МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования
«Уфимский юридический институт Министерства внутренних дел
Российской Федерации»

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему **«ОСОБЕННОСТИ ТАКТИКИ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнил
Курбанова Алина Наильевна
обучающаяся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2020 года набора, 013 учебного взвода

Руководитель
профессор кафедры,
кандидат технических наук, доцент
Харисова Зарина Ирековна

К защите рекомендуется
рекомендуется / не рекомендуется
Начальник кафедры _____ Э.Д. Нугаева
подпись
Дата защиты «___» _____ 2025 г. Оценка _____

ПЛАН

ВВЕДЕНИЕ

Стремительное развитие информационных технологий, повсеместное внедрение компьютерных систем и расширение доступа к сети Интернет, несомненно, оказали позитивное влияние на различные сферы общественной жизни. Однако наряду с этим наблюдается и негативная тенденция – рост преступлений в сфере компьютерной информации. Преступность приобретает все более изощренные формы, трансграничный характер и высокую латентность, что создает серьезные вызовы для правоохранительных органов. В связи с этим особую актуальность приобретает совершенствование тактики производства следственных действий, направленных на эффективное расследование данной категории преступлений.

За период с января по декабрь 2024 года зафиксирован рост количества преступлений, связанных с использованием информационно-телекоммуникационных технологий или совершенных в сфере компьютерной информации. Зарегистрировано 765,4 тыс. таких преступлений, что превышает показатель аналогичного периода 2023 года на 13,1%. Доля данных преступлений в общем объеме зарегистрированных преступлений увеличилась с 34,8% в 2023 году до 40,0% в 2024 году[1].

Целью настоящего исследования является разработка практических рекомендаций по совершенствованию тактики производства следственных действий при расследовании преступлений в сфере компьютерной информации, направленных на повышение эффективности раскрытия и расследования данных преступлений. Достижение указанной цели предполагает решение следующих задач:

1. Раскрыть понятие и характеристику классификации преступлений в сфере компьютерной информации;

---

[1] Краткая характеристика состояния преступности в Российской Федерации // Официальный сайт МВД РФ. URL: https://мвд.рф/reports/item/60248328 (дата обращения: 28.04.2025).

2. Рассмотреть криминалистическую характеристику преступлений в сфере компьютерной информации;

3. Выявить особенности производства отдельных следственных действий (осмотр места происшествия, допрос, обыск, экспертиза и др.) при расследовании преступлений в сфере компьютерной информации;

4. Разработать практические рекомендации по совершенствованию тактики расследования данной категории преступлений.

Объектом исследования являются общественные отношения, возникающие в процессе расследования преступлений в сфере компьютерной информации.

Предметом исследования выступает тактика производства следственных действий при расследовании данной категории преступлений.

Вопросы криминалистического обеспечения расследования преступлений в сфере компьютерной информации, как в методологическом, так и в частно-теоретическом аспектах, исследовались в трудах Бессонова А. А., Бутенко О. С., Васюкова В. Ф., Гаврилова Б. Я., Ищенко Е. П., Кузнецова А. А., Пушкарева В. В., Яблокова Н. П. и др.

Специфика применения специальных знаний при расследовании преступлений в сфере компьютерной информации анализируется в исследованиях Россинской Е. Р., Рядовского И. А., Семикаленовой А И., Усова А. И., Хатунцева Н. А. и др.

Оперативно-розыскная деятельность и использование ее результатов в рамках расследования рассматриваемой категории преступлений представлены в работах Вехова В. Б., Зуева С. В. и др.

Теоретическая значимость данного исследования обусловлена проведением комплексного анализа теоретических и практических аспектов расследования преступлений в сфере компьютерной информации в Российской Федерации, результатом которого стала разработка рекомендаций, ориентированных на повышение эффективности и оптимизацию работы лиц, осуществляющих расследование.

Практическая значимость исследования определяется возможностью применения представленных в работе предложений по совершенствованию алгоритма действий следователя при проведении отдельных следственных действий (осмотр места происшествия, допрос, обыск, выемка) по делам о преступлениях в сфере компьютерной информации с учетом специфики цифровых доказательств, включая рекомендации по применению специализированного программного обеспечения (далее – ПО) и взаимодействию со специалистами в области информационных технологий. Предложение тактических рекомендаций для практических работников, позволяющие повысить эффективность расследования данной категории дел.

Эмпирическую базу составило отечественное законодательство в рассматриваемой сфере, нормативные правовые акты, Конституция Российской Федерации, Уголовно-процессуальный Кодексом Российской Федерации и пр.

В процессе исследования применялся комплекс общенаучных, частно-научных и специальных методов. К общенаучным относятся анализ и синтез, индукция и дедукция, наблюдение и сравнение, а также структурный, системный и исторический методы познания. В качестве частно-научного метода использован социологический. Специальные методы включают сравнительно-правовой, историко-правовой, формально-юридический, методы правового моделирования и пр. Применение данной методологии позволило всесторонне исследовать предмет исследования и сформулировать обоснованные выводы.

Структура работы обусловлена целью и задачами исследования. Работа включает в себя введение, две главы, пять параграфов, заключение и список литературы.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Понятие, виды и характеристика преступлений в сфере компьютерной информации

Вопрос классификации преступлений, совершаемых с применением информационных технологий, до сих пор вызывает дискуссии в современной юриспруденции. В уголовно-правовой литературе используется разнообразная терминология для обозначения преступлений, связанных с компьютерными технологиями: «преступления в сфере компьютерной информации», «компьютерные преступления», «киберпреступления», «интернет-преступления» и другие. Каждое понятие имеет свои особенности, что обуславливает необходимость их точного определения и разграничения.

Термин «преступления в сфере компьютерной информации» закреплен законодательно и охватывает составы преступлений, предусмотренные главой 28 Уголовного кодекса Российской Федерации (далее – УК РФ). Список этих преступлений периодически расширяется, криминализируя новые общественно опасные действия, которые, по мнению законодателя, угрожают безопасности информационно-телекоммуникационных систем.

К преступлениям в сфере компьютерной информации, исходя из главы 28 УК РФ, относятся:

1. Неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ);

2. Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения ст. 272.1 УК РФ;

3. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);

4. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ);

5. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ);

6. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ).

Многозначность термина «компьютерные преступления» и отсутствие его легального определения приводят к различным трактовкам данного понятия, таким как:

1. В качестве синонима термина «преступления в сфере компьютерной информации»;

2. Для обозначения преступлений, совершаемых в информационно-телекоммуникационной сфере (информационные преступления);

3. Для обозначения преступлений, совершенных с использованием компьютерной системы или сети, внутри нее или направленных против нее (киберпреступления)[1].

В целом информационные (компьютерные) преступления охватывают деяния, совершаемые с применением информационно-телекоммуникационных технологий. Это включает как преступления, предусмотренные главой 28 УК РФ (преступления в сфере компьютерной информации), так и другие противоправные действия, осуществляемые с помощью этих технологий,

---

[1] Попова С. В., Агафонова М. С., Машин А. А. Угрозы экономической безопасности в концепции войн шестого поколения // Цифровая и отраслевая экономика. 2024. № 4. С. 55.

например, мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ) может осуществляться не только с помощью банковских карт, но и других устройств. Мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), как понятно из названия, невозможно без применения компьютерных технологий.

Конвенция о преступности в сфере компьютерной информации 2001 года классифицирует такие преступления следующим образом: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; преступления, связанные с использованием компьютерных средств; преступления, связанные с содержанием данных; преступления против авторского права и смежных прав; и проявления расизма и ксенофобии в компьютерных сетях.

Глава 28 УК РФ, относящаяся к разделу о посягательствах на общественную безопасность и общественный порядок, определяет видовым объектом этих преступлений информационную безопасность как часть общественной безопасности.

Доктрина информационной безопасности РФ, утвержденная Указом Президента РФ от 05.12.2016 № 646[1], раскрывает понятие информационной безопасности. Доктрина рассматривает информационную сферу как совокупность информации, объектов информатизации, информационных систем, интернет-ресурсов, сетей связи, информационных технологий, субъектов, работающих с информацией и технологиями, и механизмов регулирования этих отношений. Информационная безопасность, согласно указанному документу, – это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, гарантирующее реализацию прав и свобод граждан, достойный уровень жизни, суверенитет,

[1] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: http://www.consultant.ru. (дата обращения: 12.03.2025).

территориальную целостность, устойчивое развитие, оборону и безопасность государства.

Следовательно, непосредственным объектом преступлений в сфере компьютерной информации являются общественные отношения, обеспечивающие защиту личности, общества и государства от информационных угроз. Информационные угрозы представляют собой широкий спектр факторов и действий, которые могут причинить вред как отдельным лицам, так и обществу в целом, а также национальной безопасности государства в информационной сфере. Это включает в себя не только непосредственное воздействие на информационные системы и данные, но и манипулирование информацией, ее искажение, распространение дезинформации, а также ограничение доступа к достоверной информации. Преступления в сфере компьютерной информации, таким образом, являются одной из форм реализации этих угроз, непосредственно посягая на информационную безопасность и интересы личности, общества и государства. Они подрывают доверие к информационным технологиям, создают риски для экономической стабильности и могут быть использованы для достижения политических целей. С учетом обновленной Доктрины информационной безопасности Российской Федерации и вступления в силу статьи 274.1 УК РФ, понятие предмета преступлений в сфере компьютерной информации претерпело трансформацию. Ранее предмет ограничивался компьютерной информацией. В настоящее время, базируясь на расширенном толковании предмета преступления и положениях Доктрины, к предметам преступлений в сфере компьютерной информации следует относить: информацию; объекты информатизации; информационные системы; сайты (интернет-ресурсы); сети связи; информационные технологии; деятельность субъектов, связанную с формированием, обработкой информации, развитием и применением информационных технологий, а также обеспечением информационной безопасности. В широком смысле, предметом преступлений

в сфере компьютерной информации можно считать компоненты информационной инфраструктуры.

Примечательно, что в статье 274.1 УК РФ, предусматривающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, компьютерная информация выступает не только в качестве предмета, но и в качестве средства и (или) орудия преступления.

Согласно примечанию к статье 272 УК РФ, под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от способов их хранения, обработки и передачи. Данное определение ограничивает уголовно-правовую охрану информацией, передаваемой исключительно посредством электрических сигналов. Однако современные технологии используют разнообразные каналы связи, включая оптические (световые сигналы) и беспроводные (инфракрасное излучение, лазерные лучи). Следовательно, критерий представления информации в форме электрических сигналов не является универсальным и требует пересмотра. Необходимо учитывать иные характеристики компьютерной информации как предмета преступлений, предусмотренных главой 28 УК РФ.

Статья 2 Федерального закона от 27.07.2006 № 149-ФЗ[1] «Об информации, информационных технологиях и о защите информации» определяет информацию как сведения (сообщения, данные) вне зависимости от формы их представления. Данное определение характеризуется большей универсальностью и соответствует современным условиям.

---

[1]Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: http://www.consultant.ru. (дата обращения: 05.12.2025).

Словарь Ожегова[1] определяет «сведения» как знания, известия, сообщения или представления о чем-либо. «Сообщение» – это передаваемая информация или известие, а «данные» – сведения, необходимые для выводов и решений. «Информация» же трактуется как сведения о мире и процессах, воспринимаемые человеком или устройством.

Ранее глава 28 УК РФ связывала понятие компьютерной информации с ее материальным носителем. Статья 272 УК РФ предусматривала ответственность за неправомерный доступ к охраняемой законом информации, находящейся на машинном носителе, в ЭВМ, системе ЭВМ или их сети.

