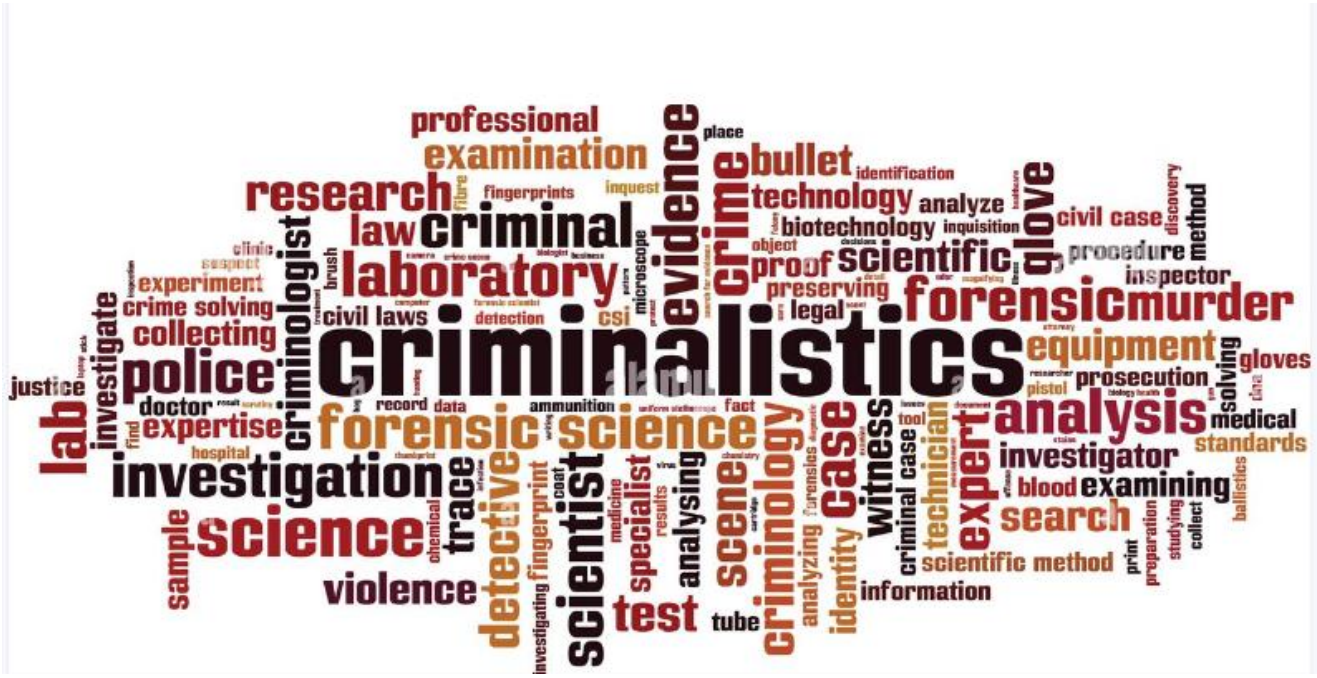
АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

РАССЛЕДОВАНИЕ КИБЕРПРЕСТУПЛЕНИЙ: ОТ ТЕОРИИ К ПРАКТИКЕ

УЧЕБНОЕ ПОСОБИЕ



г. Косшы, 2023

УДК 343.3/.7
ББК 67.408

Рецензенты:

Хан В.В. – кандидат юридических наук, ассоциированный профессор, профессор Кафедры специальных юридических дисциплин Института послевузовского образования Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан.

Шульгин Е.П. – кандидат юридических наук, начальник кафедры кибербезопасности и информационных технологий Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова.

Күнғожинов Қ.Ә. – начальник Управления досудебного расследования прокуратуры города Алматы.

Майтканов О.К. – начальник отдела по борьбе с киберпреступностью Управления криминальной полиции Департамента полиции города Астаны.

Калиев А.А., Аманкулов А.М., Кайназарова Д.Б. – Расследование киберпреступлений: от теории к практике. / Учебное пособие. – г. Косшы, 2023. – 123 с.

Раскрытие преступлений, совершаемых с использованием информационно-коммуникационных технологий и сети интернет, зависит от профессиональных знаний сотрудника, занимающегося расследованием таких дел и умелым применением их на практике.

Настоящее учебное пособие подготовлено в помощь сотрудникам следственно-оперативных подразделений правоохранительных органов, раскрывает особенности проведения расследования уголовных правонарушений данной категории.

Представленный материал будет полезен, как сотрудникам правоохранительных органов, занимающихся расследованием уголовных правонарушений, так и студентам и преподавателям вузов, изучающих вопросы противодействия киберпреступности.

УДК 343.3/.7
ББК 67.408

ISBN

Рекомендовано к изданию Учебно-методическим советом Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан

Содержание

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

КУИ	Книга учета информации
ЕРДР	Единый реестр досудебного расследования
УК	Уголовный кодекс
УПК	Уголовно-процессуальный кодекс
ОВД	Органы внутренних дел
ПК	Персональный компьютер
ОЗУ	Оперативно-запоминающее устройство
ВПО	Вредоносное программное обеспечение
МФУ	Многофункциональное устройство
ВПП	Взаимная правовая помощь
ОИА	Основная информация об абоненте
ПУ	Поставщики услуг
ЭД	Электронные доказательства

ВВЕДЕНИЕ

Развитие новых технологий неизбежно привела к росту компьютерных преступлений, которые отличаются от традиционных уголовных правонарушений высоким показателем латентности и низким уровнем раскрываемости.

Учитывая значительный материальный ущерб, наносимый киберпреступниками экономике разных стран, их предпринимателям и гражданам, правоохранительные органы во всем мире выдвигают киберпреступность на первое место среди основных видов преступлений.

Казахстан, как один из лидеров цифровизации среди стран Содружества независимых государств, также не остался в стороне.

Анализ статистических данных за последние 5 лет показал о проблемах в организации противодействия киберпреступности в Казахстане.

Согласно статистическим данным Комитета по правовой статистике в период с 2018 по 2022 годы правоохранительными органами начато досудебное расследование по **20145** уголовным правонарушениям, в том числе совершаемых:

- *с использованием сети Интернет;*

- *путем обмана или злоупотребления доверием пользователя информационной системы;*

- *путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций.*

При этом, по результатам досудебного расследования раскрыто всего **6955** или **34,5%** уголовных дел, прекращено по реабилитирующим основаниям **2030** или **10,1%**, прерваны сроки по **12 546 или 62,3%** уголовных дел.

Причины такой низкой раскрываемости дел по киберпреступлениям разные:

1) дефицит кадровых специалистов во всех правоохранительных органах, обладающих знаниями в области IT – технологий;

2) высокая профессиональная подготовка преступника;

3) недостаточное количество судебных экспертов в данной области;

4) отсутствие специализированных прокуроров и судей;

5) недостаточное количество алгоритмов и методических рекомендаций по расследованию киберпреступлений;

6) отсутствие в Казахстане единого специализированного учебного центра для правоохранительных органов в сфере расследования таких преступлений.

Все это сказывается на эффективности выявления и раскрытия киберпреступлений.

Данное учебное пособие раскрывает практически все этапы расследования и содержит учебный материал, позволяющий самостоятельно изучить методику проведения расследования преступлений, совершенных с использованием информационно-коммуникационных технологий.

ОБЩИЕ СВЕДЕНИЯ

Расследование преступлений, совершенных с использованием информационно-коммуникационных технологий и сети интернет требует от следователей определенных специальных знаний, в том числе технических.

Изучение уголовных дел данной категории показало, что основой их совершения являются:

- социальный инжиниринг, суть которого заключается в убеждении человека любым способом предоставить свои конфиденциальные, идентификационные данные;

- фишинг или поддельный интернет-сайт, применяемый для получения конфиденциальных данных *(например, логина и пароля от интернет-банкинга, номера банковской карты и другой важной информации)*;

- использование вредоносного программного обеспечения *(далее - ВПО)*, позволяющего злоумышленнику получить удаленный доступ к устройству *(компьютеру, ноутбуку, планшету)* пользователя либо похитить сведения о пользователе *(реквизиты его банковских счетов, логины и пароли)*.

Как правило, заражение компьютера пользователя или информационной сети осуществляется несколькими способами:

- путем рассылки писем под видом «официальных» на электронную почту пользователя;

- путем рекламы в социальных сетях, содержащей информацию о различных предложениях *(розыгрыши, выигрыши, получение призов, предупреждения об угрозах, осуществление платежа и т.д.)*.

К каждому из таких писем или сообщению прикрепляется ссылка на поддельный сайт, подготовленный для атаки на посетителя и зараженный ВПО.

Согласно статье 32 Уголовно-процессуального кодекса Республики Казахстан уголовные правонарушения в сфере информатизации и связи считаются правонарушениями публичного и частно-публичного обвинения.

К публичным обвинениям будут относиться уголовные правонарушения, предусмотренные статьями 205 ч.ч.2 и 3, 206 ч.ч.2 и 3, 207 ч.ч.2 и 3, 208 ч.ч.2 и 3, 209 ч.ч.2 и 3, 210 ч.ч.1, 2 и 3, 211 ч.ч.2 и 3, 212 ч.ч.1 и 2, 213 ч.ч.1, 2 и 3 Уголовного кодекса Республики Казахстан.

Уголовное преследование по этим делам осуществляется независимо от подачи жалобы потерпевшим.

К частно-публичным обвинениям относятся уголовные правонарушения, предусмотренные ст.ст.205 ч.1, 206 ч.1, 207 ч.1, 208 ч.1, 209 ч.1, 211 ч.1 Уголовного кодекса Республики Казахстан.

Производство по этим делам начинается не иначе как по жалобе потерпевшего и подлежит прекращению за примирением его с подозреваемым, обвиняемым, подсудимым лишь в случаях, предусмотренных ст. 68 УК РК.

ГЛАВА 1. НАЧАЛЬНЫЙ ЭТАП РАССЛЕДОВАНИЯ

В данной главе будут рассмотрены такие вопросы, как получение и регистрация информации о совершенном, совершаемом или планируемом преступлении, планирование расследования, а также тактика и методы проведения допроса потерпевшего и свидетелей.

1.1. Получение и регистрация информации о совершенном, совершаемом или планируемом преступлении.

Получение и регистрация информации о преступлении *(совершенном, совершаемом или планируемом)* – важный аспект в деятельности правоохранительных органов Республики Казахстан. Действующее законодательство страны устанавливает четкие правила и процедуры, которые должны быть соблюдены при получении и регистрации информации о преступлении.

Рис. 1

Получение информации о преступлении может осуществляться различными способами, включая устные или письменные жалобы и заявления граждан, организаций, информацию от свидетелей, письменные документы и другие источники, в том числе поступающие посредством информационно-коммуникационных технологий.

Правоохранительные органы должны принимать и реагировать на все полученные источники информации о возможных преступлениях и своевременно проверять такие сообщения. При получении информации о

преступлении органы правопорядка обязаны соблюдать принципы законности, презумпции невиновности и конфиденциальности.

Любая информация о преступлении должна регистрироваться в специальной базе данных, которая хранит информацию о преступлениях, лицах, участвующих в них, а также о ходе следствия и судебных решениях.

Для всех правоохранительных и специальных органов Республики Казахстан такой базой является «Единый реестр досудебных расследований» *(далее - ЕРДР)*, которая была разработана и внедрена в 2015 году, как база данных, призванная пресечь факты укрытия уголовных правонарушений.

Внедрение такой информационной системы позволяет решать сразу несколько задач одновременно, основными из которых стали обеспечение справедливости, эффективности и прозрачности уголовного судопроизводства, а также защита прав и свобод граждан.

Эффективность ЕРДР заключается в том, что он предусматривает единый порядок проведения досудебного расследования. Это установленные правила и процедуры, которые должны соблюдаться при проведении досудебного расследования. Они регламентируют действия правоохранительных и специальных органов, прокуратуры и судов на различных этапах расследования, включая сбор доказательств, работа со свидетелями, проведение экспертиз и т.д.

Иными словами – это универсальный информационный портал, где все участники процесса *(следователи, прокуроры, судьи)*, работая в единой информационной среде, могут обмениваться информацией и документами, что ускоряет и упрощает сам процесс расследования, а также обеспечивает прозрачность и доступность информации.

Кроме того, внедренный в него модуль учета и контроля повышает эффективность как ведомственной, так и прокурорской проверки соблюдения законодательства в процессе расследования уголовных правонарушений.

Ну и, конечно же, использование данной информационной системы способствует ускорению процесса досудебного расследования путем осуществления быстрого доступа к информации, возможности электронного обмена документами и автоматизации рутинных процедур, требуемых для завершения расследования уголовного дела.

Однако, несмотря на все установленные процедуры и правила, возможны случаи нарушения этих норм. Поэтому важно, чтобы граждане знали свои права и обязанности при сообщении о преступлении, а также знали, где и как обратиться, если их права нарушены.

В заключение, хотелось бы отметить, что получение информации о преступлении и ее последующая регистрация в информационной системе являются неотъемлемой частью правоохранительной деятельности в Республике Казахстан. Соблюдение законодательства и установленных процедур в этой сфере является важным условием эффективной работы правоохранительных органов и обеспечения прав и свобод граждан.

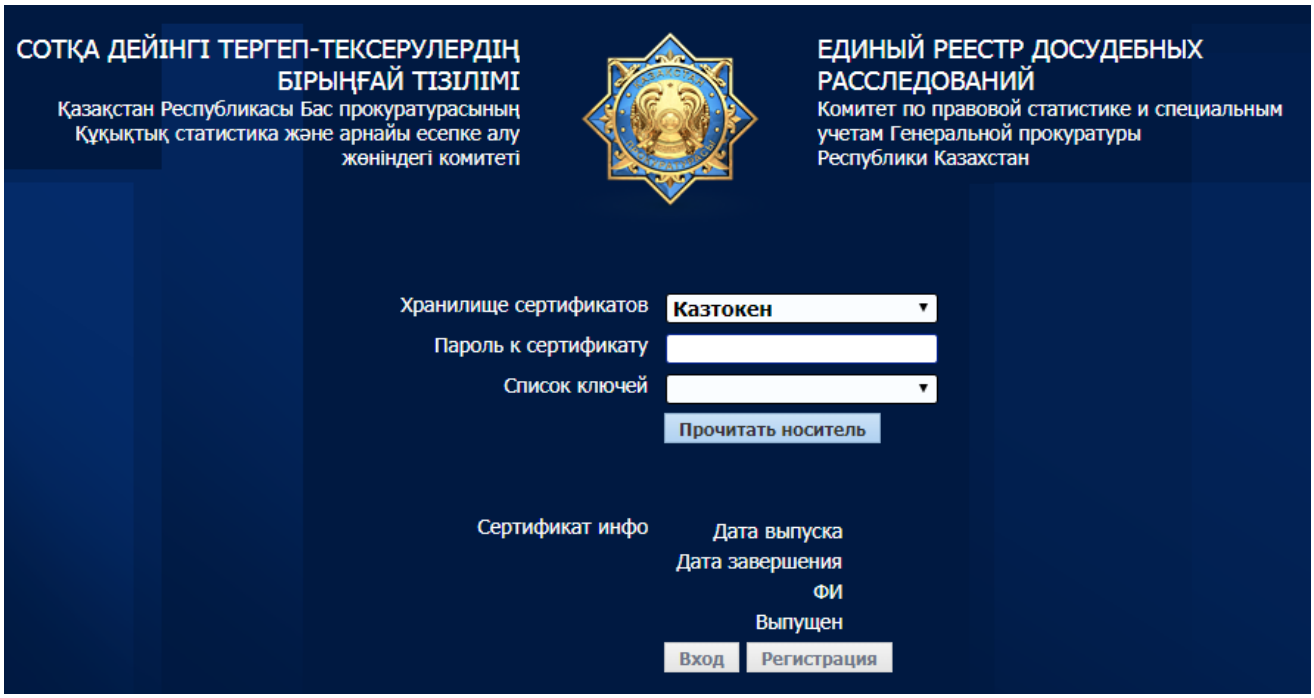
Для регистрации информации о преступлении в соответствии с Уголовно-процессуальным кодексом Республики Казахстан применяется специальная процедура.

Информация о планируемом, совершаемом или совершенном уже уголовном правонарушении принимаются оперативными дежурными органов уголовного преследования, которые производят ее фиксацию в Книге учета информации.[1]

Далее она подлежит рассмотрению уполномоченными должностными лицами в течение 24 часов с принятием решений, предусмотренных Правилами приема и регистрации заявления, сообщения или рапорта об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований, утвержденными приказом Генерального Прокурора Республики Казахстан от 19 сентября 2014 года № 89 *(далее – Правила)*.[2]

Сведения о регистрации заявления, сообщения или рапорта об уголовном правонарушении вводятся в ЕРДР незамедлительно.[3]

Рис. 2



Регистрация в Едином реестре досудебных расследований является этапом начала досудебного расследования, т.е. стадией возбуждения уголовного дела. Она производится путем заполнения формы Е-1 «Регистрация в ЕРДР» *(далее – форма Е-1)*, после сохранения которой уголовному производству автоматически присваивается регистрационный номер.

---

[1] Пункт 5 Правил приема и регистрации заявления, сообщения или рапорта об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований, утвержденных приказом Генерального Прокурора Республики Казахстан от 19 сентября 2014 года № 89 *(далее – Правила)*

[2] Пункт 8 Правил

[3] Пункт 57 Правил

Зарегистрированная информация о преступлении включает в себя данные о потерпевшем, обвиняемом, свидетелях, показаниях очевидцев, результаты следственных действий и все другие сведения, имеющие отношение к уголовному делу *(рис. 3)*.

Рис. 3

Форма Е-1
Регистрация в ЕРДР

1. Номер ЕРДР _____
Дата-время регистрации _____
Дата и время проведения неотложных следственных действий _____
2. Орган регистрации _____
3. Район (гарнизон, на транспорте) совершения _____
3.1 Номер войсковой части _____
4. Номер КУИ _____ дата КУИ "___"_____
5. Выделен из ЕРДР № _____
В отношении: в отношении уголовного правонарушения (преступления) в порядке части 3 статьи 44 УПК РК (01), в отношении лица в порядке части 1 статьи 44 УПК РК (02). _____
6. Укрыто путем: не регистрации (01), необоснованного оставления без рассмотрения и хранения в номенклатурном деле (наряде) (02), необоснованного направления в уполномоченный государственный орган или должностному лицу в соответствии с частью 5 статьи 181 УПК РК (03), необоснованное направление в уполномоченный орган, в компетенцию которого входит рассмотрение данного вопроса (04), необоснованного приобщения (05), необоснованного направления в суд по делам частного обвинения (06), путем передачи по подследственности (территориальности) без фактической передачи (07), не выделения в отдельное производство материала, имеющего признаки другого уголовного правонарушения (08), необоснованного привлечения к административной ответственности при наличии признаков уголовного правонарушения (09).
6.1 Укрытое от учета уголовное правонарушение выявлено: сотрудником Управления Комитета по правовой статистике и специальным учетам (1), прокурором (2), судом (3), ведомственным путем (4)
6.2 Орган, укрывший уголовное правонарушение (преступление) _____

Важно! Не подлежит регистрации информация (заявление, сообщения, рапорт) об уголовном правонарушении, в которой отсутствуют сведения, предусмотренные подпунктами 1 и 2 части 1 статьи 179 УПК РК.

Рассмотрение информации о преступлении – является одной из важнейших задач правоохранительных органов. Этот процесс заключается в анализе всех доступных данных и доказательств, связанных с преступлением, с целью выявления истинных обстоятельств и установления виновности лиц, совершивших преступление.

Процесс рассмотрения информации о преступлении (планируемом, совершаемом или совершенном) состоит из 2-х этапов:

Первый этап | **Сбор фактической информации о преступлении**

Здесь рассматриваются данные о месте и времени совершения преступления, характере преступления, вовлеченных в него лицах и возможных свидетелях.

На данном этапе проводится сбор различных фактов, показаний свидетелей, экспертных заключений и других доказательств, чтобы принять осознанное решение по делу. Собранные факты и доказательства помогают правоохранительным органам составить более подробную картину преступления и определить дальнейшие действия.

Второй этап | **Анализ полученных данных**

На втором этапе происходит анализ полученных данных с использованием различных методов и техник. Весь материал анализируется и проверяется на достоверность и соответствие законам и стандартам доказывания. Проводятся необходимые оперативно-розыскные мероприятия, с опросом возможных свидетелей и сбором доказательств.

По итогам рассмотрения информации, в случаях установления факта совершения уголовного правонарушения за пределами той административной территории, где правоохранительный орган ее зарегистрировал или расследование по уголовному делу относится к компетенции другого органа уголовного преследования, зарегистрированные материалы (заявления, сообщения) передаются по подследственности.

Важно! При принятии решения о передачи зарегистрированного материала (заявления, сообщения) по подследственности, он передается вместе с предметами и документами, собранными по нему[4].

Согласно подследственности, расследование уголовных правонарушений в сфере информатизации и связи в порядке предварительного следствия, дознания и протокольной формы осуществляется органами внутренних дел по всем составам, предусмотренным главой 7 Уголовного кодекса Республики Казахстан, за исключением совершенных в отношении критически важных объектов информационно - коммуникационной инфраструктуры, предварительное следствие по которым осуществляется органами национальной безопасности *(таблица 2)*.[5]

Таблица 2. Подследственность уголовных правонарушений в сфере информатизации и связи

Статья УК РК	**Форма досудебного расследования**	**Органы расследования**	
205 ч.1	протокольная форма	ОВД	

[4] ч.4 ст. 186 УПК РК
[5] ст.ст.187, 191 УПК РК

205 ч.2	протокольная форма	ОВД	
205 ч.3	предварительное следствие	ОВД	органы национальной безопасности *(если совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры)*
206 ч.1	протокольная форма	ОВД	
206 ч.2	предварительное следствие	ОВД	органы национальной безопасности *(если совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры)*
206 ч.3	предварительное следствие	ОВД	органы национальной безопасности *(если совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры)*
207 ч.1	дознание	ОВД	
207 ч.2	предварительное следствие	ОВД	органы национальной безопасности *(если совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры)*
207 ч.3	предварительное следствие	ОВД	органы национальной безопасности *(если совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры)*
208 ч.1	протокольная форма	ОВД	
208 ч.2	предварительное следствие	ОВД	органы национальной безопасности *(если совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры)*
208 ч.3	предварительное следствие	ОВД	органы национальной безопасности *(если совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры)*
209 ч.1	дознание	ОВД	
209 ч.2	предварительное следствие	ОВД	органы национальной безопасности *(если совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры)*
209 ч.3	предварительное следствие	ОВД	органы национальной безопасности *(если совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры)*
210 ч.1	дознание	ОВД	

210 ч.2	предварительное следствие	ОВД	органы национальной безопасности *(если совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры)*
210 ч.3	предварительное следствие	ОВД	органы национальной безопасности *(если совершено в отношении критически важных объектов информационно-коммуникационной инфраструктуры)*
211 ч.1	протокольная форма	ОВД	
211 ч.2	предварительное следствие	ОВД	
211 ч.3	предварительное следствие	ОВД	
212 ч.1	дознание	ОВД	
212 ч.2	предварительное следствие	ОВД	
213 ч.1	протокольная форма	ОВД	
213 ч.2	предварительное следствие	ОВД	
213 ч.3	предварительное следствие	ОВД	

Важно! Правила части первой стать 186 УПК РК не распространяются на случаи поступления заявлений, сообщений об уголовных правонарушениях, по которым требуется проведение неотложных следственных действий[6].

Вопросы для самоконтроля:

1) Кто получает и регистрирует информацию о совершенном, совершаемом или планируемом преступлении?

2) Куда регистрируется информация об уголовном правонарушении?

3) В течение какого времени информация об уголовном правонарушении, зафиксированная в КУИ, должна быть рассмотрена?

4) Что является поводами для начала досудебного расследования?

5) Назовите этапы процесса рассмотрения информации о преступлении.

6) Порядок передачи заявлений, сообщений по подследственности.

[6] ч. 3 ст. 186 УПК РК

1.2. Планирование досудебного расследования

Планирование досудебного расследования – это мыслительная деятельность следователя, направленная на определение задач расследования, а также на выбор методов и способов их решения. Иными словами, это перечень действий, которые следователь должен выполнить для успешного расследования уголовного дела. Планирование досудебного расследования является одной из важнейших стадий уголовного процесса, который включает в себя сбор и анализ значительного объема информации для выявления фактов и причин совершения преступления, установления участников и доказательств их вины.

В связи с этим, планирование досудебного расследования требует систематического подхода и детального изучения всех имеющихся данных, определения целей и задач, которые нужно достичь в ходе расследования.

Главная цель – установить все факты преступления и собрать достаточное количество доказательств для успешного завершения расследования. Задачи планирования могут включать определение потенциальных свидетелей, проведение экспертиз, изучение возможных местных объектов или документов, а также подготовку необходимой документации.

Одна из важных частей планирования – определение последовательности действий и распределение ресурсов. Это включает в себя назначение сотрудников, ответственных за различные аспекты расследования, установление сроков выполнения задач и определение доступных материальных и финансовых ресурсов.

Правильное планирование позволяет проводить расследование эффективно и в соответствии с установленными сроками.

Недооценка важности планирования и организации расследования может привести к негативным последствиям, таким как:

- *задержка в сроках расследования и неэффективное использование ресурсов;*

- *хаотичное и несистематическое проведение следственных и оперативно-розыскных мероприятий;*

- *отсутствие сотрудничества между различными органами, принимающими участие в расследовании;*

- *низкое качество предварительного расследования.*

Поэтому планирование расследования является неотъемлемым условием для правильной организации работы следователя и формирует основу для всестороннего, полного и объективного исследования обстоятельств дела в соответствии с требованиями Уголовно-процессуального кодекса Республики Казахстан.

Также важной составляющей планирования досудебного расследования является самоконтроль, в процессе которого следователь должен задать себе как минимум следующие вопросы, направленные на оптимизацию планирования и обеспечения его эффективности:

1. Какие конкретные цели и задачи необходимо достичь в ходе досудебного расследования?

2. Какие материальные и финансовые ресурсы необходимы для выполнения этих задач?

3. Какие доступные факты и доказательства могут помочь в осуществлении расследования?

4. Какие дополнительные исследования или действия необходимы для установления недостающих доказательств?

5. Какая последовательность действий оптимальна для достижения поставленных целей?

6. Какие могут быть проблемы или трудности в ходе расследования и как можно их предотвратить или преодолеть?

7. Какие альтернативные подходы или идеи могут помочь в улучшении эффективности расследования?

Ответы на эти вопросы могут помочь разработать более детальный и продуманный план действий (следственно-оперативных мероприятий), что значительно повысит вероятность успешного завершения расследования и достижения результата.

Выделяют следующие виды планирования расследования преступлений:

- *планирование отдельных следственных действий;*
- *планирование хода расследования уголовного дела;*
- *планирование работы по нескольким уголовным делам;*
- *планирование работы с группой следователей.*

Планирование отдельных следственных действий включает в себя определение ответственных лиц, необходимых для выполнения конкретного вида действия, подготовку необходимого оборудования и материалов, а также распределение ролей и задач между его участниками. Кроме того, при данном виде планирования следователь производит оценку рисков и разработку стратегии мероприятия для успешного выполнения того или иного следственного действия.

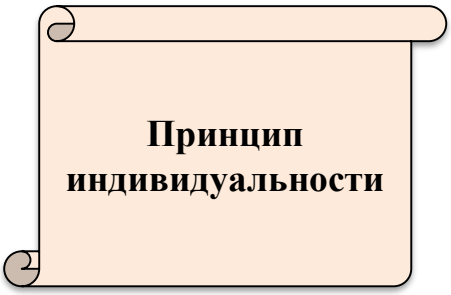
Планирование хода расследования уголовного дела включает в себя последовательность проведения следственных действий, сбор необходимых доказательств, анализ полученной информации, выявление связей между различными фактами и участниками преступления по одному уголовному делу.

Это позволяет следователям определить необходимый объем работы, организовать деятельность всех участников и прогнозировать возможные сложности или препятствия в расследовании.

Планирование работы по нескольким уголовным делам является сложным процессом, требующим систематического подхода и координации его участников, в том числе между различными правоохранительными органами.

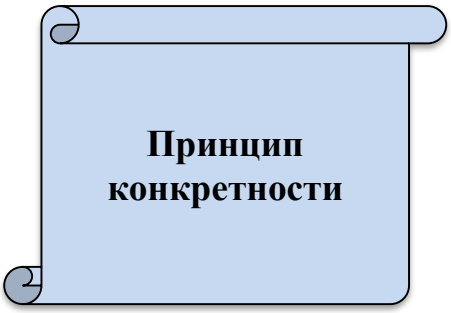
Планирование работы с группой следователей включает в себя определение структуры группы, назначение руководителя, распределение ролей и задач между участниками, установление схемы общения и взаимодействия, а также разработку системы контроля и обратной связи для эффективного управления работой группы.

Применяются следующие принципы планирования досудебного расследования.

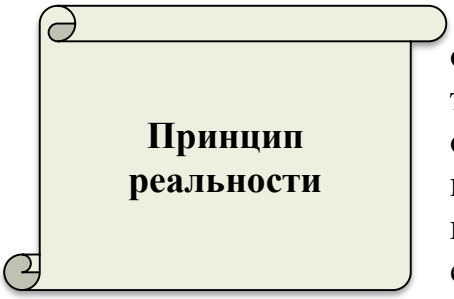


Каждое расследование уголовного дела требует индивидуального подхода, ведь нет двух идентичных преступлений. План расследования должен учитывать специфические особенности каждого конкретного случая. Творческий подход необходим для разработки уникального плана, адаптированного под конкретное преступление.

Планирование должно быть динамичным, что означает возможность корректировки и изменения плана расследования на основе новой информации, изменений в событиях или следственной ситуации. План может быть модифицирован, уточнен или дополнен даже на стадии его составления, если появляются новые данные, которые не были известны следователю ранее.



Данный принцип говорит о необходимости включения в план расследования четких и конкретных целей, задач и мероприятий. Каждый этап и действие должны быть описаны с ясными параметрами и указанием ответственных лиц. Конкретный план позволяет свести к минимуму вероятность ошибок, сбоев в расследовании.



Подразумевает создание плана расследования, основанного на доступных ресурсах, с учетом текущих возможностей правоохранительных органов. План должен быть реалистичным и выполнимым, а также учитывать наличие необходимых материальных, кадровых ресурсов для его осуществления.

Предполагает выбор наиболее эффективных мероприятий для достижения целей расследования. План должен быть оптимальным с точки зрения использования имеющихся ресурсов и достижения максимальных результатов при минимальных затратах.

В целом, эти принципы планирования расследования обеспечивают систематичность, гибкость и эффективность в работе правоохранительных органов. Они позволяют достичь максимальных результатов в расследовании

уголовных дел, обеспечить справедливость и защиту прав граждан, а также оптимизировать использование имеющихся ресурсов.

Процесс планирования расследования имеет свою структуру, состоящую из взаимосвязанных элементов, которые одновременно служат этапами этого процесса. Эти этапы включают определение целей расследования, анализ имеющихся фактов и доказательств, разработку плана действий, его реализацию, контроль и оценку достигнутых результатов.

Такими элементами является:

1) изучение первичных данных;

2) выдвижение версий;

3) определение обстоятельств, которые необходимо установить;

4) определения путей, средств и методов расследования;

5) определение последовательности и сроков решения отдельных заданий и выполнения отдельных действий;

6) определение исполнителей;

7) определение организационных мероприятий по привлечению исполнителей, обеспечению использования отдельных средств и проведению тех или других действий;

8) составление письменного плана;

9) коррекция и развитие плана.

Под первичными данными понимается полный объем фактической информации, которой следователь обладает на стадии планирования расследования. В процессе анализа полученной информации следователь определяет наличие признаков преступления, выявляет обстоятельства преступления, ищет сведения о подозреваемом, его причастности, возможных соучастниках и способах совершения преступления. На основе первичных данных формулируются следственные версии и определяются задачи, которые нужно решить.

Следственная версия – это основанное на фактических данных предположение следователя об имевших место событиях, которые могли быть связаны с совершенным преступлением или составляли его[7].

Затем разрабатывается общий план расследования уголовного дела, который в дальнейшем может быть уточнен *(дополнен)* планами конкретных следственных действий.

Обычно планируются сложные следственные действия, такие как следственный эксперимент или проверка показаний на месте, которые позволяют эффективно распределить задачи между участниками, оптимизировать использование времени и продолжительность действий.

Определение времени и места проведения следственного действия является важным элементом планирования. Местом проведения следственных действий могут быть место работы подозреваемого, свидетеля или потерпевшего, а также место жительства обвиняемого, подозреваемого, потерпевшего или свидетеля.

[7] https://esj.pnzgu.ru/files/esj.pnzgu.ru/podol_naya_nn_2020_2_13.pdf

План расследования включает в себя следующие информационные разделы:

1. Сведения об уголовном деле (статья, по которому возбуждено дело, краткое описание сути дела *(фабулу)*, лица, имеющие отношение к расследованию, важные даты).

2. Следственные версии *(предположения и гипотезы, касающиеся обстоятельств преступления)*.

3. Обстоятельства для установления *(информация о ключевых фактах и деталях, которые требуется выяснить в ходе расследования)*.

4. Перечень необходимых действий *(список оперативно-розыскных мероприятий, тактических операций, предполагаемых к выполнению)*.

5. Сведения об исполнителях или ответственных лицах.

6. Сроки исполнения мероприятий.

7. Результаты выполненных следственных действий.

В дополнение к вышеуказанным пунктам, план расследования также может включать следующие аспекты:

1. Доводы подозреваемого и методы проверки его утверждений.

2. Результаты проверки вышеуказанных доводов.

3. Мероприятия по устранению выявленных фактов или обстоятельств, способствовавших совершению преступления.

В следственной практике используются различные формы планов.

Чаще всего применяется табличная форма. Однако существуют и планы, представленные в виде набора вопросов, требующих выяснения. В данном случае следователь определяет для себя задачи по выявлению места и обстоятельств преступления.

При расследовании групповых преступлений, которые, как правило, требуют совместной работы нескольких следователей, план расследования формируется из индивидуальных планов каждого участника группы. Главным образом он основывается на делении преступлений на эпизоды, отображающие этапы расследования.

В плане прописывается, какие следственные действия проводит данный следователь, а также какие процессуальные решения он принимает или должен принять.

В случаях групповых, многоэпизодных преступлений, часто применяется планирование в форме «шахматной доски», которое, некоторым образом, аналогично игровому полю в шахматах. По горизонтали перечисляются фамилии подозреваемых, а по вертикали - эпизоды преступлений. В пересечении указываются действия определенного лица в конкретном эпизоде.

Общий план работы контролируется и при необходимости корректируется руководителем следственно-оперативной группы.

Эффективность расследования во многом зависит от грамотного планирования отдельных, чаще всего сложных и ресурсоемких следственных мероприятий.

В ходе расследования преступлений иногда возникают ситуации, когда вместо стандартного плана расследования уголовного дела, разрабатывается обычный план следственно-оперативных мероприятий. Этот план ориентирован на определение задач, требующих разрешения, а не на фиксацию фактов, которые нужно установить в соответствии со статьей 113 Уголовно-процессуального кодекса Республики Казахстан.

Следует отметить, что такой подход не соответствует нормам уголовно-процессуального закона и не учитывает принципы составления плана расследования уголовного дела.

В случае если следователь имеет на руках несколько уголовных дел, рекомендуется разработать общий календарный план, который позволяет не только контролировать сроки расследования, но и отслеживать ход расследования каждого из них. Это позволяет выполнять процессуальные действия последовательно и эффективно.

В противном случае расследование уголовных дел может быть недостаточно организованным, бессистемным и неэффективным.

По завершении расследования руководитель следственной группы должен составить отчет о завершении досудебного расследования, которое подписывается им и членами следственной группы.

