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 «**ПОНЯТИЕ, ВИДЫ И ОСОБЕННОСТИ МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)**»

Выполнил
Микиев Егор Антонович
обучающийся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2020 года набора, 012 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

В настоящее время информация является неотъемлемым элементом функционирования критически важных государственных систем, включая связь, транспорт, энергетику, финансовый сектор, оборону и государственное управление. Данная ситуация обусловила проникновение преступной деятельности в сферу компьютерной информации. Усугубляют ситуацию возможности анонимизации личности и дистанционное совершение противоправных действий, что в совокупности обеспечивает рост преступности рассматриваемого вида.

Под преступлениями в сфере компьютерной информации понимаются общественно опасные деяния, совершаемые в информационно-технологической среде и направленные на информацию в электронно-цифровой форме. Глава 28 Уголовного кодекса Российской Федерации[1] (далее – УК РФ) является основной правовой базой для квалификации данных преступлений. Статистические данные МВД России за 2024 год указывают на значительную распространенность таких преступлений. Так, 40 % от общего числа преступлений были совершены с использованием информационно-телекоммуникационных технологий, при этом таких деяний зарегистрировано на 13,1 % больше, чем в 2023 году[2].

Актуальность исследования имеет как теоретический, так и практический характер, поскольку закрепленные в современном законодательстве нормы, регламентирующие преступления в сфере компьютерной информации, как объект, охраняемый государством, должны иметь осмысленный подход,

---

[1] Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

[2] Состояние преступности на территории Российской Федерации: официальный сайт МВД России. URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 20.01.2025).

исключающий возможность двоякого толкования и правоприменения предписаний законодательства в исследуемой области.

Цель выпускной квалификационной работы состоит в комплексном изучении современных методик расследования преступлений в сфере компьютерной информации, выявлении существующих проблем расследования данного вида преступных деяний, а также формировании предложений по решению обнаруженных проблем.

В соответствии с целью были поставлены следующие задачи:

раскрыть понятия «компьютерная информация», «преступления в сфере компьютерной информации»;

рассмотреть разновидности преступлений в сфере компьютерной информации и их особенности;

изучить обстоятельства, подлежащие установлению при расследовании преступлений в сфере компьютерной информации;

изучить типичные следственные ситуации, характерные для расследования преступлений в сфере компьютерной информации;

раскрыть особенности первоначального этапа расследования преступлений в сфере компьютерной информации;

исследовать особенности производства отдельных следственных действий;

проанализировать актуальные проблемы методики расследования преступлений в сфере компьютерной информации;

сформулировать предложения по актуализации методики расследования данного вида преступного деяния.

Научная новизна исследования определяется постановкой проблемы и подходом к ее исследованию. В ходе проведенной работы был разработан комплекс теоретических положений, направленных на установление оптимальной методики расследования преступлений в сфере компьютерной информации; сформулированы предложения по совершенствованию теории информационно-компьютерного обеспечения расследования преступлений.

Объектом выпускной квалификационной работы являются общественные отношения, возникающие в процессе расследования преступлений в сфере компьютерной информацией.

Предметом исследования выступает действующее законодательство, а также научные труды, раскрывающие особенности методики расследования преступлений в сфере компьютерной информации, в том числе на основании актуальных материалов судебной практики.

Методологической базой исследования является системный и комплексный подход к изучению проблем методики расследования преступлений в сфере компьютерной информации. В качестве методов исследования использованы анализ, синтез, классификация, обобщение, моделирование и сравнение.

Структура выпускной квалификационной работы обусловлена ее целью и задачами, что позволило включить в нее введение, три главы основной части, объединяющие в себе шесть параграфов, заключение, список использованной литературы и приложения.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Понятие и сущность преступлений в сфере компьютерной информации

Понятие «компьютерная информация» является ключевым для понимания и квалификации преступлений в сфере компьютерной информации. Однако, единого и общепринятого определения этого термина не существует. Различные подходы подчеркивают разнообразные аспекты этого понятия, что важно учитывать при изучении методики расследования преступлений, в частности, совершенных с использованием информационно-телекоммуникационных технологий.

Так, профессор Ю.В. Гаврилин под компьютерной информации понимает сведения, знания или набор команд (программ), предназначенные для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинном носителе, имеющие собственника, установившего правила их использования[1]. Автор не ограничивается только «данными» (сведениями), но также включает обработанную информацию (знания) и, что очень важно, исполняемые инструкции (набор команд (программа)). Это подчеркивает, что компьютерная информация – это не только пассивные данные, но и активные элементы, способные выполнять действия. Данное определение полезно тем, что оно не просто описывает техническую сущность информации, но и включает ее правовой статус и контекст использования, что важно при рассмотрении вопросов ее защиты и ответственности за посягательства на нее.

Авторское определение понятия «компьютерная информация» профессора В.А. Мещерякова предложено как «информация, представленная в специальном (машинном) виде, предназначенном и пригодном для ее автоматизированной

---

[1] Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации : дис. ... канд. юрид. наук. Москва, 2000. С. 32.

обработки, хранения и передачи, находящаяся на материальном носителе и имеющая собственника, установившего порядок ее создания (генерации), обработки, передачи и уничтожения»[1]. Автор подчеркивает, что компьютерная информация – это ценные (имеющие собственника) данные в цифровом формате, физически существующие на носителе и предназначенные для работы с ними с помощью компьютера, причем владелец этих данных имеет право определять правила обращения с ними. Это определение подчеркивает техническую специфику (машинный вид, пригодность для автоматизированных операций) и правовой статус (собственник и его право контроля), что делает его применимым для анализа правовых аспектов, связанных с компьютерной информацией.

Положением А.С. Егорышева выступает собственное видение особенностей указанного понятия. Так, по его мнению, компьютерная информация, как предмет неправомерного доступа, обладает «определенной ценностью и способностью удовлетворять человеческие потребности, то есть является интеллектуальной собственностью государства, юридического или физического лица (группы лиц), охраняется законом и находится на материальном носителе»[2]. В данном случае автор наделяет понятие такими функциями, которые позволяет понять, что компьютерная информация, являющаяся предметом преступления (неправомерного доступа), – это не просто цифровые данные, а ценная и полезная информация, имеющая конкретного собственника, чей правовой статус защищен законом, и физически расположенная на носителе.

Похожих взглядов с профессором Ю.В. Гаврилиным относительно определения придерживается Р.А. Белевский, который считает, что компьютерная информация – это сведения, знания или набор команд

---

[1] Мещеряков, В. А. Основы методики расследования преступлений в сфере компьютерной информации : дис. ... док. Юрид. наук. Воронеж, 2001. С. 45.

[2] Егорышев А. С. Расследование и предупреждение неправомерного доступа к компьютерной информации : дис. ... канд. юрид. наук. Уфа, 2004. С. 31.