Для того чтобы человек мог воспринимать компьютерную информацию, её необходимо преобразовать с помощью программно-технических средств. В основе любой электронно-вычислительной машины лежит взаимодействие нескольких ключевых компонентов: арифметико-логического устройства, выполняющего математические и логические операции; устройства управления, координирующего работу всех остальных компонентов; запоминающего устройства для хранения данных и программ; и устройства ввода-вывода, обеспечивающего взаимодействие компьютера с внешним миром (например, клавиатура, монитор, принтер). Информация, обрабатываемая ЭВМ, представлена в цифровой форме, то есть в виде чисел. Любые данные, будь то текст, изображения, звук или видео, должны быть преобразованы в числовой формат перед обработкой компьютером. Этот процесс преобразования называется кодированием. Он оптимизирует информацию для хранения, передачи и обработки внутри ЭВМ. Обратный процесс, преобразование числовых данных в форму, понятную человеку (например, отображение текста на экране или воспроизведение звука), называется декодированием. Таким образом, кодирование и декодирование – это два фундаментальных процесса, обеспечивающих взаимодействие человека

[1] Толковый словарь русского языка: 72500 слов и 7500 фразеологических выражений / С. И. Ожегов, Н. Ю. Шведова; Российская АН, Ин-т рус. яз., Российский фонд культуры. 2-е изд. М., 1994. С. 607.

с компьютерной информацией. Разнообразие методов кодирования и декодирования позволяет работать с различными типами данных и эффективно использовать ресурсы ЭВМ.

Хранение данных в компьютере осуществляется на жестком магнитном диске или иных носителях информации посредством изменения магнитных свойств их поверхности. Данные на носителе структурированы в виде файлов, обладающих идентифицирующими атрибутами: именем, размером, типом (текстовый, графический и т.д.).

Компьютеры классифицируются по габаритам (стационарные, настольные, портативные, карманные), наличию периферийных устройств, функциональному назначению (пользовательские, серверы и т.п.). Компьютер в совокупности с периферийными устройствами образует вычислительную систему. Функциональные возможности вычислительной системы расширяются путем подключения дополнительных устройств ввода-вывода: принтера, сканера, модема, плоттера, сетевого адаптера и других. Компьютерная сеть представляет собой совокупность вычислительных машин, объединенных посредством кабельных или беспроводных каналов связи. Сеть обеспечивает обмен данными, совместное использование аппаратных ресурсов (принтеров, сканеров, дискового пространства и т.п.) и выполнение общих программ[1].

В юридической литературе существуют различные трактовки понятия «информация, охраняемая законом», являющегося ключевым для квалификации преступлений в сфере компьютерной информации. Некоторые исследователи, например, Гульбин Ю. А., полагают, что практически вся информация на машинном носителе охраняется законом. Данная позиция представляется спорной, поскольку не вся информация подлежит правовой охране, а некоторые

[1] Попов А.Н. Преступления в сфере компьютерной информации: учеб. пособ. / СПб., 2018. С.25.

виды информации, согласно законодательству, не могут иметь ограниченный доступ[1].

Гаврилин Ю. В., например, связывает охраняемую информацию с интеллектуальной собственностью, её нематериальным характером, а также хранением на машинных носителях, в ЭВМ или сетях. Однако такое определение слишком узкое, так как правовая защита распространяется и на другие виды информации, не являющиеся объектами интеллектуальной собственности, например, персональные данные или государственная тайна[2].

Степалин В. П. расширяет понятие охраняемой информации, включая в него защиту прав на вычислительную технику и тайну связи. Этот подход, напротив, слишком широк и смешивает защиту самой информации с защитой средств её обработки и передачи. Он не отражает специфику информационных правоотношений[3].

Более точным представляется подход исследователей, таких как Гуев А. Н., Кочои С. М., Савельев Д. Б., которые определяют охраняемую информацию через призму ограниченного доступа и специального правового режима. Они акцентируют внимание на том, что доступ к определенной информации регламентируется законодательством (например, законом о государственной тайне, о персональных данных и т.д.). Именно наличие специального правового режима и ограничений доступа является ключевым признаком информации, пользующейся правовой охраной. Этот подход позволяет охватить широкий спектр охраняемой информации, не ограничиваясь только объектами интеллектуальной собственности, и отражает сущность информационных правоотношений, связанных

---

[1] Гульбин, Ю.А. Преступления в сфере компьютерной информации: учеб. пособ. / Ю.А. Гульбин. М., 2007. С. 24.

[2] Гаврилин Ю. В. Научно-практический комментарий к ст. 272 УК РФ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Степалин В. П. Глава 28. Преступления в сфере компьютерной информации// Научно-практическое пособ. по применению УК РФ / Под ред. В. М. Лебедева. М., 2005. С.78.

с регулированием доступа к информации[1]. Представляется, что указанные авторы предлагают ограничительное толкование понятия «информация, охраняемая законом». Такой подход может привести к ошибочному заключению об отсутствии уголовно-правовой охраны информации, не упомянутой в законодательстве.

Вопрос об охраняемой законом информации требует дифференцированного подхода. Статья 5 Федерального закона «Об информации, информационных технологиях и о защите информации» классифицирует информацию по категории доступа и распространения: свободно распространяемая; предоставляемая по соглашению участников отношений; подлежащая предоставлению или распространению в соответствии с федеральными законами; распространение которой ограничено или запрещено. Кроме того, законодательство может устанавливать виды информации в зависимости от ее содержания или собственника (обладателя).

В ряде учебных изданий встречается толкование предмета компьютерных преступлений, включающее не только данные, но и физические носители информации. Более точным представляется подход, согласно которому предметом преступлений, предусмотренных статьями 272-274 УК РФ, является исключительно компьютерная информация, несмотря на ее неразрывную связь с техническими средствами обработки, хранения и передачи данных. Физическое воздействие на материальные носители, например, их уничтожение, должно квалифицироваться по другим статьям УК РФ, регулирующим преступления против собственности или иные правонарушения. Исключение составляет статья 274.1 УК РФ, предусматривающая ответственность за неправомерное воздействие

---

[1] Гуев А. Н. Комментарий к Уголовному кодексу Российской Федерации: для предпринимателей. М., 2000. С. 347; Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. 1999. № 1. С. 4; Комментарий к Уголовному кодексу Российской Федерации / отв. ред. В. М. Лебедев. 2-е изд. М., 2013. С. 579.

на элементы критической информационной инфраструктуры, включая аппаратные средства, осуществляемое с использованием компьютерной информации. В данном случае предметом преступления могут выступать как информация, так и компоненты инфраструктуры.

Представляется, что предметом преступлений, предусмотренных статьями 272–274 УК РФ, является исключительно компьютерная информация, несмотря на ее неотъемлемую связь с вычислительной техникой, носителями, сетями и каналами связи. Физическое воздействие на материальные носители, например, их уничтожение, следует квалифицировать как преступления против собственности или по другим статьям УК РФ. Исключение составляет статья 274.1 УК РФ, где предметом преступления могут быть элементы критической информационной инфраструктуры, включая вычислительную технику и сетевое оборудование, в случаях неправомерного воздействия на них с использованием компьютерной информации.

В юридической литературе существуют дискуссионные точки зрения относительно соотношения преступлений в сфере компьютерной информации и других преступлений. Волеводз А. Г. утверждает, что хищение компьютера или носителя информации как имущества не квалифицируется как неправомерный доступ к компьютерной информации, а влечет за собой ответственность за преступления против собственности[1]. Альтернативная точка зрения заключается в том, что хищение компьютера с последующим незаконным копированием информации влечет ответственность за неправомерный доступ к охраняемой законом компьютерной информации, независимо от способа получения носителя.

Более сложным представляется вопрос квалификации умышленного уничтожения информации путем воздействия на ее носитель. В случаях, когда стоимость информации существенно превышает стоимость носителя, возникает

---

[1] Волеводз А. Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации // Российский судья. 2002. № 9. С. 36.

вопрос о возможности квалификации деяния по главе 28 УК РФ. Однако, если компьютерная информация не является предметом, орудием или средством преступления, применение статей главы 28 УК РФ невозможно.

Охраняемая законом компьютерная информация обладает следующими признаками: информация (сведения, сообщения, данные), представленная в форме электрических сигналов, к примеру, база данных клиентов банка, хранящаяся на сервере. Сами по себе данные не имеют физической формы, а представлены в виде электрических сигналов, которые интерпретируются компьютером; может быть воспринята пользователем только посредством компьютера; информация хранится в памяти компьютера, на машинных или иных носителях информации (жесткий диск, флеш-накопитель, облачное хранилище), либо передается по каналам связи (интернет, локальная сеть). Так, например, пересылка конфиденциального документа по электронной почте; законом или правообладателем в рамках предоставленных ему законом полномочий установлен особый режим доступа, использования, распространения, передачи, защиты и других действий с данной информацией (к примеру, доступ к банковскому счету осуществляется с помощью пароля, известного только владельцу счета)[1].

Таким образом, преступления в сфере компьютерной информации – это общественно опасные деяния, нарушающие безопасность компьютерной информации и систем. Они используют компьютерные технологии как инструмент, средство или предмет преступления. К основным видам относятся неправомерный доступ к информации, создание и распространение вредоносных программ, нарушение правил эксплуатации компьютерных систем и неправомерное воздействие на критическую информационную инфраструктуру. Эти преступления характеризуются высокой латентностью,

---

[1] Эксархопуло А. А. Криминалистика: учеб. для вузов / А. А. Эксархопуло, И. А. Макаренко, Р. И. Зайнуллин. М.: Издательство Юрайт, 2025. С.230.

трансграничным характером, быстрой трансформацией способов совершения и возможностью причинения значительного ущерба.

§ 2. Криминалистическая характеристика преступлений в сфере компьютерной информации

Центральную роль в современном обществе играет стремительное развитие информационных технологий, вычислительной техники и сетевой инфраструктуры, а также их глубокая интеграция во все сферы человеческой деятельности. Однако технологический прогресс, наряду с позитивными изменениями, создает и новые возможности для злоупотребления информационно-телекоммуникационными технологиями в преступных целях, способствуя усложнению и совершенствованию методов организации киберпреступности. В связи с этим, криминалистический анализ преступлений в сфере компьютерной информации требует комплексного подхода, учитывающего не только технические особенности, но и эволюционирующую типологию преступников, их тактику и стратегии в киберпространстве, в частности, в сети Интернет. Для эффективного расследования необходимо устанавливать причинно-следственные связи в цифровой среде, разрабатывать методы получения и анализа электронных (цифровых) доказательств, совершенствовать механизмы розыска подозреваемых и обеспечивать неотвратимость юридической ответственности за данные преступления. Кроме того, криминалистика должна проактивно реагировать на постоянно меняющийся ландшафт угроз и новые технологические вызовы, разрабатывая адекватные инструменты и методики противодействия.

Ищенко Е. П. отмечает размывание границ между реальностью и виртуальностью, миром материальных объектов и информации, онлайн и офлайн деятельностью, социальной и киберсредой как отличительную черту

современности[1]. Развитие информационных технологий привело к существенной трансформации образа жизни человека. Понятие «киберпространство», изначально введенное писателем-фантастом Уильямом Гибсоном в 1982 году, описывает виртуальную реальность, существующую внутри компьютерных сетей и доступную для человеческого взаимодействия. Гибсон в своих произведениях исследовал сложные социально-философские и психологические вопросы, связанные с интеграцией человека в технологическую среду, многие из которых до сих пор активно обсуждаются. Хотя точного, универсально принятого определения киберпространства не существует, этот термин прочно укоренился в юридической, криминалистической и научной литературе. Его широкое распространение и интуитивное понимание обусловлены не только научно-фантастическими произведениями Гибсона, но и влиянием массовой культуры, а также активным обсуждением этой концепции в научном сообществе. Киберпространство сегодня понимается как сложная, динамичная среда, где происходят коммуникации, коммерческие операции, политические дискуссии и множество других видов деятельности, представляя собой неотъемлемую часть современной жизни. Именно эта многогранность и постоянная эволюция киберпространства делают его определение столь сложной задачей[2].

