ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27037— 2014

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме

ISO/IEC 27037:2012

Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») и Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 09 сентября 2014 г. № 1028-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27037:2012 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме» (ISO/IEC 27037:2012 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

В Российской Федерации настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Обозначения и сокращения 4
5 Общий обзор 5
5.1 Контекст сбора свидетельств, представленных в цифровой форме 5
5.2 Принципы, касающиеся свидетельств, представленных в цифровой форме 5
5.3 Требования к обращению со свидетельствами, представленными в цифровой форме 5
5.4 Процессы обработки свидетельств, представленных в цифровой форме 7
6 Ключевые компоненты идентификации, сбора, получения и сохранения свидетельств, представленных в цифровой форме 9
6.1 История хранения 9
6.2 Меры предосторожности на месте инцидента 10
6.3 Роли и обязанности 11
6.4 Компетентность 12
6.5 Применение разумной осторожности 12
6.6 Документирование 13
6.7 Инструктаж 13
6.8 Установление приоритетов для сбора и получения свидетельств 15
6.9 Сохранение потенциальных свидетельств, представленных в цифровой форме 15
7 Примеры идентификации, сбора, получения и сохранения свидетельств 18
7.1 Компьютеры, периферийные устройства и цифровые носители данных 18
7.2 Сетевые устройства 28
7.3 Принципы сбора, получения и сохранения для CCTV 32
Приложение А (справочное) Описание основных навыков и компетентности DEFR 35
Приложение В (справочное) Минимальные требования к документации для передачи свидетельств 38
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации 39
Библиография 40

Введение

Настоящий стандарт предоставляет руководства по конкретным процессам при обращении с потенциальными свидетельствами, представленными в цифровой форме; этими процессами являются: идентификация, сбор, получение и сохранение потенциальных свидетельств, представленных в цифровой форме. Эти процессы необходимы при проведении расследования и предназначены для поддержки целостности свидетельств, представленных в цифровой форме, т. е. являются приемлемой методикой получения свидетельств, представленных в цифровой форме, которая будет способствовать их допустимости для правовых и дисциплинарных действий, а также для других необходимых случаев. Настоящий стандарт также предоставляет общее руководство по сбору свидетельств, не представленных в цифровой форме, которые могут быть полезны на этапе анализа потенциальных свидетельств, представленных в цифровой форме.

Настоящий стандарт предназначен для предоставления руководства лицам, отвечающим за идентификацию, сбор, получение и сохранение потенциальных свидетельств, представленных в цифровой форме. К таким лицам относятся специалисты «оперативного реагирования» по свидетельствам, представленным в цифровой форме, специалисты по свидетельствам, представленным в цифровой форме, специалисты по реагированию на инциденты и руководители лабораторий судебной экспертизы. Настоящий стандарт обеспечивает уверенность в том, что ответственные лица осуществляют менеджмент потенциальных свидетельств, представленных в цифровой форме, рациональными общепризнанными способами, чтобы систематически и беспристрастно содействовать расследованию, использующему цифровые устройства и свидетельства, представленные в цифровой форме, сохраняя при этом их целостность и подлинность.

Данный стандарт также предназначен для информирования лиц, принимающих решения, которым необходимо определять достоверность передаваемых им свидетельств, представленных в цифровой форме. Он применим для организаций, нуждающихся в защите, анализе и представлении потенциальных свидетельств, представленных в цифровой форме. Он важен для директивных органов, которые создают и оценивают процедуры, связанные со свидетельствами, представленными в цифровой форме, часто являющимися частью более крупной совокупности свидетельств.

Упоминаемые в настоящем стандарте потенциальные свидетельства, представленные в цифровой форме, могут быть получены из различных цифровых устройств, сетей, баз данных и т. д. Они относятся к данным, уже имеющим цифровой формат. Настоящий стандарт не пытается охватить вопрос преобразования аналоговых данных в цифровой формат.

Вследствие недолговечности свидетельств, представленных в цифровой форме, необходимо использовать приемлемую методику, обеспечивающую уверенность в сохранении целостности и подлинности потенциальных свидетельств, представленных в цифровой форме. Настоящий стандарт не предписывает использование конкретных инструментальных средств или методов. Ключевыми доверенными компонентами при расследовании являются применяемая во время процесса методика и лица, компетентные в выполнении задач, указанных в методике. Настоящий стандарт не рассматривает методику процессуальных действий, дисциплинарных процедур и других, связанных с ними действий при обращении со свидетельствами, представленными в цифровой форме, которые выходят за рамки идентификации, сбора, получения и сохранения.

Применение настоящего стандарта требует соблюдения национальных законов, правил и предписаний. Он не должен заменять конкретные правовые требования любой юрисдикции. Вместо этого настоящий стандарт может послужить практическим руководством для любых специалистов «оперативного реагирования» по свидетельствам, представленным в цифровой форме, или специалистов по свидетельствам, представленным в цифровой форме, в расследованиях с использованием потенциальных свидетельств, представленных в цифровой форме. Он не распространяется на анализ свидетельств, представленных в цифровой форме, и не заменяет специфичных для юрисдикции требований, которые относятся к таким вопросам, как допустимость, доказательная весомость, обоснованность и другим, регулируемым в судебном порядке ограничениям на использование потенциальных свидетельств, представленных в цифровой форме, в судах общей юрисдикции. Настоящий стандарт может способствовать упрощению обмена потенциальными свидетельствами, представленными в цифровой форме, между юрисдикциями. Чтобы поддерживать целостность свидетельств, представленных в цифровой форме, пользователям настоящего стандарта необходимо адаптировать и внести поправки в представленные в настоящем стандарте процедуры на основе правовых требований к свидетельствам в конкретной юрисдикции.

Несмотря на то, что настоящий стандарт не касается вопросов подготовленности к судебным разбирательствам, адекватная подготовленность к судебным разбирательствам может существенно способствовать процессу идентификации, сбора, получения и сохранения свидетельств, представленных в цифровой форме. Подготовленность к судебным разбирательствам – это достижение организацией соответствующего уровня возможностей, который позволяет ей идентифицировать, собирать, получать, хранить, защищать и анализировать свидетельства, представленные в цифровой форме. Поскольку описанные в настоящем стандарте процессы и действия по существу являются реагирующими мерами, используемыми для расследования инцидента после его наступления, готовность к судебным разбирательствам – это упреждающий процесс попытки планирования каких-либо действий со стороны организации до наступления таких событий.

Предоставляя дополнительное руководство по реализации, настоящий стандарт дополняет ИСО/МЭК 27001 и ИСО/МЭК 27002, в частности, требованиями мер и средств контроля и управления, касающимися получения потенциальных свидетельств, представленных в цифровой форме. Кроме того, настоящий стандарт будет иметь применение в контексте, независимом от ИСО/МЭК 27001 и ИСО/МЭК 27002. Настоящий стандарт следует рассматривать совместно с другими стандартами, связанными со свидетельствами, представленными в цифровой форме, и расследованиями инцидентов информационной безопасности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме

Information technology. Security techniques.
Guidelines for identification, collection, acquisition and preservation of digital evidence

Дата введения — 2015—11—01

1 Область применения

Настоящий стандарт предоставляет руководства по конкретным видам деятельности, касающимся обращения со свидетельствами, представленными в цифровой форме, к которым относится идентификация, сбор, получение и сохранение потенциальных свидетельств, представленных в цифровой форме, которые могут иметь доказательную ценность. Настоящий стандарт предоставляет руководство по распространенным ситуациям, возникающим в процессе обращения со свидетельствами, представленными в цифровой форме, а также содействует организациям в их дисциплинарных процедурах и в облегчении обмена потенциальными свидетельствами, представленными в цифровой форме, между юрисдикциями.

Настоящий стандарт предоставляет рекомендации относительно следующих устройств и (или) функций, используемых при различных обстоятельствах:

- цифровые носители данных, используемые в типовых компьютерах, например, жесткие диски, дискеты, оптические и магнитооптические диски, устройства с аналогичными функциями;
- мобильные телефоны, «карманные» персональные компьютеры, персональные электронные устройства, карты памяти;
- мобильные навигационные системы;
- цифровые фотоаппараты и видеокамеры (включая системы видеонаблюдения);
- типовые компьютеры с сетевыми соединениями;
- сети на основе протоколов TCP/IP и других цифровых протоколов;
- устройства с функциями, аналогичными перечисленным.

Примечание 1 – Приведенный выше перечень устройств является примерным и неисчерпывающим перечнем.

Примечание 2 – Применение перечисленных выше устройств, которые существуют в различных формах, обусловлено обстоятельствами. Например, автомобильная система может включать мобильное навигационное устройство, устройство хранения данных и систему сенсоров.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных документов используют только указанное издание. Для недатированных документов используют самое последнее издание ссылочного документа (с учетом всех его изменений).

Издание официальное

ИСО/ТО 15801 Управление документацией. Хранение информации в электронном виде. Рекомендации по достоверности и надежности (ISO/TR 15801, Document management – Information stored electronically – Recommendations for trustworthiness and reliability)

ИСО/МЭК 17020 Оценка соответствия. Требования к работе различных типов контролирующих органов (ISO/IEC 17020, Conformity assessment – Requirements for the operation of various types of bodies performing inspection)

ИСО/МЭК 17025:2005 Общие требования к компетентности испытательных и калибровочных лабораторий (ISO/IEC 17025:2005, General requirements for the competence of testing and calibration laboratories)

ИСО/МЭК 27000 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология (ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary).

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000, ИСО/МЭК 17020, ИСО/МЭК 17025 и ИСО/ТО 15801, а также следующие термины с соответствующими определениями.

3.1 **получение свидетельства** (acquisition): Процесс создания копии данных в рамках определенной совокупности.

Примечание – Результатом получения свидетельства является экземпляр потенциального свидетельства, представленного в цифровой форме.

3.2 **выделенное пространство** (allocated space): Область на цифровом носителе, включая основную память, которая используется для хранения данных, в том числе метаданных.

3.3 **сбор** (collection): Процесс сбора физических элементов, которые содержат потенциальные свидетельства, представленные в цифровой форме.

3.4 **цифровое устройство** (digital device): Электронное оборудование, используемое для обработки или хранения данных, представленных в цифровой форме.

3.5 **свидетельства, представленные в цифровой форме** (digital evidence): Информация или данные, хранящиеся или передаваемые в виде двоичного кода, которые можно использовать в качестве доказательства.

3.6 **копия свидетельства, представленного в цифровой форме** (digital evidence copy): Копия свидетельства, представленного в цифровой форме, которая была создана для поддержки достоверности доказательства посредством включения свидетельства, представленного в цифровой форме, и средства верификации, причем способ верификации может быть встроенным в инструментальные средства, используемые для осуществления верификации, или независимым от них.

3.7 **специалист «оперативного реагирования» по свидетельствам, представленным в цифровой форме; DEFR** (digital evidence first responder): Физическое лицо, которое уполномочено, обучено и подготовлено действовать первым на месте инцидента, осуществляя сбор и получение свидетельств, представленных в цифровой форме, и которое несет ответственность за обращение с этими свидетельствами.

Примечание – Полномочия, обучение и подготовка являются ожидаемыми требованиями, необходимыми для получения достоверных свидетельств, представленных в цифровой форме, но отдельные обстоятельства могут приводить к тому, что физическое лицо не будет соответствовать всем трем требованиям. При этом должны быть рассмотрены местное законодательство, политика организации и конкретные обстоятельства.

3.8 **специалист по свидетельствам, представленным в цифровой форме; DES** (digital evidence specialist): Физическое лицо, которое может выполнять задачи специалиста «оперативного реагирования» по свидетельствам, представленным в цифровой форме, и которое обладает специальными знаниями, навыками и способностями, чтобы разбираться в широком спектре технических вопросов.

Примечание – Специалист по свидетельствам, представленным в цифровой форме, может обладать дополнительными навыками, например, знанием получения свидетельств из сетей, ОЗУ, программных средств операционной системы или из мэйнфрейма.

3.9 **цифровой носитель данных** (digital storage medium): Устройство, на котором могут быть записаны цифровые данные.

[Адаптировано из ИСО/МЭК 10027:1990]

3.10 **средство сохранения свидетельств** (evidence preservation facility): Безопасная среда или место, где хранятся собранные или полученные свидетельства.

Примечание – Средство для сохранения свидетельств не должно подвергаться воздействию магнитных полей, пыли, вибрации, влаги или любых других факторов внешней среды (таких как экстремальная температура или влажность), которые могут повредить потенциальные свидетельства, представленные в цифровой форме.

3.11 **значение хэш-функции** (hash value): Битовая строка, являющаяся выходным результатом хэш-функции.

[ИСО/МЭК 10118–1:2000]

3.12 **идентификация** (identification): Процесс, включающий поиск, распознавание и документирование потенциальных свидетельств, представленных в цифровой форме.

3.13 **создание образа** (imaging): Процесс создания побитовой копии цифрового носителя данных.

Примечание – Побитовая копия также называется физической копией.

Пример – При создании образа жесткого диска специалист «оперативного реагирования» по свидетельствам, представленным в цифровой форме, будет также копировать данные, которые были удалены.

3.14 **периферийное устройство** (peripheral): Устройство, подключенное к цифровому устройству для расширения его функциональных возможностей.

3.15 **сохранение** (preservation): Процесс поддержки и защиты целостности и (или) исходного состояния потенциальных свидетельств, представленных в цифровой форме.

3.16 **достоверность** (reliability): Свойство соответствия предусмотренному поведению и результатам.

[ИСО/МЭК 27000:2009]

3.17 **повторяемость** (repeatability): Свойство процесса получать такие же результаты тестирования в той же тестовой среде (тот же компьютер, жесткий диск, режим работы и т. д.).

3.18 **воспроизводимость** (reproducibility): Свойство процесса получать такие же результаты тестирования в другой тестовой среде (другой компьютер, жесткий диск, оператор и т. д.).

3.19 **повреждение** (spoliation): Осуществление или признание осуществления изменения(й) потенциальных свидетельств, представленных в цифровой форме, уменьшающее их доказательную ценность.

3.20 **системное время** (system time): Время, генерируемое системными часами и используемое операционной системой, а не время, вычисляемое операционной системой.

3.21 **фальсификация** (tampering): Намеренное осуществление или признание осуществления изменения(й) свидетельств, представленных в цифровой форме (т. е. умышленное или намеренное повреждение).

3.22 **метка времени** (timestamp): Меняющийся временной параметр, обозначающий момент времени относительно обычного начала отсчета времени.

[ИСО/МЭК 11770–1:1996]

3.23 **свободное пространство** (unallocated space): Область на цифровом носителе, включая основную память, которая никому не была выделена в операционной системе, и которая доступна для хранения данных, включая метаданные.

3.24 **валидация** (validation): Подтверждение посредством представления объективных свидетельств того, что требования, предназначенные для конкретного использования или применения, были выполнены.

[ИСО/МЭК 27004: 2009]

3.25 **функция верификации** (verification function): Функция, используемая для подтверждения идентичности двух совокупностей данных.

Примечание 1 – Никакие две неидентичные совокупности данных не должны быть представлены идентичными при использовании функции верификации.

Примечание 2 – Функции верификации обычно реализуются с использованием хэш-функций, таких как MD5, SHA1 и т. д., но могут быть использованы и другие методы.

3.26 **изменчивые данные** (volatile data): Данные, которые особенно уязвимы к изменению и могут быть легко модифицированы.

