ПРОЕКТ
Утверждены
постановлением
Кабинета Министров
Кыргызской Республики
от _____ 2023 года №___

ПРАВИЛА
идентификации, изъятия, получения, хранения и исследования цифровой информации в уголовном судопроизводстве

1. Общие положения

1. Настоящие Правила разработаны в соответствии с Уголовным процессуальным кодексом Кыргызской Республики и регламентируют практические действия органов дознания и следствия, специалистов и экспертов (далее «Специалист») при идентификации, изъятия, получении, хранении и исследовании цифровой информации по уголовным делам.
2. Целью настоящих Правил является:
   - установление для Специалиста минимальных стандартов, применимых к процессу идентификации, изъятия, получения, хранения и исследования цифровой информации для целей уголовного судопроизводства;
   - обеспечение эффективности процесса работы с цифровой информацией;
   - обеспечение целостности, достоверности и надежности цифровой информации в качестве доказательств по уголовным делам.
3. Настоящие Правила регламентируют технические аспекты процесса работы с цифровой информацией в уголовном судопроизводстве. При этом все правовые вопросы и процессуальные решения по ним регулируются в соответствии с Уголовно-процессуальным кодексом Кыргызской Республики.
4. Настоящие Правила составлены с учетом принципа технологического нейтралитета законодательства и требования, установленные в настоящих Правилах, адаптивны и применимы к различным видам технологий и не зависят от конкретных из них, не ограничивают развитие инноваций и появление новых инструментов, устанавливает равные условия для конкуренции и признания юридической силы.
5. В настоящих Правилах используются следующие понятия:
   - *Цифровая информация* – это информация, представленная посредством двоичного кодирования и обращающаяся в цифровом пространстве в результате активных действий человека, так и автоматического сохранения, в том числе, тексты, текстовые сообщения, отметки, аудио-, видео-, фотоматериалы, иные файлы, а также метаданные.

- *Цифровое устройство* – компьютеры, ноутбуки, планшеты, серверы, мобильные телефоны, смартфоны и иные аналогичные технические устройства или приспособления, используемые для генерации, ввода, обработки, хранения, передачи и получения цифровой информации.
- *Цифровое доказательство* – цифровая информация, полученная в установленном законодательством Кыргызской Республики порядке и на основе которой устанавливается наличие или отсутствие обстоятельств, имеющих значение для уголовного дела, указанных в Уголовно-процессуальном кодексе Кыргызской Республики.

2. Особенности цифровой информации

6. Цифровая информация обладает следующими особенностями:

6.1. *Цифровая сущность*: цифровая информация представляет собой результат цифрового следообразования в виде двоичного кодирования посредством комбинации двух чисел – 0 и 1 (бит);

6.2. *Абстрактность и опосредованность*: цифровая информация не может быть воспринята человеком невооруженным взглядом, и оценка цифровой информации в качестве цифрового доказательства требует определенного материального носителя;

6.3. *Интерпретируемость*: ценность цифровой информации в качестве цифрового доказательства зависит от интерпретации специалистов, вовлеченных в процесс обращения с цифровой информацией;

6.4. *Хрупкость*: цифровая информация является хрупкой, незащищенной против изменения, повреждения или уничтожения, в том числе, непредумышленного, и, следовательно, доказательственная ценность цифровой информации может быть утрачена в результате неправильного обращения с ней;

6.5. *Неограниченность в копировании*: цифровая информация может быть размножена без ограничений, что позволяет нескольким специалистам одновременно и в разных местах работать над ней;

6.6. *Многообразие форм*: цифровая информация может иметь многочисленные формы, одни из которых могут быть относительно простыми, представлены и продемонстрированы сравнительно простым способом, тогда как другие формы могут быть сложной природы, и их доказательственная сила может быть обеспечена за счет применения сложных техник и инструментов;

6.7. *Трансграничность*: цифровая информация и/или их лица, владеющие ею, могут находиться за пределами юрисдикции Кыргызской Республики;

6.8. *Необходимость специальных знаний и навыков*: обращение с цифровой информацией требует повышенной юридической и технической квалификации, специальных знаний и навыков от всех участников процесса идентификации, изъятия, получения, хранения и исследования цифровой информации.

7. При обращении с цифровой информацией специалисту рекомендуется учесть вышеуказанные ее особенности, поскольку совершение правильных или неправильных действий с цифровой информацией может влиять на состоятельность

цифровой информации в качестве цифрового доказательства и иметь конкретные правовые последствия для участников уголовного процесса.

3. Источники цифровой информации

8. Источниками цифровой информации могут послужить:
   - компьютерные системы;
   - запоминающие устройства (жесткие диски (HDD, SSD), съемные носители (CD, DVD, BD), карты памяти (SD, Micro SD card, CF), Universal Serial Bus (USB), магнитные ленты для хранения данных;
   - периферийные устройства (факс, сканнер, принтер, кард-ридер, автоответчик);
   - планшеты (Personal Digital Assistant);
   - мобильные телефоны;
   - Фото- и видеозаписывающие устройства (цифровые фото- и видеокамеры, цифровые видеорегистраторы, цифровые звукозаписывающие устройства, диктофоны, камеры внешнего видеонаблюдения);
   - портативные медиапроигрыватели;
   - консоли видеоигр;
   - компьютерные сети (Local Area Network (LAN), Wide Area Network (WAN), Port, Bandwidth, Media Access Control (MAC) address, Network Attached Storage (NAC), Redundant Array of Independent Discs (RAID), Network Interface Controller (NIC), Network Hub, Network switch, Router, Server, Firewall, Wireless Access Point).

4. Принципы и общие правила обращения с цифровой информацией

9. Принципы

10. При обращении с цифровой информацией в уголовном судопроизводстве следуют соблюдать следующие принципы:
    - *Значимость* – цифровая информация должна иметь доказательственное значение и ценность для расследуемого уголовного дела.
    - *Достоверность* – все процессы, используемые при обращении с цифровой информацией, должны быть контролируемыми и повторяемыми, а их результаты – воспроизводимыми. Орган следствия, прокурор или суд должны иметь возможность оценить действия, выполненные с цифровой информацией, в том числе посредством ознакомления и изучения документации, составленной в ходе обращения с цифровой информацией.
    - *Достаточность* – объем данных, используемых при исследовании цифровой информации, должен быть в совокупности достаточным для достижения точности и надежности выводов, сделанных по итогам исследования.

