МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
ЛУГАНСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІМ. Е.О. ДІДОРЕНКА
ДонДУВС

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПІД ЧАС РОЗСЛІДУВАННЯ КОЛАБОРАЦІЙНОЇ ДІЯЛЬНОСТІ

Практичний посібник

Київ 2025

УДК: 343.3;343.301,343.322

Авторський колектив:

Нечеснюк М.В.- провідний науковий співробітник науково-дослідної лабораторії з проблем криміналістичного забезпечення та судової експертології ННІ №2 Національної академії внутрішніх справ.

Вознюк А.А. - завідувач наукової лабораторії з проблем протидії злочинності навчально-наукового інституту № 1 Національної академії внутрішніх справ, доктор юридичних наук, професор.

Письменський Є.О. - завідувач кафедри поліцейської діяльності Луганського навчально-наукового інституту імені Е. О. Дідоренка Донецького державного університету внутрішніх справ, доктор юридичних наук, професор.

Гусєва В.О.- завідувач кафедри криміналістики та судової експертології ННІ 1 Харківського національного університету внутрішніх справ, доктор юридичних наук, професор, підполковник поліції.

Пиріг І.В. – професор кафедри кафедри криміналістики та домедичної підготовки дніпровського державного університету внутрішніх справ, доктор юридичних наук, професор.

Рекомендовано до друку науково-методичною радою Національної академії внутрішніх справ (протокол №11 від 19 грудня 2024 року).

Використання спеціальних знань під час розслідування колабораційної діяльності; Нечеснюк М.В, Вознюк А.А. ,Письменський Є.О. та ін. практ. посіб. – Київ:, Нац. акад. внутр. справ 2025.-132 с.

У практичному посібнику проведено аналіз кримінально-правової норми про колаборацію діяльність. Розглянуто елементи складу кримінального правопорушення колабораційної діяльності, визначено набір його обов'язкових ознак залежно від специфіки основного безпосереднього об'єкта та відповідної форми об'єктивної сторони.

Розглянуто основні поняття, особливості та принципи роботи з електронними (цифровими) доказами, а також кримінально-процесуальні засади вилучення комп'ютерної техніки, мобільних засобів та інформації з них.

Визначено особливості залучення спеціаліста та можливості використання судових експертиз під час розслідування колабораційної діяльності.

Для працівників поліції, органів досудового розслідування, спеціалістів-криміналістів, а також може бути використано у навчальному процесі в закладах вищої освіти в системі МВС та інших вищих навчальних закладах зі специфічними умовами навчання.

Рецензенти:

Ганна СПІЦИНА - перший заступник директора Національного наукового центру «Інститут судових експертиз ім. засл. проф.. М.С. Бокаріуса» МЮ України, доктор юридичних наук, професор.

Тетяна ТАТАРНІКОВА - заступник начальника Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України, кандидат юридичних наук.

Микола ЄФІМОВ - професор кафедри криміналістики та домедичної підготовки Дніпровського державного університету внутрішніх справ, доктор юридичних наук, професор.

УДК: 343.3;343.301,343.322

© Національна академія внутрішніх справ, 2025
©Дніпровський державний університет внутрішніх справ, 2025
©Харківський національний університет внутрішніх справ, 2025
©Луганський навчально-науковий інститут ім. Е.О. Дідоренка ДонДУВС,2025

ЗМІСТ

ВСТУП 3

Розділ 1. Колаборaційна діяльність: особливості складу кримінального правопорушення, передбаченого ст. 111-1 КК України.... 5

Розділ 2. Використання спеціальних знань спеціалістом під час залучення до розслідування колаборaційцної діяльності …… 41

2.1. Загальні положення використання спеціальних знань під час розслідування кримінальних правопорушень…….. 41

2.2. Особливості залучення спеціаліста до розслідування колаборaційної діяльності…….. 50

2.3. Джерела доказів…….. …… 53

2.4. Основні правила отримання цифрових доказів…… 61

2.5. Основні дії спеціаліста при збиранні цифрових доказів…….. 64

2.6. Основні правила вилучення комп’ютерної техніки. …… 68

2.7. Особливості вилучення мобільних пристроїв…… 73

Розділ 3. Використання можливостей судових експертиз під час розслідування колаборaційної діяльності…… 78

Додаток 1…… 90

Перелік використаних та рекомендованих джерел…… 128

ВСТУП

Збройна агресія росії та окупація нею частини території України призвела до збільшення фактів колабораційної діяльності на окупованій території та, як результат, зростання кількості зареєстрованих та розслідуваних правоохоронними органами кримінальних проваджень за такими фактами, що обумовлює необхідність створення ефективного правового механізму боротьби з цим негативним явищем.

Як показує практика, у більшості випадків колабораційну діяльність розкрити та розслідувати досить складно завдяки прихованості, вчинення її на території до якої не мають доступ правоохоронні органи і, як наслідок, виникнення проблеми з притягненням винних до кримінальної відповідальності. Все це ускладнює проведення всіх необхідних слідчих (розшукових) та процесуальних дій з метою встановлення обставин, які підлягають доказуванню у кримінальному провадженні. Вимагають визначення та проведення якомога більшого комплексу слідчих (розшукових) та процесуальних дій з метою перевірки інформації про факт можливої колабораційної діяльності, зокрема щодо підтвердження або спростування отриманої інформації про причетність особи до кримінальної колабораційної діяльності, а у випадку її підтвердження, – здобуття достатніх доказів вчинення таких злочинів.

Запорукою успішності викриття злочинів, ефективності їх розслідування та судового розгляду нині є активне застосування спеціальних знань, тобто знань у галузі науки, техніки, мистецтва, що уможливлюють одержання доказової інформації спеціально підготовленими особами.

Доказування злочинів проти основ національної безпеки може передбачати залучення спеціаліста, яким є особа, яка володіє спеціальними знаннями та навичками і може надавати консультації, пояснення, довідки та висновки під час досудового розслідування і судового розгляду з питань, що потребують відповідних спеціальних знань і навичок (частина 1 статті 71 КПК України), а також призначення та проведення різного роду судових експертиз.

Тому авторами розроблений цей практичний довідник у якому розглянуто удосконалення процесуальних механізмів збирання, виявлення, огляду, фіксації та вилучення електронних (цифрових) доказів під час розслідування колабораційної діяльності, як основного джерела доказів

Практичний довідник зорієнтовано на працівників правоохоронних органів, які не є експертами в роботі з комп’ютерними системами та мережами, проте мають знати основи отримання та аналізу такого виду доказів.

Крім того, у додатку до основного матеріалу наведені основні положення державного стандарту ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», що набув чинності з 1 січня 2019 року і представлений у виданні не як офіційне представлення.

ПОЗНАКИ ТА СКОРОЧЕННЯ

Bluetooth - технологія бездротового зв'язку
CCTV (Closed Circuit Television) – Відеоспостереження
CD (Compact Disk) – Компакт-диск
DNA (Deoxyribonucleic Acid) – ДНК - Дезоксирибонуклеїнова кислота
DEFR (Digital Evidence First Responder) – Перший відповідальний за цифровий доказ
DES (Digital Evidence Specialist) – Спеціаліст з 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
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 хеш 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
Wi-Fi (Wireless Fidelity) – Бездротова передача інформації
КК – кримінальний кодекс України
КПК – кримінальний процесуальний кодекс України
СРД – слідча (розшукова) дія
НСРД - негласна слідча (розшукова) дія

РОЗДІЛ 1. КОЛАБОРАЦІЙНА ДІЯЛЬНІСТЬ: ОСОБЛИВОСТІ СКЛАДУ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ, ПЕРЕДБАЧЕНОГО СТ. 111-1 КК УКРАЇНИ

Аналіз кримінально-правової норми про колаборaційну діяльність дає змогу визначити та охарактеризувати такі елементи складу цього кримінального правопорушення.

1. Безпосередній *об'єкт* кримінального правопорушення (основний та додатковий), включаючи його *предмет* (у межах колаборaційної діяльності в господарській (економічній) сфері)[1].

2. *Об'єктивна сторона* у восьми формах, а саме:

1) колаборaційна діяльність в інформаційній сфері (ч. 1, ч. 6 ст. 111-1 КК України);

2) колаборaційна діяльність в освітній сфері (ч. 3 ст. 111-1 КК України);

3) колаборaційна діяльність у політичній сфері (ч. 6 ст. 111-1 КК України);

4) колаборaційна діяльність у господарській (економічній) сфері (ч. 4 ст. 111-1 КК України);

5) колаборaційна діяльність в адміністративній сфері (ч. 2 і ч. 5 ст. 111-1 КК України);

6) колаборaційна діяльність у виборчій сфері (ч. 5 ст. 111-1 КК України);

7) колаборaційна діяльність у правоохоронній та судовій сферах (ч. 7 ст. 111-1 КК України);

8) колаборaційна діяльність у воєнній сфері (ч. 7 ст. 111-1 КК України).

Обстановка, яку завжди характеризують умови окупації, слід визнати обов'язковою ознакою об'єктивної сторони в кожній з її форм[2]. Для конкретних

[1] Ураховуючи досить широкий та різноманітний спектр форм колаборaційної діяльності, безпосередній об'єкт у кожному конкретному випадку визначається залежно від конкретної форми (Злочинна колаборація в умовах збройної агресії : практич. порадник з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малюка. Київ : Алерта, 2023. С. 105).

[2] Специфікою зазначеної ознаки є те, що вона текстуально не закріплена в ст. 111-1 КК України, але неодмінно випливає з самої суті колаборaціонізму як специфічного явища, що здебільшого розглядається як державна зрада з пом'якшуючими покарання обставинами. Отже, наявність умов окупації слід розглядати як таку ознаку, що дає змогу розмежувати державну зраду та колаборaційну діяльність, оскільки ця діяльність

видів колабораційної діяльності можуть визначатися й інші об'єктивні ознаки, які характеризуватимуться під час їх подальшого аналізу. Наприклад, місце вчинення колабораційної діяльності вважається обов'язковою ознакою об'єктивної сторони колабораційної діяльності у сфері освіти.

3. *Суб'єкт* кримінального правопорушення: фізична, осудна особа, яка досягла 16-річного віку та є громадянином України[3]. Водночас, згідно з п. 3 ч. 1 ст. 96-3 КК України, вчинення уповноваженою особою від імені юридичної особи будь-якого з кримінальних правопорушень, передбачених ст. 111-1 КК України, є підставою для застосування до юридичної особи заходів кримінально-правового характеру.

4. *Суб'єктивна сторона* кримінального правопорушення у формі вини у виді умислу, включаючи мету в межах колабораційної діяльності у сфері освіти[4].

Інші об'єктивні та суб'єктивні ознаки не є обов'язковими для складу розгляданого кримінального правопорушення; відповідно, їх відсутність на кваліфікацію за ст. 111-1 КК України впливати не повинна.

Окремо слід звернути увагу на те, що на противагу ч.ч. 2, 5 та 7, у всіх інших частинах ст. 111-1 КК України зазначення добровільності колабораційної діяльності відсутнє, через що постає питання: чи визнаються передбачені в цих нормах (ч.ч. 1, 3, 4, 6) дії кримінально протиправними незалежно від добровільності їх вчинення? Відповідь на це питання має бути заперечною. Незважаючи на відсутність прямої нормативної фіксації добровільності, жодні

може констатуватися лише за наявності зазначених умов. Обов'язковість цієї ознаки додатково обґрунтовується тут: Розслідування колабораційної діяльності : практ. посібник / Є. О. Письменський, С. В. Головкін, А. В. Коваленко, В. В. Коваленко. Київ : ВД Дакор, 2023. С. 102 – 106.

[3] Питання щодо того, чи можна вважати громадянина України суб'єктом вчинення колабораційної діяльності у всіх її формах, розв'язується неоднозначно. Обґрунтування того, чому лише громадянин України може бути суб'єктом колабораційної діяльності, див. тут: Письменський Є.О. Громадянин України як суб'єкт колабораційної діяльності. *Протидія кримінальним правопорушенням на деокупованих територіях* : збірник матеріалів Всеукраїнської науково-практичної конференції (м. Кропивницький, 27 жовтня 2023 року). Кропивницький, 2023. С. 16 – 20.

[4] З іншими особливостями суб'єктивної сторони колабораційної діяльності можна ознайомитися тут: Письменський Є. О. Особливості кваліфікації колабораційної діяльності за ознаками суб'єктивної сторони. *Протидія проявам тероризму та колабораціонізму в умовах війни: стан та перспективи*: матеріали Всеукраїнського круглого столу (м. Кропивницький, 24 листопада 2023 року). Донецький державний університет внутрішніх справ. Кропивницький, 2023. С. 21 – 25.

вчинені під впливом примусу («недобровільні») дії, зокрема й передбачені ст. 111-1 КК України, не можуть визнаватися кримінально протиправними[5].

Далі розглянемо елементи складу кримінального правопорушення колабораційної діяльності, визначимо конкретний набір його обов'язкових ознак залежно від специфіки основного безпосереднього об'єкта та відповідної форми об'єктивної сторони.

Колабораційна діяльність в інформаційній сфері (ч. 1, ч. 6 ст. 111-1 КК України)			
Об'єкт складу кримінального правопорушення			
Основний безпосередній об'єкт	Національні інтереси держави в інформаційній сфері	**Додатковий безпосередній об'єкт**	інформаційна безпека, культурно-ідеологічні засади української нації
Об'єктивна сторона складу кримінального правопорушення			
Суспільно небезпечне діяння (альтернативні форми)	1) заперечення здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України	2) заклики до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, до невизнання поширення державного суверенітету України на тимчасово окуповані території України	3) здійснення інформаційної діяльності у співпраці з державою-агресором та/або його окупаційною адміністрацією, спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або уникнення нею відповідальності за збройну агресію проти України (за відсутності ознак державної зради)
Обстановка	1) умови окупації; 2) публічність (у межах першої та другої форм діянь)		
Суб'єкт складу кримінального правопорушення			
фізична особа	осудна особа	особа, яка досягла 16-річного віку	особа, яка є громадянином України
Суб'єктивна сторона складу кримінального правопорушення			
Вина	умисел		

[5] Більш докладно про добровільність як специфічну ознаку колабораційної діяльності див.: Письменський Є. О. Особливості кваліфікації колабораційної діяльності за ознакою добровільності. *Актуальні проблеми кримінального права* : матеріали XII Всеукр. наук.-теорет. конф., присвяч. пам'яті проф. П. П. Михайленка (Київ, 23 листоп. 2023 р.) / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2023. С. 167 – 170.

Основним **безпосереднім об'єктом** колаборaційної діяльності в інформаційній сфері є національні інтереси держави у сфері інформаційної діяльності. Колаборaційна діяльність в інформаційній сфері має потенціал зашкоджувати інформаційній безпеці, яка так само виступає одним з елементів національної безпеки держави. З огляду на це, факультативним **додатковим об'єктом** для зазначеного виду колаборaційної діяльності є підстави визнавати інформаційну безпеку. Культурно-ідеологічні засади української нації також можуть утворювати факультативний **додатковий об'єкт.**

З **об'єктивної сторони** колаборaційна діяльність в інформаційній сфері характеризується *діянням* у таких трьох альтернативних[6] формах: 1) заперечення а) здійснення збройної агресії проти України, б) встановлення та утвердження тимчасової окупації частини території України; 2) заклики: а) до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, б) до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, в) до невизнання поширення державного суверенітету України на тимчасово окуповані території України; 3) здійснення інформаційної діяльності у співпраці з державою-агресором та/або його окупаційною адміністрацією, спрямованої на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або уникнення нею відповідальності за збройну агресію проти України (за відсутності ознак державної зради).

Через вчинення таких діянь особа по суті бере участь у здійсненні ворожої пропагандистської діяльності, метою якої є встановлення та утвердження тимчасової окупації території України, виключення відповідальності за вчинення злочину агресії та інших міжнародних злочинів тощо.

Оскільки суспільно небезпечні наслідки не визначені як обов'язкова ознака

[6] Альтернативність форм суспільно небезпечних діянь передбачає, що для настання кримінальної відповідальності достатньо вчинення хоча б одного із зазначених діянь.

цього складу кримінального правопорушення, то за своєю конструкцією він відноситься до категорії формальних. Тому кримінальне правопорушення *вважатиметься закінченим* з моменту вчинення хоча б одного із зазначених діянь, тобто після висловлювання заперечень або закликів, а так само з моменту вчинення певної дії в межах здійснення інформаційної діяльності (наприклад, після створення інформації відповідного змісту).

Обов'язковою ознакою об'єктивної сторони складу кримінального правопорушення, передбаченого ч. 1 ст. 111-1 КК України, є *обстановка*, яка має бути публічною. Тобто відповіді дії вважатимуться кримінально караними лише за умови їх вчинення в умовах публічності.

Ще одна характеристика *обстановки* вчинення колабораційної діяльності має універсальний характер, з огляду на її правову природу, і стосується будь-якої форми колабораційної діяльності. Ідеться про вчинення такої діяльності в умовах окупації, які пов'язуються з певним станом взаємодії колаборанта та окупанта (про цю ознаку йшлося вище).

Заперечення (публічне) здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України становить таку поведінку, що полягає у відкритому вираженні думки про те, що зазначені факти є такими, які реально не встановлені або відсутні, а так само у відкритому спростуванні цих фактів. Як приклад, особа стверджує (відтворює тези російської пропаганди), що наша держава готувала напад на рф, влада якої намагається через проведення «спеціальної воєнної операції» захиститися від агресії України. В одному з випадків громадянин України був засуджений за вчинення такого заперечення, що полягало у висловлюваннях на кшталт: «Харків – це російське місто», «території України належать росії», «путін гарний президент, дії якого є правильними», «бандерівські вояки вбивають жінок та дітей, а також бомблять свої міста, а потім звинувачують у всьому армію росії»[7].

[7] Вирок Орджонікідзевського районного суду м. Харкова від 15 грудня 2022 р. у справі № 644/1843/22. URL: https://reyestr.court.gov.ua/Review/107893187.

Водночас, якщо особа здійснює заперечення фактів, не пов'язаних із здійсненням збройної агресії проти України або окупацією її території, то вчинення відповідних дій не тягне кримінальної відповідальності за ч. 1 ст. 111-1 КК України.

Заклики (публічні), про які йдеться в ч. 1 ст. 111-1 КК України, передбачають відкрите звернення до певного кола осіб, що містить ідеї, погляди чи вимоги, спрямовані на те, щоб схилити цих та інших осіб до:

- підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора,

- співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора,

- невизнання поширення державного суверенітету України на тимчасово окуповані території України[8].

Публічне вчинення зазначених дій характеризує їх як такі, що мають підвищену суспільну небезпеку. Згідно з ч. 1 примітки ст. 111-1 КК України, публічним вважається поширення закликів або висловлення заперечення до невизначеного кола осіб, зокрема в мережі Інтернет або за допомогою засобів масової інформації.

Під здійсненням ***інформаційної діяльності*** розуміється створення, збирання, одержання, зберігання, використання та поширення відповідної інформації (примітка 3 ст. 111-1 КК), тобто такої, що містить підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань, обґрунтовує уникнення нею відповідальності за збройну агресію проти України.

Суб'єкт кримінального правопорушення в інформаційній сфері – спеціальний. Це фізична (ч. 1 ст. 18 КК України), осудна (ч. 1 ст. 18, ст. 19 КК

[8] Про відмежування кримінального правопорушення, передбаченого ч. 1 ст. 111-1 КК України від суміжного складу кримінального правопорушення, яке містить ст. 436-2 КК України, див.: Письменський Є. О. Ідеологічний та культурно-освітній колабораціонізм як посягання на інформаційну безпеку (на прикладі ч. 1 ст. 111–1 КК України). *Кримінально-правова охорона інформаційної безпеки* : матеріали VI міжнар. наук.-практ. конференції, м. Харків, 12 трав. 2022 р. / [ред.кол.: Л.М. Демидова (голов. ред.) та ін.]. Харків : Право, 2022. С. 82 – 85.

України) особа, яка досягла віку, з якого може наставати кримінальна відповідальність, а саме 16 років (ч. 1 ст. 18, ст. 22 КК України). Окрім цього, суб'єктом колабораційної діяльності може бути лише громадянин України.

Набуття нового громадянства без виходу з українського громадянства не може виключати відповідальності за вчинення колабораційної діяльності (натомість це не стосується осіб без громадянства, які не можуть визнаватись колаборантами). Особа вважається громадянином України, доки вона у встановленому законом порядку не буде позбавлена цього громадянства (рішення про припинення громадянства ухвалює Президент України, про що видає відповідний указ). Правильною слід визнати позицію, відповідно до якої особа до видання зазначеного указу про припинення громадянства користується всім обсягом прав та виконує всі покладені на неї обов'язки, які має громадянин України[9].

Суб'єктивна сторона колабораційної діяльності в інформаційній сфері характеризується умислом, як прямим, так і непрямим[10]. За такого умислу особа: 1) усвідомлює суспільно небезпечний характер відповідного діяння, тобто здатність через здійснення інформаційної діяльності у співпраці з державою-агресором спричинити шкоду взятим під охорону кримінального права цінностям, а саме національним інтересам держави у відповідній сфері; 2) передбачає неминучість або можливість спричинення такої шкоди; 3) бажає або свідомо припускає, що в результаті вчинення такого діяння може бути заподіяна шкода відповідному об'єктові посягання.

[9] Левчук-Микитюк А. Визначення суб'єкта складу злочину «державна зрада». *Підприємництво, господарство і право*. 2020. № 4. С. 306 – 307.

[10] Тут і далі зважатимемо на те, що безнаслідкових кримінальних правопорушень не існує. Водночас у деяких з них (залежно від моделі законодавчого описання) суспільно небезпечні наслідки визначаються як конкретна ознака, наявність якої обов'язкова для настання кримінальної відповідальності. Тож певні кримінальні правопорушення з формальним складом можуть вчинятись з обома видами умислу, бо за будь-якої конструкції складу кримінального правопорушення зміст умислу розкривається через внутрішнє ставлення особи до всіх зовнішніх ознак (включаючи об'єкт кримінального правопорушення, який завжди відбиває потенційну або реальну шкідливість діяння), і безпосередньо не зумовлюється типом використаної нормативної моделі.

Колабораційна діяльність у сфері освіти (ч. 3 ст. 111-1 КК України)			
Об’єкт складу кримінального правопорушення			
Основний безпосередній об’єкт	Національні інтереси держави у сфері освітньої діяльності	**Додатковий безпосередній об’єкт**	інформаційна безпека (*для першої форми діяння*), нормальний соціальний розвиток неповнолітніх
Об’єктивна сторона складу кримінального правопорушення			
Суспільно небезпечне діяння (альтернативні форми)	1) здійснення пропаганди	2) дії з упровадження стандартів освіти держави-агресора	
Місце вчинення злочину	заклади освіти		
Обстановка	умови окупації		
Суб’єкт складу кримінального правопорушення			
фізична особа	осудна особа	особа, яка досягла 16-річного віку	особа, яка є громадянином України
Суб’єктивна сторона складу кримінального правопорушення			
Вина	прямий умисел (*для першої форми діяння*) умисел (*для другої форми діяння*)		
Мета	сприяння здійсненню збройної агресії проти України, встановленню та утвердженню тимчасової окупації частини території України, уникненню відповідальності за здійснення державою-агресором збройної агресії проти України (*для першої форми діяння*)		

Основним **безпосереднім об’єктом** колабораційної діяльності в освітній сфері є національні інтереси держави у сфері освіти. Так само, як і в попередньому випадку, колабораційна діяльність в освітній сфері здатна зашкоджувати інформаційній безпеці (якщо йдеться про здійснення пропаганди). З огляду на це, обов’язковим **додатковим об’єктом** для зазначеного виду колабораційної діяльності є інформаційна безпека. Нормальний соціальний розвиток неповнолітніх можна вважати факультативним **додатковим об’єктом** колабораційної діяльності у сфері освіти.

Спираючись на усталені підходи до розуміння змісту освітньої діяльності, включаючи відповідні положення законодавства України, можна стверджувати, що під діяльністю у сфері освіти слід розуміти діяльність, здійснювану працівниками закладів освіти з організації, забезпечення та реалізації освітнього процесу, суть якого насамперед становить передача, засвоєння,

примноження і використання знань, умінь та інших компетенцій у осіб, які навчаються. Колабораційна діяльність у сфері освіти, своєю чергою, передбачає умисну участь громадянина України у здійсненні зазначеної діяльності на окупованій території на догоду державі-агресору, що характеризується як підривна проти України.

З **об'єктивної сторони** кримінальне правопорушення, передбачене ч. 3 ст. 111-1 КК України, характеризується *діянням* у таких двох альтернативних формах: 1) здійснення пропаганди в закладах освіти незалежно від типів та форм власності; 2) дії, спрямовані на впровадження стандартів освіти держави-агресора в закладах освіти.

Оскільки суспільно небезпечні наслідки не визначені як обов'язкова ознака цього складу кримінального правопорушення, то за своєю конструкцією він відноситься до категорії формальних. Загалом можна погодитися з тим, що воно *вважатиметься закінченим* з моменту, коли особа здійснила хоча б один пропагандистський вчинок або розпочала вчинення дій, спрямованих на зміну стандартів освіти в закладах освіти[11].

Обов'язковою ознакою об'єктивної сторони цього складу кримінального правопорушення є обстановка його вчинення в умовах окупації.

Обов'язковою ознакою об'єктивної сторони для колабораційної діяльності у сфері освіти також є ***місце злочину*****,** яким визначено заклади освіти. Треба тлумачити так, що йдеться про ті з них, які утворені на окупованій території, де освітнім закладом можна вважати будь-яку установу, яка функціонує задля здійснення освітньої діяльності.

Згідно з п. 6 ч. 1 ст. 1 Закону України «Про освіту», ***закладом освіти*** визнається юридична особа публічного чи приватного права, основним видом діяльності якої є ***освітня діяльність***, яка, відповідно до п. 17 ч. 1 ст. 1 зазначеного закону, спрямовується на організацію, забезпечення та реалізацію ***освітнього процесу*** у формальній та/або неформальній освіті. Своєю чергою,

[11] Симоненко Н. О. Кримінально-правова новела щодо колабораційної діяльності. *Вісник асоціації кримінального права України*. 2022. № 1 (17). С. 99. URL : http://vakp.nlu.edu.ua/article/view/257848.

освітній процес – це система науково-методичних і педагогічних заходів, спрямованих на розвиток особистості шляхом формування та застосування її компетентностей (п. 16 ч. 1 ст. 1 Закону України «Про освіту»). Тип (школа, ліцей, гімназія, коледж, університет тощо) та форма власності (комунальна, приватна, державна) закладу освіти на кваліфікацію не впливають.

Поняття *пропаганди*, здійснення якої в закладах освіти тягне відповідальність, згідно з ч. 3 ст. 111-1 КК, потрібно тлумачити в негативному (деструктивному) значенні. Це форма комунікації з учасниками освітнього процесу, яка передбачає маніпулювання їхньою свідомістю з метою формування та роз'яснення в них таких уявлень і позицій, що обґрунтовують сприяння здійсненню збройної агресії проти України, установлення та утвердження тимчасової окупації частини території України, уникнення відповідальності за здійснення державою-агресором збройної агресії проти України. Відповідні уявлення та позиції, замість засудження, отримують схвальну оцінку, а їх втілення видається за поведінку, яку можна наслідувати та поширювати. У цьому аспекті резонним є твердження стосовно того, що здійснення пропаганди передбачає цілеспрямоване та активне поширення спеціально підібраних аргументів, фактів, думок тощо задля ідеологічного впливу та формування певних поглядів і переконань в адресата пропаганди[12].

Приклади здійснення пропаганди в закладах освіти на окупованих територіях наводить Уповноважений Верховної Ради України з прав людини: «У школах постійно проходять рашистські агітаційні заходи, на яких дітям розповідають про «геройства» окупаційної армії і звірства «українських націоналістів». Школярів мотивують писати листи підтримки російським військовим»[13].

---

[12] Колабораційна діяльність: загальні засади кримінально-правової кваліфікації : практич. порадник / О. О. Буряк, О. І. Букрєєв, Д. О. Олєйніков, М. В. Членов / за заг. ред. засл. юриста України А. З. Швеця. Харків : Право, 2022. С. 30.

[13] Уповноважений: рашистські окупанти проводять політику деградації системи освіти на території тимчасово окупованого Криму. [Електронний ресурс] 26 травня 2022 р. URL : https://ombudsman.gov.ua/news_details/upovnovazhenij-rashistski-okupanti-provodyat-politiku-degradaciyi-sistemi-osviti-na-teritoriyi-timchasovo-okupovanogo-krimu/

Як зауважують фахівці, важливим для кримінально-правової кваліфікації за ч. 3 ст. 111-1 КК України є здійснення незаконної освітянської діяльності, яка полягає у провадженні стандартів освіти держави-агресора в закладах освіти на тимчасово окупованій території України[14]. Під *упровадженням стандартів освіти* запропоновано розуміти заходи щодо узгодження освіти з певними вимогами (стандартами)[15]. Дії, спрямовані на впровадження стандартів освіти держави-агресора в закладах освіти, можуть полягати у вчиненні будь-яких актів поведінки з виконання та втілення вимог до обов'язкових результатів навчання та компетентностей здобувачів освіти того чи іншого рівня, що розроблені державою-агресором. Ідеться про забезпечення відповідності певного рівня освіти стандартам освіти держави-агресора через участь в розробленні навчального плану або/та освітньої програми (відповідних складників цих документів), їх затвердження, надання вказівок щодо реалізації[16].