Примечание – Изменение может быть вызвано отключением электропитания или прохождением через магнитное поле. К изменчивым данным также относятся данные, меняющиеся при изменении состояния системы. Например, данные, хранящиеся в ОЗУ, и динамические IP-адреса.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения и условные обозначения:

AVI – Audio Video Interleave (формат файлов для хранения и воспроизведения видеофильмов, синхронизированных со звуком);
CCTV – Closed Circuit Television (замкнутая телевизионная система; система видеонаблюдения);
CD – Compact Disk (компакт-диск);
DEFR – Digital Evidence First Responder (специалист «оперативного реагирования» по свидетельствам, представленным в цифровой форме);
DES – Digital Evidence Specialist (специалист по свидетельствам, представленным в цифровой форме);
DVD – Digital Video/Versatile Disk (цифровой видео/многофункциональный диск);
ESN – Electronic Serial Number (электронный серийный номер);
GPS – Global Positioning System (глобальная система определения местоположения);
GSM – Global System for Mobile Communication (глобальная система мобильной связи);
IMEI – International Mobile Equipment Identity (международный идентификатор мобильного оборудования);
IP – Internet Protocol (протокол Интернет);
ISIRT – Information Security Incident Response Team (группа реагирования на инциденты информационной безопасности);
MD5 – Message-Digest Algorithm 5 (алгоритм свертки (хеширования) сообщения 5);
MP3 – MPEG Audio Layer 3 (формат звуковых файлов с компрессией 3 по технологии MPEG);
MPEG – Moving Picture Experts Group (экспертная группа по разработке спецификаций цифрового кодирования видео и аудиосигналов);
NAS – Network Attached Storage (сетевая система хранения данных);
PDA – Personal Digital Assistant («карманный» персональный компьютер);
PED – Personal Electronic Device (персональное электронное устройство);
PUK – PIN Unlock Key (ключ разблокировки PIN-кода);
RAID – Redundant Array Independent Disk (матрица независимых дисковых накопителей с избыточностью);
RFID – Radio Frequency Identification (радиочастотная идентификация);
SAN – Storage Area Network (сеть с выделенной зоной хранения данных);
SHA – Secure Hash Algorithm (алгоритм аутентификации и проверки целостности информации);
SIM – Subscriber Identity Module (модуль идентификации абонента; SIM-карта);
USB – Universal Serial Bus (универсальная последовательная шина);
Wi-Fi – Wireless Fidelity («беспроводная точность»; технология беспроводного обмена данными);
ДНК – дезоксирибонуклеиновая кислота (Deoxyribonucleic Acid — DNA);
ИБП – источник бесперебойного питания (Uninterruptible Power Supply — UPS);
ЛВС – локальная вычислительная сеть (Local Area Network — LAN);
ОЗУ – оперативное запоминающее устройство (Random Access Memory — RAM);
ПИН – персональный идентификационный номер (Personal Identification Number — PIN);
УФ – ультрафиолетовое излучение (Ultraviolet — UV).

5 Общий обзор

5.1 Контекст сбора свидетельств, представленных в цифровой форме

Использование свидетельств, представленных в цифровой форме, может требоваться в целом ряде различных сценариев, каждый из которых характеризуется соотношением между достижением качества доказательств, своевременностью анализа, восстановлением услуг и расходами на сбор свидетельств, представленных в цифровой форме. Поэтому организациям необходим процесс установления приоритетов, идентифицирующий потребности и соотношение качества доказательств, своевременность анализа и восстановления услуг, прежде чем перед DEFR будет поставлена соответствующая задача. Процесс установления приоритетов включает оценивание доступного материала для определения возможной доказательной ценности и порядка, в соответствии с которым должен осуществляться сбор/получение/сохранение потенциальных свидетельств, представленных в цифровой форме. Установление приоритетов осуществляется для сведения к минимуму риска повреждения потенциальных свидетельств, представленных в цифровой форме и максимального увеличения доказательной ценности собранных потенциальных свидетельств, представленных в цифровой форме.

5.2 Принципы, касающиеся свидетельств, представленных в цифровой форме

В большинстве юрисдикций и организаций свидетельства, представленные в цифровой форме, обусловлены тремя основополагающими принципами: значимость, достоверность и достаточность. Эти три принципа важны для всех расследований, а не только для случаев, когда свидетельства, представленные в цифровой форме, могут быть приемлемы в суде. Свидетельства, представленные в цифровой форме, являются значимыми, если они подтверждают или опровергают элемент конкретного расследуемого дела. Хотя детальное определение «достоверности» различается в разных юрисдикциях, широко поддерживается общее значение принципа «обеспечение уверенности в том, что свидетельства, представленные в цифровой форме, являются такими, как заявлено». DEFR не всегда необходимо собирать все данные или делать полную копию исходного свидетельства, представленного в цифровой форме. Во многих юрисдикциях концепция достаточности означает, что DEFR нужно собрать потенциальные свидетельства, представленные в цифровой форме, для получения возможности адекватного изучения или расследования элементов дела. Понимание этой концепции важно для DEFR, чтобы он мог надлежащим образом устанавливать приоритеты в своей работе, когда возникает вопрос времени или расходов.

Примечание – DEFR должен обеспечивать уверенность в том, что сбор потенциальных свидетельств, представленных в цифровой форме, осуществляется в соответствии с законами и предписаниями местной юрисдикции, как того требуют конкретные обстоятельства.

Все процессы, которые будут использоваться DEFR и DES, должны быть валидны (утверждены) до использования. Если валидация проводится в общем, то DEFR и DES должны подтвердить, что валидация является соответствующей для конкретного использования процессов, среды и обстоятельств, при которых процессы собираются использовать. DEFR и DES также должны:

a) документировать все действия;

b) определять и применять метод установления точности и достоверности копии свидетельств, представленных в цифровой форме, по сравнению с исходным источником;

c) сознавать, что сохранение потенциальных свидетельств, представленных в цифровой форме, не всегда может быть проведено без изменений.

5.3 Требования к обращению со свидетельствами, представленными в цифровой форме

5.3.1 Общая информация

Принципы, изложенные в 5.2, могут быть выполнены следующим образом:

- значимость: должна быть возможна демонстрация того, что полученный материал является значимым для расследования, т. е. он содержит ценную информацию для содействия расследованию конкретного инцидента и существует достаточное основание для его получения. Для проверки и обоснованности DEFR должен быть способен описать соблюдаемые процедуры и объяснить, как было принято решение о получении каждого элемента;

- достоверность: все процессы, используемые при обращении с потенциальными свидетельствами, представленными в цифровой форме, должны быть контролируемыми и повторяемыми. Результаты применения таких процессов должны быть воспроизводимыми;

- достаточность: DEFR должен принять во внимание, что было собрано достаточно данных, чтобы сделать возможным проведение надлежащего расследования. Для проверки и обоснованности DEFR должен быть способен указать, сколько данных в совокупности рассматривалось, и какие процедуры использовались для принятия решения о том, сколько и какие данные нужно получить.

Примечание – Данные могут быть собраны путем получения свидетельств и (или) осуществления мероприятий по сбору.

Существует четыре ключевых аспекта в обращении со свидетельствами, представленными в цифровой форме: контролируемость, обоснованность и либо повторяемость, либо воспроизводимость, в зависимости от конкретных обстоятельств.

5.3.2 Контролируемость

Независимый специалист по оценке или другие уполномоченные заинтересованные стороны должны иметь возможность оценивания действий, выполняемых DEFR и DES. Это достижимо путем надлежащего документирования всех предпринятых действий. DEFR и DES должны быть способны обосновать процесс принятия решения, касающегося выбора определенного порядка действий. Процессы, выполненные DEFR и DES должны быть доступны для независимой оценки с целью определения того, соблюдался ли соответствующий научный метод, технический прием или процедура.

5.3.3 Повторяемость

Факт повторяемости признается, если те же результаты теста получают при следующих условиях:

- использование такой же процедуры и метода измерений;
- использование таких же инструментальных средств и при таких же условиях;
- возможно повторение в любое время после первоначального тестирования.

Обладающий соответствующими навыками и опытом DEFR должен быть способен выполнять все процессы, описанные в документации, и прийти к тем же результатам без указаний или объяснений. DEFR должен сознавать, что могут быть обстоятельства, когда повторить тестирование невозможно, например, когда исходный жесткий диск скопирован и возвращен в использование, или когда продукт включает энергозависимую память. В этом случае DEFR должен убедиться, что процесс получения свидетельств достоверен. Для достижения повторяемости необходим контроль качества и документирование процесса.

5.3.4 Воспроизводимость

Факт воспроизводимости признается, если те же результаты теста получают при следующих условиях:

- использование такого же метода измерения;
- использование различных инструментальных средств и при различных условиях;
- возможно повторение в любое время после первоначального тестирования.

Необходимость воспроизвести результаты меняется в зависимости от юрисдикции и обстоятельств, поэтому DEFR или лицо, осуществляющее воспроизведение, должны быть осведомлены о соответствующих условиях.

5.3.5 Обоснованность

DEFR должен быть способен обосновать все действия и методы, использованные для обращения со свидетельствами, представленными в цифровой форме. Обоснование может быть достигнуто путем демонстрации того, что принятое решение было наилучшим выбором для получения всех потенциальных свидетельств, представленных в цифровой форме. С другой стороны, DEFR или DES может также продемонстрировать это, посредством успешного воспроизведения или валидации использованных действий и методов.

Организация заинтересована в найме DEFR или DES, который обладает основными навыками и компетентностью, описанными в приложении А настоящего стандарта. Это обеспечит уверенность в том, что при обращении со свидетельствами, представленными в цифровой форме, соблюдались надлежащие процессы и процедуры, обеспечивающие конечное сохранение свидетельств, представленных в цифровой форме, которые могут иметь доказательную ценность. Это также обеспечит уверенность в том, что организации могут использовать потенциальные свидетельства, представленные в цифровой форме, например, в своих дисциплинарных процедурах или в содействии обмену потенциальными свидетельствами, представленными в цифровой форме, между юрисдикциями.

Примечание – Компетенция DEFR, описанная в приложении А, ограничена функцией, которая совмещена с ролью DES, как определено в 3.8.

5.4 Процессы обработки свидетельств, представленных в цифровой форме

5.4.1 Общий обзор

Хотя полный процесс обработки свидетельств, представленных в цифровой форме, включает и другие действия (например, передача, уничтожение и т. д.), сфера рассмотрения настоящего стандарта связана только с начальным процессом обработки, состоящим из идентификации, сбора, получения и сохранения потенциальных свидетельств, представленных в цифровой форме.

По своему характеру свидетельства, представленные в цифровой форме, могут быть уязвимыми. Они могут быть изменены, фальсифицированы или разрушены в результате ненадлежащего обращения или изучения. Обработчики свидетельств, представленных в цифровой форме, должны быть компетентными в вопросе идентификации и менеджмента рисков, а также последствий возможных вариантов действий при обращении со свидетельствами, представленными в цифровой форме. Неспособность обращаться с цифровыми устройствами надлежащим образом может привести потенциальные свидетельства, представленные в цифровой форме и содержащиеся в этих цифровых устройствах, к непригодности для использования.

DEFR и DES должны следовать документированным процедурам для обеспечения уверенности в поддержке целостности и достоверности потенциальных свидетельств, представленных в цифровой форме. Указанные процедуры должны учитывать рекомендации по обращению с источниками потенциальных свидетельств, представленных в цифровой форме, и охватывать следующие основные принципы:

- сведение к минимуму обращения с исходным цифровым устройством или потенциальными свидетельствами, представленными в цифровой форме;
- учет любых изменений и документирование предпринятых действий (в такой степени, чтобы эксперт мог сформировать мнение о достоверности);
- соблюдение действующих на местах правил в отношении свидетельств;
- DEFR и DES не должны предпринимать действия, выходящие за рамки их компетентности.

Путем соблюдения базовых принципов и требований по обращению с потенциальными свидетельствами, представленными в цифровой форме, свидетельства должны быть сохранены. Все действия и логические обоснования должны документироваться, особенно в случае внесения неизбежных изменений. Каждый процесс обработки свидетельств, представленных в цифровой форме, т. е. идентификация, сбор, получение и сохранение более подробно обсуждается в нижеследующих пунктах.

5.4.2 Идентификация

Свидетельства, представленные в цифровой форме, могут быть в физическом или логическом виде. Физический вид означает представление данных в материальном устройстве. Логический вид потенциальных свидетельств, представленных в цифровой форме, относится к виртуальному представлению данных в устройстве.

Процесс идентификации включает поиск, распознавание и документирование потенциальных свидетельств, представленных в цифровой форме. В процессе идентификации должны определяться цифровые носители информации и устройства обработки, которые могут содержать потенциальные свидетельства, представленные в цифровой форме, имеющие отношение к инциденту. Данный процесс включает также действие по установлению приоритетов для сбора свидетельств, на основе их изменчивости. Для обеспечения уверенности в надлежащем порядке процессов сбора и получения свидетельств следует идентифицировать изменчивость данных, чтобы свести к минимуму ущерб для потенциальных свидетельств, представленных в цифровой форме, и получить наилучшие свидетельства. Кроме того, во время этого процесса следует идентифицировать скрытые потенциальные свидетельства, представленные в цифровой форме. DEFR и DES должны сознавать, что не все виды цифровых носителей информации могут быть легко идентифицированы и локализованы, например, облачная обработка данных, NAS и SAN добавляют виртуальный компонент к процессу идентификации.

DEFR и DES должны систематически проводить тщательный поиск элементов, которые могут содержать потенциальные свидетельства, представленные в цифровой форме. Различные виды цифровых устройств, которые могут содержать потенциальные свидетельства, представленные в цифровой форме, легко могут быть незамечены (например, из-за малого размера), скрыты или перемешаны с другим, не относящимся к делу материалом.

В 6.1 и 6.6 приводится дополнительная информация, касающаяся истории хранения и аспектов упаковки и маркировки при идентификации свидетельств, представленных в цифровой форме. В разделе 7 определены руководящие указания, относящиеся к конкретным примерам идентификации, сбора, получения и сохранения свидетельств, представленных в цифровой форме.

5.4.3 Сбор

После идентификации цифровых устройств, которые могут содержать потенциальные свидетельства, представленные в цифровой форме, DEFR и DES должны решить, будет ли осуществляться сбор или получение свидетельств в течение следующего процесса. Существует ряд влияющих на такое решение факторов, которые более детально обсуждаются в разделе 7. Решение должно быть основано на обстоятельствах.

Сбор является одним из процессов обработки свидетельств, представленных в цифровой форме, если устройства, которые могут содержать потенциальные свидетельства, представленные в цифровой форме, перемещаются из их рабочей среды в лабораторию или иную контролируемую среду для последующего получения и анализа свидетельств. Устройства, содержащие потенциальные свидетельства, представленные в цифровой форме, могут быть в одном из двух состояний: когда питание системы включено или когда питание системы выключено. В зависимости от состояния устройства требуются разные методы и инструментальные средства. К методам и инструментальным средствам, используемым для сбора данных, могут применяться специальные процедуры.

Этот процесс включает документирование всех действий, а также упаковку устройств перед их транспортировкой. Для DEFR и DES важно собрать любой материал, который может иметь отношение к потенциальной цифровой информации (например, листы бумаги с записанными паролями, подставки и силовые разъемы для встроенных устройств). При отсутствии разумной осторожности потенциальные свидетельства, представленные в цифровой форме, могут быть потеряны или повреждены. DEFR и DES должны выбрать наилучший возможный метод сбора на основе ситуации, расходов и времени, и документально оформить решение об использовании конкретного метода.

Примечание 1 – Извлечение цифровых носителей информации не всегда рекомендовано, и DEFR должен быть уверен в своей компетентности, должен осознавать необходимость и возможность выполнения этого.

Примечание 2 – В соответствии с требованиями конкретной юрисдикции должны быть документированы сведения о несобранных цифровых устройствах с обоснованием их исключения.

5.4.4 Получение свидетельств

Процесс получения свидетельств включает создание цифровой копии свидетельств, представленных в цифровой форме (например, полного жесткого диска, раздела диска, выбранных файлов), и документирование использованных методов и выполняемых действий. DEFR должен выбрать надлежащий метод получения свидетельств, исходя из ситуации, затрат и времени, и документально оформить решение об использовании конкретного метода или инструментального средства, соответственно.

Методы, используемые для получения потенциальных свидетельств, представленных в цифровой форме, должны быть четко и подробно документированы, и, насколько это практически возможно, воспроизводиться или поддаваться проверке компетентным DEFR. DEFR или DES должны получать потенциальные свидетельства, представленные в цифровой форме, безотлагательным способом, чтобы избежать, где это возможно, внесения изменений. При осуществлении этого процесса DEFR должны рассмотреть использование наиболее подходящего метода. Если в результате процесса неизбежны изменения в цифровых данных, выполняемая деятельность должна быть задокументирована для учета изменений в данных.

