

З метою збирання електронних (цифрових) доказів використовують такі інструменти та обладнання:

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;
   – бирки 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.

3.3. Тактика проведення обшуку

Відповідно до ч. 3 ст. 236 КПК України перед початком виконання ухвали (про дозвіл на обшук) слідчого судді особі, яка володіє житлом чи іншим володінням, а за її відсутності — іншій присутній особі повинна бути пред'явлена ухвала і надана її копія. Тому перед початком виконання ухвали на проведення обшуку необхідно забезпечити можливість слідчому оголосити ухвалу про проведення обшуку відповідній особі, вручити її копію.

Підтвердженням оголошення та вручення ухвали є відповідний підпис особи на одному з примірників ухвали про отримання її копії із зазначенням точного часу її отримання.

Оголосивши власнику приміщення, в якому проводиться обшук, ухвалу про проведення обшуку, вручивши її копію, оперативні працівники за дорученням слідчого мають вжити заходів, щоб не допустити залишення будь-якими особами місця обшуку до його закінчення та вчинення будь-яких дій, що заважають проведенню обшуку. Тому оперативні працівники мають заздалегідь бути обізнаними щодо наявності всіх вхідних дверей, у тому числі й аварійних виходів, а також забезпечити їх охорону та належний контрольно-пропускний режим.

На підставі положення ч. 7 ст. 223 КПК України обшук або огляд житла чи іншого володіння особи, обшук особи здійснюється з обов'язковою участю не менше двох понятих незалежно від застосування технічних засобів фіксування відповідної слідчої (розшукової) дії.

Понятими не можуть бути потерпілий, родичі підозрюваного, обвинуваченого і потерпілого, працівники правоохоронних органів, а також особи, заінтересовані в результатах кримінального провадження.

Отже, залежно від місця проведення обшуку, кількості приміщень, які підлягають обшуку, відповідно до законодавства можливо залучення як понятих більш ніж дві особи для одночасного обшуку кількох приміщень за участю слідчих, які проводять обшук, про що робиться відповідний запис у протоколі.

Перебіг і результати проведення обшуку кожного такого приміщення та/або його частини за обов'язковою участю окремого слідчого слідчої групи, не менше двох понятих, працівників кіберполіції (у подальшому мається на увазі працівників як Департаменту кіберполіції (ДКП) НП України, так і регіональних управлінь та територіальних відділів кіберполіції), власника приміщення або іншого володіння особи та/або його уповноваженого представника, особи, яка займає це приміщення, адвоката, який для участі у цій слідчій дії має надати лише вичерпний перелік документів, що підтверджують його повноваження на надання правової допомоги, можливо фіксування в Додатку до протоколу обшуку.

В ньому відображаються:

– назва виду документа: Додаток до протоколу обшуку із зазначенням дати та місця проведення обшуку, реквізитів ухвали слідчого судді, на підставі якої проводиться обшук;

– відомості про слідчого, працівників кіберполіції, власника житла чи іншого володіння особи та/або його представника, особи, яка займає вказане приміщення, адвоката — у разі його допуску до проведення слідчої дії, понятих, які присутні під час обшуку такого приміщення;

– спосіб фіксації перебігу та результатів обшуку у відповідному приміщенні та/або його частині, найменування технічних засобів, за допомогою яких здійснюється фіксація, відомості про особу, що здійснює таку фіксацію, носій інформації, на який здійснюється запис відео-файла, а також відомості про долучення оригіналу носія цифрової інформації, що містить відео файл результату проведеної слідчої дії, спосіб його упакування;

– відомості про наявність або відсутність клопотання будь-кого з учасників про застосування технічних засобів фіксації. У разі його заявлення необхідно зазначити час, коли фактично таке клопотання було заявлено, що засвідчується підписами понятих, та зазначають у додатку про порядок, умови застосування технічних засобів фіксації, особу, яка буде здійснювати таку фіксацію, носій інформації, на який записуватиметься відео-файл;

– період часу, проведення обшуку такого приміщення та/або його частини;

– перелік та найменування предметів, речей, документів із зазначенням їхніх облікових номерів, які виявлені та вилучаються під час обшуку, спосіб їх упакування;

– відомості про те, що складений Додаток до протоколу обшуку містить відомості про перебіг та результати проведення обшуку в певній частині приміщення в конкретний період часу, а також відомості про те, що складений Додаток є невід’ємною частиною протоколу обшуку.

Кожний аркуш такого додатка надається для ознайомлення понятим, присутнім, учасникам обшуку, які, ознайомившись з його змістом, своїми підписами засвідчують факт відповідності наявних записів фактично виконаним діям.

Разом із цим, обшук проводиться з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення зокрема електронних доказів, відшукання знаряддя кримінального правопорушення або майна, здобутого в результаті його вчинення, а також встановлення місцезнаходження розшукуваних осіб.

Зважаючи на те, що відповідно до ч. 3 ст. 223 КПК України слідчий, прокурор вживає належних заходів для забезпечення присутності під час проведення слідчої (розшукової) дії осіб, чиї права та законні інтереси можуть бути обмежені або порушені. Перед проведенням слідчої (розшукової) дії особам, які беруть у ній участь, роз'яснюються їх права і обов'язки, передбачені цим Кодексом, а також відповідальність, встановлена законом.

У разі проведення обшуку в житлі чи нежитлових офісних приміщеннях власниками таких приміщень можуть бути встановлені камери відеоспостереження. У такому разі працівникам оперативного підрозділу на місці необхідно своєчасно зорієнтуватися та виявити всі такі камери відеоспостереження, про що терміново доповісти слідчому.

Необхідно пам'ятати, що згідно з ч. 1 ст. 222 КПК України відомості досудового розслідування можна розголошувати лише з дозволу слідчого або прокурора і в тому обсязі, в якому вони визнають можливим.

Щоб унеможливити розголошення відомостей досудового розслідування оперативні працівники за дорученням слідчого мають вжити заходів щодо запобігання відеофіксації під час слідчої дії сторонніми камерами відеоспостереження. Як один із таких заходів є тимчасове заклеювання перед її початком об'єктивів встановлених на об'єкті слідчої дії камер відеоспостереження чорною липкою стрічкою аби власники таких камер не могли розголосити без відповідного дозволу відомостей, отриманих під час проведення такої слідчої дії, виклавши відеофайли у мережу Інтернет, передавши їх до ЗМІ, що може зашкодити інтересам досудового розслідування.

Разом із тим, відповідно до ч. 1 ст. 107 КПК України рішення про фіксацію процесуальної дії за допомогою технічних засобів під час досудового розслідування, приймає особа, яка проводить відповідну процесуальну дію. За клопотанням учасників процесуальної дії застосування технічних засобів фіксування є обов'язковим. Відповідно до змін, внесених Законом України від «Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування» виконання ухвали слідчого судді, суду про проведення обшуку **в обов'язковому порядку фіксується за допомогою звуко- та відеозаписувальних технічних засобів**.

Право безперешкодного фіксування проведення обшуку за допомогою відеозапису надається стороні захисту.

Крім того, дії та обставини проведення обшуку, не зафіксовані у записі, не можуть бути внесені до протоколу обшуку та використані як доказ у кримінальному провадженні.

Отже, у разі заявлення будь-яким учасником обшуку чи власником приміщення, в якому проводиться обшук, клопотання про застосування технічних засобів фіксування, така фіксація є обов'язковою.

Важливим є момент заявлення такого клопотання, у зв'язку з чим необхідно звернути увагу на час заявлення такого клопотання учасником слідчої дії чи особою, яка є власником приміщення, де проводиться обшук. Відомості про час заявлення такого клопотання та про початок застосування технічних засобів фіксації необхідно занести в протокол обшуку.

При цьому учасники обшуку та присутні заздалегідь повинні бути поінформовані про здійснення відеофіксації, обладнання, за допомогою якого вона буде здійснюватися, а також зовнішній носій інформації, на який буде здійснюватися відповідний запис, оригінал якого після завершення слідчої дії долучається до протоколу обшуку.

Оперативним працівникам слід пам'ятати, що в разі, якщо на місце проведення обшуку з'являється особа, яка називає себе адвокатом та вимагає пропустити її до місця проведення обшуку, слід звернути увагу на те, що відповідно до ст. 50 КПК України повноваження захисника на участь у кримінальному провадженні підтверджується:

- свідоцтвом про право на зайняття адвокатською діяльністю;
- ордером, договором із захисником або дорученням органу (установи), уповноваженого законом на надання безоплатної правової допомоги.

Оглянувши свідоцтво адвоката про право на зайняття адвокатською діяльністю, необхідно переконатися в тому, що воно не є підробленим, для чого за допомогою відомостей офіційного сайту http://erau.unba.org.ua необхідно здійснити пошук адвоката за його прізвищем, іменем, по батькові, або за допомогою номера свідоцтва та переглянути його профіль.

До того ж потрібно попросити в адвоката, крім свідоцтва про право на зайняття адвокатською діяльністю документ, який посвідчує його особу.

Установивши особу адвоката, необхідно уважно дослідити наданий адвокатом договір на надання правової допомоги. У цьому договорі необхідно звернути увагу на такі відомості:

– дата та час його укладення;

– термін дії договору;

– анкетні дані особи, з якою укладено договір;

– зміст договору, тобто якій саме особі адвокат уповноважений надавати правову допомогу та в яких справах, чи уповноважений він представляти інтереси певної особи під час проведення слідчих дій у кримінальному провадженні;

– якщо термін дії договору не зазначено, необхідно поставити адвокату питання: яким чином він може підтвердити те, що наданий ним договір не було

розірвано або визнано судом недійсним у цивільному порядку, чи може він надати такі відомості.

Якщо в наданому адвокатом договорі відсутній підпис особи, якій адвокат має намір надати правову допомогу, то адвокат не має правових підстав для її надання, а допуск такої особи до місця проведення обшуку є недопустимим, окрім випадків, коли особа самостійно заявить клопотання слідчому про надання їй правової допомоги адвокатом.

При цьому, особа має самостійно зазначити, якого адвоката вона бажає, та чи бажає вона користуватися послугами саме цього адвоката, який намагається проникнути до місця проведення обшуку.

До того ж можуть мати місце випадки потрапляння адвокатів в приміщення, де проводиться обшук, під виглядом кур'єра приватної служби з доставки кореспонденції або під іншим виглядом. Тому потрібно своєчасно реагувати на такі спроби та роз'яснювати таким особам, що в приміщенні проводиться слідча дія, доступ до цього приміщення можливий лише після її закінчення.

Вживши першочергових заходів, 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 під час проведення обшуку 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 (старший слідчо-оперативної групи) 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.

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, вносяться до протоколу обшуку.

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, із долученням бирок 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.

3.4. Джерела 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 і виїмки потрібно:

– 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.

3.4.1. Алгоритм дій під час 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 файл-еталон 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.

3.4.2. Алгоритм дій під час 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.

3.5 Фіксація електронних (цифрових) доказів

Складність сучасних комп’ютерних інформаційних систем, технологій обробки цифрових даних потребує застосування засобів і технологій правоохоронного призначення, які повинні забезпечити:

– унеможливлення запису будь-яких даних або здійснення інших змін на носієві, що підлягає дослідженню на наявність слідів злочинної діяльності;

– максимальну універсальність підключення різних типів апаратних комп’ютерних засобів, периферійного устаткування;

– функціональну підтримку програмними засобами огляду комп’ютерних даних, визначення чи перевірки контрольних файлів, копіювання даних на фізичному рівні їх представлення і запису на іншому носієві.

З технічної точки зору **для фіксації** доказів в електронній формі можна визначити два основні способи:

– фіксація на аналоговому матеріальному носієві, властивості якого характеризуються безпосереднім і, як правило, відносно незмінним відображенням інформації (фото- та відеозапис);

– фіксація на комп’ютерному носієві, фізичні властивості якого використовуються не для безпосереднього відображення інформації, а для запису-зчитування дискретних станів електромагнітного поля опосередковано через аналогово-цифровий перетворювач.

Безумовно, сьогодні створені й успішно використовуються у правоохоронній практиці різноманітні спеціалізовані апаратно-програмні комп’ютерні засоби для формування образів дисків та інших заходів комп'ютерної криміналістики, серед яких, наприклад, EPOS DiskMaster, Tableau TD3 Forensic Imager та багато інших. Але, нажаль, вони не досить розповсюджені в практичних правоохоронних підрозділах.

Тому для вирішення завдань найбільш розповсюдженої процесуальної дії щодо комп’ютерної техніки — огляду, в правоохоронній практиці, за статистикою, найчастіше застосовують відповідне типове програмне забезпечення, більшість із яких не пов’язані з високою складністю і можуть бути використані правоохоронцями, які не мають глибоких технічних знань у сфері інформаційних технологій.

З огляду на це, для вирішення вказаних вище завдань пропонується використовувати дистрибутив операційної системи **Ubuntu**, пристосований для потреб провадження огляду локальних комп'ютерних засобів та віддалених ресурсів комп'ютерних мереж. Дистрибутив «Ubuntu cyber-crime» застосовується у вигляді ISO-файла. Нова версія дистрибутиву виходить двічі на рік.

Після запису цього ISO-файла на оптичний носій інформації DVD диск, який не підлягає перезапису, створюється Live-DVD варіант операційної системи, яка може відтворюватися в оперативній пам'яті комп'ютерного засобу і не залежить від наявності або відсутності жорсткого диска комп'ютера, не вносить будь-яких змін до цього носія, якщо він є, але робить можливим огляд інформації, вміщеної на всіх приєднаних до комп'ютера носіях.

До дистрибутиву входить стандартний для Ubuntu 16.04 набір програмного забезпечення, який доповнено:

1. Програмою для запису відеограм екрана монітора «XvidCap Screen Capture».

2. Програмою для підрахунку контрольних сум «Hash Checker».

3. Програмою для віддаленого керування операційними системами Windows «Tsclient 0.150» із підтримкою протоколу RDP (Remote Desktop Protocol — протокол віддаленого робочого столу).

4. Програмою автоматичного збирання інформації про апаратне і програмне забезпечення комп'ютерного засобу.

5. Програмою для форматування підключених носіїв.

З огляду на слідчу ситуацію, вид носія інформаційної системи, електронний доказ та інші обставини слід здійснити підбір програмних засобів, що адекватно відповідають поставленим завданням розслідування. Комплект програмного забезпечення, як правило, має бути остаточно відтворений у вигляді образу оптичного диска (файла з розширенням *.iso, *.mdx, *.nrg або інших поширених форматів), для якого необхідно визначити контрольну суму.

Для забезпечення можливості підтвердження достовірності роботи програми підрахунку контрольних сум якій відводиться найважливіша роль засвідчення цілісності та автентичності зібраних доказів, необхідно створити файл-еталон.

З метою **матеріалізації носія даних запис образу оптичного диска** необхідно здійснити мінімум у 2-ох примірниках на носії відповідного типу (CD або DVD), що не підлягають перезапису. Слід зважити на те, що інформація, яка міститься навіть на неперезаписаному носієві, може бути пошкоджена під час його використання. Один із примірників має бути контрольний, інший (інші) — робочий (робочі). Контрольний примірник диска необхідно упакувати так, щоб унеможливити доступ до нього, та здійснити його опечатування стандартним шляхом.

Інформацію про процедуру створення оптичних дисків та опечатування контрольного примірника необхідно внести до протоколу із зазначенням контрольної суми використаного образу оптичного диска.

Під час проведення слідчої дії використовується лише **робочий примірник носія** даних. Після завантаження операційної системи з Live-дистрибутиву необхідно створити файл, контрольну суму якого порівняти з контрольною сумою еталонного файла, що відома заздалегідь.

Після того, як за результатами огляду будуть утворені окремі файли (скриншот, відеограма зображення монітора, образ носія та інші файли з орієнтувальною і доказовою інформацією), їх необхідно скопіювати у двох примірниках, створивши таким чином контрольний та робочий примірники отриманих доказів. Перед копіюванням цих файлів потрібно підрахувати їх контрольні суми, які внести до протоколу огляду. Контрольний примірник отриманих доказів необхідно упакувати так, щоб унеможливити доступ до нього, та здійснити його опечатування стандартним шляхом, про що також зазначити у протоколі.

Отже, після закінчення слідчої дії, крім робочих примірників усіх програмних засобів, а також даних, що вміщують доказову інформацію, до протоколу також **обов'язково мають бути долучені**:

– контрольний примірник програмного засобу, що використаний для виявлення, копіювання і записування досліджуваних даних на інший носій, а також контрольний примірник файла-еталона;

– контрольний примірник носія, що містить файли з доказовою інформацією;

– безпосередньо сам носій, що був об'єктом огляду (у разі наявності специфічних слідів, які потребують дослідження в лабораторних умовах).

Зазначені контрольні примірники повинні забезпечити можливість повторної (експертної) перевірки зафіксованих електронних доказів у разі можливих сумнівів щодо їх цілісності, автентичності та ін.

Під час огляду місця події звертають увагу на апаратні об'єкти, які містять: персональні комп'ютери (настільні, портативні), периферійні пристрої, мережеві апаратні засоби (сервери, робочі станції, активне обладнання, мережеві кабелі тощо), інтегровані системи (органайзери, мобільні телефони, інші гаджети), вбудовані системи на основі мікропроцесорних контролерів, а також електронні носії даних: мікросхеми пам'яті, магнітні і лазерні диски, магнітооптичні диски, магнітні карти, флеш-пам'ять, пластикові картки та ін.

За умови, коли слідча або оперативно-тактична ситуація вимагає невідкладного проведення огляду даних на комп'ютерному засобі, який був використаний для вчинення злочину, а його безпосереднє вилучення неможливе або недоцільне (наприклад, якщо комп'ютерний засіб неможливо вилучити

фізично — він вбудований у сейф, його корпус закріплений таким чином, що для вилучення необхідно руйнувати частину приміщення, або таке вилучення призведе до значних матеріальних збитків для підприємства, банківської установи, або комп'ютер застосовується як хостінг-сервер, на якому зберігаються сайти сторонніх осіб, такий огляд необхідно здійснювати з використанням дистрибутиву в порядку, розглянутому вище.

Спеціаліст з підрозділу кіберполіції повідомляє слідчого, учасників слідчої дії, понятих та присутніх про копіювання (знаття так званого дампу) оперативної пам'яті, браузера з історією, логінами, паролями, копіювання файлів месенджерів та даних щодо відомих мереж, до яких здійснювалося підключення, і паролів до них. Після цього з дозволу слідчого здійснюється таке копіювання. При цьому спеціаліст кіберполіції повідомляє присутнім та учасникам слідчої дії про інформацію, яка підлягає копіюванню, її місцезнаходження на носії інформації, програмне забезпечення, за допомогою якою здійснюється таке копіювання, із зазначенням умов його ліцензування, зовнішнього носія інформації, на який здійснюється та в подальшому здійснюватиметься копіювання такої інформації, його серійних, ідентифікаційних чи інвентарних номерів.

Після завершення копіювання спеціаліст кіберполіції демонструє всім учасникам обшуку та присутнім на екрані адресу зовнішнього носія інформації, на який здійснено копіювання файлів, оголошує найменування та кількість скопійованих файлів, їхні розміри, після чого здійснюється від'єднання зовнішнього носія інформації від пристрою, з якого проводилося копіювання, та його упаковування й опечатування биркою з коротким описом комп'ютерного обладнання, з якого було здійснено таке копіювання, із зазначенням на бирці облікового номера в протоколі обшуку.

У разі наявності інформації, яка підлягає доказуванню в кримінальному провадженні, необхідно доручити спеціалісту кіберпоіції **зберегти скріншоти вікон та (або) файлів**. Спеціаліст кіберполіції повідомляє про обставини такого збереження, інформуючи учасників обшуку, присутніх та понятих усі виконані ним операції чи команди, які ним були здійснені для збереження таких скріншотів.

Ця інформація заноситься до протоколу обшуку.

За необхідності потрібно виготовити файл-образ усього жорсткого диска персонального комп'ютера (ПК) чи іншого комп'ютерного засобу, про що детально відобразити в протоколі обшуку із зазначенням:

– відомостей про жорсткий диск ПК, файл-образ якого необхідно створити;

– програмного забезпечення та умови ліцензування програмного забезпечення, за допомогою якого здійснюється таке копіювання;

– зовнішнього носія інформації, на який здійснюється таке копіювання, із зазначенням його ідентифікаційних ознак (серійних чи інвентарних номерів тощо);

– період часу, за який виготовлено такий образ жорсткого диска ПК.

Після завершення створення файл-образу спеціаліст кіберполіції демонструє учасникам обшуку, присутнім та понятим факт створеного образу, описує скопійовані файли із зазначенням їх властивостей, розміру та інших даних, про що вказується в протоколі обшуку.

У разі, коли екран пристрою заблоковано, за можливості слід з'ясувати пароль користувача, а також встановити, чи увімкнене шифрування диска.

Якщо пароль доступу не надається та є впевненість у тому, що шифрування диска не застосовується, а присутнє лише блокування екрана, то слідчий доручає працівнику кіберполіції перезавантажити ПК та завантажитись у Live-режимі з будь-якого Linux-дистрибутиву, який після завершення завантаження надасть змогу переглядати та копіювати усю файлову систему даного ПК за допомогою провідника.

Якщо пароль доступу не надається та застосовується шифрування диска, то слідчий доручає працівнику кіберполіції виготовити дамп оперативної пам'яті з метою відшукування паролів, що зберігаються у ній, до моменту вимикання.

Для здійснення зазначеного можуть бути застосовані або спеціалізовані апаратно-програмні засоби, наприклад, акселератор Tableau TACC1441, або окремі багатофункціональні та спеціалізовані програмні пакети й утиліти.

Прикладом такого програмного засобу є, наприклад, **«Multi Password Recovery, MPR» —** багатофункціональна програма для Windows з розшифрування і тестування паролів на стійкість. Програма MPR автоматично знаходить і миттєво розшифровує паролі із більш ніж 110 популярних програм (FTP, E-mail клієнти, Інтернет пейджери, браузери та ін.), не потребуючи при цьому втручання користувача. Крім розшифрування, MPR показує паролі під зірочками, дозволяє скопіювати SAM-файл (де зберігаються паролі адміністратора і користувачів ОС Windows, такий файл неможливо прочитати чи скопіювати стандартними засобами. MPR дозволяє скопіювати SAM файл для подальшої обробки альтернативними програмами), видалити збережені паролі, згенерувати новий пароль, зберегти звіти на диск.

Усі свої дії та результати кожної операції працівником кіберполіції послідовно та детально повідомляються учасникам обшуку, присутнім, понятим та слідчому з метою повного, своєчасного та якісного їх відображення в протоколі обшуку та/або додатках до нього.

Після обшуку вилучені предмети, речі та документи в упакованому вигляді пред’являються учасникам обшуку, понятим та присутнім.

Складається повний текст протоколу обшуку та додатків до нього, які надаються кожному учаснику обшуку для особистого ознайомлення та підпису.

Оригінал носія інформації, на який здійснювався технічний запис перебігу та результатів проведеної слідчої дії, долучається до протоколу обшуку, про що в протоколі робиться відповідний запис.

У протоколі, відповідно до вимог ст. 104 КПК України, обов'язково повинно бути відображено конкретне місцезнаходження комп’ютера та його периферійного обладнання, обстановка та інші обставини, що можуть мати істотне значення для справи.

Слідчий повинен організувати забезпечення цілісності та збереження даних на ПК, які підлягають вимкненню з мережі живлення, для їх вилучення в ході проведення обшуку або іншої слідчої дії, а в разі неможливості вимкнення ПК з мережі живлення слідчий зобов’язаний організувати невідкладне копіювання даних в ході проведення обшуку або іншої слідчої дії, керуючись ч. 4 ст. 99 КПК України (дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також 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)

Порядок фіксації комп’ютерних слідів на віддалених ресурсах у мережі Інтернет, загалом тотожний з описаним вище. Алгоритм дій відрізняється лише специфікою процесу доступу до ресурсів і програмного забезпечення, призначеного для виконання цього завдання.

Предметом огляду також є комп’ютерна інформація, збережена або відтворена на носіях інформації, з’єднання з якими відбувається каналами телекомунікаційного зв’язку за правилами та технічними протоколами функціонування комп’ютерних мереж та мережі Інтернет.

Слідчий зобов’язаний також вживати заходів щодо забезпечення надійного збереження даних щодо доступу до крипто-гаманців (логінів, паролів тощо) та крипто-валюти, яка міститься на крипто-гаманцях, виявлених на ПК, мобільних пристроях тощо в ході проведення обшуку або інших слідчих дій.

3.6. Електронні (цифрові) докази в мережі Інтернет

Надзвичайно велика кількість електронних даних знаходиться в **глобальній комп’ютерній мережі Інтернет** (відповідно до чинної редакції Закону України «Про телекомунікації», Інтернет — всесвітня інформаційна система загального

доступу, яка логічно зв'язана глобальним адресним простором та базується на інтернет-протоколі, визначеному міжнародними стандартами).

Інтернет об’єднує між собою локальні, регіональні комп’ютерні мережі та окремі комп’ютерні системи на основі **протоколів TCP/IP** (Transmission Control Protocol/ Internet Protocol) та утворює **кіберпростір,** який слугує фізичною основою доступу до різноманітної електронної інформації. Однією з особливостей глобальної мережі є відсутність географічних та державних кордонів.

Управління глобальною мережею Інтернет не здійснюється одноосібно певною організацією чи державою.

Вирішує технічні питання Internet Activities Board (IAB), розробляє протоколи — Internet Engineering Task Force (IETF), **стандарти WWW (**World Wide Web), через які здійснюється обмін між комп’ютерами завдяки протоколу HTTP (Hypertext Transfer Protocol), розробляє WWW консорціум — World Wide Web Consortium.

Важливу роль в організації діяльності мережі Інтернет відіграє корпорація ICANN (Internet Corporation of Assigned Names and Numbers), до завдань якої належать координація систем унікальних ідентифікаторів мережі, присвоєння доменних імен (DNS, Domain Name System — Доменна система імен) що являє собою ієрархічну розподілену систему перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу. Проте зазвичай інтернет-користувачі реєструють нові імена сайтів через регіональних інтернет-реєстраторів або через провайдерів.

Провайдери Інтернет-послуг (**ISP —** Internet Service provider) **—** це організації, які надають доступ до мережі Інтернет (як безкоштовно, так і на платній основі).

Відповідно до діючого законодавства провайдери Інтернет-послуг є суб'єктами господарювання, які мають право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку. Вони не зобов'язані отримувати відповідну ліцензію на право здійснення телекомунікаційних послуг.

На відміну від них **оператор телекомунікацій —** суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж (зобов'язаний отримати ліцензію).

Провайдер хоч і може обійтися без ліцензії, в той же час зобов'язаний укласти договір на обслуговування мережі з оператором телекомунікацій, який

має ліцензію на обслуговування мережі в тому ж населеному пункті, в якому надає послуги провайдер.

Провайдери можуть також надавати на своїх потужностях послугу хостингу, що включає надання дискового простору, підключення до мережі та інших ресурсів для розміщення фізичної інформації на сервері, що постійно перебуває в мережі Internet, для того, щоб зберігати інформацію (сайтів, електронної пошти тощо), створювати різноманітні сервіси, наприклад для обміну повідомленнями (Chat room — Internet Relay Chat — IRC), «хмарних технологій», функціонування інтернет-магазинів тощо.

Постачальник послуг хостингу — особа, яка надає власникам веб-сайтів послуги і (або) ресурси для розміщення веб-сайтів або їх частин у мережі Інтернет та із забезпечення доступу до них через мережу Інтернет.

Власник веб-сайта, який розміщує свій веб-сайт або його частину в мережі Інтернет на власних ресурсах і (або) самостійно забезпечує доступ до нього з використанням мережі Інтернет, одночасно є постачальником послуг хостингу.

Користувачі широко використовують послуги міжнародних провайдерів, таких, наприклад, як Google, Yahoo та ін. Особливе значення для безперебійної роботи мережі мають організації, що володіють базовою інфраструктурою Інтернет, наприклад Укртелеком, Київстар, Vodafone, Інтертелеком тощо.

Існує кілька видів фізичних каналів зв’язку з мережею Інтернет: зв'язок через телефонну лінію за допомогою xDSL модему, оптоволоконний кабель, бездротовий зв'язок Wi-Fi та WiMAX, супутник, канали мобільного зв’язку тощо.

При документуванні ознак комп’ютерної інформації як предмета злочину встановлюються особи, які є **власниками** чи **розпорядниками** або **користувачами** інформації. Це саме стосується й власника, розпорядника та користувача комп’ютерної системи, яка зазнала кібератаки чи була знаряддям вчинення злочину.

Інформація, доступна в мережі Інтернет, у тому числі й та, що на веб-сайтах, фізично розміщена на комп’ютерному обладнанні, об’єднаному каналами зв’язку з цією мережею, та має свій ідентифікатор **— IP-адресу**, що складається з чотирьох груп цифр (октетів) у діапазоні від 0 до 255, розділених крапками, наприклад, **ip-addr: 195.47.253.2**. Така версія IP-адреси носить назву четвертої версії інтернет-протоколу — IPv4.

Унікальність IP-адрес забезпечується централізованим розподілом діапазонів адрес Адміністрацією адресного простору Інтернет (Internet Assigned Numbers Authority **— IANA**) між регіональними інтернет-реєстраторам (Regional Internet Registries **— RIR**), які розподіляють IP-адреси серед провайдерів.