Суб'єкт кримінального правопорушення, передбаченого ч. 3 ст. 111-1 КК України, – спеціальний (лише громадянин України).

Деякі категорії цих суб'єктів можуть характеризуватися додатковими ознаками, з огляду на специфіку взаємодії з ворогом. Наприклад, суб'єктом впровадження стандартів освіти держави-агресора в закладах освіти є той громадянин України, який уповноважений окупаційною адміністрацією держави-агресора на впровадження стандартів освіти (насамперед ідеться про керівника закладів освіти, заступників керівника закладу освіти, керівників структурних підрозділів закладу освіти, до компетенції яких належить

[14] Загиней-Заболотенко З. А., Присяжнюк І. І., Чаплюк О. І. Вчинення дій, спрямованих на впровадження стандартів освіти держави-агресора у закладах освіти як форма колабораційної діяльності. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2023. Вип. 79: ч. 2. С. 172– 173.

[15] Методичні рекомендації з питань кримінально-правової кваліфікації, оперативно-розшукової діяльності та кримінального провадження за ст. 111-1 КК України «Колабораційна діяльність» / С. Албул, Т. Волошанівська, А. Марченко, Г. Мудрецька, Г. Резніченко, І. Федоров, І. Чекмарьова. Одеса : ОДУВС, 2022. 67 с. URL : https:// dspace.oduvs.edu.ua/bitstream/123456789/2780/1/Метод%20Колаборація%202022.pdf

[16] Про інші особливості кримінально-правової оцінки дій, спрямованих на впровадження стандартів освіти держави-агресора в закладах освіти, див.: Письменський Є.О. Про кваліфікацію дій громадян України, спрямованих на впровадження стандартів освіти держави-агресора в закладах освіти (ч. 3 ст. 111-1 КК України). *Кримінально-правові, кримінологічні та кримінально-виконавчі заходи попередження злочинності* : матеріали Всеукраїнської наук.-практ. конф. 24 лист. 2023 р. Одеса : ОДУВС, 2023. С. 167 – 171.

впровадження стандартів освіти, членів методичних, педагогічних та вчених рад).

Суб'єктивна сторона здійснення пропаганди у сфері освіти характеризується прямим умислом. За такого умислу особа: 1) усвідомлює суспільно небезпечний характер відповідного діяння, тобто здатність через участь в освітній діяльності закладу освіти, що функціонує на окупованій території, спричинити шкоду взятим під охорону кримінального права цінностям, а саме національним інтересам держави в зазначеній сфері; 2) передбачає неминучість спричинення такої шкоди; 3) бажає в результаті вчинення такого діяння спричинити шкоду відповідному об'єктові посягання. Водночас не слід виключати вчинення впровадження стандартів освіти держави-агресора в закладах освіти як із прямим, так і непрямим умислом.

Мета є обов'язкової ознакою суб'єктивної сторони здійснення пропаганди у сфері освіти, а саме йдеться про сприяння здійсненню збройної агресії проти України, встановленню та утвердженню тимчасової окупації частини території України, уникненню відповідальності за здійснення державою-агресором збройної агресії проти України.

Водночас слід констатувати, що для установлення наявності мети здійснення пропаганди у сфері освіти є достатнім зафіксувати хоча б один з трьох варіантів (складників) мети, визначених у ч. 3 ст. 111-1 КК України: сприяння здійсненню збройної агресії проти України або встановленню та утвердженню тимчасової окупації частини території України або уникнення відповідальності за здійснення державою-агресором збройної агресії проти України.

За змістом ч. 3 ст. 111-1 КК України, мета не є обов'язкової ознакою суб'єктивної сторони дій з упровадження стандартів освіти держави-агресора.

Колабораційна діяльність в політичній сфері (ч. 6 ст. 111-1 КК України)			
Об'єкт складу кримінального правопорушення			
Основний безпосередній	Національні інтереси держави у сфері	**Додатковий безпосередній об'єкт**	Політична безпека

об'єкт	політичної діяльності		
Об'єктивна сторона складу кримінального правопорушення			
Суспільно небезпечне діяння (альтернативні форми)	1) організація заходів політичного характеру, спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або уникнення нею відповідальності за збройну агресію проти України	2) проведення заходів політичного характеру спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або уникнення нею відповідальності за збройну агресію проти України	3) активна участь у таких заходах
Обстановка	умови окупації		
Суб'єкт складу кримінального правопорушення			
фізична особа	осудна особа	особа, яка досягла 16-річного віку	особа, яка є громадянином України
Суб'єктивна сторона складу кримінального правопорушення			
Вина	умисел		

Основним **безпосереднім об'єктом** колабораційної діяльності в політичній сфері є національні інтереси держави у сфері політичної діяльності. Політична безпека утворює **обов'язковий додатковий об'єкт** для колабораційної діяльності в політичній сфері.

З **об'єктивної сторони** колабораційна діяльність в політичній сфері характеризується *діянням* у таких трьох альтернативних формах: 1) організація заходів політичного характеру, спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або уникнення нею відповідальності за збройну агресію проти України; 2) проведення заходів політичного характеру спрямованих на підтримку держави-агресора, її окупаційної адміністрації чи збройних формувань та/або уникнення нею відповідальності за збройну агресію проти України; 3) активна участь у таких

заходах.

Оскільки суспільно небезпечні наслідки не визначені як обов'язкова ознака цього складу кримінального правопорушення, то за своєю конструкцією він відноситься до категорії формальних. Тому кримінальне правопорушення *вважатиметься закінченим* з моменту вчинення хоча б одного із зазначених діянь, тобто після організації, проведення хоча б одного заходу політичного характеру, активної участі в ньому.

Обов'язковою ознакою цього складу кримінального правопорушення є обстановка його вчинення в умовах окупації.

Під ***організацією заходів політичного характеру*** розуміється така діяльність, що полягає в її впорядкуванні, ініціюванні та підготовці до проведення зазначених заходів, залученні до них визначеного або невизначеного кола осіб. Наприклад, ідеться про організаційні заходи з планування певного заходу, розроблення програми заходу, запрошення та супроводження його учасників, пошуку та облаштування місця проведення, використання технічних засобів.

Проведення заходів політичного характеру – це дії з керування та модерування процесом роботи під час таких заходів. Як стверджують фахівці, у контексті ч. 6 ст. 111-1 КК України проведення заходу – це етап, який починається з його відкриттям та, відповідно, завершується закриттям заходу, охоплюючи саму змістовну, активну та публічну його частину[17].

Активна участь у заходах політичного характеру полягає в точному та повному виконанні вказівок організаторів таких заходів, виступах та закликах до учасників заходів підтримувати державу-агресора, її окупаційні адміністрації чи збройні формування, участі в обговоренні політичних питань, роботі лічильної комісії тощо. Як зауважують дослідники, ідеться про вид діяльності, які свідчить про залученість особи до процесів, що відбуваються під час організації та проведення заходів політичного характеру, його взаємодію з

[17] Колабораційна діяльність: загальні засади кримінально-правової кваліфікації : практич. порадник / О. О. Буряк, О. І. Букреєв, Д. О. Олєйніков, М. В. Членов / за заг. ред. засл. юриста України А. З. Швеця. Харків : Право, 2022. С. 51.

учасниками процесу, та може виражатися в діях, спрямованих на підтримку порядку денного чи реалізацію прийнятих рішень, резолюцій, висновків тощо, а так само у виконанні поставлених завдань та іншому сприянні[18]. Слушною є думка про те, що лише безпосередня присутність особи на заході політичного характеру (наприклад, з певним плакатом) не може вважатися активною участю[19].

Поняття заходів політичного характеру містить примітка 2 ст. 111-1 КК України, відповідно до якої цими заходами є з'їзди, збори, мітинги, походи, демонстрації, конференції, круглі столи тощо.

Суб'єкт кримінального правопорушення, передбаченого ч. 6 ст. 111-1 КК України, – спеціальний (лише громадянин України).

Суб'єктивна сторона колабораційної діяльності в політичній сфері характеризується умислом, як прямим, так і непрямим. За такого умислу особа: 1) усвідомлює суспільно небезпечний характер відповідного діяння, тобто здатність через ту чи іншу участь у заходах політичного характеру спричинити шкоду взятим під охорону кримінального права цінностям, а саме національним інтересам держави у відповідній сфері; 2) передбачає неминучість або можливість спричинення такої шкоди; 3) бажає або свідомо припускає, що в результаті вчинення такого діяння може бути заподіяна шкода відповідному об'єктові посягання.

Колабораційна діяльність в господарській (економічній) сфері (ч. 4 ст. 111-1 КК України)			
Об'єкт складу кримінального правопорушення			
Основний безпосередній об'єкт	національні інтереси держави у сфері економічної діяльності	**Додатковий безпосередній об'єкт**	податкова безпека (для другої форми діяння)
Предмет	матеріальні ресурси		

[18] Злочинна колаборація в умовах збройної агресії: практич. порадник з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малюка. Київ : Алерта, 2023. С. 139 – 140.

[19] Кравчук О., Бондаренко М. Стаття «Колабораційна діяльність: аналіз нової статті 111-1 Кримінального кодексу України». URL : https://hrvector.org/podiyi/22-03-20-mbo.

<table>
<tr><td colspan="4">Об’єктивна сторона складу кримінального правопорушення</td></tr>
<tr><td>Суспільно небезпечне діяння (альтернативні форми)</td><td colspan="2">1) передача матеріальних ресурсів незаконним збройним чи воєнізованим формуванням, створеним на тимчасово окупованій території, та/або збройним чи воєнізованим формуванням держави-агресора</td><td>2) провадження господарської діяльності у взаємодії з державою-агресором, незаконними органами влади, створеними на тимчасово окупованій території, зокрема окупаційною адміністрацією держави-агресора</td></tr>
<tr><td>Обстановка</td><td colspan="3">умови окупації</td></tr>
<tr><td colspan="4">Суб’єкт складу кримінального правопорушення</td></tr>
<tr><td>фізична особа</td><td>осудна особа</td><td>особа, яка досягла 16-річного віку</td><td>особа, яка є громадянином України</td></tr>
<tr><td colspan="4">Суб’єктивна сторона складу кримінального правопорушення</td></tr>
<tr><td>Вина</td><td colspan="3">умисел</td></tr>
</table>

Основним **безпосереднім об’єктом** колабораційної діяльності в господарській (економічній) сфері є національні інтереси держави у сфері господарської діяльності. Колабораційна діяльність у господарській (економічній) сфері здатна зашкоджувати податковій безпеці (якщо йдеться про діяння у виді провадження господарської діяльності). З огляду на це, факультативним **додатковим об’єктом** для зазначеного виду колабораційної діяльності є податкова безпека.

Предметом колабораційної діяльності у формі матеріального забезпечення діяльності незаконних органів, підрозділів, формувань є ***матеріальні ресурси***, які утворюють базу для їх ресурсного забезпечення та з-поміж іншого охоплюють: ремонтні матеріали, сировину, напівфабрикати, електроенергію, паливо, будівлі, споруди, машини, механізми, устаткування, засоби телекомунікацій та електричного зв’язку, транспорт, зброю тощо.

З **об’єктивної сторони** колабораційна діяльність у господарській (економічній) сфері характеризується *діянням* у таких двох альтернативних формах: 1) передача матеріальних ресурсів: а) незаконним збройним чи

воєнізованим формуванням, створеним на тимчасово окупованій території, б) збройним чи воєнізованим формуванням держави-агресора; 2) провадження господарської діяльності у взаємодії з: а) державою-агресором, б) незаконними органами влади, створеними на тимчасово окупованій території, у тому числі окупаційною адміністрацією держави-агресора.

Оскільки суспільно небезпечні наслідки не визначені як обов'язкова ознака цього складу кримінального правопорушення, то за своєю конструкцією він відноситься до категорії формальних. Тому кримінальне правопорушення *вважатиметься закінченим* з моменту передачі матеріальних ресурсів та / або з початку провадження господарської діяльності, що слід вважати її виконанням.

Обов'язковою ознакою цього складу кримінального правопорушення є обстановка його вчинення в умовах окупації.

Під ***передачею матеріальних ресурсів*** незаконним збройним чи воєнізованим формуванням, створеним на тимчасово окупованій території, та/або збройним чи воєнізованим формуванням держави-агресора, треба розуміти їх надання відповідним формуванням у володіння, для тимчасового користування чи використання за цільовим призначенням. Такі ресурси можуть передаватися в будь-якій формі: зокрема, відкрито (публічно) та завуальовано, оплатно й безоплатно, з можливістю повернення та без такого.

Проведений фахівцями аналіз матеріалів кримінальних проваджень за колабораційну діяльність, передбачену ч. 4 ст. 111-1 КК України, дав змогу виділити такі поширені прояви надання матеріальних ресурсів: надання грошових коштів, постачання харчових продуктів та алкогольних напоїв, надання приміщень для проживання, забезпечення паливно-мастильними матеріалами, передача цілісних майнових комплексів, передача матеріальних цінностей (автомобілі, зброя, боєприпаси) та ін.[20].

[20] Дякур М. Д., Шевчук А. В. Щодо матеріального забезпечення як форми колабораційної діяльності в умовах воєнного стану. *ІІ Наукові читання пам'яті Ганса Гросса* : збірник тез Міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2022 р.). Чернівці : Чернівец. нац. у-нт ім. Ю. Федьковича, 2023. С. 148.

Прикладом правильної кримінально-правової оцінки, згідно з ч. 4 ст. 111-1 КК України дій особи з передачі матеріальних ресурсів окупантам, є також справа, за якою громадянин України, маючи як настоятель православного храму авторитет серед місцевих мешканців, зокрема осіб похилого віку, і приховуючи від останніх свої справжні наміри, здійснював збір продуктів харчування з них, особисто здійснював придбання товарів у продовольчому магазині, які далі передавав представникам збройних формувань країни-агресора, а також надавав їм у користування власний автомобіль для переміщення територією села[21].

Для інкримінування ч. 4 ст. 111-1 КК України колаборант необов'язково повинен бути ініціатором передачі матеріальних ресурсів. Така ініціатива може безпосередньо виходити і від окупанта. Водночас особа має діяти поза фізичним або психічним примусом, наявність якого в передбачених ст. 40 КК України випадках виключає кримінальну протиправність діяння. Отже, добровільно передати матеріальні ресурси не дорівнює ініціативі їх передання. За наявності такої ініціативи в окупанта достатньо встановити, що колаборант, передаючи матеріальні ресурси, усвідомлював можливість відмовитися від вчинення відповідних дій[22].

Щодо ***провадження господарської діяльності***, то тут можна орієнтуватися на поняття, яке містить ст. 3 Господарського кодексу України, згідно з якою господарською є діяльність суб'єктів господарювання у сфері суспільного виробництва, спрямована на виготовлення та реалізацію продукції, виконання робіт чи надання послуг вартісного характеру, що мають цінову визначеність. Фахівці наголошують, що фактично під категорію провадження господарської діяльності у взаємодії з незаконними органами влади, створеними на тимчасово окупованій території, потрапляє будь-яке постачання

[21] Вирок Конотопського міськрайонного суду Сумської області від 17 жовтня 2022 р. у справі № 577/2669/22. URL : https://reyestr.court.gov.ua/Review/106828264.

[22] Інші особливості кримінально-правової оцінки дій особи, яка передає матеріальні ресурси ворогу відповідно до ч. 4 ст. 111-1 КК України, див. тут: Письменський Є. О. Особливості кваліфікації колабораційної діяльності у формі передачі матеріальних ресурсів ворогові. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2023. Спеціальний випуск. № 2. С. 158 – 164.

товару, виконання робіт, надання послуг таким органам влади (окупаційній адміністрації) або державі-агресору[23].

Словосполучення «у взаємодії…» означає таку форму зв'язку суб'єктів, яка полягає в обов'язковій участі обидвох у відповідній господарській діяльності (виконання замовлення, об'єднання зусиль чи капіталів, реалізація продукції тощо) та спрямована на досягнення єдиної спільної мети; такою в контексті колаборації є мета спричинити шкоди інтересам України або її союзників (наприклад, встановлення та запровадження окупації частини території України, економічне ослаблення України або її союзників, зміцнення економічного потенціалу держави-агресора та ін.). Це певним чином звужувальне тлумачення кримінального закону, однак, по-перше, воно допустиме, а по-друге, дає можливість уникнути надмірної криміналізації «мирних» галузей економіки на тимчасово окупованих територіях України[24].

Як провадження господарської діяльності у взаємодії з державою-агресором, незаконними органами влади, створеними на тимчасово окупованій території, за ч. 4 ст. 111-1 КК України були кваліфіковані дії громадянина України, який отримував від військовослужбовців рф бензин і солярку, після чого, здійснював подальший їх продаж місцевому населенню, отримуючи частку з прибутку в розмірі 2 гри за 1 літр проданої продукції. Крім того, за схожою схемою, діючи спільно з представниками окупаційних сил, він реалізовував зернові культури, отримуючи за таку діяльність від окупантів паливо та харчові продукти, які в подальшому реалізовував серед місцевого населення[25].

Отже, провадження господарської діяльності у взаємодії з державою-агресором, незаконними органами влади, створеними на тимчасово окупованій території, становить таку поведінку, яка полягає в здійсненні діяльності,

---

[23] Кравчук О., Бондаренко М. Колабораційна діяльність: науково-практичний коментар до нової статті 111-1 КК. *Юридичний науковий електронний журнал*. 2022. № 3. С. 200; Науково-практичний коментар Кримінального кодексу України / за заг. ред. І. М. Копотуна. Київ : «К Н Т», 2023. С. 211.

[24] Марін О. Колабораційна діяльність: що є кримінально караним. *Academia.edu.* URL : https://bit.ly/3yq95sP.

[25] Вирок Київського районного суду м. Харкова від 20 грудня 2022 р. у справі № 953/6434/22. URL : https://reyestr.court.gov.ua/Review/107960245.

пов’язаної з виробництвом (виготовленням) продукції, торгівлею, наданням послуг, виконанням робіт. Така діяльність може мати підприємницький характер за наявності мети отримання прибутку, а так само некомерційний характер, коли мета отримання прибутку не ставиться (наприклад: діяльність пенсійних фондів, кредитних спілок, професійних спілок, житлово-будівельних кооперативів). З-поміж іншого зазначена в ч. 4 ст. 111-1 КК України взаємодія з державою-агресором, незаконними органами влади, створеними на тимчасово окупованій території, проявляється в здійсненні на їх користь певних платежів (за отриманий прибуток тощо).

Суб’єкт кримінального правопорушення, передбаченого ч. 4 ст. 111-1 КК України, – спеціальний (лише громадянин України).

При встановленні фактів здійснення зазначеної (господарської) діяльності, потрібно визначати, хто діяв і приймав рішення від імені суб’єкта господарювання. Насамперед це буде керівник, особа, яка виконує його обов’язки, або інша особа, яка діяла від імені суб’єкта господарювання (під час переговорів, укладення й підписання договору, поставки товарів, робіт, послуг). Особи, які виконували технічні функції (продавці, комірники), залежно від їхнього умислу, можуть бути пособниками в такому злочині, або їхнє діяння може не відповідати ознакам об’єктивної сторони злочину (здійснення господарської діяльності)[26].

Суб’єктивна сторона колабораційної діяльності в господарській (економічній) сфері характеризується умислом, як прямим, так і непрямим. За такого умислу особа: 1) усвідомлює суспільно небезпечний характер відповідного діяння, тобто здатність через здійснення економічної діяльності у співпраці з державою-агресором спричинити шкоду взятим під охорону кримінального права цінностям, а саме національним інтересам держави у відповідній сфері; 2) передбачає неминучість або можливість спричинення такої шкоди; 3) бажає або свідомо припускає, що в результаті вчинення такого

[26] Кравчук О., Бондаренко М. Колабораційна діяльність: науково-практичний коментар до нової статті 111-1 КК. *Юридичний науковий електронний журнал*. 2022. № 3. С. 200.

діяння може бути заподіяна шкода відповідному об’єктові посягання.

Колабораційна діяльність в адміністративній сфері (ч. 2 і ч. 5 ст. 111-1 КК України)			
Об’єкт складу кримінального правопорушення			
Основний безпосередній об’єкт	національні інтереси держави в адміністративній сфері	**Додатковий безпосередній об’єкт**	порядок реалізації управлінських повноважень, порядок формування органів з владними повноваженнями (*для третьої форми діяння*)
Об’єктивна сторона складу кримінального правопорушення			
Суспільно небезпечне діяння (альтернативні форми)	1) зайняття посади, не пов’язаної з виконанням організаційно-розпорядчих або адміністративно-господарських функцій, у незаконних органах влади, [створених на тимчасово окупованій території, зокрема в окупаційній адміністрації держави-агресора]	2) зайняття посади, пов’язаної з виконанням організаційно-розпорядчих або адміністративно-господарських функцій, у незаконних органах влади, [створених на тимчасово окупованій території, зокрема в окупаційній адміністрації держави-агресора]	3) обрання до незаконних органах влади [створених на тимчасово окупованій території]
Місце вчинення злочину	тимчасово окупована територія		
Обстановка	умови окупації		
Суб’єкт складу кримінального правопорушення			
фізична особа	осудна особа	особа, яка досягла 16-річного віку	особа, яка є громадянином України

Суб’єктивна сторона складу кримінального правопорушення	
Вина	умисел

Основним **безпосереднім об’єктом** колабораційної діяльності в адміністративній сфері є національні інтереси держави у сфері публічного управління та адміністрування.

Колабораційна діяльність в адміністративній сфері здатна зашкоджувати усталеній в Україні процедурі прийняття та реалізації управлінських рішень. З огляду на це, факультативним **додатковим об’єктом** для зазначеного виду колабораційної діяльності є порядок реалізації управлінських повноважень. Крім цього, обрання до незаконних органах влади, створених на тимчасово окупованій території, неодмінно спричиняє шкоду порядку формування органів з владними повноваженнями. Тож цей порядок також утворює **додатковий (обов’язковий) об’єкт**.

З **об’єктивної сторони** колабораційна діяльність в адміністративній сфері характеризується *діянням* у таких трьох альтернативних формах: 1) (добровільне) зайняття посади, не пов’язаної з виконанням організаційно-розпорядчих або адміністративно-господарських функцій, у незаконних органах влади, створених на тимчасово окупованій території, зокрема в окупаційній адміністрації держави-агресора; 2) (добровільне) зайняття посади, пов’язаної з виконанням організаційно-розпорядчих або адміністративно-господарських функцій, у незаконних органах влади, створених на тимчасово окупованій території, зокрема в окупаційній адміністрації держави-агресора[27]; 3) (добровільне) обрання до незаконних органах влади, створених на тимчасово окупованій території.

Оскільки суспільно небезпечні наслідки не визначені як обов’язкова ознака цього складу кримінального правопорушення, то за своєю конструкцією він

[27] Про ці форми діянь більш докладно див. тут: Письменський Є.О. Деякі особливості суспільно небезпечного діяння у складі колабораційної діяльності в адміністративній сфері. *Теоретичні та практичні проблеми розвитку кримінального права і процесу* : матеріали XII Всеукраїнського науково-практичного семінару (м. Івано-Франківськ, 8 грудня 2023 р.). Івано-Франківськ : Редакційно-видавничий відділ Університету Короля Данила, 2023. С. 95 – 99.

відноситься до категорії формальних. Тому кримінальне правопорушення *вважатиметься закінченим* з моменту вчинення одного із зазначених діянь. Цей момент, своєю чергою, пов'язується з фактичним початком виконання обов'язків за посадою, на яку призначили чи обрали певну особу.

Обов'язковою ознакою цього складу кримінального правопорушення є обстановка його вчинення в умовах окупації.

Обов'язковою ознакою об'єктивної сторони в межах колабораційної діяльності в адміністративній сфері є ***місце злочину*****,** яким визначено тимчасово окуповані території.

Під ***добровільністю***, похідні поняття від якого використовуються для характеристики окремих форм участі в діяльності незаконних органів, підрозділів, формувань, що утворені державою-агресором, розуміється така участь, що здійснюється за власною ініціативою суб'єкта колабораційної діяльності та за умови його вільного волевиявлення.

Особи, які в незаконних органах влади виконують суто професійні (лікар, статистик, соціальний працівник тощо), виробничі (як-от: водій, ювелір або працівник житлово-господарського сектору, інших подібних муніципальних структур), технічні (друкарка, технічний секретар, охоронник, провідник вагонів та ін.) функції *de jure* можуть визнаватися особами, які обіймають посади, не пов'язані з виконанням організаційно-розпорядчих або адміністративно-господарських функцій. Однак оскільки вони реалізують другорядні (допоміжні) функції, то відповідні дії можуть оцінюватися як малозначні, згідно з ч. 2 ст. 11 КК України.

У цьому контексті привертає увагу такий приклад із судової практики. Громадянка України, перебуваючи на тимчасово окупованій території, добровільно обійняла, т.зв., некерівну посаду квартальної Невоселівської селищної ради Краснолиманського району адміністрації м. Єнакієво ДНР, створеної рф. На ввірених їй вулицях у смт. Новоселівка вона, обіймаючи зазначену посаду, за вказівками керівництва окупаційної адміністрації, виконувала такі функції: сповіщала місцеве населення про збори, які проводили

представники держави-агресора; складала списки місцевих мешканців, які залишились у населеному пункті; допомагала обмежено дієздатним особам у складанні заяв на отримання палива, будівельних матеріалів тощо; прибирала адміністративні будівлі та їх прилеглі території; складала списки зруйнованих та покинутих будівель; складала списки загиблих мешканців селища; допомагала секретарю селищної ради у формуванні та видачі талонів про отримання вугілля для побутових потреб. Оскільки ці функції не належать до організаційно-розпорядчих або адміністративно-господарських, то вчинене діяння, кваліфіковане, згідно з ч. 2 ст. 111-1 КК України як добровільне зайняття громадянином України посади, не пов'язаної з виконанням організаційно-розпорядчих або адміністративно-господарських функцій, у незаконних органах влади, створених на тимчасово окупованій території[28]. Функції, які виконувала засуджена громадянка України, з огляду на вирок суду, є вичерпними і здебільшого зводяться до сприяння в забезпеченні життєдіяльності місцевих мешканців. Тож у наведеному прикладі викликає сумнів здатність відповідної поведінки спричинити істотний вплив на встановлення та утвердження тимчасової окупації частини території України.

Для порівняння. В іншій справі громадянка України добровільно обійняла посаду спеціаліста з екології та природних ресурсів у територіальному управлінні окупаційної адміністрації, здійснюючи заходи з планування роботи відділу, складання реєстрів пенсіонерів, які надійшли від пенсійного фонду, видачи довідок щодо фактичного місця проживання громадян, підготовки документів для отримання фінансової та гуманітарної допомоги від окупаційної влади тощо. Такі дії небезпідставно кваліфіковані за ч. 2 ст. 111-1 КК України як добровільне зайняття громадянином України посади, не пов'язаної з виконанням організаційно-розпорядчих функцій, у незаконних органах влади,

[28] Вирок Індустріального районного суду м. Дніпро від 15 грудня 2022 р. у справі № 202/10787/22. URL : https://reyestr.court.gov.ua/Review/107997353.

створених на тимчасово окупованій території, у тому числі в окупаційній адміністрації держави-агресора[29].

Відповідальність за колаборацію діяльність в адміністративній сфері диференціюється, зважаючи на тип посади, що обіймає особа на тимчасово окупованій території.

Зайняття ***посади, не пов'язаної з виконанням організаційно-розпорядчих або адміністративно-господарських функцій***, у незаконних органах влади – це обіймання такої посади в органах, що виконують функції влади та утворені всупереч передбаченому в Україні порядку, обов'язки за якою не передбачають здійснення: а) керівництва діяльністю інших осіб; б) управління або розпорядження майном. Прикладами таких посад можуть бути: конторський службовець, юрисконсульт, бухгалтер, працівник апарату, працівник підрозділу кадрів, інспектор з цивільного захисту.

Розглянемо такий приклад. Громадянка України, перебуваючи на тимчасово окупованій території, діючи з корисливих мотивів, добровільно обійняла посаду «секретаря» т.зв. Новоселівської селищної ради Краснолиманського району адміністрації м. Єнакієво ДНР, створеного окупаційною адміністрацією рф, яку обіймала до початку активної фази деокупації смт. Новоселівка Лиманської ТГ Краматорського району Донецької області. Перебуваючи на цій посаді, вона виконувала такі функції: проводила роботи з облаштування робочого місця для забезпечення діяльності ввіреної їй ділянки роботи; формувала електронний реєстр мешканців, які фактично проживали у смт. Новоселівка в період окупації; фіксувала в електронному реєстрі факти приїзду або виїзду місцевих мешканців смт. Новоселівка в період окупації; збирала та реєструвала заяви на отримання твердого палива для опалення (вугілля та дрова) від місцевих мешканців смт. Новоселівка; збирала кошти за розвезення вугілля до житлових будинків мешканців смт. Новоселівка; формувала електронний реєстр пошкоджених та зруйнованих у

[29] Вирок Київського районного суду м. Харкова від 07 листопада 2022 р. у справі № 953/6161/22. URL : https://reyestr.court.gov.ua/Review/107140508.