11. Цепочка сохранности

11.1. Цепочка сохранности (chain of custody) – процесс документирования и отслеживания перемещения и хранения цифровой информации и цифровых устройств, от момента их изъятия и получения до момента их использования в качестве доказательств в суде. Цепочка сохранности обеспечивается путем надлежащего документирования процесса обращения с цифровой информацией и строгого соблюдения всех

требований, установленных в настоящих Правилах, в отношении процесса изъятия, упаковки и транспортировки цифровых устройств, получения цифровой информации, их хранения, исследования и представления в качестве цифрового доказательства.

11.2. Цепочка сохранности является важным аспектом обращения с цифровой информации, поскольку:

- она обеспечивает целостность и аутентичность цифровой информации, тем самым гарантируя, что цифровая информация не была изменена, подделана или повреждена в процессе обращения с ней;
- она является базой для применения процессуальных правил о применении цифровой информации в качестве допустимых цифровых доказательств по уголовным делам;
- она, исключая все сомнения в технической и юридической корректности действий лиц, задействованных в процессе обращения с цифровой информацией, повышает доверие участников уголовного дела к данному процессу и служит целям и задачам справедливого правосудия.

12. Квалификация специалистов

12.1. Специалисты, привлеченные к обращению с цифровой информацией, должны обладать знаниями о технических свойствах цифровых устройств и цифровой информации. В частности, для участия в процессе обращения с цифровой информацией в качестве специалиста, необходимо:

- специализированное образование в области информационной безопасности, кибербезопасности, цифровой криминалистики, компьютерной науки или связанных с ними областей;
- навыки и опыт работы с цифровыми устройствами и компьютерными системами;
- знание основ уголовно-процессуального законодательства, в том числе, касающегося системы доказательств и вопросов доказывания в уголовных делах;
- умение работать с цифровыми инструментами и программным обеспечением, используемым в процессе изъятия, упаковки и транспортировки цифровых устройств, получения цифровой информации, их хранения, исследования и представления в качестве цифрового доказательства.
- умение вести документацию, описывающую процедуры и результаты обращения с цифровой информацией.

12.2. Квалификация специалиста может быть подтверждена дипломом о высшем образовании, переподготовке и повышении квалификации, а также сертификатами о прохождении специализированного обучения в сфере информационной безопасности, кибербезопасности, цифровой криминалистики и других смежных областях.

5. Подготовка

13. Специалист, привлеченный к обращению цифровой информацией, в порядке подготовки должен:

- получить всю доступную информацию о месте инцидента (адрес, наименование организации, место расположения серверов или других цифровых устройств,

наличие опасных материалов, доступность места для посторонних лиц, наличие охраны, сигнализации, данные собственника или владельца помещения и пр.);

- подготовить всё необходимое оборудование для обращения с цифровой информацией, такие как ноутбук со всеми необходимыми программными обеспечениями, устройства хранения данных с достаточной памятью, кабели, набор инструментов, плоскогубцы, шипцы, зажимы, пинцеты, фото- или видеокамера, фонарик, увеличительное стекло, маркеры, наклейки и стикеры, специальные перчатки, коробки, антистатические сумки и упаковки и т.д.
- должен убедить, что его привлечение к обращению цифровой информацией, оформлено в соответствии с уголовно-процессуальным законодательством Кыргызской Республики, в том числе, при необходимости, получены надлежащим образом судебные акты, согласия на сбор и обработку данных и пр.

14. По прибытии на месте инцидента Специалист может быть проинструктирован органом следствия, который информирует Специалисте об уголовном деле, поясняет цели и задачи предстоящей работы с цифровой информацией, сообщает круг интересов следствия и предмет доказывания.
15. Специалист, оказавшись на месте события, обязан предпринять следующие меры предосторожности и защиты цифровой информации:
    - обезопасить и взять под контроль площадку, где находятся цифровые устройства, убедиться, что на площадке отсутствуют опасные предметы, оружие, легковоспламеняющаяся жидкости предметы, и что никому из присутствующих не грозит физическая опасность;
    - изолировать место инцидента от посторонних, обеспечить удаление всех посторонних лиц от цифровых устройств и источников питания;
    - исключить общение подозреваемого с другими лицами;
    - определить поименный состав лиц, ответственных за площадку, где находятся цифровые устройства, а также состав лиц, имеющих доступ на площадку;
    - не включать и не выключать цифровые устройства;
    - зафиксировать место инцидента со всеми компонентами и кабелями в исходном положении (путем рисования на чертежах, эскизных планах, либо фотографирования или снятия на видео)
    - промаркировать все порты и кабели;
    - вести поиск нецифровых свидетельств (стикеры, ежедневники, документы, инструкции и руководства, пароли и PIN-коды и др.);
    - отказаться от помощи любых неуполномоченных лиц и персонала на месте инцидента.
16. Специалист на месте инцидента обязан оценить все риски потери цифровой информации, в том числе:
    - определить корректные методы сбора и получения цифровой информации;
    - определить оборудования, которые могут понадобиться на месте инцидента;
    - установить уровень изменчивости данных и цифровой информации;

- определить наличие или отсутствие удаленного доступа к цифровым устройствам, а также других факторов, представляющих угрозу для целостности цифровой информации;
- определить в системе наличия логической бомбы и других программ или скриптов, предназначенных для выполнения вредоносных действий, включая фальсификация, уничтожение или компрометацию данных.

17. Специалист может принять участие в допросе подозреваемого и уточнить у него следующие вопросы:
    - Кому принадлежит цифровое устройство?
    - Есть ли у подозреваемого доступ к цифровому устройству?
    - У кого есть доступ к цифровому устройству;
    - Данные об учетной записи и пароли?
    - Кто еще пользуется цифровым устройством?

6. Процесс обращения с цифровой информацией

18. Идентификация цифровой информации

18.1. Идентификация состоит из процесса поиска, распознавания и документирования потенциальной, в том числе скрытой, цифровой информации, которая имеет доказательственное значение для дела. В массиве данных, обнаруженных на месте события, специалисту крайне важно уметь отличать цифровую информацию, имеющую доказательственную ценность, потенциально способную подтвердить или опровергнуть обстоятельства по делу.