До регіональних інтернет-реєстраторів RIR належать організації:

– RIPE (Європа і деякі частини Азії);

– APNIC (Азія і Тихоокеанський регіон);

– ARIN (Північна Америка);

– LACNIC (Латинська Америка та Карибський регіон);

– AfriNIC (Африка).

Існує також шоста версія інтернет-протоколу — IPv6-адреси. IPv6-адреса складається з восьми блоків, кожен з яких включає по чотири шістнадцяткові цифри; блоки розділені двокрапкою (наприклад ipv6-addr: **2001:67c:258:2**). Це дає змогу значно збільшити кількість IP-адрес.

Слід наголосити, що будь-який пристрій, підключений до мережі, також має свою унікальну апаратну адресу — **MAC-адресу** (Media Access Control address, MAC-address), тобто адресу управління доступом до середовища. MAC-адреса — унікальне 48-бітне число, запрограмоване виробником під час його виробництва, що складається з шести частин із чисел у шістнадцятковому вигляді.

Приклад MAC-адреси — 01:B7:A3:OB:E1:19.

Унаслідок обмеженої кількості IP-адрес провайдери використовують динамічні IP-адреси (Dynamic IP Address) завдяки протоколу динамічного налаштування вузла (Dynamic Host Configuration Protocol — **DHCP**). Щоразу, коли пристрій зв'язується з мережею Інтернет, **DHCP-сервер** надає його MAC-адресі вільну IP-адресу зі списку наявних адрес. Це треба мати на увазі під час розслідування правопорушень у мережі Інтернет, бо на відміну від статичних IP-адрес, які надаються конкретному пристрою постійно, динамічні адреси можуть бути різними в різний час.

Тому при ідентифікації певного пристрою за IP-адресою набуває важливого значення час з'єднання з глобальною мережею, який потрібно вказувати у запитах провайдеру з урахуванням Всесвітнього координованого часу — UTC. Київський час відрізняється від UTC на +2 години взимку та на +3 — улітку IP X.X.X.X 24/05/2017 16:35:11 (UTC+2).

Фізично інтернет-повідомлення передаються в потрібному напрямку завдяки **роутерам —** пристроям, які відкривають IP-пакети даних (кожне повідомлення поділяється на кілька IP-пакетів), зчитують адресу, на яку направляються повідомлення, та передають їх найближчим шляхом. Одне інтернет-повідомлення, наприклад, електронний лист, може надійти до адресата різними шляхами пересилання IP-пакетів.

Водночас веб-сайти мають свої власні веб-адреси алфавітно-цифрового позначення — Єдиний покажчик ресурсу (**Uniform Resource Locator, URL)**, що є зручним для запам'ятовування користувачами, наприклад, http://www.naiau.kiev.ua (сайт Національної академії внутрішніх справ). Переведення алфавітно-цифрових назв сайтів та електронних адрес (включно написаних кирилицею) до IP-адрес здійснюється за допомогою системи DNS — Domain Name System.

Розрізняють домени трьох рівнів.

Домени першого рівня вказують на належність сайта до певної країни, наприклад:

– Ua —Україна, kyiv.ua — Київ;

– Us — США;

– Pl — Польща,

або тип організації, яка використовує домен:

– Gov — державні;

– Com — комерційні;

– Edu — навчальні тощо.

Домени другого рівня реєструються в зонах першого рівня та відділяються від назви географічної зони крапкою: zabota.ua, vuz.com

Домени третього рівня реєструються в попередніх доменах, наприклад secretar.rabota.ua.

Електронні докази в мережі Інтернет можуть міститися на веб-сайтах, електронній пошті, соціальних мережах, різноманітних форумах, у пошукових системах інформації тощо.

Здебільшого електронна інформація мережі Інтернет зберігається у вигляді **веб-сторінок**, які складаються з окремих електронних документів, що містять дані у вигляді тексту, графічних зображень, електронних таблиць, відео тощо і можуть бути переглянуті за допомогою спеціальних комп'ютерних програм — веб-переглядачів (браузерів): Internet Explorer, Mozila Firefox, Google Chrome, Opera та ін.

Сукупність веб-сторінок, об'єднаних за змістом та навігацією і розміщених за певною мережевою адресою, називається **веб-сайтом** (website).

Першим видом доказів, які можна отримати з веб-сайта, є його видимий, а другим, відповідно, невидимий зміст. Невидимий зміст — це мова програмування або його код (HTML, CSS, Javascript та ін.), що використовується для створення веб-сторінки, і фактичний зміст, який сервер направляє в браузер (програма для перегляду сайтів), а браузер його дешифрує і використовує для відображення веб-сторінки на екрані.

Код сайта допомагає отримати електронні докази щодо особливостей фактичної інформації цього сайта.

Існують також **метадані**, які можуть бути джерелом високотехнічної інформації про саму веб-сторінку. Найпростіший приклад — інформація про дату останньої модифікації веб-ресурсу (веб-сторінки, зображення і т.д.).

Таку інформацію можна отримати за допомогою безкоштовного додатка **FireBug** для Google Chrome, а також інших аналогічних програм, наприклад, **NetAnalysis®**, яка розроблена спеціально для веб-браузера судово-медичної

експертизи і підтримує всі основні настільні і мобільні браузери, проводить аналіз історії, кеш, кукі тощо, має потужні можливості створення звітів, що дозволяє швидко отримувати докази, які стосуються діяльності користувача.

Це програмне забезпечення також має потужні аналітичні інструменти, які допомагають розшифрувати і аналізувати дані.

«**BrowsingHistoryView**» **—** невелика безкоштовна програма, яка дає змогу отримати доступ до даних таких браузерів, як Internet Explorer, Mozlla Firefox, Google Chrome, Safari і відображає історію відвідування веб-сайтів у загальній таблиці. Утиліта надає інформацію про адресу відвідуваного сайта, його назву, дату і час відвідування, використовуваний браузер, профіль користувача тощо.

Додаток дозволяє проглядати історію відвіданих сторінок для будь-якого профілю користувача, зареєстрованого в системі. Є можливість експортувати отримані результати в CSV-, HTML- та XML-файл.

Під час опитування потерпілих від правопорушень, пов'язаних з використанням веб-сайтів, слід ставити такі запитання:

– яка адреса сайта (URL) (наприклад, www.ruscrime.com)?

– коли був сеанс перегляду сайта?

– чи зберіглася прінт-копія сторінки сайта?

– чи зберіглася електронна копія сайта? (якщо так, необхідно скопіювати файл).

Важливе значення при розгляді електронних даних у суді має їх достовірність.

Тому, крім зберігання копії екрана на основі функції **Print screen — PrtSc**, для збереження даних веб-сторінки доцільно використовувати функцію браузера «Зберегти як», при виконанні якої зберігається код веб-сторінки.

Також здійснюється **запис на телекамеру операції щодо відкриття сайта**, при цьому одночасно відкривається певний відомий сайт, звідки фіксується дата та час перегляду. Можливе використання і спеціальних програм, які створюють записи екрана монітора.

Для пошуку інформації про реєстратора доменного імені сайта, провайдера, місця розміщення сайта (його IP-адреси), адміністратора сайта використовується система "Whois" **—** http://Whois.com. Для отримання вказаної інформації використовуються також інші програмні засоби, наприклад, https://whoer.net/ru, www.domaintools.com, http://centralops.net тощо.

Знаючи IP-адресу комп'ютера підозрюваної особи та розуміючи правила надання доменних імен і хостингу, можна також, здійснивши зворотний пошук по Whois, побачити всі DNS/IP-записи, зареєстровані на зазначену особу.

Існує можливість пошуку за іменем, за адресою електронної пошти, номером телефону або фізичною адресою.

Пошук за IP-адресою також дає змогу визначити країну, на території якої розміщений сайт, місто, геолокацію тощо (2ip.ua). За однією IP-адресою може знаходитися декілька сайтів (на одному комп'ютері розміщено декілька програм).

Існують сервіси, наприклад, whoer.net/ru, які дають можливість переглянути всі сайти з однієї IP-адреси. Їх аналіз може надати додаткові відомості, необхідні для розслідування.

Водночас існує можливість фізичного розміщення сайта (хостінг) в іншому від провайдера місці та навіть в іншій країні. Для його визначення необхідно звертатися до провайдера — адже він здійснює відповідні налаштування.

IP-адресу конкретного комп'ютера, який працює під управлінням системи Windows7, можна отримати, якщо зайти в «Панель управління», вибрати закладку «Мережа та Інтернет», потім вибрати пункт «Інтернет підключення по локальній мережі», в якому в підпункті «Відомості» міститься інформація про IP-адресу цього комп'ютера. За допомогою сервісу http://www.bravica.net/ru/net-provider.html, https://whoer.net/ru, 2ip.ua можна визначити провайдера (Internet Service Provider, ISP) , що надає інтернет-послуги.

Для **ідентифікації IP-адреси конкретного веб-сайта** можна використати утиліту Ping або скористатися сервісом 2ip.ua.

Залежно від версії операційної системи, існують кілька способів її виконання. Найпростіший спосіб, наприклад, у версії Windows7 — натиснути клавіші «Windows»+R, після чого ввести команду ping пробіл та адресу сайта, а потім натиснути клавішу «Enter».

Також **для отримання детальної інформації** про користувача мережі, адміністратора сайта, реєстратора доменного імені тощо необхідно надіслати відповідний запит провайдеру послуг або, **якщо електронні дані знаходяться в юрисдикції іншої держави,** необхідно надіслати запит (клопотання) про міжнародну правову допомогу та отримати, наприклад, номер телефону доступу, фізичну адресу, ім'я адміністратора ресурсу тощо.

Підстави та умови надання правової допомоги та процедура написання запитів детально розглянута в **Методичних рекомендаціях щодо виконання вимог міжнародних договорів та КПК України про міжнародну правову допомогу при проведенні процесуальних дій у кримінальному провадженні** від 20 квітня 2017 р., розміщених на сайті Генеральної прокуратури України (http://www.gp.gov.ua для зареєстрованих користувачів).

На практиці оперативному працівнику або слідчому доводиться мати справу з об'єднанням різних сервісів, наприклад, електронні докази можуть міститися в інтернет-магазині, для реєстрації в якому використовуються аккаунт соціальної мережі Facebook, оплата здійснюється через онлайн банкінг Приват24, а інформація надсилається користувачам Twitter або SMS-повідомлення, тобто

електронні докази знаходяться на різних сервісах і в різних провайдерів. Подібні приклади зустрічаються досить часто, проте збирання доказів із різних джерел, незважаючи на певну складність, може бути більш продуктивним, ніж отримання доказів з одного місця.

Електронні докази можна отримати із **соціальних мереж.** Для оперативного працівника або слідчого корисною може стати інформація про **ідентифікатор** підозрюваного (**ID**), а також інформація з листування користувачів та інша інформація, наприклад, зображення, які викладаються користувачами, оскільки вони можуть містити метадані з інформацією про дату та час створення зображення, місце його створення тощо.

Ідентифікатори використовують також і в мережі он-лайн-реклами, приміром, Google. Знаючи ідентифікатор, шляхом надсилання запиту, наприклад до адміністрації банерної мережі про здійснені грошові перекази, можна встановити конкретну фізичну чи юридичну особу, яка замовляла рекламу.

Chat room. Правопорушники досить часто використовують технологію багатокористувацьких конференцій (дискусій) реального часу в текстовому режимі через мережу Інтернет **—** IRC (англ. *Internet Relay Chat*).

Хоча існують тисячі електронних каналів для дискусій, де обговорюються музика, політика, спорт тощо, злочинці можуть використовувати їх для обговорення свого сексуального досвіду, розміщення порнографічних матеріалів, установлення зв’язків із неповнолітніми з подальшим залученням їх до надання сексуальних послуг у реальному світі тощо.

У такому разі необхідно:

− установити назву Chat room;

− з’ясувати «Нік» зловмисника;

− визначити IP-адресу зловмисника;

− роздрукувати діалог зловмисника з потенційною жертвою;

− зберегти електронну копію зображення вікна комп’ютера.

Для фіксування повідомлень у чаті корисним може бути застосування сервісу Simkl (http://simkl.org), який дає змогу використовувати проміжний сервер для відповідних підключень.

Правопорушники широко використовують для спілкування такі месенджери як Skype, Viber та інші.

Ідентифікувати співрозмовника Skype можна за допомогою спеціальних програм, наприклад, Wireshark (www.wireshark.org/download.html) або Skype-resolver (www.skresolver.com).

Дізнатися IP-адресу абонента Viber, аналогічно як і у випадку зі Skype, можна за допомогою Wireshark. Для цього слід також застосувати Viber Desktop (http://viber.com/desktop).

Електронні листи. Злочинці широко застосовують електронні листи для шахрайських схем, спаму, здирництва, шантажу, зараження комп'ютерів вірусами тощо.

У таких випадках у потерпілих необхідно з'ясувати:

− Хто є Інтернет-провайдером?

− Чи існує роздруківка електронного листа?

− Чи збережена копія листа в комп'ютері?

− Яка електронна адреса правопорушника?

Часто вдається виявити злочинця через IP-адресу, яка міститься у заголовках (header) Інтернет-повідомлень, що утворюються при їх передачі.

У таких заголовках міститься інформація про ISP, IP-адресу, дату та час створення повідомлення. Доступ до технічних заголовків електронного листа здійснюється через меню поштового клієнта, який використовується.

Для отримання таких даних необхідно зберегти на накопичувачу електронне повідомлення та надати його Інтернет-провайдеру або в Департамент кіберполіції Національної поліції України для проведення відповідних процесуальних дій.

Встановити окремі відомості про одержувача електронного листа (дату та час прочитання повідомлення, IP-адресу, з якої повідомлення було прочитано) можна за допомогою сервісу https://www.readnotify.com/.

Злочинці намагаються унеможливити виявлення їх справжніх електронних адрес. Для цього вони використовують різні технології забезпечення анонімності роботи в мережі, а також програми безпечної передачі інформації. Ця обставина ускладнює встановлення місцезнаходження контактної особи.

Серед головних способів забезпечення анонімності можуть застосовуватись:

– проксі-сервери (HTTP, SOCKS 5 тощо);

– VPN-сервери;

– TOR та 2IP.

Останнім часом, особливо після блокування російських соцмереж, популярним стало використання VPN-серверів, за допомогою яких забезпечується конфіденційність інформації і приховування IP-адреси користувача. Тому, якщо користувач увійде у «VPN», то зможе дійти тільки до IP-адреси мережі «VPN», але не побачити початкової IP-адреси користувача.

Часто для заплутування слідів злочинці використовують заміну схожих букв в електронних адресах, наприклад, цифра «1» замість латинської літери «l», цифра «0» замість букви «о» тощо. Тому при підготовці запитів до Інтернет-провайдерів потрібно правильно вказувати назви сайтів та адреси електронної пошти, уважно дослідивши і вичитавши їх перед цим.

Для ідентифікації підозрюваного в мережі Інтернет часто необхідно визначити його аккаунт (обліковий запис) у певному Інтернет-сервісі, який зазвичай передбачає введення логіна та пароля).

Маючи аккаунт підозрюваного, необхідно ідентифікувати особу того, хто використовував цей аккаунт під час вчинення правопорушення (адже справжній власник аккаунта міг знаходитися в іншому місці).

У багатьох випадках обмін інтернет-повідомленнями (як злочинців між собою, так і злочинців із потерпілими) не завжди очевидний. Для дослідження таких повідомлень залучають фахівця, оскільки їх можуть знищити як потерпілий, так і злочинець. Проте за допомогою спеціального програмного забезпечення вони відновлюються.

Найпростіше виявити підозрюваного за його реальною e-mail адресою. Проте найчастіше злочинців відстежують через IP-адресу електронних повідомлень. Ці адреси містяться в заголовках кожного інтернет-повідомлення.

Тільки один користувач може мати певну адресу в певний проміжок часу. ISP може ідентифікувати аккаунт, з якого вчинено правопорушення.

Викрадення аккаунтів. Для вчинення правопорушень злочинці часто послуговуються викраденими аккаунтами (так само як і грабіжники користуються викраденими автомобілями для втечі).

Для цього використовують такі способи:

– *"троянський кінь"*. Злочинець надсилає повідомлення із заманливою інформацією (ліки за доступними цінами, як зменшити вагу тощо), в якому міститься комп’ютерний вірус. Пізніше цей вірус отримує необхідні паролі та направляє їх злочинцю;

– *шантаж або викрадення*. Злочинець надсилає листа від імені провайдера або банку та вимагає надати йому відповідні дані для поновлення аккаунту або доступу до мережі Інтернет.

Отримавши ці дані, зловмисник використовує їх для вчинення злочинів від імені невинної особи, тобто іноді, навіть коли існують певні електронні докази, дуже непросто встановити фізичну особу, яка вчинила комп'ютерний злочин через мережу Інтернет. Найчастіше все, що відомо про підозрюваного, — це його IP-адреса, MAC-адреса, адреса електронної пошти, доменне ім'я або інтернет-псевдонім — «нік». Щоб ідентифікувати фізичну особу за IP-адресою, фахівцям потрібні дані, які знаходяться в розпорядженні постачальника інтернет-послуг.

Постачальники інтернет-послуг (електронної пошти, хостінгових послуг) часто є єдиним джерелом інформації, яка дає змогу встановити зв'язок між віртуальною особистістю правопорушника і конкретною фізичною особою.

Тому незалежні власники даних часто виявляються ключовою ланкою в розслідуванні злочинів.

Отримавши аккаунт підозрюваного, необхідно з'ясувати:

– хто реально проживає за вказаною адресою;

– хто отримує традиційну пошту.

Крім того, потрібно отримати список телефонних дзвінків із цієї адреси для з'ясування можливого контакту з інтернет-провайдером, а також визначити, де здійснювався вхід в аккаунт у той час, коли вчинено правопорушення.

Наприклад, аккаунт зареєстровано в м. Києві, а під час вчинення правопорушення вхід здійснений у м. Харкові, що може свідчити про кілька версій, зокрема таких:

– аккаунт викрадений кимось із Харкова;

– аккаунт використовувався друзями або родичами без відома власника;

– власник аккаунту для вчинення злочину приїжджав до Харкова;

– власник аккаунту дозволив спільнику здійснити злочин із Харкова з метою конспірації.

Для ідентифікації підозрюваного використовується кілька методів:

1) простежуються надходження коштів. У разі інтернет-шахрайства необхідно дослідити місце надходження коштів, наприклад картковий рахунок у банку;

2) відслідковуються надходження товарів. За купівлі товарів з використанням викрадених пластикових карток необхідно простежити місце надходження замовлених речей;

3) у провайдера мобільного зв'язку з'ясовується інформація про телефонні дзвінки.

Для отримання інформації від зарубіжних провайдерів варто використовувати можливості контактного пункту "24/7" Департаменту кіберполіції Національної поліції України.

3.7. Загальний порядок вилучення комп'ютерної техніки та її зберігання

При обшуках і виїмках, пов'язаних із вилученням комп'ютерної техніки, магнітних носіїв та інформації, виникає низка питань, пов'язаних зі специфікою технічних засобів, що вилучаються. Так, необхідно передбачати дії злочинців із метою знищення комп'ютерної інформації. Наприклад, вони можуть використати спеціальне обладнання, яке в критичних випадках утворює сильне магнітне поле, що знищує магнітні записи.

З метою запобігання непорозумінням у майбутньому бажано під час вилучення носіїв інформації отримати контрольні суми їх вмісту та обов'язково вказати їх у протоколі.

Під час вилучення комп'ютерів їх слід упаковувати в полімерні пакети, де горловина пакета міцно обв'язується шовковою (капроновою) ниткою і фіксується двома подвійними простими вузлами. Вузли розміщують на діаметрально протилежних сторонах, на які клеється бирка, що містить написи з назвою та характерними особливостями предмета (номер, марка, тип та ін.), що надається, номером кримінального провадження, фабулою події або прізвищем особи, в якої вилучений предмет, місцем (або адресою), датою і часом вилучення, посадою, прізвищем, ім'ям та по батькові, особистим підписом слідчого та прізвищами, іменами та по батькові, особистими підписами понятих, присутніх під час вилучення і пакування, скріпленими печаткою.

Не допускається використання стрейч-плівки та плівкової стрічки з клейовим покриттям для пакування і закріплення паперових бирок із пояснювальними написами**.**

Слід пронумерувати всі носії інформації, а також пакети, в які вони запаковані, проставити відповідні знаки на паперових аналогах інформації.

При складанні протоколу у ньому слід вказувати серійні номери всіх вилучених блоків та їх балансові номери (за відповідною документацією бухгалтерії підприємства, установи, якщо вона наявна). Якщо номери повністю відсутні, треба докладно описати кожний блок відповідно до його індивідуальних ознак.

Для вилучення носіїв їх необхідно упакувати у жорстку негнучку коробку та опечатати її. Усі з'єднання сторін (клапанів) коробів повинні бути обклеєні паперовою стрічкою клейовим способом та скріплені печаткою.

У певних випадках можна використовувати й полімерні пакети, але з огляду на можливість несанкціонованого розрізання пакета за донну частину та потім заварювання його наново, у цьому разі необхідно обов'язково прошивати не тільки саму лише горловину пакета, а й донну його частину.

Далі слід зробити на окремому аркуші паперу докладний опис упакованих носіїв (тип кожного з них, їх кількість).

Коробка з носіями і опис поміщаються в поліетиленовий пакет, де горловина пакета міцно обв'язується шовковою (капроновою) ниткою і фіксується двома подвійними простими вузлами, які розміщують на діаметрально протилежних сторонах.

Кожна упаковка повинна опечатуватися биркою, посвідченою написами з назвою та характерними особливостями предмета (номер, марка, тип та ін.), що надається, номером кримінального провадження, фабулою події або прізвищем особи, в якої вилучений предмет, місцем (або адресою), датою і часом вилучення, посадою, прізвищем, ім'ям та по батькові, особистим підписом слідчого та

прізвищами, іменами та по батькові, особистими підписами понятих, присутніх під час вилучення і пакування, скріпленими печаткою

В окремих випадках, коли необхідно більш детально дослідити пристрої аудіо-, відео-, фотофіксації, спеціалізовані комп'ютери з нестандартним обладнанням (з платами шифрування, застарілими контролерами тощо), пристрої вводу-виводу інформації та ін., слід також вилучати дане обладнання. При цьому може знадобитися відповідний спеціаліст або певні технічні засоби.

Вилучення комп'ютерних засобів повинно проводитись в один прийом.

При перевезенні комп'ютерних засобів необхідно унеможливити їх механічні пошкодження і взаємодію з хімічно активними речовинами. Слід екранувати від впливу магнітних полів як комп'ютерні пристрої, так і магнітні носії. Такий вплив може призвести до пошкодження чи знищення інформації шляхом розмагнічування.

За відсутності автотранспорту слід організувати надійну охорону вилученого обладнання у спеціальному приміщенні.

При розміщенні вилучених об'єктів на зберігання слід дотримуватися встановлених правил зберігання і складування електронних технічних засобів.

Не можна ставити системні блоки у штабель вище трьох штук, а також розміщати на них будь-які інші предмети.

Зберігають комп'ютери і комплектуючі у сухому, теплому приміщенні. Слід довідатися, що у ньому немає мишей чи пацюків, які часто є причиною несправності апаратури. Крім того, категорично забороняється палити, приймати їжу і утримувати тварин у приміщеннях, призначених для зберігання комп'ютерної техніки і магнітних носіїв.

Недопустимо надання вилучених засобів у розпорядження підрозділу поліції, прокуратури, іншої організації (установи) з причин «виробничої необхідності», адже в процесі їх роботи можуть бути внесені зміни у файли інформації чи програми.

Такі дії можуть призвести до пошкодження чи знищення електронних доказів.

Тому неприпустимими є випадки використання вилучених як речові докази комп'ютерних засобів слідчими і оперативними працівниками для складання процесуальних документів, звітів тощо. А винні в таких діях мають нести відповідальність, навіть якщо у слідчому підрозділі вийшли з ладу всі службові комп'ютери.

3.8. Особливості вилучення мобільних пристроїв

Вилучення мобільних пристроїв iOS Apple (iPhone, iPad, iPod). Необхідно намагатися вилучити мобільний пристрій не в заблокованому вигляді або під час виконання власником мобільного пристрою лише вихідного дзвінка.

Під час *вилучення мобільного пристрою в незаблокованому стані* оперативним працівником слідчий зазначає у протоколі обшуку спосіб вилучення мобільного пристрою, його місцезнаходження, потім за участю працівника кіберполіції зазначає:

– найменування, марку та модель мобільного пристрою, місце його виявлення або особу, в якої він був фактично вилучений та за яких обставин;

– ідентифікаційні ознаки IMEI, серійний номер, із зазначенням способу ідентифікацій IMEI та серійного номера (напис на пристрої, електронна інформація під час натискання комбінації клавіш *#06# тощо);

– про те, що (у разі вилучення незаблокованого мобільного пристрою) на момент вилучення такий пристрій є незаблокований та відобразити виконані працівником кіберполіції дії з увімкнення режиму польоту та вимкнення WiFi і Bluetooth;

– перебіг та результати копіювання всього вмісту пристрою, із зазначенням всіх виконаних працівником кіберполіції дій, включаючи інформацію, що підлягає копіюванню, програмного забезпечення, за допомогою якого здійснюється таке копіювання, відомості про його ліцензування, носій інформації, на який здійснено копіювання наявної на мобільному пристрої інформації, із зазначенням ідентифікаційних номерів носія інформації (серійний чи інвентарний номер тощо).

У разі *вилучення мобільного пристрою із заблокованим екраном* роблять усе можливе, аби не дати його вимкнути, та вживають наступних заходів:

– доручають працівнику кіберполіції негайно увімкнути режим «політ» та вимкнути WiFi і Bluetooth, про що зазначають в протоколі із описом часу виконання таких дій;

– якщо увімкнути режим «політ» та вимкнути WiFi і Bluetooth не вдається, здійснюють відповідний запис у протоколі. У цьому разі доручають працівнику кіберполіції загорнути пристрій у шість шарів харчової фольги та під’єднати до джерела живлення (мобільна батарея тощо) для уникнення його вимкнення, про що зазначають в протоколі з описом часу виконання таких дій;

– звертають увагу на наявність персональних комп’ютерів, планшетів тощо у місці проведення обшуку та в разі встановленого на них програмного забезпечення iTunes доручають кіберполіції оглянути їх із метою виявлення резервної копії даних мобільного пристрою разом із паролем доступу;

– у разі повідомлення працівника кіберполіції про наявність на виявленому в місці проведення обшуку персональному комп'ютері резервної копії даних мобільного пристрою разом із паролем доступу заносять відповідні відомості до протоколу та доручають працівнику кіберполіції здійснити копіювання такої інформації.

Перебіг та результати з копіювання підлягають внесенню до протоколу, зокрема мають бути відображені відомості про:

– працівника кіберполіції, якому доручено здійснення копіювання інформації;

– програмне забезпечення, яке використовуватиметься для копіювання інформації;

– зовнішній носій інформації, на який здійснюватиметься таке копіювання, із зазначенням усіх ідентифікаційних даних такого носія інформації (серійний або інвентарний номер), із зазначенням файлів, які були скопійовані із зазначенням їх властивостей, які повідомляє працівник кіберполіції слідчому для внесення відповідних відомостей до протоколу.

У разі *виявлення пристрою у рідині* — залишають, вилучають, упаковують та зберігають пристрій у рідині, місце і час вилучення такого пристрою зазначають у протоколі. Слід пам'ятати, що недопустимо контактування таких пристроїв з повітрям, оскільки це може призвести до окислення елементів та, як наслідок, — його псування.

У разі виявлення мобільних Android пристроїв (Samsung, Huawei, Sony, Lenovo, LG, Meizu, Xiaomi тощо) насамперед роблять усе, аби вилучити пристрій із незаблокованим екраном і не дати його заблокувати або, що найгірше, вимкнути чи зашифрувати.

За можливості *вилучають пристрій до блокування екрана або під час здійснення дзвінка*, тільки вихідного, оскільки при вхідному дзвінку (в тому числі вхідному виклику у Viber, Telegram, What'sUp) пристрій не вимагає у власника зняття блокування екрана.

Доручають працівнику кіберполіції вимкнути автоблокування екрана в налаштуваннях, а в разі вимоги уведення коду доступу переходять до розділу часу автоблокування та обирають максимальний термін автоблокування, про що зазначають у протоколі обшуку.

У позитивному випадку отримання доступу до незаблокованого екрана, доручають працівнику кіберполіції негайно увімкнути режим «політ» та вимкнути WiFi і Bluetooth, про що роблять відповідні записи до протоколу обшуку із зазначенням часу виконання таких дій.

Із залученням працівника кіберполіції копіюють увесь вміст пристрою, зазначивши точну послідовність дій у протоколі обшуку. Працівник кіберполіції повідомляє слідчому детальний опис проведених дій та наголошує для зазначення в протоколі типу пристрою (його ідентифікаційних ознак) та програмного засобу (відомості про його ліцензування), за допомогою якого знято копію.

