НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

**ДСТУ ISO/IEC 27037:2017**
**(ISO/IEC 27037:2012, IDT)**

Інформаційні технології

# МЕТОДИ ЗАХИСТУ

## Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів

*Відповідає офіційному тексту*

З питань придбання офіційного видання звертайтесь
до національного органу стандартизації
(ДП «УкрНДНЦ» http://uas.org.ua)

# ПЕРЕДМОВА

1 РОЗРОБЛЕНО: Технічний комітет стандартизації «Банківські та фінансові системи і технології» (ТК 105)

2 ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ: наказ Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») від 06 грудня 2017 р. № 400 з 2019–01–01

3 Національний стандарт відповідає ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence (Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів)

Ступінь відповідності — ідентичний (IDT)

Переклад з англійської (en)

4 Цей стандарт розроблено згідно з правилами, установленими в національній стандартизації України

5 НА ЗАМІНУ ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT)

# ЗМІСТ

## НАЦІОНАЛЬНИЙ ВСТУП

Цей національний стандарт ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», прийнятий методом перекладу, — ідентичний щодо ISO/IEC 27037:2012 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence» (версія en).

Технічний комітет стандартизації, відповідальний за цей стандарт в Україні, — ТК 105 «Банківські та фінансові системи і технології».

Цей стандарт прийнято на заміну ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT), прийнятого методом підтвердження.

У цьому національному стандарті зазначено вимоги, які відповідають законодавству України.

До стандарту внесено такі редакційні зміни:

— структурні елементи стандарту: «Титульний аркуш», «Передмову», «Національний вступ», першу сторінку, «Терміни та визначення понять» і «Бібліографічні дані» — оформлено згідно з вимогами національної стандартизації України;

— слова «цей міжнародний стандарт» замінено на «цей стандарт»;

— вилучено «Передмову» до ISO/IEC 27037:2012 як таку, що безпосередньо не стосується технічного змісту цього стандарту;

— замінено крапку на кому як вказівник десяткових знаків;

— у розділі 2 наведено «Національне пояснення», виділене рамкою;

— у розділі «Нормативні посилання» наведено «Національне пояснення», виділене рамкою;

— долучено довідковий додаток НА (Перелік національних стандартів України, ідентичних європейським та міжнародним нормативним документам, посилання на які є в цьому стандарті).

Копії нормативних документів, посилання на які є в цьому стандарті, можна отримати в Національному фонді нормативних документів.

## ВСТУП до ISO/IEC 27037:2012

Цей стандарт надає настанови для специфічної діяльності з оброблення потенційних цифрових доказів, такими процесами є: ідентифікація, збирання, здобуття та збереження потенційних 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. Цей стандарт також надає загальні настанови стосовно збирання нецифрових доказів, які можуть бути корисними на стадії аналізування потенційних цифрових доказів.

Цей стандарт також спрямовано на інформування осіб, які приймають рішення, та тих, кому потрібно визначати надійність потенційних цифрових доказів, що були їм надані. Він прийнятний для організацій, яким необхідно захищати, аналізувати та презентувати потенційні цифрові докази. Він важливий для поліцейських підрозділів, які формують та запроваджують процедури щодо цифрових доказів, часто як частину доказів більшого об'єму.

Потенційні цифрові докази, розглянуті в цьому стандарті, можуть мати походження з різних типів цифрових пристроїв, мереж, баз даних тощо. Вони стосуються даних, які вже є в цифровому форматі. Цей стандарт не намагається охопити перетворення аналогових даних у цифровий формат.

Завдяки недовговічності цифрових доказів потрібно мати прийнятну методологію для гарантування цілісності та автентичності потенційних цифрових доказів. Цей стандарт не вимагає обов'язкового використання виняткових інструментів або методів. Ключовим компонентом, який забезпечує довіру в розслідуваннях, є методологія, яку застосовують протягом цього процесу, та особи, що мають кваліфікацію для виконання завдань, визначених цією методологією. Цей стандарт не стосується методології для законодавчих та дисциплінарних судових процесів, а також інших пов'язаних діяльностей під час оброблення потенційних цифрових доказів, які знаходяться поза межами сфери ідентифікації, збирання, здобуття та збереження.