В теории оперативно-розыскной деятельности киберпространство представляет собой динамическую виртуальную среду, где развиваются общественные отношения, тесно переплетенные с физическим миром через активное взаимодействие пользователей сети Интернет и использование информационных ресурсов.

Киберпространство можно определить как комплексную систему, включающую информационные технологии, сети и Интернет, формирующую

---

[1] Ищенко Е. П. О технологии искусственного интеллекта в криминалистике // 30 лет юридической науки КубГАУ. Краснодар, 2021. С. 377.

[2] Гибсон У. Ф. Идору / Уильям Гибсон. Екб: У-Фактория, 2003. С. 129.

виртуальную реальность, постоянно генерируемую и эволюционирующую благодаря взаимодействию пользователей и развитию технологических инструментов. В этой среде происходит непрерывный обмен различными видами данных в режиме реального времени.

Согласно определению Файзуллиной А. А., криминалистическая характеристика преступлений в сфере компьютерной информации представляет собой информационную модель, отражающую совокупность ключевых признаков противоправного деяния, необходимых для его раскрытия и расследования. Эта модель включает типологические особенности личности преступника и его мотивы (например, финансовая выгода, идеологические убеждения), пространственно-временные характеристики совершения преступления (например, DDoS-атака, осуществляемая из разных стран и длящаяся несколько дней), а также способ совершения преступления с учетом специфических технических деталей (например, использование определенного вредоносного ПО или уязвимости в системе безопасности)[1].

Личность преступника является центральным элементом криминалистической характеристики. Распространенное представление о преступнике как о хакере, обладающем высоким уровнем компетенций в области компьютерных технологий, не отражает многогранность данного феномена. В условиях стремительного развития цифровых технологий и повсеместной компьютеризации общественных отношений, исследование личности киберпреступника становится все более важной задачей.

Понимание мотивации, уровня технической подготовки и методов, используемых этими лицами, крайне необходимо для эффективного противодействия киберпреступности. Классификация киберпреступников по

[1] Файзуллина А.А. К вопросу о соотношении понятий «криминалистическая характеристика преступлений» и «следственная ситуация» // Инновационная наука. 2024. № 2. С. 140.

уровню их технической компетенции позволяет более точно определить потенциальные угрозы и разработать соответствующие стратегии защиты[1].

Можно выделить три основные группы:

1. Лица с разным уровнем технических навыков, которые не занимаются систематической противоправной деятельностью в киберпространстве. Их преступления могут быть связаны с неосторожностью, случайным доступом к запрещенной информации или единичными эпизодами мошенничества. Мотивация в таких случаях может быть различной, от простого любопытства до сиюминутной выгоды. Опасность этой группы заключается в большом количестве потенциальных нарушителей и непредсказуемости их действий.

2. Систематические нарушители с низким или средним уровнем навыков – эта группа представляет большую угрозу, так как ее представители целенаправленно занимаются противоправной деятельностью в киберпространстве, часто в составе организованных преступных групп. Несмотря на относительно невысокий уровень технических навыков, они используют готовые инструменты и методы, распространяемые в даркнете, что позволяет им совершать фишинг, DDoS-атаки, распространять вредоносное ПО и заниматься другими видами киберпреступлений. Их мотивация, как правило, связана с финансовой выгодой.

3. Высококвалифицированные киберпреступники – наиболее опасная группа, состоящая из лиц с высоким уровнем технической компетенции. Они способны разрабатывать собственные уникальные вредоносные программы, взламывать сложные системы защиты и проводить сложные атаки. Их мотивация может быть различной, от финансовой выгоды до политических или идеологических целей. Выявление и пресечение деятельности этой группы

---

[1] Филиппов А. Г. Криминалистическая методика: учеб. пособ. для вузов / А. Г. Филиппов [и др.]. М.: Юрайт, 2025. С. 178.

требует высокой квалификации специалистов по кибербезопасности и применения передовых технологий.

Таким образом, изучение каждой из этих групп киберпреступников, их специфических характеристик и методов работы, является критически важным для разработки эффективных мер противодействия киберпреступности и обеспечения безопасности в цифровую эпоху.

В зависимости от целей и мотивации выделяются следующие категории киберпреступников[1]:

1. Фрикеры, стремящиеся к несанкционированному доступу к информационным системам, веб-ресурсам и учетным записям пользователей, действуя по заказу или руководствуясь мотивами развлечения и совершенствования технических навыков.

2. Кибертеррористы, использующие кибератаки для дестабилизации и нанесения ущерба объектам национальной безопасности, таким как государственные учреждения и объекты критической информационной инфраструктуры.

3. Крэкеры, осуществляющие несанкционированное проникновение в компьютерные системы с использованием специализированного программного обеспечения.

4. Разработчики вредоносного программного обеспечения (вирусописатели), создающие вредоносные программы (вирусы, троянские программы и др.) для получения доступа к информации, нарушения функционирования информационных систем или реализации на теневом рынке программного обеспечения (даркнет).

5. Фишеры (фишингеры), совершающие мошеннические действия с использованием электронных средств коммуникации (электронная почта,

---

[1] Киселев А. С., Горбунова К. А. Особенности криминалистической характеристики преступлений в сфере компьютерной информации // Актуальные проблемы государства и права. 2023. С. 370.

социальные сети) для получения доступа к конфиденциальной информации и финансовым средствам жертв путем обмана.

6. Кардеры, специализирующиеся на хищении финансовых данных посредством взлома банковских систем и интернет-магазинов, получая доступ к банковским счетам, номерам кредитных карт и другим платежным данным.

7. Бот-мастера, использующие ботнеты (сети зараженных компьютеров) для проведения кибератак, распространения вредоносного ПО, атак на веб-ресурсы и достижения других целей.

Способ совершения преступления в сфере компьютерной информации, согласно Вехову В. Б., представляет собой объективно и субъективно обусловленную систему действий субъекта до, во время и после совершения преступления[1]. Эта система оставляет следы, анализ которых криминалистическими методами позволяет реконструировать событие преступления, особенности поведения правонарушителя, его личностные характеристики и определить оптимальные стратегии раскрытия преступления. В настоящее время преступления в сфере компьютерной информации выходят за рамки виртуального пространства. Отдельные виды вредоносного ПО способны не только воздействовать на информационные системы, но и оказывать непосредственное влияние на физические объекты.

Состав способов совершения компьютерных преступлений многообразен и варьируется в зависимости от изобретательности, технической оснащенности, мотивации, интеллектуальных способностей и уровня подготовки преступника. Представить исчерпывающий перечень всех возможных способов затруднительно. Среди распространенных методов можно выделить:

1. Создание и распространение вирусов, червей, троянских программ, шпионского ПО для получения контроля над компьютерными системами.

2. Использование методов социальной инженерии и фишинговых атак для получения конфиденциальной информации.

---

[1] Вехов В.Б. Компьютерные преступления. Способы совершения, методики расследования. М.: Право и Закон, 1996. С.12.

3. Несанкционированное проникновение в компьютерные сети с целью получения доступа к данным или нарушения их функционирования. Так, 12 июля 2023 года неизвестный, находясь в неустановленном месте, умышленно, реализуя преступный умысел на неправомерный доступ к охраняемой законом компьютерной информации, действуя из корыстной заинтересованности, незаконно проник в личный кабинет «Госуслуг» гр. Б. без её ведома и путем неправомерного копирования информации, а именно обновили справку 2-НДФЛ, просмотрели кредитную историю[1].

4. Кража личных данных пользователей, включая финансовую информацию, пароли и другую конфиденциальную информацию.

5. Кибершпионаж – сбор информации с помощью компьютерных систем с целью получения конкурентных преимуществ или разведывательной информации.

6. Кибертерроризм – атаки на критическую информационную инфраструктуру или захват компьютерных систем с целью нанесения ущерба или нарушения общественной безопасности.

Развитие технологий и сети интернет способствует появлению новых угроз и совершенствованию методов киберпреступников. Современные методы несанкционированного доступа к информации на смартфонах включают, например, создание искусственных отпечатков пальцев для аутентификации. Программные методы охватывают разработку, распространение и использование вредоносного ПО, модификацию легитимного ПО и его использование в преступных целях[2].

Статья 273 УК РФ определяет вредоносную программу как компьютерную информацию или программу, способную незаконно удалять,

---

[1] Уголовное дело № 1-859/2023 по обвинению Б. в совершении преступления, предусмотренного ч.1 ст. 272 УК РФ // Архив Стерлитамакского городского суда РБ.

[2] Александров И. В. Криминалистика в 5 т. Том 5. Методика расследования преступлений: учеб. для вузов. М.: Издательство Юрайт, 2025. С. 178.

блокировать, модифицировать или похищать цифровую информацию, а также нейтрализовать средства защиты компьютерной информации.

Выяснение обстановки совершения преступления, включая место и время, является важным элементом расследования любого преступления, в том числе и в сфере компьютерной информации. Однако установление этих параметров в контексте киберпреступлений представляет особую сложность, обусловленную виртуальным характером деяния, потенциальными жертвами которого могут быть как отдельные лица, так и государства. Это обуславливает специфический подход к определению места совершения преступления в сфере компьютерной информации. Данные о месте и времени совершения преступления критически важны для установления причинно-следственных связей и доказательства причастности обвиняемого.

Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37[1] разъясняет, что местом совершения киберпреступления считается место фактического осуществления преступных действий. Использование VPN-сервисов значительно затрудняет установление места совершения преступления. Кроме того, текущая геополитическая ситуация осложняет международное сотрудничество в сфере экстрадиции лиц, подозреваемых в совершении преступлений против граждан Российской Федерации. Установление времени совершения киберпреступления также сопряжено с определенными трудностями. В.В. Поляков отмечает зависимость работы некоторых программ от времени, установленного на компьютере, которое может быть изменено злоумышленником. Определение точного времени совершения преступления затрудняется отсутствием синхронизации по времени. Следовательно, киберпреступления могут быть совершены в любое время суток,

[1] Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». URL: http://www.consultant.ru. (дата обращения: 12.05.2025).

в зависимости от целей, потребностей и технических возможностей преступника[1].

Преступления в сфере компьютерной информации характеризуются рядом специфических особенностей: преступления совершаются в киберпространстве, среде, изначально лишенной физических объектов. Так, кража данных с сервера компании происходит в виртуальной среде, хотя последствия могут иметь вполне реальный характер (финансовые потери, репутационный ущерб); необходимость проведения компьютерно-технической экспертизы, для определения источника DDoS-атаки специалисты анализируют сетевые протоколы и логи серверов. Эта экспертиза включает изучение жестких дисков, сетевого трафика, программного обеспечения и других компонентов компьютерных систем; киберпреступность охватывает широкий спектр деяний (хакерство (взлом аккаунтов), распространение вредоносного ПО (вирусов, программ-вымогателей), кибермошенничество (фишинг), нарушение авторских прав в цифровой среде и другие преступления, предусмотренные главой 28 УК РФ); использование информационно-телекоммуникационных технологий в качестве инструмента для совершения других преступлений (взлом базы данных клиентов банка для последующего хищения денежных средств со счетов, тем самым это усложняет квалификацию деяния и сбор доказательств); киберпреступления могут совершаться из любой точки мира и быть направлены против жертв в других странах; расследование требует от правоохранительных органов специальных знаний и навыков в области информационных технологий, поскольку методы киберпреступников постоянно эволюционируют, так для анализа вредоносного ПО требуются специалисты, обладающие глубокими знаниями в области программирования и анализа кода; доказательства по киберпреступлениям – это электронные следы (электронно-цифровые следы), например, логи серверов, электронная переписка, сетевые

---

[1] Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. 2013. С. 114.