(программ), предназначенных для использования и управления этой информацией в ЭВМ, находящаяся в ЭВМ или на машинном носителе и имеющая собственника, установившего правила ее использования[1].

Исходя из вышеперечисленных авторских определений понятия «компьютерной информации», следует, что не существует единого подхода, поскольку специфика определения зависит от наделения автором особенных признаков, поэтому данный вопрос на сегодняшний день остается дискуссионным.

Для определения сущности данного понятия необходимо проанализировать различные подходы с точки зрения фундаментальных особенностей, раскрывающие особенность компьютерной информации сквозь призму многогранности ее аспектов.

Выделяя подходы к понятию «компьютерная информация» целесообразно отметить ее значение в жизни общества и государства.

С точки зрения технического подхода под компьютерной информацией понимаются данные, представленные в цифровой форме и обрабатываемые, хранимые или передаваемые с помощью компьютерных систем и сетей.

Особое внимание уделяется форме представления и способу обработки информации. Примерами выступают биты, байты, файлы, базы данных, цифровые изображения, аудио- и видеозаписи, программный код. С технической точки зрения отмечается точность и четкость в представленном определении, ориентированность на технологическую природу явления, однако учитывается ограниченность технического аспекта, который не всегда берет во внимание смысловое содержание и ценность информации.

С точки зрения юридического подхода компьютерная информация определяется с позиции правовой значимости и ее охраны. Информация, охраняемая законом, может быть объектом преступных посягательств. Таким

---

[1] Белевский Р. А. Методика расследования преступлений, связанных с неправомерным доступом к компьютерной информации в сетях ЭВМ : дис. ... канд. юрид. наук. Санкт-Петербург, 2006. С. 29.

образом, прежде всего делается акцент на правовом статусе и ценности информации. Примерами такого рода являются: персональные данные; коммерческая тайна; государственная и банковская тайна; авторские права на программное обеспечение и контент; информация, составляющая основу электронных документов и прочее.

Положительным аспектом при этом является ориентированность на правовое регулирование и квалификацию преступлений, а отрицательным – размытость и зависимость от конкретного законодательства. Не всегда охватываются все виды цифровой информации, которые могут быть подвергнуты преступным действиям. Однако, часто рассуждению подлежит, что именно охраняет государство: информацию, представленную в цифровом виде, или право на данную информацию. В настоящее время это является дискуссионным вопросом, поскольку согласно уголовному законодательству объектом принято признавать предоставленное государством право, при этом в юридической литературе не упоминаются конкретно «преступления, посягающие на право в сфере компьютерной информации».

С точки зрения информационного подхода компьютерную информацию рассматривают как информационный ресурс или знание, представленное в цифровой форме и обладающее ценностью для пользователя или организации.

Часто представители данного подхода фокусируются на содержании, ценности и значимости информации. Для наглядности может привести примеры в виде деловой информации, научных данных, личной переписки, финансовых отчетов, стратегической информации. В качестве положительного момента можно выделить то, что учет смыслового содержания и практической ценности информации является важным для понимания мотивации киберпреступников. Отрицательным аспектом является то, что абстрактность определения может быть сложно формализована для юридических целей.

С точки зрения функционального подхода компьютерная информация представлена посредством ее функции и роли в компьютерных системах

и процессах. Информация, которая обеспечивает работу компьютерных систем, как правило, управляет ими или является результатом их работы.

В данном случае стоит уделить внимание функциональному назначению информации. Примерами здесь могут выступить операционные системы, прикладное программное обеспечение, настройки безопасности, логи доступа, данные для обработки транзакций и результаты вычислений. Функциональный подход помогает понять, какие виды информации критически важны для функционирования компьютерных систем и, следовательно, могут быть целями киберпреступности. Однако, одновременно следует учитывать, что бывает сложно отделить функциональную информацию от других видов информации, которые хранятся в компьютерных системах.

Так, В.А. Мещеряковым сделан вывод, что преступление в сфере компьютерной информации следует понимать, как «предусмотренное уголовным законом общественно опасное деяние (действие или бездействие), направленное против информации, представленной в особом (машинном) виде, принадлежащей государству, юридическому или физическому лицу, а также против установленного государством или ее собственником порядка создания (приобретения), использования и уничтожения, если оно причинило или представляло реальную угрозу причинения ущерба законному владельцу информации или автоматизированной системы, в которой эта информация генерируется (создается), обрабатывается, передается и уничтожается, или повлекло иные опасные последствия»[1].

Анализируя сущность определений, представленных различными авторами, необходимо сформулировать собственное его видение, учитывая не только юридическую суть, предусмотренную главой 28 УК РФ, но и специфику этого вида деяний в современном мире. Тем самым, преступления в сфере компьютерной информации следует понимать, как общественно опасные посягательства, совершаемые в цифровой среде с использованием

[1] Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : дис. ... док. юрид. наук. Воронеж, 2001. С. 59.

или в отношении средств вычислительной техники, информационных систем и телекоммуникационных сетей (включая критическую информационную инфраструктуру), и направленные на нарушение установленного порядка обращения с компьютерной информацией, ее конфиденциальности, целостности, доступности, а также на дезорганизацию нормального функционирования информационных систем и сетей, что влечет причинение вреда охраняемым законом интересам личности, общества и государства. Определив понятие и сущность преступлений в сфере компьютерной информации, перейдем к их классификации и рассмотрению конкретных видов.

§ 2. Виды преступлений в сфере компьютерной информации

Преступления, предусмотренные гл. 28 УК РФ «Преступления в сфере компьютерной информации» представлены шестью составами[1]:

неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

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);

создание, использование и распространение вредоносных программ (ст. 273 УК РФ);

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

неправомерное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1 УК РФ);

нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности

[1] Уголовный кодекс Российской Федерации. 13 июня 1996 г. № 63-ФЗ.

функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ).

Согласно официальным статистическим данным, опубликованным Главным информационно-аналитическим центром МВД России, в 2024 году зарегистрировано 105, 8 тыс. преступлений в сфере компьютерной информации[1]. Анализ статистических показателей позволяют сделать вывод, что наиболее распространенными составами за предыдущий год являлись неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

Иерархической структурой объекта преступления, принятой в российской уголовно-правовой доктрине, выделяется несколько уровней: общий, родовой, видовой и непосредственный.

Уголовно-правовое значение корректного выделения и определения родового объекта исследуемой группы преступлений заключается в его способности выявлять и обосновывать те особые, уникальные свойства и характеристики, которые присущи именно данной категории деяний и отличают их от всех других видов преступлений. Данные специфические свойства, связанные с особенностями цифровой среды, предметом посягательства (информация, компьютерные системы) и способом совершения, позволяют объединить эти разнородные составы преступлений в единую группу в рамках структуры Особенной части УК РФ.