Запровадження цього стандарту потребує відповідності національним законам, правилам та нормативним документам. Він не повинен заміняти специфічні законодавчі вимоги будь-якої юрисдикції. Фактично, він може слугувати практичною настановою для DEFR або DES у дослідженнях, які охоплюють потенційні цифрові докази. Він не впливає на аналізування цифрових доказів та не замінює специфічних юридичних вимог, що стосуються таких питань, як визнання доказів, доказова вага, значущість та інші юридично контрольовані обмеження використання потенційних цифрових доказів у судах. Цей стандарт може допомогти у сприянні обміну потенційними цифровими доказами між юрисдикціями. Для підтримання цілісності цифрових доказів користувачам цього стандарту потрібно адаптувати та скоригувати процедури, описані в цьому стандарті, відповідно до специфічних законодавчих вимог юрисдикції для доказів.

Хоча цей стандарт не охоплює судової готовності, відповідна судова готовність може бути значною мірою підтримана процесами ідентифікації, збирання, здобуття та збереження цифрових доказів. Судова готовність — це досягнення відповідного рівня здатності організації для спроможності ідентифікації, збирання, здобуття, збереження, захисту та аналізування цифрових доказів. Незважаючи на те, що процеси та діяльності, описані в цьому стандарті, є в основному реактивними заходами, використовуваними в розслідуваннях інциденту після того, як він вже трапився, судова готовність є проактивним процесом спроби планування процесу дослідження інциденту.

Цей стандарт відповідає ISO/IEC 27001 та ISO/IEC 27002, зокрема вимогам заходів щодо безпеки стосовно потенційних цифрових доказів за допомогою надання додаткової настанови щодо запровадження. Крім того, цей стандарт має застосування в контексті, незалежному від ISO/IEC 27001 та ISO/IEC 27002. Цей стандарт потрібно розглядати разом з іншими стандартами, пов'язаними з цифровими доказами та розслідуваннями інцидентів інформаційної безпеки.

# ДСТУ ISO/IEC 27037:2017

## НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

# МЕТОДИ ЗАХИСТУ

## Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів

INFORMATION TECHNOLOGY

# SECURITY TECHNIQUES

## Guidelines for identification, collection, acquisition and preservation of digital evidence

Чинний від 2019–01–01

## 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

ISO/IEC 17020 Conformity assessment — Requirements for the operation of various types of bodies performing inspection

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.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

ISO/TR 15801 Керування документами. Інформація, що зберігається в електронному вигляді. Рекомендації стосовно справжності та надійності

ISO/IEC 17020 Оцінка відповідності. Вимоги до роботи різних типів органів з інспектування

ISO/IEC 17025:2005 Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій

ISO/IEC 27000 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, вологості 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

[ISO/IEC 10118-1:2000]

**3.12 ідентифікація** (*identification*)
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** (*verification 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 для 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 А, 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 потенційні 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.

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 транспортуванням. 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 встановлено 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; та

— Якщо це дозволено, дослідити місце для пошуку елементів, таких як причеплені нотатки, щоденники, 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 процесів 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 А) 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 А) 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 збирання 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 інформування 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 середо-вище 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 цифровий 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 потенційні 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 відповідальними 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 пошкодження 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 ав-

тентичність 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 гарантування 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 розслідуванні, 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.