данные, история браузера. Их сбор, анализ и представление в суде требуют специальных методов и инструментов; противодействие киберпреступности во многом опирается на превентивные меры.

Криминалистическая характеристика преступлений в сфере компьютерной информации включает сбор данных о личности преступника, способе, месте и времени совершения преступления, мотивах и целях, использованных технологиях и программном обеспечении. Компетенции следователей в области информационно-телекоммуникационных технологий играют ключевую роль в эффективности расследования. Анализ криминалистической характеристики позволяет выявить типовые способы совершения киберпреступлений и разработать адекватные меры противодействия.

Высококвалифицированные киберпреступники применяют контрмеры против правоохранительных органов, используя шифрование, программы удаленного доступа и другие методы для затруднения сбора доказательств и розыскных мероприятий. Криминалистическая характеристика способствует оптимизации процесса расследования и применению современных криминалистических методов и средств.

Основная сложность расследования киберпреступлений обусловлена их технологической сложностью и спецификой порядка совершения. Детальное выявление этапов и методов совершения киберпреступлений является важным направлением дальнейших научных исследований в данной области.

ГЛАВА 2. ТАКТИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Особенности осмотра места происшествия, обыска и выемки

На начальном этапе расследования преступлений в сфере компьютерной информации первоочередными задачами являются осмотр места происшествия, включающий в себя осмотр компьютерного оборудования, а также проведение обыска и выемки с целью обнаружения, фиксации и изъятия компьютерной информации и технических средств, имеющих отношение к расследуемому событию. Данный этап важен, так как компьютерная информация зачастую является непосредственным объектом преступного посягательства, а неправомерный доступ к ней требует незамедлительной и процессуально грамотной фиксации. Это обусловлено высокой вероятностью ее быстрой и безвозвратной модификации или уничтожения, что может привести к безвозвратной утрате важных цифровых следов преступления. Осмотр места происшествия при расследовании компьютерных преступлений приобретает особую значимость именно в связи с динамичностью цифровой среды и потенциальной возможностью изменения исходного состояния сетевых объектов, что может затруднить или сделать невозможным восстановление хронологии событий.

В расследовании преступлений в сфере компьютерной информации криминалистически значимой информацией может быть широкий спектр цифровых объектов и документов. Это не просто набор электронных данных, а те элементы, которые непосредственно связаны с расследуемым событием и могут служить доказательствами. К таким источникам относятся, в первую очередь, сами устройства вычислительной техники: серверы, персональные

компьютеры, ноутбуки, планшеты, смартфоны и другие гаджеты, которые могли быть использованы для совершения или подготовки преступления.

Кроме того, это могут быть носители информации, на которых хранятся данные: жесткие диски, флеш-накопители, а также облачные хранилища и другие виды удаленных серверов. Важны не только сами носители, но и их содержимое: файлы различных форматов (текстовые документы, изображения, видео, аудио), программное обеспечение (включая вредоносные программы), логи системных событий и приложений, сетевые данные (например, история посещенных веб-сайтов, IP-адреса), метаданные файлов (дата создания, изменения, авторство), и другие цифровые артефакты, которые могут указывать на обстоятельства преступления.

Ключевым моментом является установление прямой связи между обнаруженными цифровыми объектами и расследуемым преступлением. Только в этом случае они приобретают статус доказательств и могут быть использованы в судебном процессе. Поэтому при сборе и анализе цифровой информации важно соблюдать процессуальные нормы и фиксировать все действия для обеспечения допустимости полученных доказательств.

Последствия противоправных действий в цифровой среде проявляются в изменении характеристик объектов и документов, формируя специфические цифровые следы преступления. Процессы поиска, обнаружения, фиксации и исследования этих следов, включая документы на нетрадиционных носителях (например, в облачных сервисах), а также их изъятие и осмотр, характеризуются рядом особенностей, диктующих необходимость повышенной тщательности и применения специализированных методов и инструментов при производстве данных следственных действий. Некорректные действия на данном этапе могут скомпрометировать доказательства и поставить под угрозу весь процесс расследования.

Одной из ключевых проблем в расследовании компьютерных преступлений является определение места происшествия, которое может быть многосоставным. Ввиду многоаспектности понятия «место совершения

компьютерного преступления», поиск и фиксация цифровой информации осуществляется на различных объектах, связанных с преступлением. К таким объектам относятся места: обработки и постоянного хранения информации, подвергшейся преступному посягательству; использования компьютерного оборудования для неправомерного доступа к защищенным базам данных или создания и распространения вредоносных программ; хранения информации, незаконно полученной из других компьютерных систем и сетей; нарушения правил эксплуатации средств хранения, обработки или передачи информации и информационно-телекоммуникационных сетей; а также места наступления негативных последствий преступления[1].

При осмотре информации, размещенной в сети Интернет, следователь может установить следующие обстоятельства:

1. Факт отображения информации в определенный момент времени.

2. Адрес сайта или веб-страницы, содержащей данную информацию.

3. Принадлежность сайта или страницы конкретному физическому или юридическому лицу.

Целью осмотра места происшествия является идентификация вычислительной техники и компьютерной информации, выступающих в качестве предмета или орудия преступления, а также содержащих следы преступной деятельности.

Осмотр места происшествия при расследовании компьютерных преступлений включает исследование служебных и жилых помещений, вычислительной техники, носителей информации, документов, предметов и прочих объектов, потенциально связанных с преступлением. В силу специфики работы с компьютерной техникой и информацией, к участию в следственных действиях привлекаются специалисты различных профилей, таких как: программисты (специализирующиеся на операционных системах и прикладном программном обеспечении); электронщики; специалисты

---

[1] Протасевич А. А., Зверянская Л. П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2023. № 11. С. 46.

по средствам связи и телекоммуникациям; сетевые специалисты; специалисты в области экономики, финансов и бухгалтерского учета, в том числе обладающие навыками работы со специализированным финансовым и учетным программным обеспечением; а также другие специалисты, знания которых могут оказаться необходимыми[1].

При проведении осмотра и обыска необходимо учитывать, что компьютерное оборудование и информация могут быть одновременно предметом посягательства, орудием преступления и хранилищем доказательств. Следовательно, поиск, обнаружение, фиксация и изъятие должны охватывать все возможные следы, связанные с этими функциями, включая: данные о незаконных финансовых операциях; программы, используемые для проведения электронных платежей через интернет, включая списки транзакций с чужих счетов и кредитных карт; программы для онлайн-торговли; переписку соучастников, связанную с преступлением; информацию, составляющую государственную, коммерческую или банковскую тайну; нелицензионное программное обеспечение и базы данных; личную переписку; порнографические материалы; вредоносные программы; файлы с конфиденциальной информацией, незаконно полученной данным лицом; и зашифрованные данные, связанные с преступлением.

Кроме цифровых доказательств, важно обнаружить и изъять традиционные вещественные доказательства, такие как: распечатки с принтера; записи кодов доступа и паролей; тексты программ и документацию к программному обеспечению; записные книжки (включая электронные) с информацией о соучастниках, номерами телефонов, банковских счетов и PIN-кодами; кредитные карты, использованные для обналичивания похищенных средств; вещи, приобретенные на похищенные деньги; счета за услуги провайдера; нестандартные периферийные устройства и устройства доступа к компьютерным и телефонным сетям; документы

[1] Сысенко А. Р. Особенности осмотра места происшествия при расследовании компьютерных преступлений // Закон и право. 2020. С. 216.

и инструкции, регламентирующие работу с компьютерной системой, с пометками сотрудника; и личные документы преступников.

Если доступ к компьютерной системе осуществлялся посторонним лицом, важно сосредоточиться на поиске традиционных следов преступления, таких как отпечатки пальцев на клавиатуре, мониторе, системном блоке и мебели, следы обуви, следы взлома и проникновения в помещение.

При выемке изымаются документы, регламентирующие правила эксплуатации компьютерной техники и информационно-телекоммуникационных сетей, необходимые для установления факта нарушения этих правил. К таким документам относятся: инструкции производителя по эксплуатации оборудования и правила доступа к сетям; правила работы в компьютерной системе, установленные владельцем; журналы регистрации сбоев и технического обслуживания оборудования; материалы служебного расследования по факту нарушения правил эксплуатации; документы, подтверждающие отнесение информации к коммерческой тайне; приказы о назначении на должность и должностные инструкции; документы, подтверждающие квалификацию сотрудника для работы с оборудованием; и другие релевантные документы. Осмотры, обыски и выемки предоставляют важную информацию для дальнейшего расследования.

Обобщая рекомендации, представленные в научной литературе относительно производства осмотра места происшествия, обыска и выемки по делам о компьютерных преступлениях, можно выделить следующие тактические приемы:

1. Осмотр начинается с изучения обнаруженной вычислительной техники. Это включает определение технических параметров основного (компьютеры, серверы), периферийного (принтеры, сканеры) и вспомогательного оборудования (сетевые устройства), а также фиксацию подключения к сетям (Интернет, локальные сети);

2. Важно обеспечить сохранность всех объектов, включая программное обеспечение, данные, кабели и расположение предметов;

3. Запрещено выполнять действия с техникой (включение, выключение, запуск программ), если результат непредсказуем;

4. При участии специалиста необходимо определить назначение и состав установленного и (или) функционирующего на момент осмотра программного обеспечения. В случае обнаружения программы, осуществляющей уничтожение информации, ее действие следует остановить при содействии специалиста;

5. Копирование информации, представляющей интерес для следствия, должно производиться на предварительно подготовленные носители информации. Если копирование данных нежелательно по техническим причинам, следует изъять системный блок или иной носитель информации.

Расследование компьютерных преступлений требует специфических знаний и навыков, поэтому для достижения максимальной эффективности следователю необходимо следовать определенным криминалистическим рекомендациям:

1. Привлечение квалифицированного специалиста в области вычислительной техники и информационных технологий. В зависимости от сложности ситуации, могут потребоваться эксперты узкого профиля, например, специалисты по сетевой безопасности, анализу вредоносного ПО, восстановлению данных или эксперты по конкретным операционным системам. При работе со сложными системами или корпоративными сетями рекомендуется привлекать группу специалистов с разной специализацией для обеспечения всестороннего анализа;

2. Обеспечение взаимодействия с органами дознания, специализирующимися на расследовании преступлений в сфере информационных технологий. Их опыт и знания помогут эффективно собрать и проанализировать цифровые доказательства;

3. Проведение инструктажа для следственно-оперативной группы о специфике работы с цифровыми доказательствами. Важно подчеркнуть важность сохранения целостности данных, предотвращения их случайного изменения или удаления.

4. Обеспечение присутствия понятых, но в случае компьютерных преступлений желательно, чтобы они обладали базовыми знаниями в области вычислительной техники. Это позволит им адекватно воспринимать производимые действия и подтверждать их правильность, исключая возможность оспаривания протокола осмотра места происшествия.