Применительно к преступлениям, совершаемым в сфере компьютерной информации (в первую очередь, составам, предусмотренным гл. 28 УК РФ), видовым объектом, следует считать общественные отношения, обеспечивающие

[1] Состояние преступности на территории Российской Федерации: официальный сайт МВД России. URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 20.01.2025).

безопасность компьютерной информации[1]. Именно эти отношения являются тем типом социальных связей, которые страдают в первую очередь от рассматриваемой группы деяний и которые законодатель ставит под особую охрану, объединяя соответствующие нормы в отдельную главу УК РФ. Безопасность компьютерной информации в данном контексте понимается широко и включает такие ее свойства как конфиденциальность, целостность и доступность, а также надлежащее функционирование компьютерных систем и сетей, где эта информация обрабатывается и циркулирует.

Переходя на еще более конкретный уровень, отмечается, что непосредственным объектом выступают конкретные общественные отношения, которым причиняется вред или создается непосредственная угроза его причинения в результате совершения конкретного преступного деяния, предусмотренного отдельной статьей или частью статьи УК РФ (то есть конкретным составом преступления).

Установление дополнительных объектов преступлений в сфере компьютерной информации позволяет выделить отдельные их формы и виды (например, в качестве дополнительного объекта могут выступать: конституционный строй и безопасность государства, личные имущественные и интеллектуальные права и интересы, конституционные права и свободы человека и гражданина)[2]. Отметим, что наличие дополнительного объекта, как правило, повышает общественную опасность преступления в сфере компьютерной информации и является более значимым, ценным, чем основной объект.

---

[1] Ульянов М. В. Преступления в сфере компьютерной информации: возможности уголовно-правового воздействия и предупреждения // правопорядок: история, теория, практика. 2022. №4 (35). URL: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-kompyuternoy-informatsii-vozmozhnosti-ugolovno-pravovogo-vozdeystviya-i-preduprezhdeniya (дата обращения: 20.01.2025).

[2] Банюкова Д. В. Правовое регулирование преступлений в сфере информационных технологий // E-Scio. 2022. № 7 (70). URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-prestupleniy-v-sfere-informatsionnyh-tehnologiy (дата обращения: 12.05.2025).

Компьютерная информация является тем конкретным элементом цифровой среды, манипулируя которым (путем воздействия на ее свойства – конфиденциальность, целостность, доступность) виновный причиняет вред видовому объекту (общественным отношениям, обеспечивающим безопасность компьютерной информации) или непосредственному объекту (конкретным общественным отношениям в сфере безопасности компьютерной информации, нарушаемым данным конкретным деянием, например, отношениям по поводу конфиденциальности конкретных данных)[1].

Преступления в сфере компьютерной информации имеют специфический характер в реализации правоприменительной практики, поскольку требуют достаточного количества времени и усилий, чтобы установить конкретный состав преступления, предусмотренный гл. 28 УК РФ. Составы преступления указанной главы обладают следующими уголовно-правовыми особенностями:

1. Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». Данная статья устанавливает уголовную ответственность за посягательство на безопасность компьютерной информации, то есть на ее защищенность от несанкционированного доступа, уничтожения, блокирования, модификации и копирования. Сущность этого преступления заключается в несанкционированном проникновении в информационные системы с целью воздействия на охраняемую законом информацию или сами системы.

Непосредственным объектом выступают общественные отношения, обеспечивающие безопасность охраняемой законом компьютерной информации. В данном случае безопасность информации подразумевает ее защищенность, в первую очередь, от неправомерного доступа и последующего воздействия (уничтожения, блокирования, модификации, копирования). Следует учитывать,

---

[1] Петрова И. А., Лобачев И. А. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств // Журнал прикладных исследований. 2020. № 1. URL: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-kompyuternoy-tsifrovoy-informatsii-diskussionnye-voprosy-opredeleniya-ponyatiya-obekta-ugolovno-pravovoy-ohrany (дата обращения: 20.01.2025).

что компьютерная информация – это сведения, представленные в форме, пригодной для обработки ЭВМ. Ключевым аспектом выступает, что информация должна быть охраняемой законом, то есть для которой законом установлен специальный режим ее правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные. Неправомерный доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты[1].

В ходе изучения судебной практики был проанализирован приговор Сызранского городского суда Самарской области, в соответствии с которым гражданина А. признали виновным в совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ[2]. Судом было установлено, что гражданин А. имел доступ к информационно-биллинговой системе «SBMS», являются средством хранения, обработки и передачи компьютерной информации в информационно-телекоммуникационных сетях группы компаний «Z». Он, используя функциональные возможности указанного программного обеспечения, к которому у него имелся доступ в силу служебной необходимости, как у сотрудника компании, выходя за рамки своих служебных обязанностей, в нарушение Конституции Российской Федерации, Федерального закона от 07.07.2003 № 126-ФЗ «О связи»[3], Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) URL: https://www.consultant.ru/document/cons_doc_law_161817/ (дата обращения: 10.04.2025).

[2] Приговор Сызранского городского суда Самарской области № 1-370/2024 от 25 июля 2024 г. URL: https: //sudact.ru/regular/doc/IAumzEIDDmlX/ (дата обращения: 10.04.2025).

[3] О связи: федер. закон Рос. Федерации от 7 июля 2003 № 126-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 18 июн. 2003 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 25 июн. 2003 г. // Собр. законодательства Рос. Федерации. 2003. № 28, ст. 2895.

информации»[1], требований должностной инструкции, и локальных нормативных актов осуществил неправомерный доступ к охраняемой законом компьютерной информации – к лицевому счету абонента В., после чего внес заведомо ложные сведения о владельце абонентского номера без его согласия и без предъявления последним паспорта гражданина РФ, что повлекло за собой неправомерную модификацию компьютерной информации, хранящейся на сервере.

При изучении материалов уголовных дел установлено, что одним из распространенных составов преступлений в сфере компьютерной информации является неправомерный доступ к компьютерной информации, представляющий собой следующие обстоятельства уголовного дела: неустановленное лицо путем осуществления входа в сеть «Интернет» посредством соединения с сервером провайдера, незаконно воспользовавшись аккаунтом на портале «Госуслуги» и паролем, принадлежащим гр. К., получило неправомерный доступ к охраняемом законом компьютерной информации (Приложение 1).

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). Предписывающая законом норма устанавливает уголовную ответственность за посягательство на безопасность и конфиденциальность компьютерной информации, содержащей персональные данные, в части ее незаконного оборота и создания условий для него. Сущность этого преступления заключается в противоправных действиях с особо чувствительной информацией (персональными данными), полученной криминальным путем, или в создании инструментов для такого оборота.