У разі, якщо *пристрій вилучено із заблокованим екраном*, доручають працівнику кіберполіції негайно увімкнути режим «політ» та вимкнути WiFi і Bluetooth, про що зазначають у протоколі із описанням часу виконання таких дій.

Якщо увімкнути режим «політ» та вимкнути WiFi і Bluetooth не вдається, загортають пристрій у шість шарів харчової фольги та під'єднують до джерела живлення (мобільної батареї тощо) для уникнення його вимкнення, про що зазначають у протоколі.

Якщо фольги немає, для запобігання видаленню інформації віддаленим способом його вимикають.

Також працівнику кіберполіції доручають оглянути наявний на об'єкті ПК, планшет тощо із метою виявлення наявності у браузері збережених паролів та логінів облікового запису Playmarket Google, на якому можуть зберігатись резервні копії усього вмісту мобільного пристрою.

У разі наявності такої інформації працівник кіберполіції повідомляє про це всіх учасників обшуку та понятих, після чого, за дорученням слідчого здійснює копіювання наявної інформації, про що повідомляє всіх учасників слідчої дії, зокрема про наявність відповідної інформації, місця (адреси) її зберігання на персональному комп'ютері; програмного забезпечення, за допомогою якого здійснюватиметься копіювання; з'ємний носій електронної інформації, на який здійснюватиметься копіювання (його серійний або ідентифікаційний чи інвентарний номер).

Після завершення копіювання працівник кіберполіції демонструє учасникам обшуку та понятим факт збереженості скопійованої інформації на зовнішньому носії інформації, повідомляє про її обсяг, назви файлів, які були скопійовані.

Після цього здійснюють від'єднання зовнішнього носія інформації з персонального комп'ютера, його упакування та опечатування паперовою биркою з написом про персональний комп'ютер, з якого було здійснено копіювання інформації, короткий опис скопійованої інформації, серійний номер з'ємного носія інформації, підпис особи, якій належить персональний комп'ютер, підпис працівника кіберполіції, підписи понятих. Про все це роблять запис у протоколі.

Якщо *пристрій знайдено в рідині* — залишають, вилучають та транспортують його в рідині.

Доручають працівнику кіберполіції витягти з пристрою акумулятор, не виймаючи з рідини.

Забезпечують зберігання в рідині вилученого такого пристрою до моменту огляду, експертизи для унеможливлення контактування з повітрям, подальшим окисленням та, як наслідок, псуванням.

Якщо пристрій щойно кинуто в рідину або його кинули в рідину під час початку обшуку, в присутності працівників поліції тощо, доручають працівнику кіберполіції негайно витягти його з рідини, від'єднати акумулятор та просушити паперовими серветками, рушником, феном тощо.

Усі ці відомості підлягають обов'язковому занесенню до протоколу обшуку.

Вилучені мобільні пристрої (телефони, планшетні комп'ютери, GPS-навігатори, smart-годинники, портативні відеореєстратори тощо) **упаковуються в окремі непрозорі пакети**, що унеможливлює увімкнення пристрою в упаковці. Потім здійснюється їх опечатування биркою із зазначенням підписів: особи, в якої вилучається така інформація, працівника кіберполіції, який здійснив таке копіювання та понятих.

Разом з мобільним пристроєм необхідно, по можливості, вилучати та упаковувати також їх пристрої живлення.

Спосіб упакування повинен забезпечувати неможливість підміни або зміни об'єктів дослідження, носіїв з об'єктами дослідження, зберігання від пошкодження, псування, погіршення або втрати властивостей, завдяки яким вони мають доказове значення.

4. ПИТАННЯ, ЩО ВИРІШУЮТЬСЯ КОМП'ЮТЕРНО-ТЕХНІЧНОЮ ЕКСПЕРТИЗОЮ

Комп'ютерно-технічна експертиза (КТЕ) — одна з різновидів судових експертиз, об'єктом якої є комп'ютерна техніка та (або) комп'ютерні носії інформації, а метою — пошук і закріплення доказів. Вона є комплексом дій, виконуваних професійно підготовленими експертними працівниками, що спрямований на дослідження та аналіз автоматизації інформаційних процесів, комп'ютерної техніки, електронних носіїв, так чи інакше пов'язаних з кримінальним провадженням.

Комп'ютерно-технічна експертиза призначається з метою визначення статусу об'єкта як комп'ютерного засобу, виявлення та вивчення його ролі у правопорушенні, яке розслідується, а також отримання доступу до машинних носіїв інформації з подальшим її дослідженням.

Комп’ютерно-технічна експертиза по кримінальному провадженню може бути призначена слідчим (у рамках досудового розслідування) або судом і доручається конкретному експерту або експертній установі.

Результатом КТЕ є висновок експерта, що служить доказом по справі.

Порядок здійснення КТЕ визначений наказом МВС України від 17 липня 2017 р. № 591, яким затверджена "Інструкція з організації проведення та оформлення експертних проваджень у підрозділах судових експертиз і експертних досліджень у підрозділах Експертної служби Міністерства внутрішніх справ України".

Установи, які мають право здійснювати комп’ютерно-технічну експертизу, наведені у додатку.

У комп’ютерно-технічній експертизі існують такі підвиди експертизи: апаратно-комп’ютерна; програмно-комп’ютерна; інформаційно-комп’ютерна; комп’ютерно-мережна.

Завдання, що вирішуються комп’ютерно-технічною експертизою:

1. Виявлення інформації (за ключовими словами) та програмного забезпечення, що містяться на комп'ютерних носіях.
2. Відновлення видаленої інформації з носіїв інформації.
3. Дослідження відтворених комп’ютерних програм та відповідність певним параметрам (конкретним версіям чи вимогам на його розробку).
4. Виявлення ознак підключення до комп’ютерних мереж, наявності відвідування інтернет-ресурсів та історії переписки тощо.
5. Діагностичне дослідження технічних (апаратних) засобів комп’ютерної техніки, визначення функціональних можливостей та фактичного стану.

Вимоги до об’єктів, що надаються на дослідження в рамках КТЕ:

1. Об’єкти дослідження надаються в окремих пакуваннях, що унеможливлюють доступ до носіїв інформації безпосередньо, підключення системного блока до мережі живлення. Такі об’єкти дослідження, як мобільні телефони, планшетні комп’ютери, GPS-навігатори, smart-годинники портативні відеореєстратори тощо надаються в окремих непрозорих пакуваннях.
2. Для встановлення відповідності програмних продуктів певним параметрам експерту надається носій з копією досліджуваного програмного продукту або програмного коду, а також технічна документація до них.
3. Об’єкти дослідження (портативні комп’ютери, відеореєстратори, планшетні комп’ютери) обов’язково надаються з блоками живлення та паролями (кодами доступу).
4. Упакуванню підлягають усі об'єкти дослідження, які направляються на експертне дослідження. Бажано кожен об’єкт дослідження, носій з об'єктом дослідження упаковувати окремо.

Для скорочення строків виконання експертиз та підвищення якісної значущості висновку експерта пропонується запровадити наступний алгоритм підготовчих заходів при призначенні комп'ютерно-технічних експертиз:

– у зв’язку з великою кількістю комп’ютерного обладнання необхідно проводити попередній огляд об’єктів із залученням експертів з метою встановлення наявності даних, що можуть мати доказове значення у кримінальному провадженні і відокремлення об'єктів, які не будуть об’єктом дослідження, та з метою вирішення питання про доцільність подальшого призначення експертизи;

– обов’язково узгоджувати перелік запитань за конкретними об'єктами з фахівцями та оптимізувати кількість самих запитань. Ставити такі запитання, які стосуються безпосередньо об'єктів дослідження в конкретному кримінальному провадженні, виключаючи при цьому запитання юридичного характеру та запитання, вирішення яких не потребує спеціальних знань;

– визначати першочерговість та пріоритети дослідження наданих об'єктів;

– у разі необхідності проведення у стислі терміни дослідження значної кількості різноманітної комп’ютерної техніки (понад 5 одиниць жорстких дисків, системних блоків, ноутбуків тощо), рекомендується призначати експертизи окремими постановами та розмежуванням за групами об'єктів дослідження;

– запитання в постанові слідчого не повинні носити довідковий, правовий характер і виходити за межі компетенції експерта. Запитання повинні бути спрямовані на встановлення конкретних обставин розслідуваної події.

При призначенні апаратно-комп’ютерної експертизи на розгляд експерту можуть бути поставлені такі **запитання щодо апаратного забезпечення:**

1. Який тип, конфігурація та головні технічні характеристики наданого на дослідження апаратного засобу?
2. Чи відповідає комплектація апаратного засобу наданій технічній документації?
3. Чи внесені у конструкцію наданого апаратного засобу зміни (установка додаткових вбудованих пристроїв: накопичувачів, модулів оперативної пам’яті тощо)?
4. Чи працездатний і справний наданий на експертизу апаратний засіб?
5. Які причини несправності, непрацездатності?
6. Чи придатний для дослідження наданий машинний носій інформації?
7. Які причини відсутності доступу до машинного носія інформації?
8. Чи мають надані апаратні засоби якісь пошкодження?

При призначенні програмно-комп’ютерної експертизи на розгляд експерту можуть бути поставлені такі **запитання щодо програмного забезпечення**:

1. Який екземпляр програмного забезпечення встановлений на наданих машинних носіях, яка дата його установлення?

2. Чи є на наданих машинних носіях програмне забезпечення для …?

3. Чи є на машинних носіях, наданих на дослідження, програмне забезпечення, яке дозволяє сканувати IP-адреси комп’ютерів мережі Інтернет, що мають відкриті для віддаленого доступу із мережі Інтернет ресурси? Якщо так, то яке саме програмне забезпечення? Чи є дані, що свідчать про використання цього програмного забезпечення, якщо так, то які саме?

4. Чи є на машинних носіях, наданих на дослідження, програмне забезпечення, яке дозволяє підібрати пароль для підключення до жорсткого диска віддаленого комп’ютера? Якщо так, то яке програмне забезпечення?

5. Чи є на наданих машинних носіях програмне забезпечення для роботи з електронними платіжними системами? Якщо так, то чи є інформація про облікові дані користувачів, зареєстрованих в таких системах?

6. Чи є на машинних носіях, наданих на дослідження, шкідливі програми, що завідомо приводять до модифікації, блокування, копіювання чи знищення комп’ютерної інформації, порушення роботи ЕОМ, системи ЕОМ чи їх мережі? Якщо так, то яке їх призначення, розташування? Чи є дані, які свідчать про їх створення на досліджуваному машинному носії та розповсюдження (в тому числі через Інтернет)? Якщо так, то які саме?

7. Екземпляри яких програмних продуктів встановлені на наданих машинних носіях?

8. Чи є на наданих машинних носіях екземпляри програмних продуктів для ведення бухгалтерського обліку і податкової звітності?

9. Чи можливо вносити зміни в раніше створений документ за допомогою встановлених програмних продуктів?

10. Яку кількість облікових записів користувачів зареєстровано у встановлених екземплярах системного програмного забезпечення?

11. Чи мають встановлені зареєстровані облікові записи користувачів паролі доступу до ресурсів системного та прикладного програмного забезпечення?

12. Які права доступу мають встановлені зареєстровані облікові записи користувачів?

При призначенні інформаційно-комп’ютерної експертизи **запитання щодо інформаційного забезпечення** можуть бути сформульовані таким чином:

1. Чи є на представлених машинних носіях файли, що містять бази повідомлень електронної пошти, а також файли, які містять журнали повідомлень

програм з обміну миттєвими повідомленнями (інтернет-пейджерів)? Якщо так, то під якими обліковими даними приймались (передавались) повідомлення?

2. Чи міститься на представлених машинних носіях інформація про доступ до яких-небудь форумів в мережі Інтернет? Якщо так, то чи є інформація про облікові дані зареєстрованих в них користувачів?

3. Чи містяться на наданих на дослідження об’єктах інформація про ключові слова: «****», «***», «**»? Якщо так, то прошу скопіювати зазначену інформацію.

4. Чи є на представлених машинних носіях файли, які містять графічні зображення представлених документів?

5. Чи є на представлених машинних носіях файли, які є електронними копіями файлів, наданих для порівняльного аналізу? Якщо так, то яка дата їх створення, зміни, друку, видалення, за допомогою якого програмного забезпечення вони були створені та змінені?

6. Чи є на представлених машинних носіях файли, які містять фрагменти документів з наданих для порівняльного аналізу файлів?

7. Чи є на представлених накопичувачах на жорстких магнітних дисках сліди аномальних змін дати і часу?

8. Прошу скопіювати документи формату (doc, docx) та електроні таблиці формату (xls, xlsx).

9. На які веб-адреси мережі Інтернет та коли здійснювався вихід з наданих на дослідження об'єктів?

10. Чи є на представлених машинних носіях сліди зміни файлів з іменами … за допомогою наявного програмного забезпечення?

11. Чи міститься на наданих на дослідження об’єктах програмне забезпечення призначене для віддаленого керування комп’ютером ?

12. Чи наявні на наданих на дослідження об’єктах програми (клієнти) типу «Клієнт-банк», «Інтернет-банкінг»?

13. Чи містяться в пам’яті наданих на дослідження об'єктів інформація про вміст телефонної книги вхідних, вихідних та неприйнятих дзвінків, текстових повідомлень?

При призначенні комп’ютерно-мережної експертизи **запитання щодо мережевих ресурсів та послуг** можуть бути такі:

1. Чи можливе здійснення доступу до мережі Інтернет із використанням наданих на дослідження апаратних засобів? Якщо так, то яким чином здійснювався доступ?

2. Чи є на машинних носіях, наданих на дослідження, програмне забезпечення, яке дозволяє здійснювати з’єднання і роботу в мережі Інтернет? Якщо так, то яке саме (назва, версії)?

3. Чи є на машинних носіях, наданих на дослідження, програмне забезпечення, що дозволяє користуватися послугами електронної пошти? Якщо так, то яке саме (назва, версії)? Чи є на машинних носіях файли, що містять поштові повідомлення? Яка адреса електронної поштової скриньки, на яку отримані вхідні повідомлення?

4. Чи є на машинних носіях, наданих на дослідження, інформація про здійснення сеансів доступу до мережі Інтернет за період з … по …, в тому числі з використанням облікових даних …? Якщо так, то, які облікові дані використовувались для виходу в Інтернет? В яких файлах містяться відомості про використовувані логіни і паролі?

5. Чи є на машинних носіях, наданих на дослідження, файли, отримані шляхом копіювання з мережі Інтернет за період з … по … (у тому числі файли «cookies»).

Вказаний перелік запитань не є вичерпним і може бути розширений залежно від тих завдань, що ставитимуться перед експертом.

ВИСНОВКИ

З огляду на стрімку цифровізацію сучасного життя, яка напряму впливає й на криміногенну сферу, нова форма доказів — електронні (цифрові) докази, стають новим елементом кримінального судочинства.

Електронні (цифрові) докази існують в нематеріальному вигляді, переносяться чи копіюються на різні пристрої без втрати характеристик, мають властивість існувати в багатьох місцях одночасно, для їх відтворення необхідно використовувати технічні засоби тощо.

Тому не дивно, що цікавість до проблематики збору, фіксації та використані таких форм доказів як електронний документ, електронне повідомлення, інформація в мережі Інтернет та ін. постійно збільшується в міру зростання форм електронних (цифрових) коммунікацій, кількості використовуваних електронних носіїв інформації, застосування новітніх інформаційних технологій в злочинних діях тощо.

З 2017 року до трьох процесуальних кодексів (ЦПК, ГПК та КАС) була введена нові положення, які розширили можливості сторін щодо електронних доказів. Але КПК України інституту електронних доказів ще не отримав, в той час як злочини в кіберпросторі за останні роки значно поширилися.

Це обумовлює нагальну необхідність поглибленого кримінально-процесуального та криміналістичного вивчення зазначених доказів, так і особливостей їх використання в кримінальному судочинстві.

Очевидно, що без фундаментальних наукових досліджень у цій предметній області діяльність правоохоронних органів в зазначеному напрямку буде залишатися мало результативною.

Практичне впровадження цих методичних рекомендацій надасть змогу підвищити рівень фахової компетентності співробітників правоохоронних органів, які здійснюють повноваження досудового розслідування широкої категорії злочинів, де електронні (цифрові) докази відіграють ключове значення.

В методичних рекомендаціях визначено процесуальні аспекти отримання, зберігання та забезпечення достовірності таких доказів для подальшого їх використання у судових інстанціях, представлені покрокові алгоритми виконання відповідних процесуальних дій.

Підготовлені методичні рекомендації також засвідчують необхідність удосконалення правового регулювання сфери використання електронних (цифрових) доказів, зокрема щодо повної імплементації положень Конвенції про кіберзлочинність 2001 р., забезпечення та гарантування прав учасників

кримінального провадження та інших осіб під час здійснення досудового розслідування.

Крім того, в контексті євроінтеграції України проблема залучення закордонного досвіду використання електронних (цифрових) доказів в кримінальному процесі є актуальним напрямком наукових досліджень. Окрім того, необхідно вивчати можливості імплементації правових норм країн Європейського Союзу в законодавство України.

Тому у додатку до основного тексту рекомендацій для ознайомлення читачів наведений текст державного стандарту ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», який був прийнятий з метою гармонізації національної нормативної бази з міжнародним законодавством і розроблений методом перекладу тексту з відповідного міжнародного стандарту ISO/IEC 27037:2012 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence», що був прийнятий спільним технічним комітетом Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC) ще у 2012 році.

Рекомендації, що викладені у стандарті, стосуються специфічної діяльності з оброблення потенційних цифрових доказів, а саме процесів: ідентифікації, збирання, здобуття та збереження цифрових доказів. Ці процеси потрібні під час слідства для підтримання цілісності цифрових доказів — прийнятна методологія отримання цифрових доказів, яка буде забезпечувати їхню допустимість у законодавчих та дисциплінарних судових процесах, а також інших потрібних інстанціях.

В той же час слід розуміти, що запровадження цього стандарту потребує відповідності національним законам, правилам та нормативним документам. Саме тому у стандарті зазначається, що для підтримання цілісності цифрових доказів користувачам цього документу потрібно адаптувати та скоригувати процедури, описані в цьому стандарті, відповідно до специфічних національних законодавчих вимог.

Опанування цих методичних рекомендацій працівниками правоохоронних органів дозволить значно підвищити рівень обізнаності та професіоналізму під час проведення досудового розслідування з використанням електронних (цифрових) доказів, що у свою чергу, надасть змогу покращити результативності оперативно-службової діяльності правоохоронної системи в цілому. А застосування цих рекомендацій у навчальному процесі закладів юридичної освіти допоможе підготувати майбутніх правоохорпонців до їх практичної діяльності.

ДОДАТКИ

Додаток 1. ОСНОВНІ ТЕРМІНИ

MAC-адреса — унікальне 48-бітне число, яке запрограмоване виробником під час його виробництва, що складається з шести частин із чисел у шістнадцятковому вигляді, наприклад, 01:B7:A3:OB:E1:19.

URL (Uniform Resource Locator) — єдиний покажчик ресурсу, що є зручним для запам'ятовування користувачами, наприклад http://www.naiau.kiev.ua

Електронні (цифрові) докази — інформація, що зберігається або передається в електронній (цифровій) формі, отримана в передбаченому КПК України порядку.

Комп'ютерна мережа — сукупність програмних і технічних засобів, за допомогою яких забезпечується можливість доступу з однієї ЕОМ до програмних чи технічних засобів інших ЕОМ та до інформації, що зберігається в системі іншої ЕОМ.

Комп'ютерна система — будь-який пристрій або група взаємно поєднаних або пов'язаних пристроїв, один чи більше з яких, відповідно до певної програми, виконує автоматичну обробку даних.

Комп'ютерні дані — будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки в комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою.

Хеш-сума (контрольна сума) — деяке значення, розраховане на основі набору даних із використанням певного алгоритму, що використовується для перевірки цілісності даних при їх передачі або збереженні) за одним з математичних алгоритмів MD5, SHA-1, CRC32 або ін.

Відповідно до Закону України «Про авторське право і суміжні права»:

Автор — фізична особа, яка своєю творчою працею створила твір;

Аудіовізуальний твір — твір, що фіксується на певному матеріальному носії (кіноплівці, магнітній плівці чи магнітному диску, компакт-диску тощо) у вигляді серії послідовних кадрів (зображень) чи аналогових або дискретних сигналів, які відображають (закодовують) рухомі зображення (як із звуковим супроводом, так і без нього), і сприйняття якого є можливим виключно за допомогою того чи іншого виду екрана (кіноекрана, телевізійного екрана тощо), на якому рухомі зображення візуально відображаються за допомогою певних технічних засобів. Видами аудіовізуального твору є кінофільми, телефільми, відеофільми, діафільми, слайд-фільми тощо, які можуть бути ігровими, анімаційними (мультиплікаційними), неігровими чи іншими;

аудіодискрипція (тифлокоментування) — створення окремої звукової доріжки із закадровим описом персонажа, предмета, простору або дії у відеопродукції для сліпих, осіб з порушеннями зору та осіб з дислексією;

база даних (компіляція даних) — сукупність творів, даних або будь-якої іншої незалежної інформації у довільній формі, в тому числі - електронній, підбір і розташування складових частин якої та її упорядкування є результатом творчої праці, і складові частини якої є доступними індивідуально і можуть бути знайдені за допомогою спеціальної пошукової системи на основі електронних засобів (комп'ютера) чи інших засобів;

веб-сайт — сукупність даних, електронної (цифрової) інформації, інших об'єктів авторського права і (або) суміжних прав тощо, пов'язаних між собою і структурованих у межах адреси веб-сайту і (або) облікового запису власника цього веб-сайту, доступ до яких здійснюється через адресу мережі Інтернет, що може складатися з доменного імені, записів про каталоги або виклики і (або) числової адреси за Інтернет-протоколом;

веб-сторінка — складова частина веб-сайту, що може містити дані, електронну (цифрову) інформацію, інші об'єкти авторського права і (або) суміжних прав тощо;

виключне право — майнове право особи, яка має щодо твору, виконання, постановки, передачі організації мовлення, фонограми чи відеограми авторське право і (або) суміжні права, на використання цих об'єктів авторського права і (або) суміжних прав лише нею і на видачу лише цією особою дозволу чи заборону їх використання іншим особам у межах строку, встановленого цим Законом;

виконавець — актор (театру, кіно тощо), співак, музикант, танцюрист або інша особа, яка виконує роль, співає, читає, декламує, грає на музичному інструменті, танцює чи будь-яким іншим способом виконує твори літератури, мистецтва чи твори народної творчості, циркові, естрадні, лялькові номери, пантоміми тощо, а також диригент музичних і музично-драматичних творів;

виробник відеограми — фізична або юридична особа, яка взяла на себе ініціативу і несе відповідальність за перший відеозапис виконання або будь-яких рухомих зображень (як із звуковим супроводом, так і без нього);

виробник фонограми — фізична або юридична особа, яка взяла на себе ініціативу і несе відповідальність за перший звукозапис виконання або будь-яких звуків;

відеограма — відеозапис на відповідному матеріальному носії (магнітній стрічці, магнітному диску, компакт-диску тощо) виконання або будь-яких рухомих зображень (із звуковим супроводом чи без нього), крім зображень у вигляді запису, що входить до аудіовізуального твору. Відеограма є вихідним матеріалом для виготовлення її копій;

відтворення — виготовлення одного або більше примірників твору, відеограми, фонограми в будь-якій матеріальній формі, а також їх запис для тимчасового чи постійного зберігання в електронній (у тому числі цифровій), оптичній або іншій формі, яку може зчитувати комп'ютер;

власник веб-сайту — особа, яка є володільцем облікового запису та встановлює порядок і умови використання веб-сайту. За відсутності доказів іншого власником веб-сайту вважається реєстрант відповідного доменного імені, за яким здійснюється доступ до веб-сайту, і (або) отримувач послуг хостингу;

власник веб-сторінки — особа, яка є володільцем облікового запису, що використовується для розміщення веб-сторінки на веб-сайті, та яка управляє і (або) розміщує електронну (цифрову) інформацію в межах такої веб-сторінки. Власник веб-сайту не є власником веб-сторінки, якщо останній володіє обліковим записом, що дозволяє йому самостійно, незалежно від власника веб-сайту, розміщувати інформацію на веб-сторінці та управляти нею;

гіперпосилання — формалізований відповідно до стандартів мережі Інтернет запис адреси веб-сайту або його частини (веб-сторінки, даних). У разі якщо гіперпосилання адресує до частини веб-сайту (веб-сторінки), то, крім домену і (або) числової адреси за Інтернет-протоколом, воно може містити додаткові записи про каталоги або виклики і умови доступу до веб-сторінки, що може бути відтворена або збережена на пристроях, які можуть зчитувати та відтворювати електронну (цифрову) інформацію з використанням мережі Інтернет;

електронна (цифрова) інформація — аудіовізуальні твори, музичні твори (з текстом або без тексту), комп'ютерні програми, фонограми, відеограми, програми (передачі) організацій мовлення, що знаходяться в електронній (цифровій) формі, придатній для зчитування і відтворення комп'ютером, які можуть існувати і (або) зберігатися у вигляді одного або декількох файлів (частин файлів), записів у базі даних на зберігаючих пристроях комп'ютерів, серверів тощо у мережі Інтернет, а також програми (передачі) організацій мовлення, що ретранслюються з використанням мережі Інтернет;

інформація про управління правами — інформація, в тому числі в електронній (цифровій) формі, що ідентифікує об'єкт авторського права і (або) суміжних прав і автора чи іншу особу, яка має на цей об'єкт авторське право і (або) суміжні права, або інформація про умови використання об'єкта авторського права і (або) суміжних прав, або будь-які цифри чи коди, у яких представлена така інформація, коли будь-який із цих елементів інформації

прикладений до примірника об'єкта авторського права і (або) суміжних прав або вміщений у нього чи з'являється у зв'язку з його повідомленням до загального відома;

ім'я автора — сукупність слів чи знаків, що ідентифікують автора: прізвище та ім'я автора; прізвище, ім'я та по батькові автора; ініціали автора; псевдонім автора; прийнятий автором знак (сукупність знаків) тощо;

запис (звукозапис, відеозапис) — фіксація за допомогою спеціальних технічних засобів (у тому числі й за допомогою числового представлення) на відповідному матеріальному носії звуків і (або) рухомих зображень, яка дозволяє здійснювати їх сприйняття, відтворення або сповіщення за допомогою відповідного пристрою;

здавання у майновий найм — передача права користування і (або) володіння оригіналом чи примірником твору, фонограми, відеограми на певний строк з метою одержання прямої чи опосередкованої комерційної вигоди;

камкординг — відеозапис аудіовізуального твору під час його публічної демонстрації в кінотеатрах, інших кіновидовищних закладах особами, які перебувають у тому самому приміщенні, де відбувається така публічна демонстрація, для будь-яких цілей без дозволу суб'єкта авторського права або суміжних прав;

кардшейрінг — забезпечення у будь-якій формі та в будь-який спосіб доступу до програми (передачі) організації мовлення, доступ до якої обмежений суб'єктом авторського права і (або) суміжних прав застосуванням технічних засобів захисту (абонентська карта, код тощо), в обхід таких технічних засобів захисту, в результаті чого зазначена програма (передача) може бути сприйнята або в інший спосіб доступна без застосування технічних засобів захисту;

карикатура — твір образотворчого мистецтва, який є творчою переробкою іншого правомірно оприлюдненого твору, в тому числі персонажу твору або імені персонажу твору, що за своїм змістом має комічний, сатиричний характер або спрямовується на висміювання певних осіб або подій;

комп'ютерна програма — набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах);

контрафактний примірник твору, фонограми, відеограми — примірник твору, фонограми чи відеограми, відтворений, опублікований і (або) розповсюджуваний з порушенням авторського права і (або) суміжних прав, у тому числі примірники захищених в Україні творів, фонограм і відеограм, що ввозяться на митну територію України без згоди автора чи іншого суб'єкта авторського права і (або) суміжних прав, зокрема з країн, в яких ці твори, фонограми і відеограми ніколи не охоронялися або перестали охоронятися;

обліковий запис — формалізований згідно зі стандартами мережі Інтернет запис на комп'ютерному обладнанні (комп'ютерах, серверах), підключеному до мережі Інтернет, що ідентифікує користувача (наприклад, власника веб-сайту) на такому обладнанні, включає в себе дані про доступ до частини каталогів і програмного забезпечення комп'ютерного обладнання, а також визначає права такого доступу, що надають можливість володільцю облікового запису додавати, видаляти, змінювати електронну (цифрову) інформацію і дані веб-сайту, надавати доступ до веб-сайту або його частин, окремих даних іншим особам, припиняти функціонування такого веб-сайту або його частини в межах облікового запису;

оприлюднення (розкриття публіці) твору — здійснена за згодою автора чи іншого суб'єкта авторського права і (або) суміжних прав дія, що вперше робить твір доступним для публіки шляхом опублікування, публічного виконання, публічного показу, публічної демонстрації, публічного сповіщення тощо;

опублікування твору, фонограми, відеограми - випуск в обіг за згодою автора чи іншого суб'єкта авторського права і (або) суміжних прав виготовлених поліграфічними, електронними чи іншими способами примірників твору, фонограми, відеограми у кількості,