5. Техническое оснащение для фиксации и изъятия цифровых доказательств. Это включает в себя фотоаппараты и видеокамеры для документирования места происшествия, специализированное программное обеспечение для создания образов жестких дисков и других носителей информации, антистатические пакеты для безопасной транспортировки электронных устройств, маркировочные средства для идентификации изъятых объектов. Также могут понадобиться аппаратные блокираторы записи для предотвращения случайной модификации данных на носителях информации при их подключении к устройствам.

Соблюдение этих рекомендаций позволит максимально эффективно собрать и сохранить цифровые доказательства, что существенно повысит шансы на успешное расследование компьютерных преступлений.

Внешний осмотр компьютера рекомендуется начинать с его тыльной стороны, где расположены разъемы, кабели питания и сетевые подключения. Это позволяет идентифицировать подключенные устройства и оценить сетевую конфигурацию[1].

В протоколе осмотра необходимо детально зафиксировать: описание места установки и эксплуатации техники, наличие других электронных устройств; точное местоположение каждого устройства относительно других объектов; наличие или отсутствие подключений к внешним устройствам или сетям, находящимся вне зоны осмотра; описание внешнего вида компьютерных средств, наличие видимых повреждений, следов взлома; фиксация любых

---

[1] Хатунцев Н. А. О специальных знаниях, необходимых при исследовании компьютерных средств и систем // Актуальные проблемы российского права. 2024. № 1. С. 335.

следов, которые могут быть связаны с преступником (отпечатки пальцев, волосы и т.д.). Подробное и точное документирование всех деталей осмотра места происшествия является залогом успешного расследования компьютерного преступления.

В заключение следует подчеркнуть, что осмотр места происшествия, обыск и выемка в сфере компьютерной информации имеют свою специфику, обусловленную особенностями цифровых доказательств. Успешное расследование компьютерных преступлений требует от правоохранительных органов не только знания процессуальных норм, но и понимания технических аспектов функционирования компьютерных систем и сетей. Комплексный подход, включающий привлечение квалифицированных специалистов и тщательное документирование всех этапов следственных действий, позволяет эффективно собирать и фиксировать цифровые доказательства, что является залогом успешного раскрытия и расследования преступлений в сфере высоких технологий. Только грамотно проведенные осмотр, обыск и выемка могут обеспечить сохранность и допустимость полученных доказательств, необходимых для привлечения виновных к уголовной ответственности.

§ 2. Тактика допроса подозреваемых и (или) обвиняемых в сфере компьютерной информации

Расследование преступлений в сфере компьютерной информации предполагает осуществление комплекса следственных и иных процессуальных действий, регламентированных уголовно-процессуальным законодательством. Тактика производства данных действий детерминирована спецификой механизма совершения рассматриваемого вида преступлений. Оптимальным условием эффективного расследования является наличие у следователя глубоких познаний в области информационных технологий. Необходимость подобной квалификации обусловлена потребностью в точной

интерпретации цифровых следов, анализе сложных технических систем и продуктивном взаимодействии со специалистами в данной сфере. Отсутствие соответствующей квалификации может привести к неполному сбору доказательств, ошибкам в их оценке и, как следствие, к неправильной квалификации деяния или невозможности привлечения виновных лиц к уголовной ответственности. Поэтому специализация следователей и повышение их квалификации в сфере информационных технологий представляется актуальной задачей для совершенствования уголовного судопроизводства в условиях цифровизации.

Анализ правоприменительной практики демонстрирует, что среди следственных действий, осуществляемых при расследовании компьютерных преступлений, значительную роль играет допрос. Данное следственное действие является неотъемлемым элементом практически каждого уголовного дела. Тактика проведения допроса по данной категории дел непосредственно коррелирует со спецификой механизма совершения преступления и совокупностью влияющих факторов, как позитивных, так и негативных.

К позитивным факторам относится наличие определенного объема информации о преступном событии, полученной из различных источников (материалы предварительной проверки, результаты оперативно-розыскной деятельности и т.д.), а также сведения о допрашиваемом лице (ранее данные объяснения, протоколы иных процессуальных действий и т.д.). Негативные факторы могут включать значительный временной интервал между совершением преступления и моментом допроса, что может негативно сказаться на полноте и достоверности показаний.

Допрос потерпевших, свидетелей и обвиняемых по делам в сфере компьютерной информации требует от следователя применения особых тактических методов и приемов, учитывающих специфику данной категории дел. Под тактическим приемом в криминалистике понимается продуманная и рациональная линия поведения следователя, направленная на эффективный

сбор, исследование, оценку и использование доказательств в рамках расследования конкретного уголовного дела.

Хотя общие правила производства допроса регламентируются ст. 164 УПК РФ и применимы ко всем уголовным делам, включая дела о преступлениях в сфере компьютерной информации, специфика цифровых доказательств требует от следователя более глубокого понимания технических аспектов и умения задавать корректные вопросы, чтобы получить полную и достоверную информацию.

Например, следователю может потребоваться знание основ сетевых технологий, шифрования данных, методов взлома и других технических деталей, чтобы правильно интерпретировать показания допрашиваемого и выявить противоречия. Также важно уметь адаптировать язык вопросов к уровню технической грамотности допрашиваемого, избегая чрезмерно сложной терминологии или, наоборот, упрощений, которые могут исказить смысл показаний.

В случаях, когда в уголовном судопроизводстве участвуют несовершеннолетние, следователь обязан руководствоваться дополнительными положениями статьи 191 УПК РФ, обеспечивая защиту их прав и интересов, а также создавая доверительную атмосферу во время допроса. Это может включать в себя привлечение педагога или психолога, адаптацию языка и способа задания вопросов к возрасту и психологическим особенностям несовершеннолетнего.

Кроме того, специфика механизма компьютерного преступления обуславливает необходимость обладания знаниями о виртуальной среде, в которой оно совершается, об особенностях компьютерной информации, а также о применяемых орудиях и средствах – компьютерах, технически сложных устройствах, носителях информации, компьютерных сетях и способах доступа к ним. Данные знания необходимы для всестороннего выяснения элементов и обстоятельств преступного деяния.

Допрос подозреваемого (обвиняемого) предполагает применение определенных тактических приемов, направленных на получение информации, имеющей значение для расследования. Тактика допроса определяется совокупностью факторов, среди которых ключевыми являются:

1. Цель допроса (определение необходимой информации, ожидаемой от допроса);

2. Характеристика допрашиваемого лица (процессуальный статус, социально-демографические характеристики, личностные особенности, интеллектуальные способности, профессиональная деятельность и социальное окружение);

3. Объем информации о событии преступления, известный допрашиваемому (сопоставление информации, полученной в ходе допроса, с имеющимися следственными версиями);

4. Обстановка допроса. В идеальных условиях допрашиваемый спонтанно сообщает все известные ему обстоятельства дела. Однако, как отмечают исследователи, установление продуктивного взаимодействия с допрашиваемым не всегда возможно в силу объективных причин.

Хотя общие принципы планирования допроса свидетеля, подозреваемого и потерпевшего схожи, допрос подозреваемого имеет свою специфику. Его неотложность, обусловленная проведением непосредственно после задержания, ограничивает время на подготовку. Главная цель такого допроса – быстрое получение информации, важной для установления фактических обстоятельств дела. Допрос подозреваемого (обвиняемого) часто проходит в конфликтной обстановке. Однако, как отмечает Э.Т. Хайрулловой, нет единого мнения об оптимальных тактико-психологических методах получения достоверной и полной информации в условиях конфликтного допроса и эффективного противодействия сокрытию информации[1].

---

[1] Хайруллова Э. Т. Применение психологических приемов в тактике допроса подозреваемых и обвиняемых // Криминалистика: вчера, сегодня, завтра. 2021. С. 140.

В оптимальных условиях допрос позволяет получить достоверную информацию, подтверждающую или опровергающую фактические обстоятельства уголовного дела. Однако на практике следователю часто приходится применять специальные методы для получения необходимых данных. Существуют базовые тактические приемы, используемые следственными органами различных стран, в том числе и России, для выявления ложных показаний. Гладких А. В. определяет общую тактическую линию допроса как установление психологического контакта с допрашиваемым и активизацию его памяти при даче правдивых показаний, а в случае лжесвидетельства – изобличение и получение достоверной информации[1]. При этом фундаментальным принципом тактики допроса является строгое соблюдение законности, а принуждение к даче показаний преследуется по закону.

Анализ особенностей преступлений в сфере компьютерной информации показывает, что в 87 % случаев подозреваемыми и обвиняемыми являются начинающие пользователи или «скрипт-кидди» (молодые хакеры). В отличие от рядовых исполнителей, опытные хакеры, организаторы преступных групп и разработчики вредоносного ПО реже становятся фигурантами уголовных дел. Поэтому допросы по таким делам обычно не требуют специальных тактических приемов. Зачастую достаточно классических методов ведения допроса -в конфликтной ситуации, так как обвиняемые, как ни странно, нередко сами раскрывают детали совершенного преступления.

В ходе расследования уголовного дела по ч. 2 ст. 272 УК РФ в отношении гр. К., допрошенного в качестве подозреваемого, было установлено следующее. К., имеющий неполное среднее образование, безработный, с низким уровнем знаний в области информационных технологий, умышленно, с целью неправомерного доступа к охраняемой законом компьютерной

---

[1] Гладких А. В. Тактика ведения допроса: проблемные аспекты в криминалистике // Современные технологии в юриспруденции: применение специальных познаний. 2021. С. 28.

информации, незаконно проник в аккаунт потерпевшей без её ведома и путем неправомерного копирования информации высылал смс об одолжение денег от ее имени с целью наживиться. В ходе допроса К. полностью признал вину, предоставил изобличающие его сведения и согласился на сотрудничество со следствием, в результате чего с ним было заключено досудебное соглашение о сотрудничестве[1].

Допрос подозреваемого – это коммуникативный процесс, протекающий либо в конфликтной, либо в бесконфликтной обстановке. Конфликтная ситуация проявляется в напряженности, защитной позиции и отрицании вины допрашиваемым. Бесконфликтная же, наоборот, предполагает его готовность к сотрудничеству со следствием. В этом случае важно установить доверие и создать комфортную атмосферу, располагающую к конструктивному диалогу. Далее необходимо рассмотреть тактические рекомендации по проведению допроса в сфере компьютерной информации с учетом индивидуальных психологических особенностей подозреваемого (обвиняемого).

Подготовка к допросу по делам, связанным с киберпреступлениями, включает ряд ключевых задач. Первостепенной является тщательный анализ имеющихся материалов. Особое внимание уделяется временным параметрам совершения преступления, идентификации IP-адресов и другим цифровым следам, позволяющим реконструировать хронологию событий и оценить вероятность причастности подозреваемого. Критическая оценка источников информации на предмет достоверности, выявление потенциальных искажений, ошибок или заведомо ложных сведений – обязательный этап анализа. Выявление корреляций между отдельными эпизодами, а также обстоятельств, свидетельствующих о виновности или невиновности подозреваемого, способствует формированию целостной картины преступления.

Следующим этапом является разработка вопросов для допрашиваемого. Вопросы должны быть сформулированы четко, логично и однозначно, исключая

---

[1] Уголовное дело № 1-977/2023 по обвинению К. в совершении преступления, предусмотренного ч. 2 ст. 272 УК РФ // Архив Стерлитамакского городского суда РБ.

наличие логических ловушек или подсказок. Определение тактики и методики допроса, включая приемы и методы воздействия, а также механизмы контроля за процессом, является важной составляющей подготовки.

В отдельных случаях может быть установлен регламент по времени проведения допроса. Завершающая стадия подготовки включает сбор и проверку документальных материалов, фотографий, видеозаписей, электронных файлов и других релевантных данных.