результаті обстрілів будинків місцевих мешканців; вела табелі робочого часу працівників адміністрації смт. Новоселівка в період окупації. Поведінка зазначеної особи оцінена згідно з ч. 2 ст. 111-1 КК України за ознаками добровільного зайняття громадянином України посади, не пов'язаної з виконанням організаційно-розпорядчих або адміністративно-господарських функцій, у незаконних органах влади, створених на тимчасово окупованій території, у тому числі в окупаційній адміністрації держави-агресора[30].

Зайняття ***посади, пов'язаної з виконанням організаційно-розпорядчих або адміністративно-господарських функцій***, у незаконних органах влади – це обіймання такої посади в органах, що виконують функції влади та утворені всупереч передбаченому в Україні порядку, обов'язки за якою передбачають здійснення: а) керівництва діяльністю інших осіб; б) управління або розпорядження майном. Насамперед прикладами таких посад можуть бути керівники будь-якої ланки в незаконних органах влади та його заступники, особи, уповноважені на розпорядження майном.

Обрання до незаконних органів влади передбачає обіймання певних посад у незаконних органах влади, щодо яких проводяться вибори, замість призначення на них відповідно до встановленого державою-агресором порядку. Зазначені вибори на території, яка перебуває під окупацією, слід розглядати як незаконні. Вони можуть лише імітувати усталений у демократичному суспільстві процес волевиявлення громадян.

Тимчасово окупована територія – це частина території України, яка, унаслідок акту агресії рф, перебуває під її контролем і в межах якої органи влади та місцевого самоврядування України позбавлені можливості здійснювати свої функції.

Суб'єкт кримінального правопорушення, передбаченого ч. 2 і ч. 5 ст. 111-1 КК України, – спеціальний (лише громадянин України).

Суб'єктивна сторона колабораційної діяльності в адміністративній сфері

[30] Вирок Індустріального районного суду м. Дніпра від 20 грудня 2022 р. у справі № 202/10786/22. URL : https://reyestr.court.gov.ua/Review/108045449.

характеризується умислом, як прямим, так і непрямим. За такого умислу особа: 1) усвідомлює суспільно небезпечний характер відповідного діяння, тобто здатність через здійснення діяльності за посадою в незаконних органах влади спричинити шкоду взятим під охорону кримінального права цінностям, а саме національним інтересам держави у відповідній сфері; 2) передбачає неминучість або можливість спричинення такої шкоди; 3) бажає або свідомо припускає, що в результаті вчинення такого діяння може бути заподіяна шкода відповідному об'єктові посягання.

Колабораційна діяльність у виборчій сфері (ч. 5 ст. 111-1 КК України)			
Об'єкт складу кримінального правопорушення			
Основний безпосередній об'єкт	національні інтереси держави у виборчій сфері	**Додатковий безпосередній об'єкт**	порядок підготовки та проведення виборів до представницьких органів публічної влади
Об'єктивна сторона складу кримінального правопорушення			
Суспільно небезпечне діяння (альтернативні форми)	1) участь в організації та проведенні незаконних виборів та/або референдумів на тимчасово окупованій території	2) заклики до проведення таких незаконних виборів та/або референдумів на тимчасово окупованій території	
Місце вчинення злочину	тимчасово окупована територія		
Обстановка	1) умови окупації; 2) публічність (для другої форми діяння)		
Суб'єкт складу кримінального правопорушення			
фізична особа	осудна особа	особа, яка досягла 16-річного віку	особа, яка є громадянином України
Суб'єктивна сторона складу кримінального правопорушення			
Вина	умисел		

Основним **безпосереднім об'єктом** колабораційної діяльності у виборчій сфері є національні інтереси держави у сфері формуванням органів

представницької влади (самоуправління). Колабораційна діяльність у виборчій сфері здатна зашкоджувати усталеній в Україні процедурі народного волевиявлення. З огляду на це, обов'язковим **додатковим об'єктом** для зазначеного виду колабораційної діяльності є порядок підготовки та проведення виборів до представницьких органів публічної влади.

З **об'єктивної сторони** колабораційна діяльність у виборчій сфері характеризується *діянням* у таких двох альтернативних формах: 1) участь в організації та проведенні незаконних виборів та/або референдумів на тимчасово окупованій території; 2) заклики до проведення таких незаконних виборів та/або референдумів на тимчасово окупованій території.

Оскільки суспільно небезпечні наслідки не визначені як обов'язкова ознака цього складу кримінального правопорушення, то за своєю конструкцією він відноситься до категорії формальних. Тому кримінальне правопорушення *вважатиметься закінченим* з моменту вчинення одного із зазначених діянь. Цей момент, своєю чергою, пов'язується з початком участі в процесі організації та/або проведення незаконних виборів та/або референдумів або після здійснення хоча б одного заклику до їх проведення.

Обов'язковою ознакою цього складу кримінального правопорушення є обстановка його вчинення в умовах окупації.

Обов'язковою ознакою закликів до проведення незаконних виборів та/або референдумів є ***обстановка***, яка, згідно з ч. 5 ст. 111-1 КК України, має бути публічною. Про публічну обстановку йшлося під час аналізу складу кримінального правопорушення, передбаченого ч. 1 ст. 111-1 КК України.

Обов'язковою ознакою об'єктивної сторони в межах колабораційної діяльності у виборчій сфері є ***місце злочину*** – тимчасово окуповані території.

Участь в організації та проведенні незаконних виборів та/або референдумів насамперед становить таку поведінку, що проявляється в забезпеченні проведення виборів та/або референдумів, зокрема роботі, так званих, виборчих комісій будь-яких рівнів (керівництво, членство, спостереження за виборчим процесом). Водночас прийнятним можна визнати й

більш широке трактування відповідної ознаки, що охоплює будь-які дії, спрямовані на організацію чи проведення виборів та/або референдумів, а саме: участь в органах, які проводять незаконні вибори та/або референдуми (виборчі комісії чи інші аналогічні органи), а так само кандидатування, спостерігання, агітація (інші форми участі в їх проведенні)[31].

Варто врахувати застереження про те, що участь в організації та проведенні незаконних виборів та/або референдумів на тимчасово окупованій території передбачає участь в органах, які проводять незаконні вибори, референдуми – виборчих комісіях чи інших аналогічних органах, інша участь у проведенні виборів, наприклад, як кандидат, спостерігач від кандидата. Натомість участь у незаконних виборах, референдумах лише в ролі виборця не утворює цього складу кримінального правопорушення[32]. Останнє твердження повністю відтворюють автори одного з коментарів Кримінального кодексу України[33].

Практику інкримінування участі в проведенні незаконних виборів та/або референдумів на тимчасово окупованій території можна проілюструвати на такому прикладі. Громадянка України була засуджена за вчинення злочину, передбаченого ч. 5 т. 111-1 КК України, за ознаками участі громадянина України у проведенні незаконного референдуму на тимчасово окупованій території, вчиненого за попередньою змовою групою осіб. Як установив суд, засуджена таким чином взяла участь у проведенні незаконного референдуму: у період 23 – 27 вересня 2022 р. вона з переносною урною для бюлетенів та наданими їй бюлетенями здійснила побудинковий обхід жителів с. Дудчани Милівської ОТГ Бериславського району Херсонської області з метою їх залучення до голосування щодо виходу Херсонської області зі складу України, утворення самостійної держави та входження її до складу рф на правах суб'єкта

[31] Колабораційна діяльність: загальні засади кримінально-правової кваліфікації : практич. порадник / О. О. Буряк, О. І. Букреєв, Д. О. Олєйніков, М. В. Членов / за заг. ред. засл. юриста України А. З. Швеця. Харків : Право, 2022. С. 49.

[32] Кравчук О., Бондаренко М. Колабораційна діяльність: науково-практичний коментар до нової статті 111-1 КК. *Юридичний науковий електронний журнал*. 2022. № 3. С. 201.

[33] Науково-практичний коментар Кримінального кодексу України / за заг. ред. І. М. Копотуна. Київ : «К Н Т», 2023. С. 212.

рф. Під час проведення референдуму громадянка України активно пропонувала мешканцям с. Дудчани проголосувати у спосіб поставлення відповідних відміток у бюлетені, вела облік громадян за списком, які проголосували під час проведення незаконного референдуму. Обґрунтовуючи правильність наданої кримінально-правової кваліфікації, суд, з-поміж іншого, щодо участі в організації та проведенні незаконних виборів та/або референдумів на тимчасово окупованій території зауважує про таке: ідеться про участь в органах, що проводять незаконні вибори, референдуми (виборчі комісії чи інші аналогічні органи), іншу участь особи в проведенні виборів, наприклад, як кандидата, спостерігача від кандидата; участь у незаконних виборах, референдумах лише в ролі виборця не утворює цього складу злочину[34]. Як бачимо, у вироку фактично відтворюється вищевикладена позиція, висловлена науковцями.

Заклики (публічні) до проведення незаконних виборів та/або референдумів – це відкрите звернення до певного кола осіб, що містить ідеї, погляди чи вимоги, спрямовані на те, щоб схилити цих та інших осіб до проведення незаконних виборів та/або референдумів. Поняття та особливості закликів як інформаційної дії розглядалися під час аналізу складу кримінального правопорушення, передбаченого ч. 1 ст. 111-1 КК України.

Суб'єкт кримінального правопорушення, передбаченого ч. 5 ст. 111-1 КК України, – спеціальний (лише громадянин України).

Суб'єктивна сторона колабораційної діяльності у виборчій сфері характеризується умислом, як прямим, так і непрямим. За такого умислу особа: 1) усвідомлює суспільно небезпечний характер відповідного діяння, тобто здатність через участь у здійсненні виборчої діяльності спричинити шкоду взятим під охорону кримінального права цінностям, а саме національним інтересам держави у відповідній сфері; 2) передбачає неминучість або можливість спричинення такої шкоди; 3) бажає або свідомо припускає, що в результаті вчинення такого діяння може бути заподіяна шкода відповідному

[34] Вирок Приморського районного суду м. Одеси від 27 вересня 2023 р. у справі № 522/5664/23. URL : https://reyestr.court.gov.ua/Review/113779964.

об’єктові посягання.

<table>
<tr><td colspan="4">Колабораційна діяльність у правоохоронній та судовій сферах (ч. 7 ст. 111-1 КК України)</td></tr>
<tr><td colspan="4">Об’єкт складу кримінального правопорушення</td></tr>
<tr><td>Основний безпосередній об’єкт</td><td>національні інтереси держави у правоохоронній та судовій сферах</td><td>Додатковий безпосередній об’єкт (факультативний)</td><td>правосуддя (для першої форми діяння), правопорядок (для другої форми діяння)</td></tr>
<tr><td colspan="4">Об’єктивна сторона складу кримінального правопорушення</td></tr>
<tr><td>Суспільно небезпечне діяння</td><td colspan="2">1) зайняття посади в незаконних судових органах [створених на тимчасово окупованій території]</td><td>2) зайняття посади в незаконних правоохоронних органах [створених на тимчасово окупованій території]</td></tr>
<tr><td>Місце вчинення злочину</td><td colspan="3">тимчасово окупована територія</td></tr>
<tr><td>Обстановка</td><td colspan="3">умови окупації</td></tr>
<tr><td colspan="4">Суб’єкт складу кримінального правопорушення</td></tr>
<tr><td>фізична особа</td><td>осудна особа</td><td>особа, яка досягла 16-річного віку</td><td>особа, яка є громадянином України</td></tr>
<tr><td colspan="4">Суб’єктивна сторона складу кримінального правопорушення</td></tr>
<tr><td>Вина</td><td colspan="3">умисел</td></tr>
</table>

Основним **безпосереднім об’єктом** колабораційної діяльності у правоохоронній та судовій сферах є національні інтереси держави у сфері забезпечення правопорядку та відправлення правосуддя. Крім цього, колабораційна діяльність у правоохоронній сфері здатна зашкоджувати усталеному в Україні режиму нормального правового життя. З огляду на це, обов’язковим **додатковим об’єктом** для зазначеного виду колабораційної діяльності є правопорядок. Колабораційна діяльність у судовій сфері здатна зашкоджувати усталеному в Україні порядку діяльності суду з розв’язання соціальних конфліктів, відновлення справедливості тощо. Отже, обов’язковим

додатковим об'єктом для зазначеного виду колабораційної діяльності є правосуддя.

З **об'єктивної сторони** колабораційна діяльність у правоохоронній та судовій сферах характеризується *діянням* у таких двох альтернативних формах: 1) зайняття посади в незаконних судових органах, створених на тимчасово окупованій території; 2) зайняття посади в незаконних правоохоронних органах, створених на тимчасово окупованій території.

Оскільки суспільно небезпечні наслідки не визначені як обов'язкова ознака цього складу кримінального правопорушення, то за своєю конструкцією він відноситься до категорії формальних. Тому кримінальне правопорушення *вважатиметься закінченим* з моменту вчинення одного і зазначених діянь. Цей момент, своєю чергою, пов'язується з фактичним початком виконання обов'язків за посадою, на яку призначили чи обрали особу в незаконних правоохоронних або судових органах.

Обов'язковою ознакою цього складу кримінального правопорушення є ***обстановка*** його вчинення в умовах окупації.

Обов'язковою ознакою об'єктивної сторони в межах колабораційної діяльності у виборчій сфері є ***місце злочину*** – тимчасово окуповані території.

Зайняття посади в незаконних судових органах – це обіймання такої посади в органах, що виконують функції судової влади та утворені всупереч передбаченому в Україні порядку, обов'язки за якою передбачають здійснення діяльності, характерної для суддів, народних засідателів та присяжних, а також забезпечення судової діяльності (працівники структур на кшталт судової адміністрації тощо). Як правильно зауважує Н. Антонюк, у цій частині йдеться про зайняття не лише посади судді, адже в судових органах чітко поділена компетенція між тими, хто безпосередньо здійснює правосуддя, тобто суддями, та апаратом судів (секретарі судового засідання, помічники судді, судові

розпорядники та ін.), які забезпечують організаційну складову в діяльності суддів[35].

Зайняття посади в незаконних правоохоронних органах – це обіймання такої посади в органах, що виконують правоохоронні функції та утворені всупереч передбаченому в Україні порядку, обов'язки за якою передбачають забезпечення правопорядку в суспільстві. Зокрема, ідеться про працівників прокуратури, поліції, органів безпеки, податкової адміністрації, органів з охорони кордону та митної справи. Чіткого переліку таких органів визначити неможливо, але «встановлюючи приналежність того чи іншого органу до правоохоронного, слід виходити з того, що такі органи повинні здійснювати правоохоронну функцію, яка є основною для них»[36].

Незаконними слід вважати такі органи, які виконують квазі-функції, що притаманні суду чи будь-якій правоохоронній структурі на території України, яка є тимчасово окупованою; вони не можуть належати до правоохоронної та судової систем України. Водночас правильною є думка, згідно з якою йдеться про органи, які виконують на тимчасово окупованих територіях функції, аналогічні органам, що визнаються в Україні правоохоронними. Назва чи точна відповідність усіх функцій чи завдань того чи іншого квазіправоохоронного органу, створеного державою-агресором на тимчасово окупованих територіях, значення не мають. Окупанти можуть сформувати окрему нормативну базу, що регулює їхню діяльність[37].

Суб'єкт кримінального правопорушення, передбаченого ч. 7 ст. 111-1 КК України, – спеціальний (лише громадянин України).

Суб'єктивна сторона колабораційної діяльності у правоохоронній та судовій сферах характеризується умислом, як прямим, так і непрямим. За

---

[35] Антонюк Н. Державна зрада і колабораційна діяльність: питання кримінально-правової кваліфікації. *Слово Національної школи суддів України*. 2021. № 4 (37). С. 63.

[36] Загиней-Заболотенко З. А. Добровільне зайняття громадянином України посади у незаконних органах влади, створених на тимчасово окупованій території, а також в незаконних судових або правоохоронних органах як форми колабораційної діяльності. *Юридичний науковий електронний журнал*. 2022. № 6. С. 320.

[37] Колабораційна діяльність: загальні засади кримінально-правової кваліфікації : практич. порадник / О. О. Буряк, О. І. Букрєєв, Д. О. Олєйніков, М. В. Членов / за заг. ред. засл. юриста України А. З. Швеця. Харків : Право, 2022. С. 55.

такого умислу особа: 1) усвідомлює суспільно небезпечний характер відповідного діяння, тобто здатність через участь у здійсненні правоохоронної або судової діяльності спричинити шкоду взятим під охорону кримінального права цінностям, а саме національним інтересам держави у відповідній сфері; 2) передбачає неминучість або можливість спричинення такої шкоди; 3) бажає або свідомо припускає, що в результаті вчинення такого діяння може бути заподіяна шкода відповідному об'єктові посягання.

Колабораційна діяльність у воєнній сфері (ч. 7 ст. 111-1 КК України)			
Об'єкт складу кримінального правопорушення			
Основний безпосередній об'єкт	національні інтереси держави у воєнній сфері	**Додатковий безпосередній об'єкт**	громадська безпека
Об'єктивна сторона складу кримінального правопорушення			
Суспільно небезпечне діяння (альтернативні форми)	1) участь в незаконних збройних чи воєнізованих формуваннях, створених на тимчасово окупованій території, та/або в збройних формуваннях держави-агресора	2) надання таким формуванням допомоги у веденні бойових дій проти ЗС України та інших військових формувань, утворених відповідно до законів України, добровольчих формувань, що були утворені або самоорганізовувалися для захисту незалежності, суверенітету та територіальної цілісності України	
Обстановка	умови окупації		
Суб'єкт складу кримінального правопорушення			
фізична особа	осудна особа	особа, яка досягла 16-річного віку	особа, яка є громадянином України
Суб'єктивна сторона складу кримінального правопорушення			
Вина	умисел		

Основним **безпосереднім об'єктом** колабораційної діяльності у воєнній сфері є національні інтереси держави із забезпечення воєнної безпеки.

Колаборaційна діяльність у воєнній сфері здатна зашкоджувати існуючому в Україні стану захищеності базових цінностей суспільства. З огляду на це, обов'язковим **додатковим об'єктом** для зазначеного виду колаборaційної діяльності є громадська безпека.

З **об'єктивної сторони** колаборaційна діяльність у воєнній сфері характеризується *діянням* у таких двох альтернативних формах: 1) участь у незаконних збройних чи воєнізованих формуваннях, створених на тимчасово окупованій території, та/або в збройних формуваннях держави-агресора; 2) надання таким формуванням допомоги у веденні бойових дій проти ЗС України та інших військових формувань, утворених відповідно до законів України, добровольчих формувань, що були утворені або самоорганізовувалися для захисту незалежності, суверенітету та територіальної цілісності України.

Оскільки суспільно небезпечні наслідки не визначені як обов'язкова ознака цього складу кримінального правопорушення, то за своєю конструкцією він належить до категорії формальних. Тому кримінальне правопорушення *вважатиметься закінченим* з моменту вчинення одного із зазначених діянь. Цей момент, своєю чергою, пов'язується з початком взяття участі в незаконних збройних чи воєнізованих формуваннях або після надання таким формуванням допомоги.

Обов'язковою ознакою цього складу кримінального правопорушення є обстановка його вчинення в умовах окупації.

Спираючись на положення примітки ст. 260 КК України, ***збройні формування держави-агресора*** в загальних рисах можна визначити таким чином: це воєнізовані групи, які незаконно мають на озброєнні придатну для використання вогнепальну, вибухову чи іншу зброю. Група є воєнізованою, якщо вона має організаційну структуру військового типу, а саме: єдиноначальність, підпорядкованість та дисципліну, і в яких проводиться військова або стройова чи фізична підготовка.

Незаконними слушно визнаються ті воєнізовані або збройні формування, створення та участь у яких не передбачена ні Конституцією, ні будь-яким

іншим законом України, а отже, вони не належать до жодного із законних воєнізованих або збройних формувань[38].

Під ***участю у незаконних збройних чи воєнізованих формуваннях*** слід розуміти перебування у складі цих формувань. Таке перебування передбачає, що особа прийнята до складу подібного формування за згодою його керівників та організаторів. Учасник незаконних збройних чи воєнізованих формувань самостійно або разом з іншими учасниками вчиняє різноманітні дії в межах виконання функцій таких формувань (наступальні операції, обстріл позицій ЗСУ тощо).

Участю в незаконному воєнізованому чи збройному формуванні з-поміж іншого визнаються такі дії: чергування на блокпосту; патрулювання міста; супровід автомобілів; перевезення зброї, боєприпасів, техніки, продуктів харчування тощо; здійснення розвідувальних заходів; спостереження за переміщенням українських військ; охорона будівель, військової техніки; проведення занять із фізичної, вогневої, бойової та спеціальної підготовки[39].

Надання незаконним збройним чи воєнізованим формуванням допомоги у веденні бойових дій проти ЗС України та інших військових формувань, утворених відповідно до законів України, добровольчих формувань, що були утворені або самоорганізовувалися для захисту незалежності, суверенітету та територіальної цілісності України, означає будь-яке сприяння цим формуванням у здійсненні відповідної діяльності за винятком передачі матеріальних ресурсів, відповідальність за яку має самостійну підставу (ч. 4 ст. 111-1 КК України). Наприклад, ідеться про усунення перешкод у діяльності незаконних збройних чи воєнізованих формувань, надання їм потрібної інформації, транспорті послуги, ремонтні роботи, фінансування, участь у будівництві оборонних споруд тощо.

---

[38] Колабораційна діяльність: загальні засади кримінально-правової кваліфікації : практич. порадник / О. О. Буряк, О. І. Букрєєв, Д. О. Олєйніков, М. В. Членов / за заг. ред. засл. юриста України А. З. Швеця. Харків : Право, 2022. С. 34.

[39] Злочинна колаборація в умовах збройної агресії: практич. порадник з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малюка. Київ : Алерта, 2023. С. 144 – 145.

Фахівці зауважують, що відмінність добровільної участі громадянина України в незаконних збройних чи воєнізованих формування, створених на тимчасово окупованій території, та/або у збройних формуваннях держави-агресора від добровільної допомоги полягає в тому, що під час участі суб'єкт попередньо вступає до цих формувань та діє у їх складі, а під час допомоги – діє поза складом таких формувань як приватна особа[40].

Суб'єкт кримінального правопорушення, передбаченого ч. 7 ст. 111-1 КК України, – спеціальний (лише громадянин України).

Суб'єктивна сторона колабораційної діяльності у воєнній сфері характеризується умислом, як прямим, так і непрямим. За такого умислу особа: 1) усвідомлює суспільно небезпечний характер відповідного діяння, тобто здатність через участь у незаконних збройних чи воєнізованих формуваннях, а так само надання їм допомоги, спричинити шкоду взятим під охорону кримінального права цінностям, а саме національним інтересам держави у відповідній сфері; 2) передбачає неминучість або можливість спричинення такої шкоди; 3) бажає або свідомо припускає, що в результаті вчинення такого діяння може бути заподіяна шкода відповідному об'єктові посягання.

РОЗДІЛ 2. ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ СПЕЦІАЛІСТОМ ПІД ЧАС ЗАЛУЧЕННЯ ДО РОЗСЛІДУВАННЯ КОЛАБОРАЦІЙЦНОЇ ДІЯЛЬНОСТІ.

2.1. Загальні положення використання спеціальних знань під час розслідування кримінальних правопорушень

Спеціальні знання - це професійні знання та вміння в галузі науки, техніки, мистецтва, ремесла тощо, що необхідні для розв'язання питань, які виникають у ході досудового розслідування кримінальних проваджень та розгляду їх матеріалів у суді. Спеціальними вважають знання, що не є

[40] Колабораційна діяльність: загальні засади кримінально-правової кваліфікації : практич. порадник / О. О. Буряк, О. І. Букреєв, Д. О. Олєйніков, М. В. Членов / за заг. ред. засл. юриста України А. З. Швеця. Харків : Право, 2022. С. 59.

загальнопоширеними, загальновідомими, а лише ті, яких набули спеціалісти-професіонали в тій чи іншій галузі науки, техніки, мистецтва, ремесла тощо. Значення застосування спеціальних знань під час розслідування кримінальних правопорушень полягає в тому, що вони:

а) забезпечують можливість здобуття доказів;

б) дозволяють встановлювати такі фактичні дані, які для органолептичного сприйняття та дослідження недоступні;

в) надають можливість перевіряти достовірність фактів, встановлених органолептичними засобами;

г) дозволяє за матеріальними відображеннями вирішувати проблему ототожнення людей та речей.

Отже**, спеціальні знання** – *це не пов'язані з веденням кримінального судочинства знання, які за змістом виходять за рамки загальноосвітніх та спеціальних освітніх програм, що використовуються для досягнення юридичних цілей в ході кримінального процесу*.

Залежно від процесуальної врегульованості порядку використання спеціальних знань і, відповідно, відбиття результатів у процесуальних документах, виділяють їх непроцесуальні та процесуальні форми.

Непроцесуальні форми використання спеціальних знань під час розслідування кримінальних правопорушень мають місце тоді, коли результати їх застосування не відбиваються у процесуальних документах.

Поширеною непроцесуальною формою використання спеціальних знань є відомчі ревізії та розслідування. Вони проводяться поза рамками кримінального процесу за ініціативою органів державного управління чи іншого власника для встановлення фактів, що мають певне юридичне значення.

Наприклад, це можуть бути документальні ревізії, товарознавчі дослідження тощо, які проводяться спеціалістами окремого підприємства, організації, установи чи відомства. За результатами цих перевірок і розслідувань складаються документи, які використовуються, перш за все, зацікавленими юридичними особами та відомствами. Результати таких

відомчих ревізій та розслідувань – «акти», «висновки» та інші документи залучаються до матеріалів кримінальних проваджень, як витребувані документи згідно із ст. 93 КПК України і можуть розглядатися як процесуальні джерела доказів (ч. 2 ст. 84 КПК України).

Наступною непроцесуальною формою використання спеціальних знань під час розслідування кримінальних правопорушень є консультативна допомога спеціалістів. З цією метою використовується вже накопичений досвід спеціаліста з урахуванням особливостей конкретних обставин.

Така допомога надається в усній або письмовій формі. Письмова консультація може надаватися як фізичними, так і юридичними особами (експертними закладами, профільними науково-дослідними інститутами, вищими навчальними закладами та іншими установами і закладами) за письмовим зверненням слідчого.

Консультація є думкою спеціаліста, яка має тільки орієнтуюче значення в кримінальному провадженні. Навіть викладена письмово, вона не може розглядатися як доказ, оскільки не має процесуальних гарантій достовірності викладених відомостей.

Консультація може слугувати тільки підставою для прийняття тих чи інших тактичних або процесуальних рішень, однак відповідальність за це рішення повністю несе та посадова особа, яка прийняла його.

Процесуальні форми використання спеціальних знань відіграють більш значущу роль під час розслідування кримінальних правопорушень. Це пов’язано з тим, що факт застосування спеціальних знань у таких випадках відображається у процесуальних документах (постановах, протоколах слідчих (розшукових) і судових дій, висновках експертів). Додержання встановлених правил складання процесуальних документів є засобом забезпечення достовірності відображених в них фактів.

Під час розслідування кримінальних правопорушень процесуальні форми використання спеціальних знань застосовуються як для самостійного

вирішення певних завдань розслідування, так і для перевірки фактів, встановлених непроцесуальним шляхом.

Змішана форма використання спеціальних знань (довідково-консультаційна діяльність у кримінальному провадженні, перевірка за криміналістичними обліками, письмові пояснення спеціалістів).

Суб'єктами застосування спеціальних знань є спеціалісти та судові експерти, правовий статус яких визначає кримінальне процесуальне законодавство (ст.ст. 69 і 71 КПК України) та ЗУ «Про судову експертизу» від 25.02.1994 р.

Експертом у кримінальному провадженні є особа, яка володіє науковими, технічними або іншими спеціальними знаннями, має право відповідно до Закону України "Про судову експертизу" на проведення експертизи і якій доручено провести дослідження об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та дати висновок з питань, які виникають під час кримінального провадження і стосуються сфери її знань (ч. 1 ст. 69 КПК України).

Спеціалістом у кримінальному провадженні є особа, яка володіє спеціальними знаннями та навичками і може надавати консультації, пояснення, довідки, висновки та інші документи під час досудового розслідування і судового розгляду з питань, що потребують відповідних спеціальних знань і навичок.

У разі необхідності та за наявності підстав може бути залучено з іноземної держави, міжнародної організації як спеціаліста фахівця у галузі хімічної, біологічної, радіаційної, ядерної чи іншої зброї. (ч. 1 ст. 71 КПК України). Він звертає увагу слідчого на обставини, пов'язані з виявленням та закріпленням доказів, дає пояснення з приводу спеціальних питань, які застосовуються.

Спеціаліст відповідно до своїх обов'язків, передбачених КПК України, реалізує свої спеціальні знання у таких формах:

1) практичної діяльності (підготовка, організація та проведення окремих СРД; пошук, виявлення, фіксація та вилучення слідів (мікрооб'єктів), речових доказів, виявлення, огляд та відібрання зразків для експертного дослідження);

2) методичної діяльності (застосування науково-практичних прийомів та методів проведення окремих СРД);

3) технічної діяльності (вибір і застосування науково-технічних засобів, що використовуються для виявлення та фіксації речових доказів);

4) консультативної діяльності (надання усних та письмових роз'яснень з питань, які виникають у ході проведення слідчих (розшукових) дій, або питань, які в майбутньому будуть вирішуватись за допомогою експертизи).