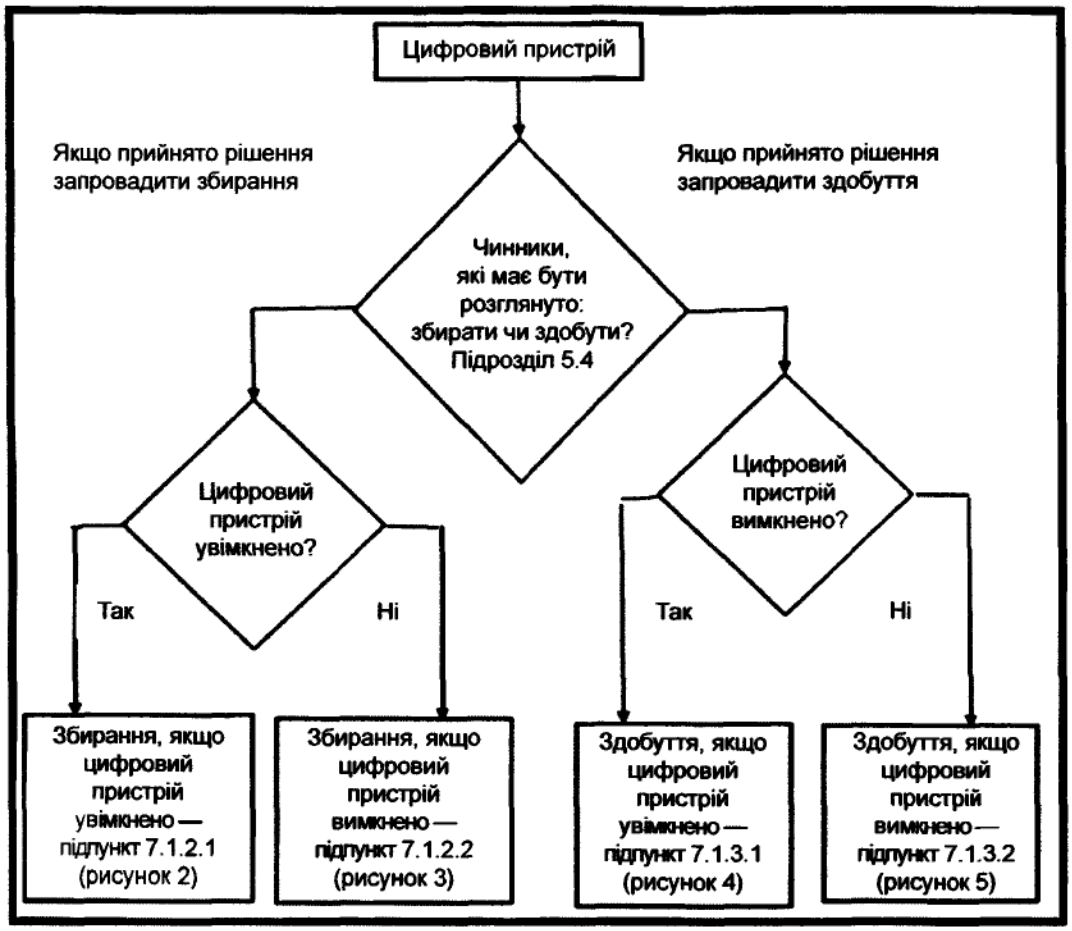


**Рисунок 1** — Настанова для процесу прийняття рішення збирати чи здобути потенційні цифрові докази

### 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. На рисунку 2 зображено основні та додаткові дії, які може бути застосовано для збирання цифрових пристроїв, якщо їх увімкнено.