здатній задовольнити, з урахуванням характеру твору, фонограми чи відеограми, розумні потреби публіки, шляхом їх продажу, здавання в майновий найм, побутового чи комерційного прокату, надання доступу до них через електронні системи інформації таким чином, що будь-яка особа може його отримати з будь-якого місця і у будь-який час за власним вибором або передачі права власності на них чи володіння ними іншими способами. Опублікуванням твору, фонограми, відеограми вважається також депонування рукопису твору, фонограми, відеограми у сховищі (депозитарії) з відкритим доступом та можливістю одержання в ньому примірника (копії) твору, фонограми, відеограми;

організація колективного управління (організація колективного управління майновими правами) — організація, що управляє на колективній основі майновими правами суб'єктів авторського права і (або) суміжних прав і не має на меті одержання прибутку;

організація мовлення — організація ефірного мовлення чи організація кабельного мовлення;

організація ефірного мовлення — телерадіоорганізація, що здійснює публічне сповіщення радіо- чи телевізійних передач і програм мовлення (як власного виробництва, так і виробництва інших організацій) шляхом передачі в ефір за допомогою радіохвиль (а також лазерних променів, гамма-променів тощо) у будь-якому частотному діапазоні (у тому числі й з використанням супутників);

організація кабельного мовлення — телерадіоорганізація, що здійснює публічне сповіщення радіо- чи телевізійних передач і програм мовлення (як власного виробництва, так і виробництва інших організацій) шляхом передачі на віддаль сигналу за допомогою того чи іншого виду наземного, підземного чи підводного кабелю (провідникового, оптоволоконного чи іншого виду);

особа — фізична або юридична особа;

пародія — твір, який є творчою переробкою іншого правомірно оприлюдненого твору або його частини, що за своїм змістом має комічний, сатиричний характер або спрямовується на висміювання певних подій або осіб;

попурі — музичний або інший твір, який є творчим підбором і розташуванням уривків інших правомірно оприлюднених творів або який імітує творчий стиль інших авторів чи виконавців або інших історичних епох;

постачальник послуг хостингу — особа, яка надає власникам веб-сайтів послуги і (або) ресурси для розміщення веб-сайтів або їх частин у мережі Інтернет та із забезпечення доступу до них через мережу Інтернет. Власник веб-сайту, який розміщує свій веб-сайт або його частину в мережі Інтернет на власних ресурсах і (або) самостійно забезпечує доступ до нього з використанням мережі Інтернет, одночасно є постачальником послуг хостингу;

похідний твір — твір, що є творчою переробкою іншого існуючого твору без завдавання шкоди його охороні (анотація, адаптація, аранжування, обробка фольклору, інша переробка твору) чи його творчим перекладом на іншу мову (до похідних творів не належать аудіовізуальні твори, одержані шляхом дублювання, озвучення, субтитрування українською чи іншими мовами інших аудіовізуальних творів);

примірник твору — копія твору, виконана у будь-якій матеріальній формі;

примірник фонограми — копія фонограми на відповідному матеріальному носії, яка виконана безпосередньо чи опосередковано із цієї фонограми і містить усі зафіксовані на ній звуки чи їх частину;

примірник відеограми — копія відеограми на відповідному матеріальному носії, яка виконана безпосередньо чи опосередковано із цієї відеограми і містить усі зафіксовані на ній рухомі зображення чи їх частину (як із звуковим супроводом, так і без нього);

продюсер аудіовізуального твору — особа, яка організує або організує та фінансує створення аудіовізуального твору;

псевдонім — вигадане ім'я, вибране автором чи виконавцем для позначення свого авторства;

публічне виконання — подання за згодою суб'єктів авторського права і (або) суміжних прав творів, виконань, фонограм, передач організацій мовлення шляхом декламації, гри, співу, танцю та іншим способом як безпосередньо (у живому виконанні), так і за допомогою будь-яких пристроїв і процесів (за винятком передачі в ефір чи по кабелях) у місцях, де присутні чи можуть бути присутніми особи, які не належать до кола сім'ї або близьких знайомих цієї сім'ї, незалежно від того, чи присутні вони в одному місці і в один і той самий час або в різних місцях і в різний час;

публічна демонстрація аудіовізуального твору, відеограми — публічне одноразове чи багаторазове представлення публіці за згодою суб'єктів авторського права і (або) суміжних прав у приміщенні, в якому можуть бути присутніми особи, які не належать до кола сім'ї або близьких знайомих цієї сім'ї, аудіовізуального твору чи зафіксованого у відеограмі виконання або будь-яких рухомих зображень;

публічний показ — будь-яка демонстрація оригіналу або примірника твору, виконання, фонограми, відеограми, передачі організації мовлення за згодою суб'єктів авторського права і (або) суміжних прав безпосередньо або на екрані за допомогою плівки, слайда, телевізійного кадру тощо (за винятком передачі в ефір чи по кабелях) або за допомогою інших пристроїв чи процесів у місцях, де присутні чи можуть бути присутніми особи, які не належать до кола сім'ї чи близьких знайомих цієї сім'ї особи, яка здійснює показ, незалежно від того, чи присутні вони в одному місці і в один і той самий час або в різних місцях і в різний час (публічний показ аудіовізуального твору чи відеограми означає також демонстрацію окремих кадрів аудіовізуального твору чи відеограми без дотримання їх послідовності);

публічне сповіщення (доведення до загального відома) — передача за згодою суб'єктів авторського права і (або) суміжних прав в ефір за допомогою радіохвиль (а також лазерних променів, гамма-променів тощо), у тому числі з використанням супутників, чи передача на віддаль за допомогою проводів або будь-якого виду наземного чи підземного (підводного) кабелю (провідникового, оптоволоконного та інших видів) творів, виконань, будь-яких звуків і (або) зображень, їх записів у фонограмах і відеограмах, програм організацій мовлення тощо, коли зазначена передача може бути сприйнята необмеженою кількістю осіб у різних місцях, віддаленість яких від місця передачі є такою, що без зазначеної передачі зображення чи звуки не можуть бути сприйняті;

репрографічне відтворення (репродукування) — факсимільне відтворення у будь-якому розмірі (у тому числі збільшеному чи зменшеному) оригіналу письмового чи іншого графічного твору або його примірника шляхом фотокопіювання або іншими подібними способами, крім запису в електронній (у тому числі цифровій), оптичній чи іншій формі, яку зчитує комп'ютер;

розповсюдження об'єктів авторського права і (або) суміжних прав — будь-яка дія, за допомогою якої об'єкти авторського права і (або) суміжних прав безпосередньо чи опосередковано пропонуються публіці, в тому числі доведення цих об'єктів до відома публіки таким чином, що її представники можуть здійснити доступ до цих об'єктів з будь-якого місця і в будь-який час за власним вибором;

службовий твір — твір, створений автором у порядку виконання службових обов'язків відповідно до службового завдання чи трудового договору (контракту) між ним і роботодавцем;

спеціальний цифровий формат для сліпих, осіб з порушеннями зору та осіб з дислексією — цифровий формат для запису аудійованої книги, яка має зручну навігацію і сприяє швидкому пошуку необхідного матеріалу (сторінка, розділ, параграф, таблиця тощо);

суспільне надбання — твори і об'єкти суміжних прав, строк дії авторського права і (або) суміжних прав на які закінчився;

твір архітектури — твір у галузі мистецтва спорудження будівель і ландшафтних утворень (креслення, ескізи, моделі, збудовані будівлі та споруди, парки, плани населених пунктів тощо);

твір образотворчого мистецтва — скульптура, картина, малюнок, гравюра, літографія, твір художнього (у тому числі сценічного) дизайну тощо;

твір ужиткового мистецтва — твір мистецтва, в тому числі твір художнього промислу, створений ручним або промисловим способом для користування у побуті або перенесений на предмети такого користування;

технічні засоби захисту — технічні пристрої і (або) технологічні розробки, призначені для створення технологічної перешкоди порушенню авторського права і (або) суміжних прав при сприйнятті і (або) копіюванні захищених (закодованих) записів у фонограмах (відеограмах) і передачах організацій мовлення чи для контролю доступу до використання об'єктів авторського права і суміжних прав;

установа — центральний орган виконавчої влади, що реалізує державну політику у сфері інтелектуальної власності;

фонограма — звукозапис на відповідному носії (магнітній стрічці чи магнітному диску, грамофонній платівці, компакт-диску тощо) виконання або будь-яких звуків, крім звуків у формі запису, що входить до аудіовізуального твору. Фонограма є вихідним матеріалом для виготовлення її примірників (копій);

цитата — порівняно короткий уривок з літературного, наукового чи будь-якого іншого опублікованого твору, який використовується, з обов'язковим посиланням на його автора і джерела цитування, іншою особою у своєму творі з метою зробити зрозумілішими свої твердження або для посилання на погляди іншого автора в автентичному формулюванні;

державна система правової охорони інтелектуальної власності — установа і сукупність експертних, наукових, освітніх, інформаційних та інших державних закладів відповідної спеціалізації, що входять до сфери управління Установи.

<u>Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційній системах»:</u>

блокування інформації в системі — дії, внаслідок яких унеможливлюється доступ до інформації в системі;

виток інформації — результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

володілець інформації — фізична або юридична особа, якій належать права на інформацію;

власник системи — фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі — отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі — діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі — дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система — організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-телекомунікаційна система — сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації — взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі — фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації — вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі — дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі — виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі — несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі — умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

телекомунікаційна система — сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації — вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України»:

індикатори кіберзагроз — показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

інформація про інцидент кібербезпеки — відомості про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

інцидент кібербезпеки (кіберінцидент) — подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

кібератака — спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;

кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

кіберзагроза — наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів;

кіберзахист — сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

кіберзлочин (комп'ютерний злочин) **—** 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;

кіберзлочинність — сукупність кіберзлочинів;

кіберпростір — середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

критична інформаційна інфраструктура — сукупність об'єктів критичної інформаційної інфраструктури;

критично важливі об'єкти інфраструктури (далі **—** об'єкти критичної інфраструктури) **—** підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей;

Національна телекомунікаційна мережа — сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв'язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

національні електронні інформаційні ресурси (далі **—** національні інформаційні ресурси) **—** систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

об'єкт критичної інформаційної інфраструктури — комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури;

система управління технологічними процесами (технологічна система) — автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

системи електронних комунікацій (комунікаційні системи) — системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв'язку, електричні

кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.

Відповідно до Закону України «Про телекомунікації»:

абонент — споживач телекомунікаційних послуг, який отримує телекомунікаційні послуги на умовах договору, котрий передбачає підключення кінцевого обладнання, що перебуває в його власності або користуванні, до телекомунікаційної мережі;

абонентна плата — фіксований платіж, який може встановлювати оператор телекомунікацій для абонента за доступ на постійній основі до своєї телекомунікаційної мережі незалежно від факту отримання послуг;

абонентський номер — сукупність цифрових знаків для позначення (ідентифікації) кінцевого обладнання абонента в телекомунікаційній мережі;

адреса мережі Інтернет — визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв;

адресний простір мережі Інтернет — сукупність адрес мережі Інтернет;

безпроводовий доступ до телекомунікаційної мережі (безпроводовий доступ) **—** електрозв'язок з використанням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися із збереженням унікального ідентифікаційного номера в межах пунктів закінчення телекомунікаційної мережі, які під'єднані до одного комутаційного центру;

взаємоз'єднання телекомунікаційних мереж — встановлення фізичного та/або логічного з'єднання між різними телекомунікаційними мережами з метою забезпечення можливості споживачам безпосередньо або опосередковано обмінюватись інформацією;

власник (володілець) кабельної каналізації електрозв'язку — суб'єкт господарювання, у власності (володінні) якого перебувають уся інфраструктура кабельної каналізації електрозв'язку або окремі її елементи, набуті на належній правовій підставі, призначені для забезпечення доступу до телекомунікаційної мережі загального користування;

голосова телефонія — обмін інформацією голосом у реальному часі з використанням телекомунікаційних мереж;

дані — інформація у формі, придатній для автоматизованої обробки її засобами обчислювальної техніки;

домен - частина ієрархічного адресного простору мережі Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється;

домен.UA — домен верхнього рівня ієрархічного адресного простору мережі Інтернет, створений на основі кодування назв країн відповідно до міжнародних стандартів, для обслуговування адресного простору українського сегмента мережі Інтернет;

домен другого рівня — частина адресного простору мережі Інтернет, що розташовується на другому рівні ієрархії імен у цій мережі;

електрозв'язок — див. "телекомунікації";

загальнодоступні (універсальні) телекомунікаційні послуги — мінімальний набір визначених цим Законом послуг нормованої якості, доступний усім споживачам на всій території України;

Інтернет — всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами;

інформаційна система загального доступу — сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних;

інформаційна безпека телекомунікаційних мереж — здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації;

інформація — відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

кабельна каналізація електрозв'язку — обладнання та споруди, призначені для прокладання, монтажу та експлуатаційного обслуговування кабелів телекомунікацій, що включають трубопроводи (канали кабельної каналізації), закладні та оглядові пристрої в колодязях, кабельних шафах, шахтах, колекторах, мостах, естакадах, тунелях, будівлях, а також приміщення для вводу кабелів і розміщення лінійного обладнання;

канал електрозв'язку — сукупність технічних засобів, призначених для перенесення електричних сигналів між двома пунктами телекомунікаційної мережі, і який характеризується смугою частот та/або швидкістю передачі;

канал кабельної каналізації електрозв'язку — окремо виділені місця в колекторах, телекомунікаційних колодязях, тунелях, акведуках, шляхопроводах, на мостах, мостових переходах, естакадах, трубопроводах, а також інші надземні та підземні інженерні споруди, що призначені для прокладання або використовуються для прокладання магістральних, з'єднувальних та розподільних проводових і оптоволоконних кабелів електрозв'язку, а також розміщення супутніх лінійних технічних засобів телекомунікацій;

кінцеве обладнання — обладнання, призначене для з'єднання з пунктом закінчення телекомунікаційної мережі з метою забезпечення доступу до телекомунікаційних послуг;

ліцензія - документ, що засвідчує право суб'єкта господарювання на здійснення зазначеного в ньому виду діяльності у сфері телекомунікацій протягом визначеного строку на конкретних територіях з виконанням ліцензійних умов;

ліцензування — видача, переоформлення, продовження терміну дії, визнання недійсними, анулювання ліцензій, видача копій та дублікатів ліцензій, ведення ліцензійних справ та ліцензійних реєстрів, контроль за додержанням ліцензійних умов, видача розпоряджень про усунення порушень ліцензійних умов;

монопольний (домінуючий) оператор телекомунікацій — оператор, який відповідно до законодавства України займає монопольне (домінуюче) становище на ринку певних телекомунікаційних послуг на території держави чи певного регіону;

Національний план нумерації - нормативно-правовий акт, який визначає структуру, регламентує розподіл та умови використання номерного ресурсу в телекомунікаційних мережах;

номерний ресурс - сукупність цифрових знаків, що використовуються для позначення (ідентифікації) мереж, послуг, пунктів закінчення мережі в телекомунікаційних мережах загального користування;

оператор телекомунікацій — - суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж;

оператор, провайдер телекомунікацій з істотною ринковою перевагою на ринку телекомунікаційних послуг — оператор, провайдер телекомунікацій, частка доходу якого на визначеному національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, ринку певних телекомунікаційних послуг протягом року, що передує проведенню аналізу ринку, перевищує 25 відсотків сумарного доходу всіх операторів, провайдерів телекомунікацій, отриманого на цьому ринку за той самий період часу, або якщо внаслідок технологічного процесу надання послуги іншому оператору, провайдеру телекомунікацій її може бути надано тільки в мережі певного оператора, провайдера телекомунікацій;

передавання даних — передавання інформації у вигляді даних з використанням телекомунікаційних мереж;

перенесення абонентського номера — телекомунікаційна послуга, що надається абоненту за його заявою, яка полягає у збереженні за абонентом наданого йому оператором телекомунікацій абонентського номера з метою використання цього номера для отримання телекомунікаційних послуг у мережі іншого оператора телекомунікацій, що надає телекомунікаційні послуги на території України;

персональний номер — абонентський номер, що присвоюється зареєстрованому абоненту за його заявою у порядку, встановленому національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, централізовано адмініструється і може використовуватися цим абонентом для отримання відповідно до договору телекомунікаційних послуг незалежно від географічного регіону України і типу цих послуг;

послуга пропуску трафіка — телекомунікаційна послуга щодо здійснення термінації та/або транзиту трафіка, що надається оператором телекомунікацій іншим операторам;

провайдер телекомунікацій — суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку;

проводовий електрозв'язок — передавання і приймання інформації із застосуванням проводових ліній з металевими або волоконнооптичними жилами;

пропуск трафіка — проходження трафіка між елементами однієї або різних телекомунікаційних мереж;

пункт закінчення телекомунікаційної мережі — місце стику (з'єднання) мережі телекомунікацій та кінцевого обладнання;

ресурси телекомунікаційних мереж — наявні в телекомунікаційних мережах кількість номерів (номерний ресурс), кількість і пропускна спроможність проводових ліній з металевими жилами, оптичними волокнами, радіоліній, каналів, трактів для передавання інформації, комутаційних станцій та вузлів, радіочастотний ресурс;

ринок телекомунікаційних послуг — сфера обігу визначених телекомунікаційних послуг, на які протягом певного часу і в межах певної території є попит і пропозиція;

розподіл номерного ресурсу — виділення номерного ресурсу з визначеного діапазону номерів для надання телекомунікаційних послуг;

розрахункова такса — сума, що визначає розмір оплати за доступ до технічних та технологічних ресурсів мереж операторів телекомунікацій (здійснення доступу) для пропуску одиниці трафіка і застосовується для операторів, які є суб'єктами господарської діяльності на території України;

розрахункова такса за послугу пропуску трафіка **—** розмір плати за термінацію або транзит одиниці трафіка між телекомунікаційними мережами операторів;

роумінг національний — телекомунікаційна послуга, яка забезпечує можливість абонентам одного оператора телекомунікацій, що надає послуги рухомого (мобільного) зв'язку на території України, отримувати телекомунікаційні послуги в телекомунікаційній мережі іншого оператора (операторів) у межах України;

рухомий (мобільний) зв'язок — електрозв'язок із застосуванням радіотехнологій, під час якого кінцеве обладнання хоча б одного із споживачів може вільно переміщатися в межах усіх пунктів закінчення телекомунікаційної мережі, зберігаючи єдиний унікальний ідентифікаційний номер мобільної станції;

споживач телекомунікаційних послуг (споживач) **—** юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб;

споруди електрозв'язку — будівлі, вежі, антени, що використовуються для організації електрозв'язку;

сталість телекомунікаційної мережі — властивості телекомунікаційної мережі зберігати повністю або частково свої функції за умови впливу на неї дестабілізуючих чинників;

суб'єкти ринку телекомунікацій — оператори, провайдери телекомунікацій, споживачі телекомунікаційних послуг, виробники та/або постачальники технічних засобів телекомунікацій;

телекомунікації (електрозв'язок) — передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах;

телекомунікаційна мережа — комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації**,** комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням;

телекомунікаційна мережа загального користування — телекомунікаційна мережа, доступ до якої відкрито для всіх споживачів;

телекомунікаційна мережа доступу — частина телекомунікаційної мережі між пунктом закінчення телекомунікаційної мережі та найближчим вузлом (центром) комутації включно;

телекомунікаційна послуга (послуга) **—** продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері телекомунікацій;

телемережі — телекомунікаційні мережі загального користування, що призначаються для передавання програм радіо- та телебачення, а також інших телекомунікаційних і мультимедійних послуг і можуть інтегруватися з іншими телекомунікаційними мережами загального користування;

термінація трафіка — встановлення, підтримка фізичного та/або логічного з'єднання, пропуск трафіка між телекомунікаційною мережею, з якої надходить виклик або ініціюється з'єднання, та кінцевим обладнанням, до якого спрямовується виклик або ініціюється з'єднання;

технічні засоби телекомунікацій — обладнання, станційні та лінійні споруди, призначені для утворення телекомунікаційних мереж;

транзит трафіка — встановлення, підтримка телекомунікаційною мережею оператора фізичного та/або логічного з'єднання, пропуск трафіка між двома іншими телекомунікаційними мережами;

транспортна телекомунікаційна мережа — мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу;

трафік — сукупність інформаційних сигналів, що передаються за допомогою технічних засобів операторів, провайдерів телекомунікацій за визначений інтервал часу, включаючи інформаційні дані споживача та/або службову інформацію;

фіксований зв'язок — телекомунікації, що здійснюються із застосуванням стаціонарного (нерухомого) кінцевого обладнання.

Додаток 2. УСТАНОВИ, ЩО ЗДІЙСНЮЮТЬ КОМП'ЮТЕРНО-ТЕХНІЧНУ ЕКСПЕРТИЗУ

1. Державний науково-дослідний експертно-криміналістичний центр (або його регіональні підрозділи)

Юридична адреса: вул. Богомольця, 10, м. Київ, 01601
Поштова адреса: 03170, м. Київ, вул. Велика Окружна, 4
Сайт http://dndekc.centrmia.gov.ua Електронна адреса: dndekc@mvs.gov.ua
Тел.: (044) 405-74-69, (044) 374-34-06, (044) 374-34-02

2. Київський науково-дослідний інститут судових експертиз

Поштова адреса: вул. Смоленська, 6, м. Київ, 03057
Сайт: http://kndise.gov.ua Електронна адреса: info@kniise.com.ua
Тел./факс: (044) 200-29-11

3. Львівський науково-дослідний інститут судових експертиз Міністерства юстиції України

Поштова адреса: вул. Липинського, 54, м. Львів, 79024
Електронна адреса: lndise@mail.lviv.ua
Тел./факс: (032) 231-70-61 – загальний відділ, (032) 231-76-13 – приймальня

4. Одеський науково-дослідний інститут судових експертиз Міністерства юстиції України

Поштова адреса: вул. Ланжеронівська, 21, м. Одеса, 65026
Електронна адреса: odndise@gmail.com
Тел./факс: (048) 722-44-66

5. ТОВ «Лабораторія комп'ютерної криміналістики»

Поштова адреса: пров. Коломийский, 13/23 Київ, 03127,
Сайт: http://cyberlab.com.ua/index.html Email: info@cyberlab.com.ua
Тел. (044) 338-3231

6. ТОВ "Незалежний інститут судових експертиз"

Поштова адреса: вул. Маршала Тимошенка, 21, м. Київ, 04212
корпус 3, офіс 7, поверх 5
Сайт https://nise.com.ua E-mail: info@nise.com.ua
Телефони: (044) 581-30-90, (044) 581-30-80, (044) 581-30-77
Факс: (044) 581-30-55

Додаток 3. ЗРАЗКИ ПРОЦЕСУАЛЬНИХ СЛІДЧИХ ДОКУМЕНТІВ

Запит до Інтернет-провайдера
щодо надання інформації про користувача IP-адреси

Шановний _____!

Слідчим управлінням ГУ НП України в м. Києві здійснюється досудове розслідування за матеріалами ЄРДР від 03.09.2019 р. № 12016100020003580000 за ч. 2 ст. 301 КК України «Розповсюдження порнографічних предметів». Установлено, що зловмисники здійснювали спілкування щодо купівлі/продажу порнографічних предметів з використанням IP-адреси 108.273.78.264 близько 15 годин 55 хвилин 02.09.2019 р.

Враховуючи вищевикладене, керуючись статтями 40, 92, 93, 133, 135 Кримінального порцесуального кодексу України, з метою повного, всебічного та неупередженого розслідування кримінального правопорушення прошу Вас надати інформацію про реквізити абонемента, який здійснював доступ до мережі Інтернетпід вказаною IP-адресою, яка належить до Вашої мережі.

З повагою
Старший слідчий СУ ГУ НП України в м. Києві

Запит до адміністрації Інтернет-ресурсу
щодо надання інформації про IP-адреси та сесії доступу до ресурсу
розповсюджувача творів, що пропагують культ насильства та жорстокості

Шановний _____!

Слідчим управлінням ГУ НП України в м. Києві здійснюється досудове розслідування за матеріалами ЄРДР від 03.09.2019 р. № 12016100020003580000 за ч. 2 ст. 300 КК України «Розповсюдження творів, що попагують культ насильства та жорстокості». Встановлено, що користувач розмістив відеоматеріал «Как нужно пытать людей» на Вашому інтеренет-сайті на інтернет-сторінці http://...

Враховуючи вищевикладене, керуючись статтями 40, 92, 93, 133, 135 Кримінального процесуального кодексу України, з метою повного, всебічного та неупередженого розслідування кримінального правопорушення прошу Вас надати таку інформацію:

– коли та портягом якого часу створений цей обліковий запис протиправного характеру «Как нужно пытать людей»;

– з якої IP-адреси створено обліковий запис користувача, який створив цю інтернет-сторінку на Вашому ресурсі;

– на кого зарестрований обліковий запис (надати повні анкетні власників сайта, інформацію з панелі адміністрування, IP-адреси, телефони тощо);

– деталізацію всіх IP-адрес та часу виходу в цей обліковий запис користувача;

– як здійснювався перегляд цього облікового запису та його наповнення (IP-адреса, установочні дані та час входу);

– яким чином оплачуються послуги за зазначене доменне імя (вид платіжної системи, яка використовувалася при поповненні балансу облікового запису користуача цієї системи (гаманці, ідентифікатори) види оплат) банківські установи, рахунки тощо.

З повагою
Старший слідчий СУ ГУ НП України в м. Києві

Запит до поштового сервісу
щодо надання інформації про рестратора електронної поштової скриньки

Шановний _____!

Слідчим управлінням ГУ НП України в м. Києві здійснюється досудове розслідування за матеріалами ЄРДР від 03.09.2019 р. № 12016100020003580000 за ч. 2 ст. 300 КК України «Розповсюдження творів, що попагують культ насильства та жорстокості». Встановлено, що зловмисник користується електроною поштовою скринькою за логіном: pytky@yacho.com

Враховуючи вищевикладене, керуючись статтями 40, 92, 93, 133, 135 Кримінального процесуального кодексу України, з метою повного, всебічного та неупередженого розслідування кримінального правопорушення прошу Вас надати таку інформацію :

– час реєстрації данооі поштової скриньки і IP-адреси, якими користувався зловмисник під час роботи з цією поштовою скринькою;

– установоччі дані користувача поштової скриньки;

– через який телефонний номер здійснювалась активація облікового запису;

– деталізацію всіх сеансів входу до цього облікового запису із зазначенням IP-адрес та часу.

З повагою
Старший слідчий СУ ГУ НП України в м. Києві

Запит до адміністрації Інтернет-ресурсу
щодо надання інформації про переписку
користувача інтернет-форуму

Шановний _____!

Слідчим управлінням ГУ НП України в м. Києві здійснюється досудове розслідування за матеріалами ЄРДР від 03.09.2019 р. № 12016100020003580000 за ч. 2 ст. 301 КК України «Збут порнографічних предметів». Встановлено, що зловмисники спілкувалися на інтернет-форумі www.XXXXX

Враховуючи вищевикладене, керуючись статтями 40, 92, 93, 133, 135 Кримінального процесуального кодексу України, з метою повного, всебічного та неупередженого розслідування кримінального правопорушення прошу Вас надати інформацію щодо історії повідомлень у вказаному інтернет-форумі користувача «Бизон».

З повагою
Старший слідчий СУ ГУ НП України в м. Києві

Запит до WEBMONEYnote
щодо встановлення IP-адреси користувача системи електронних грошей

Шановний _____!

Слідчим управлінням ГУ НП України в м. Києві здійснюється досудове розслідування за матеріалами ЄРДР від 03.09.2019 р. № 12016100020003580000 за ч. 2 ст. 301 КК України «Збут порнографічних предметів».

Встановлено, що причетні до збуту порнографічних предметів особи використовували у протиправних цілях платіжну систему WEBMONEY , за допомогою гаманця № Z135792468015.

Враховуючи вищевикладене, керуючись статтями 40, 92, 93, 133, 135 Кримінального процесуального кодексу України, з метою повного, всебічного та неупередженого розслідування кримінального правопорушення прошу Вас надати інформацію про IP-адреси компютерів, під якими було створено обліковий запис і здійснювалося використання Вашої платіжної системи за допомогою електронного гаманця № Z135792468015.

З повагою
Старший слідчий СУ ГУ НП України в м. Києві

Запит до адміністрації Інтернет-ресурсу
щодо надання інформації про IP-адреси та сесії доступу до ресурусу
розповсюджувача творів, що пропагують культ насильства та жорстокості

Шановний _____!

Слідчим управлінням ГУ НП України в м Києві здійснюється досудове розслідування за матеріалами ЄРДР від 03.09.2019 р. № 12016100020003580000 за ч. 2 ст. 300 КК України «Розповсюдження творів, що пропагують культ насильства та жорстокості». Встановлено, що користувач розмістив відеоматеріал «Как нужно пытать людей» на Вашому інтеренет-сайті на Інтернет-сторінці http://XXXXX зловмисники здійснювали спілкування щодо купівлі/продажу порнографічних предметів з використанням IP-адреси 108.273.78.264 близько 15 годин 55 хвилин 02.09.2019 р.