В процессе получения свидетельств следует создавать копию потенциального свидетельства, представленного в цифровой форме, или цифровых устройств, которые могут содержать потенциальные свидетельства, представленные в цифровой форме. И оригинал, и копия свидетельства, представленного в цифровой форме, должны быть верифицированы с помощью проверенной функции верификации (подтвержденной как точная на данный момент времени), являющейся приемлемой для лица, которое будет использовать свидетельства. И оригинал, и каждая копия свидетельства, представленного в цифровой форме, должны давать один и тот же результат при верификации.

Возможны обстоятельства, когда процесс верификации не может быть выполнен, например, при получении свидетельств в работающей системе, оригинал содержит ошибки секторов или период получения свидетельств ограничен по времени. В таких случаях DEFR должен использовать наилучший

доступный метод, и быть в состоянии обосновать и защитить выбор метода. Если создание образа не может быть проверено, то это должно быть задокументировано и обосновано. При необходимости используемый метод получения свидетельств должен иметь возможность получения выделенного и незанятого пространства.

Примечание 1 – Если процесс верификации не может быть осуществлен для источника в целом, вследствие ошибок источника, то осуществляется верификация тех частей источника, которые могут быть надежно прочитаны.

Могут быть случаи, когда невозможно или недопустимо создание копии свидетельства, представленного в цифровой форме, например, когда источник слишком велик. В таких случаях DEFR должен осуществить логическое получение свидетельства, нацеленное только на определенные типы данных, директории или адреса. Это обычно происходит на уровне файлов и разделов диска. Во время логического получения свидетельства, в зависимости от используемого метода, могут быть скопированы только активные файлы и распределенное пространство цифрового носителя информации, а удаленные файлы или нераспределенное пространство могут не копироваться. Другим примером, где такой метод может быть полезен, являются критичные для целевой задачи системы, не допускающие отключения.

Примечание 2 – Некоторые юрисдикции могут требовать особого обращения с данными, например, опечатывания в присутствии владельца данных. Опечатывание должно осуществляться в соответствии с локальными требованиями (законодательными и процессуальными).

5.4.5 Сохранение

Потенциальные свидетельства, представленные в цифровой форме, должны сохраняться для обеспечения уверенности в их полезности при расследовании Важно обеспечить защиту целостности свидетельств. Процесс сохранения включает защиту потенциальных свидетельств, представленных в цифровой форме, и цифровых устройств, которые могут содержать потенциальные свидетельства, представленные в цифровой форме, от фальсификации или повреждения. Процесс сохранения должен инициироваться и поддерживаться на протяжении всех этапов обращения со свидетельствами, представленными в цифровой форме, начиная с идентификации цифровых устройств, которые могут содержать потенциальные свидетельства, представленные в цифровой форме.

При наилучшем сценарии развития не должно быть никакого повреждения самих данных или любых связанных с ними метаданных (например, метки даты и времени). DEFR должен быть способен продемонстрировать, что свидетельства не модифицировались после их сбора или получения, или, если были внесены неизбежные изменения, предоставить логическое обоснование и документально подтвердить эти действия.

Примечание – В некоторых случаях конфиденциальность свидетельств, представленных в цифровой форме, является требованием, т. е. либо требованием бизнеса, либо правовым требованием (например, приватность). Потенциальные свидетельства, представленные в цифровой форме, должны быть сохранены способом, обеспечивающим уверенность в конфиденциальности данных.

6 Ключевые компоненты идентификации, сбора, получения и сохранения свидетельств, представленных в цифровой форме

6.1 История хранения

При любом расследовании DEFR должен нести ответственность за все полученные данные и устройства на время нахождения их в его распоряжении. Запись истории хранения – это документ, удостоверяющий хронологию перемещения и обработки потенциальных свидетельств, представленных в цифровой форме. Она должна быть начата от процесса сбора или получения свидетельств. Обычно это достигается путем регистрации истории элемента от момента его идентификации, сбора или получения группой расследования до его текущего состояния и местонахождения.

Запись истории хранения – это документ или несколько взаимосвязанных документов, детально описывающих историю хранения и фиксирующих лиц, отвечающих за обращение с потенциальными свидетельствами, представленными в цифровой форме, либо в виде цифровых данных, либо в других форматах (например, заметки на бумаге). Цель поддержания записи истории хранения состоит в создании возможности идентификации перемещения потенциальных свидетельств, представленных

в цифровой форме, и доступа к ним в любой данный момент времени. Сама запись истории хранения может содержать более одного документа, например, для потенциальных свидетельств, представленных в цифровой форме, должен быть актуальный документ, фиксирующий получение цифровых данных с конкретного устройства и перемещение этого устройства, и документация, фиксирующая последующее извлечение или копирование потенциальных свидетельств, представленных в цифровой форме, для анализа или иных целей. Запись истории хранения должна, как минимум, содержать следующую информацию:

- уникальный идентификатор свидетельства;
- лиц, имевших доступ к свидетельству, время и место происходящего;
- лиц, осуществлявших проверку свидетельства в помещении для сохранения свидетельств и вне него, и когда это происходило;
- причина выполнения проверки свидетельства (при каких обстоятельствах, и с какой целью) и соответствующее основание, если это применимо;
- любые неизбежные изменения потенциального свидетельства, представленного в цифровой форме, а также фамилию лица, ответственного за это, и обоснование внесения изменений.

История хранения должна поддерживаться на протяжении времени использования свидетельств и сохраняться в течение определенного периода времени после завершения использования свидетельств – этот период времени может быть установлен в соответствии с местной юрисдикцией сбора и получения свидетельств. Она должна устанавливаться с момента получения цифрового устройства (устройств) и (или) потенциальных свидетельств, представленных в цифровой форме, и не должна компрометироваться.

Примечание – В некоторых юрисдикциях могут быть особые требования в отношении истории хранения. DEFR должен соблюдать эти требования.

6.2 Меры предосторожности на месте инцидента

6.2.1 Общая информация

Как только DEFR появляется на месте инцидента, он должен выполнить действия по обеспечению безопасности и защиты местонахождения потенциальных свидетельств, представленных в цифровой форме. С учетом местного законодательства эти меры должны поддерживать следующее:

- обезопасить и взять под контроль площадку, содержащую устройства;
- определить, кто несет ответственность за площадку;
- обеспечить уверенность в том, что люди удалены от устройств и источников питания;
- документально отметить всех, кто имеет доступ на площадку, или всех, у кого может быть причина оказаться связанным с местом инцидента;
- если устройство включено, не выключать его, а если устройство выключено, не включать его;
- если это возможно, документально зафиксировать место события (например, эскиз, фотография или видеоизображение) со всеми компонентами и кабелями в исходном положении. Если фотоаппарата и (или) видеокамеры нет, нарисовать эскизный план системы и промаркировать порты и кабели, чтобы система могла быть проверена и восстановлена позднее;
- если это разрешено, провести на площадке поиск таких предметов, как самоклеющиеся записки, ежедневники, документы, ноутбуки или руководства по аппаратным и программных средствам с важнейшими подробностями об устройствах, такими как пароли и PIN-коды.

Примечание 1 – В некоторых юрисдикциях могут быть особые требования к приему фото и видеоматериалов в качестве доказательств. DEFR должен точно соблюдать эти требования.

Примечание 2 – DEFR должны сознавать, что потенциальные свидетельства, представленные в цифровой форме, не всегда могут быть в очевидных местах, например, может быть распределенное или виртуальное хранение.

В первую очередь DEFR должен представить себе все риски, связанные с осуществлением всех процессов по расследованию. На месте инцидента необходимо рассмотреть вопрос защиты персонала и потенциальных свидетельств, представленных в цифровой форме.

6.2.2 Персонал

До начала процесса важно провести оценку риска в отношении безопасности персонала, поскольку безопасность персонала, участвующего в процессе, является жизненно важной. Вопросы, которые должны быть рассмотрены в процессе оценки рисков для персонала, включают (но не ограничиваются) следующее:

- существует ли подозреваемое лицо(а)? Если да, есть ли у него(их) склонность к противоправным действиям?
- в течение какого времени будет проводиться работа?
- может ли место инцидента быть изолировано от посторонних?
- есть ли на площадке оружие?
- существуют ли физические опасности для присутствующих?
- может ли что-то в ближайшем окружении, включая устройства, быть сконфигурировано так, чтобы вызывать физический ущерб в случае несоответствующего обращения, например, скрытая ловушка?
- существует ли какая-либо вероятность того, что подлежащие сбору материалы могут вызвать психологическую травму или правонарушение?
- может ли место инцидента считаться ненадежным?
- оказывает ли окружающая среда влияние на возможность риска?

6.2.3 Потенциальные свидетельства, представленные в цифровой форме

DEFR должен быть осмотрителен при использовании конкретного инструментального средства для сбора или получения потенциальных свидетельств, представленных в цифровой форме. Непринятие в расчет рисков перед сбором может приводить к потере некоторых или всех потенциальных свидетельств, представленных в цифровой форме, за счет технологии, применяемой для сбора или получения свидетельств. Должна быть проведена оценка рисков для снижения возможности появления исков о возмещении ущерба.

Оценка риска включает систематическое оценивание рисков и потенциального влияния, которое они могут оказывать на изучение свидетельств, представленных в цифровой форме. Аспекты, подлежащие рассмотрению при оценке риска для свидетельств, представленных в цифровой форме, включают, но не ограничиваются, следующее:

- какой вид методов сбора/получения свидетельств должен применяться?
- какое оборудование может потребоваться на месте?
- каков уровень изменчивости данных и информации, связанных с потенциальными свидетельствами, представленными в цифровой форме?
- возможен ли удаленный доступ к любому цифровому устройству и представляет ли это угрозу для целостности доказательств?
- что произойдет в случае повреждения данных/оборудования?
- могла ли произойти компрометация данных?
- могло ли цифровое устройство быть сконфигурировано так, чтобы вызвать разрушение (например, используя логическую бомбу), испортить или запутать данные в случае выключения или неконтролируемого доступа?

6.3 Роли и обязанности

Роль DEFR включает идентификацию, сбор, получение и сохранение потенциальных свидетельств, представленных в цифровой форме, на месте инцидента. Она охватывает создание отчета по сбору и получению свидетельств, но не обязательно создание отчета по анализу. В роль DEFR также входит обеспечение уверенности в целостности и подлинности потенциальных свидетельств, представленных в цифровой форме. Для выполнения своей роли DEFR должен обладать адекватным опытом, знаниями и навыками обработки свидетельств, представленных в цифровой форме. Этот вопрос является критичным, поскольку потенциальные свидетельства, представленные в цифровой форме, легко могут быть повреждены.

DEFR может также потребоваться помощь персонала, осуществляющего техническую поддержку в соответствующих сферах. Роль DES заключается в обеспечении технической поддержки DEFR при идентификации, сборе, получении и сохранении потенциальных свидетельств, представленных в цифровой форме, на месте инцидента. DES обеспечивает экспертный анализ для DEFR. Таблица компетентности для DEFR (см. приложение А), служит справочником для определения соответствующего ему уровня компетентности.

Примечание – В контексте обработки инцидентов там, где существует ISIRT, роли DEFR и (или) DES в качестве членов группы ISIRT рассматриваются в ИСО/МЭК 27035:2011.

6.4 Компетентность

DEFR и (или) DES должны обладать соответствующей технической и юридической компетентностью (примеры, см. приложение А), и должны быть способны продемонстрировать наличие надлежащей подготовки и достаточного технического и юридического понимания при обработке свидетельств, представленных в цифровой форме, с использованием инструментальных средств для выполнения задач. Это включает понимание процессов и методов, подходящих для обработки потенциальных источников свидетельств, представленных в цифровой форме. Адекватная подготовка даст возможность DEFR обращаться с цифровыми устройствами, которые могут содержать потенциальные свидетельства, представленные в цифровой форме. Обладание лучшим набором инструментальных средств не будет гарантировать качество свидетельств, если DEFR не обладает достаточной компетентностью для выполнения своих задач.

Некоторые юрисдикции предписывают, как DEFR должны устанавливать свою квалификацию. В обязанности DEFR входит обеспечение уверенности в надлежащей осведомленности о том, что и как делать согласно соответствующим юрисдикциям. Когда требуется DEFR и (или) DES должны быть способны продемонстрировать свою компетентность в обработке потенциальных свидетельств, представленных в цифровой форме, с помощью инструментальных средств и методов, выбранных для выполнения задач. Также требуется, чтобы DEFR могли представить свидетельство постоянного поддержания своей компетентности.

DEFR должны удовлетворять следующим условиям:

- они должны иметь надлежащую и адекватную подготовку для обработки цифровых устройств в рамках действий по расследованию;
- они должны поддерживать и демонстрировать соответствующим органам свои навыки и компетентность в соответствующей области по обработке свидетельств, представленных в цифровой форме;
- обязанностью лица (лиц) и работодателя является обеспечение уверенности в том, что DEFR адекватно подготовлены и поддерживают навыки и компетентность.

Примечание – Компетентность DEFR может быть различной в разных юрисдикциях.

6.5 Применение разумной осторожности

Следует избегать любых действий, которые могут приводить к повреждению потенциальных свидетельств, представленных в цифровой форме, хранящихся в цифровых устройствах в результате преднамеренных или непреднамеренных действий. Например, воздействие магнитных полей может приводить к повреждению потенциальных свидетельств, представленных в цифровой форме, которые содержатся на магнитных носителях. DEFR не должны иметь доступ к цифровым устройствам, например, для выполнения дампа памяти из действующего цифрового устройства, если они не обладают необходимой компетентностью и не используют достоверные и валидные процессы.

Ниже приводятся некоторые условия, когда нецелесообразен сбор или получение потенциальных цифровых свидетельств, представленных в цифровой форме. DEFR должен учитывать приведенные ниже условия, но не ограничиваться ими:

- если нет юридического документа или полномочий, дающих право на сбор цифровых устройств;
- если имеется обязательство использовать другие методы (например, чтобы избежать прерывания бизнеса);
- если DEFR хочет зафиксировать способ работы подозреваемого во время злоупотребления системой;
- если сбор или получение свидетельств должны происходить скрытно в случае, если это считается законным для данной юрисдикции;
- если это критичное для целевой задачи цифровое устройство, не допускающее никакого простоя;
- если физический объем цифрового устройства слишком велик, например, сервер в информационном центре или RAID системы;
- если это критичное для безопасности цифровое устройство, остановка которого будет угрожать жизни людей;
- если это цифровое устройство, которое также обслуживает непричастные стороны.

6.6 Документирование

Документирование имеет решающее значение при обработке цифровых устройств, которые могут содержать свидетельства, представленные в цифровой форме, Во время документирования DEFR должен придерживаться следующих моментов:

- каждое предпринятое действие должно документироваться. Это делается для обеспечения уверенности в том, что во время идентификации, сбора, получения и сохранения свидетельств никакие детали не были упущены. Документирование может быть также полезно при трансграничном расследовании, при котором можно таким образом проследить за потенциальными свидетельствами, представленными в цифровой форме, которые собраны в другой части земного шара;
- если цифровые устройства включены, DEFR должен быть внимательным к установленным времени и дате. Нужно сравнить настойку времени с надежным источником времени, таким как время, синхронизируемое надежным и контролируемым источником времени. Эти настройки времени следует документировать и указывать наличие любых расхождений. Некоторые системы требуют существенного взаимодействия с пользователем для получения настроек времени и даты. DEFR должен проявлять осторожность, чтобы не модифицировать систему. Только надлежащим образом обученный персонал должен извлекать эти параметры настройки;
- DEFR должен документировать все видимое на экране цифрового устройства: активные программы и процессы, а также имена открытых документов. Эта документация должна включать описание того, что является видимым, поскольку некоторые вредоносные программы могут имитировать известные программные средства;
- любое перемещение цифровых устройств должно быть документировано в соответствии с внутренними требованиями;
- следует документировать все уникальные идентификаторы цифровых устройств и взаимосвязанных частей, такие как серийные номера и уникальную маркировку.

В приложении В приведены примеры минимального комплекта документов для обмена потенциальными свидетельствами, представленными в цифровой форме, между юрисдикциями.

Примечание – Более подробная информация о документировании приведена в разделе об управлении документооборотом и в разделе о менеджменте записей ИСО/МЭК 17025:20005.