При цьому варто розрізняти типові види консультацій спеціаліста під час розслідування кримінальних правопорушень, а саме:

1) консультації загального характеру, що дозволяють слідчому зорієнтуватися в події кримінально-протиправного діяння, його механізмі, масштабах злочинної діяльності, колі учасників тощо, у тій частині цих питань, що пов'язана зі спеціальними знаннями. Отже, такі консультації мають ознайомлювальний характер і проводяться зазвичай у період здійснення початкових, невідкладних СРД (зокрема, у процесі огляду місця події для фотографування, складення схем, планів, креслень, відбору зразків для проведення експертизи тощо);

2) конкретні консультації із спеціальних питань під час підготовки до проведення СРД. Такі консультації фахівця є засобами підвищення ефективності окремих СРД (наприклад, допит, слідчий експеримент тощо).

За допомогою і на основі таких консультацій слідчий більш точно визначає обсяг, напрям і межі з'ясування питань, що вимагають спеціальних пізнань. Для з'ясування деяких питань, що виникають при аналізі та оцінці даних, слідчий може залучати фахівця для якісного відтворення реальної картини протиправного діяння, а також перевірки достовірності фактів. Спеціаліст-консультант, беручи участь у підготовці СРД, може прогнозувати поведінку його учасників і способи унеможливлення небажаних ситуацій. Так,

під час підготовки до допиту підозрюваного можуть бути окреслені можливі варіанти помилкових пояснень фактів, спроби їх маскування тощо. При цьому досвідчений спеціаліст може рекомендувати способи викриття неточних, неповних, помилкових показань, зазначити фактичний матеріал, на який варто посилатися в таких випадках.

Тому досить поширеною процесуальною формою використання спеціальних знань є залучення спеціаліста до участі в проведенні досудового розслідування або судового розгляду.

Як спеціаліст може бути залучена особа, яка, по-перше, володіє спеціальними знаннями і навичками; по-друге, не зацікавлена у результатах розслідування; по-третє, не проводила ревізій або перевірок тощо, матеріали яких використовуються у цьому провадженні.

Для участі в процесуальних діях як спеціалісти залучаються:

- спеціалісти-криміналісти підрозділів криміналістичного забезпечення, що входять до складу органів досудового розслідування Національної поліції України;
- співробітники судово-експертних установ всіх рівнів та різної відомчої приналежності;
- компетентні працівники контролюючих органів;
- представники інших практичних, а також наукових та педагогічних колективів, які володіють глибокими знаннями у своїх галузях діяльності;
- приватні особи, що не входять до штату яких-небудь офіційних структур.

Процедура участі спеціаліста та одержані результати відображаються в протоколі слідчої (розшукової) дії.

Під час розслідування кримінальних правопорушень спеціалісти залучаються до участі в слідчих (розшукових) діях у випадках:

- відсутності у слідчого спеціальних знань і навичок, необхідних для кваліфікованої підготовки та проведення слідчої (розшукової) дії;

- недостатнього володіння слідчим прийомами та засобами швидкого і якісного виконання певної роботи, що вимагає спеціальних знань і навичок;
- необхідності з етичних чи тактичних міркувань доручити виконання певних дій саме спеціалісту;
- одночасному застосуванні декількох засобів криміналістичної техніки;
- необхідності виконати значний обсяг роботи, яка потребує спеціальних знань та навичок.

Залучення спеціаліста – право, а не обов’язок слідчого. Він сам вирішує це питання, керуючись своїми уявленнями про обсяг та складність роботи під час проведення тієї чи іншої слідчої (розшукової) дії, а також про необхідність спеціальної допомоги.

Спеціаліст бере участь у слідчих (розшукових) діях, у негласних слідчих (розшукових) діях, а також в інших процесуальних діях для сприяння у виявленні, закріпленні та вилученні предметів і документів, застосуванні технічних засобів у дослідженні матеріалів провадження, для формулювання запитань експерту, для роз'яснення сторонам і суду питань, які стосуються його спеціальних знань. Він діє лише в межах компетенції того процесуального учасника провадження в сенсі використання спеціальних знань і навичок, який доручив йому виконання певної роботи.

Спеціаліст у ході або після завершення слідчої (розшукової) дії може сприяти попередньому дослідженню слідів та інших об'єктів, висловлювати певні припущення і ймовірні висновки, що не заносяться до протоколу слідчої дії, не мають доказового значення, але можуть братися до уваги при формуванні версій, перевірятися шляхом проведення експертиз та інших слідчих (розшукових) дій. Ще одна функція спеціаліста полягає у наданні необхідних консультацій під час досудового слідства: у вивченні документів, в аналізі інформації, що міститься в показаннях конкретних осіб, у підготовці до проведення певних слідчих (розшукових) дій, в аналізі певних обставин події, що розслідується, якщо це потребує відповідних спеціальних знань. Подібні

консультації та роз'яснення можуть бути надані спеціалістом і під час дослідження доказів у ході судового розгляду

Також, спеціаліст може бути залучений для проведення для проведення досліджень, в тому числі ідентифікаційних. Відповідно до п. 4 ст. 71 КПК України спеціаліст має право: «надавати довідки, висновки з питань, що належать до сфери його знань, щодо ідентифікації особи, зброї, бойових припасів, вибухових речовин, вибухових пристроїв, слідів вибуху або пострілу, наркотичних засобів, психотропних речовин, їх аналогів і прекурсорів, сильнодіючих лікарських засобів». Таку форму використання спеціальних знань можна віднести до процесуальних, оскільки у ст. 99 КПК України зазначається можливість долучати довідки, висновки та інші документи спеціалістів до матеріалів кримінального провадження в якості документів, які є джерелами доказів.

В структурі Національної поліції України функцію спеціалістів виконують спеціалісти-криміналісти. Їх діяльність визначено наказом МВС України № 570 від 06.07.2017 року «Про організацію діяльності слідчих підрозділів Національної поліції України», зареєстрованого в Міністерстві юстиції України від 27 липня 2017 р. за № 918/30786, де зазначено:

1. Спеціаліст-криміналіст - особа, яка володіє науковими, технічними або іншими спеціальними знаннями та навичками застосування технічних або інших засобів і як спеціаліст здійснює техніко-криміналістичне забезпечення діяльності, яке полягає в комплексному застосуванні системи науково-технічних засобів розслідування.

2. Спеціаліст-криміналіст, у своїй діяльності безпосередньо підпорядковується та підзвітний начальникові слідчого підрозділу. У разі утворення у складі слідчого підрозділу криміналістичного забезпечення слідчих (розшукових) дій керівник цього підрозділу підпорядковується безпосередньо начальникові слідчого підрозділу.

3. Працівники поліції у межах компетенції зобов’язані надавати спеціалісту-криміналісту всебічну допомогу у виконанні його обов’язків.

4. Спеціаліст-криміналіст зобов’язаний виконувати усні та письмові доручення начальника відповідного слідчого підрозділу, його заступників, слідчих у встановлені строки та у визначеному законодавством порядку.

5. Спеціаліст-криміналіст залучений до проведення слідчих (розшукових) дій у порядку, передбаченому статтею 71 КПК України, як спеціаліст:

- прибуває на місце проведення слідчих (розшукових) дій з необхідними техніко-криміналістичними засобами та витратними матеріалами;

- перед початком огляду знайомиться з обставинами події, пропонує слідчому план огляду місця події, межі території огляду місця події, а також застосування конкретних науково-технічних засобів для виявлення, фіксації та вилучення слідової інформації;

- перед застосуванням техніко-криміналістичних засобів повідомляє слідчому їх характеристики, модель та серійний номер за його наявності;

- надає допомогу слідчому з виявлення, фіксації і вилучення слідової інформації;

- застосовує техніко-криміналістичні засоби, зокрема фото- і відеотехніку, безпілотні літальні апарати, технічні засоби, прилади та спеціальне обладнання, прилади швидкого встановлення геномної інформації людини, засоби для експрес-аналізу, пристрої копіювання цифрової інформації, пошукові та інші прилади з метою фіксації слідової інформації;

- надає консультації за зовнішніми характеристиками вилучених об’єктів, звертає увагу слідчого на фактичні дані, що можуть мати значення для розслідування обставин кримінального правопорушення;

- під час огляду надає слідчому допомогу у фіксації у протоколі інформації щодо знайдених слідів і речових доказів, а також (за потреби) в упакуванні об’єктів;

- за запитом слідчого надає фотографії в електронній формі або виготовляє фототаблицю слідчої (розшукової) дії;

- після закінчення чергування доповідає про результати виконаної роботи керівникові підрозділу криміналістичного забезпечення;

- здійснює відбір біологічного матеріалу в осіб і встановлює його генетичні ознаки (геномну інформацію) із застосуванням приладів швидкого встановлення геномної інформації людини у випадках, передбачених статтею 5 Закону України «Про державну реєстрацію геномної інформації людини» (за наявності відповідних технічних засобів);

- з метою встановлення зв'язків між даними, що можуть мати значення для кримінального провадження, проводить перевірки їх за інформаційною підсистемою «СЛІД» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції

2.2. Особливості залучення спеціаліста до розслідування колабораційної діяльності.

Як і при розслідуванні інших кримінальних правопорушень, розслідування колобораційної діяльності потребує суворого дотримання норм КПК.

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

– речові докази;

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

– документи, що засвідчують особу заарештованого, підозрюваного, обвинуваченого (підсудного); – інші документи, що мають значення у провадженні.

Відповідно до ст. 84 Кримінального процесуального кодексу України доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому законом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів.

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

Відповідно до ст. 99 КПК України документом є спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. До документів, за умови наявності в них відомостей, передбачених частиною першою статті 99 КПК, можуть належати: матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані); протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії; висновки ревізій та акти перевірок.

Оригіналом документа є сам документ, а оригіналом електронного документа - його відображення, якому надається таке ж значення, як документу.

Дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа.

У деяких випадках, а саме тоді, коли документ незмінний, він може мати одночасно ознаки і документа, і речового доказу.

Таким чином, слідчий, прокурор для отримання належної доказової бази колаборaційної діяльності повинен здійснити ряд слідчих (розшукових) дій. Основними слідчими (розшуковими) діями для даної категорії правопорушень, де залучається спеціаліст, є:

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

– огляд (ст. 237 КПК України).

- *призначення відповідних судових експертиз (ст. 242 КПК України).*

Крім того, пошук та вилучення доказів колаборaційної діяльності може здійснюватися шляхом:

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

- тимчасового доступу до речей і документів (ст. 159 КПК України) на підставі ухвали слідчого судді, суду;

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

– зняття інформації з електронних інформаційних систем (ст. 264 КПК України);

– дослідження інформації, отриманої при застосуванні технічних засобів (ст. 266 КПК України);

– установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України).

За результатом проведення слідчої (розшукової) або іншої процесуальної дії складають протокол, до якого може бути приєднано додатки. Серед видів додатків ч. 2 ст. 105 КПК України визначає:

1) спеціально виготовлені копії, зразки об’єктів, речей і документів;

2) письмові пояснення спеціалістів, які брали участь у проведенні відповідної процесуальної дії;

3) стенограми, аудіо-, відеозаписи процесуальної дії;

4) фототаблиці, схеми, зліпки, носії комп’ютерної інформації та інші матеріали, які пояснюють зміст протоколу.

Ці додатки повинні бути засвідчені підписами слідчого, прокурора, спеціаліста, інших осіб, які брали участь у їх виготовленні.

Очевидною є пріоритетна роль спеціаліста, залученого до процесуальної дії, у виготовленні зазначених вище додатків. Крім того, під час негласних слідчих (розшукових) дій знання спеціаліста можуть бути використані у формах: надання консультацій; надання безпосередньої технічної допомоги (фотографування, складення схем, планів, креслень, відбір зразків для проведення експертизи тощо); безпосередньої участі у проведенні негласної слідчої (розшукової) дії.

Спеціаліст може бути залучений для надання безпосередньої технічної допомоги (фотографування, складення схем, планів, креслень, відбір зразків для проведення експертизи тощо) сторонами кримінального провадження під час досудового розслідування і судом під час судового розгляду, а також для надання висновків з питань, що належать до сфери його знань, під час досудового розслідування кримінальних проступків, зокрема у випадках, передбачених ч.3 ст.214 КПК України

2.3. Джерела доказів.

Вчинення колабораційної діяльності на тимчасово окупованій території України, до якої не мають доступу працівники правоохоронних органів, ускладнює проведення всіх необхідних слідчих (розшукових) та процесуальних дій з метою встановлення обставин, які підлягають доказуванню у кримінальному провадженні.

Вимагають визначення та проведення якомога більшого комплексу слідчих (розшукових) та процесуальних дій з метою перевірки інформації про факт можливої колаборaційної діяльності, зокрема щодо підтвердження або спростування отриманої інформації про причетність особи до кримінальної колаборaційної діяльності, а у випадку її підтвердження, – здобуття достатніх доказів вчинення таких правопорушень.

Окрім обставин, визначених ст. 91 КПК України, які підлягають доказуванню у кримінальному провадженні, слід також враховувати та з'ясовувати:

- властивості інформації змінюватися на шляху від першоджерела до громадськості та правоохоронних органів;
- можливий наклеп з боку недоброзичливців;
- співпраця, вчинена під безпосереднім впливом фізичного або психологічного примусу, що можуть виключати кримінальну протиправність;
- співпраця, вчинена з метою виконання законного наказу або розпорядження.

У вказаній категорії кримінальних проваджень підлягають встановленню та дослідженню обставини, що свідчать про здійснення колаборaційної діяльності та/або призначення на посади в незаконно створених так званих органах влади на тимчасово окупованій території України, а також на підтвердження факту тимчасової окупації території України.

Як свідчить практика, колаборaційна діяльність проявляється у розміщенні публікацій, відеоматеріалів в соціальних мережах Facebook, «Одноклассники», «Youtube» тощо, які є публічно доступними, шляхом поширення їх на своїй сторінці в яких заперечується збройна агресія російської федерації проти України та здійснюються заклики до підтримки рішень та дій держави-агресора в Україні; зйомці відео з публічними закликами до підтримки рішень та дій російської федерації, яке викладається до публічного доступу в мережу Інтернет та різні канали «ТікТок», «Телеграм» тощо; лайки та

перемощування публікацій, в яких містяться матеріали, спрямовані на підтримку держави-агресора, публічне заперечення здійснення збройної агресії російської федерації проти України та публічні заклики до підтримки рішень та дій держави-агресора, розміщення коментарів, що закликають до підтримки рішень та дій держави-агресора, збройних формувань, окупаційної адміністрації держави-агресора; поширення постів, які спрямовані до невизначеного кола осіб та публічно закликають до підтримки рішень та дій держави-агресора, публічне заперечення здійснення збройної агресії проти України, яке здійснюється в публічному місці (у торговельних центрах, магазинах, подвір'ї будинку, на різних мітингах тощо), а саме висловлення повної підтримки дій агресора та публічні заклики до підтримки рішень та дій держави-агресора;

Документування та розслідування колабораційної діяльності передбачає застосування наступних методів:

1) фіксація та систематизація доступних фактів (дій, діяльності) підозрюваних осіб у ЗМІ, в тому числі в інтернет-ресурсах, на місцевому телебаченні тощо;

2) отримання аудіо-, фото- та відеосвідченнь очевидців (постраждалих) з числа місцевих жителів окупованої території;

3) аналіз ЗМІ країни-терориста щодо висвітлення стану справ на окупованих територіях;

4) отримання оригіналів/копій розпорядчих документів місцевих «керівників» населеного пункту, письмові заяви, відомості оплати праці тощо.

Тому, доказами у вказаній категорії кримінальних проваджень, переважно виступають такі документи:

- матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані), що містяться у відкритих, закритих мережах, перебувають у свідків;

- веб-сайти та сторінки в соціальних мережах незаконно створених органів влади; відкриті телеграм канали; різноманітні засоби масової

інформації, що працюють на тимчасово окупованій території України, та держави-агресора, що висвітлюють створення окупаційної владою псевдо-органів влади;

- веб-сайти, сторінки в соціальних мережах громадськості (у тому числі окремих фізичних осіб); журналістів, адвокатів, органів державної влади України та місцевого самоврядування, відкриті телеграм канали; різноманітні засоби масової інформації, що фіксують та висвітлюють воєнні злочини та злочини проти основ національної безпеки України, вчинені на тимчасово окупованій території України, а також, що висвітлюють події на тимчасово окупованій території України;

- хмарні сховища (англ. *cloud storage*, або ще *хмара*, *backup*) — це модель зберігання даних у комп'ютері, в якій цифрові дані накопичуються в логічні пули, а фізичне зберігання охоплює кілька серверів (зазвичай у різних місцях). Фізичне середовище, як правило, належить хостинговим компаніям, які ним керують. Ці постачальники хмарних систем зберігання даних відповідають за збереження наявної інформації та забезпечення доступу до неї, а також за надійну роботу фізичного середовища.

- фото, відео, аудіо файли; різноманітні відкриті та приватні месенджери, що містять у свідків;

- громадські та журналістські розслідування (заяви, письмові повідомлення, різні документи).

Типовими матеріальними слідами колаборaційної діяльності є: текстова інформація, обладнання, яким користувалася особа при передачі інформації, список контактів з якими вона тримала зв’язок, інформація із соціальних мереж, що містять фотозображення, відео- та аудіозаписи, документи на яких зафіксована інформація про факти державної зради тощо.

При передаванні інформації «слідова картина» нерідко також включає в себе також звукові сліди, які мають важливе значення для даного кримінального правопорушення. Нерідко важливе значення для встановлення механізму вчинення такого кримінального правопорушення мають виявленні

текстові повідомлення в соціальних мережах або список контактів та записані розмови, збережені фото- та відео- зображення, що вказують на колабораційну діяльність.

Встановлення та огляд засобів масової інформації, веб-сторінок, груп та каналів у месенджерах, а також соціальних мережах, дозволить отримати фото та відео вчинення колабораційної діяльності, які у сукупності з показами свідків сформують доказову базу у вказаній категорії кримінальних проваджень.

Всі ці документи, як правило, зберігаються у цифрових форматах на різних електронних носіях. Електронний носій - матеріальний носій, який використовують для записування, зберігання та відтворення інформації, обробленої засобами комп'ютерної техніки.

Носіями можуть бути апаратні об’єкти, які містять: персональні комп’ютери (настільні, портативні), периферійні пристрої, мережеві апаратні засоби (сервери, робочі станції, активне обладнання, мережеві кабелі тощо), інтегровані системи (органайзери, мобільні телефони, планшети інші гаджети), вбудовані системи на основі мікропроцесорних контролерів, а також електронні носії даних: мікросхеми пам’яті, магнітні і лазерні диски, магнітооптичні диски, магнітні карти, флеш-пам’ять, цифрові фото/відеокамери, роутери, пластикові картки тощо.

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

Основними доказами у вказаній категорії кримінальних проваджень переважно є електронні (цифрові) докази.

Електронні докази — це докази у кримінальних провадженнях, які можна отримати в електронній формі. Електронні докази отримують за допомогою електронних пристроїв, комп'ютерних носіїв інформації, а також комп'ютерних мереж, у тому числі через мережу Інтернет. Вони стають

доступними для сприйняття людиною після обробки засобами комп'ютерної техніки. Разом із поняттям «електронні докази» (electronicevidence), часто застосовують поняття «цифрові докази» (digitalevidence). Оскільки на законодавчому рівні ці поняття ще не окреслені, їх використовують паралельно. Інформація, подана у формі, придатній для її оброблення електронними засобами, відповідно до Закону України «Про електронні документи та електронний документообіг» називається даними.

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

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

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

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

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

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

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

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

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

– системне програмне забезпечення;

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

До інформаційних об’єктів (даних) віднесені: текстові і графічні документи; дані у форматах мультимедіа; інформація у форматах баз даних та інші додатки прикладного характеру.

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

Існують зовнішні та внутрішні накопичувачі інформації, а також змінні носії (CD, DVD-диски) та різноманітні USB-накопичувачі.

У цифрових камерах та мобільних телефонах широко використовуються невеликі за розмірами карти пам’яті (SD, micro SD, compact Flash CF тощо), які можуть містити значний обсяг інформації.

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

Крім того, інформацію про факти та обставини, що мають значення для кримінального провадження, можуть містити системи відеоспостереження. Слід зазначити, що в багатьох IP-камерах можуть бути накопичувачі інформації, що дають змогу здійснювати відеофіксацію та зберігати відеоматеріал без підключення до реєстратора.

Відповідно до вимог ст. 168 КПК України тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв’язку для вивчення фізичних властивостей, які мають значення для

кримінального провадження, здійснюється лише у разі, якщо вони безпосередньо зазначені в ухвалі суду. Забороняється тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків, коли їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження, або якщо такі об'єкти отримані в результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення, а також якщо доступ до них обмежується їх власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту. Слід зазначити, що відповідно до п. 4 ст. 99 КПК України копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа. Тому відповідно до вимог ст. 168 КПК України в разі необхідності слідчий чи прокурор здійснює копіювання інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційнотелекомунікаційних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста.

2.4. Основні правила отримання цифрових доказів.

Сьогодні важливим інструментом фіксування інформації з Інтернет-ресурсів - відкритих джерел є Протокол Берклі - практичний посібник з використання цифрової інформації з відкритим вихідним кодом при розслідуванні порушень міжнародного кримінального права, права людини та гуманітарного права, розроблений школою права Університету Каліфорнії в Берклі разом з представниками ООН. У ньому містяться керівні положення щодо міжнародних стандартів для проведення інтернет-розслідувань передбачуваних порушень, керівництво про методи та процедури для збирання, аналізу та зберігання цифрової інформації з дотриманням професійних, правових та етичних принципів. Відповідно до нього з метою правильного

збору та збереження отриманих даних і недопущення видалення інформації з мережі Інтернет розроблений відповідний алгоритм, який у тому числі передбачає архівізацію, опис у протоколі огляду процесу отримання та змісту інформації, графічну візуалізацію та вимоги щодо збереження на відповідному носії.

Протокол покликаний допомогти слідчим, що ведуть розслідування з використанням даних у відкритому доступі, виконувати свою роботу відповідно до професійної методології, яка в цілому відповідає юридичним вимогам та етичним нормам. Він також має на меті допомогти різним кінцевим користувачам процесу розслідування, включаючи адвокатів, суддів та інших осіб, які приймають рішення, краще зрозуміти та оцінити методи розслідування з використанням даних у відкритому доступі. Протокол однаково призначений як ресурс для досвідчених практиків та інструмент навчання та підготовки для тих, хто хоче навчитися проводити розслідування з використанням даних у відкритому доступі щодо передбачуваних порушень міжнародного права

Механізм перевірки та оцінки доказів, отриманих під час огляду комп'ютерних даних також має комплексну структуру. Особистість, інформація щодо якої виявлена під час таких оглядів може ідентифікуватися шляхом пред'явлення для впізнання, пред'явлення для впізнання за фотознімками (за відсутності такої особи, що досить поширено у провадженнях в умовах надзвичайних правових режимів та тимчасово окупованих територій); проведенням судової портретної експертизи за експертною спеціальністю 6.2 (ідентифікація особи за ознаками зовнішності за матеріальними зображеннями); проведенням судової експертизи матеріалів і засобів відео-звукозапису (фоноскопічної) експертизи та ін.

Огляд комп'ютерних даних надає можливість встановлення не тільки особи підозрюваного (обвинуваченого) та його причетності до кримінального правопорушення, але й часто є джерелом відомостей про раніше не виявлені та не зареєстровані кримінальне правопорушення. Крім того, у контексті подій, які відбуваються, необхідним є проведення лінгвістичних експертиз

(проведення семантичних досліджень усного мовлення, під час вирішуються питання, пов’язані з аналізом змісту мовлення особи (розмови)), що здебільшого проводяться саме за відомостями, отриманими з Інтернет-ресурсів. Попри те, що він зосереджений на використанні цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права, він цілком є застосовним до використання при розслідуванні інших порушень, у т. ч. колаборційної діяльності.

Крім того, докази з відкритих джерел можуть допомогти слідчим отримати більш ширше уявлення про події з різних точок зору від різних суб’єктів; можуть надати слідчим доступ до подій на територіях, які недоступні для розслідування або в доступі до котрих їм було відмовлено і саме вони допоможуть у розслідуванні воєнних злочинів, вчинених Росією на території України, оскільки дозволяє сотням правозахисникам/цям фіксувати докази вчинення злочинів за допомогою камер, телефонів, доступу до Інтернету.

Іншим документом, що регламентує порядок отримання цифрової інформації є національний стандарт ДСТУ ISO/IEC 27037:201_ (ISO/IEC 27037:2012) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів».

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 їх припустимість у законодавчих та дисциплінарних судових процесах, а також інших потрібних інстанціях. Цей стандарт також надає загальні настанови стосовно збирання нецифрових доказів, які можуть буті корисними на стадії аналізу потенційних цифрових доказів.

Цей стандарт також спрямований 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, які розглядаються 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 у 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 при обробленні потенційних цифрових доказів, які знаходяться поза межами сфери ідентифікації, збирання, здобуття та збереження.

Хоча цей стандарт не охоплює судову готовність, адекватна судова готовність може бути значною мірою підтримана процесами ідентифікації, збирання, здобуття та збереження цифрових доказів. Судова готовність – це досягнення відповідного рівню здатності організації для спроможності ідентифікації, збирання, здобуття, збереження, захисту та аналізу цифрових доказів. Незважаючи на те, що процеси та діяльності, описані в цьому стандарті, є в основному реактивними заходами, які використовують у 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 безпеки стосовно потенційних цифрових доказів за допомогою надання додаткової настанови щодо запровадження. До того ж, цей стандарт

має застосування в контексті незалежному від ISO/IEC 27001 та ISO/IEC 27002. Цей стандарт повинен розглядатися разом з іншими стандартами, пов’язаними з цифровими доказами та розслідуваннями інцидентів інформаційної безпеки. (Основні вимоги стандарту викладені у додатку 1).

2.5. Основні дії спеціаліста при збиранні цифрових доказів.

На підготовчому етапі до проведення слідчої (розшукової) дії спеціаліст повинен з’ясувати:

Яке комп’ютерне обладнання (пристрої) та програмне забезпечення може бути на місці проведення слідчої (розшукової) дії?

– Хто відповідає за обладнання (системний адміністратор)?

– Яка кількість обладнання може бути виявлена?

– Який обсяг даних потрібно буде скопіювати?

– Чи існують резервні копії даних та де вони зберігаються

На початковій стадії збирання цифрових доказів необхідно:

1. Після прибуття на місце проведення слідчої (розшукової) дії заборонити всім особам, що знаходиться в приміщенні, доторкатися до комп'ютерів, електронних носіїв, включати і виключати апаратуру та енергоживлення. Будь-які спроби здійснити які-небудь дії з комп'ютером чи підключеними до нього пристроями можуть бути розцінені як спроба знищення доказів, що варто відобразити в протоколі. Проблема полягає в тому, що на комп'ютері, який працює, багато процесів відбуваються в його короткостроковій пам'яті – оперативній пам'яті. У наші дні це цілком нормально для звичайного пристрою мати оперативну пам'ять 8 Гб. Розмір для ігрових комп'ютерів, зазвичай, становить 8-32 Гб, а оперативна пам'ять у спеціалізованих пристроях може бути ще більшою (наприклад, для тих, які призначені для редагування медіа). Вся ця потенційна інформація буде втрачена під час знеструмлення. Після вимкнення, комп'ютер «втратить» усі

незбережені документи та будь-який доступ до файлів або «послуг» у хмарних сховищах.

2. Зробити оглядову фото і відеозйомку приміщення, де знаходяться об’єкти з ймовірними цифровими доказами і додаткового обладнання, що знаходиться в ньому, до того як приступити до слідчої (розшукової) дії. Під час проведення слідчої дії також фіксують апаратні об’єкти, які містять: персональні комп’ютери (настільні, портативні), периферійні пристрої, мережеві апаратні засоби (сервери, робочі станції, активне обладнання, мережеві кабелі тощо), інтегровані системи (органайзери, мобільні телефони, інші гаджети), вбудовані системи на основі мікропроцесорних контролерів, а також електронні носії даних: мікросхеми пам’яті, магнітні і лазерні диски, магнітооптичні диски, магнітні карти, флеш-пам’ять, пластикові картки тощо.

Вживши першочергових заходів безпосередньо біля об’єкта, що цікавить слідство, необхідно (за необхідності) оглянути всі приміщення та/або їх частини, де планується проведення слідчої (розшукової) дії, на предмет наявності в них будь-яких інших осіб з метою недопущення видалення останніми будь-якої інформації з пам’яті комп’ютера, знищення ними з’ємних носіїв інформації, знищення будь-яких інших предметів або документів, які планується відшукати. Потрібно також зважати на те, що існує можливість включити до складу програмного забезпечення комп’ютера програму, яка періодично вимагає введення паролю, і, якщо декілька секунд правильний пароль не буде введений, дані в комп’ютері можуть автоматично знищуватись або зашифровуватись.

3. Разом із слідчим визначити обсяг майбутніх слідчих (розшукових) дій.

4. Вжити додаткових заходів по забезпеченню схоронності інформації, в цих цілях слід:

- вирішити питання (за необхідності) про від'єднання системи від мереж і модемів, щоб ніхто не міг стерти чи змінити інформацію з використанням комп'ютерного обладнання поза приміщенням,

- заздалегідь, по можливості, визначити ділянки комп'ютерної мережі, де можуть бути виявлені електронні докази, і взяти їх під контроль.