Враховуючи вищевикладене, керуючись статтями 40, 92, 93, 133, 135 Кримінального порцесуального кодексу України, з метою повного, всебічного та неупередженого розслідування кримінального правопорушення прошу Вас надати інформацію про реквізити абонемента, який здійснював доступ до мережі Інтернет під вказаною IP-адресою, яка належить до Вашої мережі.

З повагою
Старший слідчий СУ ГУ НП України в м. Києві

Додаток 4. Рекомендації щодо ідентифікації, збирання, здобуття та збереження електронних (цифрових) доказів, викладені в ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів»

Відповідно до наказу Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») від 6 грудня 2017 р. № 400 «Про прийняття національних нормативних документів, гармонізованих з європейськими та міжнародними нормативними документами, скасування національних нормативних документів, змін до національних нормативних документів» з 1 січня 2019 року в Україні набрав чинності державний стандарт ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів».

Цей стандарт був прийнятий з метою гармонізації національної нормативної бази з міжнародним законодавством і розроблений методом перекладу тексту з відповідного міжнародного стандарту ISO/IEC 27037:2012 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence», що був прийнятий спільним технічним комітетом Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC) ще у 2012 році.

Рекомендації, що викладені в стандарті, стосуються специфічної діяльності з оброблення потенційних цифрових доказів, а саме процесів: ідентифікації, збирання, здобуття та збереження цифрових доказів. Ці процеси потрібні під час слідства для підтримання цілісності цифрових доказів — прийнятна методологія отримання цифрових доказів, яка буде забезпечувати їхню допустимість у законодавчих та дисциплінарних судових процесах, а також інших потрібних інстанціях.

Але запровадження цього стандарту потребує відповідності національним законам, правилам та нормативним документам. Тому в стандарті зазначається, що для підтримання цілісності цифрових доказів користувачам цього документу потрібно адаптувати та скоригувати процедури, описані в цьому стандарті, відповідно до специфічних національних законодавчих вимог.

Стандарт також може допомогти у сприянні обміну потенційними цифровими доказами між юрисдикціями різних держав.

Представлений надалі текст стандарту не є його офіційним виданням.

1 **СФЕРА ЗАСТОСУВАННЯ**

Цей стандарт надає настанови для специфічної діяльності з оброблення цифрових доказів, а саме: ідентифікації, збирання, здобуття та збереження цифрових доказів, що можуть мати доказове значення. Цей стандарт надає настанови для фахівців стосовно звичайних випадків, які трапляються в процесі оброблення цифрових доказів, та допомагає організаціям в їхніх дисциплінарних процедурах та забезпеченні обміну потенційними цифровими доказами між юрисдикціями.

Цей стандарт надає настанови для таких пристроїв та/або функцій, використовуваних за різних обставин:

— Носій для зберігання цифрових даних, використовуваний у стандартних комп'ютерах, подібний жорстким дискам, гнучким дискам, оптичним і магнітооптичним дискам, цифровим пристроям з подібними функціями;
— Мобільні телефони, Персональні цифрові помічники (PDAs), Персональні електронні прилади (PEDs), карти пам'яті;
— Мобільні навігаційні системи;
— Цифрові фото- та відеокамери (зокрема CCTV);
— Стандартний комп'ютер з мережевими з'єднаннями;
— Мережі, які ґрунтовані на TCP/IP та інших цифрових протоколах, а також
— Прилади з функціями, подібними наведеним вище.

Примітка 1. Наведений вище перелік приладів надано для інформації і він не є вичерпним.

Примітка 2. Наведені вище пристрої може бути запроваджено в різні способи. Наприклад, автоматизована система може містити мобільну навігаційну систему, збереження даних та сенсорну систему.

2 **НОРМАТИВНІ ПОСИЛАННЯ**

Наведені нижче документи потрібні для застосування цього стандарту. У разі датованих посилань застосовують тільки наведені видання. У разі недатованих посилань потрібно користуватись останнім виданням нормативних документів (разом зі змінами).

ISO/TR 15801 Document management — Information stored electronically — Recommendations for trustworthiness and reliability (Керування документами. Інформація, що зберігається в електронному вигляді. Рекомендації стосовно справжності та надійності)

ISO/IEC 17020 Conformity assessment — Requirements for the operation of various types of bodies performing inspection (Оцінка відповідності. Вимоги до роботи різних типів органів з інспектування)

ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary (Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд та словник).

3 **ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ**

У цьому стандарті вжито терміни та визначення позначених ними понять згідно з ISO/IEC 27000, ISO/IEC 17020, ISO/IEC 17025 та ISO/TR 15801, а також наведені нижче.

3.1 **здобуття** (*acquisition*)
Процес створення копії даних у межах визначеного набору.

Примітка. Результатом здобуття є копія потенційних цифрових доказів

3.2 **виділений простір** (*allocated space*)

Ділянка цифрового середовища, охоплюючи первинну пам'ять, використовувану для збереження даних, охоплюючи метадані

3.3 **збирання** (*collection*)

Процес складання фізичних об'єктів, які містять потенційні цифрові докази

3.4 **цифровий пристрій** (*digital device*)

Електронне устаткування, використовуване для оброблення чи збереження даних

3.5 **цифровий доказ** (*digital evidence*)

Інформація або дані, збережені або передані в бінарному вигляді, на які можна покладатися як на докази

3.6 **копія цифрового доказу** (*digital evidence copy*)

Копія цифрового доказу, запроваджено для підтримання надійності доказу за допомогою вміщення разом цифрового доказу та засобів верифікації, де спосіб верифікації може бути вбудованим або незалежним від інструментів, використовуваних під час верифікації

3.7 **перший відповідальний за цифровий доказ**; DEFR (*Digital Evidence First Responder*)

Авторизована особа, яка пройшла навчання та кваліфікована для того, щоб діяти першою під час розслідування інциденту, здійснюючи збирання та здобуття цифрових доказів, із відповідальністю для оброблення цього інциденту.

Примітка. Повноваження, навчання та кваліфікація є обов'язковими вимогами, необхідними для здобуття надійних цифрових доказів, але індивідуальні обставини можуть призвести до того, що особа не відповідає всім трьом вимогам. У такому разі потрібно розглянути локальні закони, організаційну політику та індивідуальні обставини

3.8 **спеціаліст з цифрових доказів**; DES (*Digital Evidence Specialist*)

Особа, яка може виконувати завдання DEFR та має спеціалізовані знання, навички та здатна поводитися з широким діапазоном технічних питань.

Примітка. DES може мати навички в додаткових сферах, наприклад, здобуття з мережі, здобуття з RAM, знання програмного забезпечення операційних систем або Mainframe

3.9 **носій для збереження цифрових даних** (*digital storage medium*)

Пристрій, на якому можуть бути записані цифрові дані

[Адаптовано з ISO/IEC 10027:1990]

3.10 **пристрій для збереження доказів** (evidence preservation facility)

Безпечне середовище або місце, де зберігають докази, зібрані чи здобуті.

Примітка. Пристрій для збереження доказів не повинен піддаватися впливу магнітних полів, пилу, вібраціям, вогкості чи будь-яких інших елементів навколишнього середовища (таких як екстремальні температури або вологість), які можуть пошкодити потенційні цифрові докази всередині пристрою

3.11 **геш-значення** (*hash value*)

Рядок бітів, яка є виходом геш-функції

3.12 **ідентифікація** (identi*fi*cation)

Процес, який охоплює пошук, розпізнавання та документування потенційних цифрових доказів

3.13 **утворення образу** (*imaging*)

Процес створення порозрядної копії носія для збереження цифрових даних.

Примітка. Порозрядна копія також має назву фізичної копії.

Приклад: Під час створення образу жорсткого диску DEFR буде також копіювати вилучені дані

3.14 **периферія** (*peripheral*)

Прилад, під'єднаний до цифрового приладу для розширення його функціональності

3.15 **збереження** (*preservation*)

Процес для підтримання та убезпечування цілісності та/або оригінальних умов потенційних цифрових доказів

3.16 **надійність** (*reliability*)

Властивість логічно передбачуваних поведінки та результатів

[ISO/IEC 27000:2009]

3.17 **збіжність** (*repeatability*)

Властивість керованого процесу отримувати однакові тестові результати в однаковому тестовому середовищі (однаковий комп'ютер, жорсткий диск, режим операції тощо)

3.18 **відтворюваність** (*reproducibility*)

Властивість процесу отримувати однакові тестові результаті в різному тестовому середовищі (різні комп'ютери, жорсткий диск, режим роботи тощо)

3.19 **псування** (*spoliation*)

Дія зі здійсненням або допущенням внесення змін(и) до потенційних цифрових доказів, яка зменшує їхнє доказове значення

3.20 **системний час** (*system time*)

Час, генерований системним годинником за допомогою операційної системи; це не час, обчислюваний операційною системою

3.21 **втручання** (*tampering*)

Дія з навмисного виконання або допущення внесення змін(и) до цифрового доказу (тобто, умисне або цілеспрямоване псування)

3.22 **часовий штемпель** (*timestamp*)

Різні параметри часу, які визначають точку в часі відносно до загальної довідкової інформації про час

[ISO/IEC 11770-1:1996]

3.23 **невиділений простір** (*unallocated space*)

Простір у цифровому середовищі, охоплюючи первинну пам'ять, який не був локалізованим за допомогою операційної системи та придатний для збереження даних, охоплюючи метадані

3.24 **затвердження** (*validation*)

Підтвердження за допомогою об'єктивних доказів, що вимоги для специфічного призначеного використання або застосування виконано

[ISO/IEC 27004:2009]

3.25 **функція верифікації** (verif*i*cation function)

Функція, використовувана для підтвердження, що два набори даних — ідентичні.

Примітка 1. Два неідентичні набори даних не потрібно вважати ідентичними після функції верифікації.

Примітка 2. Функції верифікації зазвичай застосовують з використанням геш-функцій, таких як MD5, SHA1 тощо, але може бути використано інші методи

3.26 **нестійкі дані** (*volatile data*)

Дані, специфічно схильні до змін та які може бути легко модифіковано.

Примітка. Зміни може бути зумовлено виключенням живлення або переходом крізь магнітне поле. Нестійкі дані також охоплюють дані, які змінюються, коли стан системи змінюється. Прикладами можуть бути дані, збережені в RAM та динамічні IP-адреси.

4 ПОЗНАКИ ТА СКОРОЧЕННЯ

AVI (Audio Video Interleave) — Чергування аудіо та відео; CCTV (Closed Circuit Television) — Відеоспостереження; CD (Compact Disk) — Компакт-диск;

DNA (Deoxyribonucleic Acid) — Дезоксирибонуклеїнова кислота (ДНК);

DEFR (Digital Evidence First Responder) — Перший відповідальний за цифровий доказ;

DES (Digital Evidence Specialist) — Спеціаліст із цифрових доказів;

DVD (Digital Video/Versatile Disk) — Цифровий відео/універсальний диск;

ESN (Electronic Serial Number) — Електронний серійний номер;

GPS (Global Positioning System) — Глобальна система визначення місцеположення;

GSM (Global System for Mobile Communication) — Глобальна система мобільного зв'язку;

IMEI (International Mobile Equipment Identity) — Міжнародний ідентифікатор мобільного обладнання;

IP (Internet Protocol) — Інтернет-протокол;

ISIRT (Information Security Incident Response Team) — Команда реагування на інциденти інформаційної безпеки;

LAN (Local Area Network) — Локальна мережа;

MD5 (Message-Digest Algorithm 5) — Алгоритм перетворення повідомлення 5;

MP3 (MPEG Audio Layer 3) — MPEG аудіо рівень 3;

MPEG (Moving Picture Expert Group) — Група експертів з питань кіно;

NAS (Network Attached Storage) — Мережа пристроїв для збереження даних;

PDA (Personal Digital Assistant) — Персональний цифровий помічник;

PED (Personal Electronic Device) — Персональний електронний прилад;

PIN (Personal Identification Number) — Персональний ідентифікаційний номер;

PUK (PIN Unlock Key) — Ключ розблокування PIN;

RAID (Redundant Array of Independent Disks) — Надлишковий масив незалежних дисків;

RAM (Random Access Memory) — Оперативна пам'ять для тимчасового збереження даних з випадковим доступом;

RFID (Radio Frequency Identification) — Ідентифікація радіочастот;

SAN (Storage Area Network) — Мережа сховищ;

SHA (Secure Hash Algorithm) — Безпечний геш-алгоритм;

SIM (Subscriber Identity Module) — Модуль ідентифікації абонента;

USB (Universal Serial Bus) — Універсальна послідовна шина;

UPS (Uninterruptible Power Supply) — Безперебійне джерело живлення;

USIM (Universal Subscriber Identity Module) — Універсальний модуль ідентифікації абонента;

UV (Ultraviolet) — Ультрафіолет;

Wi-Fi (Wireless Fidelity) — Бездротова передача інформації.

5 ЗАГАЛЬНИЙ ОГЛЯД

5.1 Обставини для збирання цифрових доказів

Цифрові докази можуть бути потрібними для використання в низці окремих сценаріїв, кожен з яких має різний баланс між рушієм доказової якості, своєчасністю аналізування, відновлюванням послуги та вартістю збирання цифрових доказів. Тому організаціям потрібно буде запровадити процес визначення пріоритетів, який ідентифікує потреби та баланс доказової якості, своєчасності та відновлення послуг до того, як буде надано завдання ресурсам DEFR. Процес визначення пріоритетів охоплює виконання оцінювання матеріалів, доступних для визначення можливого доказового значення, та порядок, у якому потенційні цифрові докази потрібно збирати, здобувати чи зберігати. Процес визначення пріоритетів здійснюється задля мінімізації ризику, що потенційні цифрові докази будуть псуватися, та доведення до максимуму доказового значення зібраних потенційних цифрових доказів.

5.2 Принципи цифрових доказів

У більшості юрисдикцій та організацій цифрові докази ґрунтуються на трьох основних принципах: важливість, надійність та достатність. Ці три принципи є важливими в усіх розслідуваннях, але не тільки такі цифрові докази прийнятні в суді. Цифровий доказ є надійним, якщо він надає можливість засвідчувати або не засвідчувати елемент розслідуваного специфічного випадку. Хоча детальні визначення «надійність» відрізняються в різних юрисдикціях, основне значення цього принципу «гарантувати, що цифровий доказ є таким, яким він має бути» широко вживають. Не завжди потрібно для DEFR збирати всі дані або робити повну копію первісного цифрового доказу. У більшості юрисдикцій концепція достатності означає, що DEFR повинен зібрати достатню кількість потенційних цифрових доказів, щоб забезпечити можливість відповідного перевірення та дослідження елементів справи. Розуміння цієї концепції є важливим для DEFR для визначення пріоритетів зусиль правильно, якщо це стосується часу або вартості.

Примітка. DEFR повинен гарантувати, що збирання потенційних цифрових доказів відповідає локальному законодавству та нормативним документам, як це потрібно для специфічних обставин.

Усі процеси, використовувані DEFR та DES, мають бути затвердженими до їхнього використання. Якщо затвердження зроблено в екстремальних умовах, DEFR та DES мають підтвердити, що затвердження є прийнятним для їхнього специфічного використання процесів та середовища й обставин, у яких ці процеси будуть використані. DEFR та DES мають також:

a) документувати всі дії;

b) визначати та застосовувати метод для оцінювання точності та надійності копій потенційних цифрових доказів відносно первісного джерела; а також

c) зазначити, що дія збереження потенційних цифрових доказів не може завжди бути без наявності втручання.

5.3 Вимоги щодо оброблення цифрових доказів

5.3.1 *Загальні положення*

Принципи, наведені вище в 5.2, можна задовольнити так:

— Важливість: Є змога показати, що здобуті матеріали є надійними для розслідування — тобто що вони містять величини, які допомагають у розслідуванні конкретного інциденту, та що є доречна причина для їхнього здобуття. За допомогою аудиту та юрисдикції DEFR повинен мати змогу описати підтримані процедури та пояснити, як було прийнято рішення для здобуття кожного елемента.

— Надійність: Усі процеси, використані під час оброблення потенційних цифрових доказів, потрібно піддавати аудиту та вони мають бути збіжними.

— Достатність: DEFR повинен ураховувати, що достатню кількість матеріалів має бути зібрано, щоб дозволити зробити належні дослідження. DEFR повинен мати змогу з використанням аудиту та законодавства надати пояснення, яку кількість матеріалу, загалом, розглянуто та які процедури використано для вирішення питання, яку кількість та який матеріал здобуто.

Примітка. Матеріали має бути зібрано за допомогою дій зі здобуття та збирання.

Є чотири ключові аспекти в обробленні цифрових доказів: можливість аудиту, відповідність юрисдикції та збіжність або відтворюваність залежно від конкретних обставин.

5.3.2 **Можливість аудиту**

Незалежні аудитори або інші зацікавлені сторони повинні мати змогу оцінювати діяльність DEFR та DES. Це буде можливим за допомогою документування всіх запроваджених дій. DEFR та DES повинні мати змогу доказу законності процесу прийняття рішення у виборі такого плану дій. DEFR та DES мають бути доступними для незалежного оцінювання для визначення, чи запроваджено відповідні наукові методи, методики та процедури.

5.3.3 **Збіжність**

Збіжності досягають, якщо ті самі результати отримують за таких умов:

— Використання такої самої процедури та методики;

— Використання таких самих інструментів та за таких самих умов; а також

— Може бути повторено в будь-який час після первісного тесту.

DEFR з належними навичками та досвідом повинен мати змогу починати всі процеси, описані в документації, та отримувати такі самі результати без настанови або інтерпретації. DEFR повинен бути обізнаним, що можуть бути обставини, коли тест не може бути повторено, наприклад, якщо первісний жорсткий диск було скопійовано та повернуто в експлуатацію, або коли об’єкт має нестійку пам’ять. У цьому разі DEFR повинен гарантувати, що процес здобуття є надійним. Для досягнення збіжності мають бути контроль якості та документація.

5.3.4 **Відтворюваність**

Відтворюваності досягають, якщо ті самі результати тесту отримують за таких умов:

— Використання такої самої методики вимірювання;

— Використання інших інструментів та за інших умов;

— Може бути відтворено в будь-який час після первісного тесту.

Потреба у відтворюванні результатів змінюється залежно від юрисдикції та обставин, тому DEFR чи особа, яка здійснює відтворювання, має бути поінформованою стосовно прийнятних умов.

5.3.5 **Відповідність юрисдикції**

DEFR повинен мати змогу доказати відповідність юрисдикції усіх дій та методів, застосованих під час оброблення потенційних цифрових доказів. Відповідності юрисдикції може бути досягнуто демонстрацією того, що такі рішення є найкращим вибором для отримання всіх потенційних цифрових доказів. Інші DEFR або DES можуть також показати це за допомогою успішного відтворювання або затвердження дій та використовуваних методів.

В інтересах конкретної організації наймати DEFR або DES, які мають основні навички та компетенцію, як описано в додатку А цього стандарту. Це буде гарантувати, що під час оброблення потенційних цифрових доказів буде застосовано правильні процеси та процедури для забезпечення кінцевого збереження цифрових доказів, які можуть мати доказове значення. Це також гарантує, що організація буде мати змогу використання потенційних

цифрових доказів, наприклад, у своїх дисциплінарних процедурах або сприяти обміну потенційними цифровими доказами між юрисдикціями.

Примітка. Компетентність, описану в додатку A, обмежено функціями DEFR, що сумісна з роллю DES, як визначено в 3.8.

5.4 **Процеси оброблення цифрових доказів**

5.4.1 ***Загальні питання***

Хоча повний процес оброблення цифрових доказів охоплює інші діяльності (наприклад, представлення, контроль тощо), сфера застосування в цьому стандарті охоплює тільки початковий процес оброблення, який складається з ідентифікації, збирання, здобуття та збереження потенційних цифрових доказів.

Цифрові докази можуть бути нестійкими за природою. Вони можуть змінюватися, псуватися або руйнуватися під час неправильного оброблення або перевірення. Обробники цифрових доказів мають бути компетентними стосовно ідентифікації та керування ризиками та послідовності потенційних напрямів дій, якщо мають справу із цифровими доказами. Неправильна робота цифрових пристроїв для оброблення може зробити потенційні цифрові докази, яка містять ці прилади, непридатними.

DEFR та DES повинні підтримувати задокументовані процедури для гарантування цілісності та надійності потенційних цифрових доказів. Ці процедури мають містити настанови щодо оброблення джерел потенційних цифрових доказів та ґрунтуватися на таких фундаментальних принципах:

— Мінімізування оброблення первісних цифрових пристроїв або потенційних цифрових доказів;

— Пояснення будь-яких змін та документування запроваджених дій (щоб експерт мав змогу сформувати висновок щодо надійності);

— Відповідність локальним правилам стосовно доказів; та

— DEFR та DES не повинні виконувати дій поза межами їхньої компетентності.

Потенційні цифрові докази мають зберігатися відповідно до цих фундаментальних принципів та вимог оброблення потенційних цифрових доказів. Усі дії та пояснення потрібно задокументовувати, особливо у випадках, якщо може бути внесено невідворотні зміни.

Кожен процес оброблення цифрових доказів, тобто ідентифікація, збирання, здобуття та збереження докладно описано в наступних розділах.

5.4.2 ***Ідентифікація***

Цифрові докази наведено у фізичній та логічній формах. Фізична форма вміщує презентацію даних усередині реального приладу. Логічна форма потенційних цифрових доказів належить до віртуальної презентації даних усередині приладу.

Процес ідентифікації вміщує пошук, розпізнавання та документування потенційного цифрового доказу. Процес ідентифікації має ідентифікувати носій для збереження цифрових даних та пристрої для оброблення, які можуть містити потенційні цифрові докази, що стосуються інциденту. Цей процес також містить діяльність щодо визначення пріоритетів збирання доказів, який ґрунтується на їхній несталості. Цю несталість даних має бути ідентифікованою для гарантування процесів правильного збирання та здобуття даних для мінімізації пошкодження потенційних цифрових доказів та отримання найкращих доказів.

Додатково, процес має ідентифікувати ймовірність наявності прихованих потенційних цифрових доказів. DEFR та DES повинні бути обізнаними, що не всі типи носіїв для збереження цифрових даних може бути легко ідентифіковано та визначено їхнє місце розташування, наприклад, хмарні обчислювання, NAS та SAN — це додає віртуальні компоненти в процес ідентифікації.

DEFR повинен систематично здійснювати ретельний пошук елементів, які можуть містити по- тенційні цифрові докази. Різні типи цифрових пристроїв, які можуть містити потенційні цифрові докази, можуть бути легко пропущені (наприклад, через малий розмір), піддані сумніву або змішані з іншими матеріалами, що не стосуються справи.

Пункти 6.1 та 6.6 надають більше інформації стосовно послідовності аспектів охорони, пакування та позначення в процесі ідентифікації цифрових доказів. Розділ 7 визначає настанови, які стосуються специфічних моментів ідентифікації, збирання, здобуття та збереження цифрових доказів.

5.4.3 ***Збирання***

Якщо цифрові пристрої, які можуть містити потенційні цифрові докази, ідентифіковано, DEFR та DES повинні прийняти рішення щодо застосування збирання чи здобуття як наступних процесів. Є низка рішень, які на це впливають, докладніше розглянутих у розділі 7. Це рішення має ґрунтуватися на конкретних обставинах.

Збирання — це процес у процесі оброблення цифрових доказів, де пристрої, які можуть містити потенційні цифрові докази, переносяться з їхнього первісного місця розташування до лабораторії або іншого контрольованого середовища для подальшого здобуття потенційних цифрових доказів та аналізування. Пристрої, які містять потенційні цифрові докази, можуть знаходиться в одному з двох станів: коли систему ввімкнено або коли систему вимкнено. Залежно від стану приладу потрібні різні підходи та інструменти. Локальні процедури можуть застосовувати підходи та інструменти, використовувані для процесу збирання.

Цей процес вміщує документування підходу в цілому, а також пакування цих приладів перед тран- спортуванням. Для DEFR та DES важливо зібрати будь-які матеріали, які можуть бути пов’язаними з потенційною цифровою інформацією (наприклад, папір із записаними паролями, шинами та коннекторами живлення для підключених системних приладів). Якщо не буде застосовано належну обережність, потенційні цифрові докази можуть бути втраченими або пошкодженими. DEFR та DES повинні визначити кращі з можливих методів, ґрунтуючись на конкретній ситуації, вартості й часі, та задокументувати це рішення використання специфічного методу.

Примітка 1. Перенесення носія для збереження цифрових даних не завжди рекомендовано та DEFR повинен бути впевненим, що вони мають компетенцію для перенесення носія для збереження цифрових даних, та усвідомлювати, коли це доречно та дозволено робити.

Примітка 2. Деталі стосовно незібраних цифрових пристроїв має бути задокументовано відповідно до застосовуваної юрисдикції, та відповідно до вимог цієї юрисдикції.

5.4.4 ***Здобуття***

Процес здобуття вміщує створення копії цифрових доказів (наприклад, повного жорсткого диску, його частини, вибраних файлів) та документування використовуваних методів і застосованих дій. DEFR повинен визначити належний метод здобуття, ґрунтуючись на конкретної ситуації, вартості і часі, та задокументувати це рішення використання специфічного методу або інструментів.

Методи, використовувані для здобуття потенційних цифрових доказів, мають бути докладно задокументованими та, якщо це можливо, бути відтворюваними або мати змогу перевірення компетентним DEFR. DEFR або DES повинні здобувати потенційні цифрові докази так, щоб максимально зменшити втручання, де це можливо, щоб запобігти змінам, які може бути внесено. Для застосування цього процесу DEFR повинен розглянути найбільш належний метод для використання. Якщо цей процес призведе до невідворотних змін у цифрових даних, усі виконані дії, має бути задокументовано для врахування змін у даних.

Запроваджуваний метод має забезпечити копіювання цифрових доказів з потенційних цифрових доказів або цифрового пристрою, який може містити потенційні цифрові докази. Як первісне джерело, так і копія потенційного цифрового доказу мають бути підтверджені засвідченою функцією верифікації (засвідчується точність у цей момент часу), що є прийнятною для особи, яка буде використовувати цей доказ. Первісне джерело та кожна копія цифрового доказу має давати такий самий результат функції верифікації.

Процес верифікації не може бути зроблено за деяких обставин, наприклад, під час здобуття потенційних цифрових доказів з працюючої системи, якщо первісна копія містить помилкові сектори, або період часу здобуття є обмеженим. У таких випадках DEFR повинен використовувати найкращі можливі доступні методи та мати змогу підтвердити й захистити вибір цього методу. Якщо утворення образу не може бути підтвердженим, тоді це необхідно задокументувати та підтвердити. Якщо потрібно, запроваджуваний метод повинен мати змогу отримання локалізованого та нелокалізованого простору.

Примітка 1. Якщо не може бути застосовано процес підтвердження для всього джерела через помилки на джерелі, може бути використано ті частини джерела, які може бути надійно прочитано.

Можуть виникнути ситуації, у яких неможливо чи недозволено створити копію цифрового доказу, наприклад, якщо джерело є занадто великим. У таких випадках DEFR може здійснити логічне здобуття, ціллю якого будуть тільки специфічні типи даних, директорії чи окремі місця. В основному це застосовується на рівні файлів і сегментів. Під час логічного здобуття потенційних цифрових доказів можуть бути скопійовані активні файли та нефайлові структури виділеного простору; знищені файли та невиділений простір на носії для збереження цифрових даних можуть бути не скопійованими залежно від застосовуваного методу. Цей метод може бути корисним в інших ситуаціях, коли розглядувані критичні системи не може бути зупинено.

Примітка 2. Деякі юрисдикції можуть потребувати спеціального оброблення даних; наприклад, їхнє запечатування в присутності власника даних. Запечатування має бути зроблено відповідно до локальних вимог (законодавство та процедури).

5.4.5 ***Збереження***

Потенційні цифрові докази має бути збережено для гарантування їхньої придатності в розслідуванні. Важливо захистити цілісність доказів. Процес збереження містить захист від втручання та псування потенційних цифрових доказів та цифрових приладів, які можуть містити потенційні цифрові докази. Процес збереження має бути ініційованим та підтримуватися протягом процесів оброблення цифрових доказів, починаючи з ідентифікації цифрових приладів, які можуть містити потенційні цифрові докази.

У найкращому сценарії не повинно бути псування даних чи будь-яких метаданих, пов’язаних з ними (наприклад, дата та штампи часу). DEFR повинен мати змогу показати, що доказ не було модифіковано з моменту, коли його було зібрано чи здобуто, чи було зроблено логічні обґрунтування та дії було задокументовано, якщо було внесено невідворотні зміни.

Примітка. У деяких випадках потрібна конфіденційність потенційних цифрових доказів, або є вимоги бізнесу чи законодавчі вимоги (наприклад, приватність). Потенційні цифрові докази мають зберігатися так, щоб гарантувати конфіденційність даних.

6 КЛЮЧОВІ КОМПОНЕНТИ ІДЕНТИФІКАЦІЇ, ЗБИРАННЯ, ЗДОБУТТЯ ТА ЗБЕРЕЖЕННЯ ЦИФРОВИХ ДОКАЗІВ

6.1 Хронологічне документування

У будь-яких дослідженнях DEFR повинен мати змогу звітувати про всі здобуті дані та прилади в той час, коли вони знаходяться під захистом DEFR. Запис хронологічного документування є документом, який показує хронологію переміщень та оброблення потенційних цифрових доказів. Вона має охоплювати час від процесу збирання або здобуття.