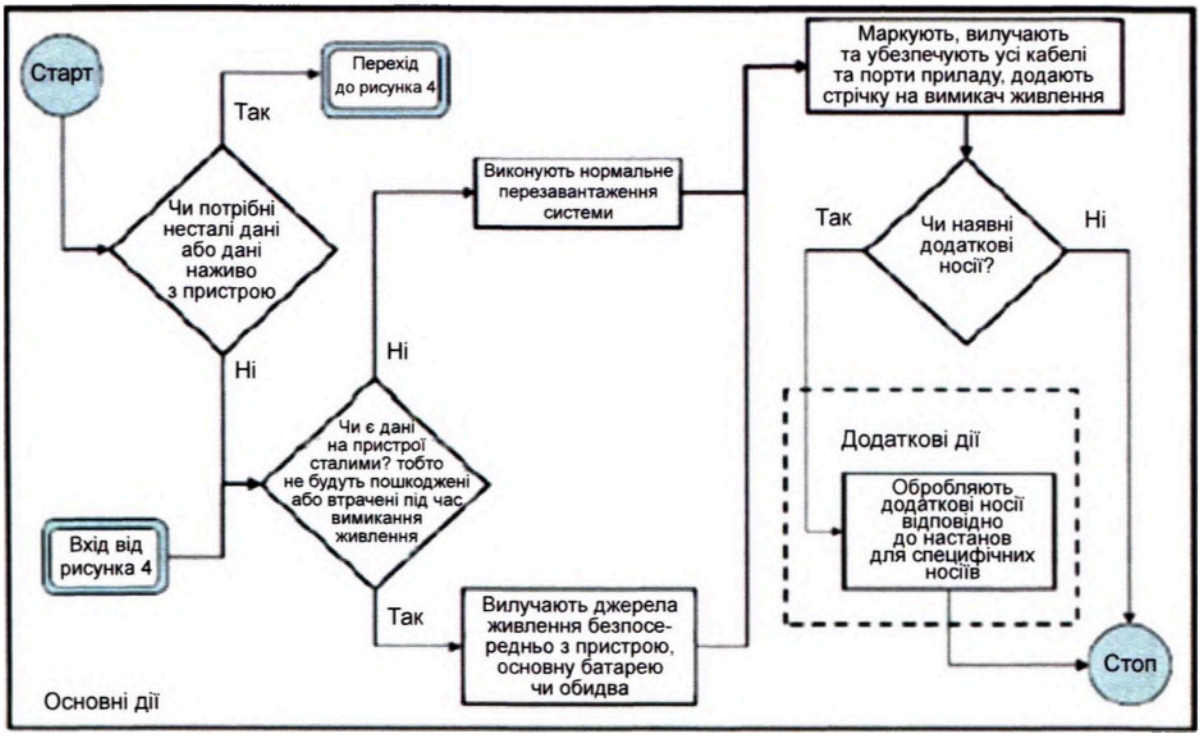


**Рисунок 2** — Настанови для збирання цифрових пристроїв, якщо їх увімкнено

**Примітка.** Усі ці дії мають відповідати локальному законодавству та нормативним документам.

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 портативного 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 застороrу 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 3 зображено основні та додаткові дії, застосовувані для збирання вимкнених цифрових пристроїв.

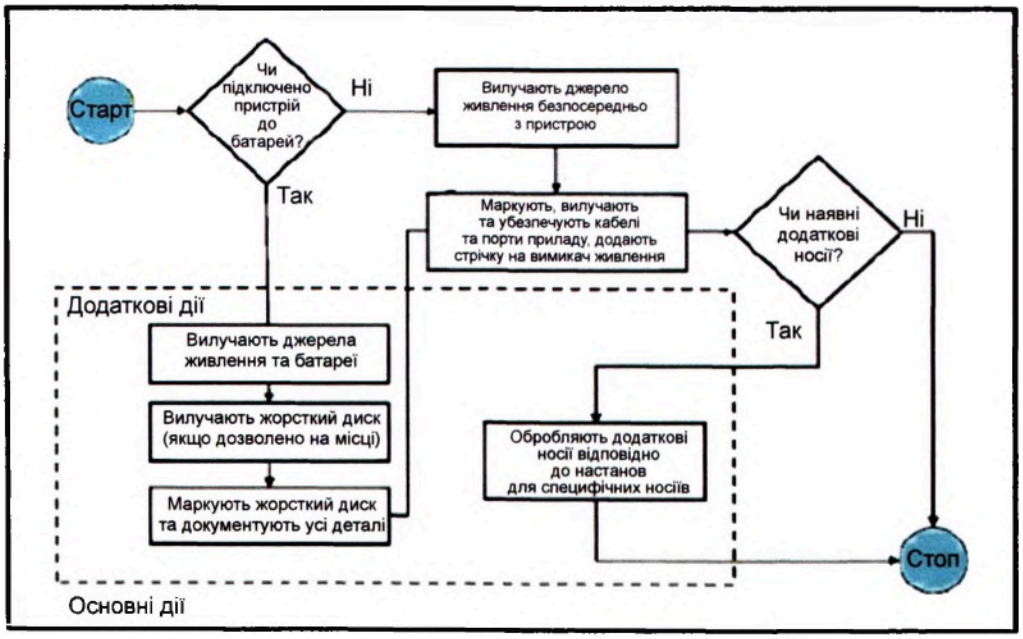


**Рисунок 3** — Настанови для збирання вимкнених цифрових пристроїв

DEFR відповідає за знання сучасних технологій та має бути ознайомлений з настановами стосовно оброблення носіїв збереження.

**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 4 зображено основні та додаткові дії, застосовувані для здобуття потенційних цифрових доказів на увімкнених цифрових пристроях.