В зависимости от характера фактических данных, их объема и содержания, планирование расследования можно разделить на два ключевых этапа:

- *первоначальный этап;*
- *последующий этап.*

Первоначальный этап начинается с момента регистрации материала в ЕРДР (начало расследования) и до выявления подозреваемого или обвиняемого.

На этом этапе предусмотрено проведение комплекса следственных действий совместно с оперативно-розыскными мероприятиями. Главная цель - выявить и зафиксировать следы преступления и другие улики как можно быстрее.

Этот этап включает в себя также выявление лиц, причастных к совершению преступления, сбор доказательств. Очень важно учесть, что на первоначальном этапе времени на промедление нет, поскольку любое затягивание выполнения действий может привести к потере важных улик и усложнить раскрытие преступления.

Последующий этап начинается с момента допроса подозреваемого по существу подозрения или предъявления обвинения и заканчивая завершением расследования.

На этом этапе уровень неотложности снижается. Это связано с тем, что на первоначальном этапе уже были предприняты меры для предотвращения уничтожения улик, сговора соучастников и вмешательства свидетелей в ход расследования.

На втором этапе расследования проводятся более глубокие проверки, такие как осмотр места происшествия, следственные эксперименты и допросы других свидетелей.

Образец составления плана расследования

План досудебного расследования
по уголовному делу № …….

Дата / время начала досудебного расследования……
Дата принятия к производству……
Дата признания подозреваемым…
Дата/время задержания …
Срок истечения содержания ……
Срок окончания расследования ……

Раздел I

Исходные данные: …….
Следственные версии:

1) ……..
2) ……..
3) ……..

Вопросы и обстоятельства, общие для всех версий	Следственные, оперативно-розыскные и иные действия	Срок	Исполнитель	Отметка о выполнении и результат

Раздел II

Следственная версия 1 …….

Выяснить		Следственные, оперативно-розыскные и иные действия	Срок	Исполнитель	Отметка о выполнении и результат
Вопросы по версии	Обстоятельства в связи с добытыми данными				

Следственная версия 2 ……

Выяснить		Следственные, оперативно-розыскные и иные действия	Срок	Исполнитель	Отметка о выполнении и результат
Вопросы по версии	Обстоятельства в связи с добытыми данными				

Следственная версия 3 ……...

Выяснить		Следственные, оперативно-розыскные и иные действия	Срок	Исполнитель	Отметка о выполнении и результат
Вопросы по версии	Обстоятельства в связи с добытыми данными				

Вопросы для самоконтроля:

1) *Что такое планирование расследования?*
2) *Назовите принципы планирования расследования?*
3) *Из каких элементов состоит план досудебного расследования?*
4) *Назовите формы планирования?*
5) *Какие этапы планирования существуют?*

1.3. Методы и тактика допроса потерпевшего и свидетелей

Допрос – это одно из важнейших этапов следственных действий, целью которого является получение от допрашиваемого лица информации о событиях, связанных с совершением преступления.

Основной тактической задачей при проведении допроса является получение от допрашиваемого лица подробной и достоверной информации обо всех обстоятельствах, связанных с преступлением. Эта информация включает в себя не только описание самого преступления, но и сведения о других фактах, которые могут быть важными для расследования уголовного дела, в том числе о лицах, которые могли быть свидетелями или участниками преступления.

В целом, допрос играет важную роль в установлении фактов и выявлении важных деталей, необходимых для успешного расследования преступления.

Выделяются 5 стадий (этапов) допроса *(схема 9)*.

I. Подготовительная стадия

В процессе подготовительной стадии следователем/дознавателем выполняются следующие действия:

1. Сбор исходных данных *(осуществляется сбор всей доступной информации, необходимой для проведения расследования)* путем:

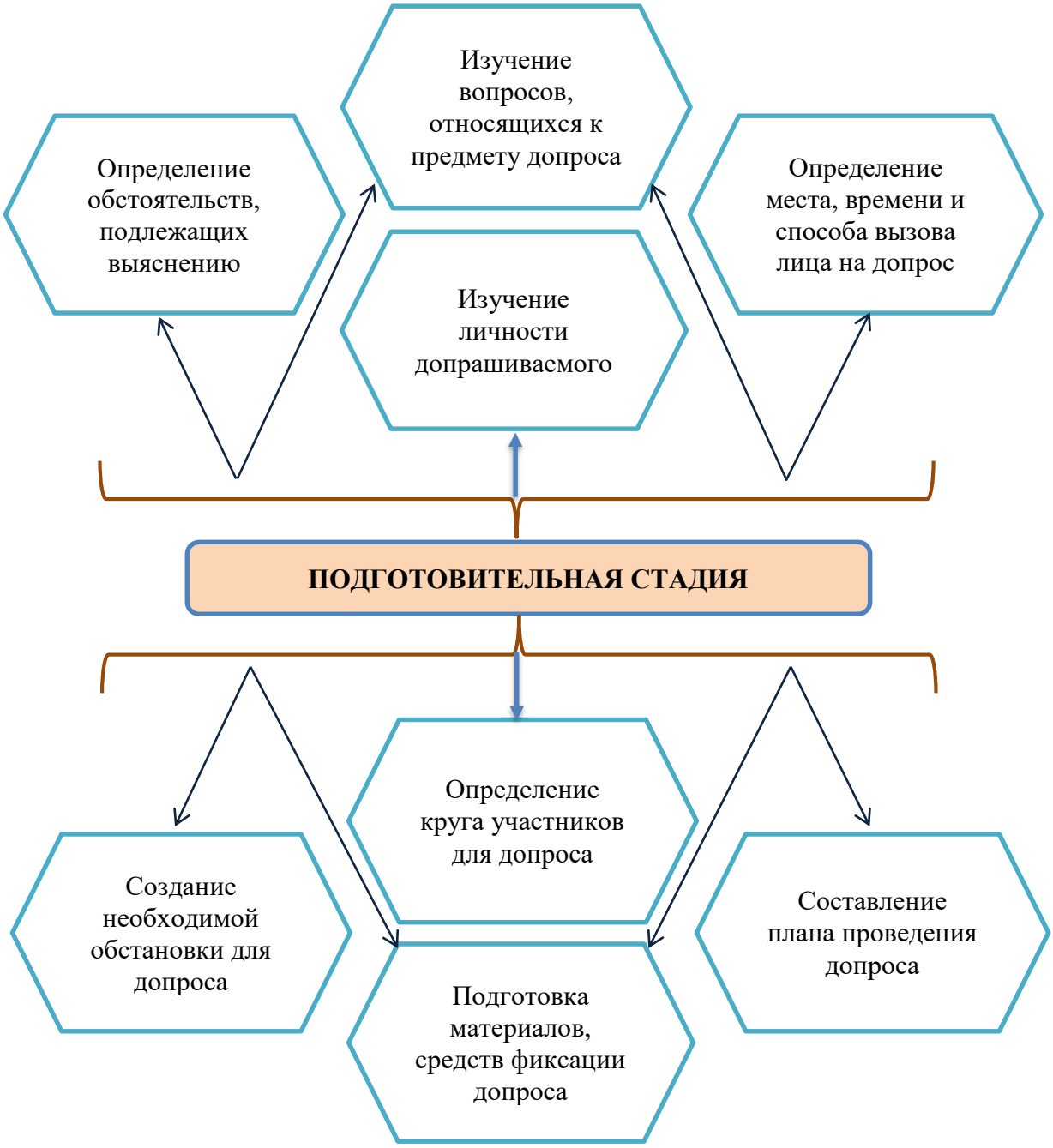
а) изучения материалов уголовного дела *(протоколы допросов, экспертные заключения, справки и другие документы, содержащие информацию о событиях, связанных с делом)*;

б) анализа вещественных доказательств *(физические предметы, следы, записи и другие материалы)* для определения их роли в расследовании и связи с устанавливаемыми обстоятельствами;

в) определения круга обстоятельств, подлежащих установлению. Это позволяет установить цели и направление дальнейших действий;

2. Обращение за помощью к специалисту, для получения дополнительной экспертной поддержки и анализа.

Схема подготовительной стадии допроса



Определение обстоятельств, подлежащих выяснению.

Подготавливаясь к допросу одного или нескольких лиц, следователю/дознавателю необходимо заблаговременно изучить материалы уголовного дела, с целью определения обстоятельств, подлежащих выяснению, в том числе их очередности.

Как правило, в первую очередь допрашиваются лица, располагающие наиболее важной информацией *(об обстоятельствах уголовного правонарушения, свидетелях, очевидцах и источниках доказательств)*, либо которые по различным причинам *(малолетний возраст, болезнь и другие)* могут забыть некоторые обстоятельства и детали.

Также учитываются разные факторы, включая возраст, состояние здоровья и другие обстоятельства, которые могут повлиять на способность свидетелей вспомнить события и детали.

Необходимо также учитывать возможность интересов сторонних лиц, включая подозреваемого, его соучастников и союзников, в исходе дела, и потенциальную вероятность того, что они могут договариваться или оказывать давление на свидетелей.

Изучение вопросов, относящихся к предмету допроса

Формулирование вопросов, требующих выяснения, является неотъемлемой частью подготовки к действиям, которые предполагают проведение расследования или допроса.

Проведя анализ материалов уголовного дела, следователь или дознаватель должен заблаговременно определить наиболее важные вопросы, которые необходимо задать допрашиваемому лицу, а также установить их последовательность.

При формулировании специфических вопросов, связанных с процессом допроса, следователь или дознаватель должен ознакомиться со специализированной литературой или проконсультироваться у соответствующего специалиста.

Изучение личности допрашиваемого.

Изучение личности лица, подвергаемого допросу, оказывает существенное влияние на успешность и эффективность проведения допроса. Выбор тактических приемов в значительной мере определяется информацией о личности допрашиваемого. Эта информация может быть получена из разных источников, таких как показания других свидетелей, характеристики из места работы или учебы, оперативные данные, а также ведомственные базы данных.

Необходимо осознавать, что иногда допрос требуется провести немедленно, но сбор информации о личности допрашиваемого по вышеуказанным методам может потребовать некоторого времени. В таких случаях важно использовать уже доступные сведения о допрашиваемом, собранных в материалах уголовного дела.

Далее информация собирается уже в процессе заполнения анкетных данных в протоколе допроса. После этого некоторые вопросы могут быть скорректированы и уточнены. Иногда для получения дополнительной

информации о личности допрашиваемого, перед допросом может проводиться обычная беседа с ним без фиксации сведений в протоколе.

Определение места, времени и способа вызова лица на допрос.

Для успешного проведения допроса следователь/дознаватель должен тщательно выбрать место, время и способ вызова лица, учитывая контекст и особенности допрашиваемого.

а) место допроса.

Обычно допросы проводятся в служебных кабинетах должностного лица правоохранительного органа. Но, в зависимости от обстоятельств, они могут также проходить по месту жительства, работы или учебы допрашиваемого.

Однако самым эффективным вариантом является проведение допроса на месте события. Это позволяет допрашиваемому лучше вспомнить обстоятельства произошедшего и более детально передать информацию.

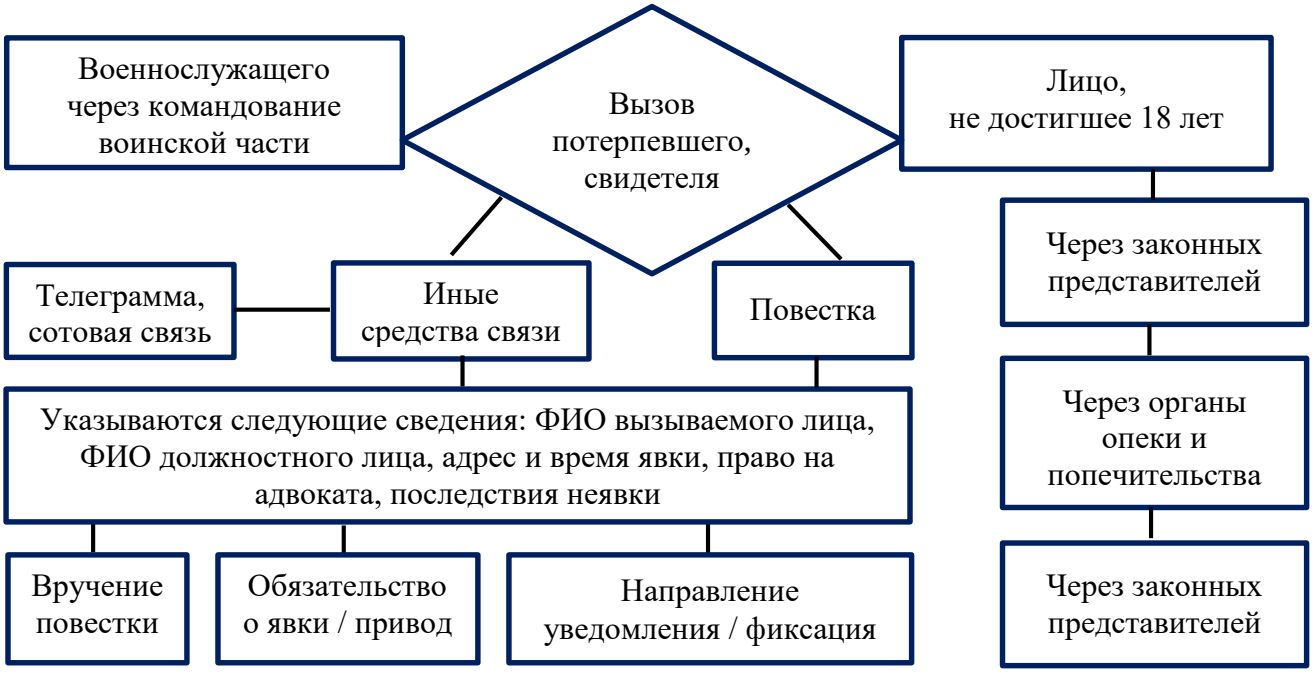
б) время допроса.

Выбор времени для допроса также имеет большое значение для эффективности и достижения результата. Психологический контакт с допрашиваемым будет легче установить, если выбрать удобное для него время. При этом, следует избегать ситуаций, когда допрашиваемый должен долго ожидать в коридоре.

в) способ вызова.

Также важно рассмотреть способ вызова допрашиваемого лица. При вызове нескольких свидетелей по одному и тому же уголовному делу следователь/дознаватель должен предпринять меры, чтобы они не могли общаться между собой до допроса. Это можно обеспечить, назначая разные часы и иногда дни для их явки. Соблюдение всех этих аспектов поможет обеспечить более эффективное и продуктивное проведение допросов в уголовном процессе.

Порядок вызова на допрос потерпевшего и свидетелей, регламентируется статьей 208 УПК РК и предусматривает выполнение определенных действий.



Создание необходимой обстановки для допроса.

Для обеспечения максимальной концентрации допрашиваемых лиц и исключения возможных отвлекающих факторов, необходимо организовать допрос в соответствующих условиях. Обычно это означает использование кабинета следователя или дознавателя, предусмотренного для индивидуальных допросов. В случае, если в одном помещении работают несколько следователей, важно назначать допросы так, чтобы они не пересекались по времени и не мешали друг другу. Также возможен вариант использования специально оборудованных кабинетов для допросов, в которых следует предпринять меры по исключению «раздражителей», таких как телефонные звонки, лишние предметы и т.д.

Определение круга участников допроса.

Для проведения допроса следователь / дознаватель имеет возможность вовлечь специалистов или экспертов, которые в свою очередь, могут предоставлять пояснения по возникающим вопросам или, с разрешения допрашивающего, задавать вопросы.

Кроме того, в ходе допроса могут участвовать следующие лица: защитники, переводчики, законные представители, опекуны, родственники несовершеннолетних и педагоги.

Подготовка материалов, подлежащих предъявлению в ходе допроса, а также средств фиксации его хода и результатов.

В процессе допроса может возникнуть необходимость предъявить допрашиваемому физические доказательства или материалы, связанные с уголовным делом. В таких случаях физические доказательства должны быть легкодоступными для следователя / дознавателя или иметься закладки в материалах дела.

Для фиксации процесса допроса и его результатов могут использоваться видеокамеры или диктофоны, и о применении этих средств делается соответствующая запись в протоколе.

Составление плана проведения допроса.

На основе анализа и оценки всех вышеупомянутых обстоятельств следователь / дознаватель должен разработать стратегию проведения допроса, в которой уже определены вопросы, требующие выяснения, их последовательность, а также порядок предъявления физических или цифровых доказательств и материалов уголовного дела.

Эта стратегия может быть выражена устно или в виде кратких заметок. Однако для наиболее сложных допросов часто разрабатывается подробный письменный план. Важно учитывать, что следователю / дознавателю следует подготовить несколько вариантов планов, поскольку обстановка на допросе может меняться внезапно.

II. Предварительная стадия

На предварительной стадии следственных действий следователь / дознаватель обязан установить личность допрашиваемого. В ходе допроса в

протоколе заполняются анкетные данные, разъясняются его права и обязанности. Важно уведомить потерпевшего и свидетеля об ответственности за дачу ложных показаний или отказ от дачи показаний.

При этом свидетель вправе отказаться от дачи показаний, которые могут повлечь за собой преследование его самого, супруга *(супруги)* или близких родственников за совершение уголовного или административного правонарушения.

Допрос в качестве свидетеля не предусматривается для следующих лиц:

- судьи и присяжные заседатели в отношении обстоятельств, связанных с уголовным делом, в котором они участвовали и решением которого принимали участие;
- защитники подозреваемых, обвиняемых, подсудимых, осужденных и их законные представители, а также представители потерпевшего, гражданского истца и ответчика, а также адвокаты свидетелей в отношении фактов, связанных с их профессиональной деятельностью;
- священнослужители в отношении информации, полученной в результате исповеди;
- лица, которые по своему возрасту или психическим и физическим особенностям не способны давать правильные показания;
- медиаторы, исключая случаи, предусмотренные законом;
- участники национального превентивного механизма, за исключением ситуаций, угрожающих национальной безопасности.

Этот этап допроса направлен на знакомство с допрашиваемым, его личностными особенностями, выяснения его позиции и установления с ним психологического контакта.

III. Стадия непосредственного допроса.

На этом этапе допроса потерпевшему или свидетелю предоставляется возможность изложить все, что им известно о произошедшем. Важно воздерживаться от лишних перебиваний допрашиваемого, если нет крайней необходимости. При этом следователь / дознаватель может задавать уточняющие вопросы без их фиксации в протоколе допроса, чтобы более детальнее выяснить обстоятельства произошедшего. Также следователь / дознаватель может указать на нерелевантные факты, о которых говорит допрашиваемый.

Кроме того, допрашиваемому предоставляется право использовать документы и записи, особенно в случаях, связанных с цифровыми данными или другой информацией.

IV. Вопросно-ответная стадия.

Следователь или дознаватель имеет право задавать вопросы с целью напоминания, уточнения или дополнения показаний допрашиваемого.

Напоминающие вопросы используются для активизации памяти допрашиваемого, уточняющие – для получения более детальной информации и дополнительные – для восполнения пробелов в предоставленных показаниях.

Важно, чтобы вопросы формулировались ясно и четко, и они не должны содержать подсказок и быть наводящими.

V. Заключительная стадия.

Когда следователь или дознаватель проводит допрос, он внимательно записывает все сказанное от первого лица, стараясь сохранить точность выражений. После этого в протоколе фиксируются вопросы и соответствующие ответы в том порядке, в котором они звучали в ходе допроса.

Необходимо не упустить из виду участие специалистов или экспертов в допросе. Их вопросы и ответы также следует отразить в протоколе для полноты и точности документации.

Обычно допрос потерпевших и свидетелей происходит в спокойной обстановке, при которой они добровольно предоставляют информацию. Однако возможны ситуации, когда допрашиваемый забывает или неправильно воспринимает некоторые детали произошедшего, что может повлиять на их точность.

В таких случаях следователь или дознаватель должны помочь допрашиваемому восстановить хронологию событий, используя определенные тактические методы. Например, потерпевший или свидетель могут быть приглашены на допрос по средствам телефонной связи или через неофициальное сообщение, что исключает необходимость формальных повесток с предостережениями.

Официальная повестка используется только в случае уклонения от явки или нарушения ранее согласованной даты. При этом, предупреждая об уголовной ответственности за отказ от дачи показаний или предоставлении заведомо ложных сведений, следователь или дознаватель должны объяснить потерпевшему или свидетелю всю серьезность и ответственность следственного действия.

Допрос, проводимый в форме хронологической последовательности, способствует более точному восстановлению событий. В таком случае допрашиваемому предлагается вспомнить все действия, начиная с определенного момента конкретного дня. Это позволяет более систематически и детально воссоздать ход событий и предоставить более полные и точные показания.

В общем, учитывая особенности уголовных правонарушений в сфере информатизации и связи, при проведении допроса потерпевшего необходимо установить следующие моменты:

- цель использования устройства / системы, например, для бухгалтерии или других целей;

- сведения о владельце и/или пользователе устройства/системы, а также информацию о паролях, логинах и данных о поставщике интернет-услуг;

- пароли для доступа к системе, программам и данным. У человека могут быть разные пароли, включая те, которые используются для BIOS, входа в систему, подключения к интернету, и другие;

- информацию о уникальных алгоритмах безопасности или методах уничтожения данных;

- данные об учетных записях в социальных сетях, таких как «Instagram», «Facebook», «ВКонтакте» и других платформах.

- сведения о внешних устройствах для хранения данных;

- руководства по использованию аппаратного или программного обеспечения, установленного на компьютере;

- информацию о получении электронных сообщений, в которых предлагается участие в розыгрышах, уведомления о выигрыше, срочные уведомления о необходимости устранения угрозы, выполнения платежей и т.д.;

- детали о прикрепленных файлах или установленном программном обеспечении, полученных в электронных письмах;

- сведения об участии в маркетинговых акциях, розыгрышах, проводимых от имени банков второго уровня, крупных компаний, известных магазинов и отдельных лиц в социальных сетях;

- информацию о регистрации в социальных сетях и на различных веб сайтах, включая анкетные данные, номера мобильных телефонов;

- информацию о банковских счетах и реквизитах банковских карт;

- сведения о получении электронных носителей из неизвестных источников, их использования на компьютере, копировании и скачивании файлов и т.д.;

В процессе допроса свидетелей, включая сотрудников организаций и обслуживающий персонал, необходимо получить ответы на следующие вопросы:

- были ли случаи прежних инцидентов кражи информации, содержащейся на электронных носителях?

- имели ли кто-то из сотрудников организации или обслуживающего персонала интерес к содержимому контейнеров *(корзин, пакетов и т.д.)*?

- совершал ли кто-то из работников неправомерные манипуляции с информацией?

- были ли нарушения установленного режима работы компьютерных систем или других средств компьютерной техники, а также необоснованные потери данных?

- срабатывали ли средства защиты компьютерной техники?

- появлялись ли в помещении, где находится компьютерная техника, посторонние лица *(электрики, сантехники, радиотехники, связисты, инспекторы противопожарной службы, контролеры горэлектросетей, охранники и т.д.)*?

- нарушались ли правила ведения журналов учета времени работы компьютерных систем *(если да, то кто допустил эти нарушения)*?

- были ли случаи необоснованных манипуляций с информацией *(изменение, стирание без серьезных на то причин)*?

- работали ли какие-либо лица сверхурочно без наличия официальных оснований?

- проявлял ли кто-то интерес к информации, не относящейся к их непосредственной деятельности?

- знают ли о лицах, посещавших другие подразделения и службы организации без достаточных оснований, где расположены компьютерные сети?

- были ли те, кто высказывал недовольство контролем над своей деятельностью?

- есть ли случаи, когда кто-то выражал недовольство рутинной работой?

- существовали ли ситуации, когда кто-то был небрежен при работе с компьютерной техникой?

- можете ли указать, где еще расположены компьютеры *(в случаях, когда они объединены в сеть, некоторые компьютеры могут находиться в других помещениях или городах)*?

- убеждены ли вы, что управленческие и технические процедуры соответствуют требованиям компьютерной безопасности?

- были ли случаи, когда телефонные переговоры были прослушаны?

Отмечаем, что этот перечень вопросов не является исчерпывающим как для потерпевшего, так и для свидетелей. Следователь/дознаватель может добавить дополнительные вопросы, учитывая обстоятельства конкретного уголовного правонарушения.

Вопросы для самоконтроля:

1) Что такое допрос?

2) Назовите 5 стадий (этапов) допроса.

3) Что включает в себя подготовительная и предварительная стадии допроса?

4) Опишите стадию непосредственного допроса.

5) Из чего состоит вопросно-ответная стадия допроса?

6) Раскройте содержание заключительной стадия допроса?

ГЛАВА 2. ОСНОВНОЙ ЭТАП РАССЛЕДОВАНИЯ

В данной главе будут рассмотрены такие вопросы, как осмотр места преступления и компьютерной техники, поиск и изъятие электронных доказательств, работа с ними, назначение судебных экспертиз, анализ заключений судебных экспертиз, розыск подозреваемого и международное сотрудничество.

2.1. Осмотр места преступления и компьютерной техники.

В современном мире информационно-коммуникационные технологии широко распространены, мы сталкиваемся с ростом компьютерных преступлений. Эти преступления отличаются от традиционных тем, что они имеют высокую латентность и низкий уровень раскрываемости.

Однако, их выявление и раскрытие становятся вызовом, так как они часто совершаются опытными преступниками, использующими сложные технические методы. В данном контексте успешное расследование компьютерных преступлений зависит от высокой квалификации сотрудников, специализирующихся на этой проблеме, и их умения применять свои знания в работе.

Необходимо отметить, что на практике иногда следователи, начиная расследование таких дел и проводя осмотр места преступления, могут столкнуться с недостаточным пониманием того, что они должны делать и как, с чего начать и на что сосредотачивать внимание.

Осмотр места преступления

Особые сложности возникают при исследовании компьютерной техники и поиске электронных улик в сети Интернет. Согласно принципам криминалистики, успешное раскрытие любого преступления во многом зависит от тщательности проведенного осмотра, выявления, фиксирования, исследования и эффективного использования следов, которые отражают различные аспекты криминальных событий.

В данном контексте, качество осмотра места происшествия, собранных улик и проведенных экспертиз играет важную роль. Осмотр места происшествия представляет собой одно из важных, а порой и неотложных следственных действий. Его целью является установление обстоятельств события, определение места и времени совершения преступления, а также обнаружение и фиксация доказательств.

Проведение осмотра места преступления в компьютерных делах представляет собой наиболее сложное и трудоемкое следственное действие. Он включает в себя непосредственное обнаружение, анализ и исследование объектов, имеющих значимость для дела, их характеристик, состояния и взаимного расположения с целью обеспечения успешного расследования компьютерных преступлений. В отличие от традиционных преступлений, где

обстановка часто более очевидна, в случае компьютерных преступлений необходимы специфические знания.

В процессе проведения этого следственного действия следователь или оперативный сотрудник должны быть знакомы не только с общей концепцией осмотра места преступления, но и с правилами изъятия компьютерной техники и другой информации, содержащей электронные доказательства. Качество выполнения этого этапа расследования существенно влияет на успешное раскрытие компьютерных преступлений.

Осмотр места происшествия в рамках дел, связанных с компьютерными преступлениями, преследует следующие цели:

- раскрытие деталей события включая метод, место и время преступления, а также идентификацию виновных лиц, путем проведения анализа обстановки на месте обнаружения признаков компьютерного преступления;
- выявление, фиксацию, изъятие и оценку следов преступления, включая как традиционные следы, известные в криминалистике, так и нетрадиционные, связанные с информационными артефактами компьютерной информации, а также различные материальные доказательства;
- предоставление необходимой информации для разработки и проверки версий событий, а также проведения оперативной работы по раскрытию компьютерных преступлений и розыску виновных лиц.

Проведение осмотра места происшествия *(будь то территория, жилище или какое-либо служебное помещение)* представляет собой отдельное следственное действие, которое нацелено на оперативное выявление следов преступления и выяснение других обстоятельств, имеющих значимость для уголовного дела.

Данное следственное действие является первичной и срочной мерой в рамках расследования киберпреступлений. Эта неотложность подчеркивается тем, что осмотр должен быть проведен незамедлительно после принятия решения следователем или дознавателем о его необходимости, но он также может быть осуществлен на любом этапе расследования.

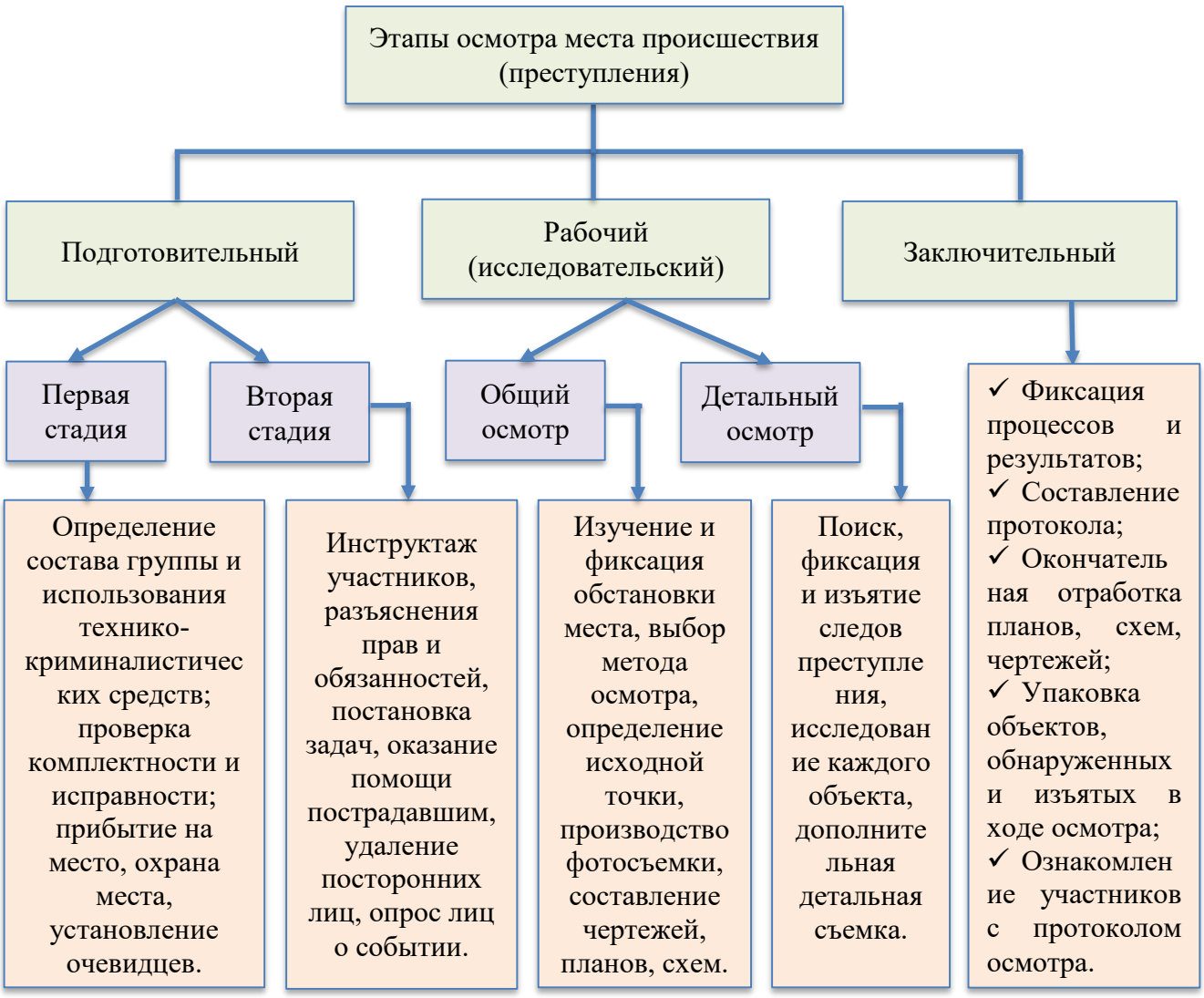
Важно различать два аспекта осмотра: место происшествие и место преступления, так как они могут различаться по характеру и целям проведения.

Осмотр места происшествия *(преступления)* направлен на выявление и установление всех ключевых аспектов. Для достижения этой цели, следователю или дознавателю необходимо:

- определить характер исследуемого события;
- определить точное место, время события, а также остальные важные обстоятельства;
- аккуратно обнаружить, исследовать и зафиксировать все следы, оставленные преступником;
- собрать и задокументировать другие следы и материальные доказательства;
- определить любые изменения в положении и характеристиках объектов до и после события;
- фиксировать фактические данные, которые, хоть и имеют отношение к делу, но не могут быть объяснены на основе первоначальной версии.

Осмотр места происшествия *(преступления)* имеет условное деление на три этапа: подготовительный, рабочий *(исследовательский)* и заключительный.

Подход и тактика, применяемые на каждом из этих этапов, представлены в графической схеме.



Подготовительный этап осмотра места происшествия *(преступления)* - это начальный и важный этап в работе следователя *(дознавателя)*, включающий в себя ряд мероприятий, направленых на обеспечение эффективного и безопасного сбора и анализа доказательств.

Начнем с того, что к осмотру места компьютерного *(кибер)* преступления необходимо готовится.

Первое. Планирование и оценка рисков.

Данное мероприятие предусматривает анализ информации *(сообщения)* о происшествии *(преступлении)*, определение потенциальных угроз безопасности *(риски потери или повреждения данных при осмотре или изъятии)* и разработка плана действий *(стратегии для сбора и обработки цифровых следов, а также сохранения целостности электронных доказательств)*.

Второе. Подготовка и определение участников (формирование команды) следственно - оперативной группы.

Учитывая технические аспекты совершения преступлений, данной категории, к осмотру следует привлечь квалифицированных специалистов в сфере IT-технологий, а также по возможности судебных экспертов, специализирующихся в данной области для анализа и изъятия цифровых следов, переводчиков *(при необходимости)*, понятых. Со всеми участниками группы проводится инструктаж, разъясняются их права и обязанности.

Третье. Получение разрешений и санкций на проведение отдельных следственных действий.

В зависимости о места проведения смотра, характера преступления, лица, совершившего уголовное правонарушение, возможно потребуется официальное разрешение или санкция суда на проведение осмотра или обыска.

Четвертое. Подготовка оборудования.

Поскольку осмотр предполагает работу с компьютерной информацией, необходимо иметь свою компьютерную технику *(обычно это ноутбук с большим объемом памяти)* и специальное программное обеспечение для изъятия данных с компьютера подозреваемого или потерпевшего без внесения в него изменений *(снятие образов дисков, анализ цифровых данных, хеширование и т.д.)*. Также необходимо иметь средства для физического обследования компьютерной техники. Все техническое оборудование должно быть заранее проверено на предмет исправности, функционирования и комплектности.

Пятое. Прибытие на место.

Обеспечивается охрана места происшествия *(преступления)*, удаляются оттуда посторонние лица *(с целью предотвращения повреждения или уничтожения доказательств)*, устанавливаются очевидцы *(если они имеются)*, оценивается ситуация, ставятся задачи каждому участнику следственно-оперативной группы, опрашиваются лица, находящиеся на месте о произошедшем событии или известных им фактах.

Таким образом, основная цель данного этапа заключается в минимизации потери данных и сохранении информации полезной для следствия.

Рабочий *(исследовательский)* этап осмотра места происшествия *(преступления)* – является ключевой частью расследования и представляет собой процесс, включающий документирование и сбор физических и электронных доказательств с целью последующего их анализа и идентификации, результаты которых могут быть использованы для реконструкции хронологии произошедших событий и установления подлинных обстоятельств происшествия.

Этот этап осмотра места происшествия *(преступления)* состоит из двух последовательных стадий:

а) общего осмотра;

б) детального осмотра.

Задачами общего осмотра являются:

- *определение границ места происшествия (преступления), с целью установления территории местности или помещения, которые необходимо подвергнуть подробному исследования и анализу;*
- *фиксация общих особенностей окружающей обстановки и видимых изменений, с целью дальнейшей регистрации и описания физических параметров, структуры и состояния места происшествия;*
- *выявление фактов и обстоятельств, которые могли привести к происшествию, включая потенциальные причины и мотивацию событий;*
- *определение возможных мест, где могут находиться следы преступления, включая, но не ограничиваясь местоположением электронных следов, которые могут быть важными для расследования;*
- *сбор первичной информации, включая свидетельские показания, с целью получения первичных данных от свидетелей и других участников происшествия для последующего анализа и проверки*.