Сьогодні значна кількість інформації зберігається у «хмарних сховищах», тобто розміщена поза місцезнаходженням фізичної чи юридичної особи. Тому присутні під час слідчої (розшукової) дії особи можуть використати наявні в них різноманітні гаджети, у тому числі мобільні телефони, для вчинення будь-яких дій з метою пошкодження, знищення, перетворення інформації, яка фактично може перебувати на відстані (навіть у межах приміщення, де відбувається слідча (розшукова) дія, тощо). З огляду на це доцільно усім присутнім при проведенні слідчої (розшукової) дії, на початку повідомити про заборону використання під час її проведення мобільних телефонів чи інших електронних пристроїв, які знаходять у них, та покласти їх на місце, доступне для поля зору слідчого, оперативного працівника, понятих, для здійснення контролю за невикористанням зазначених речей під час проведення обшуку.

Для проведення слідчої (розшукової) дії, за можливості, необхідно залучити працівників як Департаменту кіберполіції, як спеціалістів. Спеціаліст повідомляє слідчого, учасників слідчої (розшукової) дії, понятих та присутніх про копіювання (знаття так званого дампу) оперативної пам’яті, браузера з історією, логінами, паролями, копіювання файлів месенджерів та даних щодо відомих мереж, до яких здійснювалося підключення, і паролів до них. Після цього з дозволу слідчого здійснюється таке копіювання. При цьому спеціаліст повідомляє присутнім та учасникам слідчої (розшукової) дії про інформацію, яка підлягає копіюванню, її місцезнаходження на носії інформації, програмне забезпечення, за допомогою якою здійснюється таке копіювання, із зазначенням умов його ліцензування, зовнішнього носія інформації, на який здійснюється.

При працюючому комп'ютері необхідно:

- провести огляд (виїмку) комп'ютерних даних у режимі реального часу. Перш за все потрібно не дати можливості його заблокувати або вимкнути чи зашифрувати.

- визначити, яка програма використовується на початку слідчої (розшукової) дії. При виявленні працюючої програми по знищенню інформації зупинити її;

- встановити в комп'ютері наявність зовнішніх пристроїв - нагромаджувачів інформації на твердих дисках (вінчестері), а також зовнішніх пристроїв вилученого доступу до системи (підключення до локальної мережі, наявність модемів);

- відключити від мережі комп'ютер і виключити модем.

При непрацюючому комп'ютері необхідно:

- зафіксувати в протоколі, місцезнаходження зацікавленого слідство комп'ютера і його периферійних пристроїв, указавши кожен пристрій (назва, серійний номер, комплектація: наявність і тип дисководів, мережних карт та ін.), наявність з'єднання з локальною мережею чи мережами телекомунікації, стан пристроїв;

- зафіксувати порядок з'єднання між собою зазначених пристроїв;

- встановити, чи потрібен пароль для доступу до електронної інформації.

У разі, коли екран пристрою заблоковано, за можливості слід з’ясувати пароль користувача, а також встановити, чи увімкнене шифрування диска. Якщо пароль доступу не надається та є впевненість у тому, що шифрування диска не застосовується, а присутнє лише блокування екрана, то слідчий доручає спеціалісту перезавантажити ПК та завантажитись у Live-режимі з будь-якого Linux-дистрибутиву, який після завершення завантаження надасть змогу переглядати та копіювати усю файлову систему даного ПК за допомогою провідника. Якщо пароль доступу не надається та застосовується шифрування диска, то слідчий доручає спеціалісту виготовити дамп оперативної пам’яті з метою відшукування паролів, що зберігаються у ній, до моменту вимикання. Для здійснення зазначеного можуть бути застосовані або спеціалізовані апаратно-програмні засоби, наприклад, акселератор Tableau TACC1441, або окремі багатофункціональні та спеціалізовані програмні пакети й утиліти.

2.6. Основні правила вилучення комп'ютерної техніки.

Порядок тимчасового вилучення майна визначено в главі 16 КПК. Тому важливо дотримуватися цих вимог, щоб уникнути в подальшому невизнання судом, як доказів, вилучених об'єктів.

Так, ч.2 ст. 168 КПУ України визначено, що забороняється тимчасове вилучення електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків, коли їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження, або якщо такі об'єкти отримані в результаті вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення, а також якщо доступ до них обмежується їх власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту.

Таким чином, у разі, *якщо система вимагає введення паролю доступу, це може бути підставою для вилучення відповідного електронного носія інформації*. *Крім того, неповідомлення* паролів власником, володільцем або утримувачем *є формою обмеження доступу до інформації.* А це є додатковим аргументом на користь прийняття рішення щодо вилучення інформаційно-телекомунікаційних систем, їхніх невід'ємних частинах.

Важливим елементом процесу аналізу обстановки на місці проведення слідчої (розшукової) дії є можливість проведення експрес-пошуку інформації**,** як форми огляду документів під час слідчої дії. Важливо зауважити, що експрес-пошук не дозволяє проаналізувати значну частину видалених файлів, а також зашифровані та заблоковані дані, однак така дія надає можливість визначитися з наступними рішеннями при проведенні слідчої (розшукової) дії .

Технічна неможливість копіювання електронної інформації є достатнім обґрунтуванням необхідності подальшого експертного дослідження. Варто додати, що у випадку, коли з технічних причин неможливо скопіювати електронну інформацію з об'єктів, що не вказані в ухвалі слідчого судді, слідчий, прокурор можуть їх тимчасово вилучити в порядку, визначеному ч. 7

ст. 236 КПК України (як речі, що мають важливе значення для кримінального провадження). При цьому у протоколі мають бути зафіксовані виявлені відомості, що можуть бути використані як доказ факту чи обставин, які встановлюються під час кримінального провадження, а метою вилучення, за таких умов, - є забезпечення збереження цілісності інформації на електронному носії, а не вивчення фізичних властивостей, оскільки такі властивості в достатньому обсязі вивчені до ухвалення рішення про вилучення носія (абз. 2 ч. 2 ст. 168 КПК України).

Оптимальний варіант вилучення комп’ютерної техніки і машинних носіїв інформації - це фіксація їх на місці виявлення і пакування таким чином, щоб апаратуру можна було б успішно, правильно і точно, так само, як на місці виявлення, з'єднати в лабораторних умовах або в місці проведення слідства з участю фахівців.

Після того, як всі зацікавлені об’єкти оглянуто і зафіксовано у протоколі, їх необхідно упакувати і опечатати. При розбиранні обладнання треба відмічати (маркувати) обидва кінці кабелів. Якщо комп'ютер приєднано до телефонної мережі, з'ясовується: чи підключений комп'ютер до неї за допомогою модему. Якщо це телефонний роз'єм, необхідно відключити його. Якщо він підключений через модем, то вимикається напруга даного пристрою (не комп'ютера), в протокол записується номер використаного при з'єднанні телефону.

Потім вимикається монітор, процесор та відключається напруга. При цьому в протоколі слідчої дії та додатку-схемі до нього ретельно фіксується місцезнаходження ПК і його периферійних приладів, описується порядок з'єднання між собою вказаних приладів, із зазначенням особливостей (колір, кількість з'єднувальних роз'ємів, їх специфікація) з'єднувальних проводів і кабелів; перед роз'єднанням корисно здійснити відеозапис чи фотографування місць з'єднань.

Під час вилучення комп’ютерів їх слід упаковувати в полімерні пакети, де горловина пакета міцно обв’язується шовковою (капроновою)

ниткою і фіксується двома подвійними простими вузлами. Вузли розміщують на діаметрально протилежних сторонах, на які клеється бирка, що містить написи з назвою та характерними особливостями предмета (номер, марка, тип та ін.), що надається, номером кримінального провадження, фабулою події або прізвищем особи, в якої вилучений предмет, місцем (або адресою), датою і часом вилучення, посадою, прізвищем, ім’ям та по батькові, особистим підписом слідчого та прізвищами, іменами та по батькові, особистими підписами понятих, присутніх під час вилучення і пакування, скріпленими печаткою.

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

Слід пронумерувати всі носії інформації, а також пакети, в які вони запаковані, проставити відповідні знаки на паперових аналогах інформації. При складанні протоколу у ньому слід вказувати серійні номери всіх вилучених блоків та їх балансові номери (за відповідною документацією бухгалтерії підприємства, установи, якщо вона наявна). Якщо номери повністю відсутні, треба докладно описати кожний блок відповідно до його індивідуальних ознак.

Для вилучення носіїв їх необхідно упакувати у жорстку негнучку коробку та опечатати її. Усі з’єднання сторін (клапанів) коробів повинні бути обклеєні паперовою стрічкою клейовим способом та скріплені печаткою. У певних випадках можна використовувати й полімерні пакети, але з огляду на можливість несанкціонованого розрізання пакета за донну частину та потім заварювання його наново, у цьому разі необхідно обов'язково прошивати не тільки саму лише горловину пакета, а й донну його частину. Далі слід зробити на окремому аркуші паперу докладний опис упакованих носіїв (тип кожного з них, їх кількість).

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

діаметрально протилежних сторонах. Кожна упаковка повинна опечатуватися биркою, посвідченою написами з назвою та характерними особливостями предмета (номер, марка, тип та ін.), що надається, номером кримінального провадження, фабулою події або прізвищем особи, в якої вилучений предмет, місцем (або адресою), датою і часом вилучення, посадою, прізвищем, ім'ям та по батькові, особистим підписом слідчого та прізвищами, іменами та по батькові, особистими підписами понятих, присутніх під час вилучення і пакування, скріпленими печаткою

В окремих випадках, коли необхідно більш детально дослідити пристрої аудіо-, відео-, фотофіксації, спеціалізовані комп'ютери з нестандартним обладнанням (з платами шифрування, застарілими контролерами тощо), пристрої вводу-виводу інформації та ін., слід також вилучати дане обладнання.

Вилучення комп'ютерних засобів повинно проводитись в один прийом.

При перевезенні комп'ютерних засобів необхідно унеможливити їх механічні пошкодження і взаємодію з хімічно активними речовинами. Слід екранувати від впливу магнітних полів як комп'ютерні пристрої, так і магнітні носії. Такий вплив може призвести до пошкодження чи знищення інформації шляхом розмагнічування. За відсутності автотранспорту слід організувати надійну охорону вилученого обладнання у спеціальному приміщенні. При розміщенні вилучених об'єктів на зберігання слід дотримуватися встановлених правил зберігання і складування електронних технічних засобів. Не можна ставити системні блоки у штабель вище трьох штук, а також розміщати на них будь-які інші предмети. Зберігають комп'ютери і комплектуючі у сухому, теплому приміщенні. Слід довідатися, що у ньому немає мишей чи пацюків, які часто є причиною несправності апаратури. Крім того, категорично забороняється палити, приймати їжу і утримувати тварин у приміщеннях, призначених для зберігання комп'ютерної техніки і магнітних носіїв.

2.7. Особливості вилучення мобільних пристроїв

Вилучення мобільних пристроїв iOS Apple (iPhone, iPad, iPod). Необхідно намагатися вилучити мобільний пристрій не в заблокованому вигляді або під час виконання власником мобільного пристрою лише вихідного дзвінка. Під час *вилучення мобільного пристрою в незаблокованому стані* спеціалістом слідчий зазначає у протоколі слідчої (розшукової) дії спосіб вилучення мобільного пристрою, його місцезнаходження, потім за участю спеціаліста зазначає:

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

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

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

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

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

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

– якщо увімкнути режим «політ» та вимкнути WiFi і Bluetooth не вдається, здійснюють відповідний запис у протоколі. У цьому разі доручають

спеціалісту загорнути пристрій у шість шарів харчової фольги та під'єднати до джерела живлення (мобільна батарея тощо) для уникнення його вимкнення, про що зазначають в протоколі з описом часу виконання таких дій;

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

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

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

– спеціаліста, якому доручено здійснення копіювання інформації;

– програмне забезпечення, яке використовуватиметься для копіювання інформації;

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

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

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

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

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

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

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

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

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

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

У разі наявності такої інформації спеціаліст повідомляє про це всіх учасників слідчої дії та понятих, після чого, за дорученням слідчого здійснює копіювання наявної інформації, про що повідомляє всіх учасників, зокрема про наявність відповідної інформації, місця (адреси) її зберігання на персональному

комп’ютері; програмного забезпечення, за допомогою якого здійснюватиметься копіювання; з’ємний носій електронної інформації, на який здійснюватиметься копіювання (його серійний або ідентифікаційний чи інвентарний номер).

Після завершення копіювання спеціаліст демонструє учасникам обшуку та понятим факт збереженості скопійованої інформації на зовнішньому носії інформації, повідомляє про її обсяг, назви файлів, які були скопійовані. Після цього здійснюють від’єднання зовнішнього носія інформації з персонального комп’ютера, його упакування та опечатування паперовою биркою з написом про персональний комп’ютер, з якого було здійснено копіювання інформації, короткий опис скопійованої інформації, серійний номер з’ємного носія інформації, підпис особи, якій належить персональний комп’ютер, підпис працівника кіберполіції, підписи понятих. Про все це роблять запис у протоколі.

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

Усі ці відомості підлягають обов’язковому занесенню до протоколу обшуку. **Вилучені мобільні пристрої** (телефони, планшетні комп’ютери, GPS-навігатори, smart-годинники, портативні відеореєстратори тощо) **упаковуються в окремі непрозорі пакети**, що унеможливлює увімкнення пристрою в упаковці.

Потім здійснюється їх опечатування биркою із зазначенням підписів: особи, в якої вилучається така інформація, працівника кіберполіції, який здійснив таке копіювання та понятих.

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

Спосіб упакування повинен забезпечувати неможливість несанкціонованого доступу до них, підміни або зміни об’єктів дослідження, носіїв з об'єктами дослідження, зберігання від пошкодження, псування,

погіршення або втрати властивостей, завдяки яким вони мають доказове значення.

Носії інформації окремо упаковуються і помішуються в оболонки, які не несуть заряду статичної електрики.

Неприпустимо приклеювати будь-що безпосередньо на магнітний носій, пропускати через нього нитку, пробивати отвори, робити надписи, помітки, ставити печатки тощо. Усе вилучене необхідно якомога швидше передати у розпорядження експерта або фахівця для подальшого вивчення.

Застосовуючи специфічні методи під час проведення слідчої (розшукової) дії, слід за можливості збирати і традиційні докази: відбитки пальців рук, паперові документи (накази, листівки, брошури тощо).

Згідно ст. 99 КПК України документом є спеціально створений з метою збереження інформації матеріальний об’єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження.

Огляд документів полягає у їх вивченні та дослідженні з метою виявлення та фіксації ознак, що надають документам значення речових доказів.

При детальному огляді та подальшому вилученні паперового документа не можна використовувати такі технічні засоби, прийоми і методи, які можуть його пошкодити або змінити. Рекомендується поводитись з документами так, щоб не знищити сліди правопорушника і не залишити свої.

Згинати документи можна тільки по старим складкам, не можна підкреслювати або обводити окремі місця в тексті.

Іншими словами, огляд залежить від того, чи буде документ мати у справі значення речового доказу, чи матиме значення документа.

Коли документ буде власне документом як джерелом доказів, тоді слідчого цікавить лише його зміст і до справи він може не долучатися (наприклад, бухгалтерська книга із записом, що мас значення для розслідування справи).

У такому разі в протоколі, після загального описання документа, відображаються обставини, що мають значення для справи.

Загальний опис – це:

- що являє собою документ, якого оглядають;
- у кого і де він зберігався;
- походження документа, від кого він надійшов або як опинився у справі.

Якщо документ має значення речового доказу, він цікавить слідчого сам собою цілком і є незамінним.

Під час опису документа – речового доказу з'ясовуються й описуються:

– найменування документа;
– призначення;
– зовнішній вигляд;
– всі наявні реквізити;
– ознаки підроблення (якщо такі є).

У ході огляду використовуються необхідні технічні засоби, допомога спеціалістів.

У будь-якому випадку документ фотографується.

Документи недопустимо підшивати, робити на них певні замітки, додаткові перегини. Зазвичай документ вкладається в конверт, дещо більший за розміром, який своїм вільним краєм підшивається до справи.

РОЗДІЛ 3. ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ СУДОВИХ ЕКСПЕРТИЗ ПІД ЧАС РОЗСЛІДУВАННЯ КОЛАБОРАЦІЙНОЇ ДІЯЛЬНОСТІ.

Під час розслідування кримінальних правопорушень, пов'язаних із колабораційною діяльністю слід забезпечити доказування обставин, що свідчать про причетність до колабораційної діяльності та/або призначення на посади в незаконно створених органах влади на тимчасово окупованій території України, а також на підтвердження факту тимчасової окупації певної території України. Доказування обставин, що підлягають з'ясуванню під час

розслідування кримінальних правопорушень вимагає використання комплексу процесуальних засобів, зокрема й тих, що вимагають взаємодії з носіями спеціальних знань, тобто обізнаними особами. Найбільш поширеною формою застосування спеціальних знань під час розслідування кримінальних правопорушень, пов'язаних із колаборaційною діяльністю є залучення експерта до проведення судових експертиз. Згідно з проведеним аналізом вироків, опублікованих у Єдиному державному реєстрі судових рішень, найбільш поширеним і типовим для цієї категорії кримінальних правопорушень є проведення: почеркознавчої експертизи; лінгвістичної експертизи (семантико-текстуальної); комп'ютерно-технічної експертизи (експертизи комп'ютерної техніки і програмних продуктів); портретної експертизи; фототехнічної експертизи та ін. Такі види експертних досліджень характерні для цієї категорії кримінальних правопорушень у зв'язку з тим, що основними доказами у вказаній категорії кримінальних правопорушень переважно є електронні (цифрові) докази.

Цифровими доказами є матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані), що містяться у відкритих мережах (мережі Інтернет; різноманітних матеріалах засобів масової інформації; соціальних мережах), а також закритих мережах – на цифрових носіях інформації свідків (приватних месенджерах, телеграм-каналах; в особистому листуванні, що здійснюється із використанням комп'ютерної техніки, мобільних телефонів, зберігається на флеш-носіях, картах-пам'яті тощо).

Узагальнюючи слідчу, судову та експертну практику можемо зауважити, що типовими об'єктами судових експертиз у кримінальних правопорушеннях, пов'язаних із колаборaційною діяльністю, стають матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані), а саме: веб-сайти і сторінки соціальних мереж незаконно створених органів влади; відкриті телеграм канали; різноманітні матеріали, підготовлені засобами медіа, які утворені та працюють на тимчасово окупованій території

України та в державі-агресорі; веб-сайти та особисті сторінки в соціальних мережах волонтерів, журналістів, адвокатів, а також працівників органів державної влади України та місцевого самоврядування; відкриті телеграм канали; матеріали, підготовлені пресою зарубіжних країн, а також громадських організацій, які фіксують і висвітлюють воєнні злочини та злочини проти основ національної безпеки України, учинені на тимчасово окупованій території України, а також, котрі висвітлюють події на тимчасово окупованій території України; фото, відео, аудіо файли, створені потерпілими та свідками тощо.

Важливо, що дослідження цифрової інформації, котра зберігається на матеріальних носіях інформації, є насамперед те, що певна доказова інформація щодо події вчиненого кримінального правопорушення може міститися безпосередньо на ньому. Як правило, під час їх дослідження фактично проводиться аналіз і носія інформації і наявного на ньому зображення, відеозапису або звукозапису тощо, а також сліди, котрі містяться на самому носії, якщо ним є, наприклад, мобільний телефон, планшет, ноутбук.

Щодо експертизи цифрового файлу, то дослідженню підлягають сам файл (який містить текстову інформацію, аудіо- чи відео-), а також різноманітне програмне забезпечення, що використовується як «знаряддя» вчинення злочину чи задля приховання слідів його вчинення; файли, що містять сліди підробки чи фальсифікації; бази даних, вільний доступ до яких заборонено чинним законодавством у сфері охорони державної таємниці, захисту персональних даних тощо; скановані копії, фотокопії документів, обмежених для обігу тощо.

За результатами експертного дослідження окреслених об’єктів стає можливим отримання висновку експерта – самостійного процесуального джерела доказу. Тому важливо забезпечувати дотримання ряду правових та організаційних засад під час залучення експерта до проведення експертиз. Однією з таких особливостей є коректне обрання експертної установи, котрій буде доручено дослідження. За своїм родом усі окреслені експертні дослідження є різновидом криміналістичних експертиз. Згідно із Законом України «Про судову експертизу» виключно державними спеціалізованими

установами здійснюється судово-експертна діяльність, пов’язана з проведенням криміналістичних експертиз.

Таким чином, проведення типових експертиз у цій категорії кримінальних правопорушень повинно здійснюватися науково-дослідними та експертними службами Міністерства юстиції України, Міністерства внутрішніх справ України, Служби безпеки України, Міністерства оборони України та Державної прикордонної служби України. Саме за таких умов отримані висновки експерта будуть визнані належними доказами.

Особливе місце серед визначених судових експертиз і має свою специфіку, котру слід ураховувати при організації та плануванні розслідування кримінальних правопорушень, пов’язаних із колаборaційною діяльністю, займає комп’ютерно-технічна експертиза. Завдяки можливостям комп’ютерно-технічної експертизи можуть бути встановлені обставини, пов’язані з використанням ймовірним колаборантом комп’ютерно-технічних засобів, інформації та програмного забезпечення для розміщення в мережі Інтернет дописів щодо публічного заперечення здійснення збройної агресії проти України, установлення та утвердження тимчасової окупації частини території України або публічних заклики до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора тощо.

Об’єктами експертизи комп’ютерної техніки і програмних продуктів є мобільні телефони, планшети, комп’ютерна техніка. Електронні пристрої, вилучені у колаборантів слугують сховищем загальної і особистої інформації, відомостей щодо різного роду подій і явищ, дій окремих осіб, тощо. Завдяки тому, що сучасні мобільні телефони мають широкий набір функцій (здійснення і приймання дзвінків, телефонна книга, фото і відеокамера, диктофон, доступ до інтернету, створення і редагування текстових файлів і повідомлень, електронна пошта, соціальні мережі, месенджери і сервіси спілкування та ін.), вони

зберігають цифрові сліди користування цими функціями і слугують своєрідними архівами особистої інформації.

Окреслені різновиди інформації та способи її фіксації можуть бути включені до доказової бази лише за умови її виявлення, вилучення, дослідження і належного процесуального закріплення. Для якісного виконання цих завдань залучаються спеціалісти в ІТ-сфері, які за допомогою сучасних портативних апаратно-програмних комплексів «Cellebrite UFED Touch 2 Ultimate» та «Cellebrite UFED 4 PC Physical Analyzer» виявляють, декодують і аналізують цифрові дані, отримані з мобільних телефонів.

На вирішення експертизи комп'ютерної техніки і програмних продуктів при розслідуванні кримінальних правопорушень цього виду залежно від конкретних обставин, можуть бути поставлені такі типові питання: 1. Чи міститься на даному носії інформація щодо (зазначити, яка інформація цікавить) та у якому вигляді? 2. Чи містить носій досліджуваного комп'ютера інформацію про певні (зазначити, які саме) дії користувача? 3. Чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації? 4. Чи могла бути створена зазначена інформація на цьому комп'ютері чи вона перенесена з іншого носія? 5. Яким чином інформація (зазначити, яка саме) перенесена до досліджуваного комп'ютера (носія)? 6. Яка технологія та хронологія створення електронного документа (зазначити електронний документ та певний зміст)? 7. Які атрибути (час друку, редагування, створення, видалення тощо) файлів, що містять інформацію щодо певних відомостей?.

Ще один досить поширений різновид судових експертиз, який проводиться під час розслідування колаборaційної діяльності є лінгвістична експертиза мовлення. Різновидами судової лінгвістичної експертизи мовлення є семантико-текстуальна експертиза та авторознавча експертиза. Більш поширеним під час розслідування колаборaційної діяльності є проведення саме семантико-текстуальної експертизи.

Завданнями судової семантико-текстуальної експертизи в контексті з'ясування обставин державної зради є встановлення змісту понять або

висловлювань, лексичного значення слів або словосполучень, використаних у наданих на дослідження текстах або усних повідомленнях (за їх текстовими відтворенням), їх стилістичної забарвленості, смислового навантаження, характеру інформації, що міститься в них (заперечення здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України або публічні заклики до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора, до співпраці з державою агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, до невизнання поширення державного суверенітету України на тимчасово окуповані території України тощо), тобто вирішення питань мовленнєвого характеру, не пов’язаних зі встановленням фактичних даних про автора.

Об’єктами такого різновиду судової експертизи є мовлення особи, причому, як письмове, так і усне, що міститься на теноготах дописів у соціальних мережах, в аудіо та відоезаписах, у стенограмах висловлювань тощо. При цьому важливо звернути увагу на те, що висновок експерта, за результатами таких досліджень, є констатацією об’єктивного змісту тексту з позиції спеціальних знань у галузі експертних досліджень, а не правовою кваліфікацією діяння особи. Зокрема, у справі, котра розглянута Жовтоводським міським судом Дніпропетровської області проведено семантико-текстуальну експертизу писемного мовлення з метою підтвердження публічного заперечення здійснення збройної агресії проти України. Так, експертному аналізу підлягав коментар до публікації у соціальній мережі «Вконтакте». За результатами його дослідження експертом винесено категоричний висновок про те, що такий коментар за своїм семантико-текстуальним значенням є публічним запереченням збройної агресії проти України.

На вирішення семантико-текстуальної експертизи типовим є поставлення таких типових питань: Які значення мають слова, словосполучення, фрази, зафіксовані в досліджуваному тексті? Яким є об’єктивний зміст досліджуваного

словосполучення, речення, тексту, групи текстів? Чи містяться у тексті висловлювання, виражені у формі закликів до певних дій (вказати, яких саме)? Якщо так, то чи є ці заклики публічними (або який характер та форму мають ці заклики)? Чи міститься в тексті інформація позитивного або негативного характеру щодо певної фізичної або юридичної особи? Чи містяться в тексті висловлювання образливого характеру щодо певної особи? Чи є висловлювання фактичним твердженням або оціночним судженням?.

Судова авторознавча експертиза призначається за потреби дослідження різноманітних записів, текстів документів (виступів, офіційних документів, літературних творів, текстів публічних виступів тощо). Авторознавча експертиза виконує ідентифікаційні (щодо ототожнення особи автора тексту) та неідентифікаційні (діагностичні) завдання, що полягають у з'ясуванні умов складання тексту, фактів викривлення ознак писемного мовлення, місця формування мовленнєвих навичок, мови (рідної / нерідної), освіти автора документа.

У межах ідентифікаційних завдань установлюється авторство тексту стосовно конкретної людини, а також тотожність декількох анонімних текстів невідомого автора. До категорії класифікаційних завдань авторознавчої експертизи належать встановлення статі, віку, професійної належності, рівня освіти, рідної мови та місцевості, у якій проходило формування мовних навичок автора тексту. Діагностичні завдання пов'язуються з визначенням незвичного психофізіологічного стану автора тексту (сп'яніння, захворювання нервової системи, під впливом погроз тощо). Ситуаційні завдання мають комплексний характер і послідовно складаються з проміжних класифікаційних, діагностичних та ідентифікаційних завдань. Важливо, що вирішення питань, поставлених перед експертом, можливе за наявності обсягу досліджуваного тексту орієнтовно не менше ніж 100 слів. Під час підготовки матеріалів для проведення авторознавчої експертизи з метою встановлення авторства орган (особа), який (яка) призначив(ла) експертизу (залучив(ла) експерта),

повинен(на) зібрати вільні, умовно-вільні й експериментальні зразки писемного мовлення особи, яка підлягає ідентифікації.

Типовими запитаннями, що вирішуються експертами: «Чи є певна особа автором наданого на дослідження тексту? Чи є певна особа автором декількох різних текстів? Чи є автор та виконавець тексту однією або різними особами? Чи даний текст складений кількома авторами? Які риси соціально-біографічного портрета автора можна встановити за даним текстом? Якою є основна мова спілкування певної особи - автора даного тексту? Яким є місце формування мовленнєвих навичок (рідна мова) певної особи - автора даного тексту? Чи спостерігаються в тексті ознаки, які свідчать про складання тексту автором під впливом будь-яких збиваючих факторів? Чи складено текст документа особою самостійно або під диктування чи його виконано шляхом переписування? Чи складений текст документа з перекручуванням ознак писемного мовлення?».

Судова почеркознавча експертиза проводиться з метою встановлення виконавців рукописних текстів та підписів у документах, вилучених під час проведення слідчих (розшукових) дій на деокупованих територіях. Предметом дослідження є письмові тексти колаборантів, які можуть бути виявленні у так званих «виборчих комісій», у журналах та відомостях різного змісту, на актах, указах і розпорядженнях, інших «офіційних документах» органів окупаційної влади тощо. Так, окреслений різновид судової експертизи проводився у справі, котра розглядалася Червонозаводським районним судом м. Харкова, у якій встановлено, що громадянка Україна, перебуваючи на території м. Куп’янськ, Харківської області, реалізувала злочинний умисел, направлений на зайняття посади, пов’язаної з виконанням організаційно-розпорядчих функцій у незаконних органах влади, створених на тимчасово окупованій території Харківської області. Під час проведення почеркознавчої експертизи встановлено виконавця понад 40 підписів, а також чотири рукописних тексти, серед яких заява з проханням призначити на посаду та автобіографія тощо.