Зазвичай, її супроводжує простежування історії елемента від часу, коли його було ідентифіковано, зібрано або здобуто командою дослідників до поточного статусу та місця знаходження.

Запис хронологічного документування є документом чи набором пов'язаних документів, які деталізують хронологічне документування та записи, хто відповідав за оброблення потенційних цифрових доказі, або у вигляді цифрових даних, або в іншому форматі (як паперові нотатки). Ціллю підтримання записів хронологічного документування є змога ідентифікації доступу та переміщення потенційних цифрових доказів у будь-якій точці часу. Самі записи хронологічного документування можуть містити більше ніж один документ, наприклад, для потенційних цифрових доказів має бути сучасний документ, у якому записано здобуття цифрових даних на конкретному пристрої, переміщення цього пристрою та документація, яка містить послідовні виписки або копії потенційних цифрових доказів для аналізування та інших цілей.

Записи хронологічного документування мають містити таку інформацію, щонайменше:

Унікальний ідентифікатор доказу;

— Хто мав доступ до доказу та час і місце, де це зроблено;

— Хто перевіряв доказ під час уведення в та виведення з обладнання збереження доказу та коли це було зроблено;

— Чому доказ було перевірено (в якому випадку та з якою ціллю) та відповідний дозвіл, якщо його було надано; та

— Будь-які невідворотні зміни в потенційних цифрових доказах, а також ім'я особи, відповідальної за це та юрисдикцію для внесення цих змін.

Хронологічне документування має бути підтримувано протягом усього часу життя доказів та зберігатися протягом визначеного періоду часу після завершення часу життя доказів — цей період часу може бути вста- новлено відповідно до локального законодавства збирання та застосування доказів. Його має бути встановлено від моменту, коли цифрові прилади та/або потенційні цифрові докази здобуто та не повинен змінюватися.

Примітка. Деякі юрисдикції можуть мати спеціальні вимоги стосовно хронологічного документування. DEFR повинен виконувати ці вимоги.

6.2 **Застороги на місці інциденту**

6.2.1 ***Загальні положення***

DEFR повинен застосовувати дії для убезпечення та захисту місця знаходження потенційних цифрових доказів, якщо вони наставали в цьому місці. Ця діяльність має підтримувати таке, залежно від локальних законів:

— Убезпечити та контролювати місце, що містить пристрої;

— Визначити, хто винен у змінах їхнього місцезнаходження;

— Гарантувати, що особи віддалені від пристроїв та елементів живлення;

— Документувати будь-кого, хто мав доступ до місцезнаходження, та будь-кого, хто має причини бути причетним до епізоду інциденту;

— Якщо пристрій увімкнено, не треба його вимикати, та якщо пристрій вимкнено, не треба його вмикати;

— Якщо це можливо, задокументувати (наприклад, схема, фото або відео) місце, усі компоненти та кабелі в їхньому первісному положенні. Якщо камери та/або відеокамери немає, нарисувати схематичний план системи та позначки портів та кабелів так, щоб систему могло бути підтверджено та відновлено пізніше;

— Якщо це дозволено, дослідити місце для пошуку елементів, таких як причеплені нотатки, що- денники, папери, ноутбуки чи описи обладнання та програмного забезпечення з критичними деталями стосовно пристроїв, таких як паролі та PIN.

Примітка 1. Деякі юрисдикції можуть накладати спеціальні вимоги стосовно визнання фото та відеодоказів. DEFR повинен виконувати ці вимоги.

Примітка 2. DEFR повинен бути обізнаним, що потенційні цифрові докази можуть не завжди знаходитися в очевидних місцях, таких як розподілені або віртуальні сховища.

DEFR повинен із самого початку зазначити всі ризики, які виникають під час виконання всіх про- цесів протягом розслідування. Необхідно розглянути, як захистити персонал та потенційні цифрові докази на місці інциденту.

6.2.2 ***Персонал***

Важливо застосувати оцінювання ризиків стосовно безпеки персоналу до початку процесу, оскільки безпека персоналу, задіяного в процесі, є життєво важливою.

Питання, які мають бути розглянутими під час оцінювання ризиків стосовно персоналу включають, але не обмежуються, таке:

— Чи будуть присутні особи(-а), яких досліджують? Якщо присутні, чи мають вони схильність до насилля?

— Протягом якого часу доби буде проведено цю операцію?

— Чи може місце інциденту бути ізольовано від свідків?

— Чи наявна зброя в цьому місці?

— Чи є будь-який фізичний ризик для осіб, що будуть присутні?

— Чи може будь-що в близькості, охоплюючи пристрої, налагоджене так, щоб спричинити фізичне лихо, якщо неналежно обробляється, наприклад, приховану пастку?

— Чи можуть матеріали, що їх має бути зібрано, мати деяку ймовірність отримати фізіологічне ушкодження або порушення?

— Чи може місце інциденту розглядатися як небезпечне?

— Чи може оточення мати вплив на потенційний ризик?

6.2.3 ***Потенційний цифровий доказ***

DEFR повинен бути обережним під час використання специфічних інструментів для збирання або здобуття потенційних цифрових доказів. Невизначені ризики перед виконанням дій можуть призвести до втрати частини або всього в цілому потенційного цифрового доказу через технологію, запроваджену протягом збирання або здобуття.

Ризики має бути оцінено для зменшення впливу стосовно подальших пошкоджень.

Оцінювання ризиків охоплює систематичну оцінку ризиків та потенційного впливу, який вони можуть мати на дослідження цифрових доказів. Аспекти, які потрібно розглянути протягом оцінювання ризиків стосовно потенційних цифрових доказів, охоплюють, але не обмежуються таким:

— Який тип методів збирання/здобуття застосовують?

— Яке обладнання може бути потрібно на місці?

— Який рівень нестабільності (нестійкості) даних та інформації, пов’язаних з потенційними цифровими доказами?

— Чи можливий віддалений доступ до будь-яких цифрових приладів та чи складає він загрозу цілісності доказів?

— Що трапиться, якщо дані/обладнання буде пошкоджено?

— Чи може бути дані скомпрометовано?

— Чи може цифровий пристрій бути сконфігуровано так, щоб зруйнувати (наприклад, за допомогою логічної бомби), пошкодити або заплутати дані, якщо його вимкнути чи отримати доступ неконтрольовано?

6.3 **Ролі та відповідальності**

Роль DEFR охоплює ідентифікацію, збирання, здобуття та збереження потенційних цифрових доказів на місці інциденту. Вона охоплює розроблення звіту щодо збирання та здобуття, але звіт стосовно аналізування не є необхідним. Роль DEFR також охоплює гарантування цілісності й автентичності потенційних цифрових доказів. Для виконання своєї ролі DEFR повинен мати достатній досвід, навички та знання стосовно оброблення цифрових доказів. Це є критичним, оскільки потенційні цифрові докази можуть бути легко пошкоджені.

DEFR може також вимагати допомоги від персоналу технічної підтримки у відповідній сфері. Роль DES охоплює здійснення технічного підтримування DEFR в ідентифікації, збиранні, здобутті та збереженні потенційних цифрових доказів на місці інциденту. DES виконує спеціалізовану експертизу для DEFR. Матриця компетентності для DEFR (див. додаток A) служить як настанова для ідентифікації відповідних рівнів їх компетенції.

Примітка. У контексті оброблення інциденту за наявності ISIRT в ISO/IEC 27035:2011 розглянуто ролі DEFR та DES як членів ISIRT.

6.4 **Компетентність**

DEFR та DES повинні мати належні технічні та законодавчі компетенції (тобто, надані в додатку A) та продемонструвати, що вони пройшли відповідне навчання та мають достатнє технічне та законодавче розуміння для належного оброблення потенційних цифрових доказів.

Це охоплює розуміння процесів та методів, прийнятних для оброблення потенційних джерел цифрових доказів. Відповідні навички будуть потрібні DEFR для оброблення цифрових пристроїв, які містять потенційні цифрові докази. Наявність найкращого набору інструментів не буде гарантувати якості цифрових доказів, якщо DEFR не має компетенції у виконанні цих завдань.

Деякі юрисдикції приписують, як DEFR повинен доказувати свою кваліфікацію. Відповідальністю DEFR є гарантування того, що його належно поінформовано про те, як зробити це у відповідній юрисдикції. Якщо потрібно, DEFR та/або DES повинні мати змогу показати, що вони мають компетенцію для оброблення потенційних цифрових доказів з використанням інструментів та методів, визначених для виконання цих завдань. Також потрібно, щоб DEFR мав змогу надавати доказ своєї поточної компетенції.

Деякими передумовами для DEFR є такі:

— Вони мають належно та відповідно пройти навчання стосовно роботи із цифровими пристроями стосовно дослідницької діяльності;

— Вони мають показати відповідним органам у відповідній сфері та підтримувати свої навички та компетентність в обробленні потенційних цифрових доказів; та

— Відповідальністю особи(-іб) та роботодавця є гарантування, що вони відповідно пройшли навчання та підтримують навички та компетентність.

Примітка. Компетентність DEFR може змінюватися від однієї юрисдикції до іншої.

6.5 **Запровадження необхідної обережності**

Треба уникати будь-яких дій, які призведуть до псування потенційних цифрових доказів, що зберігаються в цифрових пристроях через навмисні або ненавмисні дії. Наприклад, піддавання впливу магнітних полів може псувати потенційні цифрові докази, які містяться на магнітних носіях для збереження. DEFR не повинен здійснювати доступу до цифрових пристроїв, таких що знімають дамп пам’яті із цифрових пристроїв наживо, крім випадків, якщо вони мають належну компетентність та використовують надійні та затверджені процеси.

Є деякі обставини, коли неможливо збирати чи здобувати потенційні цифрові докази. DEFR повинен розглянути такі обставини, але не обмежуватися тільки ними:

— Якщо немає законних прав чи авторизації для збирання цифрових доказів;

— Якщо є зобов’язання щодо використання інших методів (наприклад, для уникнення переривання бізнесу);

— Якщо DEFR бажає охопити особливості виконання операцій протягом зловживання системою;

— Якщо збирання або здобуття мають здійснюватися приховано, якщо це вважається легальним у рамках юрисдикції;

— Якщо це критичний пристрій, який не може простоювати;

— Якщо фізичний розмір цифрового пристрою є дуже великим, наприклад сервер у дата-центрі або RAID-система;

— Якщо це критичний цифровий пристрій безпеки, який ставить під загрозу життя, якщо буде зупинено; та

— Якщо це цифровий пристрій, який також надає послуги невинним сторонам.

6.6 **Документація**

Документація є критичною під час оброблення цифрових пристроїв, які можуть містити потенційні цифрові докази. DEFR повинен виконувати таке під час документування:

— Кожну виконувану дію має бути задокументовано. Це гарантує, що жодної деталі не було упущено під час виконання процесів ідентифікації, збирання, здобуття та збереження. Це може бути також доречним під час транскордонних розслідувань, там де потенційні цифрові докази, які збираються з іншої частини земної кулі, може бути відповідно простежено.

— DEFR повинен бути уважним до встановлення часу та дати, якщо цифрові пристрої увімкнено. Порівняти встановлення часу з надійним джерелом часу, таким як час, синхронізованим з надійним джерелом та який можливо простежити. Ці встановлення часу має бути задокументовано та зазначено, якщо є будь-яка різниця. Деякі системи потребують великого числа взаємодій з користувачем для отримання встановлення часу та дати. DEFR повинен бути обережним, щоб не модифікувати систему. Тільки належно навчений персонал повинен виправляти ці встановлення.

— DEFR повинен задокументувати все, що видно на екрані цифрового пристрою: активні програми та процеси, а також назви відкритих документів. Це документування має охоплювати опис того, що видимо, оскільки деякі зловмисні програми можуть маскуватися під добре відоме програмне забезпечення.

— Будь-які переміщення цифрових пристроїв має бути задокументовано відповідно до локальних вимог.

— Документувати всі унікальні ідентифікатори цифрових пристроїв та приєднаних частин, таких як серійні номери та унікальне маркування.

Приклади мінімального набору документації для обміну потенційними цифровими доказами між різними юрисдикціями наведено в додатку Б.

Примітка. Для докладнішої інформації стосовно документації треба звернутися до розділу керування документами та розділу керування записами ISO/IEC 17025:2005.

6.7 **Інструктаж**

6.7.1 ***Загальні положення***

Важливо, щоб DEFR та DES були відповідно проінструктовані уповноваженим органом перед виконанням їхніх завдань, особливо стосовно деяких законів про конфіденційність та обмеження (тобто, потрібні базисні знання). Важливо мати формальну сесію інструктажу для розуміння інциденту, що треба очікувати та не очікувати протягом розслідувань, та нагадування стосовно недопущення втручання та псування доказів. Інструктаж має бути достатньо суттєвим для членів, прийнятно підготовлених у розподілі ролей та відповідальності; отже буде гарантовано вилучення всіх прийнятних потенційних цифрових доказів.

6.7.2 ***Особливість цифрових доказів***

Сесія інструктажу, сфокусована чітко на специфічних настановах щодо цифрових доказів, потрібна для інформування DEFR щодо особливостей, притаманних розслідуванню. Протягом цієї сесії інструктажу DEFR та DES повинні бути ознайомлені з відповідною інформацією та докладними інструкціями стосовно потенційних цифрових доказів, які має бути зібрано чи здобуто. Це може охоплювати:

— Тип інциденту (якщо відомий);

— Дату й час інциденту (якщо відомі);

— План розслідування (збирання та/або здобуття, відома мережева діяльність, відомі вимоги щодо нестабільних (нестійких) даних, тощо);

— Розглянути, де і як потенційні цифрові докази будуть зберігатися/транспортуватися після зби- рання або здобуття;

— Специфічні інструменти, потрібні для здобуття потенційних цифрових доказів;

— Потенційні цифрові докази, які потребують специфічних типів досліджень;

— Обладнання та описи стосовно цифрових пристроїв;

— Нагадування членам команди про потребу відключити будь-які можливості Bluetooth або Wi-Fi на їхніх телефонах/комп'ютерах, щоб вони не могли випадково взаємодіяти із цифровими пристроями, за винятком телефонів/комп'ютерів, використовуваних для виявлення зв'язків.

— Важливість документування протягом розслідування; та

— Запровадження законодавчих або інших чинників, які забороняють збирання будь-яких пристроїв та потенційних цифрових доказів, що вони містять.

Ця особлива сесія інструктажу може бути частиною загальної сесії інструктажу, описаною в розділі 6.7.1.

6.7.3 ***Особливості персоналу***

Сесія інструктажу, сфокусована на специфічних настановах щодо персоналу, потрібна для ін- формування DEFR щодо особливостей, притаманних сторонам, які беруть участь у розслідуванні. Протягом цієї сесії інструктажу команда дослідників має бути ознайомлена з інструкціями стосовно персоналу. Це може охоплювати:

— Призначення, ролі та відповідальність членів команди дослідників на місці інциденту;

— Чи очікується, що інші сторони (медичний персонал, біологічні судові дослідники тощо) будуть брати участь у цих розслідуваннях;

— Вимогу до членів команди дослідників не допускати технічної допомоги від будь-яких неавторизованих осіб; та

— Вимогу до членів команди дослідників суворо дотримуватися процедури, щоб мінімізувати ризик псування потенційних цифрових доказів, такого як уникнення використання інструментів або матеріалів, які можуть спричиняти або емітувати статичну електрику або магнітне поле, що може пошкодити або зруйнувати потенційні цифрові докази.

Ця особлива сесія інструктажу може бути частиною загальної сесії інструктажу, описаною в розділі 6.7.1.

6.7.4 ***Інциденти реального часу***

Найбільш бажано, щоб розслідування інциденту було заплановано заздалегідь, але є обставини (наприклад, якщо інцидент розвивається та створює відклики), де повне планування не можливо. У таких ситуаціях команда має бути проінструктовано стосовно початкової стратегії та тактики розслідування та має дозвіл розробити нову стратегію та тактику у відповідь на існуючі умови. Інформація стосовно цього інциденту, як він розвивається, має бути поширена серед членів команди так швидко, як це можливо, щоб гарантувати, що рішення стосовно дій, які треба здійснити, було визначено ефективно та з урахуванням потреб юрисдикції.

6.7.5 ***Інша інформація стосовно інструктажу***

Окремо від інструктажу щодо цифрових доказів та персоналу, команді дослідників має бути надано інструктаж щодо іншої важливої інформації, яка охоплює:

— Визначення місця, де буде проведено розслідування, охоплюючи назву організації, адресу та карту місцевості (якщо можливо);

— Дозвіл на розслідування;

— Подробиці пошукових повноважень та інших повноважень, притаманних цьому розслідуванню, охоплюючи обмеження пошуку та конфіскації;

— Законодавчі аспекти й особливості залучення;

— Часовий діапазон розслідування;

— Обладнання, яке потрібно доставити на місце інциденту для досліджень;

— Інформація щодо логістики; та

— Потенційний конфлікт інтересів.

DEFR та DES повинні уникати ситуацій, коли може бути висунуто обвинувачення в прихованій упередженості. Прикладом прихованої упередженості є ситуація, коли DEFR копіює один комп'ютер, а не інший (який, як пізніше виявляється, містить виправдовувальні докази), ґрунтуючись на своїх уявленнях, що сформовано інструктажем.

6.8 **Визначення пріоритетів збирання та здобуття**

Під час визначення пріоритетів збирання або здобуття потенційних цифрових доказів, обов'язковим для DEFR є розуміння причин для збирання або здобуття потенційних цифрових доказів. Як загальний принцип, DEFR повинен спробувати отримати максимальну кількість даних, збережених за допомогою дій зі збирання та здобуття. Однак, може бути потрібним визначити пріоритетні елементи залежно від значення нестійкості та/або значущості/потенційних цифрових доказів. Елементи з високим релевантним/потенційним значенням цифрових доказів є такі, що найімовірніше містять дані, які безпосередньо стосуються розслідуваного інциденту.

Визначення пріоритетів унаслідок пошкодження може бути запроваджено, тільки якщо цього потребують специфічні обставини розслідуваного випадку. Потенційні цифрові докази може бути розділено на дві категорії: нестійкі та сталі. Нестійкі дані може бути легко зіпсовано або втрачено назавжди, якщо не за стосовують належну обережність для захисту цих даних. Наприклад, вимикання живлення цифрового пристрою може призвести до втрати нестійких даних. Сталі дані залишаються в середовище навіть якщо живлення вимкнено.

Оскільки деякі типи цифрових доказів можуть мати короткий термін життя, потенційні цифрові докази можуть бути легко зіпсовані або порушені. Там, де незрозуміло, чи містить циф ровий пристрій потенційні цифрові докази, або які елементи є важливішими, може виникнути потреба перевірити їх перед збиранням з використанням процесу визначення пріоритетів. Цифрові пристрої, які необхідно розглянути для збирання, охоплюють, але не обмежуються: IT-обладнанням та носіями для збереження цифрових даних, CCTV-системами, PED, автоматизованими системами, системами контролю та імпровізованими електронними системами. З початку треба здобути найбільш нестійкі по- тенційні цифрові докази, такі як RAV, простір свопінгу, запущені процеси тощо. DEFR повинен володіти глибокими знаннями для визначення пріоритетів відповідно до нестійкості.

Протягом ідентифікації DEFR повинен:

— Визначити пріоритети потенційних цифрових доказів, які може бути втрачено назавжди, якщо буде вимкнено живлення; та

— Прийняти швидкі дії для збирання та здобуття цих даних за допомогою затверджених методів.

Примітка 1. Деякі нестійкі дані можуть змінюватися через чинники, які охоплюють, але не обмежуються, переміщення, час та зміни в оточенні цифрових пристроїв — необхідно гарантувати, що такі дані збережено перед переміщення цього пристрою.

Примітка 2. Цифрові пристрої, які містять потенційні цифрові докази, можуть бути джерелом фізичних доказів (наприклад, відбитків пальців, DNA тощо). DEFR повинен бути обережним, щоб не зіпсувати такі докази, та координувати свої наступні дії з відпо- відальними особами, які збирають такі докази.

Примітка 3. Якщо допустимо наявність шифрування або шкідливого програмного забезпечення, бажано перевірити нестійкі дані.

За таких обставин час може бути обмежувальним чинником протягом дослідження. У таких випадках треба віддавати перевагу потенційним цифровим доказам, ідентифікованим як притаманним цьому специфічному інциденту.

6.9 **Збереження потенційних цифрових даних**

6.9.1 ***Загальні положення***

Під час збереження здобутих потенційних цифрових доказів та зібраних цифрових приладів під час пакування важливо убезпечити ці елементи так, щоб уникати псування або порушення. Псування може бути результатом несприятливих змін магнітного поля та електричного живлення, впливу тепла, високої або низької вологості, а також удару та вібрацій. Порушення може бути результатом дій з навмисного внесення змін або допущення внесення змін у потенційні цифрові докази. Тому є дуже критичним захистити потенційні цифрові докази в найкращий можливий спосіб та найменш використовувати первісні дані. Важливо, щоб DEFR був ознайомлений з вимогами щодо пакування у використовуваній юрисдикції.

6.9.2 ***Збереження потенційних цифрових доказів***

Усі зібрані цифрові пристрої та здобуті потенційні цифрові докази має бути захищено, наскільки це можливо, від втрати, порушення або псування. Найважливішою діяльністю в процесі збереження є підтримання цілісності та автентичності потенційних цифрових доказів та їхнього хронологічного документування.

Зібрані цифрові пристрої та здобуті потенційні цифрові докази потрібно зберігати в пристроях збереження доказів, де запроваджено заходи фізичної безпеки, такі як системи контролю доступу, системи спостереження або системи виявлення вторгнень або в іншому контрольованому середовищі для збереження потенційних цифрових доказів. Основними цілями фізичної безпеки є захист та уникнення втрат, пошкоджень та порушень, а також уможливлення здійснення аудиту.

Зібрані цифрові пристрої перед переміщенням в інше місце має бути обгорнуто чи розміщено у відповідному пакованні, придатному для цього пристрою для уникнення спотворення цифрового пристрою(-їв). Потрібно використовувати паковання, яке захищає від ударів для уникнення фізичного пошкодження будь-яких компонентів пристрою(-їв).

— DEFR повинен розглянути чутливість цифрового пристрою до статичної електрики. Якщо це дійсно існує, пристрій має бути захищено антистатичною упаковкою.

— Основні блоки системи та ноутбуки потребують захисту в належному контейнері для уникнення пошкодження або псування потенційних цифрових доказів, які можуть залишатися там.

Примітка. Використання паковання Фарадея або іншого паковання з екрануванням від радіочастот може збільшити витік батареї мобільного телефону. Це може потребувати забезпечення додаткового живлення для пристрою, доки він знаходиться в середині паковання, якщо ресурси дозволяють.

6.9.3 ***Пакування цифрових пристроїв та потенційних цифрових доказів***

6.9.3.1 Основні дії: *пакування потенційних цифрових доказів*

Основні дії потрібно виконувати, навіть якщо є зиск не виконувати їх. Це можна також розглядати як мінімальні дії, які треба виконувати. Протягом пакування DEFR повинен записувати та звертати увагу на такі основні дії:

— Не торкатися магнітних стрічок, краще працювати зі стрічками в їхніх захисних контейнерах або торкатися лише в місцях, які завідомо не містять даних (наприклад, край оптичних дисків). Це має бути зроблено, тільки якщо DEFR одягає спеціальну рукавичку.

Примітка. Спеціальні місця середовища збереження, про які відомо, що вони не містять даних, залежать від типу середовища. DEFR відповідає за знання новітніх технологій та повинен бути ознайомлений з обробленням середовищ збереження.

— Для гарантування правильної ідентифікації DEFR повинен позначати етикетками всі потенційні цифрові докази. Деякі юрисдикції мають спеціальні вимоги стосовно формату етикеток доказового матеріалу. DEFR повинен знати, та підтвердити вимоги, які потрібно застосовувати. DEFR повинен позначити етикетками всі потенційні цифрові докази, зібрані цифрові пристрої та будь-які частини обладнання, пов'язані з цими пристроями з етикетками, як на доказах. Етикетка не повинна розміщуватися безпосередньо на механічних частинах цифрового пристрою та не повинна закривати або приховувати важливу ідентифікаційну інформацію. Усі потенційні цифрові докази в зібраних пристроях мають здобути та повинні зберігатися так, щоб гарантувати цілісність цих доказів.

— Якщо можливо, цифрові пристрої з відкритими та рухомими елементами мають бути запечатаними за допомогою етикеток, які запобігають порушенню доказів, прийнятних до цього пристрою, і DEFR повинен підписати запечатування.

— Пристрої з несталими даними, обладнані батареями, мають регулярно перевірятися для гарантування того, що ці пристрої завжди мають достатнє живлення.

— Ідентифікувати та убезпечити цифрові пристрої в контейнері, який за своїм походженням прийнятний цьому пристрою для захисту від потенційних загроз.

— Комп'ютери та цифрові пристрої має бути запаковано так, щоб уникнути пошкодження від удару, вібрації, великий висоти, тепла та опромінення радіочастотами протягом транспортування.

— Магнітні носії для збереження цифрових даних потрібно зберігати в пакованні, яке є магнітно інертною, антистатичною та вільною від часточок.

— Цифрові докази можуть також містити приховані докази, відбитки чи біологічні докази. Якщо це так, необхідно запровадити відповідні дії для збереження цих потенційних доказів. Необхідно зробити образи цифрового доказу після того, як процеси збирання прихованих доказів, відбитків чи біологічних доказів було застосовано на цих пристроях. Однак рішення щодо визначення пріоритетів збирання доказів має бути ретельно оцінено з урахуванням можливості збереження цих доказів.

6.9.3.2 Додаткові дії: пакування потенційних цифрових доказів

Додаткові дії, які належать до дуже рекомендованих, має бути виконано.

Протягом пакування DEFR повинен записувати та звертати увагу на такі додаткові дії, якщо їх застосовують:

— Одягнути спеціальні рукавички, та гарантувати, що руки є чистими та сухими.

— Захистити цифрові пристрої від впливу електромагнітних джерел (наприклад, поліцейське радіо, гучномовці, рентген-апарати). Середовище пакування має бути вільним від статичної електрики.

— Середовище пакування має бути вільним від пилу, жиру та хімічних забруднювачів, які спричиняють псування через окиснення та конденсації вологи на магнітному шарі.

— Мінімізувати змогу копіефекту (перенесення сигналу від одного рулону стрічки до сусіднього рулону), яке може траплятися, якщо стрічки зберігаються протягом тривалого періоду без активного використання, призводячи до низької якості сигналу.

— Якщо потрібно, місця пакування мають бути вільними від UV-світла. UV може спричинити по- шкодження DNA або пошкодження деяких типів середовищ. DEFR повинен розглянути, чи може бути ризик від UV для потенційних цифрових доказів перед вибором місця пакування.

— Цифрові пристрої мають бути надійно захищені від теплового удару.

6.9.4 ***Транспортування потенційних цифрових доказів***

DEFR повинен зберігати зібрані цифрові пристрої та здобуті потенційні цифрові докази протягом транспортування. Потенційні цифрові докази не повинні залишатися без уваги протягом процесу транспортування. DEFR повинен підтримувати хронологічне документування протягом процесу транспортування для уникнення можливих пошкоджень або псування, та підтримувати цілісність та автентичність цифрових пристроїв та потенційних цифрових доказів. Якщо потенційні цифрові докази не транспортуються DEFR або DES, рекомендовано запровадити шифрування.

Примітка. DEFR повинен гарантувати, що збирання чуттєвий інформації та персональних даних виконується відповідно до законів локальної юрисдикції та нормативних документів із захисту інформації.

Протягом пакування та транспортування DEFR повинен бути уважним щодо можливої наявності електростатичних розрядів, які можуть зменшити доказове значення потенційних цифрових доказів. DEFR повинен гарантувати, що комп'ютери та цифрові пристрої запаковано безпечно для уникнення пошкоджень від ударів та вібрації.

Процес транспортування має бути дозволеним для керованого та контрольованого середовища. Рівень вологості, вогкості повітря та температура мають бути прийнятними для цифрових пристроїв. Треба уникати находження потенційних цифрових доказів та цифрових пристроїв у транспортному засобі протягом тривалих періодів та уникати їхнього знаходження за наявності UV.

У деяких юрисдикціях, якщо обставини не дозволяють, DEFR не може супроводжувати докази. У таких випадках може бути використано відповідні та авторизовані механізми транспортного засобу для гарантування належної безпеки доказів протягом транспортування. Документація стосовно транспортування та підтвердження цілісності паковання має бути частиною хронологічного документування.

7. **ПРИКЛАДИ ІДЕНТИФІКАЦІЇ**, **ЗБИРАННЯ**, **ЗДОБУТТЯ ТА ЗБЕРЕЖЕННЯ**

7.1 **Комп'ютери**, **периферійні пристрої та носії для збереження цифрових даних**

7.1.1 ***Ідентифікація***

7.1.1.1 Огляд та документування фізичного місця інциденту

У контексті цього розділу комп'ютери розглядають як окремі цифрові пристрої, які приймають, обробляють та зберігають дані й отримують результати. Такі комп'ютери не під'єднано до мережі, але їх може бути під'єднано до периферійних пристроїв, таких як принтери, сканери, веб-камери, MP3-плеери, GPS-системи, RFID-прилади тощо. Цифрові пристрої, які мають мережевий інтерфейс, але не підключені до мережі під час збирання або здобуття потенційних цифрових доказів, має бути розглянуто (для цілей цього стандарту) як окремий комп'ютер. Якщо комп'ютер має мережевий інтерфейс, але не було знайдено явних підключень, треба виконати дії для ідентифікації пристроїв, до яких він мав бути підключеним у недавньому минулому.