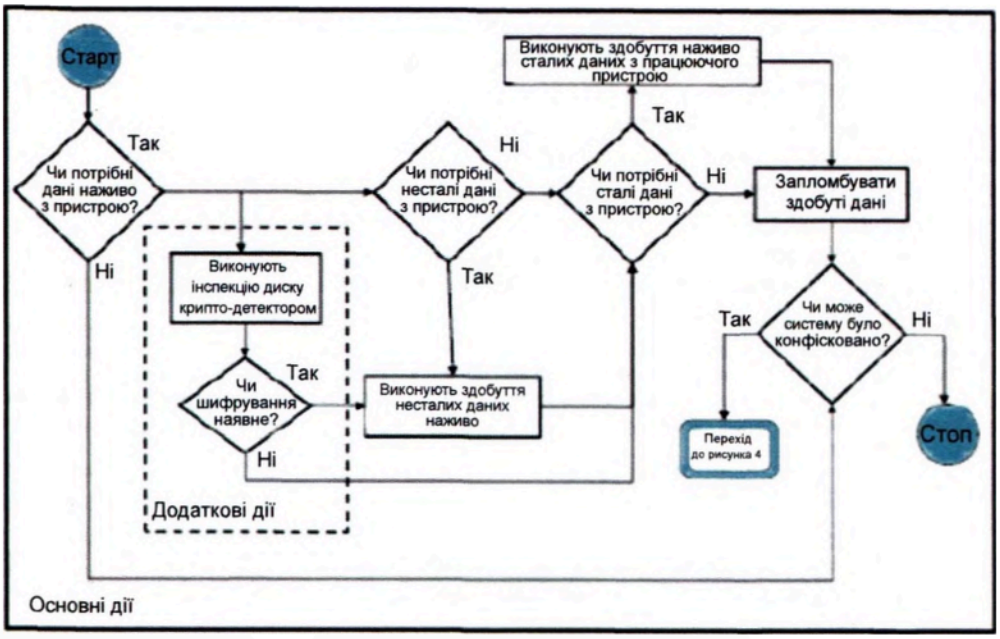


**Рисунок 4** — Настанови для здобуття потенційних цифрових доказів на увімкнених цифрових пристроях

**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 затверджених 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 застороги 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.

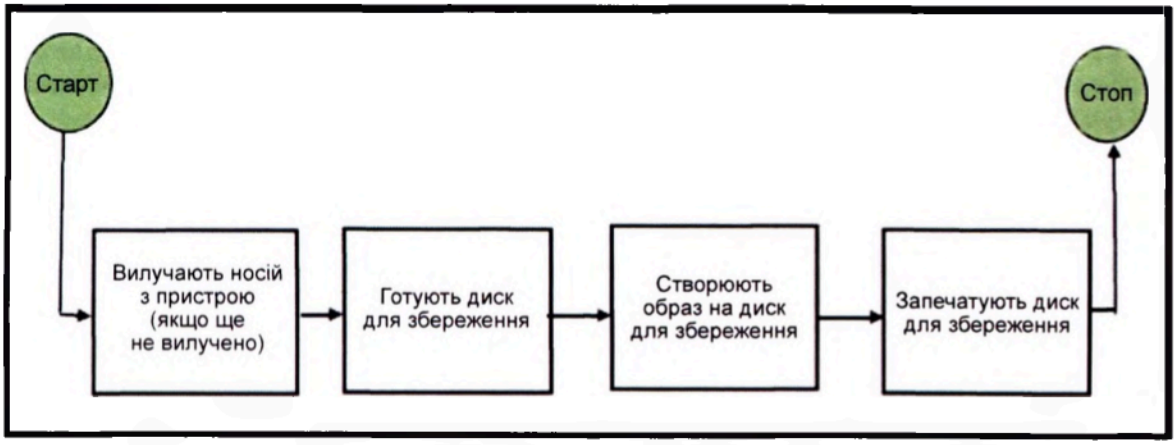


**Рисунок 5** — Настанови для здобуття потенційних цифрових доказів з вимкнених цифрових пристроїв

**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 4.

— 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 відповідати 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 рештки 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, наскільки це можливо. Зазвичай, цифрові пристрої вимкнені, DEFR не повинен їх вмикати та, якщо їх увімкнено, DEFR не повинен їх вимикати. Це може попередити небажане псування потенційних цифрових доказів. Пристрій, який має батареї, що можуть розрядитися, потребують заряджання 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 майбутню 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 цифрових пристроїв.