---

[1] Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 № 149-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июл. 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июл. 2006 г. // Собр. законодательства Рос. Федерации. – 2006. – № 31, ст. 3448.

По данному составу преступления непосредственным объектом выступают общественные отношения, обеспечивающие безопасность, неприкосновенность частной жизни и конфиденциальность компьютерной информации, содержащей персональные данные. Указанный объект тесно связан с конституционным правом граждан на неприкосновенность частной жизни, личную и семейную тайну (ст. ст. 23, 24 Конституции РФ) и регулируется, в частности, Федеральным законом «О персональных данных»[1]. Следовательно, ключевым элементом является информация, содержащая персональные данные (любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу) и представленная в компьютерном виде.

3. Создание, использование и распространение вредоносных программ (ст. 273 УК РФ). Данная правовая норма защищает прежде всего целостность, доступность и конфиденциальность компьютерной информации и защищенную работу информационных систем и сетей. В соответствии с уголовным законодательством здесь непосредственным объектом являются общественные отношения, обеспечивающие информационную безопасность, а именно нормальное функционирование и безопасность компьютерной информации, средств ее хранения, обработки или передачи, а также информационно-телекоммуникационных сетей. Объективная сторона выражается в совершении одного или нескольких из перечисленных в диспозиции статьи действий.

Создание компьютерных программ подразумевает под собой разработку, написание, модификацию компьютерных программ или иной компьютерной информации, «заведомо предназначенных» для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Сюда можно отнести написание самого кода, компиляция, тестирование и пр.

---

[1] О персональных данных от 27 июля 2006 г. № 152-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июл. 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июл. 2006 г. // Собр. законодательства Рос. Федерации. – 2022. – № 29, ст. 5233.

Использование компьютерных программ другими словами можно назвать применение таких вредоносных программ или информации по их прямому назначению, то есть для осуществления тех самых вредоносных действий, для которых они были созданы. Распространение программ – предоставление доступа к таким вредоносным программам или информации третьим лицам любым способом (продажа, дарение, обмен, размещение в открытом доступе в сети «Интернет», передача по электронной почте).

Преступление является формальным по своей конструкции в ч. 1 ст. 273 УК РФ. Это означает, что оно считается оконченным с момента совершения любого из указанных действий (создания, использования или распространения) программы или информации, «заведомо предназначенной» для вредоносных целей, независимо от того, наступили ли фактически вредные последствия (уничтожение, блокирование) или нет. Достаточно самого факта создания, использования или распространения такой программы с соответствующим назначением.

Так, приговором Центрального районного суда г. Сочи Краснодарского края гражданин К. признан виновным в совершении преступления, предусмотренного ч. 2 ст. 273 УК РФ[1].

Гражданин К., обладающий доступом в сеть «Интернет», в приложении мессенджера «Телеграмм», установленном на его технических устройствах, под псевдонимом, который привязан к абонентскому номеру, арендовал за 100 долларов США в месяц у не установленного органом предварительного следствия лица, использующего сетевой псевдоним «Макс», программное обеспечение – стилер, предназначенное для несанкционированного копирования компьютерной информации, которое сохранил в памяти указанных выше устройств, после чего получил учетную запись (логин и пароль) на сайте, доступ к панели администрирования и инструкции по настройке сервера, который будет

---

[1] Приговор Центрального районного суда г. Сочи Краснодарского края № 1-482/2024 от 11 июля 2024 г. URL: https://sudact.ru/regular/doc/lR1ThzGEqYVT (дата обращения: 10.04.2025).

осуществлять соединение компьютеров, в которые гражданин К. внедрял вредоносные программы и перенаправлял их в панель администрирования учетной записи. С помощью панели администрирования указанного вредоносного программного обеспечения гражданин К. создавал файлы с вредоносным кодом, предназначенные для установки на целевые компьютеры с целью несанкционированного извлечения из локальных защищенных хранилищ Интернет-браузеров и иных программ компьютерной информации, представляющей собой идентификаторы (логины) и аутентификаторы (пароли) от используемых пользователями компьютеров учетных записей, а также истории посещенных Интернет-ресурсов и файлов, содержащих электронные криптокошельки.

4. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). Государство по ст. 274 УК РФ защищает надежность и безопасность работы информационных систем, которые могут быть нарушены из-за несоблюдения установленных правил их использования и обслуживания. Нарушение правил эксплуатации заключаются в том, что эти правила могут быть установлены законодательством, нормативными актами, стандартами, ведомственными инструкциями, должностными обязанностями, технической документацией. Нарушение может заключаться как в активных действиях (например, отключение системы защиты без разрешения), так и в бездействии (например, непроведение обязательных работ по обслуживанию, игнорирование сигналов об ошибках).

Так, приговором Хасавюртовского городского суда Республики Дагестан гражданин А. признан виновным в совершении преступления, предусмотренного ч. 4 ст. 160 и ч. 1 ст. 274 УК РФ[1].

---

[1] Приговор Хасавюртовского городского суда Республики Дагестан 1-94/2024 от 27 февраля 2024 г. URL: https://sudact.ru/regular/doc/veqsKVcHL461/ (дата обращения: 10.04.2025).

В части, касающейся нарушения правил эксплуатации, суд установил, что согласно должностной инструкцией начальника отделения почтовой связи на гражданина О. возлагались обязанности: осуществлять ежедневный учет и контроля движения денежных средств, осуществлять перерасчет денежной наличности в конце рабочего дня и сверку фактического остатка наличных денежных средств в кассе с расчетным остатком и прочее. Гражданин О. нарушил правила эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации, повлекшее модификацию информации, выразившееся при заполнении отчета в электронном виде о движении денежных средств и сумм реализации услуг, материальных ценностей, товаров. Гражданин отразил денежные средства, тогда как фактически в указанные дни, обозначенные суммы денежных средств наличными в главную кассу не сдавались.

5. Неправомерное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1 УК РФ). Данная правовая норма устанавливает уголовную ответственность за различные виды незаконных действий, направленных против жизненно важных для функционирования государства и общества информационных систем. Главный объект защиты – критическая информационная инфраструктура РФ, то есть объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов (п. 6 ст. 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1]). Статья криминализирует такие виды неправомерного воздействия, как создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия

[1] О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 12 июл. 2017 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 19 июл. 2017 г. // Собр. законодательства Рос. Федерации. – 2017. – № 31, ст. 4736.

на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации. Сущность данного состава преступления заключается в установлении уголовно-правового запрета на любые формы несанкционированного и вредоносного воздействия на информационную инфраструктуру, имеющую критическое значение для безопасности и нормального функционирования рассматриваемых объектов в Российской Федерации, связывая ответственность с видом действия и тяжестью наступивших или угрожающих последствий.