Техническая готовность к воспроизведению цифровых доказательств обеспечивает эффективность допроса и повышает вероятность получения дополнительной информации. В силу специфики киберпреступлений, для квалифицированной подготовки к допросу целесообразно привлечение экспертов в области информационно-компьютерных технологий. Консультации специалистов компенсируют отсутствие у следователя специальных знаний в данной области и позволяют глубоко и всесторонне анализировать показания допрашиваемого.

Определение целей допроса является важнейшим этапом подготовки. Следователь применяет классические следственные приемы для сбора информации, позволяющей, как отмечает Акопян А. М., «диагностировать состояние допрашиваемых на начальных этапах и впоследствии выстроить эффективную тактику, нейтрализующую противодействие расследованию»[1].

Расследование данного вида преступлений требует глубокого изучения личности подозреваемого (обвиняемого) для установления всех обстоятельств дела и определения степени его вины. Этот процесс включает в себя сбор всесторонней характеризующей информации, которая выходит далеко за рамки простого установления личности.

Одним из ключевых направлений является допрос окружения подозреваемого – родственников, друзей, коллег, знакомых. Свидетельские

---

[1] Акопян Р. М. Проблемы тактики допроса подозреваемого (обвиняемого) // Восточно-Европейский научный журнал. 2022. С. 54.

показания позволят получить представление о его увлечениях, умениях, потенциальных мотивах и связях с другими людьми.

Параллельно с этим следователь направляет запросы в различные органы и организации: учебные заведения, места работы, интернет-провайдеров и др. Цель – получить информацию об образовании подозреваемого, его профессиональном опыте, уровне знаний и навыков в сфере информационных технологий, а также о его онлайн-активности и истории использования интернет-ресурсов. Особое внимание уделяется выявлению специализированных знаний и навыков, которые могли быть использованы для совершения преступления.

Важным этапом является установление наличия и местонахождения средств компьютерной техники, которые могли быть использованы при совершении преступления: компьютеров, ноутбуков, смартфонов, внешних носителей информации и т.д. Производится их изъятие и последующая экспертиза для поиска цифровых доказательств.

Следователь также определяет, действовал ли подозреваемый в одиночку или в составе группы. В случае группового преступления устанавливаются роли каждого участника, их взаимосвязи и иерархия.

Наконец, изучается возможная связь подозреваемого с хакерской субкультурой: участие в онлайн-форумах, группах в социальных сетях, использование специализированных программ и сервисов. Это позволяет оценить уровень технической подкованности подозреваемого, его потенциальные возможности и мотивы.

Всесторонний анализ собранной информации позволяет составить полный психологический портрет подозреваемого, выявить его мотивы и цели, а также определить степень его вовлеченности в совершенное преступление.

Выбор места проведения допроса обусловлен необходимостью обеспечения конфиденциальности и создания соответствующей психологической атмосферы. В качестве места проведения, как правило,

используется кабинет следователя. Предпочтительны специально оборудованные помещения, оснащенные аудио- и видеоаппаратурой для фиксации процесса допроса. Необходимо обеспечить безопасность помещения, исключив возможность несанкционированного доступа или наблюдения. Перед началом допроса проводится проверка работоспособности технических средств записи (микрофонов, камер и др.). Рекомендуется также исключить из помещения потенциально отвлекающие факторы, способные повлиять на концентрацию и психологическое состояние допрашиваемого.

Специфика расследования киберпреступлений обуславливает необходимость учета особенностей противодействия со стороны подозреваемых. Зачастую подозреваемые демонстрируют уверенность в своем превосходстве в области информационных технологий по сравнению со следствием. В таких случаях целесообразно привлечение специалиста, способного оказать содействие как на этапе подготовки к допросу, так и непосредственно в ходе его проведения, предоставляя экспертную поддержку следователю.

В процессе допроса неукоснительно соблюдаются процессуальные нормы и правила, предусмотренные законодательством. Это включает гарантирование прав подозреваемого, в частности, права на защиту и получение квалифицированной юридической помощи. Соблюдение всех требований УПК РФ к проведению допроса является обязательным. В соответствии с ч. 1 ст. 307 УК РФ допрашиваемый предупреждается об уголовной ответственности за дачу заведомо ложных показаний. Данная информация доводится до сведения допрашиваемого в корректной форме, спокойным и уравновешенным тоном, исключая проявление эмоционального давления, способного вызвать страх или негативные реакции.

Люди с глубокими познаниями в информационных технологиях обычно более открыты к общению во время допроса. Следователю рекомендуется использовать адаптивную стратегию, задавая уточняющие вопросы

и демонстрируя понимание технических деталей. Это способствует установлению доверительных отношений и получению более полной информации. Примеры таких вопросов: «Правильно ли я понимаю, что данная программа используется для…?», «Могли бы вы подробнее объяснить, как работает этот алгоритм?», «Корректно ли я понял ваши слова в этом контексте?», «Не могли бы вы уточнить функциональные возможности этого программного обеспечения?». Создание конфликтной ситуации, наоборот, может негативно сказаться на результативности допроса, вызывая защитную реакцию и уклонение от ответов.

Однако, как отмечают Рачева Н. В. и Поскочинова К. А., «недостаток специальных технических знаний у следователя может столкнуться с серьезным интеллектуальным противодействием со стороны преступника». Некоторые высококвалифицированные киберпреступники, осознавая ограниченные возможности следствия без специального оборудования и экспертизы, уклоняются от сотрудничества, умышленно скрывая важную информацию[1].

В ходе расследования уголовного дела по ч. 3 ст. 272 и ч. 2 ст. 273 УК РФ против гр. А. и гр. Б., обладавших высокой компетенцией в области компьютерных технологий, было установлено, что они, действуя по предварительному сговору и из корыстных побуждений, неправомерно получили доступ к защищенной информации, модифицировали и распространили ее. Оба подозреваемых активно препятствовали расследованию, давая ложные и неполные показания. Следователю пришлось тщательно анализировать протоколы допросов, запрашивать данные у интернет-провайдера и привлекать свидетелей, чтобы выявить противоречия в показаниях. В результате виновность подозреваемых была доказана[2].

---

[1] Рачева Н. В., Поскочинова К. А. Проблемные аспекты допроса подозреваемых при расследовании киберпреступлений // Технологии XXI века в юриспруденции. 2020. С. 522.

[2] Уголовное дело № 1-971/2024 по обвинению гр. А. и гр. Б. в совершении преступления, предусмотренного ч.3 ст.272, ч.2 ст. 273 УК РФ // Архив Стерлитамакского городского суда РБ.

На этапе планирования допроса, совместно со специалистом в области информационных технологий, определяется уровень технической сложности совершенного преступления. Формулируются вопросы, устанавливается их последовательность, определяется порядок предъявления имеющихся у следствия материалов. Специалист предоставляет следователю необходимую терминологию для использования в процессе допроса. Как рекомендуют некоторые исследователи, моделирование хода допроса способствует более эффективной подготовке к его проведению.

Следователю необходимо подготовить материалы дела, выделив ключевые страницы и зафиксировав факты, требующие уточнения в ходе допроса. Подготавливаются схемы, фотографии и вещественные доказательства, располагаемые в определенном порядке.

Ситуационный подход предполагает использование показаний потерпевшего и свидетелей для уточнения и дополнения модели преступления, сформированной следователем. Расхождения между показаниями и установленными фактами могут свидетельствовать либо о преднамеренном искажении информации допрашиваемым, либо о неверной интерпретации данных следователем. Для минимизации рисков подобных ошибок применяется метод моделирования, позволяющий создать графическую или компьютерную модель преступления.

Рабочий этап допроса включает следующие стадии:

1. Вступительная часть. На данном этапе устанавливается контакт с допрашиваемым. Важно продемонстрировать внимательное и уважительное отношение, особенно к свидетелям, чьи показания могут иметь существенное значение для расследования.

2. Свободный рассказ. Допрашиваемому предоставляется возможность в свободной форме изложить информацию о совершенном преступлении. Следователю необходимо активно слушать, полностью концентрируясь на рассказе допрашиваемого. Фиксация показаний посредством аудио- или видеозаписи повышает достоверность полученной информации.

3. Постановка вопросов. Начиная допрос, важно установить уровень технической компетентности подозреваемого. Необходимо уточнить у него степень владения информационными технологиями, попросить описать свой опыт работы в IT-сфере, если таковой имеется. Уточнить, какие программные продукты и операционные системы он использует регулярно. Также важно выяснить, знаком ли подозреваемый с методами взлома или обхода систем безопасности, и имеет ли он доступ к специализированному оборудованию или программному обеспечению, которое потенциально может быть использовано для совершения киберпреступлений. Переходя к вопросам, непосредственно связанным с расследуемым преступлением, необходимо выяснить, знаком ли подозреваемый с конкретными цифровыми объектами, имеющими отношение к делу, такими как IP-адреса, доменные имена или специфическое программное обеспечение. Следует попросить его объяснить свое присутствие в определенном месте или сети в указанное время, а также узнать, располагает ли он какой-либо информацией о самом инциденте, будь то атака, взлом или другое киберпреступление. В отношении цифровых следов, обнаруженных в ходе расследования, важно установить, распознает ли подозреваемый конкретные файлы, фрагменты кода или логи. Потребуется объяснение происхождения этих файлов или данных на его устройствах.

Завершающая стадия допроса включает подведение итогов, разъяснение дальнейших действий и анализ полноты достижения целей, поставленных на этапе планирования.

Тактика допроса при расследовании данного вида преступлений имеет первостепенное значение для раскрытия дела. Основные цели допроса – это реконструкция событий преступления, поиск свидетелей и идентификация потенциальных подозреваемых. Допрос подозреваемого направлен на получение информации о методах, использованных для несанкционированного доступа к компьютерной системе, о характере действий, совершенных внутри системы (например, кража данных, установка вредоносного ПО, нарушение работы системы), а также на установление, действовал ли подозреваемый в одиночку

или в составе группы. Выяснение этих ключевых деталей позволяет следователю сформировать более полную картину преступления, определить круг лиц, причастных к его совершению, и собрать необходимые доказательства для предъявления обвинения.

Кроме того, полученная в ходе допроса информация может помочь в предотвращении подобных преступлений в будущем, например, путем выявления уязвимостей в системах безопасности.

§ 3. Назначение и производство судебных экспертиз

Расширение спектра способов совершения преступлений в сфере компьютерной информации и разнообразие их составов приводят к несоответствию традиционных криминалистических методов и алгоритмов расследования специфике киберпреступлений. Это обусловлено прежде всего характером электронной (цифровой) информации, выступающей в качестве средства совершения киберпреступлений или объекта преступного посягательства. Несмотря на потенциальную доступность данной информации для широкого круга лиц, ее корректное получение, осмотр и исследование требуют участия специалистов, обладающих необходимыми компетенциями. Практически любое взаимодействие с компьютерной информацией в рамках расследования предполагает применение специальных знаний. Именно применение специальных знаний как на стадии изъятия аппаратного обеспечения, так и при последующем экспертном исследовании (включая анализ программного обеспечения и данных) позволяет придать изъятым объектам статус доказательств.

Компьютерно-техническая экспертиза (далее – КТЭ) обеспечивает принципы разработки и использования компьютерных средств, участвующих в информационных процессах, отраженных в материалах уголовных или гражданских дел. Установление объективной истины часто требует анализа

компонентов компьютерных систем и их функционала в различных областях деятельности. Несмотря на отсутствие четкого определения КТЭ в научной литературе, ее суть раскрывается через описание объектов исследования. Россинская Е. Р. связывает термин «компьютерно-техническая экспертиза» с инженерно-техническим происхождением вычислительной техники. Она отмечает историческую связь термина «компьютерная техника» с различными видами обеспечения автоматизированных систем управления (математическим, лингвистическим, техническим, программным, информационным и др.), рассматривая его как предшественника термина «судебная компьютерно-техническая экспертиза» (далее – СКТЭ)[1].