18.2. В процессе идентификации специалист определяет перечень конкретных цифровых устройств, которые могут содержать или обрабатывать цифровую информацию, имеющую доказательственное значение для дела. Обнаружив такие устройства, специалист обязан документировать тип, марку, серийные номера, номера лицензий и другие идентификационные признаки цифровых устройств.

18.3. В процессе идентификации специалист устанавливает свойства цифровых устройств, их сетевой статус (отключены, автономны, подключены к сети, соединены с другими периферийными устройствами) и техническое состояние.

18.4. В процессе идентификации цифровые устройства должны оставаться в неизменном состоянии: если они выключены, их не нужно включать, и напротив, если они включены, они должны оставаться включенными. Специалист должен сфотографировать дисплей включенных цифровых устройств с тем, чтобы зафиксировать фактическое содержание того, что выведено на дисплее. При необходимости, специалист может сделать описание содержание дисплея в письменном документе.

18.5. Специалист обязан определить состояние аккумуляторов цифровых устройств и, при необходимости, подключить их к зарядному устройству.

18.6. По итогам идентификации, специалист обязан определить потенциальную подверженность обнаруженной цифровой информации к изменениям и утрате, а также определяет порядок и приоритетность дальнейших действий по обращению с цифровой информацией.

18.7. Специалист может принять решение об изъятии цифрового устройства или получении цифровой информации, руководствуясь следующими факторами:
- технические свойства цифровой информации (изменчивость и хрупкость);
- невозможность получения доступа к дискам в виду примененного шифрования и нахождения паролей и ключей в виде изменчивых данных, на внешних устройствах и носителях;
- размер требуемой памяти;
- наличие персонала;
- временные ограничения.

18.8. По результатам процесса идентификации цифровой информации, специалист должен задокументировать следующие данные:
- дата и время обнаружения цифровой информации;
- адрес и местоположение, где была обнаружена цифровая информация;
- описание цифровых устройств, на которых была обнаружена цифровая информация (тип, марка, серийные номера, номера лицензий и другие идентификационные признаки);
- информация об установленных операционных системах, приложениях и утилитах на устройстве, включая версии и настройки;
- информация о процессах и задачах, запущенных на устройстве в момент обнаружения данных;
- описание найденных файлов и директорий, включая их названия и расширения;
- описание содержимого файлов, включая даты создания и модификации, размер и тип файла;
- описание программного обеспечения, используемого для обнаружения и анализа цифровой информации;
- информация об учетных записях;
- информация о сетевых соединениях и настройках;
- данные о системных журналах и логах, связанных с обнаружением и изъятием данных;
- описание нецифровых свидетельств (стикеры, ежедневники, документы, инструкции и руководства, пароли и PIN-коды и др.);
- Ф.И.О. и подпись специалиста, ответственного за идентификацию цифровой информации.

19. Изъятие цифровых устройств

19.1. Изъятие осуществляется в форме изъятия из рабочей среды цифровых устройств, в которых содержится цифровая информация, транспортировки в другое место для последующего получения и исследования цифровой информации.

19.2. В порядке подготовки к изъятию, специалисту на месте события крайне важно собрать любые материалы, в том числе в нецифровой форме, которые могут иметь потенциальную ценность (листы бумаги и стикеры с записанными паролями, документация и инструкции к программным обеспечениям). При необходимости,

специалист может инициировать беседу с владельцами, пользователями цифровых устройств или сетевыми администраторами о конфигурации системы, пароле администратора и иных сведениях, необходимых для получения и анализа цифровой информации.

19.3. В процессе изъятия цифровых устройств специалисту рекомендуется носить не оставляющие ворса перчатки, а также держать руки постоянно сухими и чистыми.

19.4. Процесс изъятия цифровых устройств может различаться в зависимости от наличия или отсутствия включенного питания.

19.5. **Изъятие цифровых устройств с включенным питанием**

19.5.1. При изъятии цифровых устройств с включенным питанием, специалисту рекомендуется соблюдать следующие правила:

- До того, как система питания будет выключено, необходимо принять меры по получению и сохранению изменчивых данных, имеющихся в цифровом устройстве. При этом, если есть подозрение на применение шифрования, Специалисту необходимо предусмотреть возможность логического получения цифровой информации, в том числе посредством поиска определенных ключевых слов или фраз, фильтрацию данных по различным критериям, объединение и разделение данных, а также другие операции для получения нужной информации;
- Специалисту необходимо промаркировать, отсоединить и сохранить все кабели цифрового устройства и промаркировать порты, а также, при необходимости, заклеить лентой выключатель питания;
- При сборе персональных компьютеров и ноутбуков, специалист должен проверить слот для дискет и лотки для CD дисков (если есть), удостовериться, что они пусты и задвинуты на место, а также заклеить лентой для предотвращения его открывания.

19.6. **Изъятие цифровых устройств с выключенным питанием**

19.6.1. При изъятии цифровых устройств с выключенным питанием, специалисту рекомендуется соблюдать следующие правила:

- Необходимо удостовериться, что питание действительно отключено;
- Необходимо отключить снять аккумулятор источника питания и кабель электропитания, предвари1тельно отсоединив конец, подключенный к цифровому устройству, а также отсоединить и сохранить все кабели цифрового устройства, промаркировать порты;
- При необходимости, рекомендуется заклеить лентой выключатель электропитания;
- При сборе персональных компьютеров и ноутбуков, следует избегать снятия жесткого диска на месте события. Если специалист вынужден снимать жесткий диск на месте события, необходимо обеспечить заземление, чтобы предотвратить повреждение жесткого диска от статического электричества. Снятый жесткий диск следует промаркировать и зафиксировать все его реквизиты (тип, марку, серийные номера, объем памяти и другие идентификационные признаки).

- При изъятии персональных компьютеров и ноутбуков, специалист должен проверить слот для дискет и лотки для CD дисков (если есть), удостовериться, что они пусты и задвинуты на место, а также заклеить лентой для предотвращения его открывания.