Так, приговором Ленинградского районного суда Краснодарского края гражданка А. признана виновной в совершении преступления, предусмотренного ч. 4 ст. 274.1 УК РФ[1]. Гражданка А. имела право оформления рецептов на льготные лекарственные препараты в информационной системе «Процессинговый центр льготного лекарственного обеспечения», относящейся к критической информационной инфраструктуре Российской Федерации. Гражданка А., вступив в преступный сговор с медицинской сестрой, направленный на совместное совершение преступления, связанного с нарушением правил эксплуатации и нарушением правил доступа к информационной системе, с целью придания видимых положительных результатов своей трудовой деятельности, выраженных в создании мнимой обеспеченности населения льготными лекарственными препаратами, оформила рецептурные бланков на льготные сахароснижающие препараты на имена лиц, которые в данном препарате не нуждаются не страдают заболеванием «Сахарный диабет», внесла заведомо ложные статусы «Обеспечен» льготным сахароснижающим препаратом у пациентов, которые фактически данный препарат не получали, тем самым привела к искажению сведений, содержащихся

[1] Приговор Ленинградского районного суда Краснодарского края № 1-20/2024 от 12 февраля 2024 г. URL: https://sudact.ru/regular/doc/AqzmSF1yIjWH/ (дата обращения: 10.04.2025).

в системе «ПЦ ЛЛО», относящейся к критической информационной инфраструктуре 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). Исходя из текста правовой нормы, объект преступления, предусмотренный ст. 274.2 УК РФ, охвачен понятиями «цифровая экономика» и «информационное общество». В условиях повсеместной цифровизации не правомерное использование глобальной сети «Интернет» и других сетей общего пользования представляется достаточно значимыми. Подразумевается, что уголовно-правовые нормы, закрепленные в данной статье, направлены на охрану суверенного киберпространства от информационных посягательств путем установления уголовной ответственности для тех лиц, которые должны обеспечивать устойчивость, безопасность и целостность российского киберпространства.

Таким образом, глава 28 УК РФ является жизненно важным инструментом правового регулирования и борьбы с преступностью в цифровом мире. Она охватывает широкий спектр деяний, направленных против компьютерной информации и информационных систем, и призвана обеспечить информационную безопасность общества и государства. Однако ее эффективное применение требует не только совершенствования самого законодательства в соответствии с технологическим прогрессом, но и значительных усилий по развитию компетенций правоохранительных органов, укреплению межведомственного и международного взаимодействия, а также повышению общей грамотности населения в сфере компьютерной информации. Только комплексный подход позволит успешно противостоять растущим угрозам в сфере компьютерной информации.

ГЛАВА 2. ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК УГОЛОВНО НАКАЗУЕМОЕ ДЕЯНИЕ

§ 1. Криминалистические особенности преступлений в сфере компьютерной информации

Преступления, предусмотренные главой 28 УК РФ («Преступления в сфере компьютерной информации»), обладают рядом существенных криминалистических особенностей, отличающих их от традиционных видов уголовно наказуемых деяний. Данные особенности обусловлены прежде всего нематериальной природой предмета посягательства (электронная информация, программное обеспечение) и спецификой среды совершения деяния – виртуальным пространством и информационно-телекоммуникационными системами. Главным источником доказательств при расследовании таких преступлений являются электронные следы, оставляемые в цифровой среде (метаданные, информация на носителях, сетевой трафик и пр.), что порождает специфические трудности, связанные с их обнаружением, фиксацией, изъятием и исследованием, учитывая их изменчивость, потенциальную анонимность и трансграничный характер. Криминалистическое изучение данных видов преступлений сосредоточено на выявлении и анализе особенностей способа их совершения (использование специальных программ, методов обхода защиты), механизма следообразования в цифровой среде, типологии личности преступника (часто обладающего специальными познаниями в области информационных технологий), а также специфики обстановки преступления, которая может включать как виртуальные, так и реальные компоненты. Понимание и глубокое исследование этих криминалистических особенностей является ключевым условием для разработки эффективных методик расследования и раскрытия преступлений в сфере компьютерной информации, а также для совершенствования нормативно-правовой базы и технического оснащения правоохранительных органов.

Криминалистическая характеристика компьютерных преступлений в качестве основных элементов включает способ совершения преступлений, обстановку совершения преступления и личность преступника.

Совершение компьютерных преступлений обычно проходит в три стадии: подготовка, непосредственное исполнение и сокрытие следов[1]. Хотя конкретные преступные действия весьма разнообразны, по способу взаимодействия злоумышленника с компьютером потерпевшего (где хранилась информация) методы совершения преступлений можно разделить на прямой и удаленный (опосредованный) доступ[2].

Термин «доступ» в контексте главы 28 УК РФ используется для описания действий, являющихся инструментом совершения всех предусмотренных преступлений. Данные действия могут быть реализованы двумя основными способами: путем непосредственного (прямого) или удаленного доступа[3]. Непосредственный доступ подразумевает физическое присутствие преступника на месте расположения компьютерной информации и техники и прямой физический контакт с оборудованием (например, посредством физической консол).

В случае удаленного доступа злоумышленник действует дистанционно, используя соответствующие технические и программные средства, находясь вне места нахождения объекта. Стоит отметить, что даже подготовка к удаленному доступу порой требует физического посещения целевого места. Расследование преступлений, совершаемых с использованием удаленного доступа, является наиболее трудной задачей. Практическая значимость предложенной классификации заключается в том, что каждый из указанных способов оставляет присущие только ему следы преступного воздействия.

---

[1] Зуев С. В. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебник для вузов. М. : Юрайт, 2025. С. 119.

[2] Александрова И. В. Криминалистика в 5 т. Том 5. Методика расследования преступлений : учебник для вузов. М. : Юрайт, 2025. 209 с.

[3] Багдасарян А. В. Способы совершения компьютерных преступлений // Инновационная наука. 2022. №12-2. URL: https://cyberleninka.ru/article/n/sposoby-sovershеniya-kompyuternyh-prestupleniy-1 (дата обращения: 20.01.2025).

В качестве типовых способов подготовки совершения преступления можно выделить[1]:

использование метода «социальной инженерии» в виде непосредственного контакта с потерпевшим (гражданином, сотрудниками организаций);

поиск информации в социальных сетях, посещение чатов и форумов, преступник может специально создавать виртуальную личность(в целях установления контакта);

использование поисковых систем;

поиск в базах данных «Whois» («кто есть кто»);

опрос DNS серверов (от англ. «DNS» – доменная система имен);

сканирование оборудования, подключенного к сети, с целью определения схемы атакуемой системы (уязвимые хосты, маршрутизаторы и брандмауэры);

сканирование открытых портов (получение информации о потенциальных входах в систему);

снифинг (прослушивание) (сбор в сети с помощью специальных программных инструментов информации (имена и пароли пользователей, файлы, электронная почта)).