6.7 Инструктаж

6.7.1 Общая информация

Очень важно, чтобы DEFR и DES были адекватно проинструктированы соответствующим органом до выполнения ими задач с соблюдением любых законов и ограничений в отношении конфиденциальности (т. е. принцип необходимого знания). Важно провести официальный инструктаж, чтобы обеспечить понимание инцидента, а также чего следует и чего не следует ожидать в ходе расследования и напомнить о фальсификации или повреждении свидетельств. Инструктаж должен быть достаточным, чтобы члены группы были хорошо подготовлены для выполнения своих ролей и обязанностей; обеспечивая, таким образом, уверенность в извлечении всех необходимых потенциальных свидетельств, представленных в цифровой форме.

6.7.2 Специальный инструктаж по свидетельствам, представленным в цифровой форме

Чтобы проинформировать DEFR о связанных с расследованием деталях, нужен подробный инструктаж, четко сосредоточенный на конкретных рекомендациях относительно свидетельств, представленных в цифровой форме. Во время инструктажа DEFR и DES предоставляется соответствующая информация, и даются подробные инструкции по надлежащему сбору или получению потенциальных свидетельств, представленных в цифровой форме. Это может включать следующее:

- вид инцидента (если известно);
- дату и время инцидента (если известно);
- план расследования (сбор и (или) получение свидетельств, известная сетевая активность, требования к известным изменчивым данным и т. д.);
- рассмотрение того, где и каким образом будет осуществляться хранение/транспортировка потенциальных свидетельств, представленных в цифровой форме, после их сбора или получения;
- конкретные инструментальные средства, необходимые для получения потенциальных свидетельств, представленных в цифровой форме;

- потенциальные свидетельства, представленные в цифровой форме, которые имеют отношение к конкретным видам расследования;
- оборудование и руководства, имеющие отношение к цифровым устройствам;
- напоминание членам группы о необходимости отключения на их телефонах/компьютерах любых возможностей использования Bluetooth или Wi-Fi, чтобы они случайно не взаимодействовали с цифровыми устройствами, за исключением телефонов/компьютеров, используемых для обнаружения соединений;
- важность документирования на всем протяжении расследования;
- применимые правовые или иные факторы, которые могут запрещать сбор каких-то устройств и содержащихся в них потенциальных свидетельств, представленных в цифровой форме.

Этот специальный инструктаж может составлять часть общего инструктажа, как описано в 6.7.1.

6.7.3 Специальный инструктаж в отношении персонала

Чтобы проинформировать DEFR об аспектах, связанных с вовлеченными в расследование сторонами, нужен инструктаж, четко сосредоточенный на специальных рекомендациях в отношении персонала. Во время инструктажа проводящей расследование группе будут даны инструкции, относящиеся к персоналу. Они могут включать:

- задания, роли и обязанности членов проводящей расследование группы на месте инцидента;
- ожидается ли участие в расследовании других органов (медицинского персонала, судебных медицинских экспертов и т. д.);
- напоминание членам группы о том, что не следует принимать техническую помощь от любых неуполномоченных лиц;
- напоминание членам группы о необходимости строго следовать процедуре минимизации возможного повреждения свидетельств, представленных в цифровой форме, например, избегать использования любых инструментальных средств или материалов, которые могут генерировать статическое электричество или магнитное поле, так как они могут повреждать или разрушать потенциальные свидетельства.

Этот специальный инструктаж может составлять часть общего инструктажа, как описано в 6.7.1.

6.7.4 Инциденты в реальном времени

Очень желательно, чтобы расследование инцидента планировалось заранее, но существуют обстоятельства, (например, когда инцидент развивается и когда выполняются ответные действия в режиме реального времени), при которых полное планирование не может быть выполнено. В таких ситуациях группа должна быть проинструктирована о начальной стратегии и тактике расследования, и должна существовать возможность разработки новых стратегий и тактик в ответ на сложившиеся условия. Информация о развитии инцидента, должна быть распространена между членами группы как можно быстрее, чтобы обеспечить уверенность в принятии эффективных решений в отношении предпринимаемых действий, при соответствующем подходе к необходимости их обоснования.

6.7.5 Другая информация для инструктажа

Помимо информации, относящейся к свидетельствам, представленным в цифровой форме, и к персоналу, проводящей расследование группе должна сообщаться дополнительная важная информация, включающая:

- указание расследуемой области, включая название организации, адрес и план объекта (если таковой доступен);
- мандат на проведение расследования;
- детали ордеров на обыск и других полномочий, применимых к расследованию, включая ограничения на право производить обыски и изъятия;
- правовые аспекты и последствия;
- временные рамки расследования;
- оборудование, которое необходимо доставить на место инцидента для расследования;
- информация, касающаяся материально-технического обеспечения;
- потенциальный конфликт интересов.

DEFR должен избегать попадания в ситуации, в которых он может быть обвинен в присущей необъективности. Примером такой присущей необъективности является ситуация, когда DEFR делает копию с одного компьютера, а не с другого (который, как оказывается позднее, содержит оправдывающие свидетельства) на основе восприятия, сформированного в результате инструктажа.

6.8 Установление приоритетов для сбора и получения свидетельств

При установлении приоритетов для сбора или получения потенциальных свидетельств, представленных в цифровой форме, необходимо, чтобы DEFR понимал причину сбора или получения потенциальных свидетельств, представленных в цифровой форме. Как правило, DEFR должен пытаться максимально увеличить количество данных, сохраняемых путем сбора и получения свидетельств. Может возникнуть необходимость в установлении приоритетов для элементов по изменчивости и (или) значимости/потенциальной доказательной ценности. К элементам с большой значимостью/потенциальной доказательной ценностью относятся те, которые, скорее всего, будут содержать данные, непосредственно относящиеся к расследуемому инциденту.

Установление приоритетов по изменчивости применимо только в том случае, если этого требуют конкретные обстоятельства расследуемого дела. Потенциальные свидетельства, представленные в цифровой форме, можно разбить на две категории: энергозависимые и энергонезависимые. Изменчивые данные легко могут быть разрушены или навсегда потеряны, если не применяются меры по обеспечению защиты данных. Например, отключение электропитания цифрового устройства может привести к потере изменчивых данных. Неизменчивые данные остаются на носителе даже при отключении электропитания. Поскольку некоторые виды свидетельств, представленных в цифровой форме, могут иметь короткий срок жизни, потенциальные свидетельства, представленные в цифровой форме, легко могут быть испорчены или повреждены. Если неясно, содержат ли цифровые устройства потенциальные свидетельства, представленные в цифровой форме, или какие элементы более значимы по отношению к другим, то необходимо изучить их до начала сбора, используя процесс установления приоритетов. Цифровые устройства, подлежащие рассмотрению на предмет сбора, включают (но не ограничиваются) ИТ-оборудование и цифровые носители данных, CCTV, PED, автомобильные системы, системы управления и нестандартные электронные устройства. Сначала надо получить наиболее изменчивые потенциальные свидетельства, представленные в цифровой форме, например из ОЗУ, пространства подкачки свопинга, активных процессов и т. д. DEFR должен обладать прочными знаниями для установления приоритетов в соответствии с изменчивостью.

При идентификации DEFR должен:

- установить приоритеты для потенциальных свидетельств, представленных в цифровой форме, которые будут навсегда потеряны при отключении электропитания; и
- принять незамедлительные меры для сбора и получения таких данных утвержденными методами.

Примечание 1 – Некоторые изменчивые данные могут меняться в зависимости от факторов, включающих (но не ограничивающихся) местонахождение, время и изменения в окружающих цифровых устройствах – следует обеспечить уверенность в том, что такие данные сохраняются до перемещения устройства.

Примечание 2 – Цифровые устройства, содержащие потенциальные свидетельства, представленные в цифровой форме, могут быть источником физических свидетельств (например, отпечатки пальцев, ДНК и т. д.). DEFR должны проявлять осторожность, чтобы не испортить такие свидетельства, и координировать свои действия с соответствующими специалистами по сбору свидетельств, прежде чем переходить к следующим действиям.

Примечание 3 – Если есть подозрение о наличии шифрования или вредоносной программы, необходимо исследовать изменчивые данные.

При некоторых условиях ограничивающим фактором в расследовании может быть время. В таких случаях следует отдавать предпочтение потенциальным свидетельствам, представленным в цифровой форме, которые идентифицированы как значимые для конкретного инцидента.

6.9 Сохранение потенциальных свидетельств, представленных в цифровой форме

6.9.1 Общие сведения

Для сохранения полученных потенциальных свидетельств, представленных в цифровой форме, и собранных цифровых устройств важно во время упаковки обезопасить их таким образом, чтобы исключить повреждение или фальсификацию. Повреждение может быть результатом ухудшения качества из-за воздействия магнитного или электрического поля, влияния тепла, высокой или низкой влажности, а также сотрясения и вибрации. Фальсификация может быть результатом намеренного осуществления или допущения осуществления изменений потенциальных свидетельств, представленных в цифровой форме. Поэтому важно как можно лучше защищать потенциальные свидетельства, представленные в цифровой форме, и как можно меньше использовать исходные данные. Важ-

но, чтобы DEFR был знаком с требованиями к упаковке, характерными для соответствующей юрисдикции.

6.9.2 Сохранение потенциальных свидетельств, представленных в цифровой форме

Все собранные цифровые устройства и полученные потенциальные свидетельства, представленные в цифровой форме, должны быть защищены, насколько это возможно, от потери, фальсификации или повреждения. Наиболее важным действием в процессе сохранения является поддержка целостности и подлинности потенциальных свидетельств, представленных в цифровой форме, и их истории хранения.

Собранные цифровые устройства и полученные потенциальные свидетельства, представленные в цифровой форме, должны храниться в помещении для хранения свидетельств с использованием мер и средств контроля и управления физической безопасности, таких как системы управления доступом, системы наблюдения или системы обнаружения вторжений, или в иной контролируемой среде для хранения свидетельств, представленных в цифровой форме. Основными целями физической безопасности являются обеспечение защиты и предупреждение потери, повреждения и фальсификации свидетельств, представленных в цифровой форме, а также обеспечение контролируемости.

Собранные цифровые устройства, должны быть помещены в надлежащую упаковку, соответствующую характеру устройства, для предотвращения загрязнения цифрового устройства (устройств) до транспортировки в другое место(а). Чтобы избежать физического повреждения любых компонентов устройства (устройств), может быть использована ударопрочная упаковка.

- DEFR должен рассмотреть вопрос чувствительности цифрового устройства к статическому электричеству. При наличии чувствительности следует поместить устройство в антистатический пакет.

- Основные системные блоки и ноутбуки следует помещать в соответствующий контейнер, чтобы избежать фальсификации или повреждения потенциальных свидетельств, представленных в цифровой форме, которые могут в них находиться.

Примечание – Использование клетки Фарадея или иной упаковки с экранированием радиочастоты может усилить истощение аккумулятора мобильной телефонной связи. Это может потребовать обеспечения резервного питания для находящегося в упаковке устройства, если позволяют ресурсы.

6.9.3 Упаковка цифровых устройств и потенциальных свидетельств, представленных в цифровой форме

6.9.3.1 Базовые действия: упаковка потенциальных свидетельств, представленных в цифровой форме

К базовым действиям относятся действия, которые следует выполнять, если нет достаточных оснований не делать этого. Их можно также назвать минимальными действиями, которые должны быть выполнены. Во время упаковки DEFR должен учитывать и обращать внимание на следующие базовые действия:

- не касаться самóй магнитной ленты, а брать магнитные ленты за защитный футляр или места, где, как известно, не содержатся данные (например, края оптических дисков). Это следует делать только в том случае, если DEFR носит не оставляющие ворсинок перчатки.

Примечание – Конкретные места носителей информации, где, как известно, не содержатся данные, зависят от видов носителей. DEFR обязан знать современную технологию и иметь навык обращения с носителями информации;

- для обеспечения уверенности в надлежащей идентификации DEFR должен промаркировать все потенциальные свидетельства, представленные в цифровой форме. В некоторых юрисдикциях существуют особые требования, касающиеся формата маркировки доказательного материала. DEFR должен знать требования, применимые в данном случае, и соблюдать их. DEFR должен промаркировать все потенциальные свидетельства, представленные в цифровой форме, собранные цифровые устройства и любые связанные с устройствами аппаратные части маркировкой с индикацией их вскрытия. Маркировка не должна помещаться непосредственно на механические части цифрового устройства и закрывать или скрывать важную идентификационную информацию. Все потенциальные свидетельства, представленные в цифровой форме, в собранных устройствах должны быть получены и сохранены таким образом, чтобы обеспечивалась уверенность в целостности свидетельств;

- по возможности цифровые устройства с открывающимися и подвижными элементами должны быть маркированы путем наклеивания этикетки, соответствующей устройству, с печатью для индикации вскрытия, и DEFR должен поставить подпись на печать;

- устройства с энергозависимыми данными, присоединенные к аккумуляторным батареям, следует регулярно проверять, чтобы обеспечить уверенность в том, что устройствам всегда обеспечивается достаточное электропитание;

- следует идентифицировать и поместить цифровое устройство(а) в контейнер, соответствующий характеру устройства, для защиты от потенциальных угроз;

- компьютеры и цифровые устройства должны быть упакованы таким образом, чтобы предотвратить повреждение вследствие удара, вибрации, большой высоты, тепла и влияния электромагнитного излучения во время транспортировки;

- магнитные носители данных следует хранить в магнитно-инертной, антистатической и защищенной от пыли упаковке;

- цифровые устройства могут также содержать скрытые свидетельства, отпечатки или биологические свидетельства. Поэтому должны быть предприняты соответствующие меры для сохранения потенциальных свидетельств, представленных в цифровой форме. Создание образов свидетельств, представленных в цифровой форме, следует осуществлять после проведения соответствующих процессов сбора скрытых свидетельств, отпечатков или биологических свидетельств на устройствах. Однако решение по установлению приоритетов сбора свидетельств должно тщательно оцениваться, чтобы обеспечить сохранность свидетельств.

6.9.3.2 Дополнительные действия: упаковка потенциальных свидетельств, представленных в цифровой форме

Дополнительные действия относятся к действиям, выполнение которых настоятельно рекомендуется. Во время упаковки DEFR должен обращать внимание на следующие дополнительные действия и выполнять их, где это применимо:

- носить не оставляющие ворса перчатки и обеспечивать сухость и чистоту рук;

- обеспечивать защиту цифровых устройств от влияния источников электромагнитного поля (например, полицейские рации, динамики, рентгеновские установки). Упаковочное оборудование не должно генерировать статическое электричество;

- среда упаковки не должна содержать пыли, жира или химических загрязняющих веществ, способствующих окислительным процессам или конденсации влаги на магнитном слое;

- сводить к минимуму возможность копир-эффекта (передача сигнала с одной петли магнитной ленты на соседнюю петлю), который может происходить при хранении магнитных лент в течение длительного времени без активного использования, приводя к снижению качества передачи сигнала;

- при необходимости в зонах упаковки не должно быть ультрафиолетового излучения. Ультрафиолетовое излучение может повредить ДНК или некоторые виды носителей данных. Перед выбором зоны упаковки DEFR должен рассмотреть, представляет ли ультрафиолетовое излучение риск для потенциальных свидетельств;

- должна обеспечиваться надежная защита цифровых устройств от теплового воздействия.

6.9.4 Транспортировка потенциальных свидетельств, представленных в цифровой форме

DEFR должен обеспечивать сохранность во время транспортировки собранных цифровых устройств и полученных потенциальных свидетельств, представленных в цифровой форме. Потенциальные свидетельства, представленные в цифровой форме, не должны оставаться без присмотра во время процесса транспортировки. DEFR должен поддерживать историю хранения во время процесса транспортировки для предотвращения возможной фальсификации или повреждения, а также поддержания целостности и подлинности цифровых устройств и потенциальных свидетельств, представленных в цифровой форме.

Примечание – DEFR должен обеспечить уверенность в том, что сбор чувствительной или персональной информации осуществляется в соответствии с законами и нормами местной юрисдикции о защите данных.