19.7. Процесс изъятия цифровых устройств должен быть запротоколирован в соответствии с требованиями Уголовно-процессуального кодекса Кыргызской Республики с описанием всех действий, совершенных с цифровыми устройствами.

19.8. В процессе изъятия цифровых устройств, специалист должен задокументировать, как минимум, следующие данные:

- дата и время документирования;
- дата и время изъятия цифровых устройств.
- адрес и местоположение, где были изъяты устройства;
- описание изъятых цифровых устройств, включая их тип, марку, серийные номера, номера лицензий и другие идентификационные признаки;
- описание всех деталей и принадлежностей, найденных вместе с цифровыми устройствами (зарядные устройства, кабели, батарейки, аккумуляторы и т.д.);
- описание нецифровых свидетельств (стикеры, ежедневники, документы, инструкции и руководства, пароли и PIN-коды и др.);
- любые обстоятельства, связанные с изъятием устройств по усмотрению Специалиста.
- Ф.И.О. и подпись Специалиста, ответственного за изъятие цифровых устройств.

19.9. Дополнительно специалист должен сфотографировать изъятые цифровые устройства с разных ракурсов, включая с ракурсов, показывающих их состояние и наличие каких-либо повреждений или следов вмешательства.

19.10. Изъятые цифровые устройства подлежат упаковке. Во время упаковки изъятых цифровых устройств специалист должен:

- исключить любые внешние контакты с областями и деталями цифровых устройств, где хранится цифровая информация (к примеру, магнитная лента, микросхемы, чипы памяти, порты и пр.);
- при необходимости, использовать антистатические сумки и упаковки (специальные материалы, предотвращающие накопление статического заряда на электронных компонентах и устройствах за счет многослойных пленок, которые содержат проводящие полимеры или металлические слои, которые создают эффективный экранирующий барьер для статического электричества);
- обеспечить, чтобы каждое цифровое устройство было упаковано отдельно для исключения взаимного влияния исследуемых устройств друг на друга;
- обеспечить, чтобы используемы упаковочные материалы были надежны против удара, падения, вибрации, повреждения, а также могли защитить устройства от воздействия внешних факторов, таких как тепло, влага, конденсата и пыль;
- обеспечить, чтобы каждое устройство было помечено уникальным идентификатором и подписано с указанием времени и даты изъятия. Маркировка не должна помещаться непосредственно на механические части цифрового устройства и закрывать или скрывать важную идентификационную

информацию. Цифровые устройства с открывающимися и подвижными элементами должны быть маркированы путем наклеивания этикетки с печатью для индикации вскрытия.

19.11. Специалист обязан обеспечить сохранность изъятых цифровых устройств во время их транспортировки. В частности, цифровые устройства в процессе транспортировки:

- должны храниться в безопасном месте, исключающем возможность кражи, повреждения или уничтожения;
- не должны быть оставлены без присмотра ответственных лиц;
- должны быть защищены от воздействия внешних факторов, таких как удары, падение, пыль, высокая температура, конденсат и влага.

20. Получение цифровой информации

20.1. Получение представляет собой создание цифровой копии цифровой информации и документирование использованных методов и совершенных действий в данном процессе.

20.2. Методы, используемые для получения цифровой информации, определяются специалистом исходя из технической природы и объема получаемой цифровой информации, тип устройства, на котором находится цифровая информация, формат и тип файлов, которые необходимо скопировать, а также технические возможности, доступные специалисту.

20.3. В процессе получения цифровой информации специалист должен убедиться, что используемый им метод не изменит или повредит исходную цифровую информацию во время копирования. В этих целях специалист может создать хэш-сумму исходной цифровой информации и копии, чтобы проверить, что копия является точной.

20.4. При необходимости, рекомендуется использовать метод «битового копирования» (bit-by-bit), который представляет собой способ создания точной копии цифровой информации, который копирует каждый бит (или 0 или 1) информации из оригинального источника в копию без изменения ее структуры. Этот метод гарантирует, что каждый бит исходной информации будет точно скопирован в новую копию, включая любые скрытые файлы, метаданные, удаленные файлы и другую скрытую информацию. При использовании метода «битового копирования» программное обеспечение, которое используется для копирования, сканирует и копирует каждый сектор жесткого диска (или другого источника), включая неиспользуемые области, защищенные области и все другие области, которые могут содержать цифровые доказательства.

20.5. Специалист должен убедиться, что цифровая информация копируется на надежный носитель, который имеет достаточный объем и сохранность для хранения цифровой информации в течение периода, необходимого для последующего исследования.

20.6. **Получение цифровой информации из цифровых устройств с включенным питанием**

20.6.1. При получении цифровой информации из цифровых устройств с выключенным питанием, специалисту, прежде всего, рекомендуется рассмотреть вопрос правильного получения цифровой информации, которая относится к изменчивым данным и может быть потеряна при выключении цифрового устройства (логи

сетевой активности, кэшированные страницы веб-браузера, временные файлы, копии документов, созданных и измененных пользователями, данные в реестрах и журналах событий, а также метаданные файлов, такие как дата создания, последнего изменения и доступа к файлу, другие данные, которые могут быть созданы или изменены в процессе использования устройства).

20.6.2. Для создания копии содержимого оперативной памяти компьютера в определенный момент времени может быть использован метод «снимок памяти» (memory dump). Снимок памяти может быть получен с помощью специальных программных инструментов (программы-отладчики, утилиты и др.), которые могут прочитать содержимое оперативной памяти и сохранить его в виде файла. Этот файл затем может быть анализирован для обнаружения цифровой информации с доказательственным значением. Для использования снимка памяти следует учесть, что данный процесс может занять некоторое время и может вызвать дополнительную нагрузку на систему.

20.6.3. Для обеспечения целостности и точности результатов исследования изменчивых данных, последние должны быть получены в реальном масштабе времени. Другими словами, временных метки в цифровой информации должны соответствовать реальному времени, когда эти данные были созданы или изменены. Это важно для проведения анализа и расследования событий, в которых временные метки цифровых данных могут использоваться для установления хронологии событий, идентификации подозреваемых и доказательства их причастности к событию преступления и иных обстоятельств, имеющих значение для уголовного дела. В процессе получения изменчивых данных, специалисту следует учесть, что реальный масштаб времени может быть нарушен из-за различных факторов, например, из-за ошибок настройки часов в устройстве, изменения часового пояса, неправильной настройки системных часов, использования программных средств для изменения временных меток и т.д.