На стадии подготовки преступлений могут планироваться меры по сокрытию преступления. Как правило, это характерно для профессиональных преступников, организованных групп и одиночных преступников, имеющих специальную подготовку в области информационных технологий. В ходе совершения преступления путем непосредственного доступа преступник осуществляет проникновение к компьютеру или иному месту, где находится интересующая

его информация; преодолевает охранные системы; подключает к компьютеру

[1] Савченко М. Ю. Способы совершения преступлений в сфере компьютерной информации и меры по их профилактике // Вестник КРУ МВД России. 2024. № 2 (64). URL: https://cyberleninka.ru/article/n/sposoby-soversheniya-prestupleniy-v-sfere-kompyuternoy-informatsii-i-mery-po-ih-profilaktike (дата обращения: 20.01.2025).

дополнительные устройства (съемные электронные носители информации), позволяющие получить доступ к информации; похищает электронные носители информации; обманным путем получает у потерпевшего или его сотрудников данные, обеспечивающие доступ к электронной информации и техники; иным образом противоправно получает информацию; передает потерпевшему носитель с вредоносной программой или самостоятельно вводит ее в память ЭВМ; получает доступ к компьютеру под видом правомерного пользователя или осуществляет его взлом; устанавливает в соответствующем помещении устройства, позволяющие считывать информацию с компьютера, наблюдать за действиями правомерных пользователей, осуществлять иные функции.

Удаленный доступ наиболее часто осуществляется следующими способами[1]:

подключение к телекоммуникационному оборудованию компьютерной системы (принтер, телефонную линию, модем);

проникновение в систему в результате использования системной поломки;

DDoS-атаки (от англ. «Distributed denial of services» – распределенный отказ в обслуживании);

проникновение путем подбора или «взлома» пароля;

электромагнитный перехват (получение информации без непосредственного подключения к компьютерной системе (электромагнитное излучение перехватывается из сетевого кабеля или host-ЭВМ внешним устройством));

аудиоперехват (установка в компьютерной технике специальных средств (подслушивающих устройств) для перехвата информации);

[1] Тарчоков Б. А., Хитиева А. Ж. Преступления в сфере компьютерной информации: виды и способы совершения // Журнал прикладных исследований. 2021. № 6. URL: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-kompyuternoy-informatsii-vidy-i-sposoby-soversheniya (дата обращения: 12.05.2025).

внедрение вредоносных программ (вирусов, «логических» и «временных» бомб и других), блокирующих, модифицирующих или уничтожающих информацию;

использование вредоносных программ, позволяющих обойти принятые меры защиты и технические условия обработки информации («троянский конь», программные закладки);

распространение вредоносных программ (передача на съемных электронных носителях, рассылка по электронной почте, размещение на сайтах в сети «Интернет»).

Преступники могут использовать сочетание нескольких способов. В частности, войдя в доверие к потерпевшему, преступник может получить сведения, позволяющие облегчить подбор паролей.

На основании анализа приговоров районных судов различных регионов государства можно выделить наиболее распространенные способы совершения преступлений, предусмотренных гл. 28 УК. Так, за 2024 год вынесены приговоры по следующим действиям граждан:

получение неправомерного доступа к охраняемой законом компьютерной информации, содержащейся в личном кабинете на портале «Госуслуги» (с целью дальнейшего оформления займов в кредитных организациях)[1];

неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в профиле гражданина на портале «Госуслуги», повлекший её копирование из корыстной заинтересованности (последующее использование персональных данных для хищения обманным путем денежных средств в микрокредитных организациях)[2];

неправомерный доступ к охраняемой законом компьютерной информации, повлекший копирование компьютерной информации, принадлежащей

---

[1] Приговор Индустриального районного суда г. Барнаула Алтайского края № 1-670/2024 от 2 октября 2024 г. URL: https://sudact.ru/regular/doc/iS1uyIxQRj51/ (дата обращения: 10.04.2025).

[2] Приговор Нововятского районного суда г. Кирова № 1-169/2024 от 24 сентября 2024 г. URL: https://sudact.ru/regular/doc/AgxtDyNNi8d3/ (дата обращения: 10.04.2025).

МВД России (по устному запросу старшего следователя о предоставлении сведений из системы ИБД-Р)[1];

неправомерный доступ в компьютерную программу, например, в «1С», используемую для регистрации договора клиента (без заявления клиента обращение к личной карточке абонента, копирование персональных данных последнего, внесение ранее скопированных персональных данных в новый договор на предоставление услуг связи, тем самым модифицирование информационно-биллинговую систему)[2];

неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в информационной системе «Amdocs Ensemble», принадлежащей ПАО «Вымпел-Коммуникации», где произвел модификацию (изменение) охраняемой законом компьютерной информации путем оформления абонентского номера на анкетные и паспортные данные ранее незнакомого[3];

с помощью операционной компьютерной программы, предназначенной непосредственно для сканирования заданного диапазона IP-адресов средств вычислительной техники, периодическое сканирование информационно–телекоммуникационной сети «Интернет» и получение списков IP-адресов серверов, располагающихся в сети с открытыми портами[4];

создание канала на интернет-ресурсе «Ютуб» с публикованием видео-обзоров компьютерных игр, одновременно создание сайта, на котором

---

[1] Приговор Неклиновского районного суда Ростовской области № 1-235/2024 от 17 сентября 2024 г. URL: https://sudact.ru/regular/doc/cr0FfHdCtaHj/ (дата обращения: 10.04.2025).

[2] Приговор Троицкого городского суда Челябинской области № 1-402/2024 от 11 сентября 2024 г. URL: https://sudact.ru/regular/doc/kW3bRTuiIMNE/ (дата обращения: 10.04.2025).

[3] Приговор Центрального районного суда № 1-781/2024 от 3 октября 2024 г. URL: https://sudact.ru/regular/doc/el2bC1Ssrnbq/ (дата обращения: 10.04.2025).

[4] Приговор Курганского городского суда Курганской области № 1-1197/2024 от 1 сентября 2024 г. URL: https://sudact.ru/regular/doc/iO8awTPoNbN0/ (дата обращения: 10.04.2025).

размещается доступ для скачивания «вируса», замаскированного под компьютерную игру[1];

размещение на интернет-ресурсе объявления с использованием сотового телефона в сети «Интернет» о продаже вредоносной программы «Стиллер» под другим названием[2];

выдача фиктивного «Сертификата о вакцинации COVID-19» без фактического введения вакцины гражданам с внесением недостоверных сведений в единую государственную информационную систему в сфере здравоохранения[3].