Определение порядка осмотра места происшествия зависит от ситуации и условий на месте. Во время осмотра необходимо уделить внимание каждой детали помещения или территории, а также любым предметам или следам, которые могут быть полезными для следствия. Поэтому наилучший результат достигается благодаря полному осмотру места происшествия, который может быть проведен по спирали, по концентрической, эксцентрической или фронтальной схеме.

При концентрическом методе осмотра места происшествия осмотр начинается от периферии и движется к центру. При эксцентрическом методе осмотр происходит от центра к периферии, в постепенно расширяющихся кругах. При фронтальном методе осмотр происходит линейно, по секторам или квадратам, от одной границы к другой[8].

При проведении общего осмотра места происшествия (преступления) необходимо составить схему осматриваемого помещения, отметить на ней места расположения оборудования, с помощью которого возможно было совершено преступление, сети и точки связи с системами.

[8] https://pravo.studio/osnovyi-kriminalistiki/taktika-rabochego-etapa-osmotra-mesta-76017.html

Важно, чтобы каждый шаг следователя *(дознавателя)* сопровождался фотосъемкой или видеозаписью *(при необходимости)*.

Более того, при осмотре рабочего места, компьютеров или другого оборудования, с помощью которого совершено преступление, следователь *(дознаватель)* должен выяснить следующие вопросы, обязательные для расследования киберпреступления:

- *в каком состоянии находится компьютер (включен, выключен или в режиме ожидания);*
- *подключён ли компьютер к локальной сети, наличие распределительной коробки, разветвлений, сетевых и телефонных розеток;*
- *является ли сеть проводной или беспроводной (Wi-Fi);*
- *имеются ли в осматриваемом компьютере или сети устройства удалённого доступа.*

По завершении общего осмотра места происшествия (преступления) следователь начинает осматривать его более детально.

Задачами детального осмотра являются:

- *тщательное исследование каждого квадратного метра места происшествия (преступления) с учетом мельчайших деталей;*
- *сбор всех физических доказательств (например, волосы, волокна, отпечатки пальцев, следы обуви и т.д.);*
- *фиксация местоположения каждого найденного следа относительно общей картины произошедшего;*
- *установления хронологии событий на основе найденных доказательств и свидетельских показаний;*
- *выявление возможных противоречий или несоответствий между свидетельскими показаниями, выявленными следами преступления и установленными доказательствами для создания последовательной и логической картины событий произошедшего.*

В процессе детального осмотра осуществляется тщательное изучение всех объектов и следов, обнаруженных на месте. На данном этапе допускается брать в руки рассматриваемые объекты, передвигать их с места, поворачивать и осматривать со всех сторон. Исходя из этих действий, этап детального осмотра называется динамическим[9].

Общий и детальный осмотры места происшествия (преступления) позволяют собирать максимум информации и доказательств, необходимых для последующего расследования. Они являются важным этапом криминалистической деятельности, направленным на раскрытие преступления, поэтому должны проводиться внимательно и аккуратно.

Следует обратить внимание, что на практике может отсутствовать четкое различие между общим и детальным осмотром из-за их возможного чередования.

Например, при обнаружении объекта следователь или дознаватель могут зафиксировать его в статическом состоянии, затем провести подробное

[9] Балашов Д.Н. Криминалистика: Тактика рабочего этапа осмотра места происшествия. Учебник. - М.,2005. - 503 с.

исследование, регистрируя результаты в протоколе, и после продолжить общий осмотр.

Также возможны случаи, когда осмотр места происшествия не проводится вовсе из-за его отсутствия, что больше всего относится к киберпреступлениям.

Следовательно, распознавание места совершения киберпреступления невозможно без установления обстановки совершения преступления, которая определяется в киберпространстве.

Кроме того, при расследовании киберпреступлений следует проводить осмотр следующих мест:

- где обрабатывается и хранится информация, которая подверглась преступным воздействиям:

- компьютеры и ноутбуки *(хранилища данных, включая жесткие диски, облачные аккаунты и съемные носители информации, электронные почты, логи и журналы событий систем, виртуальные машины, криптоконтейнеры, другие программы, используемые для преступных целей)*;

- мобильные устройства *(мессенджеры, социальные сети, другие приложения для коммуникации)*;

- серверы, сетевое оборудование *(маршрутизаторы, коммутаторы для анализа сетевого трафика)*, используемые преступниками;

- где преступники непосредственно используют компьютерное оборудование и сети для совершения киберпреступлений: квартира, дом, офис, игровой клуб, интернет – кафе, библиотека, иное общественное место, например, парк, кафе, ресторан, гостиница, где имеются точки доступа к интернету;

- где наступили определенные последствия от незаконных действий киберпреступников: место жительство потерпевших, если это физическое лицо или офисное помещение, если это юридическое лицо.

По завершению рабочего *(исследовательского)* этапа следователь *(дознаватель)* переходит к завершающей стадии осмотра места происшествия *(преступления)*.

Заключительный этап осмотра места происшествия *(преступления)* – представляет собой финальную часть данного следственного действия, в ходе которой следователь *(дознаватель)* повторно изучает обнаруженные и изъятые объекты, сопоставляет их с записью в протоколе, проверяет надежность и целостность упаковок с изъятыми предметами, следами, принимает меры к сохранности тех объектов и следов, которые невозможно изъять с места происшествия, но которые имеют важное значение для доказательства вины преступника.

Следователь *(дознаватель)* также проверяет правильность и полноту заполнения протокола осмотра места происшествия, подписывает его и приобщает к нему составленные планы, схемы, чертежи, фотографии.

После чего он должен ознакомить всех участников с протоколом осмотра места происшествия (преступления), получить от участников предложения и замечания (при наличии).

Осмотр компьютерной техники

Преступления, совершаемые в компьютерной системе и сети Интернет, всегда оставляют электронные следы. Это изменения, которые киберпреступник вносит в информационную систему, информацию или базу данных.

Поэтому при расследовании преступлений, совершаемых с использованием информационно-коммуникационных технологий действия следователя должны быть направлены на поиск, обнаружение и изъятие таких следов.

Однако, прежде чем приступить непосредственно к осмотру компьютерной техники и других устройств, находящихся рядом или подключенных к ней, необходимо выполнить несколько рекомендаций, направленных на обеспечение безопасности и сохранение всех следов преступления.

При этом, следует отметить, что последовательность действий следователя при производстве такого осмотра может отличаться в зависимости от места его проведения (осмотр у потерпевшего или подозреваемого).

Находясь в помещении *(квартира, офис и т.д.)*, где непосредственно находится компьютерная техника и (или) любое другое оборудование, следователь *(оперативный сотрудник, криминалист, судебный эксперт)* должен выяснить:

1) Подключено ли исследуемое устройство (компьютер, ноутбук) к источнику питания? Это можно выяснить путем визуального осмотра самого устройства, соединительных кабелей, сетевых фильтров;

2) Находится ли устройство *(компьютер, ноутбук)* во включенном состоянии или выключенном *(это можно выяснить путем визуального осмотра самого устройства)*?

Иногда бывает очень сложно определить в каком состоянии находится устройство. Визуально компьютер может выглядеть как выключенный, а на самом деле находиться в режиме ожидания. Более того, некоторые заставки на экранах компьютера могут создать впечатление, что он выключен.

Для чего это необходимо? Порядок осмотра включенной рабочей станции и выключенной имеет существенные различия. Выключенный компьютер / ноутбук не сможет предоставить те данные, которые можно получить с работающего включенного устройства.

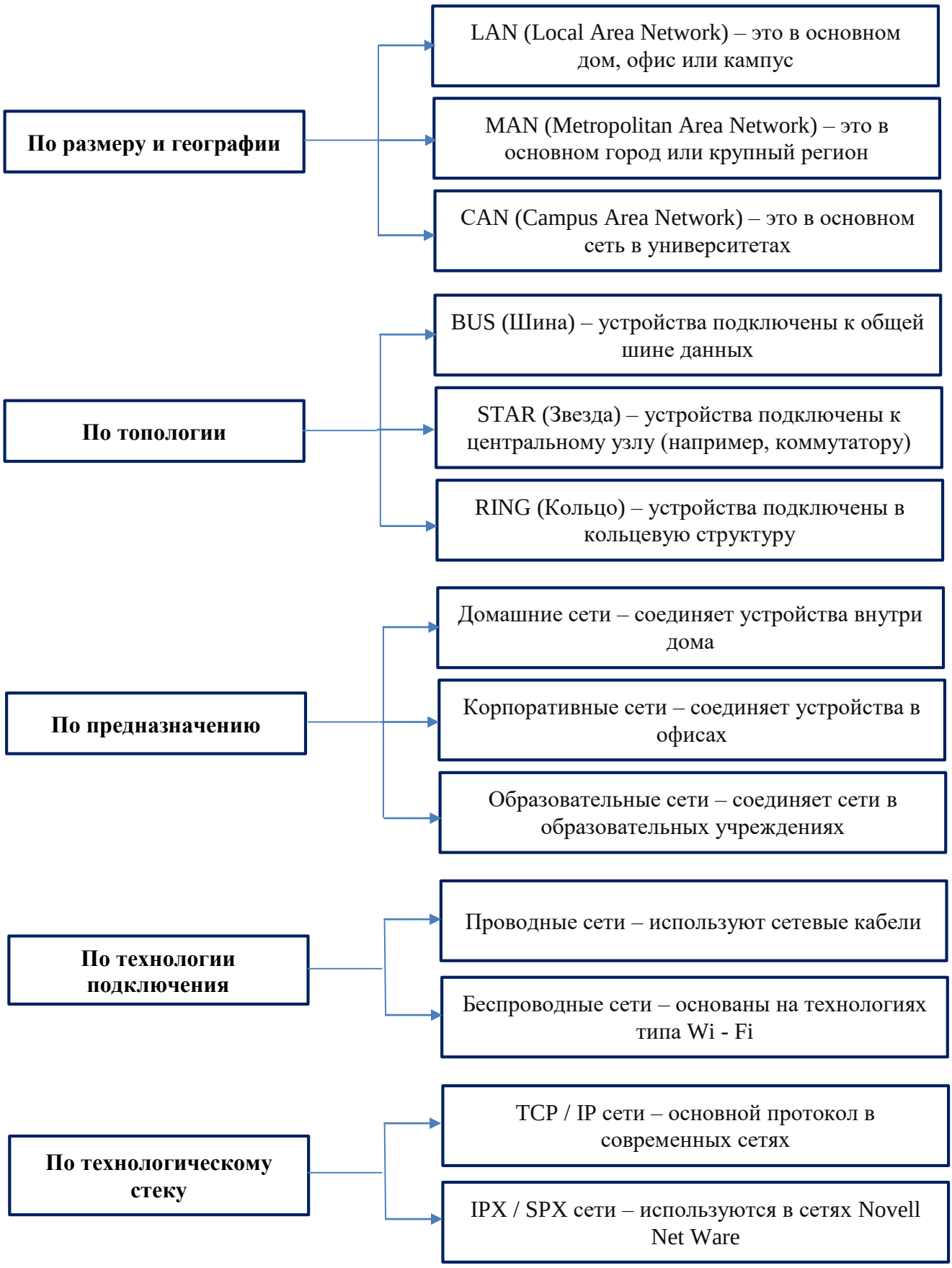
Важно! При включенном компьютере или ноутбуке необходимо обеспечить его бесперебойное питание с целью получения всех электронных доказательств, хранящихся на устройстве.

4) Имеется ли там локальная сеть?

Локальная сеть – это компьютерная сеть, позволяющая обмениваться данными между компьютерами и другими устройствами в пределах определенной территории, а также получать доступ к общим ресурсам *(например, принтерам, серверам и т.д.)*.

Устройства в локальной сети могут быть подключены к централизованному коммутатору или маршрутизатору, которые управляют передачей данных и обеспечивают связь между устройствами внутри сети, а также с внешними сетями.

Локальные сети могут быть классифицированы по различным критериям в зависимости от размера, топологии, технологии и других параметров.

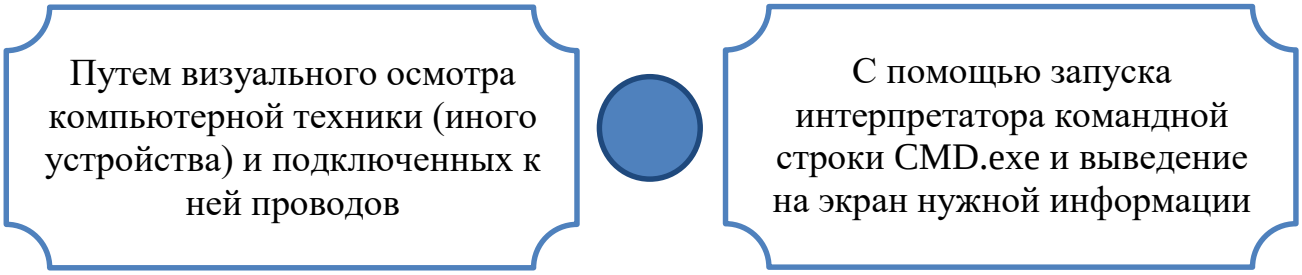


Локальные сети является важным компонентом современных информационных систем.

Для чего это необходимо? Для того, чтобы установить все устройства, подключенные к локальной сети. Бывают случаи, когда к устройству потерпевшего или преступника, подключены другие устройства, находящиеся далеко от осмотра места преступления. Иногда даже вне юрисдикции той страны, где произошло преступление.

Важно! Игнорирование данного факта может привести к тому, что на компьютер потерпевшего или преступника может воздействовать сам преступник или его сообщники, удаленно блокируя устройство или уничтожая важную информацию (следы преступления).

Подключено ли устройство *(компьютер, ноутбук, планшет, сотовый телефон и т.д.)* к локальной сети можно выяснить 2 способами.



Важно! При визуальном осмотре и других действиях с компьютерной техникой соблюдать меры предосторожности: изолировать посторонних людей с осматриваемого помещения, работать только при помощи собственного оборудования.

Для более точного определения всех подключенных устройств применяются сразу 2 вышеуказанных способа.

После этого компьютер или другое устройство отключают от локальной сети, для исключения воздействия на них с целью уничтожения электронных доказательств совершения уголовного правонарушения.

Важно! Если при работе с компьютером потерпевшего или подозреваемого установите факт воздействия на изучаемую информацию, необходимо принять меры к ее сохранению, в том числе путем немедленного отключения локальной сети от осматриваемого устройства.

В случае нахождения на месте преступления несколько компьютеров, соединенных сетью, в первую очередь устанавливают основной компьютер, управляющий всеми устройствами в сети. Его называют сервером *(на нем содержится важная информация обо всех действиях, совершаемых на рабочих станциях, подключенных к компьютерной сети)*.

Сервер – это сетевой компьютер, задача которого обрабатывать запросы других устройств, подключенных к сети. В отличии от обычного компьютера *(рабочей станции)* он обладает собственным процессором, оперативной и долговременной памятью[10].

[10] https://blog.skillfactory.ru/glossary/server/#:~:text=Сервер%20(от%20англ.%20server%20—,программное%20обеспечение%2C%20обрабатывающее%20пользовательские%20запросы

Различают 4 типа разновидностей серверов.

Осмотр должен начинаться с сервера, где следователь, криминалист или судебный эксперт должен изучить:

- журналы системных событий *(логи)*, где обычно содержатся информация о действиях пользователя компьютерной системы, доступе к системе, изменениях в системе и других активностях, указывающих на незаконные действия;
- файлы и метаданные, связанные с незаконными действиями *(например, вредоносное ПО, украденные данные или иная информация, представляющая интерес для следствия)*;
- историю браузера и онлайн активность, где можно установить интернет – ресурсы, посещаемые подозреваемым или потерпевшим, загруженные файлы и другие действия пользователя в интернете;
- метаданные файлов и временные штампы, указывающие на время создания, изменения или удаления файлов, что играет большую роль в реконструкции событий или определении участников преступления;

- сетевую активность, с помощью которой можно обнаружить незаконные действия, происходящие в сети;

- удаленный доступ и аутентификацию, позволяющую получить данные о несанкционированном доступе к серверу;

- возможные скрытые разделы или файлы, которые могут содержать важную информацию о незаконной деятельности;

- файлы реестра, предоставляющие информацию о системных настройках, установленном программном обеспечении и выполненных операциях;

- удаленные и временные файлы, содержащие информацию о временных операциях, включая удаленных файлах, которые могут свидетельствовать о незаконной деятельности.

После этого, следователь или криминалист могут приступить к изучению остальных рабочих станций *(устройств)* в сети. По возможности компьютеры должны быть осмотрены сразу одновременно.

Осмотру подлежат фотографии, которые находятся в папках или как отдельные файлы на рабочем столе, компьютерные программы, установленные или уделенные.

В случае выявления программ уничтожения информации или ее шифровки, необходимо принять меры сохранению имеющихся на компьютере данных путем приостановления или предотвращения запуска таких программ.

Важно! Все действия должен производить следователь, оперативный сотрудник или эксперт, обладающий достаточным объемом знаний для проведения данного следственного действия! Любые не профессиональные действия могут повлечь безвозвратное уничтожение электронных доказательств!

В целях исключения уничтожения вещественных доказательств осмотр рабочих станций должен быть произведен при помощи специального криминалистического оборудования без использования манипулятора и клавиатуры осматриваемой техники.

Также обращать внимание нужно и на бумаги, а точнее на записи, которые находятся возле компьютеров. Это могут быть пароли от входа в систему, электронной почты или криптоконтейнеров, установленных на устройстве и т.д.

Все следственные действия, выполняемые следователем с компьютерной техникой, должны быть отражены в протоколе осмотра и зафиксированы фото /видеосъемкой.

В рамках данного процесса осуществляется захват изображений экрана компьютерного монитора с целью создания фотографий или скриншотов, где четко фиксируются информационные данные, включая дату и время, активные программы либо программы, предварительно запущенные на вычислительной системе, открытые текстовые и PDF-файлы, а также изображения и фотографии.

Важно! Перед тем как закрыть или свернуть текстовый файл, необходимо убедится в его сохранении на жестком диске или внешнем носителе сотрудника, производящего осмотр!

Для установления программ, запущенных на компьютере, можно выполнить одно из следующих действий:

а) открыть диспетчер задач путем одновременного нажатия клавиш Ctrl + Alt + Delete и перейти на вкладку «Процессы», где в одном из столбцов можно увидеть текущие запущенные программы.

б) посмотреть на рабочую панель компьютера и путем наведения курсора мышки увидеть названия запущенных программ *(они располагаются слева направо)*.

Важное значение при осмотре компьютерной техники имеет установление информации, содержащей: электронные доказательства совершенного преступления и пароли от учетных записей, социальных сетей, почтовых сервисов.

Данные сведения могут быть получены путем исследования содержимого дисков и рабочего стола компьютера, содержащих различную информацию.

Важно! Перед тем как работать с дисками компьютера (внутренними или внешними) необходимо снять их образ и работать уже исключительно с копиями, чтобы не допустить внесение изменений на диск. Не выполнение данного действия может повлечь признание доказательств, содержащихся на электронном носителе не допустимыми!

Вопросы для самоконтроля:

1) Какие цели преследует осмотр места компьютерного преступления?

2) Из каких этапов состоит осмотр места происшествия (преступления)?

3) Что включает в себя подготовительный этап осмотра места происшествия (преступления)?

4) Что включает в себя рабочий (исследовательский) этап осмотра места происшествия (преступления)?

5) Что включает в себя заключительный этап осмотра места происшествия (преступления)?

6) Опишите порядок осмотра компьютерной техники.

2.2. Поиск, обнаружение и изъятие электронных доказательств.

В ходе расследования преступлений, совершенных с использованием компьютерной техники и *(или)* другого оборудования *(устройств)* особое значение играют электронные доказательства, которые хранятся в компьютерной системе, сети и сети интернет.

Следователь *(криминалист)* должен знать и понимать, что из себя они представляют, где именно они находятся и как их можно получить.

Если при расследовании обычных традиционных преступлений, орган уголовного преследования понимает, где и как он может получить

доказательства, то по преступлениям данной категории без определенных знаний и навыков, иногда даже технических, процесс обнаружения и изъятия электронных доказательств вызывает особые затруднения.

Что представляют собой электронные доказательства?

Электронные доказательства – это любые данные, которые были созданы, переданы, получены или хранятся в электронном формате и могут служить для подтверждения или опровержения фактов в правовом контексте.

К ним могут относиться: электронные сообщения, метаданные файлов, веб-сайты, фотографии, видеозаписи, журналы системных событий, записи телефонных звонков, данные социальных сетей, а также иная цифровая информация.

Особенностью электронных доказательств и главной их отличительной чертой от традиционных, является их **неустойчивость.** Это означает, что они могут измениться в определенный момент времени под воздействием компьютерных программ или при взаимодействии с ними сторонними пользователями.

В связи с этим важную роль в расследовании таких преступлений играют оперативность и осторожность для обеспечения сохранности и целостности электронных доказательств.

Важно! Работать необходимо исключительно с копиями электронных доказательств, которые можно получить с помощью специализированных устройств или программного обеспечения, позволяющие без внесения изменений в систему получать копии необходимых данных.

К таким устройствам относятся блокираторы записи, которые предотвращают запись данных на образ памяти при его снятии.

Аппаратный блокиратор записи

Основная их функция – защита целостности информации в процессе снятия образа памяти. То есть, предотвращают любые попытки записи на оригинальный носитель данных.

Они бывают программными и аппаратными. Ярким примером программного блокиратора записи является право доступа в операционную систему устройства.

Аппаратные блокираторы записи – это физические устройства или компоненты, предназначенные для ограничения возможности записи или изменения данных в компьютерных системах.

Ниже представлены некоторые примеры аппаратных блокираторов записи:

1) физические переключатели (Write-Protect Switches) - устанавливаются на устройствах хранения данных (флеш-накопители, карты памяти, жесткие диски);

2) контроллеры доступа (Data Access Controllers) – работают на уровне интерфейса между устройствами хранения данных и компьютерной системой (блокируют запись на основе заданных параметров или разрешают ее только определенным пользователям);

3) защищенные USB-накопители – имеют встроенный механизм защиты данных (могут включать аппаратное шифрование данных, биометрическую аутентификацию, функцию блокировки записи);

4) специализированные аппаратные модули безопасности – физические устройства, предназначенные для обеспечения безопасности и защиты криптографических ключей и операций.

Электронные доказательства должны соответствовать следующим критериям:

При работе с электронными доказательствами придерживаются следующих принципов:

1. *Принцип целостности данных предписывает, чтобы действия специалиста не приводили к физическим изменениям данных, электронных устройств или носителей информации, которые могут служить в качестве юридически значимых доказательств.*

2. *Принцип документирования процесса предполагает, что любые действия, связанные с электронными доказательствами, должны быть документированы, и эти документы должны быть сохранены для возможной проверки, чтобы независимая сторона могла повторить эти действия и получить аналогичные результаты. Это также включает подробное описание процессов обыска и конфискации, условий хранения и передвижения электронных данных.*

3. *Принцип законности подразумевает, что лица и органы, занимающиеся сбором и обработкой электронных доказательств, обязаны соблюдать законы и правила, регулирующие сбор, анализ и использование таких доказательств.*

4. *Принцип надлежащей подготовки предусматривает, что осмотр места преступления и изъятие доказательств должны проводиться только после тщательной подготовки и квалифицированными специалистами, обладающими необходимым уровнем знаний и навыков для обнаружения, сбора и обработки цифровых доказательств с соблюдением установленных стандартов.*

Поиск электронных доказательств.

Первичный осмотр компьютерной техники потерпевшего и обыск у подозреваемого должны осуществляться квалифицированными сотрудниками органа уголовного преследования или привлекаемыми ими IT-специалистами, которые умеют обращаться с электронными доказательствами.

Так как любые неквалифицированные действия могут привести к безвозвратной их утере либо признания их недопустимыми в качестве доказательств.

В зависимости от вида преступления, электронные доказательства могут храниться на самом устройстве, в компьютерной системе или сети, а также интернете.

Компьютерная система – это комплекс аппаратных средств *(устройства ввода, вывода и хранения информации)* и программных компонентов *(системные и прикладные программы)*, предназначенных для обработки информации и решения различных вычислительных задач. К ней относятся как отдельные персональные компьютеры, так и серверы, мейнфреймы, кластеры и другие типы компьютеров, выполняющие разные функции и масштабы задач.

Устройства ввода информации – это периферийные устройства, которые используются для ввода данных и команд в компьютер или другие электронные устройства.

Клавиатура – устройство, которое позволяет пользователям вводить текст и команды нажатием клавиш с символами и специальных функциональных клавиш.

Мышь – устройство управления, которое позволяет пользователям перемещать указатель по экрану и взаимодействовать с объектами на экране, щелкая и перемещая указатель мыши.

Графический планшет – устройство, которое позволяет пользователям вводить рукописный ввод или графические изображения с помощью специального стилуса или ручки и записывать рисунки или рукописный текст.

Сенсорные экраны – устройства, которые позволяют пользователям взаимодействовать с компьютером или устройством, прикасаясь к поверхности экрана, обычно пальцами или стилусом.

Сканеры – устройства, используемые для преобразования физических документов или изображений в цифровой формат, которые затем могут быть обработаны на компьютере.

Цифровые фотоаппараты – устройства, используемые для съемки фотографий и видео, которые можно загрузить на компьютер для редактирования, обработки или совместного использования.

Микрофоны – устройства, используемые для записи звука, который может быть преобразован в цифровой формат и обработан на компьютере.

Считыватели штрих-кодов – устройства, используемые для сканирования и считывания штрих-кодов, содержащих информацию о чем-либо.

Устройства вывода информации – это устройства, которые используются для отображения или вывода информации пользователю в удобном и читаемом формате.

Мониторы – устройства вывода, используемые для отображения графической, текстовой и видеоинформации на экране. Существует много типов мониторов, включая жидкокристаллические мониторы, светодиодные мониторы, OLED-мониторы и другие

Принтеры – позволяют создавать физические копии документов, фотографий и другой информации, хранящейся в электронном виде. Существует много типов принтеров, таких как лазерные, струйные, матричные и т.д., каждый со своими уникальными функциями и областями применения.

Проекторы – используются для проецирования изображений и видео на большие экраны, стены или другие поверхности. Они широко используются на презентациях, в аудиториях и кинотеатрах, а также в домашних кинотеатрах

Аудиоустройства – включает динамики, наушники и другие устройства, используемые для воспроизведения звука. Они могут быть встроены в устройство или подключены к нему через различные интерфейсы.

Устройства хранения информации – это физические или электронные устройства, предназначенные для хранения различных данных.

Жесткие диски (HDD) – это устройства на магнитных дисках для хранения данных. Они имеют большие объемы памяти и часто используются в настольных компьютерах и серверах.

Твердотельные накопители (SSD) – это твердотельные накопители хранения данных, обеспечивающие высокую скорость чтения и записи. Они часто используются в ноутбуках, смартфонах и планшетах.

USB-накопители – это портативные устройства хранения данных (флэш-накопители), которые позволяют передавать и хранить данные между различными устройствами. Они удобны и просты в использовании.

Оптические диски – это устройства для хранения мультимедийных данных. К ним относятся: компакт-диски (CD), DVD-диски и Blu-

Облачное хранилище – это хранение данных на удаленных серверах через Интернет. Популярные облачные сервисы включают Google Диск, Dropbox, Amazon S3 и т.д.

Сетевое хранилище (NAS) – устройства NAS, которые позволяют создавать сетевые хранилища для обмена данными между различными устройствами в домашних или офисных сетях.

Магнитные ленты – менее популярные устройства, которые используются для долгосрочного архивирования больших объемов данных.

Внешние жесткие диски – это устройства, которые подключаются к компьютерам через порты USB или e-SATA, используются для резервного копирования данных или расширения хранилища.

Кроме вышеуказанных устройств, электронные доказательства могут храниться в оперативной памяти (ОЗУ) компьютера, ноутбука, планшета, мобильного телефона и т.д. Она важная составная часть, отвечающая за временное хранение информации и программ, которые в данный момент запущены и работают.

Оперативная память RAM (Random Access Memory), является одним из основных типов памяти в компьютерах. Оперативная память выполняет ряд важных функций, связанных с обработкой данных и выполнением программ.

В ней откладываются сведения о запущенных на компьютере приложениях и об операционной системе, о последних действиях пользователя, в том числе загруженных и удаленных программах.

Она обеспечивает высокоскоростной доступ пользователя к данным, позволяя компьютеру выполнять операции быстро и эффективно.

Различают несколько разновидностей оперативной памяти.

СТАТИЧЕСКАЯ	ДИНАМИЧЕСКАЯ	ГРАФИЧЕСКАЯ
SRAM – работает быстрее и энергоэффективнее, но менее емкий и более дорогой, чем DRAM. использует бистабильные ячейки для хранения данных и не требует постоянного обновления	DRAM - работает медленнее, чем другие типы памяти, но обычно имеет большую емкость. Он использует конденсаторы для хранения данных и требует постоянного обновления информации для их сохранения	VRAM - обеспечивает высокую пропускную способность и производительность при обработке видео и графики. специально разработан для хранения графических данных, используемых видеокартами.

Оперативная память RAM – это энергозависимая часть системы компьютерной памяти. Это означает, что информация в ней хранится временно до тех пор, пока устройство *(компьютер, ноутбук и т.д.)* работает, то есть подключено питание.

Важно! Перед выключением компьютера всегда снимайте образ оперативной памяти!

Если следователь *(оперативный сотрудник, эксперт)* перед тем, как отключить компьютер не примет меры по сохранению данных, хранящихся в ОЗУ, не снимет образ оперативной памяти, он может навсегда потерять важную для расследования информацию:

- *последние сообщения, отправленные подозреваемым через интернет (например, социальные сети или электронную почту);*
- *пароли от учетных записей или аккаунтов социальных сетей;*
- *ключи от криптоконтейнеров, где возможно будет храниться информация (фотографии, документы, другие данные) о незаконных действиях подозреваемого;*
- *комментарии, оставленные на форумах, информация, переданная с помощью программ мгновенного обмена сообщениями или с использованием чатов, встроенных в электронные игры;*
- *информация о последних скачанных файлах, об открытых сетевых соединениях и т.д.*

Также ОЗУ может сохранять страницы и изображения с веб-сайтов *(даже если в браузере включен режим защиты приватности, отключены кеш и сохранение истории посещений сайтов)*.

Снятие образа оперативной памяти или как иногда говорят «дампа памяти» *(RAM-damp)* обязательно необходимо выполнять перед началом исследования содержимого рабочей станции (компьютера) и до отключения ее от питания.

Для снятия образа оперативной памяти имеется множество различных программных продуктов, работающих в разных операционных системах. Одни из них платные, другие бесплатные. Ниже представлены наиболее распространённые программы для получения дампа памяти.

MemDump – это утилита командной строки, используемая для создания образа оперативной памяти в системах Windows. Это позволяет Вам создавать дампы памяти процесса и сохранять их для последующего анализа.

FTK Imager – эта программа широко используется в цифровой криминалистике для получения изображений различных типов данных, включая изображения оперативной памяти. Он предоставляет удобный интерфейс для получения изображений оперативной памяти и их последующего анализа.

Volatility – это популярный фреймворк для анализа виртуальной памяти в цифровой криминалистике. Его можно использовать для получения изображений оперативной памяти и последующего анализа содержимого, такого как процессы, сетевые подключения, открытые файлы и другие важные данные.

Magnet RAM Capture – это программное обеспечение, предназначенное для захвата изображений оперативной памяти с компьютеров под управлением операционных систем Windows. Это позволяет анализировать память для выявления потенциальных угроз и собирать ценную информацию для цифровой криминалистики.

WinDbg – это мощный инструмент отладки от Microsoft, который можно использовать для получения дампов памяти, включая полные дампы памяти, мини-дампы и дампы ядра.

Belkasoft RAM Capturer – это небольшой инструмент судебной экспертизы, предназначенный для надежного извлечения всех данных из энергозависимой части системы памяти компьютера.
(условно бесплатная)

Разберем пример захвата образа оперативной памяти на примере утилиты **«Belkasoft Live RAM Capturer».** Данное программное обеспечение разработано с учетом потребностей криминалистов, специалистов по информационной безопасности. С помощью данной утилиты можно получить копию содержимого оперативной памяти в обход механизмов активной защиты, таких как **nProtect Game Guard**, используя привилегированный режим ядра операционной системы.

В составе «Belkasoft Live RAM Capturer» предусмотрены как 32-битная, так и 64-битная версии драйвера для операционной системы Windows, что дает возможность работе программы в привилегированном режиме ядра операционной системы[11].

Для захвата дампа оперативной памяти с помощью программы «Belkasoft Live RAM Capturer» необходимо скачать ее с официального сайта разработчика - https://belkasoft.com/ru/ram-capturer *(установка программы достаточно проста и не отличается от установки других программ)*. Далее Вам нужно запустить программу от имени администратора и нажать кнопку «Пуск». Программа начнет сканирование системы и создаст дамп оперативной памяти в формате - **.mem.** По умолчанию дамп оперативной памяти сохраняется в папку, где находится сама программа, однако вы можете указать и другую папку для сохранения. Чтобы указать путь для сохранения дампа, выберите вкладку «Настройки» и укажите путь в соответствующем поле. Размер дампа

[11] Belkasoft RAM Capturer скачать бесплатно (software4pc.ru)

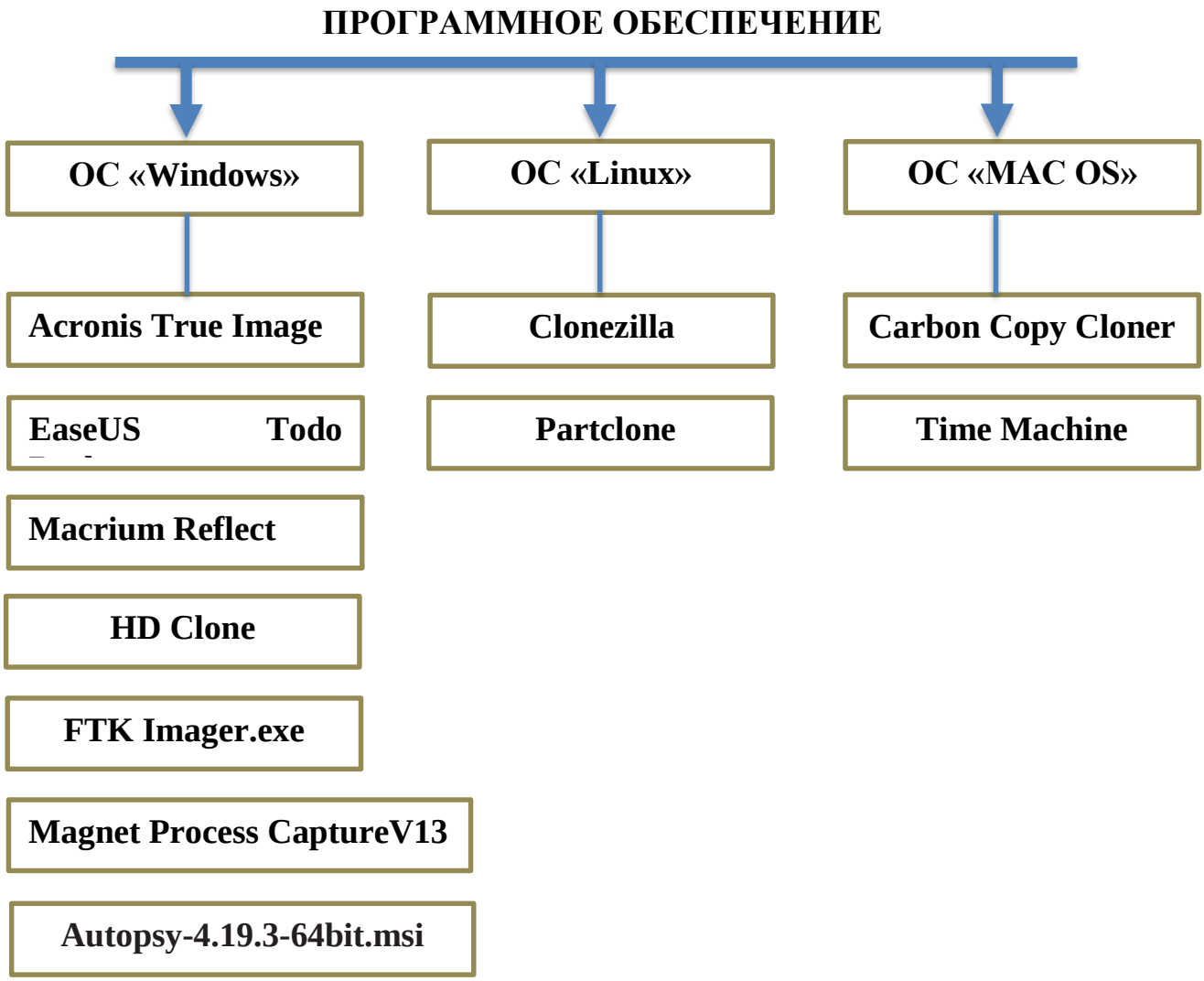
оперативной памяти по умолчанию составляет 512 МБ *(есть возможность увеличить размер вручную)*[12].