Орієнтовний перелік запитань, що може виноситися на розв'язання судового експерта, представлений, зокрема, такими питаннями: 1. Чи виконано рукописний текст (рукописні записи) у документі (назва документа та його реквізити, графа, рядок) певною особою? 2. Чи виконані рукописні тексти (рукописні записи) у документі (документах) (назва документа та його реквізити, графа, рядок) однією особою? 3. Чи виконано підпис від імені особи (прізвище, ім'я, по батькові особи, від імені якої зазначено підпис) у документі (назва документа та його реквізити, графа, рядок) тією особою, від імені якої він зазначений, чи іншою особою? 4. Чи виконано рукописний текст у документі (назва документа та його реквізити, графа, рядок) під впливом збиваючих факторів (природних, штучних)? 5. Чи виконано підпис від імені особи (прізвище, ім'я, по батькові особи, від імені якої зазначено підпис) у документі (назва документа та його реквізити, графа, рядок) під впливом збиваючих факторів (природних, штучних)? 6. Особою якої статі виконано рукописний текст? 7. До якої групи за віком належить виконавець рукописного тексту?

Обов'язковими умовами, яких слід дотримуватися для забезпечення вирішення ідентифікаційних, діагностичних завдань цього виду експертного дослідження на етапі підготовки до призначення судової почеркознавчої експертизи, є: 1) направлення на дослідження оригіналів документів; 2) додержання правил відібрання експериментальних зразків почерку, а також отримання умовно-вільних і вільних порівняльних зразків у достатній кількості та необхідної якості, безсумнівного походження; 3) направлення на дослідження експерта разом із об'єктами дослідження ще й інформації про стан здоров'я виконавця підпису, записів, тексту тощо; відомостей про безпосередні умови виконання досліджуваного документа; 4) чітке, коректне й однозначне формулювання запитань, котрі виносяться на вирішення експерта та ін..

Вагомим значенням у вирішенні завдань, пов'язаних із підтвердженням колаборційної діяльності відіграє портретна експертиза. Основним завданням судової портретної експертизи є ідентифікація особи (трупа) за фотознімками

та відеозаписами. Портретна експертиза, зокрема, проводилася у справі, котра розглядалася у зв'язку із учиненням громадянкою України колаборційної діяльності. Відповідно до висновку експерта Харківського науково-дослідного експертно-криміналістичного центру МВС України №СЕ-19/121-23/6989-ФП від 18.04.2023, убачається наступне, що зображення особи жіночої статі, зафіксовані на кадрах чотирьох різних відеофонограм і зображення особи на ім'я ОСОБА_30 , ІНФОРМАЦІЯ_2 , зафіксовані на фото з файлів «Огляд особової справи ОСОБА_3 сторінки 1 та 6 відповідно до опису.pdf», – належать одній і тій самій особі». Тобто на портретну експертизу можуть бути направлені і фотозображення, і відеофайли.

Об'єктами судової портретної експертизи у кримінальних провадженнях за фактами колаборційної діяльності найчастіше є фотознімки з ворожих інтернет-ресурсів з публікаціями про діяння, що підпадають під ознаки колабораціонізму, та фрагменти відеозаписів із зображеннями підозрюваних осіб, на яких зафіксована їхня протиправна діяльність. Портретна експертиза найчастіше призначається під час розслідування діянь, що були вчинені на тимчасово окупованих територіях, з метою встановлення особи колабораціоніста за ознаками зовнішності. Як порівняльні матеріали в розпорядження експерта подаються фотознімки чи відеозаписи із зображенням достовірно встановлених осіб. Такі фотознімки можна отримати шляхом витребування відповідних документів від українських органів влади чи місцевого самоврядування. Найчастіше, це особова картка громадянина з державної міграційної служби. Відеозаписи, із зображенням певної особи, яка цікавить слідство, можна віднайти на інтернет-ресурсах, якщо ця особа брала участь у якихось передачах на українських теле- чи інтернет-каналах до переходу на бік ворога і ведучий її представляв. У разі вилучення в підозрюваного документів на його ім'я, виданих органами влади України, наприклад, паспорта громадянина України, фотографія з нього також може бути надана експертові для проведення порівняльного дослідження. Важливо, щоб на дослідження судово-портретної експертизи, окрім об'єкта дослідження,

надавалися порівняльні матеріали (зразки для порівняльного дослідження) належної якості, котрі відповідають вимогам достовірності, зіставлення і повноти.

Судова експертиза відео-, звукозапису під час розслідування колабораційної діяльності може проводитися у випадках, коли виникає потреба з'ясування технічних умов і технології отримання відео, звукозапису й ототожнення особи за фізичними параметрами голосу.

Технічна експертиза документів, проводиться з метою встановлення способу та відносної давності виготовлення документу, способу нанесення відтиску печатки чи штампа тощо. Так, при проведенні слідчих (розшукових) дій на деокупованих територіях можуть бути вилучені «документи», видані незаконними органами влади, створеними на тимчасово окупованій території, у тому числі окупаційними адміністраціями держави-агресора. Це можуть бути паспорти громадянина росії чи, так званих, «лнр», «днр», технічні паспорти на автотранспортні засоби, водійські посвідчення, так звані, «виборчі бюлетені», різні довідки з відтисками печаток і штампів, кліше печаток і штампів тощо. У таких випадках може виникнути необхідність встановлення способу нанесення відтиску печатки чи штампа, способу та відносної давності виготовлення документу тощо. З цією метою має призначатися саме технічна експертиза документів, яка поділяється на експертизу реквізитів документів, експертизу друкарських форм та експертизу матеріалів документів і має свою специфіку, яку потрібно враховувати.

Ситуаційно, залежно від обставин конкретного кримінального провадження за фактами колабораційної діяльності, можуть призначатися трасологічна, психолого-лінгвістична, психіатрична та інші види судових експертиз, результати досліджень яких можуть бути використані для проведення всебічного і об'єктивного розслідування таких кримінальних правопорушень і належними чином забезпечити ефективність судового розгляду.

Також наразі розповсюдженими є випадки фіксації воєнних злочинів, а також злочинів проти основ національної безпеки (державної зради, колабораційної діяльності) громадськими організаціями, волонтерськими рухами, приватними особами, журналістами, у яких можуть зберігатися відповідні відомості та докази. Крім того, певні докази такої діяльності можуть бути у представників органів державної влади, місцевого самоврядування, різних підприємств, установ та організацій, які виїхали з тимчасово окупованої території України. Установлення таких організацій, рухів, осіб, та журналістів можливе шляхом витребування відомостей в органах державної влади та місцевого самоврядування, що дозволить отримати документи, які підтверджують факт колабораційної діяльності та проведення вже слідчим огляду відповідних джерел інформації.

З метою забезпечення доступності інформації у відкритих джерелах, як визначено Офісом Генерального прокурора, слід використовувати Протокол Берклі. Задля виконання таких завдань може бути залучено відповідних фахівців у галузях комп'ютерної техніки, комп'ютерної інженерії тощо, зокрема, для проведення огляду комп'ютерних даних та інших процесуальних дій. Такі заходи є перспективними у розслідуванні колабораційної діяльності з огляду на те, що отримана цифрова копія документа з мережі Інтернет прирівнюється до оригіналу.

Отже, під час розслідування колабораційної діяльності важливе значення відіграє залучення обізнаних осіб до участі в кримінальному провадженні. Доказовим потенціалом наділені безумовно процесуальні форми використання спеціальних знань, такі як: залучення експерта до проведення експертизи та участь спеціаліста в слідчих (розшукових) і негласних слідчих (розшукових) діях. Нехтувати перспективами означених форм не можна, через можливість втрати доказового потенціалу окремими матеріальними і цифровими об'єктами, тому важливо своєчасно проводити заходи як щодо збору порівняльних зразків для експертного дослідження, так і направлення їх на кваліфіковане дослідження.

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 зустрічаються у процесі оброблення цифрових доказів, та допомагає організаціям в їх дисциплінарних процедурах та забезпеченні обміну потенційними цифровими доказами між юрисдикціями.

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

- Носій для зберігання цифрових даних, який використовують 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 основані на TCP/IP та інших цифрових протоколах, а також
- Прилади з функціями, подібними наведеним вище.

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

Примітка 2. Наведені вище пристрої можуть бути запроваджені різними способами. Наприклад, автоматизована система може містити мобільну навігаційну систему, збереження даних та сенсорну систему.

НОРМАТИВНІ ПОСИЛАННЯ

Наведені нижче документи необхідні 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 managemen*t *systems – Overview and vocabulary*

ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

Для цілей цього документу вживаються терміни і визначення понять із ISO/IEC 27000, ISO/IEC 17020, ISO/IEC 17025 та ISO/TR 15801, а також нижченаведені.

3.1 здобуття (*acquisition*)

Процес створення копії даних в межах визначеного набору

Примітка. Результатом здобуття є копія потенційних цифрових доказів.

3.2 виділений простір (*allocated space*)

Ділянка цифрового середовищі, включаючи первинну пам'ять, яка використовується 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, яке використовується для оброблення або 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, яка запроваджується для підтримання надійності доказу за допомогою включення разом цифрового доказу та засобів верифікації, де спосіб верифікації може бути вбудованим або незалежним від інструментів, які використовуються під час здійснення верифікації

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

Особа, яка авторизована, 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 вимогам, які необхідні для здобуття надійних цифрових доказів, але індивідуальні обставини можуть призвести до того, що особа не відповідає усім трьом вимогам. У такому випадку, 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 у 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 зберігаютьдокази, що були зібрані або здобуті

Примітка. Пристрій для збереження доказів не повинен піддаватися впливу магнітних полів, пилу, вібраціям, вогкості або 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 дані, які були вилучені.

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 повторюваність (*repeatability*)

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

3.18 відтворюваність (*reproducibility*)

Властивість процесу отримувати однакові тестові результаті у різному тестовому середовище (різний комп'ютер, жорсткий диск, режим роботи тощо)

3.19 псування (*spoliation*)

Дія із здійснення або допущення внесення змін(и) до потенційних цифрових доказів, яка зменшує їх доказове значення

3.20 системний час (*system time*)

Час, який генерується системним годинником за допомогою операційної системи; це не час, який обчислюється 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 у часі відносно до загальної довідкової інформації про час

3.23 невиділений простір (*unallocated space*)

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

3.24 затвердження (*validation*)

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

[ISO/IEC 27004:2009]

3.25 функція верифікації (*verification function*)

Функція, яка використовується для підтвердження, що два набори даних є ідентичними

Примітка 1. Два неідентичних набори даних не повинні вважатися ідентичними після функції верифікації.

Примітка 2. Функції верифікації зазвичай застосовують з використанням геш функцій, таких як MD5, SHA1 тощо, але можуть використовуватися інші методи.

3.26 нестійкі дані (*volatile data*)

Дані, які специфічно схильні до змін та можуть бути легко модифіковані

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

ЗАГАЛЬНИЙ ОГЛЯД

Обставини для збирання цифрових доказів

Цифрові докази можуть бути потрібними для використання у низці окремих сценаріїв, кожний з яких має різний баланс між рушієм доказової якості, своєчасністю аналізу, 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, в якому потенційні цифрові докази повинні збиратися, здобуватися або зберігатися. Процес визначення пріоритетів здійснюється задля мінімізації ризику, що потенційні цифрові докази будуть псуватися, та доведення до максимуму доказового значення потенційних цифрових доказів, що були зібрані.

Принципи цифрових доказів

У більшості юрисдикцій та організацій цифрові докази базуються на трьох основних принципах: важливість, надійність та достатність. Ці три принципи є важливими в усіх розслідуваннях, але не тільки такі цифрові докази прийнятні у суді. Цифровий доказ є надійним, якщо він надає можливість засвідчувати або не засвідчувати елемент специфічного випадку, який розслідується. Хоча детальні визначення «надійність» відрізняються в різних юрисдикціях, основне значення цього принципу «гарантувати, що цифровий доказ є таким, яким він повинен бути» широко використовується. Не завжди потрібно для DEFR збирати усі дані або робити повну копію первісного цифрового доказу. В більшості юрисдикцій концепція достатності означає, що DEFR має зібрати достатню кількість потенційних цифрових доказів, щоб забезпечити можливість адекватної перевірки та дослідження елементів справи. Розуміння цієї концепції є важливим для DEFR для визначення пріоритетів зусиль правильно, коли 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, які використовують DEFR та DES, повинні бути затвердженими до їх використання. Якщо затвердження було зроблено в екстремальних умовах, DEFR та DES мають підтвердити, що затвердження є прийнятним для їх специфічного використання процесів та середовища і обставин, в яких ці процеси будуть використані. DEFR та DES повинні також:

a) документувати усі 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.

Вимоги щодо оброблення цифрових доказів.

Загальні положення

Принципи, що наведені вище в розділі 5.2, можна задовольнити таким чином:

- Важливість: Мається можливість показати, що здобуті матеріали є надійними для розслідування – тобто що вони містять величини, які допомагають в розслідуванні конкретного інциденту, та що існує доречна причина для їх здобуття. За допомогою аудиту та юрисдикції DEFR повинен мати можливість описати підтримані процедури та пояснити, як було прийнято рішення для здобуття кожного елементу.
- Надійність: Усі процеси, які були використані під час оброблення потенційних цифрових доказів, повинні піддаватися аудиту та бути повторюваними.
- Достатність: DEFR повинен приймати до уваги, що достатня кількість матеріалів повинна бути зібрана для того, щоб дозволити зробити належні дослідження. DEFR повинен мати можливість з використанням аудиту

та законодавства надати пояснення, яка кількість матеріалу, в цілому, була розглянута та які процедури були використані для вирішення питання, яка кількість та який матеріал був здобутий.

Примітка. Матеріали мають бути зібрані за допомогою дій зі здобуття та збирання.

Існує чотири ключових аспекти в обробленні цифрових доказів: можливість аудиту, відповідність юрисдикції та повторюваність або відтворюваність в залежності від конкретних обставин.

Можливість аудиту

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

Повторюваність

Повторюваність досягається коли ті самі результати отримуються за таких умов:

- Використання такої самої процедури та методики;
- Використання таких самих інструментів та за таких же умов; а також
- Може бути повторено в будь-який час після первісного тесту.

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

Відтворюваність

Відтворюваність досягається, коли ті самі результати тесту отримуються за таких умов:

- Використання такої самої методики вимірювань;
- Використання інших інструментів та за інших умов;
- Може бути відтворено в будь-який час після первісного тесту.

Потреба у відтворюванні результатів змінюється в залежності від юрисдикції та обставин, тому DEFR або особа, яка здійснює відтворювання, повинна бути поінформованою стосовно прийнятних умов.

Відповідність юрисдикції

DEFR повинен мати можливість доказати відповідність юрисдикції усіх дій та методів, які були застосовані під час оброблення потенційних цифрових доказів. Відповідність юрисдикції може бути досягнута демонстрацією того, що такі рішення є найкращим вибором для отримання усіх потенційних цифрових доказів. Інші DEFR або DES можуть також показати це за допомогою

успішного відтворювання або затвердження дій та методів, що використовувались.

В інтересах конкретної організації наймати DEFR або DES, які мають основні навички та компетенцію, як описано у Додатку А цього стандарту. Це буде гарантувати, що під час оброблення потенційних цифрових доказів будуть застосовуватися правильні процеси та процедури для забезпечення кінцевого збереження цифрових доказів, які можуть мати доказове значення. Це також гарантує, що організація буде мати можливість використання потенційних цифрових доказів, наприклад, в своїх дисциплінарних процедурах або сприяти обміну потенційними цифровими доказами між юрисдикціями.

Примітка Компетентність, описана у Додатку А, обмежена функціями DEFR, що сумісна з роллю DES, як визначено в розділі 3.8.

Процеси оброблення цифрових доказів

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 перевірки. Обробники цифрових доказів мають бути компетентними стосовно ідентифікації та управління ризиками і послідовності потенційних напрямів дій, коли мають справу з 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 повинні містити настанови щодо оброблення джерел потенційних цифрових доказів та базуватися на таких фундаментальних принципах:

- Зведення до мінімуму оброблення первісних цифрових пристроїв або потенційних цифрових доказів;
- Пояснювати будь-які зміни та документувати запроваджені дії (щоб експерт мав можливість сформувати висновок щодо надійності);
- Відповідати локальним правилам стосовно доказів; та
- DEFR та DES не повинні виконувати дії поза межами їх компетентності.

Потенційні цифрові докази повинні зберігатися відповідно до цих фундаментальних принципів та вимог оброблення потенційних цифрових доказів. Усі дії та пояснення потрібно задокументовувати, особливо у випадках, коли можуть бути внесені невідворотні зміни. Кожний процес оброблення цифрових доказів, тобто ідентифікація, збирання, здобуття та збереження детально описаний в наступних розділах.

Ідентифікація.

Цифрові докази представляються в фізичній та логічній формі. Фізична форма включає презентацію даних всередині реального приладу. Логічна форма потенційних цифрових доказів відноситься до віртуальної презентації даних всередині приладу.

Процес ідентифікації включає пошук, розпізнавання та документування потенційного цифрового доказу. Процес ідентифікації повинен 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 базується на їх несталості. Ця несталість даних має бути ідентифікованою для гарантування процесів правильного збирання та здобуття даних для зведення до мінімуму пошкодження потенційних цифрових доказів та отримання найкращих доказів. Додатково, процес повинен ідентифікувати вірогідність наявності прихованих потенційних цифрових доказів. DEFR та DES мають бути обізнаними, що не всі типи носіїв для збереження цифрових даних можуть бути легко ідентифіковані та визначене їх місце розташування, наприклад, хмарні обчислювання, NAS і SAN – це додає віртуальні компоненти в процес ідентифікації.

DEFR має 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 мають відношення до справи.

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

Збирання.

Коли цифрові пристрої, які можуть містити потенційні цифрові докази, ідентифіковані, DEFR та DES повинні прийняти рішення щодо застосування збирання чи здобуття як наступних процесів. Існує ряд рішень, які на це впливають, більш докладно розглянуті в розділі 7. Це рішення повинно базуватися на конкретних обставинах.

Збирання – це процес в процесі оброблення цифрових доказів, де пристрої, які можуть містити потенційні цифрові докази переносяться з їх первісного місця розташування до лабораторії або іншого контрольованого середовища для подальшого здобуття потенційних цифрових доказів та аналізу. Пристрої, які містять потенційні цифрові докази, можуть знаходиться в одному з двох станів: коли система увімкнена або коли система вимкнена. В залежності від стану приладу потрібні різні підходи та інструменти. Локальні процедури можуть застосовувати підходи та інструменти, які використовуються для процесу збирання.

Цей процес включає 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, базуючись на конкретної ситуації, вартості і часі, та задокументувати це рішення використання специфічного методу.

Примітка 1. Перенесення носія для збереження цифрових даних не завжди рекомендується і DEFR має 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 цифрових пристроїв, які не були зібрані, мають бути задокументовані відповідно до юрисдикції, яка застосовується, та відповідно до вимог цієї юрисдикції.

Здобуття

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

Методи, що використовуються для здобуття потенційних цифрових доказів, повинні бути докладно задокументованими та, якщо це можливо, бути відтворюваними або мати можливість перевірки компетентним DEFR. DEFR або DES повинні здобувати потенційні цифрові докази таким чином, щоб максимально зменшити втручання, де це можливо, для того, щоб запобігти змінам, які можуть бути внесені. Для застосування цього процесу DEFR має розглянути найбільш належний метод для використання. Якщо цей процес призведе до невідворотних змін в цифрових даних, усі дії, що були виконані, повинні бути задокументованими для врахування змін у даних.

Метод здобуття, що запроваджується, повинен забезпечити копіювання цифрових доказів із 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 повинна давати такий самий результат функції верифікації.

Процес верифікації не може бути зроблений в деяких обставинах, наприклад, при здобутті 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 і захистити вибір цього

методу. Якщо утворення образу не може бути підтвердженим, тоді це необхідно задокументувати та підтвердити. Якщо потрібно, метод здобуття, що запроваджується, повинен мати можливість отримання локалізованого і нелокалізованого простору.

Примітка 1. Коли не може бути застосований процес підтвердження для всього джерела через помилки на джерелі, можуть бути використані ті частини джерела, які можуть бути надійно прочитані.

Можуть виникнути ситуації, в яких неможливо або недозволено створити копію цифрового доказу, наприклад, коли джерело є занадто великим. В таких випадках, DEFR може здійснити логічне здобуття, ціллю якого будуть тільки специфічні типи даних, директорії або 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 не бути скопійованими в залежності від метода, що застосовується. Цей метод може бути корисним в інших ситуаціях, коли критичні системи, що розглядаються, не можуть бути зупинені.

Примітка 2. Деякі юрисдикції можуть вимагати спеціального оброблення даних; наприклад, їх запечатування у присутності власника даних. Запечатування повинно бути зроблено відповідно до локальних вимог (законодавство і процедури).

Збереження

Потенційні цифрові докази повинні бути збережені для гарантування їх 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 повинне бути псування даних або будь-яких метаданих, що пов’язані з ними (наприклад, дата та штампи часу). DEFR повинен мати можливість показати, що доказ не був модифікований з моменту, коли він був зібраний або здобутий, чи були зроблені логічні обґрунтування та дії були задокументовані, якщо були внесені невідворотні зміни.

Примітка. В деяких випадках вимагається конфіденційність потенційних цифрових доказів, або існують вимоги бізнесу чи законодавчі вимоги (наприклад, приватність). Потенційні цифрові докази мають зберігатися таким чином, щоб гарантувати конфіденційність даних.

Ключові компоненти ідентифікації, збирання, здобуття та збереження цифрових доказів.

Хронологічне документування

В будь-яких дослідженнях DEFR повинен мати можливість звітувати про всі здобуті дані та прилади в тої 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 елементу від часу, коли він був ідентифікований,

зібраний або здобутий командою дослідників до поточного статусу та місця знаходження.

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

- Унікальний ідентифікатор доказу;
- Хто мав доступ до доказу та час і місце, де це було зроблено;
- Хто перевіряв доказ під час введення в та виведення із обладнання збереження доказу і коли це було зроблено;
- Чому доказ був перевірений (в якому випадку та з якою ціллю) та відповідний дозвіл, якщо він був наданий; та
- Будь-які невідворотні зміни в потенційних цифрових доказах, а також ім'я особи, яка була відповідальна за це та юрисдикцію для внесення цих змін.

Хронологічне документування повинен підтримуватися протягом всього часу життя доказів та зберігатися протягом визначеного періоду часу після завершення часу життя доказів – цей період часу може бути встановлений відповідно до локального законодавства збирання та застосування доказів. Він повинен бути встановленим від моменту, коли цифрові прилади та/або потенційні цифрові докази були здобуті и не повинен змінюватися.

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

Застереження на місці інциденту

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 наступне, залежно від локальних законів:

- Убезпечити та контролювати місце, що містить пристрої;
- Визначити, хто винен в змінах їх 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 є увімкненим, не треба його вимикати, та якщо пристрій є вимкненим, не треба його вмикати;

- Якщо це можливе, задокументувати (наприклад, схема, фото або відео) місце, усі компоненті і кабелі в їх первісному положенні. Якщо камера та/або відеокамера відсутні, нарисувати схематичний план системи та позначки портів та кабелів таким чином, щоб система могла бути підтверджена та відновлена пізніше; та
- Якщо це дозволено, дослідити місце для пошуку елементів, таких як причеплені нотатки, щоденники, папери, ноутбуки або описи обладнання і програмного забезпечення з критичними деталями стосовно пристроїв, таких як паролі та PIN.

Примітка 1. Деякі юрисдикції можуть накладати спеціальні вимоги стосовно визнання фото та відео доказів. 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 з самого початку зазначити усі ризики, які виникають під час виконання усіх процесів протягом розслідування. Необхідно розглянути, яким чином захистити персонал та потенційні цифрові докази на місці інциденту.

Персонал

Важливо застосувати оцінювання ризиків стосовно безпеки персоналу до початку процесу, оскільки безпека персоналу, задіяного у процесі, є життєво важливою. Питання, які мають бути розглянутими під час оцінювання ризиків стосовно персоналу включають, але не обмежуються, наступне:

- Чи будуть присутні особа(и), яких досліджують? Якщо присутні, чи мають вони схильність до насилля?
- Протягом якого часу доби буде проведена ця операція?
- Чи може місце інциденту бути ізольоване від свідків?
- Чи наявна зброя в цьому місці?
- Чи існує будь-який фізичний ризик для осіб, що будуть присутні?
- Чи може будь-що у близькості, включаючи пристрої, налагоджене таким чином, щоб викликати фізичне лихо, якщо обробляється неналежним чином, наприклад, приховану пастку?
- Чи можуть матеріали, що повинні бути зібрані, мати деяку вірогідність отримати фізіологічне пошкодження або порушення?
- Чи може місце інциденту розглядатися як небезпечне?
- Чи може оточення мати вплив на потенційний ризик?

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, що була запроваджена протягом збирання або здобуття. Ризики повинні бути оцінені для зменшення впливу з точки зору подальших пошкоджень.

Оцінювання ризиків включає 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, включають, але не обмежуються наступним:

- Який тип методів збирання/здобуття застосовується?
- Яке обладнання може бути потрібним на місці?
- Який рівень нестабільності (нестійкості) даних та інформації, які пов'язані із 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 пошкоджене?
- Чи можуть бути дані скомпрометовані?

Чи може цифровий пристрій бути зконфігурований таким чином, щоб зруйнувати (наприклад, за допомогою логічної бомби), пошкодити або заплутати дані, якщо його вимкнути або отримати доступ неконтрольованим чином?

Ролі та відповідальності

Роль DEFR охоплює ідентифікацію, збирання, здобуття та збереження потенційних цифрових доказів на місці інциденту. Вона включає розроблення звіту щодо збирання та здобуття, але звіт стосовно аналізу не є необхідним. Роль DEFR також включає гарантування цілісності та 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 включає здійснення технічної підтримки 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. В контексті оброблення інциденту при наявності ISIRT в ISO/IEC 27035:2011 розглянуті роли DEFR та DES як членів ISIRT.

Компетентність

DEFR та DES повинні мати належні технічні та законодавчі компетенції (тобто, ті, що надані в Додатку А) та продемонструвати, що вони пройшли відповідне навчання та мають достатнє технічне та законодавче розуміння для оброблення потенційних цифрових доказів належним чином. 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 якість 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 він належним чином поінформований про те, як зробити це у відповідній юрисдикції. Якщо

потрібно, DEFR та/або DES повинні мати можливість показати, що вони мають компетенцію для оброблення потенційних цифрових доказів із використанням інструментів та методів, визначених для виконання цих завдань. Також вимагається, щоб DEFR мав можливість надавати доказ своєї поточної компетенції.

Деякими передумовами для DEFR є наступні:

- Вони повинні належним чином та адекватно пройти навчання стосовно роботи із цифровими пристроями з точки зору дослідницької діяльності;
- Вони повинні показати відповідним органам у відповідній сфері та підтримувати свої навички та компетентність в обробленні потенційних цифрових доказів; та
- Відповідальністю особи (осіб) та роботодавця є гарантування,що вони адекватно пройшли навчання та підтримують навички та компетентність.

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

Запровадження необхідної обережності

Слід 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 доступ до цифрових пристроїв, таких що знімають дамп пам'яті з цифрових пристроїв наживо, крім випадків, якщо вони мають належну компетентність та використовують надійні та затверджені процеси.

Існують деякі обставини, коли неможливо збирати або здобувати потенційні цифрові докази. DEFR повинен розглянути наступні обставини, але не обмежуватися тільки ними:

- Якщо відсутні законні права або авторизація для збирання цифрових доказів;
- Якщо існують 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 повинні здійснюватися приховано, якщо це вважається легальним в рамках юрисдикції;
- Якщо це критичний пристрій, який не може простоювати;
- Якщо фізичний розмір цифрового пристрою є дуже великим, наприклад сервер в дата-центрі або RAID система;
- Якщо це критичний цифровий пристрій безпеки, який ставить під загрозу життя, якщо буде зупинений; та
- Якщо це цифровий пристрій, який також надає послуги невинним сторонам.

Документація

Документація є критичною при обробленні цифрових пристроїв, які можуть містити потенційні цифрові докази. DEFR повинен дотримуватися наступного під час документування:

- Кожна дія, що виконується, повинна бути задокументована. Це гарантує, що жодна деталь не була упущена 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 земною кулі, можуть бути простежені відповідним чином.
- DEFR повинен бути уважним до встановлення часу та дати, якщо цифрові пристрої увімкнені. Порівняти встановлення часу з надійним джерелом часу, таким як час, що синхронізований з надійним джерелом та який можливо простежити. Ці встановлення часу повинні бути задокументовані та зазначено, якщо присутня 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 належним чином навчений персонал повинен виправляти ці встановлення.
- DEFR повинен задокументувати усе, що видимо на екрані цифрового пристрою: активні програми та процеси, а також назви відкритих документів. Це документування повинно включати опис того, що видимо, оскільки деякі зловмисні програми можуть маскуватися під добре відоме програмне забезпечення.
- Будь-які переміщення цифрових пристроїв повинні бути задокументовані відповідно до локальних вимог.
- Документувати усі 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 наведені в Додатку Б.