Вторым по значимости элементом криминалистической характеристики компьютерных преступлений выступает обстановка их совершения, что обусловлено тем, что именно в ней формируется следовая картина преступного события. Ключевое влияние на условия совершения преступлений в этой обстановке оказывают такие факторы, как пространственные, временные, производственно-бытовые, поведенческо-психологические и информационные.[4].

Пространственные характеристики обстановки компьютерных преступлений отличаются территориальной разобщенностью. Данная особенность проявляется в том, что различные элементы преступления могут находиться в разных местах, например: место причинения вреда, место нахождения преступника, место расположения промежуточного компьютера, место хранения криминалистически значимой информации и место нахождения компьютеров с доступом в глобальные и локальные сети.

Временный фактор, играет особую, часто критическую роль в преступлениях, совершаемых в сфере компьютерной информации, значительно отличаясь от их проявления в традиционных видах преступлений. Многие

---

[1] Приговор Даниловского районного суда Ярославской области № 1-44/2024 от 13 июня 2024 г. URL: https://sudact.ru/regular/doc/XYf4UTzmlToW/ (дата обращения: 10.04.2025).

[2] Приговор Райчихинского городского суда Амурской области № 1-104/2024 от 7 мая 2024 г. URL: https://sudact.ru/regular/doc/pVmvLxn8r01/ (дата обращения: 10.04.2025).

[3] Приговор Заднепровского районного суда г. Смоленска № 1-199/2024 от 18 июня 2024 г. URL: https://sudact.ru/regular/doc/icBznkeWeDLq/ (дата обращения: 10.04.2025).

[4] Марьясис И. В. Криминалистические характеристики компьютерных преступлений / Инновационная наука. 2021. № 12-2. URL: https://cyberleninka.ru/article/n/kriminalisticheskie-harakteristiki-kompyuternyh-prestupleniy (дата обращения: 20.01.2025).

компьютерные преступления (например, DDoS-атаки, несанкционированный доступ, заражение вирусом) могут происходить практически мгновенно или за очень короткий промежуток времени (секунды, минуты), что резко контрастирует с длительностью совершения большинства физических преступлений. Цифровые следы, являющиеся основными доказательствами, крайне недолговечны и могут быть легко изменены, удалены или перезаписаны (например, данные в оперативной памяти, временные файлы, сетевой трафик). Время реакции на обнаружение преступления и начала расследования становится критически важным для сохранения этих доказательств.

Особенности поведенческо-психологических факторов обусловлены цифровой средой совершения преступлений и характером взаимодействия преступника, жертвы и объекта посягательства. Так, преступник не видит жертву лицом к лицу, что значительно снижает уровень эмпатии, устраняет страх немедленной физической реакции жертвы или свидетелей. Так же возможность скрыть свою личность (или использовать псевдоним) в сети уменьшает страх быть пойманным и понести наказание, а также избежать социального порицания, что способствует более рискованному и менее социально одобряемому поведению. Многие компьютерные преступления (фишинг, мошенничество, вымогательство) строятся на прямом психологическом воздействии на жертву – использовании ее доверчивости, страха, жадности, любопытства, чувства срочности. Цифровая среда может создавать иллюзию неуловимости, что психологически облегчает принятие решения о совершении преступления.

Особенности цифровых факторов обусловлены тем, что информация (данные, программы) является либо непосредственным объектом посягательства, либо средством совершения преступления (вредоносный код). Следует отметить, что информация нематериальна, легко копируется, передается на любые расстояния и может быть уничтожена или изменена без физического воздействия. Немаловажным условием является, что преступления оставляют специфические цифровые следы, которые являются основным источником доказательств, но могут быть легко подделаны или уничтожены.

Таким образом, анализ теоретических и практических особенностей позволяет выявить ключевые криминалистические особенности преступлений в сфере компьютерной информации. Уникальная природа информации как объекта и средства посягательства, ее нематериальность, легкая тиражируемость и взаимосвязанность информационных систем определяют специфику механизма совершения таких преступлений и, как следствие, особенности формирования цифровой следовой картины. Понимание этих особенностей критически важно для эффективного выявления, расследования и раскрытия данных видов преступлений, поскольку традиционные криминалистические подходы требуют существенной адаптации и дополнения специализированными методами работы с электронными доказательствами и цифровыми следами.

§ 2. Особенности производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации

При расследовании преступлений в сфере компьютерной информации традиционные следственные действия приобретают ряд специфических особенностей, обусловленных природой цифровых доказательств, их изменчивостью, зависимостью от специализированных знаний и технологий.

Производство следственных действий является фундаментальным этапом досудебного расследования, направленным на собирание, проверку и оценку доказательств, необходимых для установления обстоятельств, подлежащих доказыванию по уголовному делу. Несмотря на закрепление в УПК РФ общих принципов и правил их проведения, каждое из них обладает специфическим набором особенностей, обусловленных его процессуальной природой, целевым назначением, объектом воздействия, спецификой тактических приемов и строгими требованиями уголовно-процессуального законодательства. Игнорирование или недостаточное понимание этих особенностей при практическом применении может повлечь за собой не только снижение эффективности расследования, но и нарушение прав участников процесса,

процессуальные ошибки, снижение доказательственной ценности полученной информации или даже признание ее недопустимой в соответствии со ст. 75 УПК РФ. Таким образом, детальное изучение и учет особенностей производства отдельного следственного действия не просто желательно, но и является необходимым условием для обеспечения законности, обоснованности и эффективности всего процесса расследования, а также для формирования качественной доказательственной базы по уголовному делу. Понимание этих нюансов позволяет следователю или дознавателю правильно избрать тактику проведения действия, обеспечить соблюдение прав и законных интересов граждан, а также минимизировать риски утраты или искажения важной для дела информации.

Данные преступления обладают рядом специфических черт, которые влияют на тактику и методику следственных действий. Общие особенности, влияющие на следственные действия[1]:

дистанционность и трансграничность (т.е. преступления могут совершаться из любой точки мира, а серверы и данные могут находиться в разных юрисдикциях, что усложняет установление места совершения преступления и сбор доказательст)в;

виртуальная среда обуславливает, что местом преступления часто является не физическое пространство, а виртуальное (компьютерная сеть, сервер, аккаунт в социальной сети, что требует иных подходов к осмотру места происшествия и фиксации следов);

скоротечность и изменчивость информации указывает на то, что цифровая информация легко изменяется, удаляется или уничтожается. Оперативность действий следователя крайне важна для сохранения доказательств;

---

[1] Попов А. М., Дубовицкий А. И. Особенности производства осмотра по преступлениям в сфере компьютерной информации // Вестник экономической безопасности. 2020. № 1. URL: https://cyberleninka.ru/article/n/osobennosti-proizvodstva-osmotra-po-prestupleniyam-v-sfere-kompyuternoy-informatsii (дата обращения: 20.01.2025).