20.6.4. При получении изменчивых данных, специалист должен использовать логический файл-контейнер (специальный файл в формате ZIP, RAR, TAR, ISO и другие, который содержит в себе другие файлы и папки, и обычно используется для хранения и организации данных на компьютере или другом устройстве). Для обеспечения безопасности и конфиденциальности полученных данных, специалист может зашифровать логический файл-контейнер, а также хэшировать с фиксацией значения хэш-суммы.

20.6.5. При получении цифровой информации специалисту следует применить специализированные инструменты, которые сканируют жесткий диск на наличие зашифрованных разделов, показывают, какие диски подключены к компьютеру, как организована файловая система, какие данные передаются по сети, указывают на использование шифрования трафика, а также могут расшифровывать зашифрованные данные, если имеются ключи или пароли для расшифровки.

20.7. **Получение цифровой информации из цифровых устройств с выключенным питанием**

20.7.1. При получении цифровой информации из цифровых устройств с выключенным питанием, специалисту необходимо удостовериться, что устройство действительно выключено.

20.7.2. Если это применимо, следует удалить ОЗУ из выключенного устройства, если оно еще не удалено. Это может быть необходимо для получения изменчивых данных, таких как данные о процессах и открытых сетевых подключениях, которые могут быть хранены только в памяти устройства во время его работы.

20.7.3. Нежелательно извлекать носителя цифровой информации из цифрового устройства, так как это увеличивает риск повредить или перепутать его с другими носителями.

20.8. **Получение цифровой информации из критических важных систем без возможности выключения**

20.8.1. В случаях, когда цифровая информация содержатся в критически важных системах, которые не могут быть выключены (серверы информационных центров, обслуживающие других пользователей, системы наблюдения, государственные, банковские, медицинские информационные системы, системы управления производством и пр.), специалист может провести частичное получение цифровой информации. В этом случае специалист должен исследовать информационную систему, чтобы определить, какие данные в ней находятся и какие источники можно использовать для получения доступа к необходимым данным. Кроме этого, специалисту следует изучить структуру информационной системы (какие имеются базы данных, таблицы и поля), а также применять логические инструменты для поиска и извлечения данных.

20.9. После завершения получения цифровой информации специалист обязан верифицировать полученные данные для обеспечения их подлинности и целостности. Для этого, специалист может использовать различные методы, включая использование хэш-функций, электронно-цифровой подписи, биометрию и фотографирование.

20.10. Если процесс верификации не может быть осуществлен для источника цифровой информации в целом вследствие ошибок источника, то осуществляется верификация тех частей источника, которые могут быть надежно получены и прочитаны.

20.11. Специалист обязан надлежащим образом документировать процесс получения цифровой информации с указанием следующих данных:

- дата и время документирования;
- даты и время получения цифровой информации;
- адрес и местоположение, где была получения цифровая информация;
- описание процедуры получения цифровой информации: когда и как был получен доступ к информации, какие инструменты использовались, какие файлы были скопированы или извлечены;
- список всех скопированных или извлеченных файлов и их наименования, пути к файлам, а также их хеш-суммы, чтобы обеспечить целостность информации;
- подробное описание всех использованных программ и инструментов для получения и обработки цифровой информации;

- описание хранилища, где хранятся копии полученной цифровой информации, включая место хранения, даты создания, доступ к хранилищу и наличие каких-либо дополнительных мер безопасности;
- любые замечания или примечания, которые могут быть полезны для дальнейшего исследования, такие как наличие зашифрованных файлов, защищенных паролем документов или наличие скрытых разделов на носителях и пр.;
- Ф.И.О. и подпись специалиста, ответственного за получение цифровой информации.

21. Хранение цифровой информации

21.1. Хранение цифровой информации должно отвечать следующим требованиям:

- цифровая информация должна храниться в безопасном месте, к которому имеют доступ только уполномоченные лица. Кроме этого, любое посещение места хранения цифровой информации должно быть отражено в специальном журнале с указанием данных посетителя, цели посещения, даты, времени и продолжительности посещения;
- для хранения цифровой информации следует использовать безопасные средства хранения, такие как сейфы, железные шкафы, антистатические сумки, и упаковки;
- место хранения должно обеспечить защиту цифровой информации от внешних воздействий, в том числе от тепли, влаги, конденсата и пыли.

7. Исследование цифровой информации

22. Вопросы для исследования

22.1. Приступая к исследованию цифровой информации, специалист должен искать ответы на вопросы, сформулированные ему органами следствия и судом.

22.2. Предметом исследования цифровой информации не являются правовые вопросы, следовательно, специалист не вправе давать на них ответы. В частости, специалист не вправе отвечать на вопросы о наличии или отсутствии состава преступления, виновности или невиновности подозреваемого и обвиняемого, законности или незаконности их действия и бездействия, наличия или отсутствия обстоятельств, смягчающих или отягчающих ответственность и пр.

22.3. Специалист вправе обратиться с просьбой уточнить либо переформулировать заданные ему вопросы с тем, чтобы исключить правовые вопросы из предмета исследования.

22.4. Специалист в ходе исследования цифровой информации обязан сконцентрироваться исключительно на технических аспектах и сформулировать ответы на заданные ему вопросы. При необходимости, специалист имеет право указать на обнаруженные в ходе исследования обстоятельства, имеющие значение для дела, по поводу которых ему не были поставлены вопросы.

22.5. Конкретные вопросы, на которые необходимо ответить в ходе исследования цифровой информации, формулируются органами следствия или судом, в зависимость от обстоятельств дела, состава цифровых устройств, имеющих отношение к уголовному делу. Наиболее типичные вопросы, подлежащие изучению

в рамках исследования цифровой информации, указаны в Приложении 1 к настоящим Правилам.

23. Рабочая копия цифровой информации

23.1. При проведении исследования цифровой информации специалист применять методы и инструменты исследования не к оригиналу цифровой информации, находящейся в цифровом устройстве, а к рабочей копии цифровой информации, созданной по итогам процесса получения цифровой информации.