Во время процесса упаковки и транспортировки DEFR должен быть осведомлен о возможности образования электростатических разрядов, которые могут нанести ущерб доказательной ценности потенциальных свидетельств, представленных в цифровой форме. DEFR должен убедиться, что на

время транспортировки компьютеры и цифровые устройства упакованы безопасным образом, предупреждающим повреждения от ударов и вибрации.

Процесс транспортировки должен предусматривать благоприятные и контролируемые условия. Уровень влажности и температуры должны быть подходящими для цифровых устройств. Следует избегать продолжительного нахождения потенциальных свидетельств, представленных в цифровой форме, и цифровых устройств в транспортном средстве, а также оберегать их от воздействия УФ.

В соответствии с некоторыми юрисдикциями или, когда не позволяют обстоятельства, DEFR не может сопровождать свидетельства. В таких случаях должны использоваться соответствующие и надежные механизмы перевозки, чтобы обеспечить надлежащую безопасность свидетельств во время транспортировки. Документация по транспортировке и верификация целостности упаковки должны стать частью истории хранения.

7 Примеры идентификации, сбора, получения и сохранения свидетельств

7.1 Компьютеры, периферийные устройства и цифровые носители данных

7.1.1 Идентификация

7.1.1.1 Поиск и документирование физического места инцидента

В контексте данного раздела компьютеры считаются автономными цифровыми устройствами, которые получают, обрабатывают и хранят данные и создают результаты. Эти компьютерные устройства не подключены к сети, но могут быть соединены с такими периферийными устройствами, как принтеры, сканеры, веб-камеры, MP3-плееры, GPS, RFID и т. д. Цифровое устройство, имеющее сетевой интерфейс, но не подключенное к нему во время сбора или получения свидетельств, следует считать (для целей настоящего стандарта) автономным компьютером. Если компьютер имеет сетевой интерфейс, но явного соединения по нему не обнаружено, должны быть предприняты действия по определению устройств, которые могли быть подключены в недавнем прошлом.

Обычно место инцидента вмещает различные виды цифровых носителей информации. Цифровые носители информации используются для сохранения данных цифровых устройств и отличаются объемом памяти. Примерами цифровых носителей являются (но не ограничиваются) внешние переносные жесткие диски, флэш-память, CD-диски, DVD-диски, Blu-Ray-диски, дискеты, магнитные ленты и карты памяти.

Прежде чем может быть проведен сбор или получение свидетельств, нужно рассмотреть аспекты сохранности потенциальных свидетельств, представленных в цифровой форме. Эти аспекты описаны в 6.2.1 и 6.2.2. Однако DEFR необходимо самому убедиться в том, что автономное устройство не было недавно подключено к сети. При наличии подозрений о недавнем отключении автономного устройства от сети, его следует рассматривать как сетевое устройство для обеспечения уверенности в надлежащем обращении с другими частями сети. DEFR должен отметить и рассмотреть, по крайней мере, следующее:

- DEFR должен документировать тип и марку любых используемых цифровых устройств и идентифицировать все компьютеры и периферийные устройства, которые могут потребоваться на начальном этапе сбора или получения свидетельств. При возможности, должны быть документированы серийные номера, номера лицензий и другие идентификационные признаки (в том числе физические повреждения);

- на этапе идентификации состояние компьютеров и периферийных устройств должно оставаться неизменным. Если компьютеры или периферийные устройства выключены, их не следует включать. Если компьютеры или периферийные устройства включены, DEFR не должен выключать их, иначе потенциальные свидетельства, представленные в цифровой форме, могут быть повреждены;

- если компьютеры включены, DEFR должен сфотографировать или зафиксировать в письменном документе то, что выведено на их экранах. Любой письменный документ должен включать описание того, что видно фактически (например, приблизительное положение окон, заголовков и содержания);

- устройство, имеющее аккумуляторные батареи, которые могут разрядиться, следует подключить к зарядному устройству, для обеспечения уверенности в том, что информация не будет потеряна. На этом этапе DEFR необходимо определить и собрать потенциальные зарядные устройства и кабели;

- DEFR должен также рассмотреть вопрос использования детектора сигналов беспроводной сети для обнаружения и идентификации сигналов от беспроводных устройств, которые могут быть спрятаны. Возможны случаи, когда детектор сигналов беспроводной сети не используется из-за финансовых и временных ограничений, тогда DEFR должен документировать это. При обнаружении любых сетевых устройств DEFR должен продолжать процесс обработки свидетельств, как описано в 7.2.2.2 настоящего стандарта. В том случае, если должно быть использовано активное сканирование (т. е. передача, прием и (или) анализ радиосигналов) сетевых устройств, сканирующие устройства должны быть выключены до тех пор, пока не будет оценена возможность взаимодействия их с другими устройствами на месте инцидента. Члены проводящей расследование группы должны помнить, что некоторые устройства на месте инцидента могут обнаруживать присутствие устройств активного сканирования, и вызвать действия, которые могут испортить потенциальные свидетельства или, в крайних случаях, привести к активации скрытых ловушек.

Примечание 1 – Если имеется много цифровых устройств, в некоторых юрисдикциях допустимо включение цифровых устройств на месте инцидента, чтобы определить их значимость для расследования. Это делается с учетом времени обработки и финансовых затрат, которые могут возникнуть, если будут собраны не относящиеся к делу цифровые устройства. Если устройство включается для оценки на месте инцидента, DEFR должен обеспечить уверенность в том, что на протяжении процесса поддерживается исчерпывающая запись действий.

Примечание 2 – Что касается сохранения состояния энергопитания цифрового устройства, то должны учитываться результаты определения изменчивости и соответствующего процесса установления приоритетов. Если принимается решение о том, что основной критичной информацией является изменчивая информация на диске, то можно сфотографировать экран этой работающей системы и вынуть разъем питания. Если значимой является изменчивая информация, хранящаяся в памяти, то нужно оставить систему включенной, чтобы сделать возможным получение свидетельств.

7.1.1.2 Сбор свидетельств, не представленных в цифровой форме

DEFR должен рассмотреть вопрос сбора свидетельств, не представленных в цифровой форме. Для этого руководитель группы должен определить лицо, отвечающее за оборудование на месте инцидента, которое сможет предоставить дополнительную информацию и документацию, такую как пароли цифровых устройств и другие значимые детали. DEFR необходимо документировать фамилию и должность этого лица.

DEFR также может потребоваться проведение сбора некоторых свидетельств путем бесед с лицами, у которых может быть полезная или значимая информация о потенциальных свидетельствах, представленных в цифровой форме, или цифровых устройствах, подлежащих сбору. Любые ответы должны точно и аккуратно документироваться. Этими лицами могут быть системный администратор, владелец устройства, а также пользователи компьютера и периферийных устройств. Во время этого устного сбора свидетельств DEFR может запрашивать информацию, например, информацию, касающуюся конфигурации системы, и пароль администратора/суперпользователя. Эта дополнительная информация может быть полезна на этапе анализа потенциальных свидетельств, представленных в цифровой форме. Эти беседы следует документально оформлять для обеспечения уверенности в точности деталей, а также в том, что документально оформленные утверждения не могут быть изменены. DEFR, должен быть знаком с требованиями соответствующей юрисдикции, относящимися к сбору свидетельств, не представленных в цифровой форме.

7.1.1.3 Процесс принятия решения для проведения сбора и получения свидетельств

При принятии решения о сборе цифровых устройств или получении потенциальных свидетельств, представленных в цифровой форме, нужно учитывать несколько факторов, включающих следующее, но не ограничивающихся этим:

- изменчивость потенциальных свидетельств, представленных в цифровой форме, которая обсуждается в 5.4.2 и 6.8;
- наличие полного шифрования диска или зашифрованных томов, пароли или ключи которых могут находиться в виде изменчивых данных в ОЗУ, на внешних токенах, смарт-картах, других устройствах или носителях;
- критичность системы, которая обсуждается в 5.4.4, 7.2.1.2 и 7.1.3.4;
- правовые требования юрисдикции;
- ресурсы, такие как размер требуемой памяти, наличие персонала, и временные ограничения.

На рисунке 1 представлен обзор процесса принятия решения для проведения сбора или получения свидетельств.



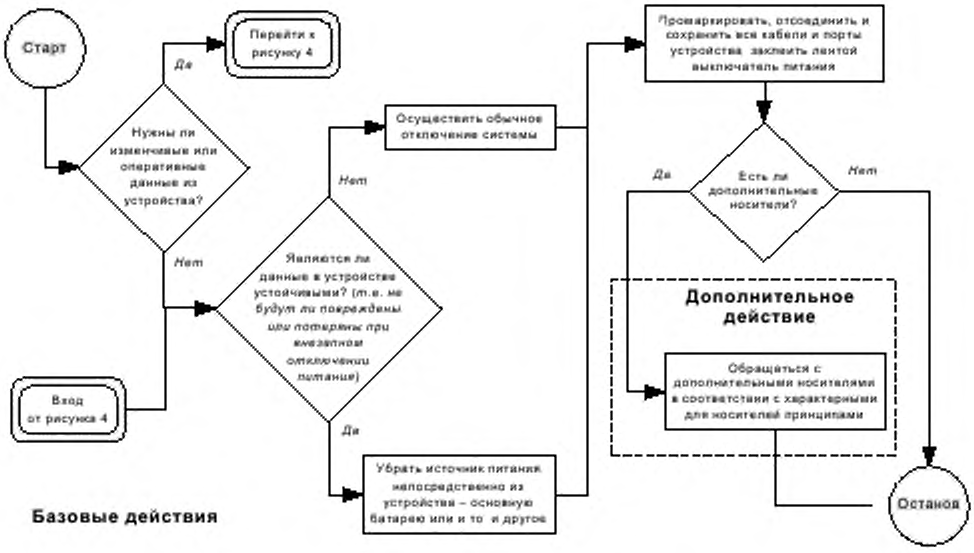
Р и с у н о к 1 — Принятие решения о сборе или получении свидетельств, представленных в цифровой форме

7.1.2 Сбор

7.1.2.1 Цифровые устройства с включенным питанием

7.1.2.1.1 Общий обзор

Если питание цифрового устройства включено, DEFR может следовать ряду рекомендаций по сбору. Не все эти рекомендации являются идеальными и соответствующими для любых случаев, некоторые применимы только в определенных случаях. Соответственно, рекомендации можно классифицировать как базовые или дополнительные. Базовые действия должны выполняться при всех обстоятельствах, тогда как дополнительные действия должны выполняться в уместных и применимых случаях в зависимости от конкретного устройства или обстоятельств. Рисунок 2 иллюстрирует базовые и дополнительные действия, применимые к сбору цифровых устройств с включенным питанием.



Р и с у н о к 2 — Рекомендации по сбору цифровых устройств с включенным питанием

П р и м е ч а н и е – Все указанные действия должны осуществляться в соответствии с законами и предписаниями местной юрисдикции.

DEFR обязан знать современную технологию и руководства по обращению с носителями информации.

7.1.2.1.2 Базовые действия: сбор цифровых устройств с включенным питанием

DEFR должен следовать приведенным ниже базовым действиям во всех случаях, касающихся потенциальных свидетельств, представленных в цифровой форме. Эти руководства применимы, когда DEFR принимает решение о сборе цифровых устройств с включенным питанием:

- до выключения системы следует рассмотреть вопрос получения изменчивых данных из цифрового устройства и его текущего состояния. Криптографические ключи и другие критические данные могут находиться в активной памяти или в неактивной памяти, которая еще не была очищена. При подозрении на шифрование следует рассмотреть вопрос логического получения данных. Если шифрование действительно имеет место, нужно помнить, что действующая серверная операционная система может не заслуживать доверия, поэтому необходимо рассмотреть вопрос использования соответствующих надежных и утвержденных инструментальных средств;

- конфигурацией цифрового устройства может быть определено, нужно ли DEFR завершать работу устройства посредством обычных административных процедур или следует вынуть вилку кабеля электропитания устройства из розетки электропитания. Чтобы определить лучший подход в данных обстоятельствах, DEFR может потребоваться консультация с DES. Если принято решение вынуть штепсельную вилку, DEFR должен отключить кабель электропитания, отсоединив предварительно конец, подключенный к цифровому устройству, а не к розетке электропитания. Нужно осознавать, что в устройстве, подключенном к ИБП данные могут быть изменены, если кабель электропитания отсоединить от розетки электропитания на стене, а не от ИБП устройства.

П р и м е ч а н и е 1 – При отключении питания включенного цифрового устройства любые потенциальные свидетельства, представленные в цифровой форме, которые хранятся в зашифрованных томах, будут недоступны, если не сохранен ключ дешифрования. Также могут быть потеряны потенциально ценные оперативные (рабочие) данные, такие как корпоративные данные или данные цифровых устройств, управляющих медицинским оборудованием, приводя к искам о возмещении убытков или потере человеческих жизней. Поэтому DEFR должен обеспечить уверенность в том, что изменчивые данные собраны, до отключения питания.

Примечание 2 – Существуют аппаратные устройства, позволяющие не прерывая питания отключить включенное устройство от сети электропитания, переключив его на портативный ИБП. Существуют также специальные устройства, перемещающие курсор мыши на экране, которые могут использоваться для предотвращения появления экранной заставки. Оба эти устройства предоставляют полезные инструментальные средства при обращении с включенным устройством, на котором шифрование может быть активным. В случае сбора устройств с включенным питанием для поддержания питания при транспортировке и упаковке работающей системы следует рассматривать вопросы, связанные с обеспечением охлаждения, защитой от механических ударов и т. д.;

- промаркировать, отсоединить и сохранить все кабели цифрового устройства и промаркировать порты, чтобы система могла быть восстановлена на более позднем этапе;
- заклеить лентой выключатель питания, если это необходимо, чтобы предотвратить изменение состояния выключателя. Рассмотреть вопрос о надлежащем документировании состояния выключателя до заклеивания лентой или изменения его положения.

7.1.2.1.3 Дополнительные действия: сбор цифровых устройств с включенным питанием

Ниже приведены дополнительные действия, которые являются применимыми в зависимости от конфигурации конкретного цифрового устройства:

- если это ноутбук, то обеспечить уверенность в получении изменчивых данных, прежде чем убирать аккумуляторную батарею. DEFR должен сначала извлечь основной аккумулятор источника питания вместо того, чтобы нажимать на кнопку питания для выключения ноутбука. DEFR должен также отметить, имеется ли адаптер источника питания, и, если он имеется, убрать его после удаления аккумулятора.

Примечание 1 – Цифровое устройство может быть сконфигурировано так, что при нажатии кнопки питания на нем запустится сценарий, который может изменять или удалять информацию в системе перед отключением или предупреждать подключенные системы о возникновении неожиданного события, так что эти системы могут стирать данные, имеющие доказательную ценность, прежде чем они будут идентифицированы. Оно может быть также сконфигурировано таким образом, чтобы приводить в действие устройство, предназначенное для причинения физического вреда DEFR и другим присутствующим лицам;

- заклеить лентой слот для дискет, если он есть;
- удостовериться, что лотки для CD или DVD дисков задвинуты на место; отметить, являются ли они пустыми, содержат диски или не проверены; заклеить лентой слот для предотвращения его открывания.

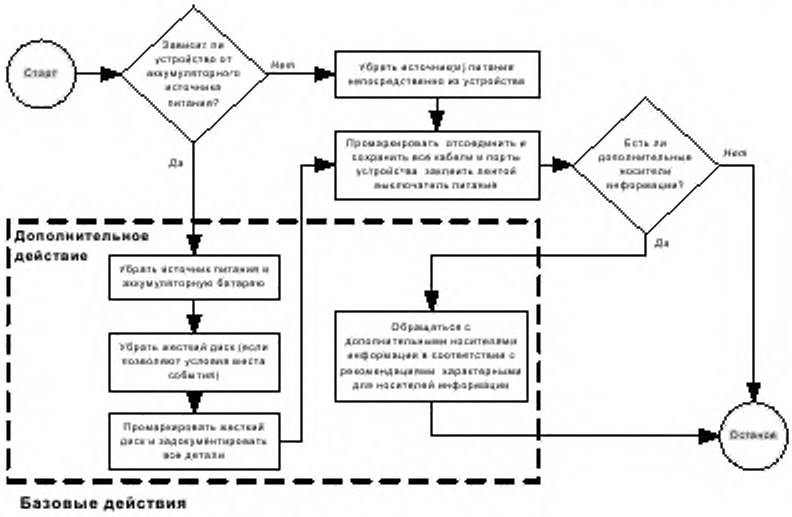
Примечание 2 – Если в устройстве оставлен носитель информации, который можно использовать для загрузки, то при следующем включении устройство может загрузиться с этого носителя, а не с жесткого диска (или флеш-памяти инструментальных средств для криминалистического исследования) в зависимости от установок базовой системы ввода/вывода (BIOS) компьютера.