После того, как Вы создали дамп оперативной памяти, можно переходить к поиску других электронных доказательств, находящихся в рабочей станции *(компьютере)*.

Важно! Нельзя работать на компьютере подозреваемого, пользоваться его клавиатурой, манипулятором (мышью) с целью исключения потери электронных доказательств!

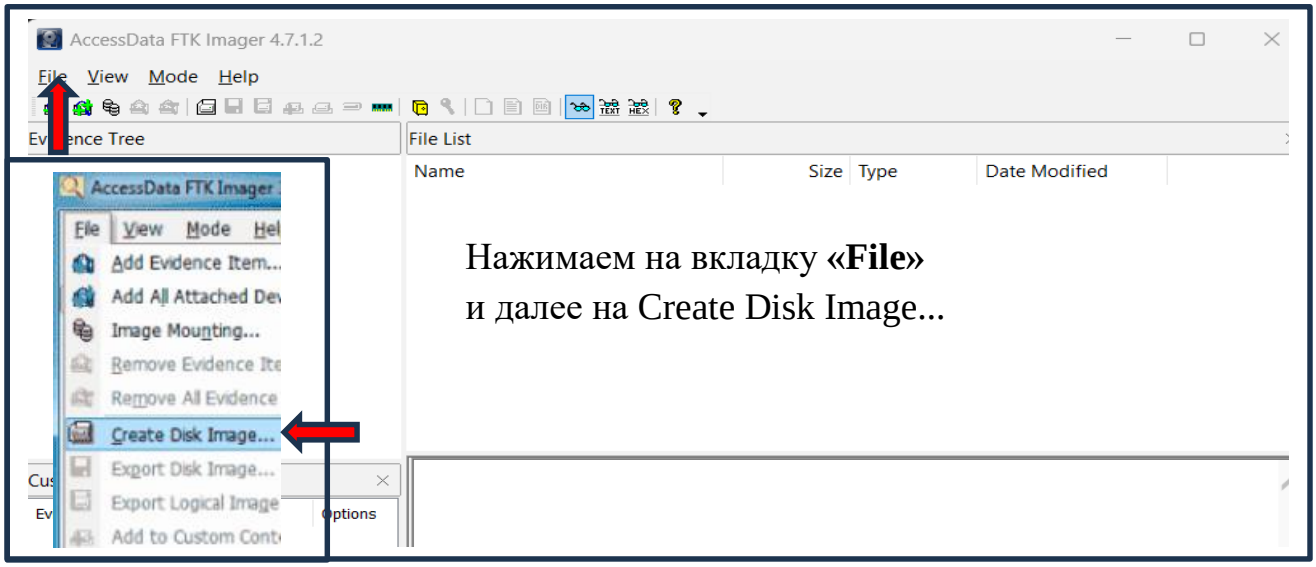
В зависимости от типа операционной системы *(Microsoft Windows, Unix, Linux, Mac OS)* выбирается соответствующая программа для снятия образа жесткого диска с целью последующей работы с ним на предмет поиска цифровых следов преступления.

Существует огромное количество различного программного обеспечения, предназначенного для снятия образа жесткого диска. Выбор зависит от поставленной задачи перед следователем, его возможностей и используемой им операционной системы.

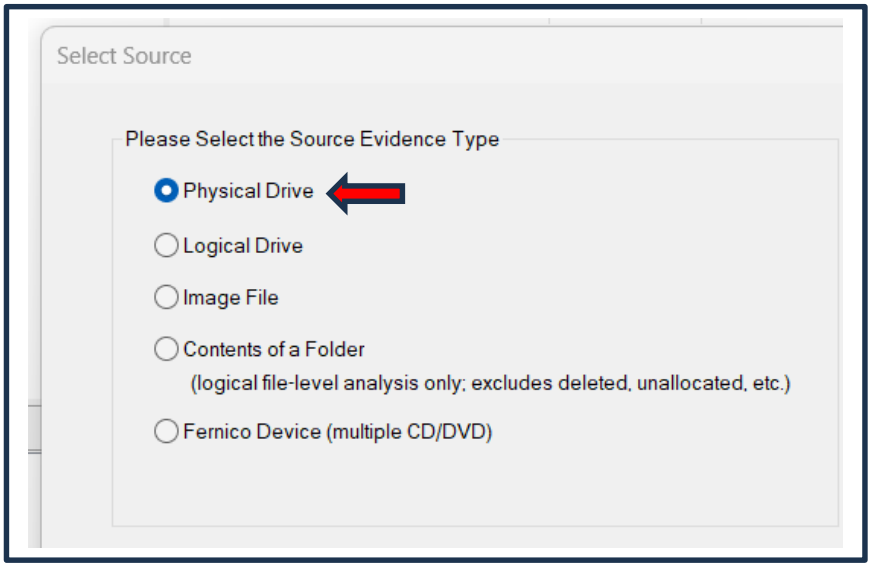


[12] Практические советы по использованию Belkasoft Live RAM Capturer для эффективного создания дампа оперативной памяти в формате .mem (anyquestion.info)

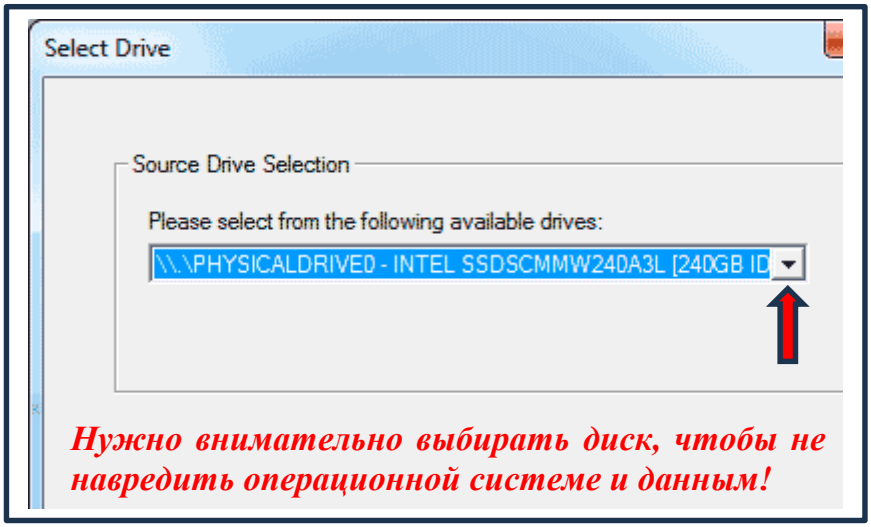
Разберем пример снятия образа жесткого диска с помощью программы **FTK Imager.exe.** Для начала скачаем данное программное обеспечение с официального сайта - [Exterro-E-Discovery&Information Governance Software](). После чего устанавливаем программу на компьютер, следуя инструкциям. По завершению кликаем по ярлыку программы и запускаем ее.



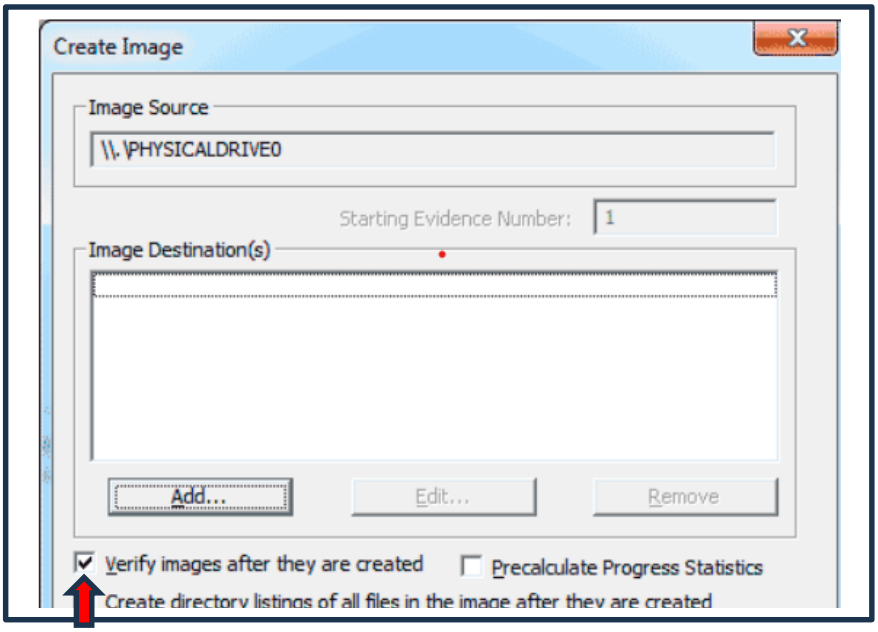
Нажимаем на вкладку **«File»**
и далее на Create Disk Image...



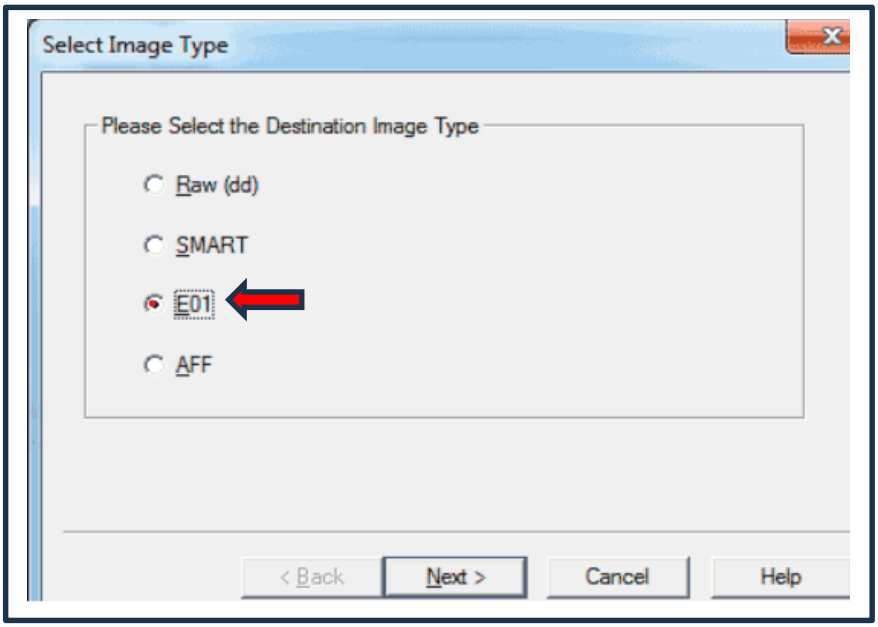
Ставим галочку на
«Physical Drive»



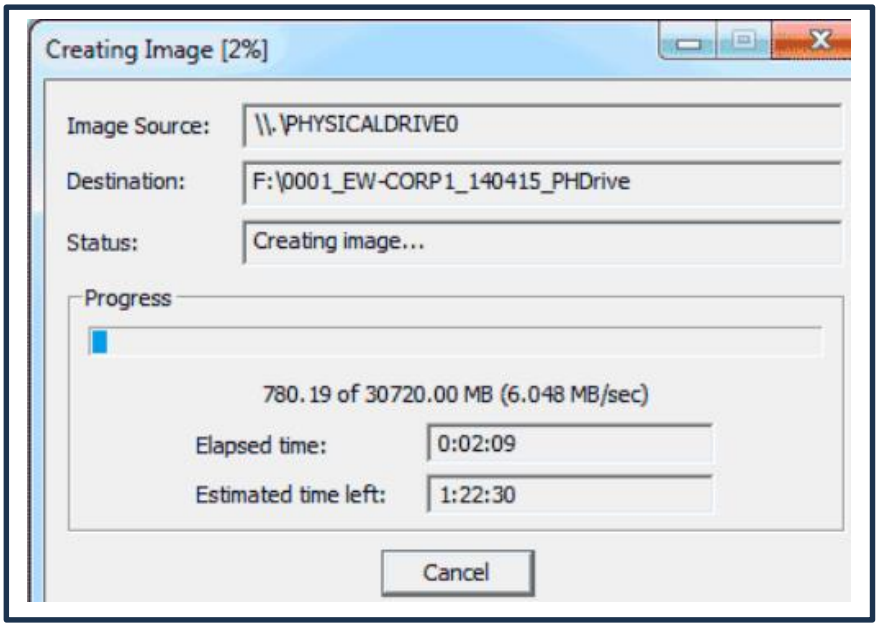
В открывшемся окне
выбираем наш
исследуемый диск



После чего необходимо поставить галочку на вкладке «Верификация»



Выбираем тип файла, например, E01 и нажимаем «Next»



Ждем завершения процесса создания образа нашего исследуемого диска

Важно! Нельзя работать с оригиналами дисков, чтобы случайным образом не внести изменения в них и признания электронных доказательств не допустимыми!

После того, как следователь сделает образы оперативной памяти (ОЗУ) и жесткого диска, можно просмотреть содержимое рабочей станции *(компьютера)*.

При просмотре необходимо обращать внимание на любые подозрительные файлы. Например, на фотографии, которые сохранены в документе WORD вместо обычного формата, предназначенного для фото и картинок JPEG.

Одним из способов маскировки логина и пароля является именно такая форма сохранения фотографий или рисунков. Обнаруженные данные для авторизации могут быть ключами к зашифрованным контейнерам, в том числе криптоконтейнерам, аккаунтам почтовых сервисов, социальных сетей и т.д.

При просмотре компьютера необходимо обращать внимание на все открытые и ранее открывавшиеся приложения, документы, аудио / видеофайлы.

Электронные доказательства можно обнаружить в истории браузера.

Браузер – это программное обеспечение, позволяющее просматривать веб-страницы в интернете, сохранять их, осуществлять поиск необходимой информации, запоминать пароли и т.д.

Просмотр истории браузера, как на компьютере потерпевшего, так и подозреваемого позволит собрать следующую информацию *(при условии, что она не была удалена или не включена функция «не сохранять историю»)*:

- какие веб-сайты посещал пользователь, какие из них сохранены в закладках;
- о его предпочтениях, данные авторизации *(файлы «Cookie»)*;
- сведения о сохраненных паролях;
- какие запросы делал пользователь в поисковых системах;
- данные, которые вводил пользователь в формах на отдельных веб-страницах, где такие условия предусмотрены;

- сведения о расширениях браузера, их активности и взаимодействии с веб-сайтами.

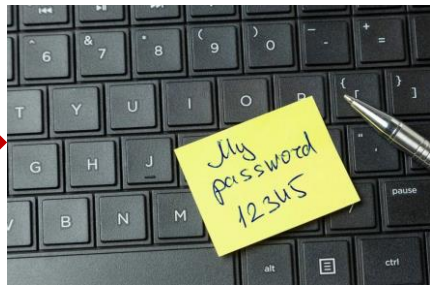
Существует более 50 различных браузеров. Самыми распространенными из них являются: Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, Opera, Brave, Vivaldi, Tor Browser, Microsoft Internet Explorer.

Электронные доказательства можно также обнаружить в почтовых сервисах, социальных сетях, мессенджерах.

Следы преступления или доказательства можно найти не только в самом компьютере, но и на системном блоке, мониторе, клавиатуре или под клавиатурой, манипуляторе (мыши), а также кабельных соединениях, периферийных устройствах, флэш-носителях, выносных жёстких дисках, модемах и прочих устройствах.

Например, небольшие заметки на листочках с указанием логина или пароля, номера телефона или анкетные данные, которые будут иметь значение при установлении участников преступления или получения дополнительных доказательств.

Иногда пароли пишут на соединительных кабелях, модемах, флеш-носителях, дисках, на манипуляторе *(мыши)*, клавиатуре или под ними, под монитором или на его задней стенке, на процессоре или внутри него, сетевом фильтре, под столом или стулом *(креслом)*, на стене, двери, настольной лампе и т.д.



Поэтому осмотру подлежат все вышеуказанные вещи и предметы, видимые и скрытые, обнаруженные при производстве следственного действия.

На месте преступления могут находиться дополнительные комплектующие, подсоединяемые к рабочей станции *(компьютеру, ноутбуку)*. Например, роутеры, концентраторы, коммутаторы.

Коммутатор – это устройство, позволяющее объединять множество различных устройств (например, компьютеры, принтеры, серверы, МФУ и др.) в одну общую локальную сеть, позволяя ее пользователям обмениваться информацией.

Роутер или маршрутизатор – это устройство, принимающее сетевой сигнал от провайдера (поставщика интернет-услуг) и передающее его всем другим устройствам в сети.

Концентратор – это устройство, позволяющее объединять несколько компьютерных сетевых узлов в одном или нескольких сегментах сети. Он выполняет функцию ретранслятора сигнала, копируя и передавая данные с одного узла на другой. В отличие от коммутатора концентратор не анализирует содержимое пакетов или их заголовки, а просто передает их всем подключенным узлам.

Внутри данных сетевых устройств хранятся электронные доказательства, совершенного преступления, которые можно обнаружить при просмотре:

- журналов сетевого трафика *(содержат информацию о передаче данных между устройствами и серверами)*;
- журналов подключения *(отражаются сведения о датах, метках времени и используемых портах)*;
- адреса макетов устройств *(позволит идентифицировать устройства в сети по их физическим адресам)*;
- журнала DHCP *(предоставят информацию о присвоении IP-адресов устройствам в сети)*;
- таблицы ARP *(сохраняют список IP-адресов, используемых для идентификации устройств в сети и соответствующих им MAC-адресов)*;
- файлов конфигурации *(предоставят информацию о настройках устройства, включая маршрутизацию, фильтрацию и правила безопасности)*;
- журнала Firewall *(содержат сведения о заблокированных или авторизованных сетевых подключениях)*;
- системных журналов *(предоставят информацию о событиях на уровне операционной системы устройства)*.

Важно! Для работы с данными устройствами необходимо обладать соответствующей квалификацией или предоставить возможность выполнить все действия по поиску электронных доказательств IT-специалисту, имеющему соответствующий опыт работы в сфере цифровой криминалистики.

К примеру, подключаться к исследуемому роутеру *(маршрутизатору)* необходимо только при помощи собственного соответствующего оборудования, используя безопасные методы для предотвращения внесения изменений в данные устройства или их утраты.

Каждое действие следователя должно документироваться путем внесения записи в протокол осмотра, сопровождаться фото и видеосъемкой. Иногда требуется присутствие понятых для фиксации тех или иных действий следователя, криминалиста или IT-специалиста.

Электронные доказательства могут храниться также на CD или DVD дисках, флеш-носителях, съемных дисках, обнаруженных в ходе осмотра места преступления или обыска.

Обнаружение и изъятие электронных доказательств.

В криминалистике существует «Принцип обмена», сформулированный доктором Эдмоном Локаром. Он гласит следующим образом: «Каждый контакт оставляет след, при контакте между двумя объектами произойдет отмен», то есть преступник что-то принесет на место преступления и уйдет с чем-то оттуда[13].

Следуя данному принципу, можно предположить, что действия, которые происходят в информационно-коммуникационной среде, практически всегда оставляют цифровые следы. Преступник, совершая преступления с помощью современных технологий (компьютера, ноутбука, сотового телефона, интернета) вносит изменения в информационную систему, сети и данные. Задача следователя - знать где можно обнаружить данные цифровые следы, найти их и правильно изъять.

Цифровые следы или их еще называют цифровые отпечатки, найденные на месте преступления позволяют:

- *установить лиц, причастных к преступлению;*
- *воссоздать хронологию произошедших событий;*
- *выявить методы и тактики преступников.*

Отсюда следует, что обнаружение и изъятие электронных доказательств является важным этапом расследования киберпреступлений.

Цифровые отпечатки бывают двух видов: активные – данные, предоставляемые пользователем *(персональные данные, видео, аудио, изображение и т.д.)* и пассивные – данные, которые непреднамеренно оставляет пользователь в интернете *(к примеру, история просмотра в браузере)*[14].

Эти виды цифровых отпечатков могут быть использованы в качестве электронных доказательств, поэтому подлежат изъятию и приобщению к материалам уголовного дела.

Изъятие цифровых следов происходит следующим образом и состоит из нескольких этапов:

[13] https://translated.turbopages.org/proxy_u/en-ru.ru.3d94800f-656323c8-12a33e03-74722d776562/https/en.wikipedia.org/wiki/Locard%27s_exchange_principle#:~:text=В%20криминалистике%20принцип%20Локара%20гласит%2С,образом%3А%20"Каждый%20контакт%20оставляет%20след"

[14] https://www.unodc.org/e4j/ru/cybercrime/module-4/key-issues/digital-evidence.html

То есть, сначала создают образы оперативной памяти и жесткого диска, при необходимости создают образ ядра операционной системы, потом CD / DVD диска, внешнего жесткого и SSD диска, флеш-носителя и других карт памяти и после приступают к процессу изъятия информации, хранящихся в электронной почте, социальных сетях, мессенджерах.

Ядро операционной системы содержит информацию о происходящих в ней событиях – вход в систему, изменение файлов, установка программ и других активностях пользователя.

Каждый этап имеет свою последовательность, несоблюдение которой может привести к утрате отдельных видов электронных доказательств.

Важным условием использования в последующем изъятых электронных доказательств является их проверка на целостность, подлинность и достоверность. Это достигается путем вычисления криптографического значения хеш-суммы оригинала и копии электронных доказательств. Если они совпадают, то изъятая копия *(дубликат)* является зеркальным отражением оригинала и может быть использована в суде в качестве доказательств.

Для вычисления хеш-суммы существует множество различных программ, распространенными из которых являются:

1) HashMyFiles (для операционной системы «Windows»);

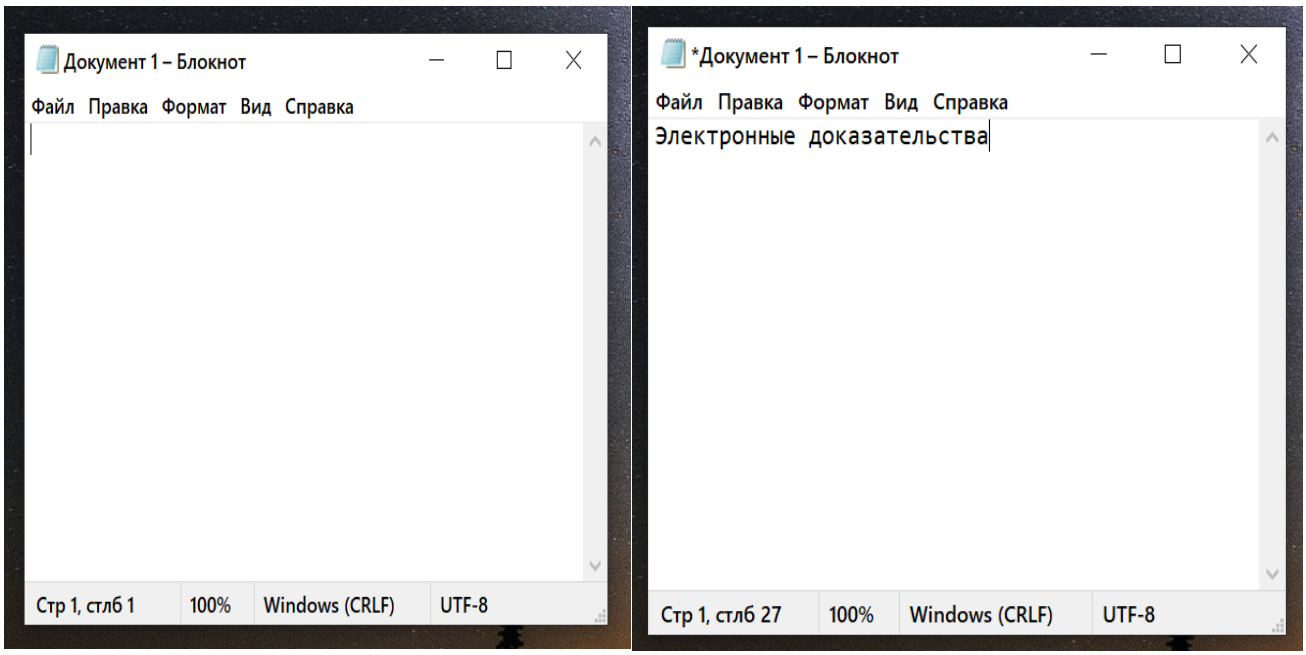
2) HashTab (для операционных систем «Windows» и «macOS»);

3) QuickHash (для операционных систем «Windows», «macOS» и «Linux»);

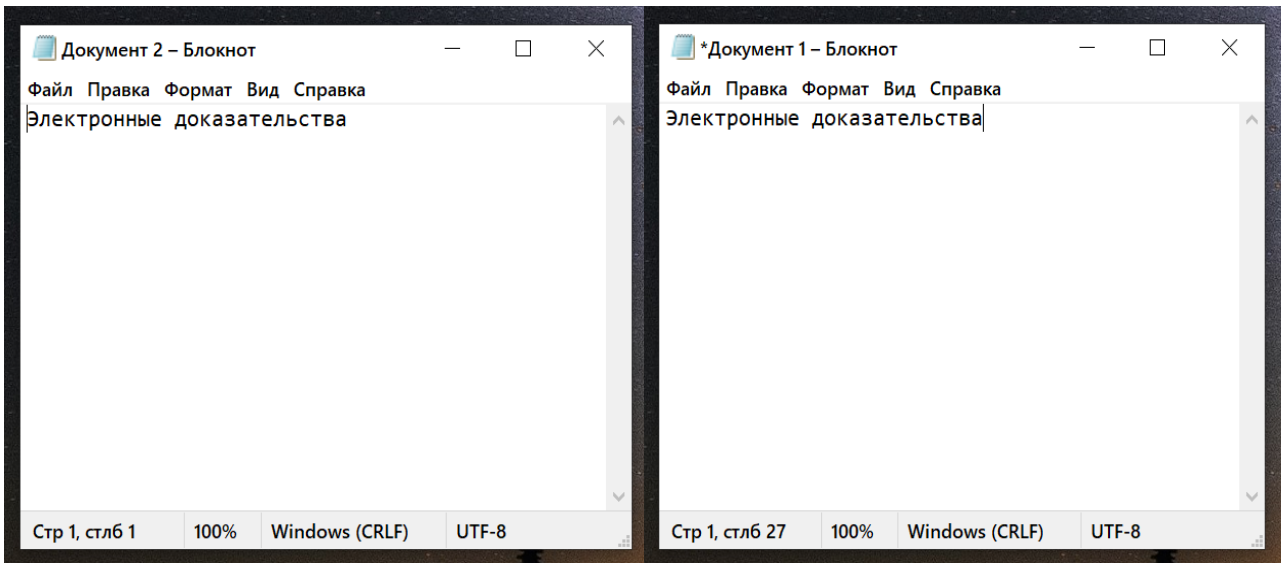
4) Whirlpool (для операционных систем «Unix» и «Linux»);

5) Blake2 (для операционных систем «Unix» и «Linux»).

Рассмотрим способ криптографического вычисления хеш - суммы с помощью программы **HashMyFiles**.

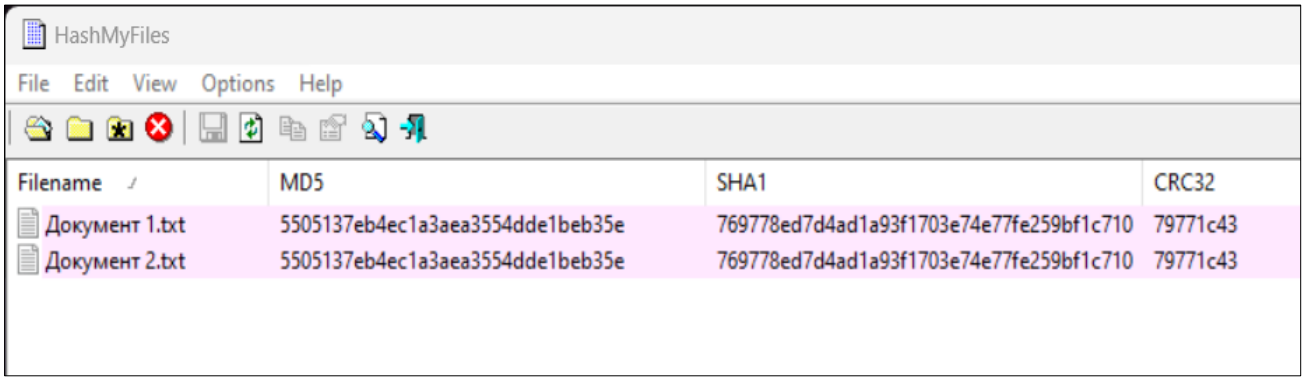


1) Создаем текстовый документ и пишем в нем слова «Электронные доказательства»;

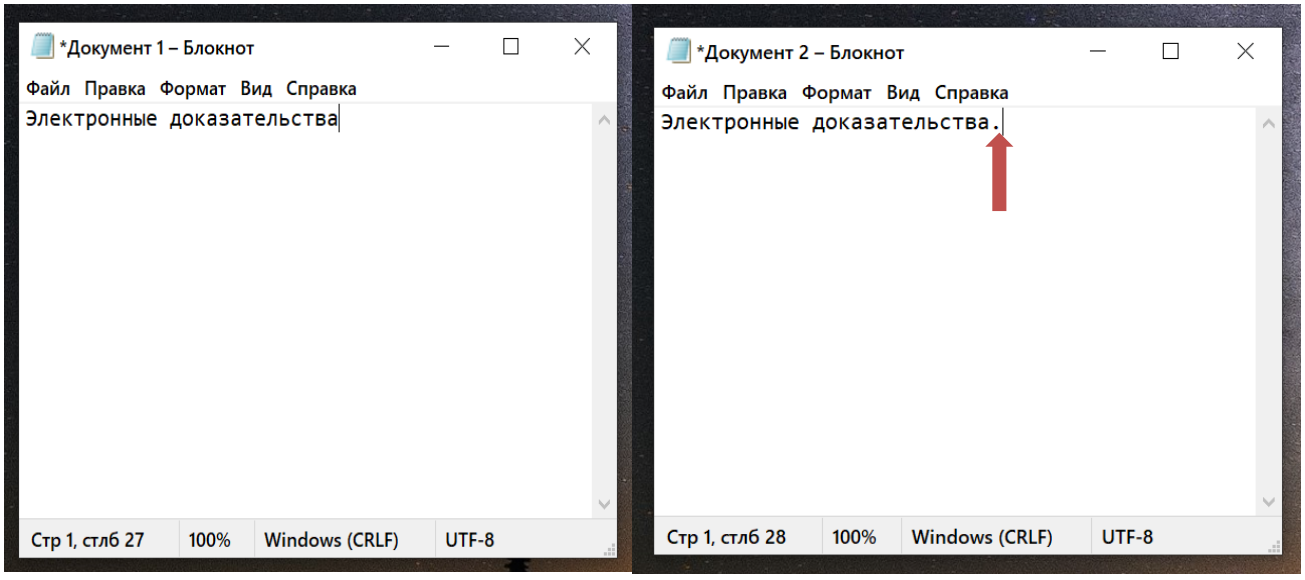


2) Делаем копию первого документа и открываем 2 файла *(должны убедиться, что эти 2 файла идентичны и записи в них одинаковы)*;

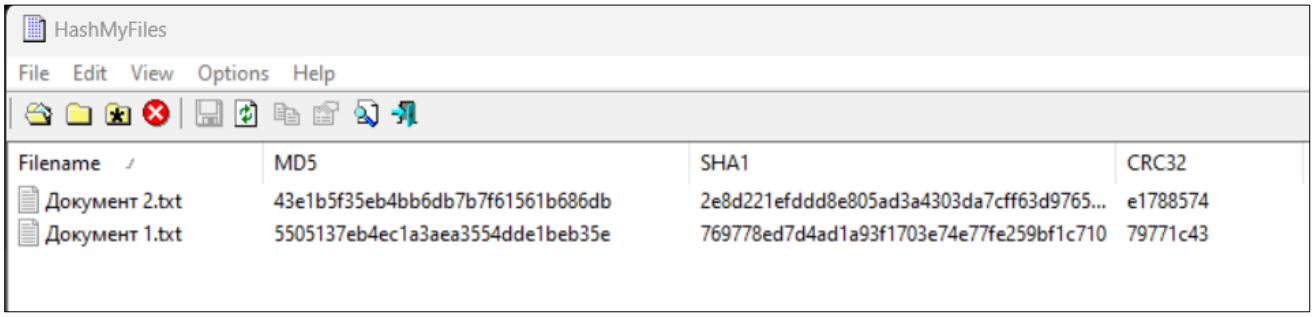
3) Запускаем программу **HashMyFiles** и переносим туда 2 файла *(должны убедиться, что хеш-суммы двух файлов идентичны)*;



4) Снова открываем созданный нами «Документ 2» и после слов «Электронные доказательства» ставим точку или запятую.



5) Снова запускаем программу **HashMyFiles** и переносим туда 2 файла *(теперь должны убедиться, что хеш-суммы двух файлов разные)*;



Этот пример наглядно показывает нам насколько файлы подвержены изменениям, которые следователь может допустить при несоблюдении основных требований в ходе изъятия электронных доказательств.

Однако, следует отметить, что вышеуказанный способ и процесс изъятия электронных доказательств с компьютеров, не применим к мобильным устройствам *(сотовым телефонам)*. Для них существует иной порядок и другое программное обеспечение.

После выполнения всех вышеуказанных действий изъятые электронные доказательства должны быть упакованы в специальные пакеты или контейнеры, исключающие несанкционированный доступ к ним.

Важно! Необходимо использовать антистатические пакеты для предотвращения статических разрядов, которые могут повлиять на электронные доказательства.

Изъятые компьютерная техника или сотовые телефоны *(смартфоны)* также должны быть упакованы в специальные антистатические пакеты и опечатаны таким образом, чтобы обеспечить их целостность и сохранность, а также исключить возможность несанкционированного доступа к ним, в том числе включение или выключение устройства.

Для дополнительной защиты от механических повреждений могут быть использованы картонные коробки, которые также опечатываются пломбой или лентой. На самой коробке или пакете указываются данные о месте, времени и сотруднике, который произвел изъятие, понятых, количестве и названии предмета. Также указываются сведения о лице, у которого изъято устройство. Если участвовали понятые, то они должны поставить подписи на опечатанных пакетах или коробках.

Если изъятию подлежит несколько компьютеров, то имеет смысл произвести маркировку каждого элемента: процессора, монитора, клавиатуры, соединительных кабелей и подключенных к ним устройств.

Сотовые телефоны могут быть помещены в пакет «Фарадея», а при его отсутствии в обычную алюминиевую фольгу в несколько слоев, чтобы исключить отправку и получение сообщений на данное устройство.

Важно! Все действия с вышеуказанными вещественными доказательствами должны быть произведены в условиях, исключающих

оставления на них следов (например, от пальцев рук следователя или криминалиста).