23.2. Рабочая копия цифровой информации позволяет проводить анализ и исследование без воздействия на оригинал, что обеспечивает сохранность цифровой информации в первоначальном виде, защищает ее от изменения и исключает риск повреждения или уничтожения цифровой информации.

24. Специалисту следует иметь в виду, что наиболее эффективность исследования и точность результатов достигается при использовании комплексного подхода, включающего в себя применение нескольких методов исследования цифровой информации.

8. Отдельные способы исследования цифровой информации

25. Исследование файловых систем

25.1. Файловая система представляет собой метод организации данных на компьютере или другом устройстве хранения данных. Она определяет, как файлы будут храниться, идентифицироваться, доступны и управляться на жестком диске, флеш-накопителе, в облаке или другом носителе. Файловая система обеспечивает способ доступа к файлам и папкам на устройстве, а также управляет пространством на жестком диске или другом носителе, чтобы эффективно использовать его.

25.2. Исследование файловых систем включается в себя:

- анализ структуры файловой системы (изучение способа, которым файлы и папки организованы на жестком диске или другом хранилище, включая определение типа файловой системы, изучение содержимого корневого каталога, анализ структуры и связи каталогов, атрибутов файлов и папок (метаданных), обнаружение скрытых файлов и папок);
- применение специализированных программных обеспечений для сканирования и анализа файловой системы на наличие конкретных типов файлов, ключевых слов или других характеристик, которые указывают на наличие важной искомой цифровой информации;
- применение специализированных программных обеспечений для анализа метаданных в различных форматах файлов;
- применение специализированных программных обеспечений для обнаружения и восстановления удаленных или поврежденных данных, в том числе метаданных;
- работа с зашифрованными файлами (использование известных паролей и ключей, использование уязвимостей в защите данных, использование перехваченной информации, применение специализированных программ по расшифровке файлов путем обнаружения ключей или перебора, а также

коммуникация с поставщиком услуг для получения помощи в расшифровке файлов).

26. Исследование метаданных

26.1. Метаданные – это данные, которые описывают другие данные. Метаданные представляют собой информацию о том, каким образом были созданы, использованы или модифицированы другие данные. Метаданные могут включать в себя различные сведения, такие как название, автора, дату создания, размер, формат, расположение, источник и т.д.

26.2. Исследование метаданных включает в себя:

- поиск и идентификацию файлов, содержащих метаданные;
- применение специализированных программ для извлечения метаданных из файлов;
- анализ полученных метаданных, включая:
  - идентификацию автора файла, его имя пользователя и электронную почту;
  - определение GPS-координат и временных зон, в которых был создан файл;
  - определение даты и времени создания и изменения файла;
  - идентификацию типа устройств, на котором был создан или изменен файл;
  - идентификацию программного обеспечения, использованного для создания или изменения файла;
  - определение целостности данных путем анализа контрольной суммы файла;
  - определение источника, откуда был получен файл;
  - анализ информации о сетевых устройствах, включая IP-адреса, MAC-адреса;
  - анализ информацию о контактах (адреса электронной почты или номера телефонов);
  - анализ данных о цифровых подписях или сертификатах, используемых для проверки подлинности и целостности файла и др.

27. Исследование лог-файлов

27.1. Лог-файлы – это файлы, которые содержат записи о событиях, происходящих в операционной системе, приложениях, сетях, базах данных и других компонентах информационной системы. Лог-файлы могут использоваться для обнаружения и анализа инцидентов безопасности, идентификации проблем и ошибок, а также для мониторинга работы информационной системы в целом.

27.2. Исследование лог-файлов включает в себя:

- сбор лог-файлов из системы, приложения или сети с помощью различных методов, включая локальный, централизованный, с помощью агентов или API;
- фильтрация и сортировка лог-файлов для выявления событий, связанных с инцидентом, в том числе:

- по алфавиту (лог-файлы могут быть отсортированы в алфавитном порядке по названию файла или по содержанию определенного поля);
- по временному штампу (лог-файлы могут быть отсортированы по времени, когда зарегистрированные события произошли);
- по уровню важности (лог-файлы могут быть отсортированы, к примеру, на ошибки, предупреждения или информационные сообщения);
- по идентификатору устройства (лог-файлы могут быть сгруппированы по названию устройства или приложения, которое зарегистрировало запись);
- по категориям событий (лог-файлы могут быть отсортированы по категориям событий, таких как сетевые события, события безопасности и пр.);

- анализ содержимого лог-файлов для определения причин и последствий событий;
- идентификация аномальных событий, которые могут указывать на присутствие злоумышленника в системе или нарушения безопасности;
- восстановление цепочки событий для определения последовательности действий злоумышленника и возможных уязвимостей системы;

28. Исследование сетевого трафика

28.1. Сетевой трафик – это поток данных, передаваемых между устройствами в сети. Сетевой трафик может содержать информацию, отправленную и полученную устройствами, такую как веб-страницы, электронная почта, файлы, мультимедийные файлы, сообщения и т.д. Сетевой трафик может передаваться по различным протоколам, таким как TCP (Transmission Control Protocol) и UDP (User Datagram Protocol), а также могут быть зашифрованы для обеспечения безопасности передачи данных. С помощью анализа сетевого трафика можно определить, какие данные были переданы в сети, как они были переданы, откуда они были отправлены, кому были отправлены и какие были ответы на передачу данных.

28.2. Исследование сетевого трафика включает в себя:

- захват сетевого трафика с помощью специальных программных инструментов;
- определение протоколов, используемых в сетевом трафике, такие как TCP, UDP, HTTP и др.;
- фильтрация и анализ сетевого трафика на предмет выявления интересующей информации;
- извлечение метаданных из сетевого трафика для их последующего исследования;
- восстановление данных, переданных в сети

29. Исследование IP-адреса и DNS

29.1. IP-адрес (Internet Protocol address) – это уникальный числовой идентификатор, присвоенный каждому устройству, подключенному к сети интернет или локальной сети. IP-адрес позволяет маршрутизаторам и другим устройствам пересылать данные между устройствами в сети, указывая IP-адрес получателя и отправителя. IP-адрес

также может использоваться для идентификации и отслеживания пользователей в сети.