Термин «компьютерно-техническая экспертиза» считается наиболее подходящим, так как оно охватывает и аппаратные объекты (персональные компьютеры, периферийные устройства, сетевое оборудование, мобильные телефоны, иммобилайзеры, карты памяти и др.), так и ПО, информационные данные (текстовые и графические документы, базы данных, лог-файлы), а также компоненты компьютерных сетей[2]. В практике экспертной деятельности часто встречаются мультимедийные данные, такие как видео- и аудиозаписи. Таким образом, данный термин адекватно отражает широкий спектр объектов исследования в рамках данного вида экспертизы.

Россинская Е. Р. и Галяшина Е. И. определяют СКТЭ как исследование, проводимое с целью определения статуса объекта как компьютерного средства, выявления его роли в расследуемом преступлении и получения доступа к информации на носителях данных для последующего анализа. Данное определение, в целом, корректно отражает назначение СКТЭ. Однако авторы сужают предмет КТЭ до технического исследования компьютера, в то время как ключевой задачей расследования киберпреступлений является установление

---

[1] Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: моногр. М.: Норма: Инфра-М, 2018. С.233.

[2] Сысенко А. Р., Смирнова И. С., Тимошенко С. Е. Проблемы назначения и производства судебной компьютерно-технической экспертизы // Сибирское юридическое обозрение. 2020. С. 523.

цифровых (виртуальных) следов преступной деятельности в сети Интернет и идентификация лица, совершившего данную деятельность[1].

Таким образом, несмотря на то, что компьютер (в широком смысле, включая любое электронно-вычислительное устройство, его компоненты и носители цифровой информации) входит в область исследования КТЭ, он не всегда является ее непосредственным предметом. Техническая диагностика компьютерного оборудования сама по себе не всегда достаточна для достижения целей расследования киберпреступлений. Ключевое значение имеет установление факта использования компьютера для совершения противоправных действий.

В рамках КТЭ эксперт, реконструируя процесс формирования следов с учетом особенностей отображения цифровых (виртуальных) следов, анализирует механизм их образования и возможность его реализации в конкретных условиях.

Целью КТЭ является получение информации о таких видах противоправной деятельности, как: несанкционированный доступ к информационным системам и перехват данных; хищение оплаченного времени в информационно-телекоммуникационных сетях; распространение вредоносного программного обеспечения; распространение материалов, содержащих детскую порнографию; нарушение авторских прав в сфере программного обеспечения; мошенничество с использованием банкоматов и платежных систем; мошенничество в области мобильной связи и платежей; изготовление и распространение специальных технических средств, предназначенных для негласного получения информации; незаконное распространение баз данных, содержащих конфиденциальную информацию; сетевой экстремизм и использование информационных сетей для осуществления террористической деятельности.

---

[1] Россинская Е. Р., Галяшина Е. И. Настольная книга судьи: судебная экспертиза. М.: Проспект, 2011. С. 275.

Компьютерно-техническая экспертиза охватывает широкий спектр объектов, начиная с аппаратного обеспечения, такого как компьютеры, периферийные устройства (мышь, клавиатура, принтер), сетевое оборудование (роутеры, коммутаторы), встраиваемые системы (например, системы управления в автомобилях), комплектующие, носители информации (жесткие диски, флешки) и заканчивая программным обеспечением (операционные системы, приложения) и самой информацией, представленной в разнообразных форматах, включая текстовые документы, изображения, видео и базы данных.

Развитие КТЭ в России напрямую связано с потребностями правоохранительной системы и развивается параллельно с эволюцией информационных технологий и платформ. Предметом КТЭ являются фактические данные, которые устанавливаются путем анализа принципов работы компьютерных систем и информационных процессов. Эти данные используются в качестве доказательств в гражданских, уголовных и административных делах.

Классификация КТЭ основана на исследовании компонентов современных электронных устройств, таких как смартфоны, компьютеры и коммуникаторы. Выделяют четыре основных вида КТЭ:

1. Аппаратная (техническая) экспертиза – изучает физические компоненты компьютерных систем (определение причины выхода из строя жесткого диск);

2. Программная экспертиза – анализирует программное обеспечение (выявление вредоносного кода в программе);

3. Информационная (данные) экспертиза – исследует информацию, созданную пользователем (восстановление удаленных файлов);

4. Сетевая экспертиза – фокусируется на сетевых взаимодействиях и инфраструктуре (анализ сетевого трафика для определения источника атаки).

Подготовка к назначению КТЭ включает следующие этапы:

1. Сформулировать конкретные вопросы, на которые эксперт должен дать ответы;

2. Определить необходимые материалы – следует определить, какие материалы уголовного дела необходимы эксперту для проведения исследования, и обеспечить их копирование (протоколы осмотра места происшествия, изъятые цифровые устройства);

3. Правильно отобрать и упаковать объекты, которые будут исследоваться (компьютер, смартфон, флеш-накопитель);

4. Оформить постановление или определение о назначении экспертизы;

5. Определиться с экспертным учреждением.

Тщательная подготовка к назначению КТЭ существенно повышает ее эффективность и способствует успешному расследованию.

Проведение компьютерно-технической экспертизы регулируется общими процессуальными нормами, так как специализированного законодательства в этой области пока не разработано. Часто встречающейся ошибкой при назначении КТЭ является постановка перед экспертом вопросов правового характера, например, «Является ли установленное программное обеспечение контрафактным?». Такая формулировка недопустима, поскольку эксперт, обладающий специальными техническими знаниями, не компетентен давать юридические оценки. Решение о контрафактности ПО является прерогативой суда, основывающегося на совокупности доказательств, включая заключение эксперта. Подобные вопросы приводят к смешению компетенций суда и эксперта, что может стать основанием для оспаривания заключения экспертизы.

Так, при рассмотрении материалов уголовного дела, возбужденного по признакам преступлений, предусмотренных п. «а» ч. 3 ст. 272.1, ч. 2 ст. 159 УК РФ, в ходе которого было установлено, что неустановленное лицо, находясь в неустановленном месте, умышленно, из корыстных побуждений, с целью хищения чужого имущества, получил конфиденциальные данные, позволяющие осуществлять беспрепятственный доступ, совершил неправомерный доступ к охраняемой законом информации, содержащейся в личном аккаунте в мессенджере «Телеграмм», где продолжая свой единый

преступный умысел, направленный на тайное хищение чужого имущества, из корыстных побуждений, используя персональные данные и личный аккаунт гр. Р., от ее имени похитило денежные средства. В связи с изложенным, для установления обстоятельств, имеющих значение для уголовного дела, была назначена судебно-компьютерная экспертиза и поставлены перед экспертов следующие вопросы:

1. Какие файлы были скачаны на представленный на экспертизу сотовый телефон?

2. Какие действия совершались в системе в указанный период времени?

3. Имеются ли на представленном на экспертизу сотовом телефоне файлы, детектируемые вирусными приложениями?

4. Были ли использованы вредоносные программы, программы удаленного доступа?

5. Имеются ли на представленном на экспертизу сотовом телефоне сведения о переписке посредством приложения «Телеграмм»[1]?

Поляков В. В. и Шебалин А. В. отмечают, что следователи при составлении постановления о назначении КТЭ зачастую не указывают ее вид, ограничиваясь родовым названием, информация о виде экспертизы извлекается из анализа поставленных вопросов и предоставленных материалов. Хотя это и не является прямым нарушением процессуального законодательства, отсутствие в постановлении указания конкретного рода и вида экспертизы или их некорректное указание свидетельствует о недостаточном понимании следователем целей исследования. Следствием этого может быть некорректная формулировка вопросов эксперту, что, в свою очередь, приводит к необходимости проведения повторной КТЭ (нарушение принципов разумного срока судопроизводства и обеспечения доступа

[1] Уголовное дело № 1-653/2022 по обвинению Р. в совершении преступления, предусмотренного п. «а» ч. 3 ст. 272.1, ч. 2 ст. 159 УК РФ // Архив Стерлитамакского городского суда РБ.

к правосудию) или признанию заключения эксперта недопустимым доказательством (ст. 75 УПК РФ).

В постановлении следует указать возможность корректировки экспертом поставленных вопросов или добавления собственных (в соответствии с ч. 2 ст. 204 УПК РФ). Это обусловлено более глубоким знанием экспертом специфики исследуемого объекта и области компьютерно-технической экспертизы.

Россинская Е. Р. справедливо отмечает проблему роста числа негосударственных экспертных учреждений, не обладающих достаточной квалификацией в области судебных КТЭ, что приводит к многочисленным ошибкам.

При назначении компьютерно-технической экспертизы (КТЭ) следователь, дознаватель или суд обязаны тщательно подойти к выбору экспертного учреждения или конкретного эксперта.

Отсутствие четких квалификационных требований к компьютерно-техническим экспертам, в сочетании с пробелами в процедуре их выбора, создает серьезные риски. Неквалифицированный эксперт может не только предоставить ошибочные результаты, но и повредить или уничтожить аппаратные средства и данные, что приведет к утрате важных доказательств.

Например, эксперт с обширным опытом в области ремонта компьютерного оборудования может не обладать достаточными знаниями в области анализа вредоносного программного обеспечения или восстановления удаленных данных. В другом случае, эксперт, специализирующийся на сетевых технологиях, может не иметь достаточной компетенции для анализа данных, извлеченных с мобильных устройств.

Существующий пробел в законодательстве, касающийся квалификации компьютерно-технических экспертов, необходимо устранить. Диплом о техническом образовании и общий опыт работы в IT-сфере не являются достаточными гарантиями компетентности в специфических областях КТЭ, таких как анализ вредоносного ПО, восстановление данных, исследование

сетевых атак, анализ криптовалютных транзакций и т.д. Необходима разработка четких критериев оценки квалификации экспертов, специализирующихся на различных видах компьютерно-технических исследований, а также прозрачной процедуры их аттестации и аккредитации.

Развитие информационных технологий обусловливает необходимость тщательной проверки соответствия опыта и знаний эксперта конкретному роду и виду проводимой КТЭ.

Проведение КТЭ начинается с раздельного изучения объектов экспертизы, анализа их общих и частных признаков и свойств, решения диагностических и идентификационных задач. Некоторые вопросы требуют проведения экспертных экспериментов. Идентификационные задачи решаются путем сравнительного исследования для выявления совпадений или различий признаков объектов, а также сопоставления их с образцами или эталонами.

На заключительном этапе исследования формулируются выводы в виде ответов на поставленные вопросы. Выводы основываются на представленных эксперту или выявленных им данных об объекте исследования, а также на общих научных положениях электроники, радиотехники и программирования.

В результате анализа заключений компьютерно-технических экспертиз были выявлены следующие проблемы:

1. Некорректная формулировка вопросов из-за отсутствия предварительных консультаций следователи часто задают вопросы, выходящие за рамки компетенции экспертов или требующие длительного исследования, что увеличивает сроки проведения экспертиз;

2. Многообъектные исследования в рамках одного постановления. Направление нескольких объектов (системных блоков, жестких дисков, ноутбуков) на исследование в рамках одного постановления затрудняет восприятие результатов. Рекомендуется выносить отдельное постановление на каждый объект для более четкого и структурированного заключения;

3. Недостаточность или несоответствие предоставленных материалов: Следователи иногда предоставляют неполные или нерелевантные материалы, необходимые для проведения экспертизы;

4. Несвоевременное назначение экспертиз. Значительная задержка между вынесением постановления и поступлением материалов в экспертный центр негативно влияет на сроки расследования.