Зазвичай, місця інцидентів містять різні типи носіїв для збереження цифрових даних. Носії для збереження цифрових даних використовують для збереження даних від цифрових пристроїв та вони відрізняються об'ємом пам'яті. Приклади носіїв для збереження цифрових даних включають, але не обмежуються, зовнішні портативні жорсткі дисководи, флеш-носії, CD, DVD, Blu-ray диски, гнучкі диски, магнітні стрічки та карти пам'яті.

Перед тим, як можна запровадити будь-яке здобуття чи збирання, необхідно розглянути питання безпеки потенційних цифрових доказів. Ці питання описано в 6.2.1 та 6.2.2. Однак DEFR повинен бути обережним у переконанні, що пристрій, який виявляється окремим, не був нещодавно підключеним до мережі. Якщо є припущення, що зараз окремий цифровий пристрій був нещодавно відключеним, має бути зроблено спробу обробляти його як мережевий пристрій, щоб впевнитися, що інші частини мережі працюють правильно. DEFR повинен записувати та звертати увагу хоча б на таке:

— DEFR повинен задокументувати тип та назву будь-якого використовуваного цифрового пристрою та ідентифікувати всі комп'ютери та периферійні пристрої, які потрібно здобути чи зібрати протягом початковою стадії. Має бути також задокументовано серійні номери, номери ліцензій та інші ідентифікаційні позначки (охоплюючи фізичне пошкодження), там, де це можливо зробити.

— На стадії ідентифікації статус комп'ютерів та периферійних пристроїв має залишатися як є. Якщо комп'ютери вимкнено, не треба їх вмикати. Якщо комп'ютери або периферійні пристрої увімкнено, DEFR не повинен їх вимикати, що в іншому разі може зіпсувати потенційні цифрові докази.

— Якщо комп'ютери ввімкнено, DEFR повинен сфотографувати або зробити паперовий документ стосовно того, що зображено на екранах. Будь-який паперовий документ має містити опис того, що реально видно (наприклад, приблизні позиції вікон, назв та контенту).

— Пристрої, що мають батареї, які можуть розрядитися, потребують зарядки батарей для гаран- тування того, що інформацію не буде втрачено.

DEFR повинен також розглянути за допомогою детектора бездротових сигналів питання пошуку та ідентифікації бездротових сигналів від бездротових пристроїв, що може бути приховано. Можуть скластися такі обставини, коли детектор бездротових сигналів не використовують через обмеження вартості та часу, і DEFR повинен це задокументувати. Якщо буде знайдено будь-які мережеві пристрої, DEFR повинен продовжувати процес оброблення доказів, як описано в 7.2.2.2 цього стандарту. Там, де використовують активне сканування (тобто, широкополосне та/або вибіркове) для мережевих пристроїв, пристрої сканування має бути вимкнено на час оцінювання ймовірності того, що ці пристрої можуть взаємодіяти з іншими пристроями на місці. Члени команди повинні пам'ятати, що певний пристрій на місці може визначити наявність активних пристроїв сканування та використання активного сканування може призвести до тригерних подій, які можуть зіпсувати потенційні цифрові докази та можуть, в екстремальних обставинах, призвести до активації маскувальних дій.

Примітка 1. У деяких юрисдикціях дозволено вмикати цифрові пристрої на місці події для визначення їхньої доречності в роз- слідуванні, якщо наявна велика кількість цифрових пристроїв. Це відбувається з урахуванням часу оброблення та вартості, які можуть бути недоречними, якщо будуть оброблятися непричетні цифрові пристрої. Якщо пристрій було увімкнено для оцінювання на місці, DEFR повинен гарантувати, що докладні нотатки застосованих дій підтримуються протягом цього процесу.

Примітка 2. Для збереження статусу живлення цифрового пристрою має бути розглянуто результати несталості та процесу визначення пріоритетів. Якщо прийнято рішення, що найкритичніша інформація є сталою інформацією на диску, тоді треба сфотографувати екран консолі цієї працюючої системи та вимкнути її. Якщо наявна нестала інформація в пам'яті, тоді критично важливо залишити систему ввімкнутою, щоб мати змогу виконати здобуття її інформації.

7.1.1.2 Збирання нецифрових доказів

DEFR повинен розглянути збирання нецифрових доказів. Для цього лідер команди повинен ідентифікувати осіб, які відповідають за обладнання на місці. Ці особи можуть надати додаткову інформацію та документацію, таку як паролі до цифрових пристроїв та інші відповідні подробиці. DEFR повинен задокументувати імена та посади цих осіб.

DEFR може також потребувати збирання деяких доказів в опитуваннях осіб, які можуть мати корисну або потрібну інформацію щодо потенційних цифрових доказів або цифрових пристроїв, що збираються. Будь-які відповіді має бути точно задокументовано. Ці особи можуть включати системного адміністратора, власника пристрою та користувачів комп'ютера та периферійних пристроїв. Протягом такого вербального збирання доказів DEFR може

домагатися інформації такої, як конфігурація системи та пароль адміністратора/рутовий пароль. Така додаткова інформація може бути корисною на стадії аналізування потенційних цифрових доказів. Ці опитування має бути задокументовано для гарантування того, що подробиці є точними та задокументовані твердження не може бути змінено. DEFR повинен бути ознайомлено з відповідними вимогами законодавства стосовно збирання нецифрових доказів.

7.1.1.3 Процес прийняття рішень для збирання та здобуття

Під час прийняття рішення щодо збирання цифрових пристроїв або здобуття потенційних цифрових доказів необхідно розглядати кілька чинників, які охоплюють, але не обмежуються таким:

— несталість потенційних цифрових доказів, що обговорено в 5.4.2 та 6.8;

— наявність шифрування всього диску або зашифрованих частин, де парольна фраза чи ключі зберігаються як несталі дані в RAM, на зовнішніх токенах, смарт-картах, інших пристроях або середовище;

— критичність системи, наведеної в 5.4.4, 7.2.1.2 та 7.1.3.4;

— вимоги законодавства, та

— ресурси, такі як потрібний розмір сховища, наявність персоналу, часові обмеження.

На рисунку 1 зображено огляд процесу прийняття рішення запроваджувати збирання чи здобуття.

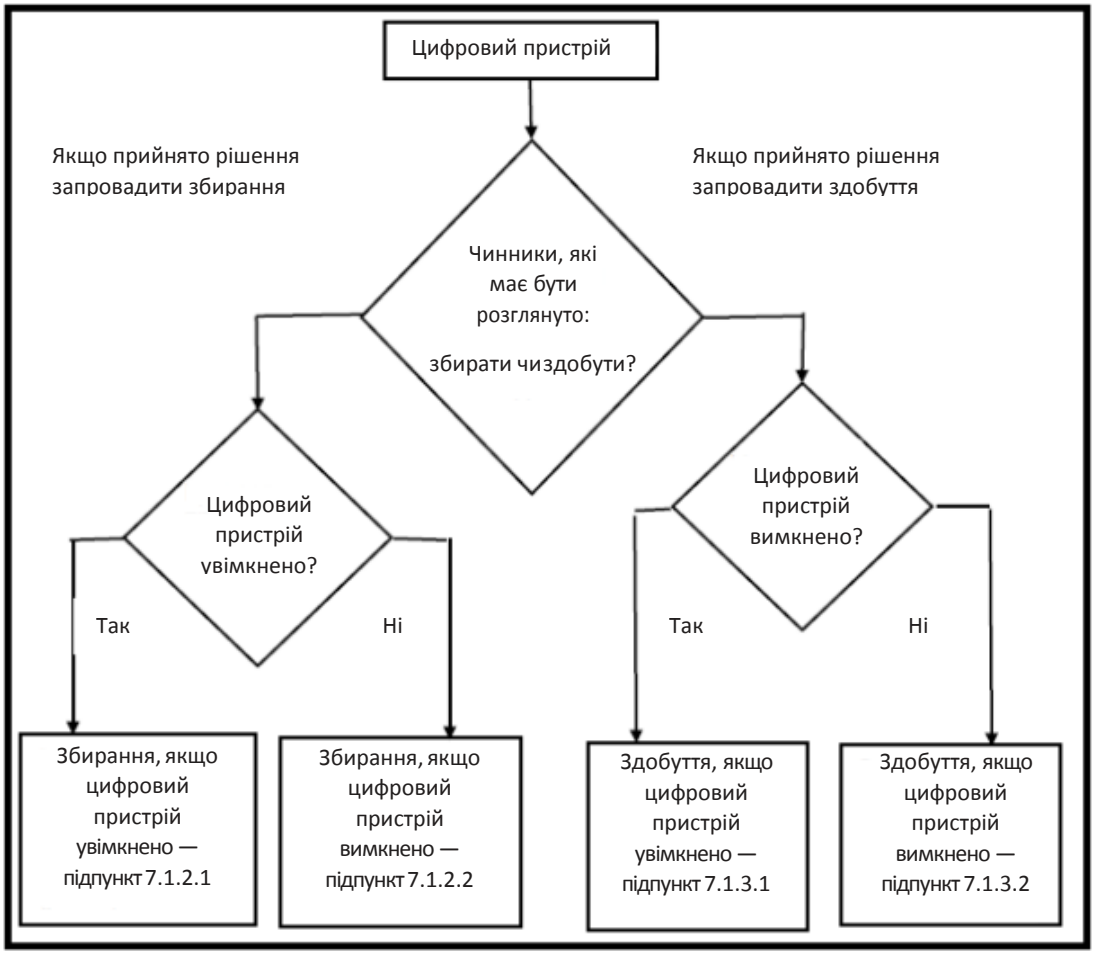

Рисунок 1 — Настанова для процесу прийняття рішення збирати чи здобути потенційні цифрові докази

7.1.2 ***Збирання***

7.1.2.1 Цифрові пристрої увімкнено

7.1.2.1.1 Загальні положення

DEFR може використовувати кілька настанов для збирання даних, якщо цифровий пристрій увімкнено. Не всі настанови є ідеальними та їх можна використовувати для будь-яких випадків; деякі настанови прийнятні тільки для специфічних випадків. Відповідно, настанови може бути покласифіковано як основні або додаткові. Основні дії потрібно застосовувати для всіх обставин, у той самий час додаткові дії потрібно запроваджувати, якщо вони доречні, та можуть бути застосовані залежно від унікального приладу чи обставин.

DEFR відповідає за знання сучасних технологій та має бути ознайомлено з настановами стосовно оброблення носіїв для збереження.

7.1.2.1.2 Основні дії: *збирання увімкнених цифрових пристроїв*

Такі основні дії має бути запроваджено в усіх випадках стосовно потенційних цифрових доказів. Ці настанови застосовують, якщо DEFR прийняв рішення, що мають збиратися цифрові пристрої, якщо їх увімкнено:

— Розглянути здобуття несталих даних із цифрових пристроїв та поточний стан перед вимкненням системи. Ключі шифрування та інші критичні дані може бути розміщено в активній пам’яті або в неактивній пам’яті, яку не буде очищено. Розглянути логічне здобуття, якщо запроваджено шифрування. У цьому разі треба враховувати, що чинна основна операційна система може бути ненадійною, тому треба розглянути використання відповідних надійних та затверджених інструментів.

— Конфігурація цифрового пристрою може визначати, чи потребує DEFR вимикання цього пристрою за допомогою звичайних адміністративних процедур чи вилку пристрою має бути вилучено з розетки живлення. DEFR може потребувати консультації з DES для визначення найкращого підходу, доречного для специфічних обставин. Якщо прийнято рішення про вилучення вилки з розетки, DEFR повинен вилучити кабель живлення, з початку вилучаючи кінець, підключений до цифрового пристрою, а не кінець, що підключений до розетки. Треба бути обережним, оскільки пристрій, підключений до UPS, може змінювати дані, якщо кабель живлення вилучається з розетки, а не з пристрою.

Примітка 1. Якщо живлення буде відключено від працюючого пристрою, будь-які потенційні докази, що зберігаються в зашифрованому вигляді, будуть недоступні, доки не буде отримано ключ дешифрування. Потенційна цінність «живих» даних може бути також втраченою, що призведе до пошкоджень або втрат людських життів, таких як корпоративні дані або цифрові пристрої, що керують медичним обладнанням. Тому, DEFR повинен гарантувати, що несталі дані будуть зібрані до вимкнення живлення.

Примітка 2. Є пристрої, які дозволяють пристрій, що увімкнений, відключити від джерела живлення та перемістити його до пор- тативного UPS без переривання живлення цього пристрою. Є також похитування мишкою, які може бути використано для уникнення активації програми блокування екрана. Обидва ці пристрої надають доречні інструменти, якщо виконують дослідження увімкненого пристрою, де може бути запроваджено шифрування. Якщо увімкнені пристрої збираються так, що живлення підтримується, пакування та транспортування діючих систем повинна мати заходи, пов’язані із забезпеченням охолодження, захисту від механічних ударів тощо.

— Забезпечити позначки, відключення та убезпечення всіх кабелів від цифрового пристрою та забезпечити позначки портів так, щоб систему могло бути реконструйовано пізніше.

— Помістити стрічку поверх вимикача живлення, якщо потрібно, для уникнення зміни стану живлення. Розглянути, чи стан вимикача задокументовано відповідно перед закриттям його стрічкою або переміщенням.

7.1.2.1.3 Додаткові дії: *збирання увімкнених цифрових пристроїв*

Треба запроваджувати додаткові дії, які є доречними залежно від конфігурації специфічного цифрового пристрою.

— Для ноутбука треба гарантувати, що несталі дані було здобуто перед вилученням батареї. DEFR повинен вилучити основне джерело живлення одразу, замість виключення клавіші живлення на ноутбуці для його перезавантаження. DEFR повинен також звернути увагу, якщо наявний адаптер живлення, та, якщо це так, тоді вилучити адаптер живлення після вилучення батареї.

Примітка 1. Натискання клавіші живлення на цифровому пристрої може бути сконфігуровано так, що буде запущено скрипт, який може змінювати інформацію або видаляти інформацію із системи перед перезавантаженням або надавати засторогу приєднаній системі, що виявлено несподівану ситуацію, яка може призвести до стирання даних, що мають доказове значення, перед тим, як їх ідентифіковано. Пристрій може бути також сконфігуровано так, щоб запустити пристрій так, щоб він навмисно завдав шкоди DEFR та іншім присутнім особам.

— Розмістити стрічку поверх слоту гнучких дисків, за наявності.

— Необхідно впевнитися, що лотки слотів CD або DVD розміщено на своїх місцях; звернути увагу, чи ці лотки слотів порожні, містять диски або не перевірялися; та закрити лоток слотів стрічкою для уникнення його відкриття.

Примітка 2. Якщо будь-який завантажуваний носій залишено в слоті, тоді в момент, коли цей пристрій буде увімкнено наступного разу, він може загружатися із цього носія, а не із жорсткого диску (або з інструментів драйвера гнучкого диску) залежно від установок BIOS комп'ютера.

— DEFR повинен виконувати збирання нецифрових доказів відповідно до законодавчих процедур для гарантування того, що будь-які докази припустимі.

7.1.2.2 Вимкнені цифрові пристрої

7.1.2.2.1 Загальні положення

DEFR може використовувати ряд настанов для збирання, якщо цифровий пристрій вимкнено. Не всі дії, що містяться в цих настановах, може бути застосовано для всіх обставин. Отже необхідно визначити відмінності між тими діями, що може бути застосовано в усіх випадках (основні дії), та тими, що можуть бути застосовані тільки в деяких випадках (додаткові дії).

На рисунку 2 зображено основні та додаткові дії, застосовувані для збирання вимкнених цифрових пристроїв.

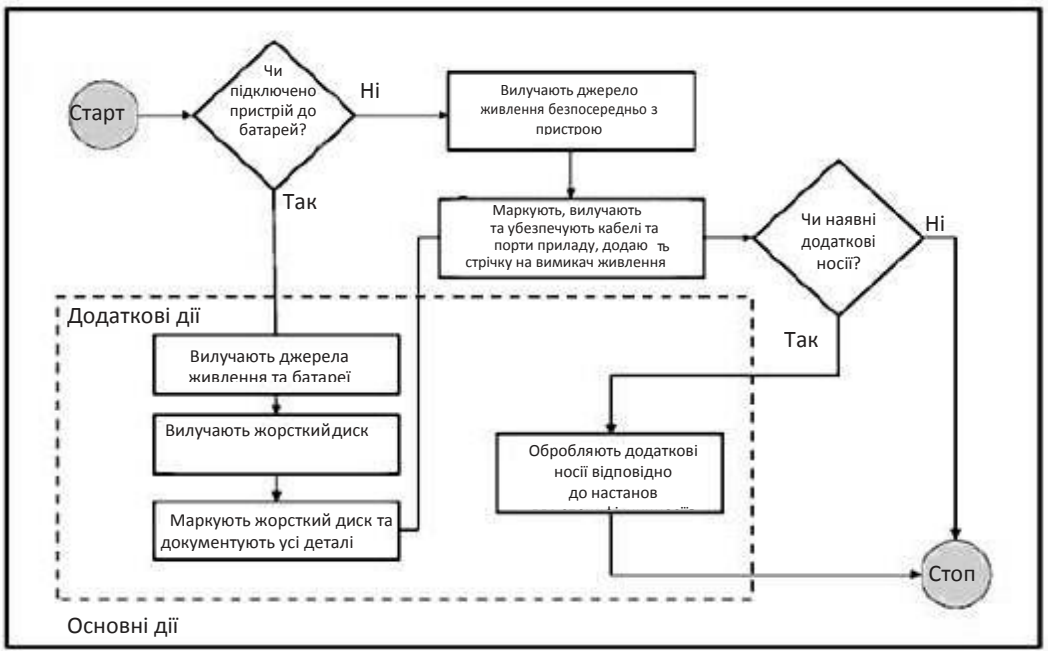

Рисунок 2 — Настанови для збирання вимкнених цифрових пристроїв

7.1.2.2.2 Основні дії: *збирання вимкнених цифрових пристроїв*

Такі дії є рекомендованими основними діями для збирання, якщо цифровий пристрій вимкнено:

— Вилучити кабель живлення так: з початку вилучити кінець, підключений до цифрового пристрою, а не кінець, підключений до розетки.

— Вилучити та убезпечите всі кабелі від цифрових пристроїв та помістити позначки на портах так, щоб систему могло бути реконструйовано пізніше.

— Помістити стрічку на вимикачі живлення, за потреби, для уникнення зміни стану вимикача. Упевнитися, чи стан вимикача було правильно задокументовано перед тим, як він був закритий стрічкою або відкритий.

Примітка. Зазвичай носій для збереження не повинен бути вилученим із блока цифрового пристрою до того, як буде зроблено здобуття потенційних цифрових доказів, оскільки його вилучення збільшує ризик пошкодження або плутанини його з іншими носіями для збереження. Має бути розроблено та запроваджено локальні процедури стосовно потреби вилучення носіїв для збереження даних із цифрових пристроїв.

7.1.2.2.3 Додаткові дії: *збирання вимкнених цифрових пристроїв*

Такі дії є додатковими діями, які є доречними для збирання вимкнених цифрових пристроїв залежно від конфігурації специфічного цифрового пристрою:

— З початку треба впевнитися, що ноутбук дійсно виключено, оскільки деякі з них можуть бути в режимі очікування. Треба бути обережними, оскільки деякі ноутбуки можуть вмикатися в разі відкриття кришки. Потім перейти до вилучення основної батареї живлення ноутбука.

— Якщо умови на місці дослідження потребують вилучення жорсткого диска, DEFR повинен бути обережним під час заземлення цифрового пристрою для уникнення впливу статичної електрики щодо пошкодження дисководу жорсткого диска. В іншому разі, дисковод жорсткого диску не повинен вилучатися на місці. Розмістити позначку на дисководі жорсткого диска, як підозрілого диску, та задокументувати всі деталі, такі як тип, назва модулі, серійний номер та розмір дисководу жорсткого диска.

— Розмістити стрічку поверх слоту гнучких дисків, за наявності.

— Необхідно впевнитися, що лотки слотів CD або DVD розташовано на своїх місцях; звернути увагу, чи ці лотки слотів порожні, містять диски або не перевірялися; та закрити лотки слотів стрічкою для уникнення його відкриття.

Примітка. Якщо будь-який завантажуваний носій залишено в слоті, тоді в момент, коли цей пристрій буде увімкнено наступного разу, він може завантажуватися з носія, а не з жорсткого диска (або з інструментів драйвера гнучкого диску) залежно від установок BIOS комп'ютера.

7.1.3 ***Здобуття***

7.1.3.1 Увімкнені цифрові пристрої

7.1.3.1.1 Загальні положення

Є три сценарії, у яких може виникнути потреба здобуття цифрових доказів: якщо цифровий пристрій увімкнено, якщо цифровий пристрій вимкнено та якщо цифровий пристрій увімкнено, але не може бути вимкнено (таких як критичні цифрові пристрої).

У всіх цих сценаріях DEFR потребує отримання точної копії цифрових доказів з носія для збереження цифрового пристрою, який підозрюється в тому, що він містить потенційні цифрові докази.

Якщо не можливо зробити образ цифрового пристрою, необхідно здобути точні копії специфічних файлів, які можуть містити потенційні цифрові докази. Ідеально, має бути зроблено як затверджену мастер-копію, так і робочу копію. Мастер-копію не можна використовувати знову, хоча вона потрібна для підтвердження контенту робочої копії або виконання заміни робочої копії після пошкодження першої робочої копії.

DEFR може запроваджувати низку настанов для здобуття, якщо визначено, що цифровий пристрій увімкнено. Не всі настанови є ідеальними та підходять для всіх випадків; деякі настанови може бути застосовано тільки для специфічних випадків. Відповідно, настанови може бути покласифіковано як основні або додаткові. Необхідно розглянути можливість того, що увімкнені системи може бути введено в режим блокування екрана чи автоблокування та що існують приховані значення до будь-яких спроб для уникнення цього. Наприклад, коливання мишкою буде потребувати встановлення USB-ключа для реєстрації та найімовірніше може викликати модифікацію за будь-яких інших дій. Використання доречних методів буде мінімізувати приховані значення таких дій.

На рисунку 3 зображено основні та додаткові дії, застосовувані для здобуття потенційних цифрових доказів на увімкнених цифрових пристроях.

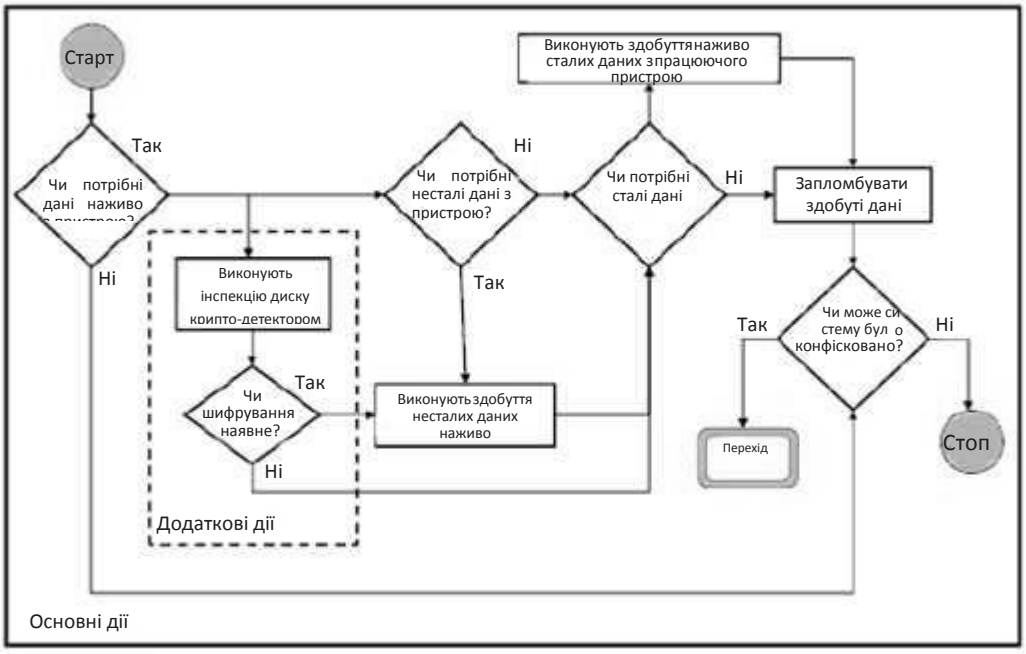

Рисунок 3 — Настанови для здобуття потенційних цифрових доказів на увімкнених цифрових пристроях

7.1.3.1.2 Основні дії: *здобуття потенційних цифрових доказів на увімкнених цифрових пристроях*

Такі дії є основними діями, які має бути запроваджено DEFR у всіх випадках здобуття потенційних цифрових доказів на увімкнених цифрових пристроях:

— З початку розглянути здобуття потенційних цифрових доказів, які можуть бути втраченими, якщо цифровий пристрій буде вимкнено. Також відомо для несталих даних, таких як дані, що зберігаються в RAM, запущених процесах, мережевих з'єднаннях та установках дати/часу. Якщо необхідно здобути сталі дані з пристроїв, які ще працюють, має бути розглянуто здійснення здобуття на ввімкнених системах.

— Запровадження здобування наживо необхідно для здобуття даних наживо від пристроїв, які ще працюють. Здобуття несталих даних наживо в RAM дає змогу відновлення важливої інформації, такий як статус мережі, декодовані прикладні програми та паролі. Ці процеси відрізняються та потребують використання різних наборів інструментів.

— DEFR повинен ніколи не довіряти програмам у системах. Із цієї причини, там, де це можливо, рекомендовано користуватися затвердженим інструментом, отриманим DEFR (для статичного бінарного коду). DEFR повинен мати компетенцію застосування затверджених інструментів та бути компетентним щодо врахування впливу таких інструментів на систему (наприклад, переміщення потенційних цифрових доказів, контент пам'яті, яка під час

завантаження програмного забезпечення змінює нумерацію сторінок, тощо). Усі виконані дії та отримані зміни, зроблені в потенційних цифрових доказах, має бути задокументовано та зрозуміло. Якщо неможливо визначити подібні впливи на систему задіяних інструментів або зміни, що є результатом дій, не може бути визначено однозначно, це також має бути задокументовано.

— Під час здобуття несталих даних DEFR повинен адаптувати використання логічного файлового контейнера, де це можливо, та задокументувати їхні геш-значення, коли контейнер містить файл(и) несталих даних. Там, де це неможливо, потрібно використовувати контейнер, такий як ZIP-файл; потім для цього файла має бути обчислено геш-значення і це значення задокументовано. Отриманий файловий контейнер має зберігатися на носії для збереження цифрових даних, підготований для цієї цілі, тобто відформатований.

— Застосувати процес створення образу наживо для сталого збереження з використанням за- тверджених інструментів створення образу. Отримана копія цифрового доказу має зберігатися на носії для збереження цифрових даних, підготованого для цієї цілі. Краще використовувати нові носії для збереження цифрових даних, застосування копій цифрових доказів від затверджених процесів гарантує цілісність даних під час реконструкції. Тому очищені носії для збереження цифрових даних будуть недоречними. Якщо образ збережено в логічному файловому контейнері, DEFR повинен гарантувати, що цей образ не може бути зіпсованим або пошкодженим.

Примітка. Якщо пристрій заблоковано, фізичний доступ може здійснюватися за допомогою інших засобів, які мають змогу прямого доступу, наприклад, Firewire інтерфейс.

7.1.3.1.3 Додаткові дії: здобуття потенційних цифрових доказів на ввімкнених цифрових пристроях

Такі дії є додатковими діями, які є доречними для здобуття потенційних цифрових доказів на ввімкнених цифрових пристроях залежно від конфігурації специфічного цифрового пристрою:

— Розглянути здобуття несталих даних з RAM, якщо підозрюють наявність шифрування. З початку перевіряють, чи дійсно це саме такий випадок, за допомогою перевірення необробленого диска чи за допомогою деяких утиліт для пошуку зашифрованої інформації. Якщо це саме такий випадок, треба враховувати, що працююча основна операційна система може бути ненадійною та треба розглянути використання відповідних надійних та затверджених інструментів.

— Використовувати надійне джерело часу та документувати час кожної здійсненої дії.

— Може бути доречним об’єднати DEFR зі здобутими потенційними цифровими доказами за допомогою цифрових підписів, біометрії та фотографії.

Примітка 1. Натискання клавіші живлення на цифровому пристрої може бути сконфігуровано так, що буде запущено скрипт, який може змінювати інформацію або віддаляти інформацію із системи перед перезавантаженням або надавати засторогу приєднаній системі, що виявлено несподівану ситуацію, яка може призвести до стирання даних, що мають доказове значення перед тим, як їх ідентифіковано. Пристрій може бути також сконфігуровано в такий спосіб, щоб запустити пристрій так, щоб він навмисно завдав шкоди DEFR та іншим присутнім особам

7.1.3.2 Вимкнені цифрові пристрої

7.1.3.2.1 Загальні положення

Легше обробляти вимкнені цифрові пристрої, ніж увімкнені цифрові прилади, оскільки нема потреби здобуття несталих даних. На рисунку 5 зображено дії, які може бути застосовано для здобуття потенційних цифрових доказів з вимкнених цифрових приладів.