29.2. DNS (Domain Name System) – это система, которая переводит доменные имена в IP-адреса. DNS позволяет пользователям вводить понятные для человека доменные имена вместо IP-адресов, которые являются числовыми идентификаторами устройств в сети. DNS также обеспечивает распределенное хранение и управление информацией о доменных именах и их соответствующих IP-адресах.

29.3. Исследование IP-адресов и DNS включает в себя:

- сбор информации о IP-адресах и DNS, связанных с расследуемым инцидентом, в том числе путем изучения записей лог-файлов, данных сетевых диспетчеров, информации от провайдеров интернет-услуг и другие источники;
- анализ IP-адресов посредством специализированных инструментов (WHOIS, GeoIP и др.), в том числе для определения их местоположения, владельца и др. сведений;
- анализ DNS, связанный с расследуемым инцидентом, чтобы определить, какие домены и поддомены были связаны с ним;
- сопоставление данных с другими сведениями, полученными в ходе исследования (к примеру, сравнение IP-адреса с источниками атак или с данными о входе в систему).

30. Исследование браузера

30.1. Браузер – это программа, которая позволяет просматривать веб-страницы и интерактивно взаимодействовать с веб-сайтами в интернете. Браузер работает в качестве интерфейса между пользователем и интернетом, обеспечивая отображение веб-страниц на экране компьютера или мобильного устройства. Браузер загружает веб-страницы, используя протокол HTTP или HTTPS, и отображает их в удобном для пользователя виде. Он также может обрабатывать различные элементы на веб-страницах, такие как ссылки, изображения, видео и формы. Браузер может содержать ценную информацию о том, какие веб-сайты были посещены, какие данные были введены, какие файлы были загружены и другие подробности, которые могут служить в качестве доказательства по уголовному делу.

30.2. Исследование браузера включает в себя:

- изучение файлов cookies, которые содержат информацию о посещенных веб-сайтах, а также о пользовательских идентификаторах и паролях, используемых для входа на эти сайты;
- анализ содержимого кэша браузера, который содержит временные копии веб-страниц и изображений, которые были загружены ранее.
- анализ истории браузера, содержащей список посещенных веб-сайтов, а также даты и время посещения;
- изучение расширений браузера, которые могут использоваться для доступа к конфиденциальным данным, таким как пароли и личные данные пользователей;
- анализ содержимого веб-страниц, включая анализ текста на странице, анализ изображений, метаданных, ссылок, форм, кода и пр.

31. Исследование электронной почты

31.1. Электронная почта (или email, от англ. «electronic mail») – это электронный способ обмена сообщениями между пользователями компьютеров, который использует интернет-протоколы для передачи информации. Электронная почта позволяет пользователям отправлять и получать сообщения с использованием адресов электронной почты, которые состоят из двух частей, разделенных символом «@»: имя пользователя и имя домена. Электронная почта может содержать текстовое сообщение, прикрепленные файлы, изображения, звуковые файлы и другие данные. Отправитель сообщения может также указать, кому и в какое время должно быть доставлено сообщение. Электронная почта является одним из наиболее популярных и распространенных средств коммуникации в современном мире и используется для переписки в рабочих и личных целях, а также для рассылок и рекламных кампаний.

31.2. Исследование электронной почты включает в себя:

- применение специализированных программ для сбора электронных писем и ассоциированных с ними метаданных, таких как IP-адреса отправителей и получателей, даты и время отправки и получения писем, а также размеры файлов.
- анализ метаданных, в том числе для определения источника писем и их маршрута, например, для определения, были ли письма отправлены с поддельных адресов или используются анонимные прокси-серверы;
- анализ содержимого писем, в том числе, при помощи поисковых запросов, сравнения текста в письмах и т.д.;
- восстановление удаленных писем посредством специальных программ;
- анализ устройств, в том числе сервисов и серверов электронной почты или компьютеров отправителей и получателей писем.

32. Исследование онлайн-сервисов

32.1. Онлайн-сервисы – это интернет-ресурсы и программы, которые предназначены для использования через Интернет и предоставляют доступ к различным сервисам и функционалу, в том числе для коммуникации, обработки данных, хранения и обмена информацией, развлечений и многого другого. К онлайн-сервисам можно отнести электронную почту, системы облачного хранилища файлов, социальные сети, онлайн-магазины, музыкальные и видео-стриминговые сервисы, веб-браузеры, онлайн-карты и навигаторы, онлайн-образование, онлайн-банкинг и финансовые сервисы, платежные системы, видеоконференции, сервисы для работы с документами, сервисы для заказа и доставки еды, онлайн-игры и многое другое.

32.2. Общий подход к исследованию онлайн-сервисов заключается в следующем:

- сбор доступных данных о пользователе, такие как имя, учетная запись, фотографии, друзья, сообщения, лайки и другой информации;
- анализ собранных данных с использованием различных методов, таких как поиск по ключевым словам, статистический анализ и сопоставление данных из разных источников;
- анализ метаданных, такие как IP-адреса, даты и времена доступа, источник запроса и другие данные;
- исследование контактов пользователя;
- использование специализированных инструментов, в том числе:

- социальные инженерные инструменты (специальные программы и методы для исследования онлайн-сервисов с целью получения информации о пользователях, мониторинга и анализа их активности, их привычек, предпочтений и связей, а также для выявления потенциальных уязвимостей);
- анализаторы метаданных (специальные программные инструменты, которые позволяют извлекать и анализировать метаданные для обнаружения и изучения следов деятельности пользователей, их сетевой активности, отслеживания перемещений файлов или обнаружения сетевых атак.

- сотрудничество с провайдерами онлайн-сервисов, в том числе для получения доступа к дополнительной информации и данных о пользователях.

32.3. Идентификация пользователя в онлайн-сервисе и определение принадлежности исследуемого аккаунта к конкретному лицу является сложным и многоступенчатым процессом, который включает в себя:

- сбор всех доступных данных о аккаунте (никнейм, адрес электронной почты, номер телефона, IP-адрес, MAC-адрес, IMEI-номер, и другие данные);
- анализ cookie и других данных, которые могут быть связаны с конкретным пользователем;
- сбор дополнительных данных о лице, которому предположительно принадлежит аккаунт (такие как ФИО, адрес проживания, дата рождения и другие персональные данные);
- анализ собранных данных с использованием различных методов (анализ IP-адресов, сравнение данных из разных источников и т.д.);
- анализ сообщений, отправленных с аккаунта, анализ действий и поведения пользователя в сети;
- запрос у провайдеров онлайн-сервиса информации об аккаунте и его владельце.
- сопоставление собранных и исследованных данных.