Для решения этих проблем и повышения эффективности расследования уголовных дел необходимо улучшить взаимодействие между следственными и экспертными подразделениями как на этапе назначения, так и в процессе проведения компьютерно-технических экспертиз.

ЗАКЛЮЧЕНИЕ

В заключение следует констатировать, что стремительное развитие информационных технологий, обусловившее повсеместное внедрение компьютерных систем и расширение доступа к сети Интернет, наряду с позитивным влиянием на различные сферы общественной жизни, привели к росту преступлений в сфере компьютерной информации. Трансграничный характер, высокая латентность и изощренность форм киберпреступности представляют собой серьезный вызов для правоохранительных органов, актуализируя необходимость совершенствования тактики производства следственных действий, направленных на эффективное расследование данной категории преступлений.

Преступления в сфере компьютерной информации представляют собой общественно опасные деяния, посягающие на безопасность компьютерной информации и систем, использующие компьютерные технологии в качестве инструмента, средства или предмета преступления. Ключевыми видами таких преступлений являются неправомерный доступ к информации, создание и распространение вредоносных программ, нарушение правил эксплуатации компьютерных систем и неправомерное воздействие на критическую информационную инфраструктуру. Отличительными чертами данной категории преступлений выступают высокая латентность, трансграничный характер, динамичное развитие способов совершения и потенциал причинения значительного ущерба.

Анализ криминалистической характеристики рассматриваемых преступлений позволяет выявить типовые способы их совершения и разработать адекватные меры противодействия. Центральным элементом криминалистической характеристики преступлений в сфере компьютерной информации является личность преступника. Современные киберпреступники, обладающие высокой квалификацией, активно применяют противодействие

правоохранительным органам, используя шифрование, программы удаленного доступа и другие методы, затрудняющие сбор доказательств и проведение розыскных мероприятий. Детальное изучение криминалистической характеристики способствует оптимизации процесса расследования и эффективному применению современных криминалистических методов и средств. Основная сложность расследования киберпреступлений обусловлена их технологической сложностью и спецификой порядка совершения. Дальнейшие научные исследования должны быть направлены на детальное выявление этапов и методов совершения киберпреступлений.

Специфика цифровых доказательств обуславливает особенности проведения осмотра места происшествия, обыска и выемки в сфере компьютерной информации. Успешное расследование рассматриваемых преступлений требует от правоохранительных органов не только знания процессуальных норм, но и понимания технических аспектов функционирования компьютерных систем и сетей. Комплексный подход, включающий привлечение квалифицированных специалистов и тщательное документирование всех этапов следственных действий, позволяет эффективно собирать и фиксировать цифровых следов преступной деятельности в сети Интернет, что является ключевым фактором успешного раскрытия и расследования преступлений в сфере высоких технологий. Грамотно проведенные осмотр, обыск и выемка обеспечивают сохранность и допустимость полученных доказательств, необходимых для привлечения виновных к уголовной ответственности.

Тактика допроса при расследовании киберпреступлений ориентирована на выяснение обстоятельств произошедшего, установление свидетелей и выявление подозреваемых. В ходе допроса подозреваемого устанавливается способ получения доступа к компьютерной системе, характер совершенных действий, а также факт индивидуального или группового характера преступления.

Подготовительный этап включает анализ материалов дела, определение целей допроса с применением классических следственных приемов,

изучение личности подозреваемого (обвиняемого), выбор и подготовку места проведения допроса, определение состава участников и техническое обеспечение с использованием современных информационных технологий. Планирование допроса, осуществляемое совместно со специалистом, предполагает оценку технической сложности преступления, формулирование вопросов и определение их последовательности, а также порядка предъявления имеющихся материалов. Специалист предоставляет следователю необходимую терминологию. Рабочий этап включает вступительную часть, стадию свободного рассказа и стадию постановки вопросов (открытых, дополняющих, уточняющих, детализирующих и др.). Важным аспектом является демонстрация внимательного и уважительного отношения к допрашиваемому. Завершающая стадия состоит из окончания беседы, оценки результатов и рефлексии, направленной на анализ собственных действий и решений в ходе допроса.

Для повышения эффективности расследования уголовных дел данной категории и решения выявленных проблем необходимо оптимизировать взаимодействие между следственными и экспертными подразделениями как на этапе назначения, так и в процессе проведения компьютерно-технических экспертиз. Это позволит повысить качество и достоверность экспертных заключений, что в конечном итоге будет способствовать более эффективному раскрытию и расследованию преступлений в сфере компьютерной информации.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020 г. // Официальный интернет– портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 23.04.2025).

2. Уголовно-процессуальный кодекс Российской Федерации: [Электронный ресурс]: федеральный закон от 18 декабря 2002 г. № 174-ФЗ. – URL: http://www.consultant.ru. (дата обращения: 10.11.2024). – Текст: электронный.

3. Уголовный кодекс Российской Федерации: [Электронный ресурс]: федеральный закон от 13 июня 1996 г. № 63-ФЗ. – URL: http://www.consultant.ru. (дата обращения: 05.12.2024). – Текст: электронный.

4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» – URL: http://www.consultant.ru. (дата обращения: 05.12.2025). – Текст: электронный.

5. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» – URL: http://www.consultant.ru. (дата обращения: 12.03.2025). – Текст: электронный.

II. Учебная, научная литература и иные материалы

1. Акопян Р. М. Проблемы тактики допроса подозреваемого (обвиняемого) // Восточно-Европейский научный журнал. 2022. № 7. С. 54-56.

2. Александров И. В. Криминалистика в 5 т. Том 5. Методика расследования преступлений: учебник для вузов. М.: Издательство Юрайт, 2025. 242 с.

3. Бастрыкина А. И. Криминалистика : учебник для вузов. М.: Издательство Юрайт, 2025. 643 с.

4. Белевитина Ю. В. Криминологический портрет личности киберпреступника в современной России // Инновационная наука. 2022. № 12. С. 61-64.

5. Вехов В. Б. Компьютерные преступления. Способы совершения, методики расследования. М.: Право и Закон, 1996. 182 с.

6. Гаврилин Ю. В. Научно-практический комментарий к ст. 272 УК РФ [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

7. Гладких А. В. Тактика ведения допроса: проблемные аспекты в криминалистике // Современные технологии в юриспруденции: применение специальных познаний. 2021. С. 27-29.

8. Горбунова К. А., Киселев А. С. Тактика производства следственных действий при расследовании преступлений в сфере компьютерной информации : монография. М.: Проспект, 2023. 88 с.

9. Григорян С. А. Особенности личности современного «киберпреступника» // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2024. № 8. С. 103-106.

10. Гуев А. Н. Комментарий к Уголовному кодексу Российской Федерации: для предпринимателей. М., 2000. 120 с.

11. Гульбин, Ю.А. Преступления в сфере компьютерной информации [Текст]: учебное пособие / Ю.А. Гульбин. М.: «Статут» 2007. 68 с.

12. Драпкин Л. Я. Криминалистика. Криминалистическая тактика: учебник для вузов / ответственный редактор Л. Я. Драпкин. – 2-е изд., перераб. и доп. М.: Издательство Юрайт, 2025. 230 с.

13. Жижина М. В., Завьялова Д. В. Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах: монография. М.: Проспект, 2023. 149 с.

14. Здравомыслов Б. В. Уголовное право Российской Федерации. Особенная часть: учебник / под ред. Б. В. Здравомыслова. 2-е изд. М., 2000. 552 с.

15. С. В. Зуев, В. Б. Вехов. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебник для вузов. М.: Издательство Юрайт, 2025. 243 с.

16. Ищенко Е. П. О технологии искусственного интеллекта в криминалистике // 30 лет юридической науки КубГАУ. 2021. С. 375-380.

17. Клебанов Л. Р., Полубинская С. В. Компьютерные технологии в совершении преступлений диверсионной и террористической направленности // Вестник Российского университета дружбы народов. 2020. № 3. С. 717-734.

18. Кочои С. М, Савельев Д. Б Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. 1999. № 1. С. 4-10.

19. Краткая характеристика состояния преступности в Российской Федерации // Официальный сайт МВД РФ. URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 28.04.2025).

20. Мартынова Н. В. Некоторые аспекты криминологической характеристики личности киберпреступника // Студенческий вестник. 2024. № 17. С. 7-10.

21. Могунова М. М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) // Вестник Саратовской государственной юридической академии. 2022. № 4. С. 135-141.

22. Морозова Т. В., Жуковский С. Ф., Зуева В. В. Психологические и рече-коммуникативные тактики ведения допроса в ходе предварительного следствия // Гуманитарная парадигма. 2024. № 4. С. 131-138.

23. Поляков В. В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. 2023. № 2. С. 114-116.

24. Попов А.Н. Преступления в сфере компьютерной информации: учебное пособие / СПб, 2018. 68 с.

25. Попова С. В., Агафонова М. С., Машин А. А. Угрозы экономической безопасности в концепции войн шестого поколения // Цифровая и отраслевая экономика. 2024. № 4. С. 55-63.

26. Протасевич А. А., Зверянская Л. П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2023. № 11. С. 45-47.

27. Рачева Н. В., Поскочинова К. А. Проблемные аспекты допроса подозреваемых при расследовании киберпреступлений // Технологии XXI века в юриспруденции. 2020. С. 520-529.

28. Степалин В. П. Глава 28. Преступления в сфере компьютерной информации// Научно-практическое пособие по применению УК РФ / Под ред. В. М. Лебедева. М., 2005. 140 с.

29. Сулейманов Р. Т., Атик Х. Б. Общая характеристика личности киберпреступника // Научный электронный журнал Меридиан. 2021. № 4. С. 114-116.

30. Файзуллина А. А. К вопросу о соотношении понятий «криминалистическая характеристика преступлений» и «следственная ситуация» // Инновационная наука. 2024. № 2. С. 140-142.

31. Филиппов А. Г. Криминалистическая методика: учебное пособие для вузов / А. Г. Филиппов [и др.]. М.: Юрайт, 2025. 402 с.

32. Хайруллова Э. Т. Применение психологических приемов в тактике допроса подозреваемых и обвиняемых // Криминалистика: вчера, сегодня, завтра. 2021. № 4. С. 138-144.

33. Хатунцев Н. А. О специальных знаниях, необходимых при исследовании компьютерных средств и систем // Актуальные проблемы российского права. 2024. № 1. С. 332-339.

34. Эксархопуло А. А. Криминалистика : учебник для вузов / А. А. Эксархопуло, И. А. Макаренко, Р. И. Зайнуллин. М.: Издательство Юрайт, 2025. 477 с.

III. Эмпирические материалы

1. Уголовное дело № 1-977/2023 по обвинению К. в совершении преступления, предусмотренного ч.2 ст.272 УК РФ // Архив Стерлитамакского городского суда РБ.

2. Уголовное дело № 1-971/2024 по обвинению гр. А. и гр. Б. в совершении преступления, предусмотренного ч.3 ст.272, ч.2 ст. 273 УК РФ // Архив Стерлитамакского городского суда РБ.

3. Уголовное дело № 1-859/2023 по обвинению Б. в совершении преступления, предусмотренного ч.1 ст.272 УК РФ // Архив Стерлитамакского городского суда РБ.

4. Уголовное дело № 1-653/2022 по обвинению Р. в совершении преступления, предусмотренного ч.2 ст.272 УК РФ // Архив Стерлитамакского городского суда РБ.

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и служебную тайну. _____ А.Н. Курбанова