DEFR должен проводить сбор свидетельств, не представленных в цифровой форме, в соответствии с процессуальным правом для обеспечения уверенности в приемлемости любых свидетельств.

7.1.2.2 Цифровые устройства с выключенным питанием

7.1.2.2.1 Общий обзор

Когда питание цифрового устройства выключено, DEFR может следовать ряду рекомендаций по сбору. Не все содержащиеся в этих рекомендациях действия могут быть уместны во всех обстоятельствах. Таким образом, должно быть сделано различие между действиями, применимыми во всех случаях (базовые действия), и действиями, которые могут применяться лишь в некоторых случаях (дополнительные действия). На рисунке 3 показаны базовые и дополнительные действия, применимые к сбору цифровых устройств с выключенным питанием.



Р и с у н о к 3 — Рекомендации по сбору цифровых устройств с выключенным питанием

DEFR обязан знать современную технологию и руководства по обращению с носителями информации.

7.1.2.2.2 Базовые действия: сбор цифровых устройств с выключенным питанием

Ниже приведены рекомендуемые базовые действия по сбору цифровых устройств с выключенным питанием:

- отключить кабель электропитания, предварительно отсоединив конец, подключенный к цифровому устройству, а не конец, подключенный к розетке электропитания;
- отсоединить и сохранить все кабели цифрового устройства и промаркировать порты, чтобы система могла быть восстановлена на более позднем этапе;
- заклеить лентой выключатель электропитания, если это необходимо для предотвращения изменения состояния выключателя. Рассмотреть вопрос о надлежащем документировании состояния выключателя до заклеивания лентой или изменения его положения.

П р и м е ч а н и е – В большинстве случаев носитель информации не должен извлекаться из цифрового устройства, пока не будет принято решение о получении свидетельств, так как его извлечение увеличивает риск повредить или перепутать его с другими носителями. Должны быть разработаны и выполнены локальные процедуры, касающиеся необходимости извлечения носителей информации из цифровых устройств.

7.1.2.2.3 Дополнительные действия: сбор цифровых устройств с выключенным питанием

Ниже приведены дополнительные действия, которые являются применимыми для сбора цифровых устройств с выключенным питанием в зависимости от конфигурации конкретного цифрового устройства:

- прежде всего, следует удостовериться, что питание ноутбука действительно отключено, так как некоторые ноутбуки могут находиться в режиме ожидания. Необходимо знать, что некоторые ноутбуки могут быть включены путем открытия крышки. Затем снять основной аккумулятор источника питания ноутбука;
- если требуется снять жесткий диск в реальных рабочих условиях, DEFR должен позаботиться о заземлении цифрового устройства, чтобы предотвратить повреждение жесткого диска от статического электричества. Иначе не следует снимать жесткий диск на месте эксплуатации. Необходимо промаркировать жесткий диск как подозрительный и документально зафиксировать все детали, такие как марка, название модели, серийный номер и объем жесткого диска;
- заклеить лентой слот для дискет, если он есть;
- удостовериться, что лотки для CD или DVD дисков задвинуты на место; отметить, являются ли они пустыми, содержат диски или не проверены; заклеить лентой слот для предотвращения его открывания.

Примечание – Если в устройстве оставлен носитель информации, который можно использовать для загрузки, то при следующем включении устройство может загрузиться с этого носителя, а не с жесткого диска (или флеш-памяти инструментальных средств для криминалистического исследования) в зависимости от установок BIOS .

7.1.3 Получение свидетельств

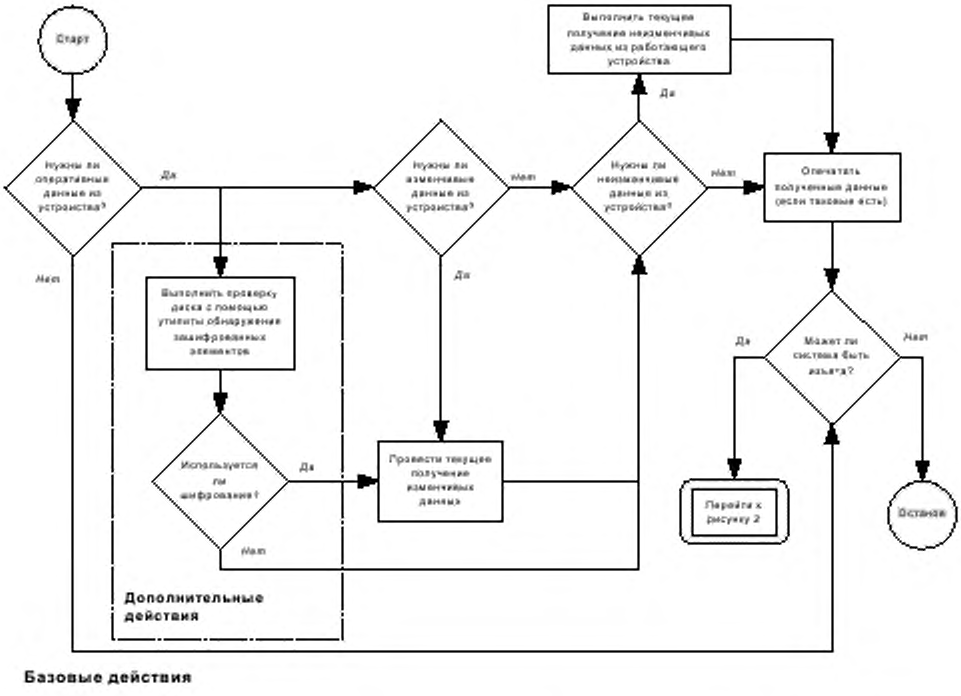
7.1.3.1 Цифровые устройства с включенным питанием

7.1.3.1.1 Общий обзор

Существуют три сценария, по которым можно проводить получение свидетельств: когда питание цифровых устройств включено, когда питание цифровых устройств выключено и когда питание цифровых устройств включено, но не может быть выключено (например, критичные для целевой задачи цифровые устройства). При всех трех сценариях DEFR обязан сделать точную копию свидетельств, представленных в цифровой форме, с носителей информации цифровых устройств, которые предположительно могут содержать потенциальные свидетельства, представленные в цифровой форме.

Если образ носителей нельзя получить, могут быть получены точные копии определенных файлов, которые предположительно могут содержать потенциальные свидетельства, представленные в цифровой форме. В идеале должна быть создана верифицированная главная копия и рабочая копия. Главную копию не следует использовать вновь, если только не требуется верифицировать содержание рабочей копии или создать замену рабочей копии после повреждения первой рабочей копии.

Когда питание цифрового устройства включено, DEFR может следовать ряду рекомендаций, касающихся получения свидетельств. Не все рекомендации являются идеальными и уместными для любых случаев; некоторые применимы только для определенных случаев. Соответственно, рекомендации можно классифицировать как обязательные или дополнительные. Следует обратить внимание на возможность того, что система с включенным питанием может войти в режим экранной заставки или автоматической блокировки и что возможны последствия любых действий, предпринимаемых для предотвращения этого. Например, применение программы имитации работы пользователя, потребует использования USB-ключа, что будет зарегистрировано системой, и эти действия, по тем или иным причинам, вызовут нежелательные изменения данных. Влияние последствий таких действий должно быть сведено к минимуму путем использования надежных методов. На рисунке 4 показаны базовые и дополнительные действия, применимые к получению свидетельств из цифровых устройств с включенным питанием.



Р и с у н о к 4 — Рекомендации по получению свидетельств из цифровых устройств с включенным питанием

7.1.3.1.2 Базовые действия: получение свидетельств из цифровых устройств с включенным питанием

Ниже приведены базовые действия, которым DEFR должен следовать во всех случаях, касающихся получения потенциальных свидетельств, представленных в цифровой форме, из цифровых устройств с включенным питанием:

- прежде всего, необходимо рассмотреть вопрос получения потенциальных свидетельств, представленных в цифровой форме, которые могут быть потеряны при выключении цифрового устройства. Они также известны как изменчивые данные, например, данные, хранящиеся в ОЗУ, данные работающих (активных) процессов, сетевых соединений и установки даты/времени. В случаях необходимости получения неизменчивых данных с устройств, которые все еще работают, должен быть рассмотрен вопрос выполнения получения свидетельств из устройства с включенным питанием;

- чтобы получить оперативные (рабочие) данные из работающих устройств, необходимо получать их в реальном масштабе времени. Получение в реальном масштабе времени изменчивых данных из ОЗУ может позволить восстановить ценную информацию, такую как состояние сети, дешифрованные приложения и пароли. Получение данных в реальном масштабе времени может проводиться с консоли или удаленно через сеть. Эти процессы различаются и требуют использования разных наборов инструментальных средств;

- DEFR никогда не должен доверять программам в системах. По этой причине DEFR рекомендуется использовать, где это возможно, собственные доверенные инструментальные средства (статические исполняемые файлы). DEFR должен быть компетентным в использовании валидных инструментальных средств и быть компетентным, чтобы учесть влияние, которое могут оказывать такие инструментальные средства на систему (например, замещение потенциальных свидетельств, представленных в цифровой форме, посредством вытеснения существующего содержимого страниц памяти при загрузке программного средства и т. д.). Все выполненные действия и результирующие изменения в потенциальных свидетельствах, представленных в цифровой форме, должны быть доку-

ментально оформлены и поняты. Если невозможно определить вероятное влияние введения инструментальных средств в систему, или нельзя с уверенностью определить результирующие изменения, этот факт также должен документироваться;

- при получении изменчивых данных DEFR должен использовать логический файл-контейнер, где это возможно, и зафиксировать значение его хэш-функции, когда он содержит файл(ы) изменчивых данных. Когда это невозможно, следует использовать такой контейнер, как ZIP-файл, который затем должен хэшироваться и должно быть зафиксировано значение хэш-функции. Получившиеся в результате файлы-контейнеры должны быть сохранены на цифровом носителе данных, который подготовлен для этих целей, т. е. отформатирован;

- выполнить процесс создания образа текущей энергонезависимой памяти с использованием утвержденного инструментального средства создания образа. Полученное свидетельство, представленное в цифровой форме, должно храниться на цифровом носителе информации, который был подготовлен для этой цели. Хотя предпочтительно использовать новый цифровой носитель информации, использование полученных достоверными процессами копий свидетельств, представленных в цифровой форме, обеспечивает уверенность в целостности данных при восстановлении. Таким образом, цифрового носителя информации, который был заново отформатирован, будет достаточно. Если образ должен храниться в логическом файле-контейнере, DEFR должен обеспечить уверенность в том, что образ не может быть поврежден или испорчен.

Примечание – В ситуациях, когда устройство заблокировано, физический доступ может быть получен с помощью других средств, дающих возможность прямого доступа к памяти, например, интерфейс Firewire.

7.1.3.1.3 Дополнительные действия: получение свидетельств из цифровых устройств с включенным питанием

Ниже приведены дополнительные действия, которые относятся к получению свидетельств из цифровых устройств с включенным питанием, в зависимости от конфигурации конкретного цифрового устройства:

- если есть подозрение на использование шифрования диска, то необходимо рассмотреть вопрос получения изменчивых данных в ОЗУ. Сначала нужно проверить, действительно ли это так, подвергнув диск проверке с использованием какой-либо утилиты, обнаруживающей шифрование. Если это действительно так, нужно помнить о том, что действующая серверная операционная система может не заслуживать доверия, так что нужно рассмотреть вопрос использования соответствующих надежных и утвержденных инструментальных средств;

- необходимо использовать надежный источник времени и документировать время каждого выполненного действия;

- целесообразно установить связь между DEFR и полученными свидетельствами, представленными в цифровой форме, используя, например, цифровые подписи, биометрию или фотографирование.

Примечание – Цифровое устройство может быть сконфигурировано так, что при нажатии кнопки питания на нем запустится сценарий, который может изменять или удалять информацию в системе перед отключением или предупреждать подключенные системы о возникновении неожиданного события, так что эти системы могут стирать данные, имеющие доказательную ценность, прежде чем они будут идентифицированы. Также оно может быть сконфигурировано таким образом, чтобы приводить в действие устройство, предназначенное для причинения физического вреда DEFR и другим присутствующим лицам.

7.1.3.2 Цифровые устройства с выключенным питанием

7.1.3.2.1 Общий обзор

Обращение с цифровым устройством с выключенным питанием проще, чем с цифровым устройством с включенным питанием, поскольку нет необходимости в получении изменчивых данных. На рисунке 5 показаны действия, применимые к получению свидетельств из цифровых устройств с выключенным питанием.



Рисунок 5 — Рекомендации по получению свидетельств из цифровых устройств с выключенным питанием

7.1.3.2.2 Получение свидетельств из цифровых устройств с выключенным питанием

Ниже приведены действия, относящиеся к получению свидетельств, когда питание цифрового устройства выключено:

- необходимо обеспечить уверенность в том, что устройство действительно выключено;
- если это применимо, то следует удалить ОЗУ из цифрового устройства с выключенным питанием, если оно еще не удалено. Нужно промаркировать запоминающее устройство как подозрительное и документально зафиксировать все детали, такие как марка, название модели, серийный номер и объем запоминающего устройства;
- выполнить процесс создания образа посредством использования валидного инструментального средства для создания образа, чтобы получить копию свидетельства, представленного в цифровой форме, подозреваемого диска.

Примечание – В большинстве случаев носитель информации не должен извлекаться из цифрового устройства, пока не будет принято решение о получении свидетельств, так как его извлечение увеличивает риск повредить или перепутать его с другими носителями. Должны быть разработаны и выполнены локальные процедуры, касающиеся необходимости удаления жестких дисков.

7.1.3.3 Цифровые устройства, критичные для целевой задачи

В некоторых случаях питание цифровых устройств нельзя отключить из-за критичного характера систем. К таким системам относятся серверы в информационных центрах, которые также могут обслуживать добросовестных клиентов, системы наблюдения, медицинские системы и многие другие, которые могут оказывать критическое влияние в случае их прерывания или выключения. При обращении с такими системами следует проявлять особую осторожность.

Если цифровое устройство не может быть выключено, нужно провести текущее и (или) частичное получение свидетельств, как обсуждается в 7.1.3.1.3 и 7.1.3.4.

7.1.3.4 Частичное получение свидетельств

Частичное получение свидетельств может осуществляться по нескольким причинам, например:

- объем запоминающего устройства системы слишком велик для получения его копии (например, сервер базы данных);
- система является слишком критичной, чтобы допустить выключение;
- только когда выделенные для получения данные, содержат другие несоответствующие данные в той же системе; или
- в случае ограничений, поступающих от правового органа, например, ордер на обыск, ограничивающий рамки получения свидетельств.

Когда принимается решение о проведении частичного получения свидетельств, выполняемые действия должны включать следующее, но не ограничиваться этим:

- нужно идентифицировать директорию(и), файлы(ы) и любые необходимые частные опции системы, доступные для получения желаемых данных;
- провести логическое получение таких установленных данных.