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 середовище, 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 ідентифікують 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.

ДОДАТОК А
(довідковий)

# ОПИС БАЗОВИХ НАВИЧОК ТА КОМПЕТЕНЦІЇ DEFV

**Таблиця А.1** — Приклади опису компетенції

| № | Основні навички | Опис основних навичок | Опис компетенції | | |
|---|---|---|---|---|---|
| | | | Обізнаність (1) | Знання (2) | Досвід (3) |
| 1 | Ідентифікація цифрових доказів | Характеризувати цифрові пристрої, компоненти, інформацію, яка може надати допомогу розслідуванню, та закони, доречні для оброблення потенційних цифрових доказів і пов'язаних з комп'ютером кримінальні злочини. Ідентифікувати вимоги до інструментів для збирання та здобуття даних та пристроїв і оцінювання ризиків | Загальний користувач IT та адміністрування в багатьох типах IT-пристроїв та мережевих пристроїв; процедури розслідування на місці злочину; значення доказової інформації; мережеві приховано підключені пристрої та оцінювання ризиків | Лог-журнали та конфігурація системи/прикладних програм; ідентифікація системи та лог-журналів прикладних програм, охоплюючи лог-журнали електронної пошти, веб лог-журнали, лог-журнали доступу, файли паролів, файли системної конфігурації, інформація хоста стосовно IP; функціональність та залежність пристроїв; можливість розуміння впливу на сталі та несталі докази | Спеціальний аналіз; інтерпретація лог-журналів для пошуку втручань в ідентифікації інших систем, які піддано впливу (деякі юрисдикції вимагають підтвердження наявності доказів перед збиранням); ідентифікація паролів, потрібна для підозрілих пристроїв перед збиранням; ідентифікація мережевих діаграм та механізмів контролювання доступу для розуміння залежностей; підтвердження зв'язку з IP та MAC адрес для пристрою |

Кінець таблиці А.1

| № | Основні навички | Опис основних навичок | Опис компетенції | | |
|---|---|---|---|---|---|
| | | | Обізнаність (1) | Знання (2) | Досвід (3) |
| 2 | Збирання цифрових доказів | Вимоги до інструментів та запровадження пакування цифрових доказів, захист від загроз середовища. Ці сфери охоплюють гарантування інформації | Загальна безпека збирання даних; принципи та дизайн основних інструментів; визначення найкращого методу збирання для збереження максимально доречної до інциденту інформації | Формування та виконання процесу збирання; збирання доказів; підготування документів стосовно доказів; хронологічне документування доказів, контролювання якості процесу збирання доказів; проведення опитувань | Оптимізація процесу збирання; документування доказів, які не може бути здобуто через різні обмеження; збирання паролів, ключів, захисних ключів-заглушок та іншої інформації, потрібної для аналізування в лабораторії |
| 3 | Здобуття цифрових доказів | Застосування в логічній формі вимог до здобуття потенційних цифрових доказів, гарантування відтворюваності, можливості аудиту, збіжності та захисту. Ці сфери охоплюють здобуття, яке виконується на увімкнених системах, на вимкнених системах та мережевих прихованих системах | Розуміння інформації, доступної в цифрових пристроях, базах даних, системах, що генерують документи, даних, що генеруються користувачем та несталих даних; файлових структурах систем Unix та Windows, а також прикладних програм, обізнаність впливом на несталі дані | Знання, як визначити вимоги до носіїв збереження; виконання процедури здобуття через формування образу (наприклад, часткове або повне здобуття з носіїв для збереження цифрових даних); здобуття на увімкнених системах, здобуття на вимкнених системах, генерація геш-значення | Можливість здійснювати здобуття на носіях для збереження цифрових даних, охоплюючи RAID, бази даних, побутових та мініатюрних пристроях; розуміння відмінностей та впливу на різні методи здобуття |
| 4 | Збереження цифрових доказів | Застосування та оцінювання вимог для збереження потенційних цифрових доказів, розуміння чинників та параметрів, які впливають на їхню точність. Ці сфери охоплюють методологію, підтримування хронологічного документування, оброблення комп'ютерних пристроїв та оброблення носіїв для збереження цифрових даних | Розуміння вимог та процедур для підтримання хронологічного документування та вимог законодавства; вплив середовища, такі як вологість, температура та удари на цифрові пристрої; розуміння варіантів пакування, вимог для транспортування та збереження | Знання як генерувати документи для аудиту доказів; визначати параметри для документів; гарантування інформаційної безпеки, загрози, вразливості та заходи захисту для цифрових доказів | Застосовувати заходи для убезпечення цифрових доказів, від великих пристроїв до мініатюрних ручних пристроїв; деталі процедури документування доказів |