33. Документирование результатов исследования цифровой информации

33.1. Результаты исследования цифровой информации должны быть документированы специалистом путем составления письменного отчета.

33.2. Отчет по итогам исследования цифровой информации состоит из следующих элементов:

1. Вводная часть:

- дата, время начала и окончания исследования;
- юридическое основание для исследования (реквизиты постановления органа следствия или судебного акта);
- место исследования;
- Ф.И.О. специалиста;
- вопросы, поставленные перед специалистом для исследования;
- список всех цифровых устройств, представленных на исследование;

- список всех типов цифровой информации, представленной на исследование;

2. Исследовательская часть:
   - описание методов и технологий, использованных при исследовании цифровой информации, включая программное и аппаратное обеспечение, использованные алгоритмы и процедуры;
   - подробное и последовательное изложение процесса исследования и всех выявленных при этом фактических данных;
   - описание полученных результатов исследования;

3. Выводы:
   - ответы на вопросы, поставленные перед специалистом для исследования;

4. Заключительная часть:
   - Ф.И.О. специалиста;
   - Подпись специалиста.

33.3. Не допускается вписывать в текст отчета дополнительных отдельных слов или предложений, зачеркивание слов и т.д.. Все внесенные поправки должны быть заверены подписью специалиста.

33.4. Конкретная структура (последовательность изложения) исследовательской части отчета определяет специалист, в зависимости от особенностей исследования. При этом исследовательская часть отчета должна быть изложена языком, понятным для лица, не имеющего специальных познаний в цифровой криминалистике. При невозможности обойтись без специальных терминов их смысл должен быть разъяснен.

33.5. Выводы составляются после окончания всех процессов исследования в соответствии с поставленными перед специалистом вопросами. Допускается объединение близких по смыслу вопросов и изменение их последовательности (без изменения первоначальной формулировки вопроса). При неясности содержания вопросов специалист может указать, как он понимает тот или иной вопрос.

34. Выводы следует излагать четко и конкретно, не допуская различного их толкования.

34.1. Выводы должны представлять собой научно обоснованные, мотивированные ответы на поставленные вопросы, к которым он приходит в результате всестороннего и объективного анализа данных исследования цифровой информации, результатов дополнительных исследований, изучения специализированной документации и использование других материалов. Если специалист использовал нормативные материалы и справочные данные, то он указывает, какие именно. Не допускается применение непроверенных (не апробированных) методик.

34.2. Вопросы, выходящие за пределы своих специальных познаний, специалист оставляет без ответа, отмечая это в выводах.

35. Если возможности науки и практики или характера исследуемых объектов не позволяет дать категорический, обоснованный ответ на конкретный вопрос, специалист имеет право отказаться от дачи ответа на этот вопрос.

Приложение 1 к Правилам
идентификации, изъятия, получения,
хранения и исследования цифровой информации
в уголовном судопроизводстве

Наиболее типичные вопросы, подлежащие изучению в рамках исследования цифровой информации

- Какие данные были удалены или изменены на компьютере, можно ли их восстановить?
- Были ли обнаружены следы взлома компьютерной системы, и если да, то какие?
- Какие файлы были созданы или изменены на компьютере за период с ____ по ____ года?
- Какие программы были установлены или использовались на компьютере за период с ____ по ____ года?
- Были ли обнаружены следы удаленной работы на компьютере?
- Были ли обнаружены следы удаленных сообщений, электронной почты или других форм электронной связи?
- Какая информация была найдена на мобильных устройствах?
- Были ли обнаружены следы взлома социальных сетей, и если да, то какие данные могут быть извлечены из этих учетных записей?
- Какие данные могут быть извлечены из облаков, связанных с уголовным делом, и как это может помочь в расследовании?
- Какая информация может быть получена из камер наблюдения или других устройств видеонаблюдения, связанных с уголовным делом, и как она может быть использована в расследовании?
- Какие приложения были установлены на мобильном телефоне, и как часто они использовались?
- Были ли обнаружены какие-либо изменения в настройках мобильного телефона?
- Какие сообщения, звонки и медиафайлы были отправлены или получены на мобильном телефоне за период с _____ по _____ года?
- Были ли обнаружены какие-либо признаки удаления данных с мобильного телефона, и если да, то какие данные были удалены?
- Какая информация была найдена в контактных списках, заметках или календаре на мобильном телефоне?
- Какая информация была найдена в приложениях для социальных сетей на мобильном телефоне?
- Были ли обнаружены какие-либо признаки использования мобильного телефона в конкретном местоположении в определенное время?

- Какая информация была найдена в медиафайлах на мобильном телефоне, таких как фотографии или видео?
- Были ли обнаружены какие-либо следы удаленных сообщений или вызовов на мобильном телефоне?
- Какие данные могут быть извлечены из облачных хранилищ, связанных с мобильным телефоном?
- Какие социальные сети были использованы, и как часто они использовались?
- Какие сообщения были отправлены или получены через социальные сети, и как они могут быть связаны с преступлением?
- Были ли обнаружены какие-либо признаки удаления данных, связанных с социальными сетями, и если да, то какие данные были удалены?
- Какая информация была найдена в профиле на социальной сети, такая как контакты, сообщества, фотографии, и как она может быть связана с событием преступления?
- Какая информация была найдена в сообщениях, отправленных через социальные сети, такая как местоположение, время отправки, и как она может быть использована в расследовании?
- Были ли обнаружены какие-либо признаки использования социальных сетей во время события преступления, например, отправка сообщений в определенное время или использование функции голосовых заметок?
- Какие данные могут быть извлечены из облачных хранилищ, связанных социальными сетями, и как они могут помочь в расследовании?
- Были ли обнаружены какие-либо манипуляции с данными в профиле на социальной сети, например, фальшивые профили или изменения настроек приватности?
- Какие данные могут быть использованы для определения идентичности пользователя, и как они могут быть связаны с преступлением?