7.1.3.5 Цифровые носители информации

На месте инцидента можно обнаружить различные виды цифровых носителей информации. Обычно они являются наименее изменчивым видом данных и могут иметь самый низкий приоритет во время сбора и получения свидетельств. Это не означает, что они не важны, поскольку во многих слу-

чаях внешние цифровые носители информации будут содержать свидетельства, которые ищут аналитики. DEFR должен обеспечить следующее:

- проверить и документально оформить расположение (например, отсека для установки дискового накопителя, кабеля и разъема, порта USB и т. д.), марку, модель и серийный номер (если они есть) любого обнаруженного цифрового носителя информации;

- принять решение, осуществлять ли сбор идентифицированного цифрового носителя информации или получение свидетельств на месте, решение должно быть основано на характере инцидента и доступных ресурсах. Чтобы проводить получение на месте для цифрового носителя информации (в основном жесткого диска), следует обратиться к рисунку 4;

- если DEFR принимает решение, и ему дается разрешение осуществлять сбор цифровых носителей информации, то собранные носители информации должны быть завернуты или помещены в соответствующую упаковку;

- промаркировать все цифровые носители информации и любые связанные с ними детали. Эта маркировка не должна наноситься непосредственно на механические части цифровых устройств и закрывать или скрывать важную идентификационную информацию, такую как серийный номер, номер модели и номер детали. Со всех собранных устройств должно быть организовано получение свидетельств, и они должны храниться таким образом, чтобы была обеспечена уверенность в целостности собранных носителей информации. Там где это возможно свидетельства должны быть заклеены этикеткой с печатью для индикации вскрытия, и DEFR или ответственное лицо должны поставить подпись на печать;

- собранные цифровые носители информации должны храниться в среде, пригодной для обеспечения сохранности данных;

- разные цифровые носители информации имеют разные возможности хранения данных. DEFR должен знать допустимый максимальный период времени возможного хранения данных на носителе, который определен соответствующей юрисдикцией.

7.1.4 Сохранение

После завершения процесса получения свидетельств DEFR должен принять окончательное решение в отношении полученных данных, используя функции верификации или цифровые подписи, чтобы определить, какие копии свидетельств, полученных в цифровой форме, эквивалентны оригиналам. Кроме того, аспекты безопасности требуют мер и средств контроля и управления, которые применяют принципы сохранения конфиденциальности, целостности и доступности потенциальных свидетельств, представленных в цифровой форме. В целях защиты от хищения должны быть рассмотрены факторы окружающей среды с принятием соответствующих мер. DEFR должен обеспечить следующее:

- использовать соответствующую функцию верификации для предоставления свидетельств того, что скопированные файлы эквиваленты оригиналам;

- целесообразно установить связь между DEFR и полученными свидетельствами, представленными в цифровой форме, используя, например, цифровые подписи, биометрию или фотографирование.

Все собранные цифровые устройства требуют обеспечения соответствующей сохранности. Различные виды цифровых устройств могут требовать различных методов сохранения. Потенциальные свидетельства, представленные в цифровой форме, требуется сохранять на всем протяжении времени их существования, которое может варьироваться в разных юрисдикциях и организационной политике.

Примечание – DEFR может использовать биометрию в качестве альтернативы процессу заверения полученных данных с помощью функций верификации или цифровой подписи. Биометрия использует физические и поведенческие характеристики для определения личности человека. Связывая биометрическую характеристику с полученным свидетельством, можно обеспечить уверенность в том, что свидетельство не может быть испорчено без компрометации биометрической характеристики.

7.2 Сетевые устройства

7.2.1 Идентификация

7.2.1.1 Общий обзор

В контексте данного подраздела в качестве сетевых устройств рассматриваются компьютеры или иные цифровые устройства, соединенные с сетью проводным или беспроводным способом. Та-

кие сетевые устройства могут включать мэйнфреймы, серверы, настольные компьютеры, точки доступа, коммутаторы, концентраторы, маршрутизаторы, мобильные устройства, PDA, PED, Bluetooth-устройства, системы CCTV и многие другие. Обратите внимание, что если цифровые устройства подключены к сети, трудно установить, где хранятся искомые потенциальные свидетельства, представленные в цифровой форме. Данные могут находиться в любом месте в сети.

При идентификации цифровых устройств учитываются их компоненты, такие как фирменные знаки производителей, серийные номера, специальные подставки и адаптеры источников питания. DEFR может рассматривать следующие аспекты в качестве средств идентификации:

- характеристики устройства. Марка и производитель цифрового устройства иногда могут быть идентифицированы по его наблюдаемым характеристикам, особенно в случае существования уникальных элементов дизайна;

- интерфейс устройства. Разъем питания часто бывает характерным для производителя и надежно способствует идентификации;

- маркировка устройства. Для выключенных мобильных устройств полезной может оказаться информация, считанная из углубления для аккумулятора, особенно, когда она связана с соответствующей базой данных. Например, IMEI – это уникальный 15-разрядный номер в десятичном представлении, указывающий производителя, номер модели и страну для GSM-устройств; ESN – это уникальный 32-битный идентификатор, зафиксированный на чипе мобильного телефона производителем; первые 8-14 бит идентифицируют производителя, а остальные – присвоенный серийный номер;

- обратный поиск. В случае мобильных телефонов, если номер телефона известен, обратный поиск может использоваться для идентификации сетевого оператора.

Вследствие того, что мобильные устройства обычно бывают небольшого размера, DEFR должен уделить особое внимание выявлению всех видов мобильных устройств, которые могут иметь отношение к делу. DEFR должен охранять место предполагаемого инцидента и обеспечивать уверенность в том, что никто не удалит мобильные или любые другие цифровые устройства с места инцидента. Цифровые устройства, которые могут содержать потенциальные свидетельства, представленные в цифровой форме, должны быть защищены от несанкционированного доступа.

Примечание – В некоторых случаях связь не должна быть прервана. Нужно проинформировать уполномоченных лиц о возможных проблемах (например, невозможность уведомления неизвестного лица о выключении устройства).

7.2.1.2 Поиск и документирование на физическом месте инцидента

Прежде чем может быть проведен сбор или получение свидетельств, место инцидента должно быть зафиксировано в визуальной форме с использованием фотоаппарата, видеокамеры или эскизного плана места инцидента так, как оно выглядит со стороны входа. Выбор метода фиксирования нужно сопоставлять с обстоятельствами, расходами, временем, доступными ресурсами и приоритетами. DEFR должен документально оформить все иные предметы на месте инцидента, которые могут содержать потенциально необходимые материалы, такие как рукописные заметки, записки-наклейки, ежедневники и т. д.;

- DEFR должен документально оформить вид, марку, модель и серийные номера всех используемых цифровых устройств и идентифицировать все цифровые устройства, которые могут потребоваться для сбора или получения свидетельств на этом начальном этапе. Если потребуется, должны быть документально оформлены и собраны все мобильные устройства и связанные с ними элементы, такие как карты памяти, SIM-карты, зарядные устройства, подставки, обнаруженные на месте инцидента, их соответствующие серийные номера и любые идентифицирующие особенности. Нужно также попытаться найти исходную упаковку мобильных телефонов, она может содержать PIN- и PUK-коды;

- если устройство подключено к сети, DEFR должен определить предоставляемые устройством услуги, чтобы понять зависимости и выяснить критичность устройства в сети, прежде чем принимать решение об отключении его от сети. Это является важным, если устройства обслуживают критичные для целевой задачи функции, не допускающие никакого простоя, или если требуется избежать разрушения потенциальных свидетельств, представленных в цифровой форме. Однако если окажется, что существуют сетевые угрозы устройствам, DEFR может потребоваться принять решение об отсоединении устройства от сети, чтобы защитить потенциальные свидетельства, представленные в цифровой форме;

- если сетевым устройством является CCTV, DEFR должен отметить число камер, подключенных к системе, а также то, какие из этих камер ведут активную запись. DEFR должен отметить марку, модель и основные параметры системы, такие как параметры настройки экрана, текущие параметры записи и место хранения, чтобы в случае необходимости внесения изменений для содействия процессу сбора и получения свидетельств, можно было вернуть систему в исходное состояние;

- насколько это возможно, состояние цифровых устройств должно оставаться неизменным. Обычно, если цифровые устройства выключены, DEFR не должен их включать, а если цифровые устройства включены, DEFR не должен их выключать. Это может предотвратить ненужное повреждение потенциальных свидетельств, представленных в цифровой форме. Устройство, имеющее аккумуляторные батареи, которые могут разрядиться, следует подключить к зарядному устройству для обеспечения уверенности в том, что информация не будет потеряна. DEFR необходимо определить на этом этапе потенциальные зарядные устройства и кабели. Если дата транспортировки и изучения устройства неизвестна, может быть целесообразным выключить его, чтобы свести к минимуму возможность повреждения содержащихся в устройстве данных;

- DEFR необходимо также рассмотреть вопрос использования детектора сигналов беспроводной сети для обнаружения и идентификации сигналов от беспроводных устройств, которые могут быть спрятаны. Возможны случаи, когда детектор сигналов беспроводной сети не используется из-за финансовых и временных ограничений, тогда DEFR должен документально оформить это.

7.2.2 Сбор, получение и сохранение свидетельств

7.2.2.1 Общий обзор

DEFR нужно решить, осуществлять ли сбор или получение потенциальных свидетельств, представленных в цифровой форме, из цифровых устройств. Выбор должен быть сопоставлен с обстоятельствами, расходами, временем, доступными ресурсами и приоритетами.

Если DEFR принимает решение об отключении устройств от сети, процесс сбора или получения потенциальных свидетельств, представленных в цифровой форме, будет продолжаться как описано в 5.4. В том случае, если устройства не могут быть отключены от сети из-за критичности их функций или вероятности разрушения потенциальных свидетельств, представленных в цифровой форме, DEFR должен оперативно провести получение свидетельств, пока устройства остаются подключенными к сети.

Примечание – Крайне важно наличие надежных стандартных процедур, использующих валидные инструментальные средства, в сочетании с надлежащей документацией и подготовленным опытным DEFR.

Сбор и получение потенциальных свидетельств, представленных в цифровой форме, с сетевых мобильных устройств осложняется тем, что они могут иметь несколько режимов работы и способов взаимодействия, таких как Bluetooth, радиочастотный, сенсорный экран, инфракрасный. Кроме того, различные производители мобильных устройств используют разные виды операционных систем, что требует разных методов получения свидетельств. Также существует широкий диапазон карт памяти, которые могут использоваться в мобильных устройствах, и удаление этих карт памяти из включенных мобильных устройств может помешать действующим процессам.

Обычно мобильные устройства, такие как PDA и мобильные телефоны, должны быть включены для получения потенциальных свидетельств, представленных в цифровой форме. Эти устройства могут постоянно изменять свою операционную среду, когда они включены, например, может корректироваться датчик времени. Связанная с этим проблема состоит в том, что две копии свидетельства, представленного в цифровой форме, одного и того же устройства могут не пройти стандартные функции верификации, такие как хэширование. В такой ситуации более приемлемыми могут быть альтернативные функции верификации, выявляющие области совместимости и (или) различий.

Важно, чтобы DEFR не вносил на место инцидента устройства Wi-Fi или Bluetooth, которые могут изменить информацию об установлении связи на потенциальных устройствах-свидетельствах. Это особенно важно, если при расследовании требуется знать, между какими устройствами была установлена связь.

Если DEFR принимает решение о проведении процесса получения свидетельств, сетевые устройства следует оставить работающими для дальнейшего анализа, чтобы обнаружить другие устройства, соединенные с сетевыми устройствами. DEFR должен учесть возможность саботажа, осуществляемого подозреваемым через активное сетевое соединение, и принять решение либо о проведении мониторинга сети, либо об отсоединении от неё.

7.2.2.2 Рекомендации по сбору сетевых устройств

В некоторых случаях может быть уместно оставить сетевые устройства подключенными к сети, чтобы DEFR и (или) DES с соответствующими полномочиями могли проводить мониторинг и документирование. Там где это необходимо сбор устройств должен осуществляться описанным ниже образом:

- DEFR должен изолировать устройство от сети, когда будет ясно, что никакие значимые данные не будут перезаписаны в результате этого действия, а в важных системах (например, в системах управления аппаратурой в больницах) не произойдет никакого сбоя. Это можно сделать, вынув разъем из гнезда проводного сетевого соединения с телефонной системой или сетевым портом, или отключив соединение с беспроводной точкой доступа;

- перед отключением от проводной сети DEFR должен отследить соединения с цифровыми устройствами и промаркировать порты для последующего восстановления сети. Устройство может иметь более одного вида связи. Например, в случае компьютера это могут быть проводные ЛВС, беспроводной модем и карты мобильного телефона. PED могут быть также подключены к сети через соединения Wi-Fi, Bluetooth или соединения мобильной телефонной сети. DEFR должен попытаться идентифицировать все виды связи и предпринять соответствующие действия для защиты потенциальных свидетельств, представленных в цифровой форме, от разрушения;

- нужно сознавать, что выключение питания сетевых устройств в этот момент может уничтожить изменчивые данные, такие как данные активных процессов, сетевых соединений и данные, хранящиеся в памяти. Серверная операционная система может быть не заслуживающей доверия и сообщать неверную информацию. DEFR должен зафиксировать изменчивую информацию, используя надежные верифицированные методы, перед выключением питания устройств. Соединения сетевых устройств могут быть отключены, когда DEFR будет уверен, что в результате не будут потеряны никакие потенциальные свидетельства, представленные в цифровой форме;

- если сбор предшествует получению свидетельств и известно, что устройство имеет энергозависимую память, устройство должно быть постоянно подключено к источнику питания;

- если мобильное устройство выключено, его следует тщательно упаковать, опечатать и промаркировать. Это делается для того, чтобы избежать любого случайного или намеренного срабатывания клавиш или кнопок. В качестве меры предосторожности DEFR должен также рассмотреть вопрос использования клетки Фарадея или экранированных контейнеров;

- при некоторых обстоятельствах мобильные устройства должны быть отключены при сборе с целью предотвращения изменения данных. Изменения могут происходить через исходящие и входящие соединения или команды, которые могут вызывать разрушение потенциальных свидетельств, представленных в цифровой форме;

- впоследствии с каждым цифровым устройством до его изучения следует обращаться так, как если бы оно являлось автономным устройством (см. 7.1). Во время изучения его следует считать сетевым устройством.

Примечание – Это можно осуществить сформировав сеть, используя съемные устройства хранения информации в качестве передающей среды. DEFR должен рассмотреть, могли ли собранные устройства использоваться таким образом, и искать информацию о других устройствах с неавтоматическим переносом файлов для такой сети.

7.2.2.3 Рекомендации по получению свидетельств из сетевых устройств

В ситуации, когда устройства подключены к сети, существует возможность соединения устройства более чем с одной физической и (или) виртуальной сетью. Например, устройство, которое кажется имеющим одно видимое физическое сетевое соединение, в действительности может входить в виртуальную частную сеть и быть виртуальной машиной с более чем одним IP-адресом. Поэтому перед отключением устройства от сети DEFR должен провести логическое получение данных, связанных с логическим сетевым соединением (например, подключение к Интернет). Связанные с этим данные включают IP-конфигурацию и таблицы маршрутизации, но не ограничиваются этим.

Для сетевых устройств, которые должны быть постоянно включены, необходимо предотвращать взаимодействие устройства с беспроводной радиосетью, включая устройства на базе GPS. DEFR должен применять разрешенные национальным законодательством методы блокирования радиосигналов. Однако следует позаботиться об обеспечении уверенности в том, что устройство имеет адекватный источник питания, поскольку методы блокирования могут привести к использованию его до-

полнительной мощности при попытке связаться с сетью. Методы блокирования могут включать следующее, но не ограничиваться этим:

- использование устройства радиоэлектронного подавления, которое способно блокировать передачу путем создания сильных помех, посылая сигналы в том же диапазоне частот, который используется мобильным устройством.

Примечание 1 – Использование радиоэлектронного подавления может привести к нарушению правовых требований некоторых юрисдикций.

Примечание 2 – Использование радиоэлектронного подавления может негативно влиять на функционирование ряда электронных устройств, таких как медицинское оборудование;

- использование экранирования рабочей области для безопасного проведения изучения в фиксированном месте. Для предотвращения соединений с сетью экранирование может осуществляться для всей рабочей области или с использованием клетки Фарадея, обеспечивающей портативность. Однако подведение кабелей питания в клетку Фарадея является трудноразрешимой проблемой, поскольку без надлежащей изоляции они могут действовать как антенна, сводя на нет само назначение клетки. Рабочее пространство тоже может быть очень ограниченным;

- использование экранирования рабочей области для безопасного проведения изучения в фиксированном месте. Для предотвращения соединения с сетью может использоваться радиочастотное экранирование рабочего пространства или контейнера (клетка Фарадея).