**Таблиця А.2** — Визначення компетенції

| | |
|---|---|
| 1 | Обізнаність — Розпізнавати, ідентифікувати — говорити, коли потрібна допомога |
| 2 | Знання — Добувати знання на формальних тренінгах чи роботі в команді. Вкладати, брати участь — дія за допомогою |
| 3 | Досвід — Затверджений досвід через застосування в робочому оточенні. Робота без нагляду. Застосовувати, демонструвати — без допомоги |

**Примітка.** Компетенція DEFR може варіюватися від однієї юрисдикції до іншої.

ДОДАТОК В
(довідковий)

## 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.

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.

## БІБЛІОГРАФІЯ

1 ILAC–G19:2002 Guidelines for forensic science laboratories. Available from: www.ilac.org/ documents/ g19_2002.pdf

2 IOCE G8 proposed principles for the procedures relating to digital evidence. Available from: http://ioce.org/core.php?ID=5

3 ISO/IEC 15489:2001 Information and Documentation — Records Management

4 ISO/IEC 17024:2003 Conformity assessment — General requirements for bodies operating certification of persons

5 ISO/IEC 17043:2010 Conformity assessment — General requirements for proficiency testing

6 ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements

7 ISO/IEC 27002 Information technology — Security techniques — Information security management systems — Code of practice for information security management

8 ISO/IEC 24760-1 Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts

9 ISO/IEC 27031:2010 Information technology — Security techniques — Guidelines for ICT readiness for business continuity

10 ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management

11 Forensic Science Society Academic Accreditation Standards & CPD. Available from: http://www.forensic-science-society.org.uk

12 Guidelines for evidence collection and archiving. Available from: http://www.ietf.org/rfc/rfc3227.txt.

ДОДАТОК НА
(довідковий)

# ПЕРЕЛІК НАЦІОНАЛЬНИХ СТАНДАРТІВ УКРАЇНИ, ІДЕНТИЧНИХ ЄВРОПЕЙСЬКИМ ТА МІЖНАРОДНИМ НОРМАТИВНИМ ДОКУМЕНТАМ, ПОСИЛАННЯ НА ЯКІ Є В ЦЬОМУ СТАНДАРТІ

ДСТУ EN ISO/IEC 17020:2014 Оцінка відповідності. Вимоги до роботи різних типів органів з інспектування (EN ISO/IEC 17020:2012, IDT)

ДСТУ ISO/IEC 17025:2006 Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій (ISO/IEC 17025:2005, IDT)

ДСТУ EN ISO/IEC 17024:2014 Оцінка відповідності. Загальні вимоги до органів, що проводять сертифікацію персоналу, (EN ISO/IEC 17024:2012, IDT)

ДСТУ EN ISO/IEC 17043:2017 (EN ISO/IEC 7043:2010; ISO/IEC 17043:2010, IDT) Оцінка відповідності. Загальні вимоги до перевірки професійного рівня

ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT) Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів

ДСТУ ISO/IEC 27001:2015 ( ISO/IEC 27001:2013; Cor 1:2014, IDT) Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги

ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки

ДСТУ ISO/IEC 24760-1:2016 (ISO/IEC 24760-1:2011, IDT) Інформаційні технології. Методи захисту. Структура керування ідентифікаційною інформацією. Частина 1. Термінологія та поняття

ДСТУ ISO/IEC 27031:2015 Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу (ISO/IEC 27031:2011, IDT).

Код згідно з ДК 004: 35.040

**Ключові слова:** цифрові докази, потенційні цифрові докази, цифрові пристрої, мережеві цифрові пристрої, збирання цифрових пристроїв, здобуття потенційних цифрових доказів, збереження потенційних цифрових доказів, доказове значення, забезпечення цілісності та надійності цифрових доказів.