Вопросы для самоконтроля:

1) Что такое электронное доказательство?

2) Назовите критерии электронных доказательств.

3) Каким принципам придерживаются при работе с электронными доказательствами?

4) Что такое оперативная память?

5) Какая информация может храниться в оперативной памяти?

6) Какие электронные доказательства хранятся в сетевых устройствах?

7) Что является важным условием использования в будущем электронных доказательств?

2.3. Транспортировка и хранение электронных доказательств.

Изъятые в ходе осмотра места преступления электронные доказательства подлежат транспортировке в орган уголовного преследования для осуществления работы с ними и обеспечения сохранности до принятия окончательного решения по уголовному делу.

Под транспортировкой электронных доказательств понимается процесс физического перемещения и передачи устройств, содержащих цифровую информацию, имеющую важное значение для расследования уголовного правонарушения.

Важно! Следователь несет ответственность за сохранность и целостность устройств, содержащих электронные доказательства при их транспортировке до передачи на хранение ответственному лицу либо судебному эксперту для проведения судебной экспертизы.

Нужно помнить и понимать, что электронные доказательства являются не стабильными, подверженными изменениям, следовательно вопросу транспортировки нужно придавать особое значение.

Необходимо придерживаться следующих мер безопасности:

- не допускать механические повреждения корпусов устройств, где хранятся электронные доказательства, а также каких-либо химических воздействий на них;

- учитывать, что магнитное поле, создаваемое энергосистемой транспортного средства, может оказать негативное влияние на устройства хранения электронных доказательств. Поэтому их транспортировка должна осуществляться в антистатических пакетах и коробках, исключающих размагничивание носителей информации.

Хранение электронных доказательств – это важный этап расследования уголовного правонарушения, направленный на сохранение и обеспечение

целостности цифровой информации, которая может быть использована в качестве доказательства в ходе судебного рассмотрения уголовного дела.

Рассматривают 2 формы хранения электронных доказательств:

- *физическая (складское помещение, камера хранения вещественных доказательств, офис, кабинет);*

- *облачная (облачные сервисы хранения данных).*

При физическом хранении электронных доказательств учитываются следующие факторы:

а) количество изъятой техники, оборудования, цифровой информации (соблюдать правила хранения и складирования);

б) условия хранения электронных доказательств (помещение для хранения должно быть сухим, теплым, отапливаемым);

в) наличие журналов учета вещественных доказательств;

г) безопасность хранения электронных доказательств.

При облачном хранении электронных доказательств учитываются следующие факторы:

а) безопасность и целостность данных;

б) сроки хранения электронных доказательств;

в) наличие журналов учета электронных доказательств;

г) резервное копирование;

д) управление доступом.

Основным преимуществом хранения электронных доказательств в цифровом формате является их масштабируемость и экономия ресурсов. В отличие от бумажных документов, электронные доказательства занимают меньше места, легко масштабируются и могут быть быстро распространены и обработаны.

Ниже приведены наиболее известные облачные платформы.

Amazon Web Services	Microsoft Azure	Google Cloud
IBM Cloud	Dropbox	Microsoft OneDrive
Google Disk	Box	Apple iCloud

Облачные технологии становятся все более популярным методом хранения электронных доказательств благодаря их высокой доступности, надежности и масштабируемости. Однако при использовании облачных хранилищ необходимо учитывать возможные угрозы безопасности и принимать соответствующие меры для защиты информации.

Необходимо придерживаться следующих мер безопасности:

- использовать многоуровневую аутентификацию;
- использовать антивирусное программное обеспечение;
- ограничить количество сотрудников, имеющих доступ к данным.

Вопросы для самоконтроля:

1) Что понимается под транспортировкой электронных доказательств?

2) Опишите меры безопасности, которые необходимо соблюдать при транспортировке электронных доказательств.

3) Назовите формы хранения электронных доказательств.

4) Какие факторы учитываются при физическом хранении электронных доказательств?

5) Какие факторы учитываются при облачном хранении электронных доказательств?

6) Перечислите меры безопасности, которые необходимо придерживаться при облачном хранении информации.

7) Из каких этапов состоит процесс изъятия электронных доказательств?

2.4. Назначение судебных экспертиз.

В процессе расследования преступлений следователь сталкивается с вопросом назначения судебных экспертиз, наименование которых определяется исходя из поставленных им целей и задач.

По компьютерным преступлениям *(киберпреступлениям)* согласно приказу Министра юстиции Республики Казахстан от 27 апреля 2017 года № 484 назначается **судебно-экспертное исследование средств компьютерной технологии**. Это вид судебно-медицинской экспертизы, направленный на изучение и анализ цифровой информации, компьютерных систем и технологий.

Объектами данной экспертизы являются[15]:

№	Наименование	Содержание
1	Аппаратные объекты	- различные виды персональных компьютеров *(настольные, портативные, карманные и так далее)* с основными блоками *(системные блоки, мониторы)*, внутренними узлами, деталями, комплектующими и т.д.; - периферийные устройства различного вида и назначения; - сетевые аппаратные средства *(серверы, рабочие станции, активное оборудование, сетевые кабели и т.д.)*; - дисковые накопители данных *(жесткие диски HDD, флоппи-диски FDD, CD-ROM, CD-RW, DWD-ROM, флэш-карты USB)*.

[15] https://adilet.zan.kz/rus/docs/V1700015180

2	Программные объекты	- системное программное обеспечение *(различные операционные системы для персональных компьютеров и локальных сетей MS-DOS, UNIX, Windows различных версий и так далее, вспомогательные программы – утилиты, средства разработки и отладки программ, служебная системная информация и так далее)*; - различные прикладные программные продукты *(приложения общего назначения: текстовые и графические редакторы, системы управления базами данных, электронные таблицы, редакторы презентаций)*; - приложения специального назначения для решения задач в определенной области науки, техники, экономики и так далее.
3	Информационные объекты	- файлы, подготовленные с использованием указанных выше и других программных средств *(с расширениями текстовых форматов .txt, .doc, графических форматов .bmp, .jpg, .cdr, форматов баз данных .dbf, .mdb, электронных таблиц.xls, cal и др.)*; - данные в форматах мультимедиа.
4	Объекты, содержащие информацию, необходимую для производства экспертных исследований	- различные документы *(договоры на покупку, создание (передачу)* научно-технической продукции; - акты сдачи-приема научно-технической продукции; - калькуляции стоимости предпродажной подготовки компьютерной техники и периферийных устройств и прочие; - сопроводительная документация к поставляемой на исследование компьютерной, вычислительной технике *(периферийным устройствам, магнитным носителям)*, различные справочные данные, инструкции пользователя, а также материалы дел.

При производстве данной экспертизы решаются следующие вопросы:

1) По аппаратным средствам:

- *каковы технические характеристики представленной компьютерной техники;*

- *возможно ли использование представленного технического комплекса для осуществления тех или иных функциональных задач (например, выхода в Интернет, запись компакт-дисков);*

- *каковы ориентировочные даты создания вычислительного комплекса с заданными возможностями и даты изготовления его отдельных блоков.*

2) По программным продуктам:

- *какая операционная система установлена в представленном системном блоке;*

- имеется ли в представленном системном блоке, установленное программное обеспечение (указывается название);

- находится ли данное программное обеспечение в работоспособном состоянии;

- каковы дата и время установки программного обеспечения (указывается название);

- имеются ли в предоставленных системных блоках программы, приводящие к неправомерному доступу к охраняемой законом компьютерной информации, внесению изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ;

- каковы основные функции представленного программного обеспечения;

- каково назначение представленных программ для ЭВМ;

- возможно ли осуществление заданного вида деятельности с использованием представленных технических средств и размещенного на нем информационного и специального программного обеспечения (запись компакт-дисков, подготовка и изготовление поддельных денежных знаков).

3) По информационным объектам:

- имеется ли на представленном магнитном диске или в составе технических средств вычислительной техники необходимое информационное обеспечение для решения какой-либо конкретной функциональной задачи;

- имеются ли на представленных магнитных носителях файлы с документами, относящимися к той или иной сфере деятельности (файлы с изображениями денежных знаков, бланками юридических лиц и оттисками печатей);

- имеются ли на представленных магнитных носителях ранее удаленные файлы (указываются названия);

- имеются ли на магнитном носителе какая-либо информация, если да, то каков вид ее представления;

- каково дата и время создания файлов (указываются названия).

2.5. Изучение и анализ заключений судебных экспертиз.

Заключение любой судебной экспертизы является одним из важных источников доказательства при расследовании уголовных правонарушений.

Получив результаты судебно-экспертного исследования средств компьютерной технологии, следователь должен внимательно изучить данный документ и проанализировать его путем сопоставления материалов уголовного дела и имеющихся доказательств с выводами судебного эксперта.

В соответствии с требованиями статьи 25 УПК РК, следователь оценивают доказательства по своему внутреннему убеждению, основанному на совокупности рассмотренных доказательств, руководствуясь при этом законом и совестью. В случае неясности или неполноты заключения судебной экспертизы и при отсутствии необходимости повторного ее назначения, следователь в соответствии со статьей 285 УПК РК может допросить эксперта.

Проведением судебных экспертиз разрешаются следующие задачи[16]:

Идентификационные задачи	Направлены на отождествление объекта по его отображениям, установление групповой принадлежности.
Диагностические задачи	Состоят в выявлении механизма события; времени, способа и последовательности действий, событий, явлений, причинных связей между ними; природы, качественных и количественных характеристик объектов, их свойств и признаков, не поддающихся непосредственному восприятию.
Классификационные задачи	Направлены на установление соответствия объекта определенным заранее заданным характеристикам и отнесение его на этом основании к определенному классу, роду, виду.

Таким образом, результат судебно-экспертного исследования средств компьютерной технологии помогает следователю понять, как произошло киберпреступление и скорректировать план расследования.

Вопросы для самоконтроля:

1) Что является объектами судебно-экспертного исследования средств компьютерной технологии?

2) Какие вопросы ставятся в постановлении о назначении судебной экспертизы по аппаратным средствам?

3) Какие вопросы ставятся в постановлении о назначении судебной экспертизы по программным продуктам?

4) Какие вопросы ставятся в постановлении о назначении судебной экспертизы по информационным объектам?

5) Какие задачи разрешаются проведением судебной экспертизы?

6) Раскройте содержание идентификационных задач.

7) Раскройте содержание диагностических задач.

8) Раскройте содержание классификационных задач.

[16] Методы и способы получения доказательственной информации с электронных носителей: учебное пособие / сост. М. В. Старичков, А. А. Шаевич. – Иркутск: ФГКОУ ВО ВСИ МВД России, 2015. – 88 с.

2.6. Международное сотрудничество.

В большинстве случаев, совершенные киберпреступления имеют трансграничный характер, поскольку преступники выбирают для совершения своих противоправных деяний те страны, где менее развита система предупредительных мер информационной безопасности.

Поэтому эффективность противодействия киберпреступности зависит от совместных усилий и координации действий правоохранительных органов разных стран и международных организаций.

Так или иначе на определенном этапе расследования киберпреступлений следственные подразделения правоохранительных органов сталкиваются с вопросами международного сотрудничества, успех которого зависит от нескольких факторов:

1) Наличие соответствующего национального законодательства, предусматривающего ответственность за все виды уголовных правонарушений, подпадающих под понятие киберпреступность.	В Казахстане предусмотрена уголовная ответственность за киберпреступления. Однако национальное законодательство необходимо привести в соответствие с международной классификацией видов киберпреступлений для эффективного взаимодействия с международными организациями такими, как Интерпол, Европол, правоохранительными органами разных стран.
2) Ратификация двусторонних, региональных и многосторонних договоров в области борьбы с киберпреступностью.	Казахстан рассматривает вопрос присоединения к Будапештской конвенции по борьбе с киберпреступностью
3) Готовности к взаимному обмену информацией о киберугрозах и инцидентах.	Создание в Казахстане службы CERT, как и во многих других государствах, позволяет своевременно и эффективно выявлять, а также предупреждать киберпреступления.

Отсутствие обоюдного признания странами одного из видов киберпреступлений позволяет лицам, их совершившим оставаться безнаказанным в той стране, где такая ответственность не предусмотрена.

Например, в следствие отсутствия соответствующего законодательства на Филиппинах в 2000 году, невозможно было привлечь к уголовной ответственности создателя и распространителя компьютерного вируса «Love Bug»[17].

[17] https://www.unodc.org/e4j/ru/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

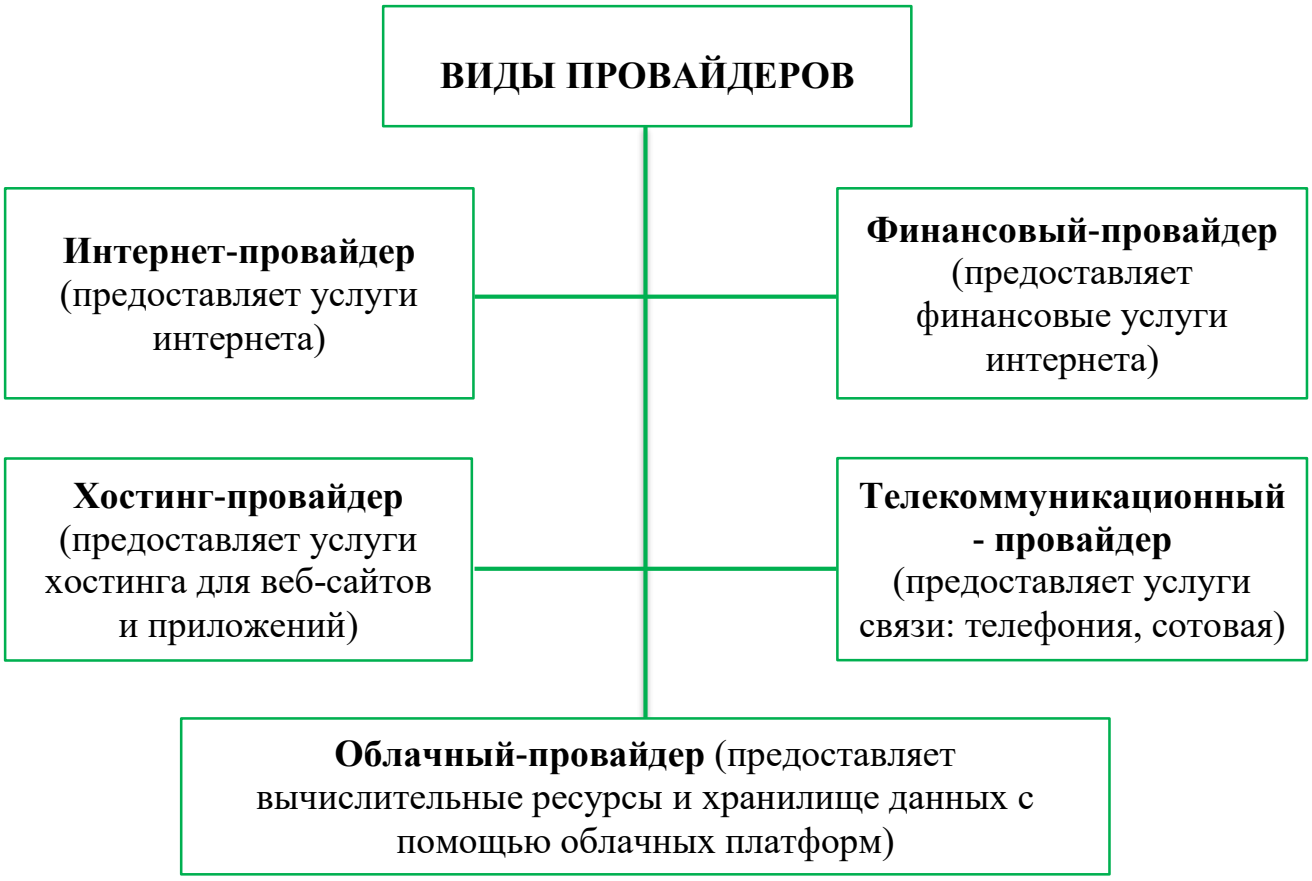
Однако существуют исключения, которые прописаны в статье 29 (3) Конвенции Совета Европы о компьютерных преступлениях 2001 года, согласно которой не требуется обоюдного признания соответствующего деяния преступлением при необходимости неотложного обеспечения сохранности компьютерных данных, хранящихся в компьютерной системе, расположенной на территории той страны, куда намереваются в рамках взаимной правовой помощи *(далее - ВПП)* направить просьбу о проведении обыска и выемки[18].

В свою очередь государство, к которому обратились за международной правовой помощью, может отклонить данную просьбу другого государства в случае нарушения им международных обязательств в области прав человека.

Отклонение запроса об оказании международной правовой помощи также может произойти из-за несоблюдения процедурных требований, связанных со сроком хранением электронных доказательств.

Одним из важных процессов и причин направления международных запросов о ВПП является получение электронных доказательств, которые хранятся у провайдеров.

Провайдеры – это организации, предоставляющие какие-либо услуги в той или иной области. Отсюда следует, что существуют разные типы провайдеров, которые подразделяются в зависимости от вида предоставляемых услуг.



[18] https://www.unodc.org/e4j/ru/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html

В процессе расследования киберпреступлений следователь может столкнуться с разными видами провайдеров, у которых необходимо получить сведения. Однако не всегда такие провайдеры готовы к сотрудничеству с правоохранительными органами. В большинстве случаев провайдеры услуг отказывают следственным органам в предоставлении информации по объективным причинам, к которым можно отнести сроки хранения информации и условия конфиденциальности.

Более того, один и тот же вид провайдера может хранить разную информацию. Например, два провайдера, предоставляющих услуги интернета в одном государстве могут отличаться по типу данных, которые они сохраняют и политики безопасности.

На практике правоохранительные органы многих государств сталкиваются с одинаковыми проблемами. Они связаны со сроками хранения информации у Интернет-провайдера *(от 1-го до 6-ти месяцев)*. Учитывая длительность процесса исполнения международных запросов о взаимной правовой помощи, не всегда правоохранительные органы успевают «заморозить» данные, хранящиеся у поставщика интернет-услуг.

На данный процесс также может оказывать влияние и законодательство, действующее в стране, исполняющая запрос о ВПП. Если сроки хранения данных и порядок доступа к ним не урегулирован нормативным правовым актом, то и требовать исполнения провайдером поручения о сохранности данных не всегда представляется возможным.

Кроме того, в каждой стране существуют разные подходы к вопросу предоставления информации, хранящейся у провайдера. Например, законодательство США требует наличие судебного постановления для получения данных, не относящихся к контенту *(данные абонента и IP-адреса)* и ордер на обыск, если наоборот он связан с контентом. В то время как в Турции таких разрешений правоохранительным органам не требуется. В Казахстане действует разрешительная процедура для получения данных от различных провайдеров услуг.

Все эти факторы влияют на эффективность международного сотрудничества в области противодействия киберпреступности.

Кроме Европейской Конвенции о компьютерных преступлениях есть также:

- Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации 2001 года. В нем тоже имеются положения, раскрывающие формы сотрудничества, способы и условия, при которых возможна взаимная правовая помощь;

- Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий 2010 года. Содержит процедурные положения сотрудничества, в том числе в части подачи и удовлетворения международных запросов о взаимной правовой помощи;

- Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 года. Она рассматривает вопросы взаимного обмена информацией по компьютерным преступлениям.

Противодействие киберпреступности невозможно без:

- постоянного повышения квалификации сотрудников правоохранительных органов разных стран *(это происходит путем взаимного обмена опытом и обучения новейшим методикам и тактикам проведения расследования по отдельным видам киберпреступлений)*;

- сотрудничества с частным сектором *(государственно-частное партнерство позволяет разрабатывать совместные меры предотвращения и расследования киберпреступлений, путем информирования населения о киберугрозах, разработки национального программного обеспечения, участия в отдельных этапах расследования)*;

- разработки международных соглашений по вопросам противодействия киберпреступности.

Вместе с тем, отсутствие знаний и соответствующих криминалистических инструментов значительно снижает возможности правоохранительных органов в борьбе с киберпреступностью и соответственно негативно влияет на международное сотрудничество.

К проблемам сотрудничества также можно отнести:

- культурные и языковые барьеры *(вследствие особенностей той или иной страны и используемого ими языка общения)*;

- отсутствие единых стандартов в сфере обмена информацией;

- слабая техническая оснащенность подразделений, осуществляющих борьбу с киберпреступностью *(не позволяет обеспечивать поиск и изъятие цифровых доказательств)*.

Решение этих проблем возможно через:

- создание специальных форумов или платформ в глобальной сети интернет для своевременного обмена информацией, передовым опытом борьбы с киберпреступлениями;

- разработку единых стандартов в сфере обмена информацией и расследования преступлений данной категории;

- взаимное оказание помощи в предоставлении технических решений *(программных обеспечений)*;

- обучение сотрудников правоохранительных и судебных органов *(что позволит странам увеличивать количество высококвалифицированных специалистов)*;

- разработку и реализацию научно-исследовательских проектов в области кибербезопасности.

Взаимная правовая помощь по делам о киберпреступлениях

Запросы о взаимной правовой помощи между Казахстаном и другими странами по киберпреступлениям должны подаваться в письменной форме и включать в себя следующую информацию:

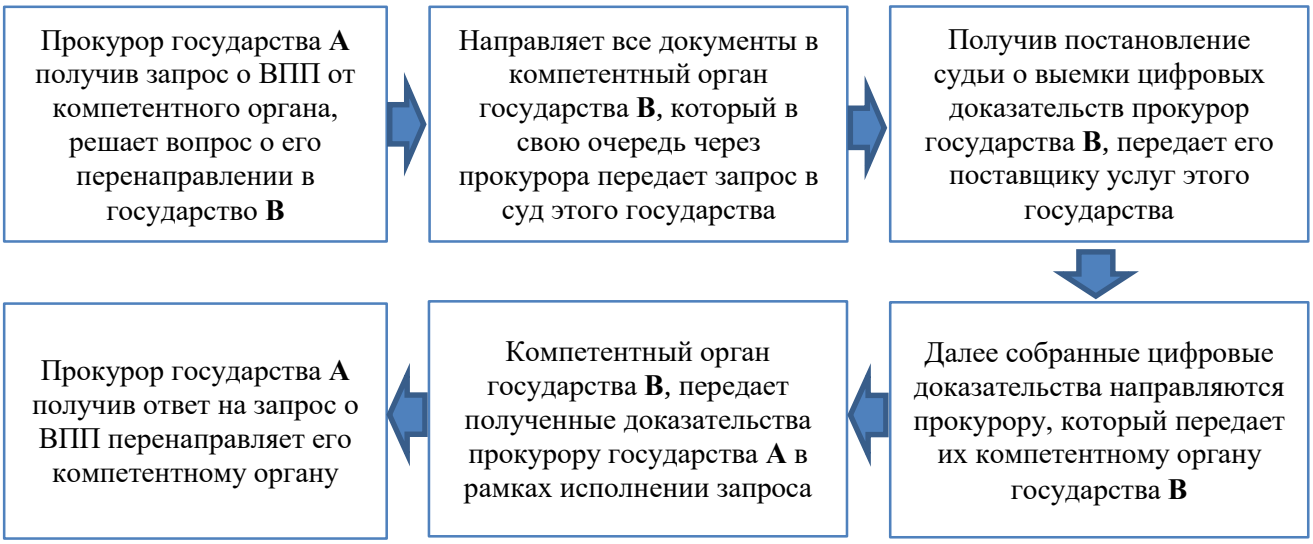
- название правоохранительного органа, подающего запрос;

- цель и содержание запроса *(следует предоставить достаточное количество информации для положительное принятия решения, например, сведения о каждом подозреваемом, на каком этапе находится расследование, какие электронные доказательства необходимы, а также использовать официальные формулировки)*;

- в связи с чем направлен запрос *(расследование преступления или уже судебное разбирательство, при необходимости следует сослаться на международный договор, соглашение)*;

- описание совершенного правонарушения и нарушенных нормативных правовых актов *(кроме ссылок на законодательство, необходимо указывать наказание, которое может быть назначено)*.

Процесс запроса о взаимной правовой помощи может выглядеть следующим образом:



Описанный процесс о ВПП не является общепринятым и обязательным для всех государств, задействованных в борьбе с киберпреступностью!

Некоторые государства могут рассматривать вопрос об оказании взаимной правовой помощи только при выполнении определенных условий, например, при соблюдении принципа взаимности *(Япония, Украина, Бразилия)*. Более того, даже при наличии соглашения об экстрадиции, не всегда лицо, в отношении которого поступил запрос, может быть выдано запрашивающей стороне. Например, несмотря на существующий договор об экстрадиции между Соединенным Королевством Великобритании и Соединенными Штатами Америки, подписанный в 2003 году, британский хакер Lauri Love не был экстрадирован *(дело от 2017 года)*[19].

Кроме вышеуказанных способов взаимодействия и международного сотрудничества имеются также и неофициальные каналы обмена информацией между правоохранительными органами разных стран. Тип, характер и объем информации, подлежащей обмену, зависит от самого государства.

[19] https://www.unodc.org/e4j/ru/cybercrime/module-7/key-issues/informal-international-cooperation-mechanisms.html

В отдельных странах это могут быть добровольные показания свидетелей, полученных по каналам видеосвязи, из открытых источников *(Австралия)*[20].

Поскольку официальные способы передачи информации *(запросы о взаимной правовой помощи)* занимают длительное время *(до 6 месяцев и в отдельных случаях больше)*, неофициальные каналы обмена данными являются самыми эффективными в расследовании преступлений.

Однако не всегда они могут быть использованы в качестве доказательств.

Например, Японии разрешается исполнять запросы, поступившие по неофициальным каналам только при условии, что другая страна не намерена использовать эту информацию в качестве доказательств. Если же страна намеревается использовать эту информацию в качестве доказательства, необходимо направить официальный запрос об оказании взаимной правовой помощи[21].

В качестве эффективной площадки для обмена информацией можно использовать:

- международную полицейскую организацию Интерпол, которая работает 24 часа в сутки в 190 странах мира;

- Европол - полицейскую службу Европейского Союза, главный офис которой располагается в Гааге. Основными целями организации являются координация усилий национальных служб в борьбе с международной организованной преступностью и улучшение обмена информацией между национальными полицейскими службами[22].

Требования к составлению запросов о ВПП по киберпреступлениям.

Запрос о получении электронных доказательств должен[23]:

- быть законным *(… в соответствии с законами и процедурами запрашивающего и запрашиваемого государств, а также в соответствии с их международными обязательствами по соблюдению прав человека, в частности тех, которые установлены Международным пактом о гражданских и политических правах и документами Комитета по правам человека)*;

- обеспечивать уважение всех прав человека *(включая право на жизнь; право не подвергаться пыткам и жестокому, бесчеловечному или унижающему достоинство обращению; право на свободу и личную неприкосновенность; право на неприкосновенность частной жизни; право не подвергаться дискриминации; право на свободу мысли, совести и религии; право на свободное выражение мнений; право на мирные собрания; право на свободу ассоциаций; право на свободу передвижения; справедливое и публичное разбирательство дела компетентным, независимым и беспристрастным судом, созданным на основании закона)*;

- быть необходимым для поддержки судебного преследования лица, совершившего преступление, или для доказательства невиновности подозреваемого, а также соразмерным этим целям;

---

[20] Доклад Комитета по правам человека ООН. Том II. A/63/40 (Vol.II). Нью-Йорк, 2008 год

[21] https://www.unodc.org/e4j/ru/cybercrime/module-7/key-issues/informal-international-cooperation-mechanisms.html

[22] https://ru.wikipedia.org/wiki/Европол

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN

- **учитывать воздействие на третьих лиц** и предотвращать посягательства на личные сообщения лиц, в отношении которых не осуществляется расследование;

- **подпадать под действие систем независимого надзора**, как со стороны судебных механизмов, так и со стороны других органов, уполномоченных обеспечивать правомерное поведение правоохранительных органов и спецслужб.

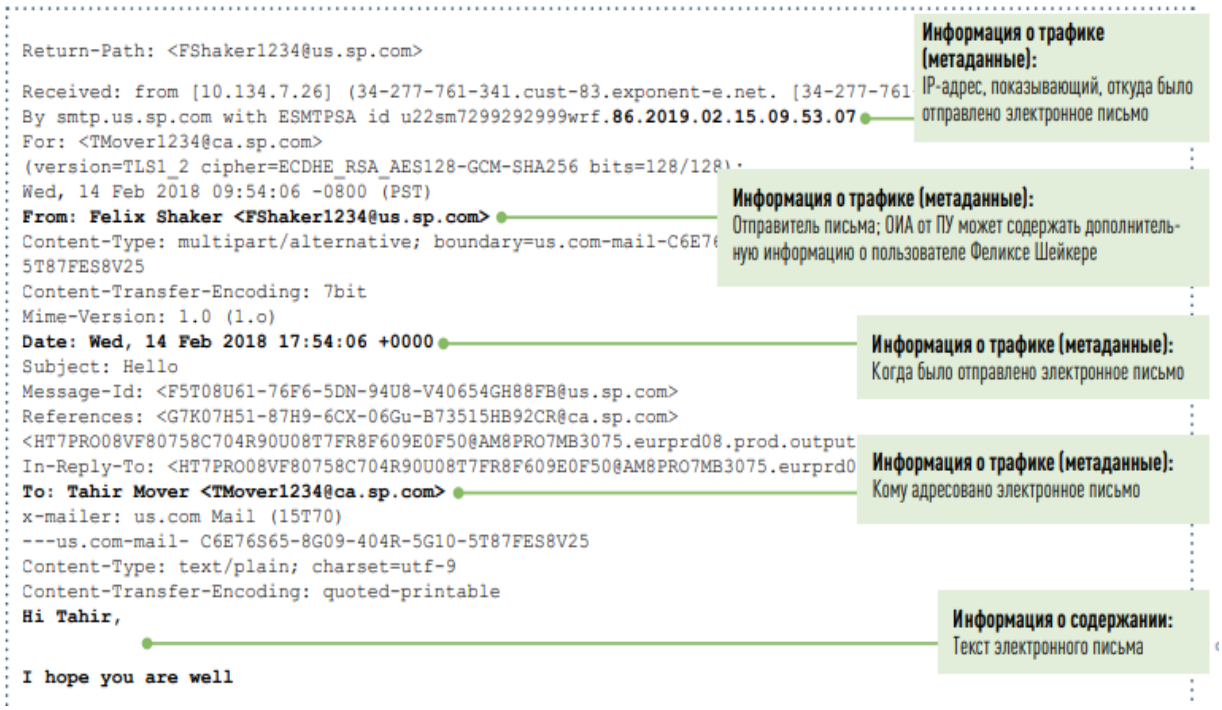
Ниже представлены сведения об основных категориях электронных доказательств, которые чаще всего запрашиваются при ВПП[24].

	Хранящиеся электронные доказательства	**Электронные доказательства, собираемые в режиме реального времени**
Основная информация об абоненте (ОИА)	Имя абонента (пользователя); может включать сведения о том, как долго абонент пользовался конкретной услугой, а также IP-адрес, с которого впервые был совершен вход в систему, номер телефона пользователя, адрес электронной почты, вид услуги, включая идентификатор, связанные устройства, данные о проверке использования услуги, все IP-адреса, использованные пользователем для входа в свою учетную запись, время, дата и продолжительность всех сеансов.	
Информация о трафике (без информации о содержании)	• Метаданные, связанные с оказанием услуг; включают данные, касающиеся подключения, трафика или места, откуда осуществляется связь (например, IP-адрес или MAC-адрес); • Журналы регистрации доступа, в которых фиксируются время и дата доступа конкретного физического лица к услуге, а также IP-адрес, с которого доступ осуществлялся; • Журналы транзакций, в которых фиксируются продукты или услуги, полученные конкретным физическим лицом от поставщика или третьего лица (например, приобретение места в облачном хранилище). Информация о любых изображениях, документах, размеров файлов, объем переданных данных.	Перехват информации о том, с кем и откуда объект осуществляет контакт — например, статические и динамические IP-адреса
Информация о содержании	Тело или текст электронного письма, сообщения, запись в блоге или социальной сети, видео, изображения	Перехват тела или текста электронного письма, сообщения, записи в блоге или социальной

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN, с. 43.

	или аудиоматериалы, хранящиеся в цифровом формате (кроме данных об абоненте или метаданных), а также данные геолокации, списки контактов, черновики электронных писем, удаленные и доступные электронные письма, дамп страниц, резервные копии, данные геолокации, дамп ящика электронной почты.	сети, видео, изображений или аудиоматериалов, хранящихся в цифровом формате (кроме данных об абоненте или метаданных), а также данных геолокации.

Пример, необработанного электронного сообщения, отображающий хранящиеся электронные доказательства:



Перед направлением запроса о ВПП следователь должен: убедиться в сохранности электронных доказательств у поставщика услуг *(далее - ПУ)*, определить способ запроса электронных доказательств и куда необходимо направлять такой запрос *(места, где хранятся электронные доказательства)*.

Во-первых, учитывая, что каждый ПУ имеет свои сроки хранения информации, которые регулируются национальным законодательством той страны, откуда планируется запросить данные, то нужно понимать, что по истечении этого срока, возможность удовлетворения запроса о ВПП может быть сведена к минимуму.

Например, политика безопасности мессенджера «WhatsApp» предусматривает уничтожение недоставленных сообщений со своих серверов через 30 дней. Соответственно, правоохранительному органу нужно убедиться, что ПУ располагает этими электронными доказательствами.

Во-вторых, необходимо иметь в виду, что отдельные государства могут не исполнять запросы о ВПП в отношении тех уголовных правонарушений, где сроки лишения свободы менее 1 года или незначительный материальный ущерб

(например, США). Следовательно, целесообразно связаться с правоохранительным органом того государства, откуда планируется получить данные электронные доказательства и выяснить данный вопрос.

В-третьих, ПУ может находиться в одной стране, а его сервера располагаться в абсолютно другом государстве *(при неправильном определении места хранения данных может быть упущено время и доказательства будут утеряны).*

Поэтому, некоторые ПУ предоставляют правоохранительным органам возможность связаться с ними напрямую по вопросам обеспечения сохранности цифровых данных и выяснить все детали.

Обеспечение сохранности электронных доказательств

Политика безопасности любого ПУ заключается в обеспечении безопасности данных и защиты конфиденциальной информации. В контексте расследования киберпреступлений для правоохранительных органов одним из важных вопросов является сохранение электронных доказательств *(далее - ЭД)* поставщиком услуг, который обеспечивает это путем осуществления «Снэпшота» *(Snapshot),* что означает фиксирование состояния какой-либо системы или данных в определенный момент времени.

В соответствии с этим предусматривается следующий алгоритм взаимодействия правоохранительных органов с ПУ:

Четвертый шаг алгоритма взаимодействия предусматривает уведомление пользователя и раскрытие информации, что означает информирование поставщиком услуг владельца учетной записи в отношении которого правоохранительные органы предпринимают попытки собрать сведения. Это происходит по двум причинам:

1) Политика безопасности ПУ, предусматривающая такое уведомление;

2) Программное обеспечение установленное на серверах ПУ предусматривает автоматическую рассылку писем владельцам учетной записи.

Однако, не все ПУ осуществляют такое уведомление, поэтому правоохранительному органу перед направлением запроса ПУ, необходимо выяснить данный вопрос.

В случае получения подтверждения, что ПУ не уведомляет владельцев учетной записи, в отношении которых производится сбор информации, правоохранительный орган все равно указывает в своем запросе требование о неразглашении сведений о проведении расследования.