Примечание 3 – Требуется валидация всех методов блокирования беспроводного доступа к сетям на соответствующих частотах. Эта валидация должна распространяться на кабели, проходящие через экранирующую оболочку;

- использование заменителя (U)SIM-карты, который имитирует идентификатор исходного устройства и предотвращает доступ к сети устройства. Эти карты могут «обмануть» устройство, принимающее их за оригинальную (U)SIM-карту, и позволяют проводить безопасное изучение в любом месте. Требуется валидация (U)SIM-карты для устройства и сети до использования;

- блокирование сетевых услуг путем договоренности с компанией, предоставляющей услуги мобильной связи, и определения деталей блокируемых услуг (например, идентификатор оборудования, идентификатор абонента или номер телефона). Однако такая информация не всегда легкодоступна — процесс согласования и подтверждения может вызывать задержку.

DEFR может выполнить оперативное получение свидетельств из мобильного устройства, прежде чем убрать аккумуляторную батарею (например, для доступа к SIM-карте). Это делается с целью предотвращения потери потенциально важной информации в ОЗУ телефона или для ускорения процесса изучения (например, когда считается, что устройство может быть защищено ПИН- и (или) PUK-кодом, на получение которых уйдет много времени).

Примечание 4 – DEFR должен обеспечивать уверенность в том, что сбор и получение потенциальных свидетельств, представленных в цифровой форме, осуществляется в соответствии с законами и предписаниями местной юрисдикции, как того требуют конкретные обстоятельства.

7.2.2.4 Рекомендации по сохранению сетевых устройств

Вследствие характера цифровых устройств и потенциальных свидетельств, представленных в цифровой форме, принципы сохранения сетевых устройств аналогичны принципам сохранения для компьютеров, периферийных устройств и цифровых носителей информации. См. 7.1.4, где приведены детальные рекомендации по сохранению устройств.

7.3 Принципы сбора, получения и сохранения для CCTV

DEFR должен понимать, что подход к извлечению фрагмента видеозаписи из компьютера или встроенного цифрового видеомагнитофона системы CCTV отличается от традиционного извлечения свидетельств, представленных в цифровой форме, из компьютера. Ниже приведены специальные рекомендации по получению потенциальных свидетельств для систем CCTV:

- до начала процесса получения свидетельств DEFR, прежде всего, должен определить, записала ли система видеофрагмент, представляющий интерес. Затем DEFR должен определить временной интервал требуемого отснятого видеоматериала, сравнить время системы с истинным временем и отметить любое расхождение. DEFR должен также определить, с каких камер необходимо и возможно получение свидетельств. Он должен отметить марку и модель системы. Эта информация может потребоваться для обеспечения надлежащих программных средств воспроизведения;

- DEFR должен получить все представляющие интерес видеозаписи камер видеонаблюдения на интересующее время, чтобы сохранить дополнительную следственную информацию, которая может быть разработана позднее. DEFR должен отметить все камеры, соединенные с CCTV и определить, вели они запись или нет;

- DEFR должен определить объем запоминающего устройства системы CCTV, а также то, когда в ней запланирована перезапись видеоинформации (поверх ранее записанной). Эта информация позволит DEFR понять, как долго будет храниться видеозапись в системе, прежде чем будет потеряна. Должны быть приняты меры для обеспечения уверенности в том, что свидетельства не будут изменены. Для видеосвидетельств, представленных в цифровой форме, необходимо обеспечить защиту записи;

- существует несколько вариантов, которые DEFR может выбирать для получения потенциальных свидетельств, представленных в цифровой форме, из систем CCTV:

1) получение видеофайлов, путем их записи на CD/DVD/Blu-Ray-диск, но это может быть неосуществимо, если видеофайл слишком велик;

2) получение видеофайлов, путем их записи на внешний носитель информации;

3) получение видеофайлов через сетевое соединение. Это может быть доступно, если система CCTV имеет сетевой порт;

4) использование функции преобразования видеофайлов CCTV в другие форматы файла (обычно MPEG или AVI), являющиеся сжатой версией отснятого видеоматериала. Это должно использоваться как крайнее средство, поскольку восстановление сжатых данных изменяет исходные данные, и всегда убирает детали изображения. Не рекомендуется полагаться на восстановленные сжатые данные для изучения того, существуют ли исходные данные и доступны ли они для анализа.

Примечание 1 – Качество преобразованного видеоматериала может быть не таким хорошим, как у исходного отснятого материала;

5) если невозможно сразу получить копии свидетельства, представленного файлом в цифровой форме, с имеющегося записывающего устройства, DEFR или DES должны пытаться получить аналоговые копии с аналогового выхода исходного записывающего устройства, используя соответствующее аналоговое устройство записи;

- после завершения получения свидетельств, полученный файл должен быть проверен, чтобы убедиться в получении надлежащего файла или надлежащей части файла;

- необходимо также проверить воспроизводимость файла в других системах с помощью программных средств воспроизведения (для цифровых форматов файлов) — большинство CCTV являются частными и их файлы могут не воспроизводиться при использовании других программных средств воспроизведения. Соответствующие программные средства воспроизведения могут быть доступны для скачивания из CCTV одновременно с видеоданными;

- цифровой носитель информации, содержащий полученный файл, следует рассматривать как основную копию свидетельств, представленных в цифровой форме. Если файл был загружен в ноутбук или карту памяти / USB-устройство, то с них незамедлительно должна быть сделана надежная основная копия;

- после этого DEFR должен перезапустить CCTV, если она была отключена. Это должно быть сделано в присутствии уполномоченного лица.

В случае, когда получение свидетельств на месте происшествия невозможно, DEFR может принять решение о сборе цифровых носителей информации. Быстрым методом является замена жесткого диска CCTV чистым или абсолютной копией жесткого диска. Однако перед использованием этого метода DEFR должен оценить ряд рисков, таких как совместимость нового жесткого диска с системой и совместимость снятого жесткого диска с другими системами для проведения изучения.

Примечание 2 – В некоторых системах имеется сменный жесткий диск в специальном контейнере, но этот жесткий диск может потребовать аппаратных средств системы для воспроизведения.

Если ни один из вышеупомянутых методов невозможен, то вся CCTV должна быть снята с места инцидента и процесс получения свидетельств должен осуществляться в лаборатории судебной экспертизы. Это является последним средством для DEFR при условии, что это физически возможно, поскольку некоторые CCTV являются очень большими и сложными. Перед проведением этого DEFR должен еще раз оценить риски правовых последствий и страхования.

В зависимости от характера цифровых устройств и потенциальных свидетельств, представленных в цифровой форме, рекомендации по сохранению CCTV аналогичны рекомендациям по сохранению компьютеров, периферийных устройств и цифровых носителей информации. Рекомендации по сохранению CCTV см. в 7.1.4.

Приложение А
(справочное)

Описание основных навыков и компетентности DEFR

Таблица А.1 — Примеры описаний компетентности

№	Основные навыки	Описание основных навыков	Описание компетентности		
			Осведомленность (1)	Знания (2)	Умение (3)
1	Идентификация свидетельств, представленных в цифровой форме	Характеристики цифровых устройств, компонентов и информации, которые могут помочь расследованию, а также соответствующих законов для обработки потенциальных свидетельств, представленных в цифровой форме, и нарушений, связанных с использованием компьютера. Определение требований к инструментальным средствам для сбора и получения данных и устройств, а также оценка риска	Обычное использование ИТ и администрирование многих видов ИТ-устройств и сетевых устройств; следственные действия на месте нарушения; определение состояния устройства; значение доказательной информации; следственный анализ сети и связанных с ней устройств и информации	Журналы регистрации и конфигурация систем/приложений; идентификация системных журналов и журналов приложений, включая контрольные журналы электронной почты, сетевые контрольные журналы, журналы регистрации доступа, файлы паролей, файлы конфигураций, информация IP-хоста; функциональные возможности и зависимости устройств; знание факторов, влияющих на изменчивые и неизменчивые свидетельства	Специальный анализ; интерпретация контрольных журналов с целью обнаружения вторжений и выявления других затронутых систем (некоторые юрисдикции требуют представить подтверждающие доказательства до начала сбора); определение паролей, необходимых для соответствующих устройств, до начала сбора; определение схемы сети и механизмов управления доступом для понимания зависимостей; связывание IP-адресов и MAC-адресов * для идентификации устройства в сети

Продолжение таблицы А.1

№	Основные навыки	Описание основных навыков	Описание компетентности		
			Осведомленность (1)	Знания (2)	Умение (3)
2	Сбор свидетельств, представленных в цифровой форме	Требования к инструментальным средствам и осуществление упаковки свидетельств, представленных в цифровой форме, защита от угроз внешней среды. Знание областей, обеспечивающих доверие к информации	Общая безопасность сбора данных; принципы действия и конструкция основных инструментальных средств; определение лучшего метода сбора для сохранения максимума информации, имеющей отношение к инциденту	Выполнение и описание процесса сбора; сбор свидетельств; создание документации по свидетельствам; история хранения свидетельств; контроль качества процесса сбора свидетельств; опрос подозреваемых	Оптимизация процесса сбора; документальное подтверждение того, что не может быть получено вследствие различных ограничений; сбор паролей, ключей, защитных ключей-заглушек и другой информации, необходимой для проведения анализа в лаборатории
3	Получение свидетельств, представленных в цифровой форме	Применение требований получения потенциальных свидетельств, представленных в цифровой форме, в логическом виде, обеспечение уверенности в повторяемости, воспроизводимости и возможности обоснования. Охватываемые сферы включают получение свидетельств из систем с включенным питанием, систем с выключенным питанием и следственный анализ сети	Понимание информации, доступной в цифровых устройствах, базах данных, генерируемых системой записях, генерируемых пользователем данных и изменчивых данных; структура системных файлов и приложений Unix и Windows; понимание влияния на изменчивые данные	Знание того, как определить потребности в памяти; выполнение процедуры создания образа (например, цифрового носителя информации в целом или его части); получение свидетельств, осуществляемое из систем с включенным питанием и систем с выключенным питанием; генерация значений хэш-функции	Способность осуществлять получение свидетельств из цифровых носителей информации, включая RAID, базы данных, приборы и миниустройства; понимание зависимостей и влияния на различные методы получения свидетельств

Окончание таблицы А.1

№	Основные навыки	Описание основных навыков	Описание компетентности		
			Осведомленность (1)	Знания (2)	Умение (3)
4	Сохранение свидетельств, представленных в цифровой форме	Применение и оценка требований сохранения потенциальных свидетельств, представленных в цифровой форме, понимание факторов и параметров, влияющих на их точность. Охватываемые сферы включают методику, поддержку истории хранения, обращение с компьютерными устройствами и обращение с цифровыми носителями	Понимание требований и процедур для поддержки истории хранения согласно правовым требованиям; влияния факторов внешней среды, таких как влажность, температура и вибрация на цифровые устройства; понимание вариантов упаковки, требований транспортирования и хранения	Знание того, как создать документацию по проверке свидетельств; определение параметров для документирования; обеспечение уверенности в информационной безопасности, угрозы, уязвимости и меры и средства контроля и управления для свидетельств, представленных в цифровой форме	Применение мер для обеспечения безопасности свидетельств, представленных в цифровой форме, в виде больших и миниатюрных переносных устройств; процедуры документирования деталей происшедшего в свидетельствах

* MAC-адрес — (Media Access Control address) аппаратный адрес устройства, присоединённого к сетевой среде.

Таблица А.2 — Определение компетентности

1	Осведомленность – Распознание, определение – при необходимости обращение за помощью
2	Знание – Приобретенное путем формального обучения или работы в группе. Содействие, участие – действие с помощью
3	Умение – Доказанный опыт в результате применения в рабочей среде. Работа без надзора. Применение, демонстрация – действие без помощи

Примечание – Компетентность DEFR может различаться в зависимости от юрисдикции.

Приложение В
(справочное)

Минимальные требования к документации для передачи свидетельств

DEFR должны нести ответственность за полученные данные и цифровые устройства в любое время, пока данные и цифровые устройства находятся под их контролем. Для поддержания такого контроля DEFR должен быть квалифицированным, надлежащим образом обученным и уполномоченным. Однако вследствие того, что местное законодательство является определяющим фактором в отношении способности DEFR соответствовать всем трем ожидаемым требованиям, компетентность DEFR может различаться в разных юрисдикциях. В результате может получиться, что требования к документации для обмена свидетельствами, представленными в цифровой форме, между юрисдикциями окажутся различными в разных юрисдикциях.

Соответственно, для содействия обмену потенциальными свидетельствами, представленными в цифровой форме, между юрисдикциями нужно определить минимальный набор требований к документации. Эти требования к документации нужно рассматривать вместе с особенностями документирования, упомянутыми в 6.6. Поскольку настоящий стандарт не заменяет конкретных правовых требований любой юрисдикции, он служит в качестве практического руководства по передаче потенциальных свидетельств, представленных в цифровой форме, через границы юрисдикций.

Минимальной документированной информацией, подлежащей передаче, является:

- наименование и адрес компетентного органа;
- изложение полномочий, уровня обучения и квалификации DEFR;
- цель изучения;
- какие действия были выполнены;
- кто и когда осуществлял их;
- история хранения, относящаяся к конкретному расследованию;
- описательный перечень собранных и полученных потенциальных свидетельств, представленных в цифровой форме, и цифровых носителей информации;
- информация, касающаяся любого рассмотрения, тестирования или исследования, использованная в отношении созданной копии свидетельства.

Характерные для юрисдикции требования могут включать следующее:

- если свидетельством считается экспертное заключение, то признание соответствующего кодекса проведения экспертных доказательств;
- постановление суда, определяющее, какая документация должна быть передана и причины ее передачи.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/ТО 15801	—	*
ИСО/МЭК 17020:2012	IDT	ГОСТ Р ИСО/МЭК 17020 – 2012 «Оценка соответствия. Требования к работе различных типов органов инспекции»
ИСО/МЭК 17025:2005	IDT	ГОСТ Р ИСО/МЭК 17025 – 2009 «Общие требования к компетентности испытательных и калибровочных лабораторий»
ИСО/МЭК 27000:2009	IDT	ГОСТ Р ИСО/МЭК 27000 – 2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание – В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:
– IDT — идентичный стандарт.

Библиография

[1] ILAC–G19:2002. Guidelines for forensic science laboratories. Доступно на сайте: gost.e-ecolog.ru 9_2002.pdf

[2] IOCE, G8 proposed principles for the procedures relating to digital evidence. Доступно на сайте: http://ioce.org/core.php?ID=5

[3] ISO/IEC 15489:2001, Information and Documentation – Records Management (ИСО/МЭК 15489:2001 Информация и документация. Управление записями) *

[4] ISO/IEC 17024:2003, Conformity assessment – General requirements for bodies operating certification of persons (ИСО/МЭК 17024:2003 Оценка соответствия. Общие требования к органам, проводящим сертификацию персонала) *

[5] ISO/IEC 17043:2010, Conformity assessment – General requirements for proficiency testing (ИСО/МЭК 17043:2010 Оценка соответствия. Общие требования к проверке квалификации лабораторий) *

[6] ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements

[7] ISO/IEC 27002, Information technology – Security techniques – Information security management systems – Code of practice for information security management

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

[9] ISO/IEC 27031:2010, Information technology – Security techniques – Guidelines for ICT readiness for business continuity

[10] ISO/IEC 27035:2011, Information technology – Security techniques – Information security incident management

[11] Forensic Science Society Academic Accreditation Standards & CPD. Доступно на сайте: http://www.forensic-science-society.org.uk

[12] Guidelines for evidence collection and archiving. Доступно на сайте: gost.e-ecolog.ru

* Официальный перевод этого стандарта находится в Федеральном информационном фонде.

УДК 006.034: 004.056: 004.057.2 ОКС 35.040

Ключевые слова: информационная технология, мера и средство контроля и управления, свидетельство в цифровой форме, идентификация свидетельств, сбор свидетельств, получение свидетельств, сохранение свидетельств, специалист по свидетельствам

Подписано в печать 02.12.2014. Формат 60x84⅛.
Усл. печ. л. 5,58. Тираж 32 экз. Зак. 5164

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»,
123995 Москва, Гранатный пер., 4.
www.gostinfo.ru
gost.e-ecolog.ru
gost.e-ecolog.ru