Примітка. Для більш детальної інформації стосовно документації зверніться до розділу управління документами та розділу управління записами ISO/IEC 17025:2005.

Інструктаж

Загальні положення

Важливо, щоб DEFR та DES були адекватно проінструктовані уповноваженим органом перед виконанням їх завдань, особливо стосовно деяких законів про конфіденційність та обмеження (тобто, потрібні базисні знання). Важливо мати формальну сесію інструктажу для розуміння інциденту, що слід очікувати та не очікувати протягом розслідувань, та нагадування стосовно недопущення втручання та псування доказів. Інструктаж повинен бути достатньо суттєвим для членів, які добре підготовані в розподілі ролей та відповідальності; таким чином буде гарантоване вилучення усіх прийнятних потенційних цифрових доказів.

Особливість цифрових доказів

Сесія інструктажу, яку сфокусовано 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 із відповідною інформацією та детальними інструкціями стосовно потенційних цифрових доказів, які повинні бути зібрані або здобуті. Це може включати:

- Тип інциденту (якщо відомий);
- Дата та 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 необхідність відключити будь-які можливості Bluetooth або Wi-Fi на їх телефонах/комп`ютерах, щоб вони не могли випадково взаємодіяти з цифровими пристроями, за виключенням телефонів/комп`ютерів, які використовуються для виявлення зв'язків.
- Важливість документування протягом розслідування; та
- Запровадження законодавчих або інших факторів, які забороняють збирання будь-яких пристроїв та потенційних цифрових доказів, що вони містять.

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

Особливості персоналу

Сесія інструктажу, яка чітко сфокусована на специфічних настановах щодо персоналу, потрібна для інформування DEFR щодо особливостей, притаманних сторонам, які приймають участь в розслідуванні. Протягом цієї сесії інструктажу команда дослідників повинна бути ознайомлена із інструкціями стосовно персоналу. Це може включати:

- Призначення, роли та відповідальність членів команди дослідників на місці інциденту;
- Чи очікується, що інші сторони (медичний персонал, біологічні судові дослідники, тощо) будуть приймати участь в цих розслідуваннях;
- Вимога до членів команди дослідників не допускати технічної допомоги від будь-яких неавторизованих осіб; та
- Вимога до членів команди дослідників суворо дотримуватися процедури для того, 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, яка описана в розділі 6.7.1.

Інциденти реального часу

Найбільш бажано, щоб розслідування інциденту були заплановані заздалегідь, але існують обставини (наприклад, коли інцидент розвивається та створює відклики), де повне планування не можливе. В таких ситуаціях команда повинна бути проінструктована стосовно початкової стратегії і тактики розслідування та має дозвіл розробити нову стратегію та тактику у відповідь на існуючи умови. Інформація стосовно цього інциденту, як він розвивається, повинна бути поширена серед членів команди так швидко, як це можливо, для того, щоб гарантувати, що рішення стосовно дій, які слід здійснити, могли бути визначені ефективно та з урахуванням потреб юрисдикції.

Інша інформація стосовно інструктажу

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

- Визначення місця, де буде проводиться розслідування, включаючи назву організації, адресу та карту місцевості (якщо можливо);
- Дозвіл на розслідування;
- Подробиці пошукових повноважень та інших повноважень, притаманних цьому розслідуванню, включаючи обмеження пошуку та конфіскації;
- Законодавчі аспекти та 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 можуть бути висунуто обвинувачення у прихованій упередженості. Прикладом прихованої упередженості є ситуація, коли DEFR копіює один комп’ютер, а не інший (який, як пізніше виявляється містить виправдовувальні докази), базуючись на своїх уявленнях, що були сформовані інструктажем.

Визначення пріоритетів збирання та здобуття

При визначенні 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 із збирання та здобуття. Однак, може бути потрібним визначити пріоритетні елементи в залежності від значення нестійкості та/або значимості/потенційних цифрових доказів. Елементи з високим релевантним/потенційним значенням цифрових доказів є такі, що найбільш ймовірно містять дані, які безпосередньо стосуються інциденту, що розслідується.

Визначення пріоритетів внаслідок пошкодження може бути запроваджено, тільки якщо цього потребують специфічні обставини випадку, що розслідується. Потенційні цифрові докази можуть бути розділені на дві категорії: нестійкі та сталі. Нестійкі дані можуть бути легко зіпсовані або втрачені назавжди, якщо не застосовується належна обережність для захисту цих даних. Наприклад, вимикання живлення цифрового пристрою може призвести до втрати нестійких даних. Сталі дані залишаються в середовище навіть якщо живлення вимкнено. Оскільки деякі типи цифрових доказів можуть мати короткий термін життя, потенційні цифрові докази можуть бути легко зіпсовані або порушені. Там, де незрозуміло, чи містить цифровий пристрій потенційні цифрові докази, або які елементи є більш важливі, 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, процеси, що запущені, тощо. DEFR повинен володіти глибокими знаннями для визначення пріоритетів відповідно до нестійкості.

Протягом ідентифікації DEFR повинен:

- Визначити пріоритети потенційних цифрових доказів, які можуть бути втрачені 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 факторам, які охоплюють, але не обмежуються, переміщення, час та зміни в оточенні цифрових пристроїв – необхідно гарантувати, що такі дані збережені 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. Коли допускається наявність шифрування або шкідливого програмного забезпечення, бажано перевірити нестійкі дані.

За таких обставин час може бути обмежуючим фактором протягом дослідження. У таких випадках треба віддавати перевагу потенційним цифровим доказам, ідентифікованим як такі, що притаманні цьому специфічному інциденту.

Збереження потенційних цифрових даних

Загальні положення

При збереженні здобутих потенційних цифрових доказів та зібраних цифрових приладів під час пакування важливо убезпечити ці елементи таким чином, 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 в потенційні цифрові докази. Тому, є дуже критичним захистити потенційні цифрові докази найкращим можливим чином та найменш використовувати первісні дані. Важливо, щоб DEFR був ознайомлений з вимогами щодо пакування в юрисдикції, що використовується.

Збереження потенційних цифрових доказів

Усі зібрані цифрові пристрої та здобуті потенційні цифрові докази повинні бути захищеними, наскільки це можливо, від втрати, порушення або псування. Найбільш важливою діяльністю в процесі збереження є підтримання цілісності та автентичності потенційних цифрових доказів та їх хронологічного документування.

Зібрані цифрові пристрої та здобуті потенційні цифрові докази повинні зберігатися в пристроях збереження доказів, де запроваджені заходи фізичної безпеки, такі як системи контролю доступу, системи спостереження або системи виявлення вторгнень або в іншому контрольованому середовище для збереження потенційних цифрових доказів. Основними цілями фізичної безпеки є захист та уникнення втрат, пошкоджень та порушень, а також забезпечення можливості здійснення аудиту.

Зібрані цифрові пристрої перед переміщення в інше місце повинні бути обгорнуті або розміщені у відповідній упаковці, що придатна для цього пристрою для уникнення спотворення цифрового пристрою(ів). Повинна використовуватися упаковка, яка захищає від ударів для уникнення фізичного пошкодження будь-яких компонентів пристрою(ів).

- DEFR повинен розглянути чутливість цифрового пристрою до статичної електрики. Якщо це дійсно існує, пристрій повинен бути захищеним антистатичною упаковкою.
- Основні блоки системи та ноутбуки потребують захисту у належному контейнері для уникнення пошкодження або псування потенційних цифрових доказів, які можуть залишатися там.

Примітка. Використання упаковки Фарадея або іншою упаковки з екрануванням від радіо частот може збільшити витік батареї мобільного телефону. Це може потребувати забезпечення додаткового живлення для пристрою, поки він знаходиться в середині упаковки, якщо ресурси дозволяють.

Пакування цифрових пристроїв та потенційних цифрових доказів

6.9.3.1 Основні дії: пакування потенційних цифрових доказів

Основні дії повинні виконуватися навіть якщо існує гарна причина не виконувати їх. Це може також розглядатися як мінімальні дії, які треба виконувати. Протягом пакування DEFR повинен записувати та звертати увагу на наступні основні дії:

- Не торкатися магнітних стрічок, краще працювати зі стрічками в їх захисних контейнерах або торкатися лише в місцях, які завідомо не містять даних (наприклад, край оптичних дисків). Це повинно 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 помічати етикетками всі потенційні цифрові докази. Деякі юрисдикції мають спеціальні вимоги стосовно формату етикеток доказового матеріалу. DEFR повинен бути знати, та підтвердити це, вимоги, які мають застосовуватися. DEFR повинен помітити 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 пристроїв повинні бути здобути та зберігатися таким чином, щоб гарантувати цілісність цих доказів.
- Якщо можливо, цифрові пристрої з відкритими та рухомими елементами повинні бути запечатаними за допомогою етикеток, які запобігають порушенню доказів, що підходять до цього пристрою, і DEFR повинен підписати запечатування.
- Пристрої з несталими даними, які обладнані батареями, повинні регулярно перевірятися для гарантування того, що ці пристрої завжди мають достатнє живлення.
- Ідентифікувати та убезпечити цифрові пристрої в контейнері, який за своєю природою підходить цьому пристрою для захисту від потенційних загроз.
- Комп'ютери та цифрові пристрої повинні бути запаковані таким чином, щоб уникнути пошкодження від удару, вібрації, великий висоти, тепла та опромінення радіо частотами протягом транспортування.
- Магнітні носії для збереження цифрових даних повинні зберігатися в упаковці, яка є магнітно інертною, антистатичною та вільною від часточок.
- Цифрові докази можуть також містити приховані докази, відбитки або 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 або біологічних доказів були застосовані на цих пристроях. Однак, рішення щодо визначення пріоритетів збирання доказів повинно бути ретельно оцінено з урахуванням можливості збереження цих доказів.

6.9.3.2 Додаткові дії: пакування потенційних цифрових доказів

Додаткові дії, які відносяться до таких, що дуже рекомендуються, мають бути виконані. Протягом пакування DEFR повинен записувати та звертати увагу на наступні додаткові дії, якщо вони застосовуються:

- 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 повинно бути вільним від статичної електрики.

- Мінімізувати можливість копіефекту (перенесення сигналу від одного рулону стрічки до сусіднього рулону), яке може зустрічатися коли стрічки зберігаються протягом тривалого періоду без активного використання, призводячи до низький якості сигналу.
- Якщо потрібно, місця пакування повинні бути вільними від UV світла. UV може викликати пошкодження DNA або пошкодження деяких типів середовищ. DEFR повинен розглянути, чи може існувати ризик від UV для потенційних цифрових доказів перед вибором місця пакування.
- Цифрові пристрої повинні бути надійно захищені від теплового удару.

Транспортування потенційних цифрових доказів

DEFR повинен зберігати зібрані цифрові пристрої та здобуті потенційні цифрові докази протягом транспортування. Потенційні цифрові докази не повинні залишатися без уваги протягом процесу транспортування. DEFR повинен підтримувати хронологічне документування протягом процесу транспортування для уникнення можливих пошкоджень або псування, та підтримувати цілісність та автентичність цифрових пристроїв та потенційних цифрових доказів. Якщо потенційні цифрові докази не транспортуються DEFR або DES, рекомендується 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 присутності електростатичних розрядів, які можуть зменшити доказове значення потенційних цифрових доказів. DEFR повинен гарантувати, що комп'ютери та цифрові пристрої запаковані безпечно для уникнення пошкоджень від ударів та вібрації.

Процес транспортування має бути дозволеним для керованого та контрольованого середовища. Рівень вологості, вогкості повітря та температура повинні бути підходящими для цифрових пристроїв. Слід уникати находження потенційних цифрових доказів та цифрових пристроїв в транспортному засобі протягом тривалих періодів та уникати їх знаходження при наявності UV.

В деяких юрисдикціях, якщо обставини не дозволяють, DEFR не може супроводжувати докази. В таких випадках, можуть використані відповідні та авторизовані механізми транспортного засобу для гарантування належної безпеки доказів протягом транспортування. Документація стосовно транспортування та підтвердження цілісності упаковки повинна становиться 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

В контексті цього розділу комп`ютери розглядаються як окремі цифрові пристрої, які приймають, обробляють та зберігають дані та отримують результати. Такі комп`ютери не під'єднанні мережі, але можуть бути під`єднанні 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, повинні розглядатися (для цілей цього стандарту) як окремий комп'ютер. Якщо комп'ютер має мережевий інтерфейс, але не було знайдено явних підключень, слід виконати дії для ідентифікації пристроїв, до яких він мав бути підключеним в недавньому минулому.

Зазвичай, місця інцидентів містять різні типи носіїв для збереження цифрових даних. Носії для збереження цифрових даних використовуються 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 або збирання, необхідно розглянути питання безпеки потенційних цифрових доказів. Ці питання описані в розділах 6.2.1 та 6.2.2. Однак, DEFR повинен бути обережним у запевненні самого себе, що пристрій, який виявляється окремим, не був нещодавно підключеним до мережі. Коли існує припущення, що зараз окремий цифровий пристрій був нещодавно відключеним, повинна бути зроблена спроба обробляти його як мережевий пристрій для того, щоб впевнитися, що інші частини мережі працюють коректно. DEFR повинен записувати та звертати увагу хоча б на наступне:

- DEFR повинен задокументувати тип та назву будь-якого цифрового пристрою, що використовувався, та ідентифікувати всі комп'ютери і периферійні пристрої, які потрібно здобути або зібрати протягом початковою стадії. Повинні бути також задокументовані серійні номери, номери ліцензій та інші ідентифікаційні позначки (включаючи фізичне пошкодження), там це можливо зробити.
- На стадії ідентифікації статус комп'ютерів та периферійних пристроїв повинен залишатися як він є. Якщо комп'ютери були вимкнені, не треба їх вмикати. Якщо комп'ютери або периферійні пристрої були увімкнені, DEFR не повинен їх вимикати, що в противному випадку може зіпсувати потенційні цифрові докази.
- Якщо комп'ютери увімкнені, DEFR повинен сфотографувати або зробити паперовий документ стосовно того, що показано на екранах. Будь-який паперовий документ повинен 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 інформація не буде втрачена.
- DEFR повинен також розглянути за допомогою детектора бездротових сигналів питання пошуку та ідентифікації бездротових сигналів від

бездротових пристроїв, що можуть бути приховані. Можуть скластися такі обставини, коли детектор бездротових сигналів не використовується із-за обмежень вартості та часу, і DEFR повинен це задокументувати. Якщо будуть знайдені будь-які мережеві пристрої, DEFR повинен продовжувати процес оброблення доказів, як описано в розділі 7.2.2.2 цього стандарту. Там, де використовується активне сканування (тобто, широкополосне та/або вибіркове) для мережевих пристроїв, пристрої сканування повинні бути вимкнені на час оцінювання вірогідності того, що ці пристрої можуть взаємодіяти з іншими пристроями на місці. Члени команди повинні пам'ятати, що певний пристрій на місці може визначити присутність 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. В деяких юрисдикціях дозволено вмикати цифрові пристрої на місці події для визначення їх доречності в розслідуванні, якщо присутня велика кількість цифрових пристроїв. Це робиться з урахуванням часу оброблення та вартості, які можуть бути недоречними, якщо будуть оброблятися непричетні цифрові пристрої. Якщо пристрій був увімкнений для оцінювання на місці, DEFR повинен гарантувати, що докладні нотатки дій, що були застосовані, підтримуються протягом цього процесу.

Примітка 2. Для збереженні статусу живлення цифрового пристрою повинні бути розглянуті результати несталості та процесу визначення пріоритетів. Якщо прийнято рішення, що найбільш критична інформація є сталою інформацією на диску, тоді треба сфотографувати екран консолі цієї працюючої системи та її вимкнути. Якщо наявна несталі інформація в пам'яті, тоді критично важливо залишити систему увімкнутою для того, 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 деталі. 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 повинні бути точно задокументовані. Ці особи можуть включати системного адміністратора, власника пристрою та користувачів комп'ютеру 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 аналізу потенційних цифрових доказів. Ці опитування повинні бути задокументовані для гарантування того, що деталі є точними та задокументовані твердження не можуть бути змінені. DEFR повинен бути ознайомлений з відповідними вимогами законодавства стосовно збирання нецифрових доказів.

7.1.1.3 Процес прийняття рішень для збирання та здобуття

При прийнятті рішення щодо збирання цифрових пристроїв або здобуття потенційних цифрових доказів необхідно розглядати декілька факторів, які охоплюють, але не обмежуються наступним:

- несталість потенційних цифрових доказів, що обговорено в розділах 5.4.2 та 6.8;
- існування шифрування всього диску або зашифрованих частин, де парольна фраза або ключі зберігаються як несталі дані в RAM, на зовнішніх токенах, смарт-картах, інших пристроях або середовище;
- критичність системи, яка обговорюється в розділах 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.

7.1.2 Збирання

7.1.2.1 Цифрові пристрої увімкнені

7.1.2.1.1 Загальні положення

DEFR може використовувати декілька настанов для збирання даних, коли цифровий пристрій увімкнений. Не всі настанови є ідеальними та можуть використовуватись для будь-яких випадків; деякі настанови можуть підходити тільки для специфічних випадків. Відповідно, настанови можуть бути класифіковані як основні або додаткові. Основні дії повинні застосовуватись для усіх обставин, в той же час додаткові дії повинні запроваджуватись, коли доречні та можуть бути застосовані, в залежності від унікального приладу або обставин. На рисунку 2 показані основні та додаткові дії, які можуть бути застосовані для збирання цифрових пристроїв, коли вони увімкнені.

Примітка. Всі ці дії повинні відповідати локальному законодавству та нормативним документам.

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

7.1.2.1.2 Основні дії: збирання увімкнених цифрових пристроїв

Наступні основні дії повинні бути запроваджені в усіх випадках стосовно потенційних цифрових доказів. Ці настанови застосовуються, коли DEFR прийняв рішення , що повинні збиратися цифрові пристрої, коли вони увімкнені:

- Розглянути здобуття несталих даних з цифрових пристроїв та поточний стан перед вимкненням системи. Ключі шифрування та інші критичні дані можуть бути розміщені в активної пам’яті або в неактивної пам’яті, яка не буде очищена. Розглянути логічне здобуття, коли запроваджено шифрування. В цьому випадку слід мати на увазі, що діюча основна операційна система може бути ненадійною, тому слід розглянути використання відповідних надійних та затверджених інструментів.
- Конфігурація цифрового пристрою може визначати чи потребує DEFR вимикання цього пристрою за допомогою звичайних адміністративних

процедур або вилка пристрою повинна бути вилучена з розетки живлення. DEFR може потребувати консультації з DES для визначення найкращого підходу, який доречний для специфічних обставин. Якщо прийнято рішення про вилучення вилки з розетки, DEFR повинен вилучити кабель живлення з початку вилучаючи кінець, що підключений до цифрового пристрою, а не кінець, що підключений до розетки. Слід бути обережним, оскільки пристрій, підключений до UPS, може змінювати дані, якщо кабель живлення вилучається із розетки, а не з пристрою.

Примітка 1. Якщо живлення буде відключено від працюючого пристрою, будь-які потенційні докази, що зберігаються у зашифрованому вигляді, будуть недоступні, поки не буде отриманий 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 управляють медичним обладнанням. Тому, DEFR повинен гарантувати, що несталі дані будуть зібрані до вимкнення живлення.

Примітка 2. Існують пристрої, які дозволяють пристрій, що увімкнений, відключити від джерела живлення та перемістити його до портативного UPS без переривання живлення цього пристрою. Існують також похитування мишкою, які можуть бути використані для уникнення активації програми блокування екрана. Обидва ці пристрої надають доречні інструменти, якщо проводяться дослідження увімкненого пристрою, де може бути запроваджено шифрування. Якщо увімкнені пристрої збираються таким чином, що живлення підтримується, пакування та транспортування діючих систем повинна мати заходи, які пов'язані із забезпеченням охолодження, захисту від механічних ударів, тощо.

- Забезпечити позначки, відключення та убезпечення усіх кабелів від цифрового пристрою та забезпечити позначки портів таким чином, щоб система могла бути реконструйована пізніше.

- Помістити стрічку поверх вимикача живлення, якщо потрібно, для уникнення зміни стану живлення. Розглянути чи стан вимикача відповідним чином задокументований перед закриттям його стрічкою або переміщенням.

7.1.2.1.3 Додаткові дії: збирання увімкнених цифрових пристроїв

Слід запроваджувати додаткові дії, які є доречними в залежності від конфігурації специфічного цифрового пристрою.

- Для ноутбука слід гарантувати, що несталі дані були здобуті перед вилученням батареї. DEFR повинен вилучити основне джерело живлення одразу, замість виключення клавіші живлення на ноутбуці для його перезавантаженням. 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 сконфігуроване таким чином, що буде запущений скрипт, який може змінювати інформацію або видаляти інформацію із системи перед перезавантаженням або надавати попередження приєднаній системі, що виявлено несподівана ситуація, яка може призвести до стирання даних, що мають доказове значення, перед тим, як вони ідентифіковані. Пристрій може бути також сконфігурований таким чином, щоб запустити пристрій так, щоб він навмисно завдав шкоди DEFR та іншім присутнім особам.

- Розмістити стрічку поверх слоту гнучких дисків, якщо він присутній.

- Необхідно впевнитися, що лотки слотів CD або DVD розміщені 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 увімкнений наступного разу, він може загружатися з цього носія, а не з жорсткого диску (або з інструментів драйверу гнучкого диску) в залежності 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, коли цифровий пристрій вимкнений. Не всі дії, що містяться в цих настановах можуть бути застосовані для усіх обставин. Таким чином, необхідно визначити відмінності між тими діями, що можуть застосовуватися в усіх випадках (основні дії), та тими, що можуть бути застосовані тільки в деяких випадках (додаткові дії). На рисунку 3 показані основні та додаткові дії, які застосовуються для збирання вимкнених цифрових пристроїв.

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

7.1.2.2.2 Основні дії: збирання вимкнених цифрових пристроїв

Наступні дії є рекомендованими основними діями для збирання, коли цифровий пристрій вимкнений:

- Вилучити кабель живлення таким чином: з початку вилучити кінець, що підключений до цифрового пристрою, а не кінець, що підключений до розетки.
- Вилучити та убезпечите усі кабелі від цифрових пристроїв та помістити позначки на портах так, щоб система могла бути реконструйована пізніше .
- Помістити стрічку на вимикачі живлення, якщо потрібно, для уникнення зміни стану вимикача. Впевнитись чи стан вимикача був правильно задокументований перед тим, як він був закритий стрічкою або відкритий.

Примітка. Зазвичай носій для збереження не повинен бути вилученим із блоку 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. Повинні бути розроблені та запроваджені локальні процедури стосовно необхідності вилучення носіїв для збереження даних з цифрових пристроїв.

7.1.2.2.3 Додаткові дії: збирання вимкнених цифрових пристроїв

Наступні дії є додатковими діями, які є доречними для збирання вимкнених цифрових пристроїв в залежності від конфігурації специфічного цифрового пристрою:

- З початку треба впевнитися, що ноутбук дійсно виключений, оскільки деякі з них можуть находиться у режимі очікування. Слід бути обережними, оскільки деякі ноутбуки можуть включатися при відкритті кришки. Потім

перейти до вилучення основної батареї живлення ноутбука.

- Якщо умови на місці дослідження потребують вилучення жорсткого диску, DEFR повинен бути обережним при заземлення цифрового пристрою для уникнення впливу статичної електрики щодо пошкодження дисководу жорсткого диска. В противному випадку, дисковод жорсткого диску не повинен вилучатися на місці. Розмістити позначку на дисководі жорсткого диску, як підозрілого диску, та задокументувати усі деталі, такі як тип, назва модулі, серійний номер та розмір дисководу жорсткого диску.
- Розмістити стрічку поверх слоту гнучких дисків, якщо він присутній.
- Необхідно впевнитися, що лотки слотів CD або DVD розміщені 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 увімкнений наступного разу, він може загружатися з носія, а не з жорсткого диску (або з інструментів драйверу гнучкого диску) в залежності від установок BIOS комп'ютера.

7.1.3 Здобуття

7.1.3.1 Увімкнені цифрові пристрої

7.1.3.1.1 Загальні положення

Існує три сценарію, в яких може виникнути необхідність здобуття цифрових доказів: коли цифровий пристрій увімкнений, коли цифровий пристрій вимкнений та коли цифровий пристрій увімкнений, але не може бути вимкненим (таких як критичні цифрові пристрої). В усіх цих сценаріях DEFR потребує отримання точної копії цифрових доказів з носія для збереження цифрового пристрою, який підозрюється в том, 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, повинні бути зроблені як затверджена мастер-копію та і робоча копія. Мастер-копія не повинна використовуватися знову, хоча вона потрібна для підтвердження контенту робочої копії або виконання заміни робочої копії після пошкодження першої робочої копії.

DEFR може запроваджувати ряд настанов для здобуття, коли визначено, що цифровий пристрій увімкнений. Не всі настанови є ідеальними та підходять для всіх випадків; деякі настанови можуть застосовані тільки для специфічних випадків. Відповідно, настанови можуть бути класифіковані як основні або додаткові. Необхідно розглянути можливість того, що увімкнені системи можуть бути введені в режим блокування екрану або автоблокування та що існують приховані значення до будь-яких спроб для уникнення цього. Наприклад, коливання мишкою буде вимагати встановлення USB ключа для реєстрації та найбільш вірогідно може викликати модифікацію при будь-яких інших діях. Використання доречних методів буде мінімізувати приховані значення таких дій. На рисунку 4 показані основні та додаткові дії, які застосовуються для здобуття потенційних цифрових доказів на увімкнених цифрових пристроях.

Примітка 1. Натискання клавіші живлення на цифровому пристрої може бути сконфігуроване таким чином, що буде запущений скрипт, якій може змінювати інформацію або віддаляти інформацію із системи перед перезавантаженням або надавати попередження приєднаній системі, що виявлено несподівана ситуація, яка може призвести до стирання даних, що мають доказове значення перед тим, як вони ідентифіковані. Пристрій може бути також сконфігурований таким чином, щоб запустити пристрій так, щоб він навмисно завдав шкоди DEFR та іншім присутнім особам

7.1.3.1.2 Основні дії: здобуття потенційних цифрових доказів на увімкнених цифрових пристроях

Наступні дії є основними діями, які повинні бути запроваджені DEFR в усіх випадках здобуття потенційних цифрових доказів на увімкнених цифрових пристроях:

- З початку розглянути здобуття потенційних цифрових доказів, які можуть бути втраченими, якщо цифровий пристрій буде вимкненим. Також відомо для несталих даних, таких як дані, що зберігаються в RAM, запущених процесах, мережевих з'єднаннях та установках дати/часу. У випадках, коли необхідно здобути сталі дані з пристроїв, які ще працюють, повинне бути розглянуте здійснення здобуття на увімкнених системах.
- Запровадження здобування наживо необхідно для здобуття даних наживо від пристроїв, які ще працюють. Здобуття несталих даних наживо в RAM робить можливість 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 в системах. З цієї причині, 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 загрузки програмного забезпечення змінює нумерацію сторінок, тощо). Усі дії, що були виконані, та отримані зміни, що були зроблені в потенційних цифрових доказах, повинні бути задокументовані та зрозумілі. Якщо неможливо визначити подібні впливи на систему задіяних інструментів або зміни, що є результатом дій, не можуть бути визначені однозначно, це також повинно бути задокументовано.
- Під час здобуття несталих даних DEFR повинен адаптувати використання логічного файлового контейнеру, де це можливо, та задокументувати їх геш-значення, коли контейнер містить файл(и) несталих даних. Там, де це неможливо, повинен використовуватися контейнер, такій як ZIP файл; потім для цього файлу повинно бути обчислене геш значення і це значення задокументоване. Отриманий файловий контейнер повинен зберігатися на носії для збереження цифрових даних, який підготований для цієї цілі, тобто відформатований.
- Застосувати процес створення образу наживо для сталого збереження з використанням затверджених інструментів створення образу. Отримана копія

цифрового доказу повинна зберігатися на носії для збереження цифрових даних, який підготований для цієї цілі. Краще використовувати нові носії для збереження цифрових даних, застосування копій цифрових доказів від затверджених процесів гарантує цілісність даних при реконструкції. Тому, носії для збереження цифрових даних, які очищені, будуть недоречними. Якщо образ збережений в логічному файловому контейнері, DEFR повинен гарантувати, що цей образ не може бути зіпсованим або пошкодженим.

Примітка. В ситуаціях, коли пристрій заблокований, фізичний доступ може здійснюватися за допомогою інших засобів, які мають можливість прямого доступу, наприклад, Firewire інтерфейс.

7.1.3.1.3 Додаткові дії: здобуття потенційних цифрових доказів на увімкнених цифрових пристроях

Наступні дії є додатковими діями, які є доречними для здобуття потенційних цифрових доказів на увімкнених цифрових пристроях в залежності від конфігурації специфічного цифрового пристрою:

- Розглянути здобуття несталих даних з RAM, коли підозрюється наявність шифрування. З початку перевірте чи дійсно це саме такій випадок, за допомогою перевірки необробленого диску або за допомогою деяких утиліт для пошуку зашифрованої інформації. Якщо це саме такий випадок, слід мати на увазі, що працююча основна операційна система може бути ненадійною та слід 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.

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 показані дії, які можуть бути застосовані для здобуття потенційних цифрових доказів з вимкнених цифрових приладів.