При обращении к поставщику услуг, в том числе находящихся в другом государстве, необходимо придерживаться следующих рекомендаций к форме запроса[25]:

• указывайте правильные идентификаторы, чтобы ПУ мог легко найти нужных пользователей или учетные записи *(если речь идет о нескольких учетных записях, на каждый профиль может потребоваться отдельный запрос)*;

• обязательно укажите тип данных *(ОИА, информация о трафике или информация о содержании)* и срок, на который требуется обеспечить их сохранность, а также отношение этих данных к расследуемому преступлению;

• сократите запрашиваемый набор данных до того, что вам действительно необходимо *(ограничьтесь конкретными продуктами или услугами, относящимися к делу; не делайте запрос слишком объемным – это самая распространенная причина, по которой большинство ПУ отказываются выполнить запрос об обеспечении сохранности)*;

• обоснуйте запрос *(укажите, как запрошенная информация поможет в расследовании)*;

• внесите в календарь напоминание на случай, если нужно будет направить запрос о продлении срока хранения данных *(направляйте запрос о продлении не позднее чем за две недели до истечения текущего срока)*;

• согласившись выполнить запрос, ПУ обычно выдает идентификационный номер. Его следует указывать в любой корреспонденции с ПУ, например по вопросу о продлении срока хранения данных *(этот идентификационный номер следует также указать в ЗВПП, чтобы подтвердить обеспечение сохранности запрошенных электронных доказательств)*. Судебное распоряжение, выданное в адрес ПУ в запрашиваемом государстве, будет содержать идентификационный номер из ЗВПП, чтобы ПУ мог быстро найти требуемые электронные доказательства.

Следует отметить, что в отдельных странах отсутствуют обязательные требования по направлению запроса о ВПП для получения электронных доказательств. В таких государствах правоохранительные органы могут получить электронные доказательства путем:

- прямых запросов поставщику услуг *(с согласия пользователя, если пользователь скончался или имеется согласие его ближайших родственников на раскрытие информации, в отношении основной информации об абоненте или трафике)*;

- поиска в открытых источниках *(например, для примерного определения местоположения пользователя с помощью общедоступных онлайн инструментов, таких как IP-адрес; установления владельцев доменных имен,*

[25] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN

получения доказательств совершенного преступления через учетные записи в общедоступных социальных сетях);

- прямого обращения к пользователю учетной записи с просьбой о предоставлении ЭД;

- полицейского сотрудничества на основании судебного приказа или в рамках добровольного раскрытия информации;

- получения согласия у пользователя учетной записи или у его ближайших родственников о предоставлении поставщиком услуг необходимых ЭД из учетной записи.

Важно! Прежде чем правоохранительные органы одного государства смогут запрашивать электронные доказательства в другом государстве, нужно убедиться в том, что возможности на национальном уровне уже исчерпаны!

С типовыми формами вышеуказанных запросов можно ознакомиться в ***приложениях № 1.***

Вопросы для самоконтроля:

1) Дайте определение термину «провайдер»?

2) Назовите виды провайдеров.

3) Назовите основные проблемы международного сотрудничества в сфере расследования киберпреступлений.

4) Какая информация должна быть отражена в запросе о ВПП?

5) Назовите площадки для обмена информацией в сфере расследования киберпреступлений.

6) Назовите требования к составлению запросов о ВПП по киберпреступлениям.

7) Какие основные категории электронных доказательств запрашиваются при ВПП?

8) Что должен сделать следователь перед направлением запроса о ВПП?

9) Назовите алгоритм взаимодействия правоохранительных органов с поставщиками услуг.

ГЛАВА 3. ЗАВЕРШАЮЩИЙ ЭТАП РАССЛЕДОВАНИЯ.

В данной главе будут рассмотрены такие вопросы как розыск и задержание подозреваемого, способы определения геолокации используемого устройства с помощью IP и MAC адресов, их виды, особенности допроса подозреваемого.

3.1. Розыск подозреваемого.

Розыск киберпреступника и его идентификация являются наиболее сложными задачами для следственно-оперативных подразделений правоохранительных органов. Это связано с тем, что преступления совершаются с использованием различных технологий, позволяющих оставаться анонимными в сети интернет. Но даже при всем этом, правоохранительные органы находят и разрабатывают новые методики и тактики поиска киберпреступника.

Какие бы ни использовал преступник способы сокрытия своих незаконных действий в сети интернет, компьютерной системе, сетевых устройствах и т.д. остаются электронные следы, которые можно обнаружить, изъять и проанализировать. Это позволяет следственным органам не просто составить картину преступления, но и найти тот цифровой след, позволяющий установить его местонахождение и задержать.

Специалисты по интернет – разведке рассматривают разные способы поиска интересующих их лиц через сеть интернет, технологии которых можно применить и к розыску преступников, в том числе по киберпреступлениям.

Одним из основных способов поиска преступника является определение геолокации устройства, используемого разыскиваемым лицом.

Термин «геолокация» означает определение точного географического местоположения устройства *(например, сотового телефона, планшета, ноутбука, навигатора, смарт-часов и других девайсов)* с помощью различных способов и технологий:

1	**GPS** (Глобальная система позиционирования)	Спутниковая система, которая использует сеть спутников для точного определения местоположения на поверхности Земли.
2	**Wi-Fi, сотовые данные**	Многие устройства *(смартфоны, планшеты, смарт-часы и т.д.)*, используют информацию о близлежащих точках доступа Wi-Fi или вышках сотовой связи для определения своего местоположения.
3	**IP-адрес**	Интернет-провайдер может предоставить информацию о точном географическом местоположении, используя IP-адрес устройства.
		Некоторые устройства могут использовать

4	**Bluetooth**	сигналы Bluetooth для определения местоположения в пределах ограниченного радиуса.
5	**Навигационные данные из мобильных приложений**	Многие приложения на смартфонах и других устройствах запрашивают доступ к данным геолокации для предоставления услуг, основанных на местоположении, таких как карты, рекомендации ресторанов и другие.

Наиболее точными способами определения координат являются использование навигационных систем **GPS** или **ГЛОНАСС**, которые обычно обеспечивают погрешность не более 2 метров. Если нет доступа к спутниковым системам, можно приблизительно определить местоположение с помощью мобильных базовых станций, но погрешность значительно возрастает[26].

Процесс определения местоположения с помощью GPS включает в себя несколько этапов:

Геолокацию также можно получить с помощью **IP-адреса** и **MAC-адреса**.

IP-адрес *(англ. Internet Protocol Address)* – это уникальный числовой или буквенно-числовой идентификатор, который присваивается поставщиком интернет-услуг *(провайдером)* каждому устройству *(например, компьютеру, ноутбуку, планшету, принтеру, маршрутизатору и т.д.)*.

Благодаря данной технологии можно идентифицировать и различать устройства в сети, правильно маршрутизировать и доставлять информацию между различными устройствами.

[26] https://bezlimit.ru/blog/geolokatsiya-chto-eto-takoe/

Существует только определенные версии IP-адресов:

IPv4 – самая распространенная версия IP-адресов, которая состоит из **32**-разрядных чисел *(выглядит так: «192.168.1.1»)*.

IPv6 – новая версия IP-адресов, состоящая из **128**-разрядных чисел *(выглядит так: «*2001:0db8:85a3:0000:0000:8a2e:0370:7334*»)*.

IP-адрес имеет следующие основные функции: 1) идентификация устройства; 2) маршрутизация данных; 3) обеспечения связи в сети; 4) сетевая безопасность. IP-адреса могут меняться и быть неизменными, работать во внутренней сети и в глобальной сети Интернет.

IP-адреса подразделяются

- **Статические –** при каждом подключении не меняется, остается неизменными (выдают организациям)
- **Динамические –** при новом подключении меняется (присваивается домашним роутерам)
- **Внутренние** (локальные) – помогают устройствам общаться между собой внутри одной сети (дом или офис – 192.168.1.1).
- **Внешние** (глобальные) – позволяющие устройствам общаться с другими устройствами в сети Интернет (203.0.113.1).

В процессе назначения IP-адресов участвуют следующие организации:

- **ICANN** *(Internet Corporation for Assigned Names and Numbers)* – глобальная некоммерческая организация, ответственная за управление системой доменных имен *(DNS)* и присвоение глобальных IP-адресов. ICANN делегирует управление IP-адресами региональным интернет-реестрам *(RIR)* и координирует их деятельность;
- **RIRs** *(Regional Internet Registries)* – организации, ответственные за распределение глобальных IP-адресов в различных регионах мира. Каждый региональный интернет-регистратор обслуживает определенный географический регион:

ARIN (American Registry for Internet Numbers)	для Северной Америки
RIPE NCC (Réseaux IP Europeens Network Coordination Centre)	для Европы, Ближнего Востока и некоторых стран Средней Азии
APNIC (Asia-Pacific Network Information Centre)	для Азиатско - Тихоокеанского региона

LACNIC (Latin American and Caribbean Internet Addresses Registry)	для Латинской Америки и Карибского бассейна
AFRINIC (African Network Information Centre)	для Африки

- **ISP** *(Internet Service Provider)* – поставщики интернет-услуг, такие как телекоммуникационные компании и интернет-провайдеры, которые получают свой региональный IP-адресный блок от RIR. Они, в свою очередь, могут назначать IP-адреса своим клиентам.
- **LIR** *(Local Internet Registry)* – отдельные организации, которые получают статические IP-адреса блок непосредственно от RIR или ISP и управляют ими непосредственно через LIR.

Для локальных сетей, не подключенных напрямую к Интернету, используются частные IP-адреса, назначаемые организациями самостоятельно. Их использование ограничено в пределах конкретной локальной сети.

Они определены в следующих диапазонах:

- от 10.0.0.0 до 10.255.255.255;
- от 172.16.0.0 до 172.31.255.255;
- от 192.168.0.0 до 192.168.255.255.

Необходимо иметь ввиду, что технология NAT *(Network Address Translation)*, позволяет нескольким устройствам внутри сети подключаться к Интернету, используя один и тот же внешний IP-адрес.

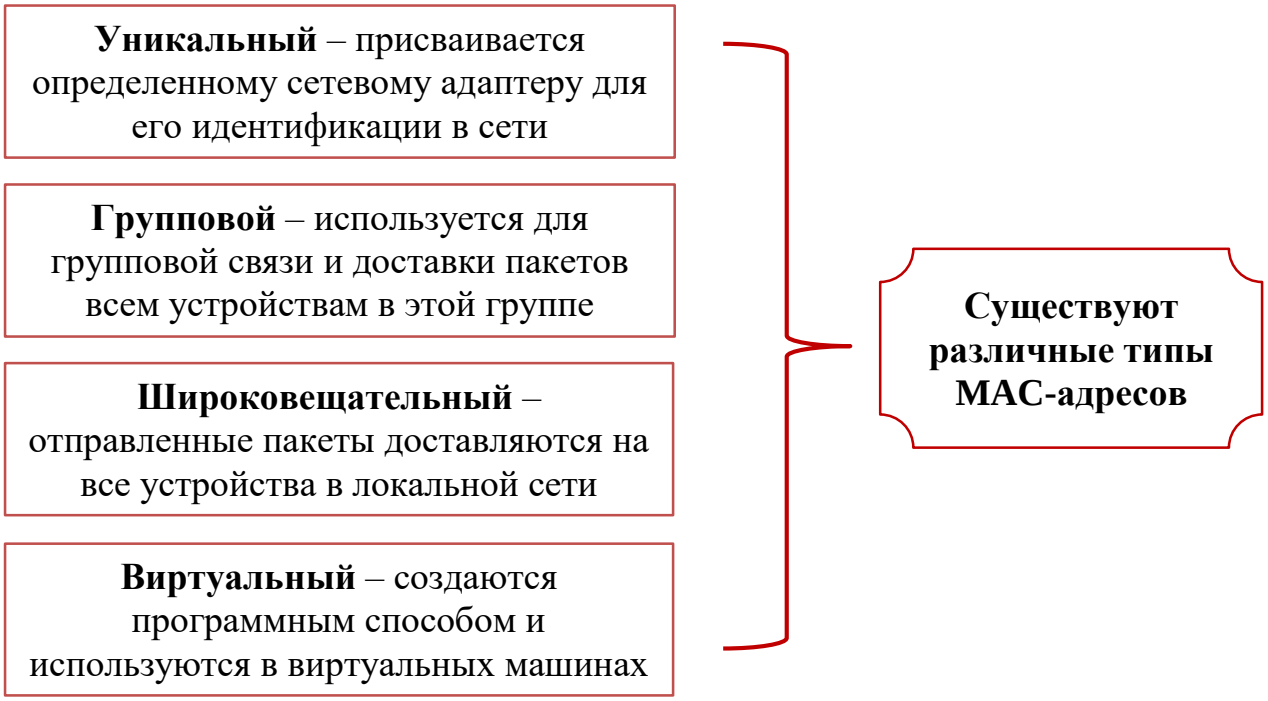
Для поиска устройства в сети Интернет, которым пользуется или пользовался преступник, может быть применим следующий алгоритм действий:

1. Поиск IP-адреса, по которому можно установить местонахождение устройства *(чтобы найти устройство с использованием сети интернет необходимо знать его IP-адрес)*;
2. Работа с сервисами геолокации, например, WHOIS или 2Ip, которые могут дать интересующие сведения *(например, название города, страны и провайдера)*;
3. Работа с командной строкой дает дополнительную информацию по IP-адресу *(требуется введение таких команд, как «ping» или «traceroute», для определения активности и маршрута к устройству с определенным IP-адресом)*;
4. Взаимодействие с провайдером, у которого можно запросить более детальную информацию *(относительно присвоения IP-адреса устройству, а также за кем это устройство зарегистрировано)*;
5. Использование других специализированных сервисов и программ.

Важно отметить, что преступники для своих незаконных действий могут использовать средства анонимизации *(например, VPN, прокси-сервера и другие технические решения)*.

MAC-адрес – это уникальный физический адрес устройства, помогающий идентифицировать его среди других устройств. Он присваивается производителем сетевого оборудования и прописывается на сетевой карте, работает на втором уровне модели OSI *(канальный уровень передачи данных)*,

состоит из 12 шестнадцатеричных символов, разделенных двоеточиями или тире[27]. Может выглядеть следующим образом: **00:1A:2B:3C:4D:5E.**



MAC-адрес имеет следующие функции: 1) идентификация устройства; 2) обеспечение уникальности; 3) разрешение коллизий; 4) фильтрация трафика; 5) контроль доступа. Следует отметить, что существуют механизмы для изменения *(клонирования)* MAC-адреса на некоторых устройствах с целью обеспечения дополнительной анонимности в сети.

№	**Ключевые отличия IP / MAC - адресов:**	
	MAC - адрес	**IP – адрес**
1	Работает на втором уровне *(канальном уровне)* модели OSI, обеспечивая связь внутри локальной сети.	Работает на третьем уровне *(сетевом уровне)* модели OSI, отвечает за маршрутизацию и глобальную адресацию в сети.
2	Уникален для каждого сетевого адаптера и назначается производителем оборудования.	Уникален внутри сети, но не на глобальном уровне, особенно в частных сетях.
3	Используется для локального обмена данными внутри сегмента сети, не выходя за его пределы.	Используется для глобальной адресации и маршрутизации данных в сети, позволяя устройствам в разных сетях взаимодействовать друг с другом.
4	Связан с протоколами канального уровня, такими как Ethernet.	Связан с протоколами сетевого уровня, такими как IPv4 и IPv6.

[27] https://wiki.merionet.ru/articles/chto-takoe-mac-adres-i-kak-ego-uznat/

В процессе передачи данных по сети используется комбинация MAC-адреса *(для локальной доставки внутри сегмента)* и IP-адреса *(для глобальной маршрутизации и доставки между сегментами)*.

Чтобы найти преступника, а точнее установить его местонахождение посредством использования интернет-технологий и, в частности, с помощью IP и MAC – адресов, можно использовать следующие алгоритмы действий, которые приведут к определенному результату.

Как уже ранее упоминалось, любые действия, которые пользователь совершает в интернете, не остаются не замеченными. Даже осуществляя ничем не приметную переписку по электронной почте, **мы оставляем в компьютере или интернете электронные следы**. Задача сотрудника, осуществляющего розыскные мероприятия или расследование преступления, обнаружить данные следы и установить местонахождение скрывшегося лица.

Рассмотрим несколько способов определения местонахождения подозреваемого с помощью определенных алгоритмов поиска, основанных на использовании IP и MAC – адресов.

Определение геолокации устройства с помощью IP-адреса

С учетом вышеизложенной информации сформулируем вывод о том, что IP-адрес фактически является виртуальным паспортом человека, который может многое сказать о пользователе интернета. Например, выдать информацию о его провайдере, примерном местонахождении, а также сообщить другие сведения, интересные для органа уголовного преследования.

Для того, чтобы произвести поиск по IP-адресу, правоохранительным органам необходимо сначала его установить. В расследовании уголовных правонарушений, совершенных с использованием информационно-коммуникационных технологий, следователи могут столкнуться с разными ситуациями:

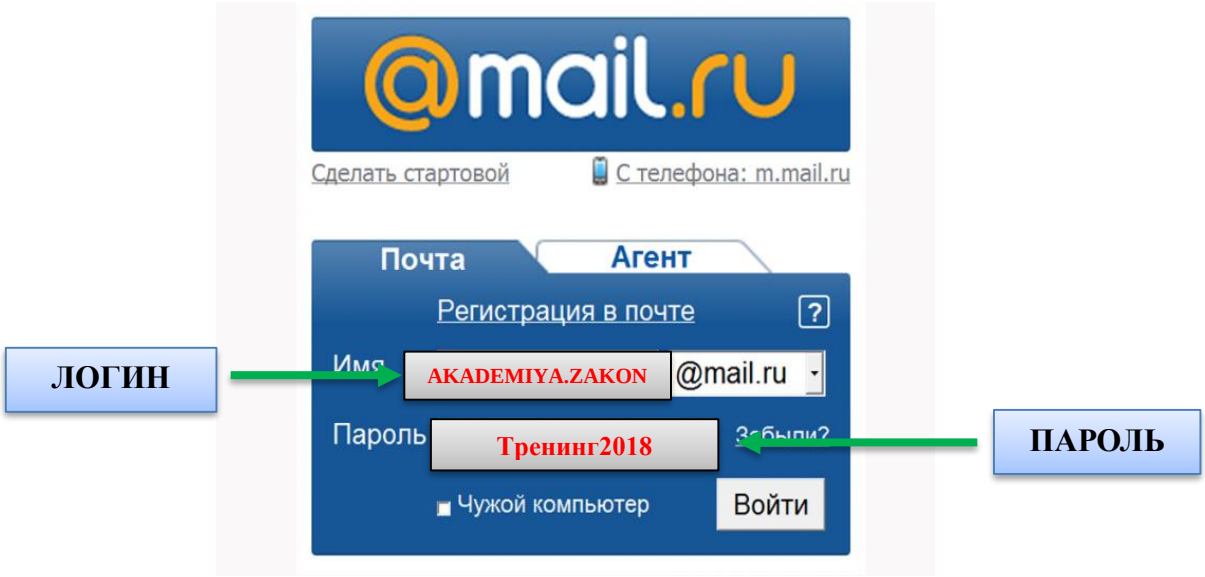
- *орган уголовного преследования располагает информацией о конкретных лицах, с кем осуществляет переписку субъект (подозреваемый), скрывшийся от органов расследования, с целью последующего установления IP-адреса;*
- *орган уголовного преследования не располагает такой информацией (требуется использование других способов установления IP-адреса)*.

Первый вариант. Может рассматриваться в том случае, когда у органа расследования имеется доступ к почтовому ящику того человека, с кем ведет переписку находящееся в розыске лицо *(например, данный человек добровольно оказал содействие органам расследования, предоставляя доступ к своему почтовому сервису, либо имеется санкция суда)*. Это могут быть сообщники, компаньоны *(коллеги)*, друзья, родственники и т.д.

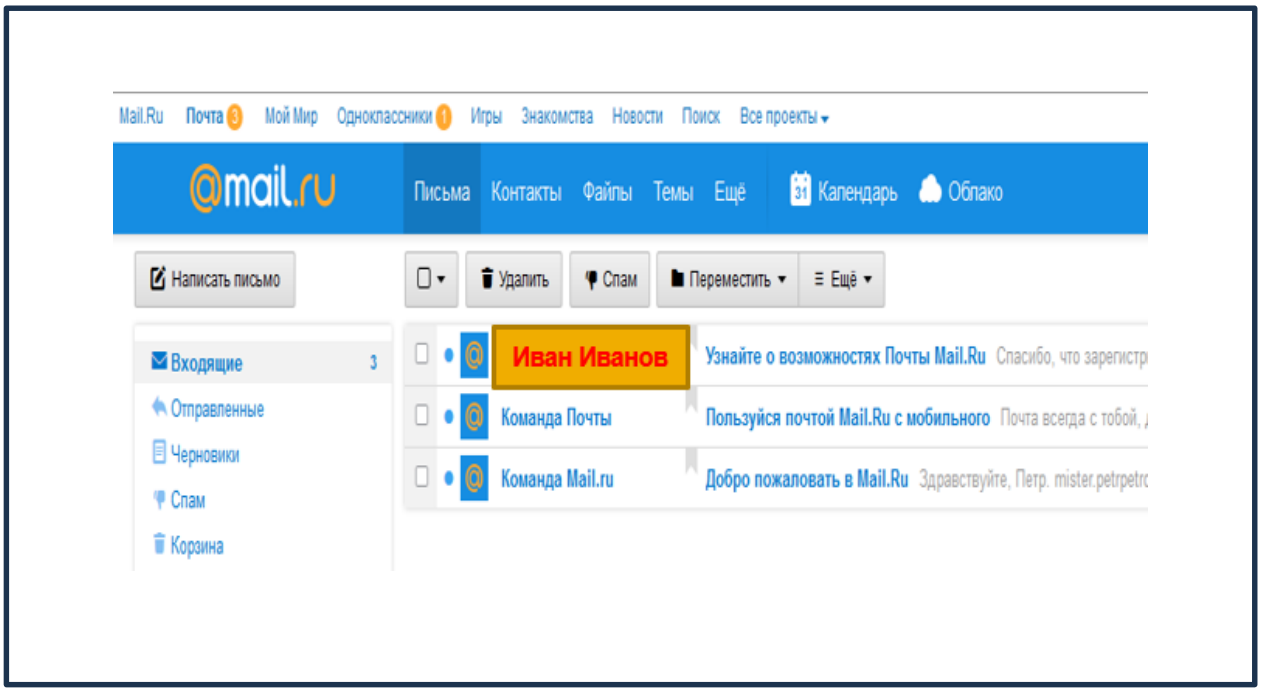
Для этого, следователю необходимо на компьютере или ноутбуке открыть электронное сообщение от подозреваемого, найти раздел с названием «Еще», кликнуть по нему и далее пройти в подраздел с названием «Служебные заголовки». В открывшемся окне можно обнаружить IP-адрес. Следователю

нужно скопировать его, после чего открыть один из интернет – сервисов по определению геолокации с помощью IP-адреса *(2IP или Whois)*. И данный сервис может нам предоставить небольшую, но важную информацию о местонахождении устройства, которому присваивался обнаруженный IP-адрес, названии провайдера, его контактные данные. С целью установления более подробной информации следует связаться с провайдером и получить конкретные данные. Алгоритм вышеуказанных действий выглядит следующим образом *(на примере электронной почты «mail.ru»)*:

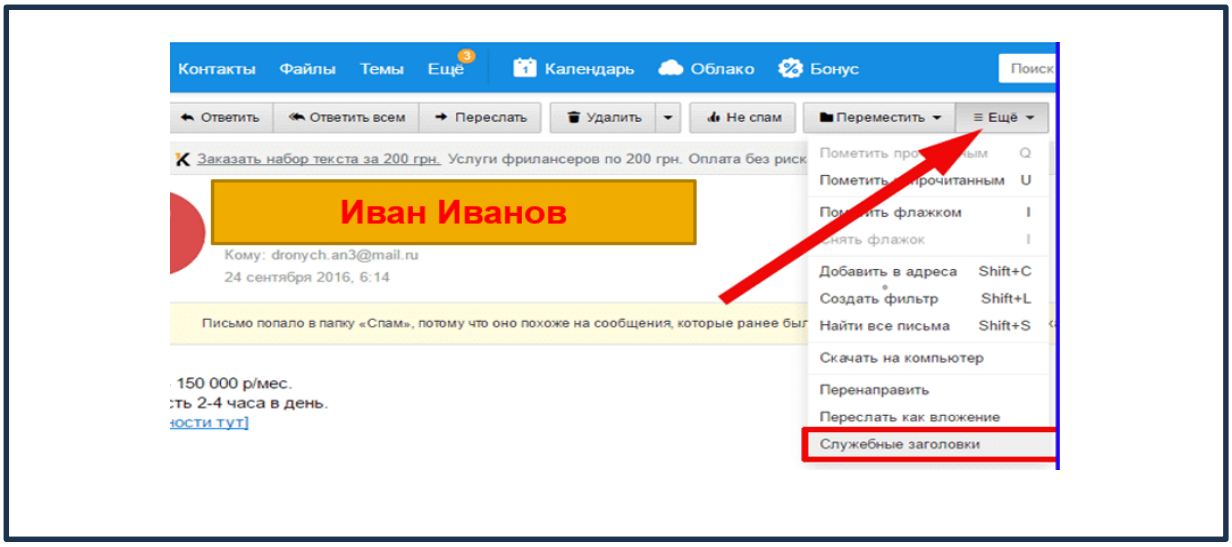
Шаг 1.



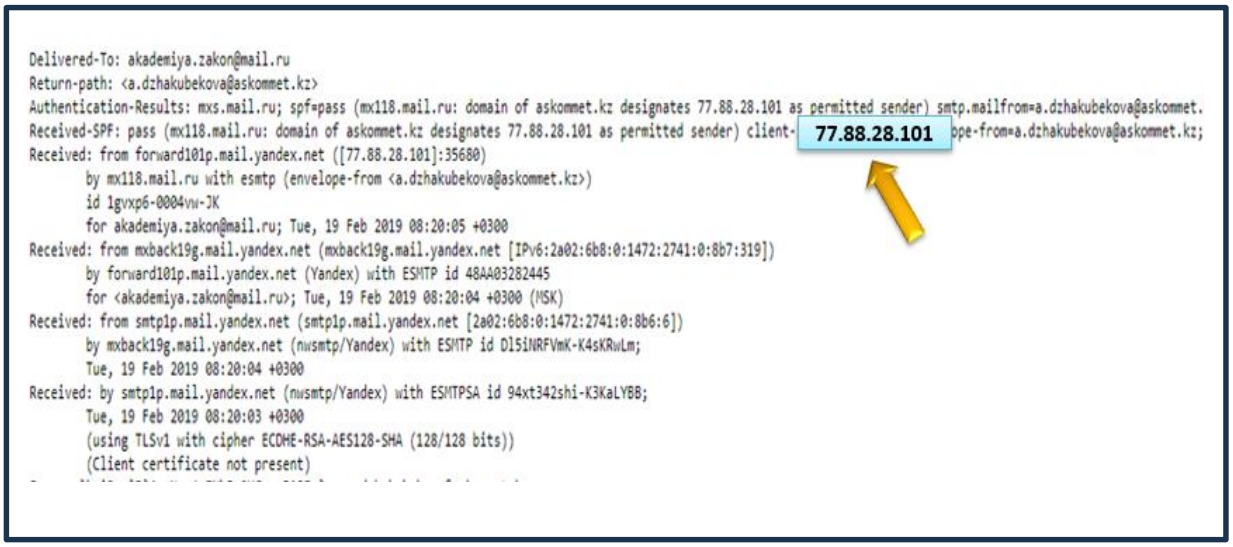
Шаг 2.



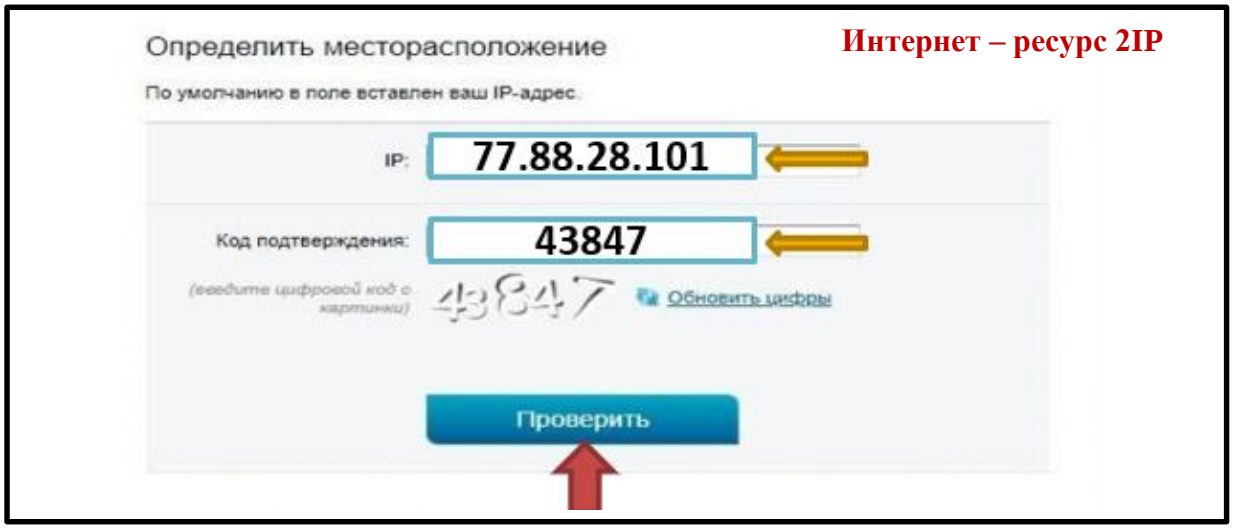
Шаг 3.



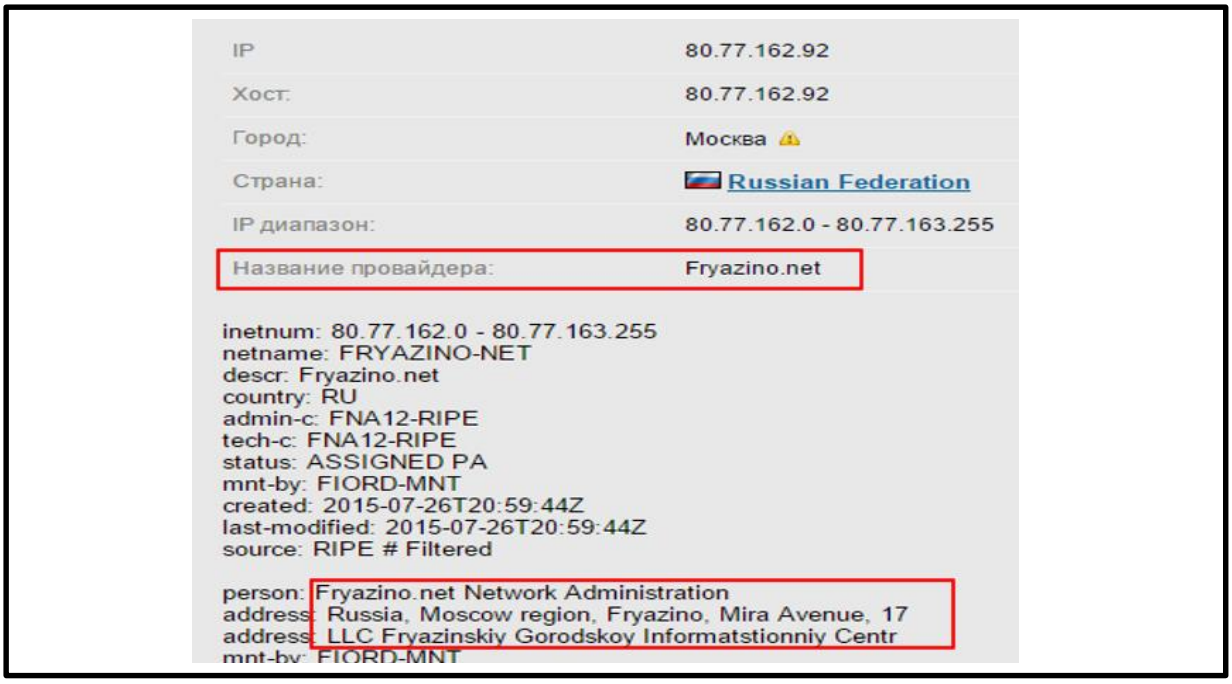
Шаг 4.



Шаг 5.



Шаг 6.



Таким образом, интернет-сервис выдает информацию о том, что IP-адрес **77.88.28.101** выдан провайдером **FRYAZINO-NET**, который осуществляет свою деятельность на территории г. Москва, РФ.

Если наш подозреваемый не использовал средства анонимизации типа VPN, то это может означает, что скрывшееся лицо сейчас находится где-то в Москве Российской Федерации. Для более точного определения местонахождения, уже нужно работать непосредственно с провайдером *(поставщиком интернет-услуг),* который может предоставить более детальную информацию.

Второй вариант. Орган уголовного преследования не располагает информацией о лицах, с кем осуществляет переписку субъект *(подозреваемый)*, скрывшийся от органов расследования, при этом требуется установить IP-адрес.

Для рассмотрения данного варианта орган расследования как минимум должен располагать информацией об электронном адресе, которым пользуется скрывшийся от следствия подозреваемый.

С помощью данного электронного адреса и специальной программы с названием **«IP-Logger»** *(находится в открытом доступе в Интернете)*, следователь может установить IP-адрес и соответственно местонахождение подозреваемого.

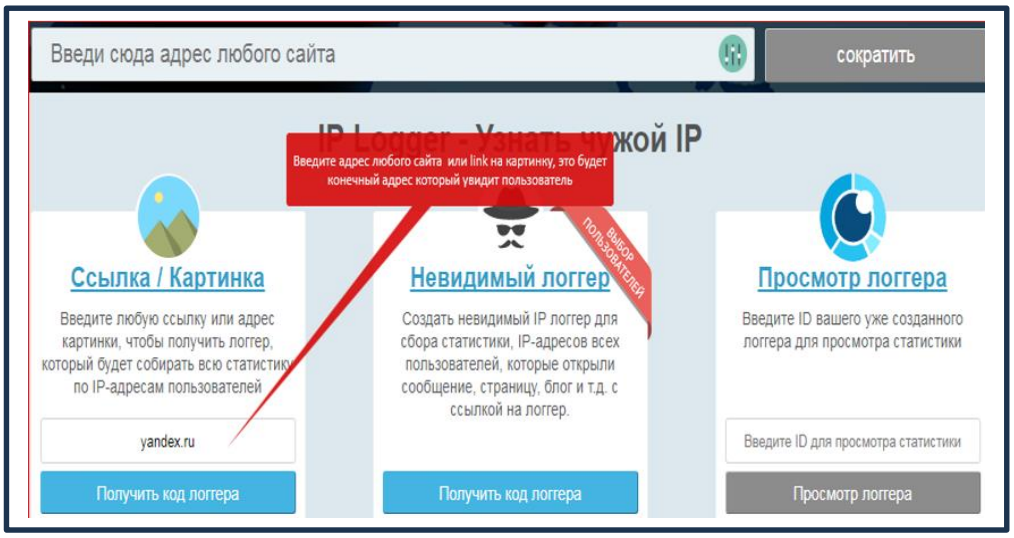
Нам необходимо найти в Интернете программу «IP-Logger» *(скачивать и устанавливать на компьютер, как приложение не требуется)*, открыть ее и в разделе «Ссылка / Картинки» написать название любого сайта, который должен открываться, когда человек кликает по интернет-ссылке. Далее нажимаем на вкладку «Получить код логгера», после чего открывается один из разделов программы, где уже сформирована короткая ссылка для сбора IP-адресов.