7.1.3.2.2 Здобуття з вимкнених цифрових пристроїв

Такі дії є діями зі здобуття потенційних цифрових доказів, якщо цифрові пристрої вимкнено:

— Упевнитися, що пристрій дійсно вимкнений.

— Якщо потрібно, вилучити носій із вимкненого цифрового пристрою, якщо цього ще не було зроблено. Розмістити позначку на носії, як підозрілому носії, та задокументувати всі деталі, такі як тип, назва моделі, серійний номер та розмір носія.

— Створити образ за допомогою затверджених інструментів створення образу для формування копії цифрових доказів з підозрілого диску.

Примітка. Здебільшого носій не вилучається із цифрового пристрою, доки виконується здобуття потенційних цифрових доказів, оскільки його вилучення збільшує ризик пошкодження або плутанини його з іншими носіями для збереження даних. Має бути розроблено та запроваджено локальні процедури стосовно потреби вилучення носія для збереження із цифрових пристроїв.

7.1.3.3 Критичні цифрові пристрої

У деяких випадках цифрові пристрої не може бути вимкнено через критичну природу в системах. Це системи, такі як сервери в дата-центрах, які також надають послуги невинним клієнтам, системи життєзабезпечення, медичні системи та багато інших, які можуть надати критичний вплив, якщо вони перервуть роботу чи їх буде вимкнено. Треба бути особливо обережними під час роботи з такими системами.

Якщо цифровий пристрій не може бути вимкнено, виконують здобуття наживо та/або часткове здобуття потенційних цифрових доказів, як описано в 7.1.3.1.2 та 7.1.3.4.

7.1.3.4 Часткове здобуття

Часткове здобуття може здійснюватися внаслідок кількох причин, таких як:

— системне сховище є дуже великим, щоб бути здобутим (наприклад, сервер баз даних);

— система є дуже критичною, щоб бути вимкненою;

— якщо вибрані дані, що мають бути здобутими, містять інші недоречні дані в середині тої самої системи; або

— якщо законодавчі обмеження повноважень, такі як судове розпорядження на розслідування, яке обмежує сферу застосування здобуття.

Якщо прийнято рішення щодо здійснення часткового здобуття, дії з такого здобуття охоплюють, але не обмежуються, такими:

— Ідентифікувати папку(-и), файл(и) чи будь-які доречні власні системні опції, доступні для здобуття бажаних даних.

— Виконати логічне здобуття цих ідентифікованих даних.

7.1.3.5 Носії для збереження цифрових даних

На місці інциденту може бути знайдено різні типи носіїв для збереження цифрових даних. Зазвичай є найменш несталі типи даних та вони можуть мати найнижчий пріоритет протягом збирання та здобуття. Це не означає, що вони є неважливими, оскільки в багатьох випадках зовнішні носії для збереження цифрових даних містять докази, досліджувані аналітиками. DEFR повинен гарантувати таке:

— Перевірити та задокументувати місце (наприклад, відсік дисководів, кабелі та конвектори, USB-слоти тощо) виробника, модель та серійних номер (якщо є) для кожного знайденого носія для збереження цифрових даних.

— Прийняти рішення чи збирати ідентифіковані носії для збереження цифрових даних або виконати здобуття на місці; рішення має бути прийнято на основі природи інциденту та доступних ресурсів. Для виконання здобуття потенційних цифрових доказів (з основного жорсткого диску) на місці, див. рисунок 3.

— Якщо DEFR прийняв рішення та має дозвіл збирати носії для збереження цифрових даних, зібрані носії має бути запаковано або розміщено у відповідному пакованні.

— Нанести позначки на носії для збереження цифрових даних та будь-які пов’язані з ним частини. Позначки доказів не повинно бути розміщено безпосередньо на механічних частинах носія для збереження цифрових даних, не повинні закривати або маскувати важливу інформацію,

таку як серійний номер, номер моделі та номери частин. Усі зібрані носії має бути здобуто та збережено так, щоб гарантувати цілісність зібраних носіїв. Якщо можливі докази має бути запаковано за допомогою пломб, що порушуються від втручання, тоді DERF або задіяний персонал, повинні підписати ці позначки.

— Зібрані носії для збереження цифрових даних потрібно зберігати в середовищі, прийнятному для збереження даних.

— DEFR повинен бути обізнаним стосовно допустимого максимального періоду часу, визначеному відповідним законодавством, стосовно можливості збереження даних на носії для збереження цифрових даних.

7.1.4 ***Збереження***

Після завершення процесу здобуття DEFR повинен запечатати здобуті дані з використанням функцій верифікації або цифрових підписів для визначення того, що цифрові копії еквівалентні оригіналам. Додатково, аспекти безпеки потребують застосування засобів безпеки, які здійснюють збереження конфіденційності, цілісності та надійності потенційних цифрових доказів. Для захисту від псування, властивості середовища відпо- відати належним вимогам. DEFR потребує гарантування такого:

— Використання відповідних функцій верифікації, щоб надавати докази, скопійовані файли еквівалентні оригіналам.

— Може бути доречним об’єднати DEFR зі здобутими потенційними цифровими доказами за допомогою цифрових підписів, біометрії та фотографії.

Усі зібрані цифрові прилади має бути належно збережено. Різні типи потенційних цифрових доказів можуть потребувати різних методів збереження. Потенційні цифрові докази необхідно зберігати протягом їхнього часу життя, який може змінюватися в різних юрисдикціях та організаційних політиках.

Примітка. Як альтернатива опечатування здобутих даних із затвердженими функціями верифікації або цифровими підписами, DEFR також може використовувати біометричні дані. Біометрія використовує фізичні характеристики та особливості поведінки для визначення ідентифікації особи. Якщо біометричні дані долучено до здобутих потенційних цифрових доказів, можна гарантувати, доказ не може бути скомпрометованим без компрометації біометричних даних.

7.2 **Мережеві пристрої**

7.2.1 ***Ідентифікація***

7.2.1.1 Загальні положення

У контексті цього розділу мережеві пристрої розглядають як комп’ютери або інші цифрові пристрої, підключені до мережі в дротовому чи бездротовому режимі. Такі мережеві прилади можуть охоплювати мейнфрейми, сервери, настільні комп’ютери, комутатори, концентратори, маршрутизатори, мобільні прилади, PDA, PED, Bluetooth прилади, CCTV системи тощо. Зазначимо, що якщо цифровий пристрій підключено до мережі, важно визначити, де саме потенційні цифрові докази, які необхідно розглянути, зберігаються. Ці дані може бути розміщено будь-де в мережі.

Ідентифікація цифрових пристроїв містить компоненти, такі як логотипи виробника, серійні номери, шини й адаптери живлення. DEFR може розглянуті такі аспекти як засоби ідентифікації:

— Характеристики пристрою: Модель та виробник цифрового пристрою іноді може бути ідентифікований за його видимими характеристиками, особливо якщо є унікальний дизайн елементів.

— Інтерфейс пристрою: Конектор живлення часто є специфічним для виробника та може надавати допомогу в ідентифікації.

— Позначки пристрою: Для вимкнених мобільних пристроїв може бути доречною інформація, отримана із середини порожнини блока батареї, особливо коли її пов’язано з

відповідними базами даних. Наприклад, IMEI є номером з 15 цифр, який показує виробника, тип моделі та країну затвердження для GSM-пристроїв; ESN — це унікальний 32-бітний ідентифікатор, задокументований на безпечному чипі в мобільному телефоні виробником — перші 8...14 біт ідентифікують виробника та решткі бітів ідентифікують приписаний серійний номер.

— Зворотний пошук: У разі мобільних телефонів, якщо телефонний номер цього телефону відомий, зворотний пошук може бути використано для ідентифікації мережевого оператора.

Завдяки загальним малим розмірам мобільних пристроїв DEFR повинен бути особливо обережним під час ідентифікації всіх типів мобільних пристроїв, які можуть бути причетними в цьому разі. DEFR повинен убезпечити місце інциденту та гарантувати, що ніхто з осіб не виніс мобільні та будь-які інші цифрові пристрої з місця інциденту. Цифрові пристрої, які можуть містити цифрові докази, має бути захищено від несанкціонованого доступу.

Примітка. У деяких випадках комунікація не повинна перериватися. Треба поінформувати авторизованих осіб щодо можливих проблем (наприклад, попередити невідомих осіб стосовно вимкнені пристрої).

7.2.1.2 Дослідження та документування фізичного місця інциденту

Перед тим, як може бути зроблено здобуття чи збирання, місце інциденту має бути задокументовано візуальним способом за допомогою фотографування, відеозйомки або схематичного зображення місця, яким воно було на вході. Метод документування потребує збалансування обставин, вартості, часу, наявних ресурсів та пріоритетів. DEFR повинен задокументувати всі інші елементи на місці інциденту, які можуть містити потенційно доречні матеріали, такі як короткі записки, стикери, щоденники тощо.

— DEFR повинен задокументувати типи, бренди, моделі та серійні номери будь-яких використовуваних пристроїв та ідентифікувати всі цифрові прилади, які можуть потребувати здобуття потенційних цифрових доказів і збирання, на цієї початковій стадії. Усі мобільні пристрої та їхні відповідні елементи, такі як карти пам'яті, SIM-карти, зарядні пристрої та шини, знайдені на цьому місці, їхні відповідні серійні номери та будь-які ідентифікаційні особливості має бути задокументовано та зібрано, якщо потрібно. Постаратися також знайти оригінальне паковання мобільних телефонів; вона може містити нотатки з PIN та PUK-кодами.

— Якщо пристрій є мережевим, DEFR повинен ідентифікувати послуги, що надаються цими пристроями, для розуміння залежності та визначення критичності цього пристрою в середині мережі перед тим, як прийняти рішення стосовно відключення цього пристрою від мережі. Це є важливим, якщо цей пристрій надає послуги з критичних функцій, що не можуть бути терпимими до будь-яких відключень або для уникнення пошкодження потенційних цифрових доказів. Однак, якщо виявляється змога здійснення мережевих загроз цьому пристрою, DEFR може потребувати прийняття рішення стосовно відключення цього пристрою від мережі для захисту потенційних цифрових доказів.

— Якщо мережевим пристроєм є CCTV-система, DEFR повинен записати номери камер, підключених до системи, а також те, які із цих камер дійсно працюють. DEFR повинен також записати тип моделі, модель та основні установки системи, такі як установки дисплея, установки поточного запису та розміщення місця збереження інформації так, щоб полегшити процес збирання та здобуття в разі, якщо зміни має бути зроблено; це потім надасть можливість повернути систему до первісного стану.

— Статус цифрових пристроїв має залишатися таким, якій він є. Зазвичай, цифрові пристрої вимкнені, DEFR не повинен їх вмикати та, якщо їх увімкнено, DEFR не повинен їх вимикати. Це може попередити небажане псування цифрових доказів. Пристрій, який має батареї, що можуть розрядитися, потребують зарядження для гарантування того, що інформацію не буде втрачено. DEFR повинен ідентифікувати потенційні зарядні пристрої та кабелі протягом цієї стадії. Якщо пристрій буде транспортуватися та перевірятися в деяку невизначену дату, може бути доречним вимкнути його для мінімізації можливості пошкодження даних, які містяться в цьому пристрої.

— DEFR повинен також розглянути використання детектора бездротових сигналів для виявлення та ідентифікації бездротових сигналів від бездротових пристроїв, що можуть бути прихованими. Можуть бути обставини, коли детектор бездротових сигналів не використовують через вартості та обмежень часу, та DEFR повинен задокументувати цей факт.

7.2.2 Збирання, здобуття та збереження

7.2.2.1 Загальні положення

DEFR повинен прийняти рішення, чи збирати або здобувати потенційні цифрові докази від цифровихпристроїв. Якщо DEFR прийняв рішення стосовно відключення пристроїв, процес збирання або здобуття потенційних цифрових доказів буде виконано, як описано в 5.4. Якщо пристрої не може бути відключено від мережі через критичності їх функцій або ймовірності порушення потенційних цифрових доказів, DEFR повинен виконати здобуття наживо, доки пристрої залишаються підключеними до мережі.

Примітка. Критично важливо мати чинні, стандартні процедури, які використовують затверджені інструменти, разом з прийнятною документацією та DEFR, який пройшов навчання та має відповідний досвід.

Збирання та здобуття потенційних цифрових доказів від мережевих мобільних пристроїв ускладнено, оскільки вони можуть бути в багатьох станах та режимах взаємодії, таких як Bluetooth, радіочастотному, сенсорному та інфрачервоному. Додатково, різні виробники мобільних пристроїв використовують різні типи операційних систем, які потребують різних методів здобуття доказів. Є також широкий діапазон карт пам’яті, використовуваних у мобільних пристроях, та видалення цих карт пам’яті з увімкнених мобільних пристроїв може взаємодіяти із запущеними процесами.

Зазвичай, мобільні пристрої, такі як PDA та мобільні телефони мають бути увімкненими, щоб здобути потенційні цифрові докази. Ці пристрої можуть безперервно змінювати своє операційне середови ще, коли їх увімкнено, наприклад, може бути оновленим час. Пов’язаною проблемою є те, що дві копії цифрових доказів одного й того самого пристрою можуть не пройти стандартні функції верифікації, такі як розрахунок геш. У такій ситуації може бути застосовано альтернативні функції верифікації, які іденти- фікують елементи співпадіння та різниці.

Важливо, щоб DEFR не вносив Wi-Fi та Bluetooth пристрої на місце розслідувань, які можуть змінювати подібну інформацію на пристроях з потенційними доказами. Це має особливу важливість, якщо дослідникам необхідно знати, які прилади були підключеними до мережі.

Якщо DEFR прийняв рішення застосовувати процес здобуття, мережеві пристрої мають залишатися працюючими для подальшого аналізування для визначення інших пристроїв, підключених до цього мережевого пристрою. DEFR повинен розглянути можливість саботажу через активні мережеві з’єднання та прийняти рішення моніторити систему або відключитися.

7.2.2.2 Настанови для збирання мережевих пристроїв

У деяких обставинах може бути доцільним залишити мережеві пристрої підключеними до мережі, так щоб DEFR бо DES з відповідними правами змогли моніторити та документувати їхню активність. Якщо такої потреби немає, пристрої мають збиратися, як описано нижче:

— DEFR повинен ізолювати пристрій від мережі, коли відомо, що потрібні дані буде перезаписано за допомогою такій дії та це не призведе до неправильного функціонування важливих систем (таких як системи керування обладнанням у госпіталях). Це може бути зроблено за допомогою відключення дротових мережевих з’єднань до телефонних систем або мережевих портів або зробити неможливим з’єднання з точкою бездротового доступу.

— Перед відключенням від дротових мереж DEFR повинен відстежувати підключення до цифрових пристроїв та позначити порти для подальшої реконструкції мережі в цілому. Пристрій може мати більше ніж один метод комунікацій. Наприклад, комп'ютер може мати дротове підключення до LAN, бездротовий модем та карти мобільного телефона. PED може бути підключено до мережі через Wi-Fi, Bluetooth з'єднання або з'єднання через мобільну телефонну мережу. DEFR повинен спробувати ідентифікувати всі методи комунікацій та застосувати відповідні дії для захисту від пошкоджень потенційних цифрових доказів.

— Треба бути обережним, оскільки видалення живлення від мережевих пристроїв у цьому місці може пошкодити несталі дані, такі як працюючі процеси, мережеві з'єднання та дані, що зберігаються в пам'яті. Основна операційна система може бути ненадійною та надавати фальшиву інформацію. DEFR повинен захопити цю інформацію за допомогою довірчих затверджених методів перед відключенням живлення від пристроїв. Якщо DEFR є впевненим, що потенційні цифрових доказів не буде втрачено в результаті, з'єднання від цього цифрового пристрою може бути видалено.

— Якщо збирання має переваги над здобуттям та відомо, що пристрій містить несталу пам'ять, пристрій має бути безперервно підключеним до живлення.

— Якщо мобільний пристрій вимкнено, обережно запакувати, запечатати та надайте позначки. Це надасть змогу уникнути випадкових або навмисних операцій з ключами або клавішами. Як додаткову передбачливість, DEFR повинен також розглянути використання паковання Фарадея або екранувальний бокс.

— У деяких обставинах мобільний пристрій має бути вимкнено протягом збирання для запобігання зміненню даних. Це може бути через вихідні або вхідні з'єднання або команди, які можуть спричинити пошкодження потенційних цифрових доказів.

— Пізніше кожен цифровий пристрій може бути оброблено як окремий пристрій (див. 7.1) протягом його досліджень.

Примітка. Можливо запровадити вид мережі з використанням пересувного пристрою для збереження як транзитне середовище. DEFR повинен розглянути чи можна зібраний пристрій використовувати так та шукати інформацію стосовно інших пристроїв у такому таємничому стані.

7.2.2.3 Настанови для здобуття з мережевих пристроїв

Якщо цифрові пристрої підключено до мережі, є змога ці прилади підключити до більше ніж однієї (1) фізичної або віртуальної мережі. Наприклад, пристрій, який, як здається, підключено до однієї (1) видимої фізичної мережі, може фактично працювати у віртуальній приватній мережі (VPN) та з віртуальною машиною з більше ніж однією (1) IP-адресою. У такому разі перед відключенням цього пристрою від мережі, DEFR повинен виконати логічне здобуття даних, пов'язаних з логічним мережевим з'єднанням (наприклад, інтернет-сполучення). Ці пов'язані дані охоплюють, але не обмежуються, IP-конфігурацію та таблиці маршрутизації.

Для мережевих пристроїв, які потребують безперервного увімкненого живлення, пристрій має бути захищено від взаємодії з бездротовими радіомережами, охоплюючи пристрої із GPS. DEFR повинен користуватися методами, дозволеними локальним законодавством, для ізоляції радіосигналів. Однак, треба бути обережним для гарантування того, що пристрій має відповідне джерело живлення, оскільки методи ізоляції можуть призвести до використання додаткової енергії за спроб підключення до мережі. Методи ізоляції можуть охоплювати, але не обмежуватися, такі:

— Використання пристроїв блокування, які можуть заблокувати передачу за допомогою створення сильної інтерференції, коли пристрій випромінює сигнали в тому самому діапазоні частот, які використовують мобільні пристрої.

Примітка 1. Використання пристроїв блокування може порушувати законодавчі вимоги в деяких юрисдикціях.

Примітка 2. Використання пристроїв блокування може негативно впливати на поведінку електронних приладів, таких як медичне обладнання.

— Використання екранованих робочих місць для здійснення перевірянь безпечно на фіксованому місці. Екранування може бути зроблено для повного робочого місця або за допомогою встановлення тента Фарадея, який дає змогу зробити це портативно. Кабелі живлення в цьому тенті є проблематичними, однак, оскільки без належної ізоляції вони можуть діяти як антенна, скасовуючи цілі тента. Робоче місце може бути також дуже обмежувальним.

— Використання екранованих робочих місць для здійснення перевірянь безпечно у фіксованому місце. Радіочастотне екранування робочого простору або контейнера (контейнер Фарадея) може бути використано для уникнення з'єднань з мережею.

Примітка 3. Усі методи блокування бездротового доступу до мереж має бути затверджено для використання на відповідних частотах. Таке затвердження має також розповсюджуватися на кабелі, які проходять через екранування.

— Використання замінника (U)SIM, який імітує ідентифікацію оригінального приладу та попереджує доступ мережі до цього пристрою. Такі карти мають змогу обдурювати цей пристрій в прийманні його за оригінальний (U)SIM та дозволяти, щоб перевірення здійснювалися безпечно в будь-якому місці. (U)SIM має бути затвердженим для цього пристрою та мережі перед його користуванням.

— Заблокувати послуги мережі за допомогою домовленості з оператора мобільних послуг та ідентифікації деталей послуг, що будуть заблоковані (наприклад, ідентифікація обладнання, іден тифікація передплатника чи номер телефону). Однак, така інформація не завжди легкодоступна, коли процес координації та підтвердження може заподіяти затримування.

DEFR може здійснити здобуття наживо для мобільного пристрою перед тим, як вилучити батарею (наприклад, за допомогою доступу до SIM-карти). Це може бути зроблено для уникнення втрати потенційно важливої інформації в RAM телефону або для прискорення процесу перевірення (наприклад, там, де вважають, що пристрій може бути захищено PIN та/або PUK, що потребує значного часу для їхнього отримання).

Примітка 4. DEFR повинен гарантувати, що збирання та здобуття потенційних цифрових доказів відповідає локальним законам та нормативним документам, що потребує врахування конкретних обставин.

7.2.2.4 Настанови для збереження мережевих пристроїв

З урахуванням природи цифрових пристроїв та потенційних цифрових доказів, настанови для збереження мережевих пристроїв подібні збереженню комп'ютерів, периферійних пристроїв та носіїв для збереження цифрових даних. Див. 7.1.4 для докладної настанови стосовно збереження пристроїв.

7.3 **Збирання**, **здобуття та збереження для CCTV**

DEFR повинен розуміти, що підхід до вилучення відеопослідовностей з комп'ютера, вбудованого до DRV CCTV-системи, відрізняється від вилучення звичайного здобуття цифрових доказів з комп'ютера. Нижче наведено специфічні настанови для здобуття потенційних цифрових доказів із CCTV-систем:

— Перед початком процесу здобуття DEFR повинен з початку визначити, чи задокументувала система відеопослідовність, що викликає інтерес. Потім DEFR повинен визначити фрагмент часу потрібного відеоматеріалу та порівняти системний час із правильним часом та записати будь-які відмінності. DEFR повинен також визначити, які камери потрібні, та чи може здійснити процес здобуття окремо з кожної камери. DEFR повинен записати тип та модель системи. Ця інформація може бути потрібною, щоб визначити правильну відповідь програмного забезпечення.

— DEFR повинен здобути всі записи всіх доречних камер протягом часу, який зумовлює інтерес, для збереження інформації, яку буде додатково досліджено пізніше. DEFR повинен записати всі камери, підключені до системи та визначити, чи дійсно вони вели записи або не вели записів.

DEFR повинен визначити розмір носія для збереження цифрових даних, а також коли система повинна за процедурою перезаписувати відеоінформацію.

Ця інформація буде надавати DEFR знання того, як довго ця відеопослідовність буде залишатися в системі перед тим, як її буде втрачено. Цю дію має бути зроблено для гарантування того, що доказ не було змінено. Для цифрових відеодоказів захист записів має бути зроблено на місці.

— Є кілька опцій, які DEFR може вибрати для здобуття потенційних цифрових доказів від CCTV-систем:

1) Здобути відеофайли за допомогою записи їх на CD/DVD/Blu-ray диск, але це може бути непрактичним, якщо відеофайли занадто великі.
2) Здобути відеофайли за допомогою запису їх на зовнішній носій для збереження цифрових даних.
3) Здобути відеофайли через мережеве з'єднання. Це може бути зроблено, якщо CCTV-систему обладнано мережевим портом.
4) Застосувати здатність CCTV-системи до експорту відеофайлів в інші формати (зазвичай MPEG або AVI), які є стиснутою версією відеопослідовності. Це може бути використано тільки як останню спробу, оскільки відновлення зі стиснутого стану може змінити оригінальні дані та завжди вилучає деталі зображення. Не рекомендовано залучати відновлені дані для перевірення, якщо є оригінальні дані та вони доступні для аналізування.

Примітка 1. Якість вилученої відеопослідовності може бути не такою гарною, як якість оригіналу.

5) Там ще неможливо пряме здобуття цифрових доказів за допомогою копіювання файлів на записувальному пристрої, DEFR та DES повинні спробувати здобути аналогові копії з аналогового виходу, який є на оригінальному пристрої, що здійснив запис, з використанням доречних аналогових пристроїв для запису.

— Протягом комплектації здобуття, здобуті файли має бути перевірено для підтвердження того, що були здобуті правильні файли або частини файлів. Файли мають бути також перевірено за допомогою програмного забезпечення програвача (для форматів файлів цифрових пристроїв) для можливості їхнього програвання на інших системах — більшість CCTV систем є унікальними та файли не можуть бути обов'язково програватися з використанням іншого програмного забезпечення програвача. Правильне програмне забезпечення для програвання може бути доступним для завантаження із CCTV-системи разом з даними.

— Носій для збереження цифрових даних, який містить здобуті файли, має оброблятися як мастер-копія цифрових доказів. Якщо файли завантажено на ноутбук або карту пам'яті/USB пристрій, тоді постійну мастер-копію має бути зроблено із цих пристроїв якнайшвидше.

— Потім DEFR повинен перезавантажити CCTV-систему, якщо її вимкнено. Це має бути зроблено в присутності авторизованих осіб.

Якщо непрактично виконувати здобуття на місці, DEFR може прийняти рішення стосовно збирання носіїв для збереження цифрових даних. Швидким методом є заміна жорсткого диска CCTV-системи на порожній диск або клон жорсткого диску. Однак DEFR повинен оцінити серйозні ризики перед застосування цього методу, такі як сумісність нових дисководів жорстких дисків із системою та сумісність вилученого дисководу жорсткого диска з іншими системами для досліджень.

Примітка 2. Деякі системи мають пересувний дисковод жорсткого диска в кеді, але такий дисковод може потребувати обладнання системи для програвання.

Якщо жоден з наведених вище методів є неможливим, тоді CCTV-систему в цілому має бути вилучено в місця інциденту та процес здобуття має бути виконано в судової лабораторії. Це буде останньою спробою та припущення для DEFR, що це фізично можливо зробити, оскільки деякі CCTV-системи є дуже великі та складні. Знову DEFR повинен оцінити ризики стосовно законодавчого прийняття та гарантії перед вилученням системи.

З урахуванням походження цифрових пристроїв та потенційних цифрових доказів, настанови для збереження CCTV-системи подібні збереженню комп'ютерів, периферійних пристроїв та носіїв для збереження цифрових даних. Див. 7.1.4 для докладної настанови стосовно збереження пристроїв.

МІНІМАЛЬНІ ВИМОГИ ДО ПЕРЕМІЩЕННЯ ДОКАЗІВ

DEFR повинен відповідати за здобуті дані та цифрові пристрої протягом усього часу, коли вони знаходяться під його захистом. Для підтримання цього контролювання DEFR повинен бути відповідно авторизований, навчений та кваліфікований. Однак, оскільки локальні закони є визначним чинником у змозі DEFR відповідати всім трьом очікуваним вимогам, компетенція DEFR може змінюватися від одної юрисдикції до іншої. Це може призвести до того, що вимоги до документації для переміщення цифрових доказів між юрисдикціями не будуть однаковими в різних юрисдикціях.

Відповідно, потрібно визначити мінімальний набір вимог до документації для забезпечення обміну потенційними цифровими доказами між юрисдикціями. Ці вимоги до документації необхідно розглядати стосовно наведених у розділі 6.6. Оскільки цей стандарт не замінює специфічних вимог законодавства в будь-якій юрисдикції, він залишається практичною настановою для переміщення потенційних цифрових доказів скрізь кордони юрисдикцій.

Примітка 1. Мінімальна документація для комунікації складається з: доречних імен та адрес відповідних органів; стан авторизації, навчання та кваліфікації DEFR; цілі перевірення; того, які дії виконано; хто робив це та коли; хронологічне документування, яке стосується специфічного розслідування; описовий перелік потенційних цифрових доказів та носіїв для збереження цифрових даних, які було зібрано та здобуто; та інформація стосовно будь-яких перевірень, тестів або досліджень, застосованих для створення копій доказів. Специфічні вимоги юрисдикції можуть охоплювати таке: якщо докази розглядають як думку експерта, підтвердження відповідного Expert Witness Code of Conduct; та ордер суду, де визначено, яку документацію потрібно перемістити та причини для цього переміщення.

Науково-методичне видання

Гуцалюк Михайло Васильович
Гавловський Владислав Данилович
Хахановський Валерій Георгійович
Самойлов Станіслав Вадимович
Киричок Володимир Миколайович
Степанець Дмитро Сергійович
Одинокова Ольга Анатоліївна
Кагітін Сергій Миколайович
Школьніков Владислав Ігоревич

Загальна редакція: Корнейко Олександр Васильович

ВИКОРИСТАННЯ ЕЛЕКТРОННИХ (ЦИФРОВИХ) ДОКАЗІВ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ

Методичні рекомендації

Видання друге, доповнене

Відповідальний за випуск та комп'ютерна верстка: О. В. Корнейко

Відділ підготовки навчально-наукових видань
Національної академії внутрішніх справ.
03035, м. Київ, пл. Солом'янська, 1.
Свідотцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготовників і розповсюджувачів видавничої продукції ДК № 4155 від 13.09.2011.
Підписано до друку 21.08.2020. Формат 60х84/16. Папір офсетний.
Ум.-друк. арк. 6,05. Тираж 50 прим.

Друк: ФОП Поліщук О. В.
Свідотцтво субєкта видавничої справи ДК № 2142 від 31.03.2015.
07400, м. Бровари, вул. Незалежності, 2, кв. 148.
тел. (044) 592-13-49