7.1.3.2.2 Здобуття з вимкнених цифрових пристроїв

Наступні дії є діями з здобуття потенційних цифрових доказів, коли цифрові пристрої вимкнені:

- Впевнитися, що пристрій дійсно вимкнений.
- Якщо потрібно, вилучити носій із вимкненого цифрового пристрою, якщо це ще не було зроблено. Розмістити позначку на носії, як підозрілому носії, та задокументувати усі 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. В більшості випадків носій не вилучається з цифрового пристрою до тих пор, поки виконується здобуття потенційних цифрових доказів, оскільки його вилучення

збільшує ризик пошкодження або плутанини його з іншими носіями для збереження даних. Повинні бути розроблені та запроваджені локальні процедури стосовно необхідності вилучення носія для збереження з цифрових пристроїв.

7.1.3.3 Критичні цифрові пристрої

У деяких випадках цифрові пристрої не можуть бути вимкненими із-за критичної природи в системах. Це системи, такі як сервера в дата-центрах, які також надають послуги невинним клієнтам, системи життєзабезпечення, медичні системи та багато інших, які можуть оказувати критичний вплив, якщо вони перервуть роботу або будуть вимкнені. Слід бути особливо обережними при роботі з такими системами.

Коли цифровий пристрій не може бути вимкненим, виконується здобуття наживо та/або часткове здобуття потенційних цифрових доказів, як описано в розділах 7.1.3.1.2 та 7.1.3.4.

7.1.3.4 Часткове здобуття

Часткове здобуття може здійснюватися в наслідок декількох причин, таких як:

- системний сховище є дуже великим, щоб бути здобутим (наприклад, сервер баз даних);
- система є дуже критичною, щоб бути вимкнений;
- коли тільки вибрані дані, що повинні бути здобуті, містять інші недоречні дані в середині той самої системи; або
- коли існують законодавчі обмеження повноважень, такі як судове розпорядження на розслідування, яке обмежує сферу застосування здобуття.

Коли прийнято рішення щодо здійснення часткового здобуття, дії з такого здобуття охоплюють, але не обмежуються, наступними:

- Ідентифікувати папку(и), файл(и) або будь-які доречні власні системні опції, які доступні для здобуття бажаних даних.
- Виконати логічне здобуття цих ідентифікованих даних.

7.1.3.5 Носії для збереження цифрових даних

На місці інциденту можуть бути знайдені різні типи носіїв для збереження цифрових даних. Зазвичай існують найменш несталі типи даних та вони можуть мати найнижчий пріоритет протягом збирання та здобуття. Це не означає, що вони є неважливими, оскільки у багатьох випадках зовнішні носії для збереження цифрових даних містять докази, які досліджують аналітики. DEFR повинен гарантувати наступне:

- Перевірити та задокументувати місце (наприклад, відсік дисководів, кабелі та конвектори, USB слоти, тощо) виробника, модель та серійних номер (якщо існує) 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 прийматися на основі природи інциденту та доступних ресурсів. Для виконання здобуття потенційних цифрових доказів (з основного жорсткого диску) на місці, дивись рисунок 4.
- Якщо DEFR прийняв рішення та має дозвіл збирати носії для збереження цифрових даних, зібрані носії повинні бути запаковані або

розміщені у відповідної упаковці.

- Нанести позначки на носії для збереження цифрових даних та будь-які пов’язані з ним частини. Позначки доказів не повинні бути розміщені 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. Всі зібрані носії повинні бути здобуті та збережені таким чином, щоб гарантувати цілісність зібраних носіїв. Якщо можливі докази повинні бути запаковані за допомогою пломб, що порушуються від втручання, тоді DERF або задіяний персонал, повинні підписати ці позначки.
- Зібрані носії для збереження цифрових даних повинні зберігатися в середовище, яке підходить 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. В доповнення, 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 наступного:

- Використання відповідних функцій верифікації для того, щоб надавати докази, що скопійовані файли еквівалентні оригіналам.
- Може бути доречним об’єднати DEFR зі здобутими потенційними цифровими доказами за допомогою цифрових підписів, біометрії та фотографії.

Усі цифрові прилади, які були зібрані, повинні бути збережені належним чином. Різні типи потенційних цифрових доказів можуть потребувати різних методів збереження. Потенційні цифрові докази необхідно зберігати протягом їх 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 додані 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

В контексті цього розділу мережеві пристрої розглядаються як комп’ютери або інші цифрові пристрої, які підключені до мережі в дротовому або бездротовому режимі. Такі мережеві прилади можуть охоплювати мейнфрейми, сервери, настільні комп’ютери, комутатори, концентратори,

маршрутизатори, мобільні прилади, PDA, PED, Bluetooth прилади, CCTV системи та інші. Зазначимо, що якщо цифровий пристрій підключений до мережі, важно визначити, де саме потенційні цифрові доказі, які необхідно розглянути, зберігаються. Ці дані можуть бути розміщені будь-де в мережі.

Ідентифікація цифрових пристроїв включає компоненти, такі як логотипи виробника, серійні номери, шини та адаптери живлення. DEFR може розглянуті наступні аспекти як засоби ідентифікації:

- Характеристики пристрою: Модель та виробник цифрового пристрою іноді може бути ідентифікований за його видимими характеристиками, особливо якщо існує 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, яка отримана з середини порожнини блоку батареї, особливо коли вона пов'язана із відповідними базами даних. Наприклад, IMEI є номер 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.
- Зворотній пошук: У випадку мобільних телефонів, якщо телефонний номер цього телефону відомий, зворотній пошук може бути використаний для ідентифікації мережевого оператора.

Завдяки загальним малим розмірам мобільних пристроїв DEFR повинен бути особливо обережним під час ідентифікації усіх типів мобільних пристроїв, які можуть бути причетними в цьому випадку. 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 повинні бути захищеними від несанкціонованого доступу.

Примітка. В деяких випадках комунікація не повинна перериватися. Слід 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 або збирання, місце інциденту повинно бути задокументовано візуальним способом за допомогою фотографування, відеозйомки або схематичного зображення місця, яким воно було при вході. Метод документування потребує збалансування обставин, вартості, часу, наявних ресурсів та пріоритетів. DEFR повинен задокументувати усі 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 пристроїв, що використовувались, та ідентифікувати усі цифрові прилади, які можуть потрібувати здобуття потенційних цифрових доказів і збирання, на цієї початковій стадії. Усі мобільні пристрої та їх відповідні елементи, такі як карти пам'яті, SIM карти, зарядні пристрої та

шини, які були знайдені на цьому місці, їх відповідні серійні номери та будь-які ідентифікаційні особливості повинні бути задокументовані та зібрані, якщо потрібно. Постаратися також знайти оригінальну упаковку мобільних телефонів; вона можу 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 можливість 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 з цих камер дійсно працюють. DEFR повинен також записати тип моделі, модель та основні установки системи, такі як установки дисплея, установки поточної записи та розміщення місця збереження інформації так, щоб полегшити процес збирання та здобуття в разі, якщо зміни повинні бути зроблені; це потім надасть можливість повернути систему до первісного стану.
- Статус цифрових пристроїв повинен залишатися таким, якій він є, наскільки це можливо. Зазвичай, цифрові пристрої вимкнені, DEFR не повинен їх увіткати та, якщо вони увімкнені, DEFR не повинен їх вимикати. Це може попередити небажане псування потенційних цифрових доказів. Пристрій, який має батареї, що можуть розрядитися, потребують зарядження для гарантування того, що інформація не буде втрачена. 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 існувати обставини, коли детектор бездротових сигналів не використовується із-за 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 виконуватися, як описано в розділі 5.4. У випадку, коли пристрої не можуть бути відключені від мережі із-за критичності їх функцій або вірогідності порушення потенційних

цифрових доказів, DEFR повинен виконати здобуття наживо, поки пристрої залишаються підключеними до мережі.

Примітка. Критично важливо мати чинні, стандартні процедури, які використовують затверджені інструменти, разом з гарною документацією та DEFR, який пройшов навчання та має відповідний досвід.

Збирання та здобуття потенційних цифрових доказів від мережевих мобільних пристроїв ускладнено, оскільки вони можуть існувати в багатьох станах та режимах взаємодії, таких як Bluetooth, радіочастотному, сенсорному та інфрачервоному. В доповнення, різні виробники мобільних пристроїв використовують різні типи операційних систем, які потребують різних методів здобуття доказів. Існує також широкий діапазон карт пам`яті, що використовуються в мобільних пристроях, та видалення цих карт пам`яті з увімкнених мобільних пристроїв може взаємодіяти з процесами, що запущені.

Зазвичай, мобільні пристрої, такі як PDA та мобільні телефони повинні бути увімкненими для того, щоб здобути потенційні цифрові докази. Ці пристрої можуть безперервно змінювати своє операційне середовище, коли вони увімкнені, наприклад, може бути оновленим час. Пов`язаною проблемою є то, що дві копії цифрових доказів одного і того ж пристрою можуть не пройти стандартні функції верифікації, такі як розрахунок кеш. В такій ситуації можуть бути застосовані 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 повинні залишатися працюючими для подальшого аналізу 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 їх активність . Якщо така необхідність відсутня, пристрої повинні збиратися як описано нижче:

- DEFR повинен ізолювати пристрій від мережі, коли відомо, що потрібні дані будуть перезаписані за допомогою такій дії та це не призведе до неправильного функціонування важливих систем (таких як системи керування обладнанням в 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 відслідкувати підключення до цифрових пристроїв та позначити порти для подальшої реконструкції мережі в цілому. Пристрій може мати більш ніж один метод

комунікацій. Наприклад, комп'ютер може мати дротове підключення до LAN, бездротовий модем та карти мобільного телефону. PED може бути підключений до мережі через Wi-Fi, Bluetooth з'єднання або з'єднання через мобільну телефонну мережу. DEFR повинен спробувати ідентифікувати усі методи комунікацій та застосувати відповідні дії для захисту від пошкоджень потенційних цифрових доказів.

- Слід бути обережним, оскільки видалення живлення від мережевих пристроїв в 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 цифрові докази не будуть втрачені в результаті, з'єднання від цього цифрового пристрою можуть бути видалені.

- Якщо збирання має переваги над здобуттям та відомо, що пристрій містить несталу пам'ять, пристрій повинен бути безперервно підключеним до живлення.

- Якщо мобільний пристрій вимкнений, обережно запакувати, запечатати та надайте позначки. Це надасть можливість уникнути випадкових або навмисних операцій з ключами або клавішами. В якості додатковою передбачливості, DEFR повинен також розглянути використання упаковки Фарадея або екрануючий бокс.

- В деяких обставинах мобільний пристрій повинен бути вимкненим протягом збирання для запобіганню зміненню даних. Це може бути викликано через вихідні або вхідні з'єднання або команди, які можуть викликати пошкодження потенційних цифрових доказів.

- Пізніше, кожний цифровий пристрій може оброблятися як окремий пристрій (див. розділ 7.1) протягом його досліджень.

Примітка. Можливо запровадити вид мережі з використанням пересувного пристрою для збереження як транзитне середовище. DEFR повинен розглянути чи може пристрій, що був зібраний, використовуватися таким чином та шукати інформацію стосовно інших пристроїв в такому скритному стані.

7.2.2.3 Настанови для здобуття з мережевих пристроїв

У випадках, коли цифрові пристрої підключені до мережі, існує можливість , ці прилади підключені до більш ніж однієї (1) фізичній або віртуальній мережі. Наприклад, пристрій, який , як здається, підключений до однієї (1) видимої фізичної мережі може фактично працювати у віртуальній приватній мережі (VPN) та з віртуальною машиною з більш ніж однією (1) IP адресою. У такому випадку 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 включають, але не обмежуються, IP конфігурацію та таблиці маршрутизації.

Для мережевих пристроїв, які потребують безперервного увімкненого живлення, пристрій повинен бути захищеним від взаємодії з бездротовими радіомережами, охоплюючи пристрої з GPS. DEFR повинен користуватися

методами, які дозволені локальним законодавством, для ізоляції радіосигналів. Однак, слід бути обережним для гарантування того, що пристрій має адекватне джерело живлення, оскільки методи ізоляції можуть призвести до використання додаткової енергії при спробах підключення до мережі. Методи ізоляції можуть охоплювати, але не обмежуватися, наступні:

- Використання пристроїв блокування, які можуть заблокувати передачу за допомогою створення сильної інтерференції, коли пристрій випромінює сигнали в тому самому діапазоні частот, що 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 перевірок безпечно на фіксованому місці. Екранування може бути зроблено для повного робочого місця або за допомогою встановлення тенту Фарадея, якій дозволяє зробити це портативно. Кабелі живлення в цьому тенті є проблематичними, однак, оскільки без належної ізоляції вони можуть діяти як антенна, скасовуючи цілі тенту. Робоче місце може бути також дуже обмежувальним.

- Використання екранованих робочих місць для здійснення перевірок безпечно в фіксованому місце. Радіочастотне екранування робочого простору або контейнеру (контейнер Фарадея) може бути використано для уникнення з'єднань з мережею.

Примітка 3. Усі методи блокування бездротового доступу до мереж повинні бути затверджені для використання на відповідних частотах. Таке затвердження повинно також розповсюджуватися на кабелі, які проходять через екранування.

- Використання замінника (U)SIM, який імітує ідентифікацію оригінального приладу та попереджує доступу мережі до цього пристрою. Такі карти мають змогу обдурювати цей пристрій в прийманні його за оригінальний (U)SIM та дозволяти, щоб перевірки здійснювались безпечно в будь-якому місці. (U)SIM повинен 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, ідентифікація передплатника або номер телефону). Однак, така інформація не завжди легко доступна, коли процес координації та підтвердження може заподіяти затримку.

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 прискорювання процесу перевірки (наприклад, там, де вважається, що пристрій може бути захищеним PIN та/або PUK, що потребує значного часу для їх 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. розділ 7.1.4 для детальній настанови стосовно збереження пристроїв.

7.3 Збирання, здобуття та збереження для CCTV

DEFR повинен розуміти, що підхід до вилучення відеопослідовностей з комп'ютеру, який вбудований до DRV CCTV системи відрізняється від вилучення звичайного здобуття цифрових доказів з комп'ютеру. Нижче наведені специфічні настанови для здобуття потенційних цифрових доказів з CCTV систем:

- Перед початком процесу здобуття DEFR повинен з початку визначити чи задокументувала система відео послідовність, що викликає інтерес. Потім DEFR повинен визначити фрагмент часу відео матеріалу, що потрібний, 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 для того, щоб визначити правильну відповідь програмного забезпечення.
- DEFR повинен здобути усі записи усіх доречних камер протягом часу, який викликає інтерес, для збереження інформації, що буде додатково досліджена пізніше. DEFR повинен записати усі камери, що підключені до системи та визначити чи дійсно вони вели записи або не вели записи.

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 відео послідовність буде залишатися в системі перед тим, як вона буде втрачена. Ця дія повинна бути зроблена для гарантування того, що доказ не був змінений. Для цифрових відео доказів захист записів повинен бути зроблений на місці.

- Існує декілька опцій, які DEFR може обрати для здобуття потенційних цифрових доказів від CCTV систем:

1) Здобути відео файли за допомогою записи їх на CD/DVD/Blu-ray диск, але це може бути непрактичним, якщо відео файли занадто великі.
2) Здобути відео файли за допомогою записи їх на зовнішній носій для збереження цифрових даних.
3) Здобути відео файли через мережеве з'єднання. Це може бути зроблено, якщо CCTV система обладнана мережевим портом.
4) Застосувати здатність CCTV системи до експорту відео файлів в інші формати (зазвичай MPEG або AVI), які є зжатою версією відео послідовності. Це може бути використано тільки як остання спроба, оскільки відновлення із зжатого стану може змінити оригінальні дані та завжди вилучає деталі зображення. Не рекомендується залучати відновлені дані для перевірки, якщо існують оригінальні дані та вони доступні для аналізу.

Примітка 1. Якість вилученою відео послідовності може не такій гарною,як якість оригіналу.

5) Там, ще неможливо пряме здобуття цифрових доказів за допомогою копіювання файлів на пристрої, що їх записав, DEFR та DES повинні спробувати здобути аналогові копії з аналогового виходу, який існує на оригінальному пристрої, що здійснив запис, з використання доречних аналогових пристроїв для записи.

- Протягом комплектації здобуття, здобуті файли повинні бути перевірені для підтвердження того, що були здобуті правильні файли або частини файлів. Файли повинні бути також перевірені за допомогою програмного забезпечення програвача (для форматів файлів цифрових пристроїв) для можливості їх 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 з CCTV системи разом із даними.
- Носій для збереження цифрових даних, який містить здобуті файли, повинен оброблятися як мастер-копія цифрових доказів. Якщо файли були завантажені на ноутбук або карту пам'яті/USB пристрій, тоді постійна мастер-копія повинна бути зроблена з цих пристроїв як найскоріше.
- Потім DEFR повинен перезавантажити CCTV систему, якщо вона була вимкнена. Це повинно бути зроблено в присутності авторизованих осіб.

У випадках, коли непрактично виконувати здобуття на місці, DEFR може прийняти рішення стосовно збирання носіїв для збереження цифрових даних. Швидким методом є заміна жорсткого диску 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 з системою та сумісність вилученого дисководу жорсткого диску з іншими системами для досліджень.

Примітка 2. Деякі системи мають пересувної дисковод жорсткого диску в кеді, але такий дисковод може потребувати обладнання системи для програвання.

Якщо жоден з наведених вище методів є неможливим, тоді CCTV система в цілому повинна бути вилучена в місця інциденту та процес здобуття повинен виконуватися 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. Знов, DEFR повинен оцінити ризики стосовно законодавчого прийняття та гарантії перед вилученням системи.

З урахуванням природи цифрових пристроїв та потенційних цифрових доказів, настанови для збереження CCTV системи подібні збереженню комп'ютерів, периферійних пристроїв та носіїв для збереження цифрових даних. Див. розділ 7.1.4 для детальній настанови стосовно збереження пристроїв.

ПЕРЕЛІК ВИКОРИСТАНИХ ТА РЕКОМЕНДОВАНИХ ДЖЕРЕЛ.

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

2. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

3. Кримінальний процесуальний кодекс України: Закон України від 03.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

4. Про організацію діяльності слідчих підрозділів Національної поліції України Наказ МВС України від 06.07.2017 № 570. URL: https://zakon.rada.gov.ua/laws/show/z0918-17#Text

5. Про електронні документи та електронний документообіг. Закон України від 22 травня 2003 року № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

6. Про затвердження Інструкції «Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні»: наказ Генеральної прокуратури України, МВС, СБУ, Адміністрації ДПС, Мінфіну, Мінюсту України від 16.11.12 р. №114/1042/516/1199/936/1687/5. URL:https://zakon.rada.gov.ua/laws/show/v0114900-12#Text

7. ДСТУ ISO/IEC 27037:201_ (ISO/IEC 27037:2012) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів»

8. Розслідування колабораційної діяльності : практ. посібник / Є. О. Письменський, С. В. Головкін, А. В. Коваленко, В. В. Коваленко. Київ : ВД Дакор, 2023. С. 102 – 106.

9. Злочинна колаборація в умовах збройної агресії : практич. порадник з кримінально-правової оцінки та розмежування / за заг. ред. В. В. Малюка. Київ : Алерта, 2023. С. 105)

10. Письменський Є.О. Громадянин України як суб'єкт колабораційної діяльності. *Протидія кримінальним правопорушенням на деокупованих територіях* : збірник матеріалів Всеукраїнської науково-практичної конференції (м. Кропивницький, 27 жовтня 2023 року). Кропивницький, 2023. С. 16 – 20.

11. Письменський Є. О. Особливості кваліфікації колабораційної діяльності за ознаками суб'єктивної сторони. *Протидія проявам тероризму та колабораціонізму в умовах війни: стан та перспективи*: матеріали Всеукраїнського круглого столу (м. Кропивницький, 24 листопада 2023 року). Донецький державний університет внутрішніх справ. Кропивницький, 2023. С. 21 – 25.

12. Письменський Є. О. Особливості кваліфікації колабораційної діяльності за ознакою добровільності. *Актуальні проблеми кримінального права* : матеріали XII Всеукр. наук.-теорет. конф., присвяч. пам'яті проф. П. П. Михайленка (Київ, 23 листоп. 2023 р.) / [редкол.: В. В. Чернєй,

С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ : Нац. акад. внутр. справ, 2023. С. 167 – 170.

13. Письменський Є. О. Ідеологічний та культурно-освітній колабораціонізм як посягання на інформаційну безпеку (на прикладі ч. 1 ст. 111–1 КК України). *Кримінально-правова охорона інформаційної безпеки* : матеріали VI міжнар. наук.-практ. конференції, м. Харків, 12 трав. 2022 р. / [редкол.: Л.М. Демидова (голов. ред.) та ін.]. Харків : Право, 2022. С. 82 – 85.

14. Письменський Є.О. Деякі особливості суспільно небезпечного діяння у складі колабораційної діяльності в адміністративній сфері. *Теоретичні та практичні проблеми розвитку кримінального права і процесу* : матеріали XII Всеукраїнського науково-практичного семінару (м. Івано-Франківськ, 8 грудня 2023 р.). Івано-Франківськ : Редакційно-видавничий відділ Університету Короля Данила, 2023. С. 95 – 99.

15. Письменський Є. О. Особливості кваліфікації колабораційної діяльності у формі передачі матеріальних ресурсів ворогові. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2023. Спеціальний випуск. № 2. С. 158 – 164.

16. Кравчук О., Бондаренко М. Колабораційна діяльність: науково-практичний коментар до нової статті 111-1 КК. *Юридичний науковий електронний журнал*. 2022. № 3. С. 200; Науково-практичний коментар Кримінального кодексу України / за заг. ред. І. М. Копотуна. Київ : «К Н Т», 2023. С. 211.

17. Левчук-Микитюк А. Визначення суб'єкта складу злочину «державна зрада». *Підприємництво, господарство і право*. 2020. № 4. С. 306 – 307.

18. Симоненко Н. О. Кримінально-правова новела щодо колабораційної діяльності. *Вісник асоціації кримінального права України*. 2022. № 1 (17). С. 99. URL : http://vakp.nlu.edu.ua/article/view/257848.

19. Колабораційна діяльність: загальні засади кримінально-правової кваліфікації : практич. порадник / О. О. Буряк, О. І. Букрєєв, Д. О. Олєйніков, М. В. Членов / за заг. ред. засл. юриста України А. З. Швеця. Харків : Право, 2022. С. 30.

20. Методичні рекомендації з питань кримінально-правової кваліфікації, оперативно-розшукової діяльності та кримінального провадження за ст. 111-1 КК України «Колабораційна діяльність» / С. Албул, Т. Волошанівська, А. Марченко, Г. Мудрецька, Г. Резніченко, І. Федоров, І. Чекмарьова. Одеса : ОДУВС, 2022. 67 с. URL : https://dspace.oduvs.edu.ua/bitstream/123456789/2780/1/Метод%20Колаборація%202022.pdf

21. Загиней-Заболотенко З. А., Присяжнюк І. І., Чаплюк О. І. Вчинення дій, спрямованих на впровадження стандартів освіти держави-агресора у закладах освіти як форма колабораційної діяльності. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2023. Вип. 79: ч. 2. С. 172– 173.

22. Дякур М. Д., Шевчук А. В. Щодо матеріального забезпечення як форми колабораційної діяльності в умовах воєнного стану. *ІІ Наукові читання пам'яті*

Ганса Гросса : збірник тез Міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2022 р.). Чернівці : Чернівец. нац. у-нт ім. Ю. Федьковича, 2023. С. 148.

23. Антонюк Н. Державна зрада і колабораційна діяльність: питання кримінально-правової кваліфікації. *Слово Національної школи суддів України*. 2021. № 4 (37). С. 63.

24. Тимчишен А. М. Спеціальні знання у кримінальному процесі України: теорія та практика : дис. докт. юр. наук : 12.00.09 / Донецький державний університет внутрішніх справ. Кропивницький, 2023. 438с. URL: https://dnuvs.ukr.education/wp-content/uploads/2023/10/dysertacziya_tymchyshyn.pdf

25. Криміналістика : Мультимедійний підручник / П.Є Антонюк, А.О. Антощук, О.О. Вакулик та ін. Київ, 2021. Національна академія внутрішніх справ. URL:https://arm.naiau.kiev.ua/books/criminalistics/info/lec21.html#:~:text

26. Криміналістичне забезпечення розслідування кримінальних проступків/ кол. авторів; за заг. ред. В.В. Чернєя, [Текст]: практ. посіб. – Київ:, 2022. – 177 с.

27 Мальгіна А.С. Використання методики розслідування участі у терористичній групі чи терористичній організації під час розслідування колабораційної діяльності. *Актуальні питання кримінально-правової кваліфікації, документування та розслідування колабораціонізму :* матеріали Всеукраїнської науково-практичної конференції (Одеса, 21 липня 2022 року). Одеса, 2022. С. 61–65.

28. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

29. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін. ; за заг. ред. О.В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. С. 38.

30. Актуальні проблеми при розслідуванні кримінальних проступків, пов'язаних з колабораційною діяльністю : методичні рекомендації / розроб.: Г. Тетерятник, Г. Мудрецька, Г. Резніченко. — Одеса : Видавництво «Юридика», 2023. — 40 с.

31. Черемнова А. І., Бєлік Л. С. Цифрова інформація як об'єкт експертного дослідження в умовах діджиталізації: проблема та перспективи розвитку. *Криміналістика і судова експертиза*. 2023. № 68. С. 61-62.

32. Пиріг І. В., Бідняк Г. С. Використання спеціальних знань на досудовому розслідуванні: навч. посібник. Дніпро.Дніпроп. держ. ун-т внутр. справ, 2019. 140 с.

33. Особливості проведення огляду місця події в умовах збройного конфлікту : методичні рекомендації / С. В. Обшалов, Д. Б. Санакоєв, К. О. Чаплинський та ін. ; Дніпропетровський державний університет внутрішніх справ. Одеса : Видавництво «Юридика», 2023. 40 с.

34. Пиріг І. В. Використання спеціальних знань при розслідуванні злочинів, учинених в умовах воєнного стану. *Науковий вісник Дніпропетровського державного університету внутрішніх справ: Науковий журнал.* 2022. Спеціальний випуск № 2 (121). С. 348-353. DOI: 10.31733/2078-3566-2022-6-348-353.

35. Про судову експертизу: Закон України від 25.02.1994 № 4038-XII (зі змінами та доповненнями) // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/4038-12 (дата звернення: 01.08.2024).

36. Авдєєва Г. Цифрові докази у кримінальному провадженні. Omul, criminologia, știința. Culegerea materialelor științifice elaborate în baza comunicărilor de la Conferința științifică internațională, 40 de ani de activitate pe făgașul învățământului și științei și 65 de ani de viață a criminologului Valeriu Bujor, 24 martie 2023, Chișinău. Ediția a 2-a, Vol. 1, 2023. P. 374.

37. Кобець М. В. Апаратно-програмний комплекс «Cellebrite Ufed» як засіб отримання інформації з мобільних терміналів. Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану : матеріали міжвідом. наук.-практ. конф. (Київ, 30 берез. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 70–73.

38. Розслідування колабораційної діяльності: практичний посібник \ Є.О. Письменний, С.В. Головкін, А.В. Коваленко, В.В. Коваленко. Київ : Дакор, 2024. С. 221.

39. Розслідування колабораційної діяльності: практичний посібник \ Є.О. Письменний, С.В. Головкін, А.В. Коваленко, В.В. Коваленко. Київ : Дакор, 2024. С. 222.

40. Вирок Жовтоводського міського суду Дніпропетровської області від 07 квітня 2023 року у справі №176/694/23. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/110107356 (дата звернення: 01.08.2024).

41. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: наказ Міністерства юстиції України URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (дата звернення: 06.08.2024).

42. Харитонова О. І. Авторське право та авторознавча лінгвістична експертиза у цифрову добу: монографія. Одеса: Фенікс, 2017. С. 125.

43. Вирок Червонозаводського районного суду м. Харкова від 17.10.2023 у справі № 646/1971/23. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/114252516 (дата звернення: 01.08.2024).

44. Тюлєнєв С. А. Можливості почеркознавчої експертизи у розслідуванні рейдерства. *Вісник Одеського науково-дослідного інституту судових експертиз Міністерства юстиції України.* 2023. №14. С. 37.

45. Коваленко В. В. Стан використання можливостей судових експертиз під час розслідування колабораційної діяльності (за матеріалами судово-слідчої

практики). *Вісник Луганського навчально-наукового інституту імені Е. О. Дідоренка*. 2024. № 1. С. 304.

46. Доказування злочинів про колаборaційну діяльність: проблемні питання закону. Українська гельсінська спілка з прав людини. URL: https://www.helsinki.org.ua/articles/dokazuvannia-zlochyniv-pro-kolaboratsiynu-diialnist-problemni-pytannia-zakonu/ (дата звернення: 01.08.2024).

47. Про організацію проведення слідчих дій зі збору та збереження цифрової інформації з відкритих джерел: лист-орієнтування Офісу Генерального прокурора керівникам обласних прокуратур від 28.08.2021 № 18/1-386. URL: https://zakononline.com.ua/documents/show/500229___686193 (дата звернення: 01.08.2024).

48. Яновська О. Докази та доказування у кримінальному провадженні в умовах воєнного стану: практика Верховного Суду. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2022_prezent/2022_09_28_Ianovska_.pdf (дата звернення: 01.08.2024).