Следователю требуется скопировать ее и отправить со своего частного *(не рабочего)* электронного адреса на электронный адрес подозреваемого. Как

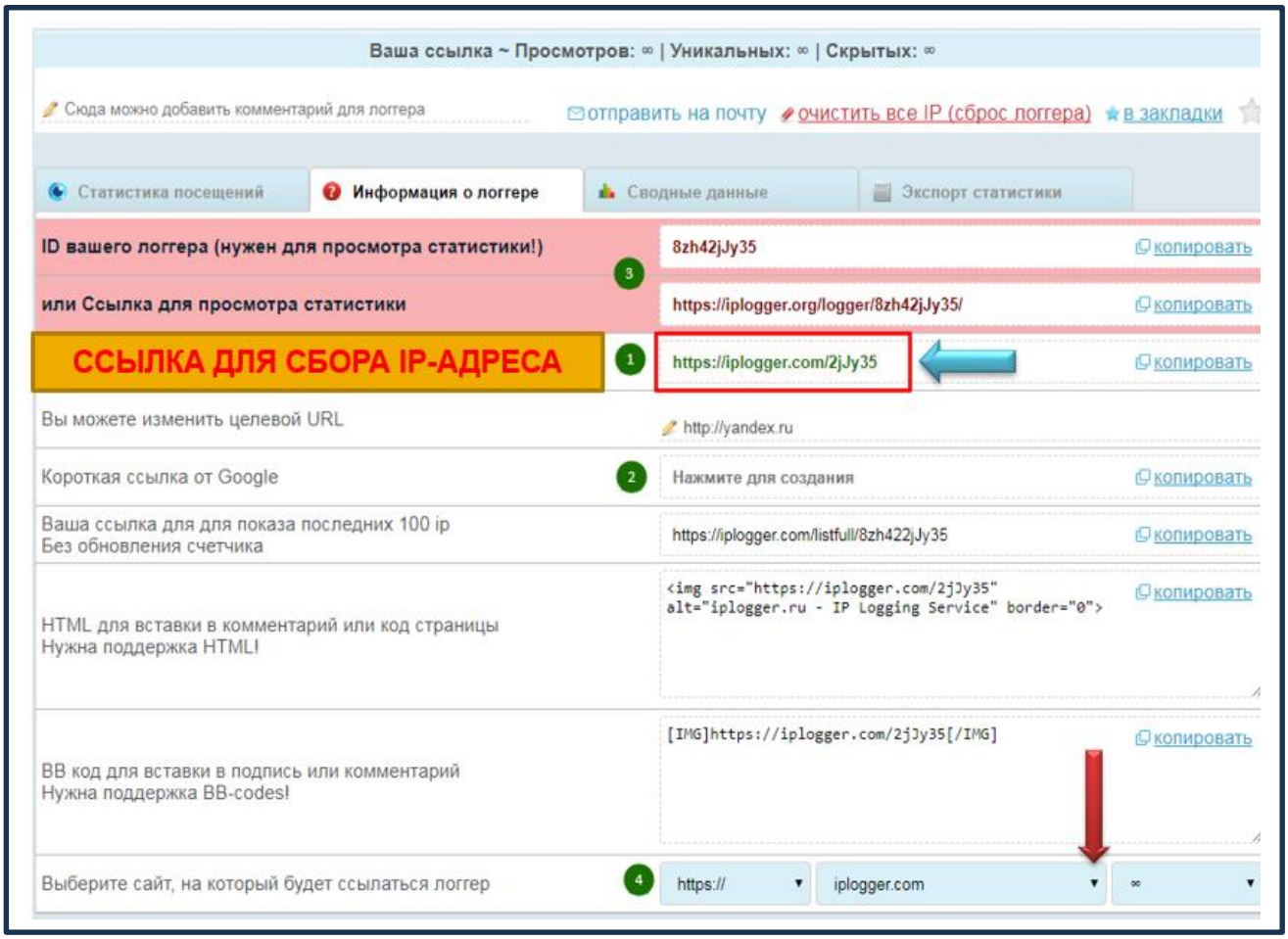
только он пройдет по данной короткой интернет-ссылке, в программе «IP-Logger» в разделе «Статистика посещений» мы можем обнаружить его IP-адрес и дополнительно: время, дату, страну, город и даже устройство, которое использовал подозреваемый.

Алгоритм действий может выглядит следующим образом:

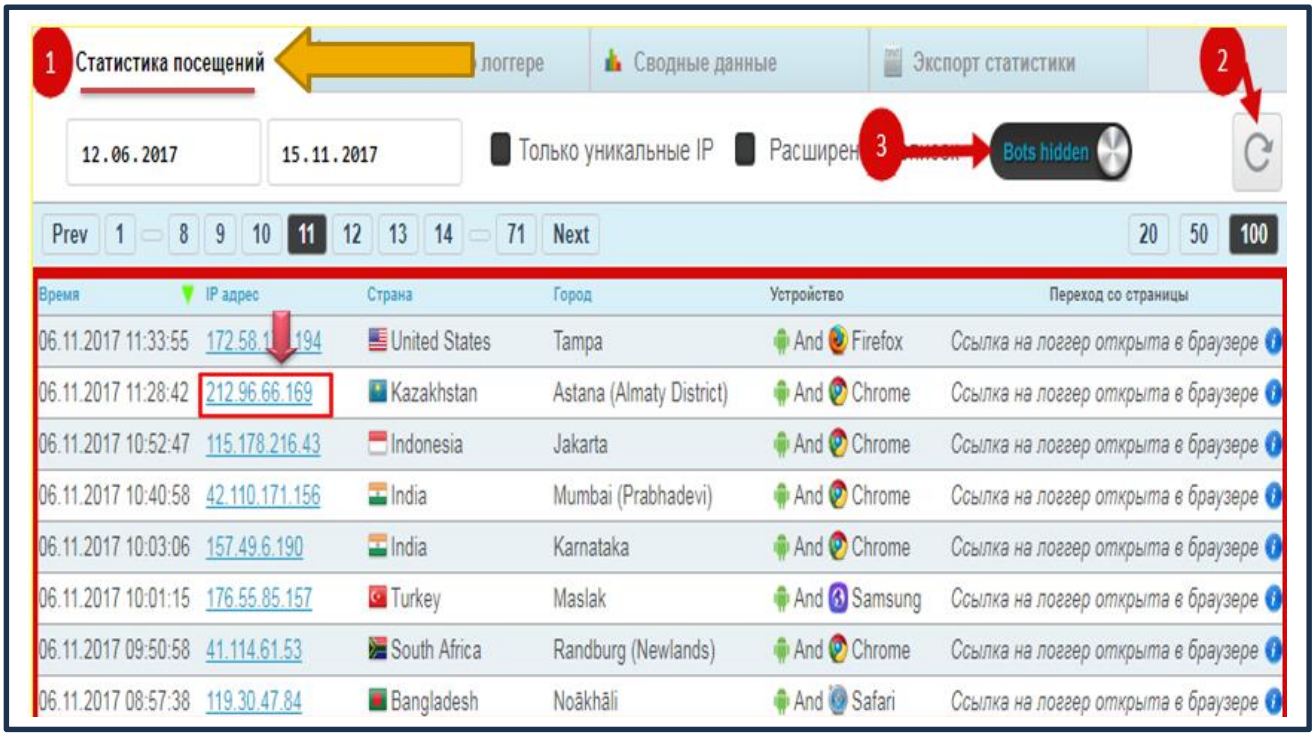
Шаг 1.



Шаг 2.



Шаг 3.



Таким образом, данная программа позволяет следователю получить информацию, необходимую для продолжения поиска *(розыска)* подозреваемого: время, дату, IP-адрес, страну, город, операционную систему и браузер.

Важно! Для того, чтобы разыскиваемый человек прошел по сформированной программой интернет-ссылке и «засветил» свой IP-адрес необходимо использовать «Социальную инженерию».

Социальная инженерия – это метод манипуляции людьми с целью получения конфиденциальной информации или выполнения определенных действий[28].

Определение геолокации устройства с помощью MAC-адреса/

Определять местонахождение человека можно также и с помощью **mac-адреса**, если информация о нем была получена органом уголовного преследования.

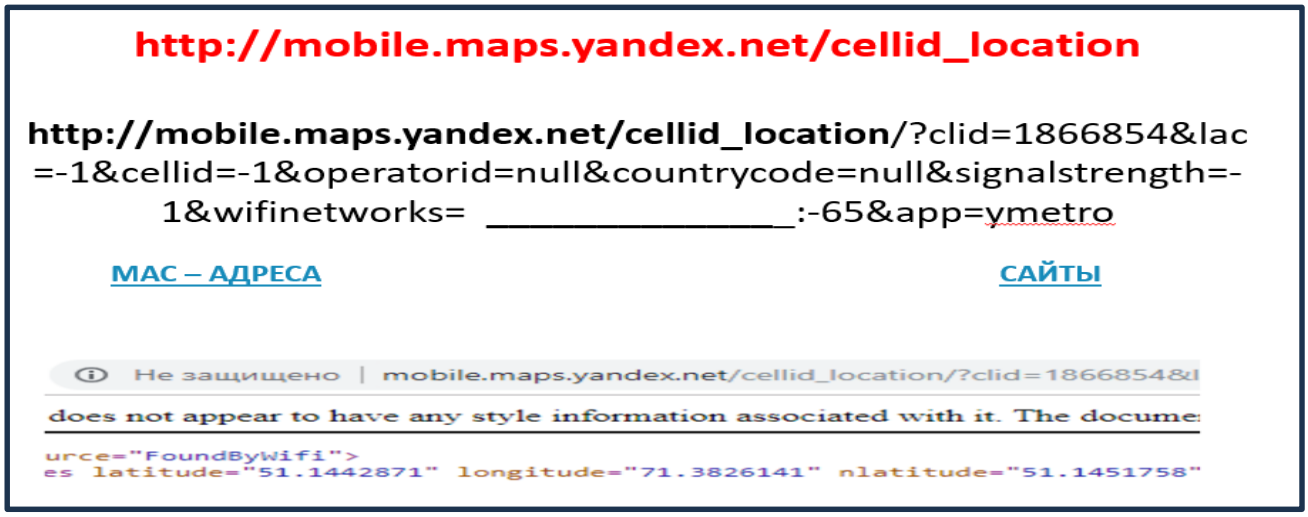
Для поиска информации о местонахождении скрывшегося лица с помощью mac-адреса используют следующие инструменты поиска:

- **mobile.maps.yandex.net;**
- **alexell.ru/network/mac-geo.**

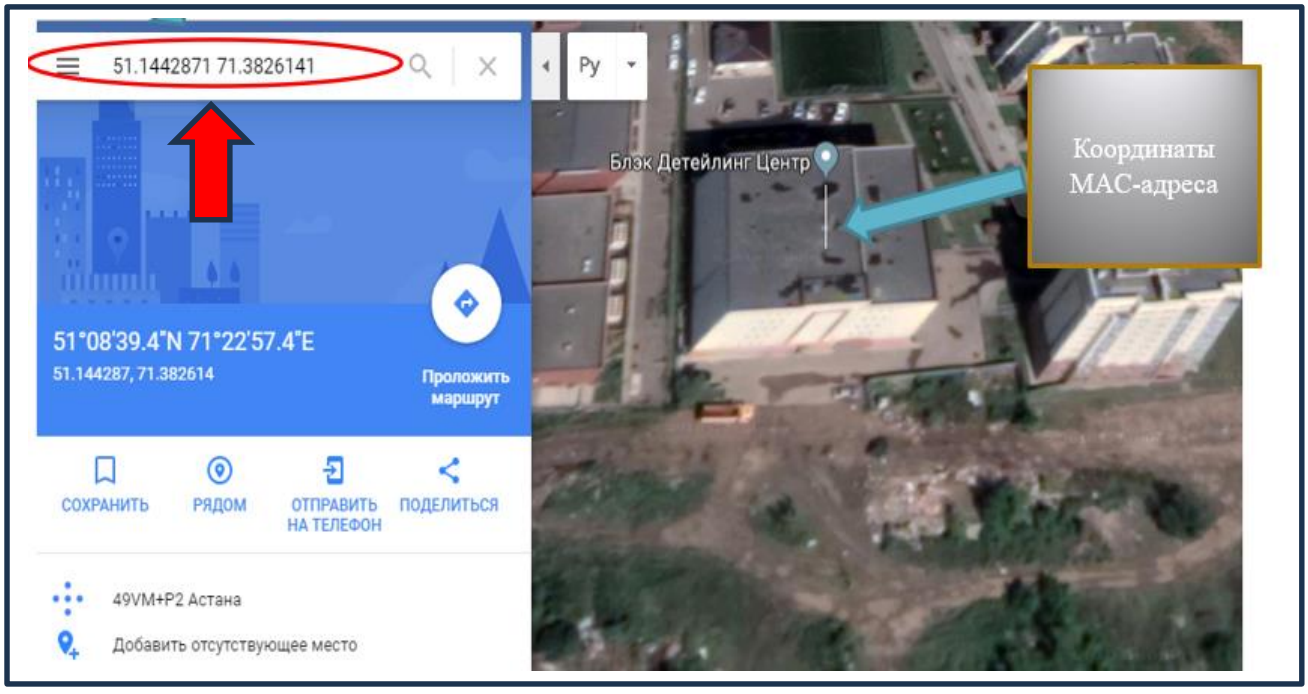
Если с помощью первого инструмента можно получить просто географические координаты устройства *(долгота и широта)*, имеющего соответствующий mac-адрес, которые в последующем необходимо вставлять в одну из интернет-карт *(yandex или google)*, то во втором инструменте уже имеется такая функция, определяющая геолокацию.

[28] http://go.microsoft.com/fwlink/p/?LinkId=255141

Следователь открывает любой из представленных инструментов и в поисковой строке вводит данные о mac-адресе, после чего запускает поисковик.



https://alexell.ru/network/mac-geo/https://alexell.ru/network/mac-geo/



Интернет – это организованная система сбора, обработки и передачи информации, основанная на большом количестве баз данных, включая поисковые системы, онлайн-каталоги, блоги, форумы, социальные сети и другие ресурсы.

Поэтому проводить поисковые (розыскные) мероприятия можно также с помощью других инструментов.

Вопросы для самоконтроля:

1) Назовите основной способ поиска киберпреступника.

2) Что такое IP-адрес?

3) Что такое MAC-адрес?

4) Назовите ключевые отличия IP-адреса от MAC-адреса.

5) Для чего предназначена программа IP-Logger?

6) Назовите интернет-сервисы по определению геолокации.

3.2. Задержание подозреваемого.

Задержание подозреваемого является одним из важных этапов досудебного расследования. Данный процесс представляет собой временное ограничение свободы человека, в отношении которого есть основания полагать, что оно совершило уголовное правонарушение. Максимальный срок задержания не может превышать 72 часа. Это время, которое отведено органу уголовного преследования для закрепления доказательств совершения уголовного правонарушения лицом, в отношении которого принято решение о его задержании.

В соответствии со статьей 128 Уголовно-процессуального кодекса Республики Казахстан, должностное лицо органа уголовного преследования вправе задержать лицо, подозреваемое в совершении преступления, за которое может быть назначено наказание в виде лишения свободы, при наличии хотя бы одного из следующих оснований:

1) когда это лицо застигнуто при совершении преступления или непосредственно после его совершения.

2) когда очевидцы (свидетели), в т.ч. потерпевшие, прямо укажут на данное лицо как на совершившее преступление либо задержат это лицо в порядке, предусмотренном статьей 130 УПК.

3) когда на этом лице или его одежде, при нем или в его жилище будут обнаружены явные следы преступления.

4) когда в полученных материалах оперативно-розыскной, контрразведывательной деятельности и (или) негласных следственных действий в отношении лица имеются достоверные данные о совершенном или готовящемся им преступлении.

Учитывая характеристики электронных доказательств, их неустойчивость и чувствительность к любым изменениям, задержание киберпреступника представляет собой сложный процесс, к которому необходимо тщательно готовится.

Подготовка к задержанию состоит из нескольких этапов:

1. Сбор информации:

а) об особенностях места проживания киберпреступника (дом или квартира);

б) о лицах, проживающих с ним (родственники, друзья, соучастники преступления);

в) о наличии домашних животных (имеются ли собаки, особенно бойцовских пород, которые могут препятствовать быстрому задержанию);

2) Планирование:

а) определение состава группы, которые будут участвовать в задержании;

б) составление детального плана действий каждого участника, включая определение времени, даты и места задержания);

3) Подготовка технических средств и программ *(ноутбука, адаптеров, жестких дисков, криминалистических программ и т.д.)*;

4) Инструктаж группы, участвующей в задержании киберпреступника *(разъяснение каждому участнику его роли и задач в задержании)*;

5) Координация их действий *(от слаженности действий каждого участника зависит успешное задержание киберпреступника и сохранение электронных доказательств)*;

6) Реализация операции по задержанию киберпреступника *(непосредственное задержание киберпреступника и сохранение электронных доказательств совершенного им преступления)*.

Важно! Любое неверное действие со стороны лиц, осуществляющих задержание киберпреступника, связанное с обеспечением безопасности электронных доказательств, будет способствовать их безвозвратной утере или приведет к невозможности их использования в доказывании его вины в совершении конкретного уголовного правонарушения.

Ниже приведены основные риски, с которыми может столкнуться следственно-оперативная граппа при задержании киберпреступника и способы их минимизации.

Первое. Уничтожение электронных доказательств.

В случае любой угрозы, связанной с задержанием и арестом, подозреваемый будет попытаться каким-либо способом уничтожить все цифровые следы своих противоправных действий, которые будут свидетельствовать о его причастности к тому или иному преступлению.

Поэтому, следователь должен иметь четкий и детальный план действий, с которым ознакомить каждого участника следственно-оперативной группы, задействованного в задержании киберпреступника, чтобы свести к минимуму время между принятием решения о задержании и его фактическим

осуществлением, а также предотвратить уничтожение электронных доказательств.

Второе. Сопротивление при задержании.

Киберпреступники могут владеть приемами самообороны или рядом с ними могут оказаться люди из охранного агентства, обладающие знаниями в области физической безопасности личности, которые будут оказывать сопротивление при задержании.

В связи с чем следователь должен провести предварительный анализ рисков и разработать стратегию действий для минимизации физической угрозы жизни и здоровью сотрудников, участвующих в задержании.

Третье. Юридические аспекты.

Иногда для задержания киберпреступника необходимо иметь разрешительные документы (санкцию суда);

Четвертое. Отсутствие технических средств.

Следователь должен быть готовым к тому, что объем информации, которые необходимо изъять с компьютера киберпреступника может превышать объем памяти жесткого диска, используемого для сохранения электронных доказательств.

Поэтому он должен иметь несколько запасных жестких дисков для сохранения всех электронных доказательств.

Отсутствие предварительного анализа возможных рисков скорее всего приведет к провалу операции по задержанию киберпреступника, который сможет уничтожить электронные доказательства своего преступления или заблокировать доступ к ним на неопределенное время, что будет препятствовать расследованию уголовного дела.

Вопросы для самоконтроля:

1) Из каких этапов состоит процесс подготовки к задержанию киберпреступника?

2) Назовите риски, с которыми может столкнуться СОГ при задержании киберпреступника.

3) Что включает в себя этап «Сбор информации»?

4) Что включает в себя этап «Подготовка технических средств и программ»?

3.3. Особенности допроса подозреваемого.

Допрос подозреваемого в киберпреступлении представляет собой следственное действие, направленное на выяснение всех обстоятельств, совершенного им уголовного правонарушения, связанного с использованием информационных технологий.

Одним из ключевых аспектов успешного проведения данного вида допроса является подготовка следователя к его проведению, которая включает в себя:

- **изучение** терминологии, используемой киберпреступниками; методов совершения подозреваемым киберпреступления; цели и задач используемых киберпреступниками программ и средств для совершения преступления *(например, вредоносного программного обеспечения)*; заключения судебной экспертизы; личности киберпреступника;

- **выяснение** мотива и цели преступления.

Перед допросом следователь составляет перечень вопросов, исходя из полученной информации, накопленной при расследовании уголовного дела *(заключение судебного эксперта, специалиста, собранных и проанализированных электронных доказательств и т.д.)*.

К участию в допросе могут быть привлечены IT-специалисты, которые могут пояснить суть технических деталей, о которых сообщает киберпреступник, а также помочь следователю правильно сформулировать вопрос подозреваемому.

Важно! Нельзя подозреваемым давать возможность прикасаться к изъятой компьютерной технике для исключения возможности уничтожения электронных доказательств.

По мнению многих зарубежных практиков *(следователей)*, допрос подозреваемого в первые минуты задержания наиболее эффективный и играет решающую роль в раскрытии преступления, сборе и фиксации цифровых следов.

Это связано с тем, что он может находиться в состоянии стресса, связанного с его задержанием.

В большинстве случаев такой допрос позволяет получить пароли от зашифрованных файлов, папок, дисков, криптоконтейнеров, логинов и паролей от рабочей станции *(стационарный компьютер, ноутбук)*, на которой работал киберпреступник.

В последующие дни после задержания, подозреваемый может давать ложные показания с целью избежания ответственности. Поэтому допрос требует тщательной подготовки.

На эффективность допроса также могут оказать влияние и другие факторы.

Например, киберпреступником может овладеть желание продемонстрировать свои технические знания, и он сам расскажет о методе совершения им преступления, чтобы заявить о себе общественности или наоборот он может попытаться скрыть определенные аспекты своих действий с целью избежания ответственности.

Понимание психологических особенностей киберпреступников также требует подготовки следователя.

Таким образом, успех и эффективность допроса подозреваемого в киберпреступлении будет зависеть не только от профессиональной технической компетентности следователя, но и понимания психологических аспектов, которые можно использовать во время допроса.

Ниже представлены рекомендации для следователя по проведению допроса подозреваемого в совершении киберпреступления:

1) Установление контакта с подозреваемым *(психологические методы, такие как сопереживание и непредвзятый тон, помогают создать комфортную обстановку и расположить подозреваемого к диалогу)*;

2) Активное слушание *(важно не перебивать подозреваемого и предоставить ему возможность самому рассказать о событиях преступления. Это не только укрепляет взаимодействие, но и может предоставить полезную информацию для дальнейших вопросов)*;

3) Использование невербальных сигналов *(жесты, мимика, и тон голоса, могут выявить эмоциональные реакции подозреваемого, что будет способствовать эффективности допроса)*;

4) Смена темы *(изменение темы разговора может быть использовано для оценки реакции подозреваемого, а также способствовать более открытому выражению мыслей)*;

5) Поддержка подозреваемого *(создание впечатления поддержки и сотрудничества может помочь подозреваемому чувствовать себя более комфортно. Это может снизить напряженность и способствовать более открытому обмену информацией)*.

6) Предъявление доказательств *(такой подход будет иметь эффект тогда, когда подозреваемый отказывается говорить или пытается давать ложные показания. Демонстрация доказательств и краткое их описание будет влиять на готовность к диалогу и сотрудничеству со следствием)*.

Указанный перечень рекомендаций не является исчерпывающим и может быть расширен следователем с учетом многих факторов, в том числе личности киберпреступника, особенностей совершенного им преступления, готовности к сотрудничеству и т.д.

Вопросы для самоконтроля:

1) Что включает в себя подготовка к допросу подозреваемого?

2) От чего зависит успех и эффективность допроса киберпреступника?

3) Назовите основные рекомендации по проведению допроса киберпреступника.

ЗАКЛЮЧЕНИЕ

Данное учебное пособие представляет собой структурированный и всесторонний подход к общему пониманию и освоению комплексной темы расследования киберпреступлений.

В представленной работе авторы раскрыли все этапы расследования: от регистрации заявления о киберпреступлении до задержания и допроса киберпреступника, совершившего уголовное правонарушение в сфере информационно-коммуникационных технологий.

В нем содержатся полезные практические советы, как для следователя, так и специалиста-криминалиста по осмотру места преступления и компьютерной технике, поиску, обнаружению, изъятию, сохранению и транспортировке электронных доказательств, допросу потерпевшего и подозреваемого, назначению судебной экспертизы.

Подробно рассмотрены вопросы использования специальных знаний в расследовании, особенно в использовании программного обеспечения по поиску и изъятию электронных доказательств. Приведены в качестве примеров отдельные компьютерные программы по снятию образов оперативной памяти и жесткого диска.

Авторы составили пошаговый алгоритм действий по применению технологии хеширования для обеспечения достоверности полученных электронных доказательств.

Исключительную значимость приобретает материал технического содержания, где детально описываются устройства и технологии, скрывающие цифровые следы, однако имеющие важное значение в расследовании киберпреступлений.

Раскрыта тема международного сотрудничества с отражением проблемных вопросов взаимодействия правоохранительных органов с поставщиками услуг по сохранению и получению электронных доказательств.

Вся информация, которая изложена в учебном пособии представлена в удобной и доступной форме, что помогает лучше усвоить весь учебный материал.

Таким образом, данное учебное пособие предоставляет не только базовые знания по расследованию киберпреступлений, но и обеспечивает применимость этих знаний на практике в современных условиях работы следователей.

Приложение № 1

ТИПОВЫЕ ЗАПРОСЫ В ОТНОШЕНИИ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ[29]

Вариант 1

	Укажите ФИО лица, направляющего запрос Укажите название государственного / судебного органа Укажите номер телефона с международным кодом Укажите официальный адрес электронной почты
ЗАПРОС ОБ ОБЕСПЕЧЕНИИ СОХРАННОСТИ в адрес (УКАЖИТЕ НАЗВАНИЕ ПУ)	
Введение	Я *(укажите ФИО, должность, номер пропуска или иной идентификационный номер сотрудника правоохранительного органа, прокуратуры или судебного органа, направляющего запрос)* обладаю необходимыми правовыми полномочиями для подачи настоящего запроса, и я расследую следующие преступления: *перечислите уголовные преступления и укажите, каким нормам законодательства они противоречат.*
Идентификатор учетной записи	В отношении обеспечения сохранности *(укажите идентификатор учетной записи, например, имя пользователя, URL или иной идентификатор, обозначенный ПУ)*.
Указание данных учетной записи, сохранность которых должна быть обеспечена	Я прошу обеспечить сохранность доказательств (укажите, какой именно информации - ОИА, информации о содержании (или всего перечисленного), начиная с даты получения настоящего запроса, поскольку эта информация связана с расследованием (укажите каким образом ОИА, информация о трафике или информация о содержании (или все перечисленное) связаны с расследованием (например, объект расследования)).
Указание об уведомлении пользователя о запросе	**НЕ ИНФОРМИРУЙТЕ ПОЛЬЗОВАТЕЛЯ УЧЕТНОЙ ЗАПИСИ О НАШЕМ ЗАПРОСЕ!** Я прошу Вас не раскрывать информацию о существовании настоящего запроса абоненту или какому-либо иному лицу, кроме тех, которым необходимо ее знать для выполнения настоящего запроса. Если выполнение настоящего запроса может привести к постоянному или временному прекращению обслуживания учетной (ых) записи (ей) или иным образом предупредить пользователя учетной (ых) записи (ей) о Ваших действиях по обеспечению сохранности указанной ниже информации, прошу Вас связаться со мной в кратчайшие сроки, не предпринимать до этого никаких действий.
Указание о ссылочном номере сохранения и сроке его действия	Прошу направить на мой адрес электронной почты ссылочный номер сохранения и дату истечения срока действия распоряжения об обеспечении сохранности.
Заключение	Я подтверждаю, что обладаю необходимыми правовыми полномочиями для подачи настоящего запроса и по имеющимся у меня сведениям его содержание является правдивым.
Дата и время	Если потребуется какая-либо дополнительная информация, прошу связаться со мной по указанному номеру телефона или адресу электронной почты. Укажите дату и время запроса. Добавьте ФИО и подпись сотрудника, а также официальную печать государственного / судебного органа, направившего запрос.

[29] Практическое руководство по порядку запроса электронных доказательств из других стран. Управление Организации Объединенных Наций по наркотикам и преступности.

Вариант 2

<table>
<tr><td colspan="2">Укажите ФИО лица, направляющего запрос
Укажите название государственного / судебного органа
Укажите номер телефона с международным кодом
Укажите официальный адрес электронной почты</td></tr>
<tr><td colspan="2">ПРЯМОЙ ЗАПРОС в адрес (НАЗВАНИЕ ПУ) на ДОБРОВОЛЬНОЕ РАСКРЫТИЕ ИНФОРМАЦИИ</td></tr>
<tr><td>Введение</td><td>Я (укажите ФИО, должность, номер пропуска или иной идентификационный номер сотрудника правоохранительного органа, прокуратуры или судебного органа, направляющего запрос) обладаю необходимыми правовыми полномочиями для подачи настоящего запроса, и я расследую следующие преступления: перечислите уголовные преступления и укажите, каким нормам законодательства они противоречат.</td></tr>
<tr><td>Разрешение</td><td>Укажите ФИО и должность (например, прокурор/следственный судья или руководитель). Приложите разрешающий документ (например, санкцию суда о предоставлении ОИА и (или) информации о трафике). Проверьте необходимость в направлении разрешающих документов в адрес ПУ. Направьте прямой запрос в адрес ПУ (укажите идентификатор учетной записи).</td></tr>
<tr><td>Название и контактные данные ПУ</td><td>В отношении добровольного раскрытия данных (укажите идентификатор учетной записи)</td></tr>
<tr><td>Указание запрашиваемых данных учетной записи</td><td>Какая информация Вам необходима: IP-адрес, номер телефона, адрес электронной почты, номер IMEI, MAC-адрес, лицо (лица), данные которого (ых) запрашиваются, название сервиса.</td></tr>
<tr><td>Указание конкретных запрашиваемых данных, связанных с расследованием и временного интервала</td><td>Указанная учетная запись связана с расследованием (укажите, каким образом ОИА и (или) информация о трафике связана с расследованием).
Основная информация об абоненте, в том числе (отметьте и заполните в соответствующих случаях):
- ФИО, адрес, дата рождения, контактная информация, адрес электронной почты, номер телефона и прочая информация, касающаяся личности пользователя/абонента;
- дата и время первой регистрации, тип регистрации, копия договора, средства подтверждения личности в момент регистрации, копии документов, представленных абонентов, тип услуги, включая идентификатор, IP-адрес, номер SIM- карты, MAC-адрес и связанное (ые) устройство (а);
- информация профиля (имя пользователя, фото профиля);
- данные о проверке использования услуги, такие как альтернативный адрес электронной почты, предоставленный пользователем / абонентом;
- данные дебетовой или кредитной карты (предоставленные пользователем для целей выставления).
Информация о трафике, в том числе:
- Интернет (отметьте и заполните в соответствующих случаях);
- записи/журналы IP-соединений для целей идентификации;
- маршрутная информация (IP-адрес источника, IP-адрес (а) пункта, назначения, номер (а) порта(ов), браузер, информация из заголовка сообщения электронной почты, идентификатор сообщения);
- идентификатор базовой станции, включая сведения о географическом положении (координаты X/Y) на момент начала и окончания соединения;
- объем данных;</td></tr>
</table>

	- *веб-хостинг* (отметьте и заполните в соответствующих случаях); - *файлы регистрации, инциденты, история покупок, прочая информация о трафике*, в том числе: история расходования предоплаченного остатка; список контактов; временной интервал *(укажите временной интервал, за который запрашивается информация и обоснуйте со ссылкой на расследования).*
Указание контактных данных для направления информации.	Ответы следует направлять электронной почтой по адресу *(укажите адрес электронной почты для передачи запрошенных электронных доказательств и срок направления ответа)*.
Указание о не уведомлении пользователя о запросе	**НЕ ИНФОРМИРУЙТЕ ПОЛЬЗОВАТЕЛЯ УЧЕТНОЙ ЗАПИСИ О НАШЕМ ЗАПРОСЕ.** Если сохранить конфиденциальность, как описано выше, не представляется возможным, прошу уведомить меня до исполнения настоящего запроса *(укажите конкретные причины для не уведомления пользователя, например, продолжающееся расследование, т.е. предупреждение подозреваемого приведет к уничтожению улик и избежание возможного ареста).*
Заявление или аффидевит для подтверждения подлинности запрашиваемых данных	Мы просим представить заявление или аффидевит, подтверждающие подлинность запрашиваемых электронных доказательств, чтобы подтвердить, что вы являетесь их хранителем *(приложите типовую форму заявления или аффидевита, чтобы помочь составить его в приемлемом формате)*. Обратите внимание, что некоторые ПУ могут не заполнять такую форму, поскольку их данные предусматривают само аутентификацию).
Заключение	Я подтверждаю, что обладаю необходимыми правовыми полномочиями для подачи настоящего запроса и по имеющимся у меня сведениям его содержание является правдивым. Если потребуется какая-либо дополнительная информация, прошу связаться со мной по указанному номеру телефона или адресу электронной почты. Добавьте ФИО, дату и официальную печать государственного органа, направившего запрос, а также подпись предоставившего разрешение сотрудника/работника прокуратуры или судебного органа / подтверждающую подпись старшего сотрудника в случае запроса правоохранительного органа.

Вариант 3

Укажите адрес центрального органа запрашиваемого государства Укажите ссылочный номер Уважаемые господа! Запрос об оказании правовой помощи: (укажите название операции) Укажите ФИО обвиняемого или подозреваемого (ых)	
В ОТНОШЕНИИ ХРАНЯЩИХСЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ	
Срочность	Уточните, является ли запрос действительно срочным *(злоупотребление ссылками на срочность может привести к затруднениям и задержкам в рассмотрении других дел)*. Если это так, укажите причины срочности *(например, угроза для жизни или угроза причинения серьезного физического вреда).*
Основание запроса	Я имею честь обратиться к Вам с запросом об оказании помощи в соответствии с положениями *(укажите соответствующий Договор о взаимной правовой помощи по уголовным делам).*
	Во избежание причинения ущерба расследованию я прошу компетентные органы в Вашей стране не уведомлять лицо (включая

<table>
<tr><td>Конфиденциальность</td><td>любой из объектов) о существовании и содержании настоящего запроса об оказании взаимной правовой помощи, а также о любых действиях, предпринимаемых в ответ на него. Я также прошу принять иные меры к обеспечению конфиденциальности.
Если сохранить конфиденциальность, как описано выше, не представляется возможным, прошу уведомить меня до исполнения настоящего запроса об оказании взаимной правовой помощи.</td></tr>
<tr><td>Цель запроса</td><td>Это запрос о получении доказательств (укажите тип доказательств, например, содержание электронных писем и поставщика услуг) для использования в рамках судебного преследования (включая любые связанные разбирательства по вопросам наложения ареста на имущество, конфискации имущества и обеспечения принудительного исполнения, а также любые связанные с ними вспомогательные производства) в отношении следующего объекта.</td></tr>
<tr><td colspan="2">Если известны подозреваемые/обвиняемые, укажите следующее:
<table>
<tr><th>ОБЪЕКТ</th><th>ДАТА РОЖДЕНИЯ</th><th>МЕСТО РОЖДЕНИЯ</th><th>ГРАЖДАНСТВО</th><th>АДРЕС</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td colspan="2">Если известен только IP-адрес сервера, укажите следующее:
<table>
<tr><th>IP-АДРЕС</th><th>ХОСТИНГОВАЯ КОМПАНИЯ (название и адрес)</th></tr>
<tr><td></td><td></td></tr>
</table></td></tr>
<tr><td>Сводная информация о фактах и об истории разбирательств</td><td>Представьте хронологию расследования и краткую информацию по расследуемым преступлениям, за совершение которых осуществляется судебное преследование в отношении каждого объекта.</td></tr>
<tr><td>Обеспечение сохранности</td><td>Запрос об обеспечении сохранности в отношении соответствующей учетной записи был составлен (укажите соответствующий правоохранительный орган) и направлен (укажите дату), срок действия - до (укажите дату), ссылочный номер – (укажите ссылочный номер).</td></tr>
<tr><td>Укажите во всех запросах</td><td>1. Направляются такие-то запросы, проводятся беседы с такими-то лицами и истребуются такие-то вещественные доказательства.
2. Любые записи представляются в качестве вещественных доказательств в любых заявлениях вместе с пояснениями в отношении технических терминов, используемых в таких записях.
3. Любая информация, хранящаяся на компьютере в любой форме, будет сохранена и защищена от несанкционированного внешнего воздействия, а также будет предоставлена следователям (укажите название ведомства, ведущего расследование / ФИО следственного судьи / ФИО допрашивающего судьи) для использования в ходе любого последующего судебного разбирательства.
4. Любые материалы, предоставленные мне в соответствии с настоящим запросом могут быть использованы в ходе любого уголовного преследования или иных судебных производств, связанных с этим делом, включая разбирательства по вопросам наложения ареста на имущество или конфискации имущества, а также любые связанные с ними вспомогательные производства, включая разбирательства касающиеся любых нарушений распоряжений судом, изменения, пересмотра и обеспечения принудительного исполнения таковых.
5. Направляются запросы и предоставляются разрешения в отношении оригиналов или подписанных и заверенных копий любых представленных заявлений, а также документов, полученных в ходе сбора информации по запросам на их вызов (укажите запрашивающее государство) для использования в рамках любых уголовных производств, судебных разбирательств, а также разбирательств по вопросу конфискации имущества и обеспечения принудительного исполнения.</td></tr>
</table>

	6. При необходимости укажите: следователю предоставляется разрешение приехать и присутствовать при анализе доказательств, полученных от поставщика услуг, до их передачи.
Взаимность в процессуальном законодательстве (укажите только при наличии взаимности в законодательстве)	Я подтверждаю, что запрашиваемая помощь, обозначенная выше, согласно текущему законодательству (укажите запрашивающее государство) может быть получена по аналогичному запросу об оказании такой помощи, направленному в государственные органы (укажите запрашивающее государство).
Передача электронных доказательств	Прошу Вас направлять любые электронные доказательства мне по вышеуказанному адресу, а также сообщить, если Вы хотели бы получить назад любые документы по окончании производства в (укажите запрашивающее государство).
Контактные данные	Надлежащим контактным лицом в случае возникновения любых вопросов относительно настоящего запроса является *(укажите ФИО по делу/следственного судьи / допрашивающего судьи, в зависимости от конкретного случая).* ФИО, адрес, эл. почта, прямой номер телефона: + (укажите), номер факса. Я буду благодарен, если Вы сможете держать (укажите ФИО работника прокуратуры/следственного или допрашивающего судьи) и следователя в курсе о ходе выполнения настоящего запроса. Заранее благодарю Вас за Ваш ценный вклад и помощь по этому делу. С уважением, (ФИО)

Вариант 4

Укажите адрес центрального органа запрашиваемого государства Укажите ссылочный номер Уважаемые господа! Запрос об оказании правовой помощи: (укажите название операции) Укажите ФИО обвиняемого или подозреваемого (ых)	
В ОТНОШЕНИИ СБОРА ИНФОРМАЦИИ О ТРАФИКЕ ИЛИ ИНФОРМАЦИИ О СОДЕРЖАНИИ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ	
Срочность	Уточните, является ли запрос действительно срочным *(злоупотребление ссылками на срочность может привести к затруднениям и задержкам в рассмотрении других дел)*. Если это так, укажите причины срочности *(например, угроза для жизни или угроза причинения серьезного физического вреда)*.
Основание запроса	Я имею честь обратиться к Вам с запросом об оказании помощи в соответствии с положениями *(укажите соответствующий Договор о взаимной правовой помощи по уголовным делам).*
Конфиденциальность	Во избежание причинения ущерба расследованию я прошу компетентные органы в Вашей стране не уведомлять лицо (включая любой из объектов) о существовании и содержании настоящего запроса об оказании взаимной правовой помощи, а также о любых действиях, предпринимаемых в ответ на него. Я также прошу принять меры к обеспечению того, чтобы ни одно из лиц, у которых запрашиваются доказательства, не уведомляли об этом никакие другие лица. Если сохранить конфиденциальность, как описано выше, не представляется возможным, прошу уведомить меня до исполнения настоящего запроса об оказании взаимной правовой помощи.
Цель запроса	Это запрос о получении доказательств *(укажите тип доказательств, например, содержание электронных писем и поставщика услуг)* для использования в рамках судебного преследования *(включая любые*

<table>
<tr><td></td><td>связанные разбирательства по вопросам наложения ареста на имущество, конфискации имущества и обеспечения принудительного исполнения, а также любые связанные с ними вспомогательные производства) в отношении следующего объекта.</td></tr>
<tr><td colspan="2">Если известны подозреваемые/обвиняемый, укажите следующее:
<table>
<tr><th>ОБЪЕКТ</th><th>ДАТА РОЖДЕНИЯ</th><th>МЕСТО РОЖДЕНИЯ</th><th>ГРАЖДАНСТВО</th><th>АДРЕС</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td colspan="2">Если известен только адрес электронной почты или имя пользователя в социальной сети, укажите следующее:
<table>
<tr><th>АДРЕС ЭЛЕКТРОННОЙ ПОЧТЫ ИЛИ ИМЯ ПОЛЬЗОВАТЕЛЯ В СОЦИАЛЬНОЙ СЕТИ</th><th>ПОСТАВЩИК УСЛУГ (название и адрес)</th></tr>
<tr><td></td><td></td></tr>
</table></td></tr>
<tr><td>Сводная информация о фактах и об истории разбирательств</td><td>Пример: Г-н X создал поддельную личность под именем «г-н Н» и считается частью запрещённой организации «Война со всеми». Также можно доказать, что г-н X от имени «г-на Н» создал три веб-сайта в Интернете, содержащие джихадистские видеоролики, снятые во время военных действий на территории Сирийской Арабской Республики.
Г-н X использовал ноутбук, принадлежащий компании, в которой он работал. Полиция обнаружила учетную запись электронной почты на компьютере, связанном с г-ном X, посредством вручения национального судебного приказа и получения следующей основной информации об абоненте (ФИО и адрес).
Соответствующий адрес электронного почты был использован в качестве контактного при создании вышеуказанных веб-сайтов.
Получатель электронного письма от г-на X сообщила полиции, что он отправил ей электронное письмо с призывом отправиться в Сирийскую Арабскую Республику и «привезти джихад домой» и копии электронных писем от г-на X, отправленных с адреса.
Известно, что г-н X использует интернет-кафе Web and Coffee в Мейдаптауне, территория которого контролируется полицией Мейдаптауна. Проведя наблюдение по мониторам, сотрудники полиции увидели, как X осуществляет доступ к джихадистским видеороликам, что подтверждается показаниями владельца интернет-кафе Web and Coffee.
Следствие считает, что отслеживание в режиме реального времени информации о трафике учетной записи от г-на X поможет в дознании в части установления лиц, которым г-н X отправляет ссылки на джихадисткие веб-сайты, которые используются для популяризации войны на территории Сирийской Арабской Республики. Отслеживание в режиме реального времени содержания сообщений учетной записи также покажет с кем работает г-н X, а также обсуждал ли он и другие лица свои планы о том, чтобы привезти джихад домой. При необходимости укажите национальное распоряжение суда о предоставлении информации и(или) соответствующие решения других компетентных национальных органов.</td></tr>
<tr><td>Запрашиваемая помощь и требуемый формат доказательств</td><td>После получения соответствующего ордера, распоряжения суда или иного распоряжения, осуществлять мониторинг следующей учетной записи (укажите идентификатор учетной записи, например, x@SP.com), зарегистрированный в (укажите название и адрес ПУ для вручения любого ордера или иного распоряжения суда), а также собирать всю информацию о трафике или информацию о содержании, поступающую в адрес указанной учетной записи или исходящую от нее, с (укажите дату) по (укажите дату).</td></tr>
<tr><td>Взаимность в процессуальном</td><td>Я подтверждаю, что запрашиваемая помощь, обозначенная выше, согласно текущему законодательству (укажите запрашивающее</td></tr>
</table>

законодательстве	государство), может быть получена по аналогичному запросу об оказании такой помощи, направленному в государственные органы (укажите запрашивающее государство).
Передача электронных доказательств	Прошу Вас направлять любые электронные доказательства мне по вышеуказанному адресу, а также сообщить, если Вы хотели бы получить назад любые документы по окончании производства в (укажите запрашивающее государство).
Контактные данные	Надлежащим контактным лицом в случае возникновения любых вопросов относительно настоящего запроса является *(укажите ФИО по делу/следственного судьи / допрашивающего судьи, в зависимости от конкретного случая).* ФИО, адрес, эл. почта, прямой номер телефона: + (укажите), номер факса. Я буду благодарен, если Вы сможете держать (укажите ФИО работника прокуратуры/следственного или допрашивающего судьи) и следователя в курсе о ходе выполнения настоящего запроса. Заранее благодарю Вас за Ваш ценный вклад и помощь по этому делу. С уважением, (ФИО)

Приложение № 2

СПИСОК ПРОВАЙДЕРОВ УСЛУГ[30]

1	ADOBE	BOOKING.COM	**GOOGLE**
2	AIRBNB	BOX	HOOP MESSENGER
3	ALIBABA	BUMBLE	HUSHMAIL
4	AMAZON	CLOUDFLARE	JUSTPASTE.IT
5	4CHAN	BLACKBERRY	GOFUDME.COM
6	AMINO	DISCORD	KIK
7	APPLE	DROPBOX	LINE
8	ARCHIVE.ORG	EBAY	LINKEDIN
9	ASKFM	**FACEBOOK**	MEETME
10	ATLASSIAN	**INSTAGRAM**	MEGA
11	BAAZ	GAB	MEWE
12	BADOO	GODADDY	MICROSOFT
13	NETFLIX	SNAPCHAT	UBER
14	OMEGLE	SOUNDCLOUD	VIBER
15	OVH	SUPESPOT	VIMEO
16	PAYPAL	TAM TAM	WECHAT
17	MOCOSPACE	SKYPE	TWITTER
18	PINTEREST	**TELEGRAM**	**WHATSAPP**
19	PROTONMAIL	TEXTNOW	WICKR
20	PUBLIC INTEREST REGISTRY	THREEMA	WIKIMEDIA FOUNDATION
21	REDDIT	**TIKTOK**	WORDPRESS
22	ROCKET.CHAT	TINDER	YAHOO!
23	SHOPIFY	TUMBLR	ZELLO
24	SIGNAL	TWITCH	ZOOM

[30] Практическое руководство по порядку запроса электронных доказательств из других стран. Управление Организации Объединенных Наций по наркотикам и преступности.

Приложение № 3

НАИМЕНОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ЕГО ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

№	Наименование	Функциональное назначение
1	Autopsy-4.19.3-64bit.msi	Программа для исследования жесткого диска
2	USB_Write_Blocker_ALL _Windows_v1.3	Программный блокировщик записи USB
3	Volatility	Анализ волатильных данных
4	WiresharkPortable64_4.0.1.paf	Инструмент для анализа сетевых протоколов
5	FTK Imager.exe	Сбор и анализ волатильных данных. Захват ОЗУ
6	Testdisk-7.0	Программа для восстановления разделов файловых систем и данных
7	HashMyFiles.exe	Утилита, позволяющая вычислить контрольную сумму одного или несколько файлов при помощи алгоритмов MD-5, SHA-1 b CRC32
8	MagnetProcessCaptureV13	Инструмент, позволяющий захватывать память отдельных запущенных процессов, обеспечивает меньшую фрагментацию данных, лучшее восстановление больших типов данных
9	RegRipper	Инструмент для извлечения информации из реестра
10	Belkasoft RAM Capturer	Инструмент для снятия образа оперативной памяти компьютера
11	Pro Discover Forensics	Захват и анализ данных дисков компьютера
12	USBRip	Утилита для восстановления истории подключения USB-носителей к компьютерам под управлением Linux
13	Exif Tool	Чтение, запись и редактирование метаданных в файлах различных графических форматов
14	FOCA	Инструмент для поиска метаданных и скрытой информации в документах, загруженных в интернет
15	MacOs Artifact Parsing Tool	Инструмент для обработки образов дисков Mac и извлечения данных
16	Andriller	Утилита для сбора данных с Android-устройств

17	AVML	Портативный инструмент для сбора даных из энергозависимой памяти Linux – систем
18	Paladin	Инструмент цифровой криминалистики на базе Ubuntu
19	Encase	Приложение для восстановления цифровых улик с жестких дисков
20	Bulk_Extractor	Инструмент, позволяющий сканировать образы дисков, файлы, каталоги файлов и извлекать из них информацию

Приложение № 4

ГЛОССАРИЙ

1) **IP-адрес –** это уникальный числовой или буквенно-числовой идентификатор, который присваивается поставщиком интернет-услуг (провайдером) каждому устройству (например, компьютеру, ноутбуку, планшету, принтеру, маршрутизатору и т.д.).

2) **IP-Logger –** это программный инструмент, предназначенный для отслеживания IP-адресов пользователей интернета.

3) **Браузер** – это программное обеспечение, позволяющее просматривать веб-страницы в интернете, сохранять их, осуществлять поиск необходимой информации, запоминать пароли и т.д.

4) **Внешние жесткие диски** – это устройства, которые подключаются к компьютерам через порты USB или e-SATA, используются для резервного копирования данных или расширения хранилища.

5) **VPN** – это технология, обеспечивающая защищенное соединение между устройством пользователя и интернетом.

6) **Интернет –** это организованная система сбора, обработки и передачи информации, основанная на большом количестве баз данных, включая поисковые системы, онлайн-каталоги, блоги, форумы, социальные сети и другие ресурсы.

7) **Жесткие диски (HDD) –** это устройства на магнитных дисках для хранения данных. Они имеют большие объемы памяти и часто используются в настольных компьютерах и серверах.

8) **GPS –** навигационная система определения геолокации устройства.

9) **Криптоконтейнер –** это защищенное и зашифрованное хранилище, используемое для хранения криптовалюты.

10) **Командная строка** – это интерфейс взаимодействия с операционной системой, который позволяет пользователю вводить команды для управления компьютером.

11) **Магнитные ленты –** менее популярные устройства, которые используются для долгосрочного архивирования больших объемов данных.

12) **MAC-адрес –** это уникальный физический адрес устройства, помогающий идентифицировать его среди других устройств.

13) **Облачное хранилище** – это хранение данных на удаленных серверах через Интернет. Популярные облачные сервисы включают Google Диск, Dropbox, Amazon S3 и т.д.

14) **ОЗУ** (оперативно-запоминающее устройство) – это энергозависимая часть системы компьютерной памяти.

15) **Оптические диски** – это устройства для хранения мультимедийных данных. К ним относятся: компакт-диски (CD), DVD-диски и Blu-ray.

16) **Прокси-сервер -** это промежуточный сервер, используемый для передачи запросов между клиентом и удаленным сервером.

17) **Провайдер –** это организации, предоставляющие какие-либо услуги в той или иной области.

18) **Сервер** – это сетевой компьютер, задача которого обрабатывать запросы других устройств, подключенных к сети.

19) **Сетевое хранилище (NAS)** – устройства NAS, которые позволяют создавать сетевые хранилища для обмена данными между различными устройствами в домашних или офисных сетях.

20) **SSD диск** – это устройство хранения данных, использующее флеш-память для хранения информации.

21) **Твердотельные накопители (SSD)** – это твердотельные накопители хранения данных, обеспечивающие высокую скорость чтения и записи.

22) **USB-накопители** – это портативные устройства хранения данных (флэш-накопители), которые позволяют передавать и хранить данные между различными устройствами.

Приложение № 5

ЗАДАНИЯ В ТЕСТОВОЙ ФОРМЕ

1. Какое из следующих действий является частью осмотра места компьютерного преступления?

a) Сбор характеристик подозреваемого
b) Розыск киберпреступника
c) Анализ сетевого трафика
d) Изучение физического расположения компьютерной техники

2. Что включает в себя процесс осмотра места компьютерного преступления?

a) Допрос подозреваемого
b) Направление запроса провайдеру
c) Анализ системных логов компьютера
d) Изучение личности киберпреступника

3. Каким образом осуществляется фиксация исходного состояния компьютерной техники в ходе осмотра?

a) Создание резервных копий важных файлов
b) Применение аппаратных средств для копирования данных
c) Отключение компьютера от сети
d) Работа с системными логами

4. Какие меры обеспечивают целостность данных при осмотре места компьютерного преступления?

a) Использование шифрования для защиты данных
b) Запуск антивирусного сканирования
c) Создание точек восстановления системы
d) Сбор данных без их изменения

5. Что представляют собой цифровые следы в контексте осмотра места компьютерного преступления?

a) Информацию о сетевых узлах
b) Электронные следы, оставленные в результате действий пользователя компьютерной системы
c) Детальное исследование физической среды
d) Характеристики компьютерного оборудования

6. Какие инструменты могут использоваться при анализе компьютерной техники в рамках осмотра места преступления?

a) Программы для восстановления удаленных данных
b) Цифровые аппаратные средства для копирования информации
c) Антивирусные программы

d) Все варианты верны

7. Каким образом можно обеспечить безопасность при осмотре места компьютерного преступления?

a) Применение методов социальной инженерии

b) Использование шифрования для защиты данных

c) Ограничение физического доступа

d) Применение методов криптоанализа

8. Какие действия следует предпринять перед началом осмотра места компьютерного преступления?

a) Провести допрос подозреваемого

b) Создать резервные копии данных

c) Запустить программу антивирусного сканирования

d) Определить периметр осмотра

9. Что представляет собой метод стеганографии в контексте поиска и изъятия электронных доказательств?

a) Процесс извлечения данных из изображений

b) Сокрытие информации с использованием криптографических алгоритмов

c) Анализ поведения пользователей в сети

d) Использование специализированных инструментов для обнаружения скрытых сообщений

10. Какие трудности могут возникнуть при поиске и изъятии электронных доказательств в зашифрованных файлах?

a) Невозможность выявить местонахождение компьютера

b) Сложности в обнаружении файлов с помощью антивирусных программ

c) Отсутствие доступа к содержимому файлов без расшифровки

d) Проблемы с идентификацией владельца устройства

11. Какие методы можно применить для анализа электронных доказательств в случае удаленных файлов?

a) Использование программ для восстановления файлов с жесткого диска

b) Анализ электромагнитных излучений компьютерной техники

c) Применение аппаратных средств для дублирования данных

d) Запуск программ для обнаружения вредоносных программ

12. Каким образом цифровая подпись может быть связана с поиском и изъятием электронных доказательств?

a) Определение географического местоположения, подписавшего документ

b) Установление личности пользователя по характеристикам подписи

c) Обнаружение поддельных цифровых подписей в документах

d) Применение криптографии для защиты цифровых данных

13. Что представляет собой метод карвинга при восстановлении электронных доказательств?

a) Процесс анализа сетевого трафика на предмет аномалий

b) Извлечение данных из утерянных или поврежденных файлов

c) Проведение кибер-профилирования подозреваемого

d) Создание бэкапов для предотвращения потери информации

14. Какие методы аутентификации могут усложнить поиск и изъятие электронных доказательств?

a) Использование биометрических данных

b) Применение паролей и PIN-кодов

c) Шифрование данных в памяти устройства

d) Отключение интернет-соединения

15. Какие технологии могут быть использованы для анализа электронных доказательств на мобильных устройствах?

a) Анализ журналов сетевого трафика

b) Программы для восстановления удаленных SMS-сообщений

c) Использование технологии блокчейн для хранения данных

d) Проведение аудита безопасности Wi-Fi-сетей

16. Каким образом может влиять шифрование данных на процесс поиска и изъятия электронных доказательств?

a) Увеличение сложности аутентификации

b) Затруднение доступа к содержимому файлов без расшифровки

c) Снижение эффективности аппаратных средств для копирования данных

d) Использование технологии VPN для обхода шифрования

17. Что представляет собой процесс «сетевой активации» в работе с электронными доказательствами?

a) Запуск сетевого сканирования для поиска уязвимостей

b) Использование сетевых ресурсов для хранения доказательств

c) Применение специализированных сетевых протоколов для анализа трафика

d) Активация беспроводных сетей для повышения эффективности работы

18. Что представляет собой метод «динамического анализа» при обработке электронных доказательств?

a) Изучение изменений в системных логах в реальном времени

b) Анализ динамических характеристик компьютера при работе с различными программами

c) Проведение аудита безопасности статических файлов

d) Запуск анализа при отключенной сетевой активности

19. Какие технологии могут быть применены для обнаружения скрытых данных в электронных доказательствах?

a) Применение методов стеганографии

b) Активация биометрического сканера

c) Программирование алгоритмов для создания искусственного интеллекта

d) Запуск анализа поведения пользователей в социальных сетях

20. Какая из нижеперечисленных не является основной целью судебной экспертизы по компьютерным преступлениям?

a) Установление источника кибератаки

b) Анализ мотивации киберпреступника

c) Определение объема ущерба

d) Восстановление удаленных файлов

21. Какую роль может выполнять судебный эксперт при расследовании случаев фишинга?

a) Анализ антивирусных программ на зараженном компьютере

b) Идентификация использованных средств шифрования

c) Восстановление удаленных электронных писем

d) Определение методов идентификации поддельных веб-сайтов

22. Какой механизм международного сотрудничества используется для обмена информацией о киберугрозах и инцидентах в режиме реального времени?

a) INTERPOL

b) Europol

c) CIRCL

d) CERT

23. Какие проблемы могут возникнуть при международном сотрудничестве в области расследования киберпреступлений?

a) Различия в правовых системах

b) Отсутствие квалифицированных специалистов

c) Недостаточное количество киберпреступников

d) Уровень цифровой грамотности населения

24. Какие методы могут быть использованы для оценки достоверности показаний подозреваемого при допросе?

a) Анализ мимики и жестов подозреваемого

b) Применение фальшивых доказательств

c) Проведение допроса в условиях стресса

d) Запуск анализа голоса подозреваемого

Приложение № 6

СИТУАЦИОННЫЕ ЗАДАЧИ

Задание № 1.

Поступило сообщение о совершенном киберпреступлении, и Вы прибыли на место (ТОО «Шанс»), где установили, что компьютерная система организации была подвергнута вирусной атаке.

Вопросы:

1) Опишите шаги, которые Вы предпримете, прибыв на место преступления;

2) Объясните, какие инструменты и методы Вы будете применять для обеспечения целостности и сохранности электронных доказательств?

Задание № 2.

Вы получили информацию о совершенной кибератаке на корпоративную сеть компании ТОО «Квартал».

Вопросы:

1) Поясните, как Вы проведете осмотр места преступления;

2) Укажите, какие шаги Вы предпримите и какие инструменты будете использовать для выявления цифровых следов преступления?

Задание № 3.

В Отдел полиции поступило заявление от компании «Квантум» об утечке конфиденциальной информации.

Вопросы:

1) Опишите порядок осмотра места киберпреступления;

2) Опишите последовательность действий, начиная с осмотра компьютеров сотрудников и заканчивая выявлением возможного источника утечки.

Задание № 4.

Вы прибыли на место предполагаемого киберпреступления в офис компании «Белый ветер», где руководитель заявил о краже конфиденциальных данных.

Вопрос:

Какие будут Ваши первые шаги и как Вы осмотрите компьютерное оборудование?

Задание № 5.

Вы получаете заявление от гр. Нурланова Н. о том, что неизвестное лицо незаконно получило доступ к его домашней сети Wi-Fi и похитило личные данные.

Вопрос:

Какие шаги Вы предпримете при осмотре домашнего компьютера и роутера?

Задание № 6.

Компания-разработчик программного обеспечения обратилась с заявлением о кибератаке на их сервера, где возможно были украдены исходные коды.

Вопросы:

Как вы будете осматривать сервера компании?

Задание № 7.

Гр. Садыков Т. обратился в полицию с заявлением о том, что его личные данные были скомпрометированы через вредоносное ПО на его личном ноутбуке и украдены.

Вопрос:

Что будете делать при осмотре компьютера, опишите все Ваши шаги?

Задание № 8.

Вы получили информацию о взломе корпоративного электронного журнала компании «Луч», которая содержит конфиденциальные отчеты и информацию о клиентах.

Вопрос:

Опишите, как Вы начнете расследование, включая этапы осмотра места преступления, анализа цифровых следов и идентификации методов вторжения.

Задание № 9.

Владелец интернет-магазина сообщил о возможной утечке данных кредитных карт клиентов. Ваша задача - расследовать данный инцидент и принять решение.

Вопрос:

Опишите, как Вы начнете расследование, включая осмотр серверов, анализ электронных платежей и взаимодействие с провайдерами платежных услуг.

Задание № 10.

Компания «Кит» обратилась в полицию, где сообщила, что кто-то украл конфиденциальные данные сотрудников и корпоративные секреты. Вы прибыли на место преступления.

Вопрос:

Какие шаги Вы предпримете для выявления источника утечки, определения ущерба?

Задание № 11.

Сотрудники компании «Тайга» стали жертвами социальной инженерии и фишинговых атак, что позволило киберпреступникам получить доступ к их кредитным картам и украсть деньги.

Вопрос:

Опишите Ваши шаги по расследованию данного преступления.

Приложение № 7

ВОПРОСЫ К ЭКЗАМЕНУ

1) Какие шаги предпринимаются при осмотре места киберпреступления?
2) Каким образом проводится осмотр компьютерной техники с целью выявления цифровых следов?
3) Почему важно обеспечивать сохранность электронных улик во время осмотра места преступления?
4) Какие особенности учитываются при допросе потерпевшего?
5) Как следует обращаться с электронными доказательствами, предоставленными потерпевшим?
6) Каким образом проводится поиск электронных доказательств?
7) Как обеспечивается целостность и аутентичность изъятых электронных доказательств?
8) Как анализируются электронные доказательства?
9) Почему международное сотрудничество важно для расследования киберпреступлений?
10) Какие механизмы существуют для обмена информацией и опытом между странами при расследовании киберпреступлений?
11) Как обеспечивается согласованность правовых аспектов при международном сотрудничестве в расследованиях киберпреступлений?
12) Какие сложности могут возникнуть при розыске киберпреступника в виртуальной среде?
13) Каким образом осуществляется задержание киберпреступника и какие особенности следует учесть?
14) Как проводится допрос киберпреступника, учитывая технические и процессуальные особенности?
15) Какие меры предосторожности следует предпринять перед физическим осмотром места киберпреступления?
16) Как можно определить, что компьютерная техника была подвергнута воздействию вредоносных программ или атаки?
17) Как осуществляется сбор и документирование электронных доказательств в ходе осмотра?
18) Как обеспечить цифровую целостность электронных следов в процессе осмотра?
19) Как влияет физическое расположение компьютерной техники на процесс расследования?
20) Какие основные вопросы следует задать потерпевшему для выявления особенностей инцидента?
21) Каким образом допрос потерпевшего может помочь в выявлении возможных характеристик киберпреступника?
22) Почему важно учитывать психологические аспекты при допросе потерпевшего в случае киберпреступления?

23) Каким образом можно эффективно допрашивать потерпевшего с учетом технической специфики киберпреступлений?

24) Как использование специализированных терминов может повлиять на эффективность допроса киберпреступника?

25) Какие технические средства используются при поиске электронных доказательств?

26) Как обеспечивается целостность и аутентичность изъятых электронных доказательств?

27) Каким образом проводится анализ жестких дисков для выявления цифровых следов?

28) Какие меры принимаются для защиты электронных доказательств от случайного удаления или повреждения?

29) Каковы преимущества и сложности международного сотрудничества в расследовании киберпреступлений?

30) Какие организации и структуры занимаются координацией международного сотрудничества в борьбе с киберпреступлениями?

31) Каким образом различия в законодательстве могут повлиять на международное сотрудничество при киберпреступлениях?

32) Как организовать эффективную коммуникацию и обмен информацией между странами при расследовании киберпреступлений?

33) Каким образом технические аспекты усложняют розыск киберпреступника?

34) Какие технические и юридические аспекты следует учитывать при задержании киберпреступника?

35) Как провести допрос киберпреступника с учетом его технической компетенции?

36) Какие меры безопасности следует предпринять при задержании киберпреступника с целью минимизации рисков?

37) Каким образом сотрудничество с техническими экспертами может помочь в эффективном допросе киберпреступника?

38) Какие основные шаги включает в себя процесс физического осмотра места киберпреступления?

39) Как обеспечить сохранность цифровых следов при осмотре компьютерной техники?

40) Каким образом можно зафиксировать состояние компьютерной системы на момент осмотра?

41) Как влияют факторы среды на сохранность электронных улик в момент осмотра места преступления?

42) Какие вопросы необходимо задать потерпевшему для получения полной картины инцидента?

43) Какие методы используются для поиска электронных доказательств?

44) Как проводится анализ цифровых доказательств и какие инструменты используются для их обработки?

45) Каким образом можно обеспечить адекватное хранение и документирование электронных доказательств?

46) Какие преимущества международного сотрудничества в расследованиях киберпреступлений?

47) Каким образом происходит розыск киберпреступника в виртуальной среде?

48) Какие методы и техники используются при задержании киберпреступника?

49) Каким образом осуществляется допрос киберпреступника и какие особенности должны быть учтены при таком допросе?

50) Как обеспечить безопасность и сохранность электронных доказательств во время задержания и допроса киберпреступника?

Приложение № 8

Программа курса
(проект)

Академия правоохранительных органов
при Генеральной прокуратуре Республики Казахстан

«Утверждаю»
Директор Института
профессионального обучения
_____ Н. Даниев
«*» ****** 20**г.**

УЧЕБНАЯ ПРОГРАММА
курса повышения квалификации «Особенности проведения досудебного расследования киберпреступлений»

Начало курса: _____
Окончание курса: _____

г. Косшы, 2023г.

Обоснование (актуальность курса):

Основным условием успешной работы правоохранительных органов служит эффективная система повышения квалификации их сотрудников.

С целью формирования высококвалифицированного кадрового состава сотрудников правоохранительных органов, приобретения ими специальных навыков, познаний и умений имеется потребность в эффективном обучении, которое бы позволило повысить эффективность выполнения сотрудниками служебных обязанностей.

Данная учебная программа направлена на подготовку сотрудников следственно-оперативных подразделений правоохранительных органов в сфере расследования киберпреступлений.

Цель обучения: приобретение сотрудниками правоохранительных органов навыков и знаний, необходимых для эффективного расследования киберпреступлений.

Задачи обучения: подготовить сотрудников правоохранительных органов к анализу и классификации киберпреступлений, проведению осмотра места преступления, компьютерной техники, работе с электронными доказательствами.

Контингент слушателей: сотрудники органов прокуратуры, Службы экономических расследований и Антикоррупционной службы.

Ожидаемый эффект:

По окончанию обучения слушатель должен,

знать: особенности проведения осмотра места киберпреступления и компьютерной техники, направления поиска электронных доказательств, порядок их упаковки и транспортировки, требования к назначению судебной экспертизы и другие вопросы, связанные с расследованием преступлений данной категории.

уметь: проводить осмотр места преступления и компьютерной техники, делать образы оперативной памяти и жесткого диска, работать с программным обеспечением, связанным с поиском электронных доказательств, упаковывать и транспортировать электронные доказательства, назначать по ним судебные экспертизы.

Продолжительность курса: 5 дней или 30 академических часов, форма обучения - очная.

Форма контроля: тестирование.

ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование модулей, тем	Всего часов	в том числе:	
			лекционные занятия	практические занятия
	Входной контроль			
1.	**Модуль 1. Осмотр места компьютерного преступления**			
1.1	Особенности осмотра места	3	1	2

	компьютерного преступления и компьютерной техники			
ВСЕГО:		**3**	**1**	**2**
2.	**Модуль 2. Электронные доказательства**			
2.1.	Понятие и виды электронных доказательств	1	1	
2.2	Поиск, обнаружение и изъятие электронных доказательств	3	1	3
2.3	Работа с программным обеспечением по созданию образов оперативной памяти и жесткого диска	7		7
2.4	Хеширование файлов	2	1	2
2.5	Упаковка и транспортировка электронных доказательств	3	1	2
ВСЕГО:		**18**	**4**	14
3.	**Модуль 3. Назначение судебных экспертиз**			
3.1	Понятие и виды судебных экспертиз, назначаемых по делам о киберпреступлениях	1	1	
3.2	Подготовка постановлений о назначении судебной экспертизы	2		2
ВСЕГО:		**3**	**1**	**2**
4.	**Модуль 4. Международное сотрудничество. Поиск и задержание киберпреступника**			
4.1	Международные аспекты расследования компьютерных преступлений	1	1	
4.2	Розыск киберпреступника и его задержание	2	1	1
4.3	Особенности допроса подозреваемого	3	1	2
ВСЕГО:		**6**	**3**	**3**
ИТОГО:		**30**	**9**	**21**
	Выходной контроль			

«Эти курсы обучения, как и все другие мероприятия Академии, освещаются на официальном сайте Академии и наших страничках в социальных сетях».

Сайт: academy-gp.kz

Facebook: academygp

Instagram: academy_ gp.kz

Подписывайся! «Будь в курсе актуальных мероприятий по развитию профессиональных навыков сотрудников правоохранительных органов».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Правил приема и регистрации заявления, сообщения или рапорта об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований, утвержденные Приказом Генерального Прокурора Республики Казахстан от 19 сентября 2014 года № 89.
2. *Там же.*
3. *Там же*.
4. Уголовно-процессуальный кодекс Республики Казахстан.
5. *Там же.*
6. *Там же.*
7. https://esj.pnzgu.ru/files/esj.pnzgu.ru/podol_naya_nn_2020_2_13.pdf - интернет-ресурс.
8. https://pravo.studio/osnovyi-kriminalistiki/taktika-rabochego-etapa-osmotra-mesta-76017.html - интернет-ресурс.
9. Балашов Д.Н. Криминалистика: Тактика рабочего этапа осмотра места происшествия. Учебник. - М.,2005. - 503 с.
10. https://blog.skillfactory.ru/glossary/server/#:~:text=Сервер%20(от%20англ.%20server%20—,программное%20обес печение%2C%20обрабатывающее%20пользовательские%20запросы – интернет-ресурс.
11. Belkasoft RAM Capturer скачать бесплатно (software4pc.ru) – интернет-ресурс.
12. Практические советы по использованию Belkasoft Live RAM Capturer для эффективного создания дампа оперативной памяти в формате .mem (anyquestion.info) – интернет-ресурс.
13. https://translated.turbopages.org/proxy_u/en-ru.ru.3d94800f-656323c8-12a33e03-74722d776562/https/en.wikipedia.org/wiki/Locard%27s_exchange_principle#:~:text=В%20криминалистике%20принцип%20Локара%20гласит%2C,образом%3A%20"Каждый%20контакт%20оставляет%20след" – интернет-ресурс.
14. https://www.unodc.org/e4j/ru/cybercrime/module-4/key-issues/digital-evidence.html - интернет-ресурс.
15. https://adilet.zan.kz/rus/docs/V1700015180 - интернет-ресурс.
16. Методы и способы получения доказательственной информации с электронных носителей: учебное пособие / сост. М. В. Старичков, А. А. Шаевич. – Иркутск: ФГКОУ ВО ВСИ МВД России, 2015. – 88 с.
17. https://www.unodc.org/e4j/ru/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html - интернет-ресурс.
18. https://www.unodc.org/e4j/ru/cybercrime/module-7/key-issues/formal-international-cooperation-mechanisms.html - интернет-ресурс.
19. https://www.unodc.org/e4j/ru/cybercrime/module-7/key-issues/informal-international-cooperation-mechanisms.html - интернет-ресурс.
20. Доклад Комитета по правам человека ООН. Том II. A/63/40 (Vol.II). Нью-Йорк, 2008 год.

21. https://www.unodc.org/e4j/ru/cybercrime/module-7/key-issues/informal-international-cooperation-mechanisms.html - интернет-ресурс.
22. https://ru.wikipedia.org/wiki/Европол - интернет-ресурс.
23. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN – интернет-ресурс.
24. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN – интернет-ресурс.
25. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN – интернет-ресурс.
26. https://bezlimit.ru/blog/geolokatsiya-chto-eto-takoe/ - интернет-ресурс.
27. https://wiki.merionet.ru/articles/chto-takoe-mac-adres-i-kak-ego-uznat/ - интернет-ресурс.
28. http://go.microsoft.com/fwlink/p/?LinkId=255141 – интернет-ресурс.
29. Практическое руководство по порядку запроса электронных доказательств из других стран. Управление Организации Объединенных Наций по наркотикам и преступности. https://www.unodc.org/documents/organized-crime/GPTOC/GPTOC2/_ebook.pdf - интернет-ресурс.
30. Там же.

Калиев А.А. Расследование киберпреступлений: от теории к практике. / Учебное пособие. – г. Косшы, 2023. – 123 с.

Подписано в печать 28.12.2023 г. Формат 60Х84/16
Усл. печ. л. ____. Тираж 15 экз. Заказ №_____

Отпечатано в типографии
Академии правоохранительных органов
при Генеральной прокуратуре Республики Казахстан
г. Косшы, ул.Республики, 16