специальные знания предусматривают, что расследование требует от следователя и оперативных сотрудников понимания основ компьютерных технологий, сетевых протоколов, принципов работы программного обеспечения. Необходимость привлечения специалистов-компьютерщиков;

анонимность значит, что преступники часто используют средства анонимизации в сети (VPN, Tor, прокси-серверы), что затрудняет их идентификацию и установление местоположения;

легитимность использования компьютерных систем обуславливает, часто преступления совершаются с использованием легально принадлежащих компьютеров и сетей, что затрудняет выявление преступной деятельности на начальном этапе.

Далее необходимо рассмотреть особенности отдельных следственных действий:

1. Осмотр места происшествия является одним из наиболее неотложных и информационно насыщенных следственных действий, имеющих целью обнаружение, фиксацию и изъятие следов преступления, орудий преступления, предметов и документов, имеющих значение для уголовного дела, а также выяснение обстановки происшествия. Традиционно под местом происшествия понималось физическое пространство – участок местности, помещение, транспортное средство, где было совершено преступление или обнаружены его следы. Однако в условиях развития информационных технологий и увеличения доли преступлений, совершаемых в цифровой среде, понятие «места происшествия» рассматривается. Сегодня местом происшествия может быть не только физическая локация, но и виртуальное пространство – серверы, веб-сайты, электронные почтовые ящики, аккаунты в социальных сетях, облачные хранилища и иные информационные ресурсы, где хранятся, обрабатываются или передаются данные, являющиеся следами преступления.

Указанная трансформация влечет за собой специфические особенности производства осмотра. Фиксация виртуального «места происшествия» требует

применения особых технических средств и тактических приемов. Вместо традиционных фототаблиц и планов местности используются скриншоты, запись видео с экрана, составление подробных протоколов осмотра веб-страниц с указанием их структуры, содержания, гиперссылок. Критически важным является точное документирование технических параметров: URL-адресов, IP-адресов, а также точного времени и даты проведения осмотра, что придает полученным данным доказательственную значимость и позволяет проверить их достоверность.

Неотъемлемой частью осмотра, связанного с цифровыми следами, становится тщательный осмотр и последующее изъятие компьютерной техники и носителей информации, которые могут содержать эти следы, что включает осмотр компьютеров, серверов, мобильных устройств, внешних накопителей, сетевого оборудования. При осмотре такой техники фиксируются ее идентификационные данные (марка, модель, серийный номер), состояние, наличие подключенных устройств[1]. Как правило, изъятию подлежит вся техника, которая потенциально может содержать имеющую значение для дела информацию. Процедура изъятия должна быть оформлена строго в соответствии с требованиями УПК РФ, с обеспечением сохранности объектов, упаковки, исключающей несанкционированный доступ и изменение данных, а также с составлением подробного протокола.

Учитывая специфику работы с цифровой информацией и компьютерной техникой, для надлежащего проведения осмотра «цифрового» места происшествия и изъятия связанных с ним объектов обязательно привлекается специалист в области компьютерных технологий (цифровой криминалистики). Специалист оказывает помощь следователю в обнаружении, правильной

---

[1] Гайнельзянова В. Р. Криминалистический аспект рассмотрения осмотра места происшествия в ходе расследования преступлений в сфере компьютерной информации // Государственная служба и кадры. 2022. № 2. URL: https://cyberleninka.ru/article/n/kriminalisticheskiy-aspekt-rassmotreniya-osmotra-mesta-proisshestviya-v-hode-rassledovaniya-prestupleniy-v-sfere-kompyuternoy (дата обращения: 20.01.2025).

фиксации, изъятии цифровых следов и техники, обеспечивая их целостность, неизменность и допустимость как доказательств. Таким образом, эффективное производство осмотра места происшествия в современных условиях требует не только владения традиционными криминалистическими методами, но и глубокого понимания особенностей работы с цифровой информацией и тесного взаимодействия со специалистами в этой области.

2. Обыск представляет собой одно из наиболее эффективных следственных действий, направленных на принудительное обследование помещений, территорий, транспортных средств или лиц с целью обнаружения и изъятия предметов, документов и ценностей, имеющих значение для уголовного дела, а также обнаружения разыскиваемых лиц. В условиях роста числа преступлений, совершаемых в цифровой среде, цель обыска существенно расширяется. Так ключевым направлением становится поиск и изъятие не только традиционных материальных объектов, но и цифровых следов: компьютерной техники, носителей информации (жестких дисков, флеш-накопителей, оптических дисков, карт памяти), электронных документов, программного обеспечения, а также сведений, имеющих доказательственное значение, таких как пароли, логины, ключи шифрования, и, самое главное, информации, прямо или косвенно подтверждающей причастность конкретного лица к совершению преступления.

Особенностью современного обыска, связанного с расследованием киберпреступлений, является возможность его проведения не только в физическом пространстве (по месту жительства, работы подозреваемого/обвиняемого, в офисах компаний), где может находиться компьютерная техника, но и на основании соответствующего судебного решения, в виртуальном пространстве. Также можно рассмотреть возможность «виртуального обыска» под которым следует понимать процессуальное действие по получению доступа, обследованию и изъятию данных из электронных почтовых ящиков, аккаунтов в социальных сетях, облачных хранилищ, серверов

и иных удаленных информационных ресурсов, контролируемых лицом, у которого проводится обыск, или содержащих искомые данные[1].

Успех и законность проведения обыска, особенно при работе с цифровыми объектами, во многом зависит от тщательной предварительной подготовки. Она включает не только традиционное планирование, но и определение конкретного перечня искомых цифровых объектов и информации, изучение особенностей используемых подозреваемым или обвиняемым информационных систем, а также подготовку специализированных технических средств для безопасного доступа к компьютерной технике, копирования (клонирования) данных и их предварительного анализа на месте обыска. Необходимым является привлечение специалиста в области компьютерных технологий, который оказывает помощь следователю в обнаружении, оценке, фиксации и изъятии цифровых объектов и данных.

Критически важным аспектом обыска, связанного с изъятием носителей цифровой информации, является обеспечение сохранности данных. Любое неосторожное действие может привести к случайному повреждению, изменению или даже уничтожению доказательственной информации. Поэтому при изъятии компьютерной техники и носителей информации применяются методы, исключающие несанкционированное изменение данных: создание точных побитовых копий (клонирование жестких дисков) с использованием аппаратных или программных блокираторов записи, фиксация состояния системы на момент изъятия. Данные действия должны быть подробно отражены в протоколе обыска.

При проведении обыска и изъятии цифровых носителей необходимо строго соблюдать конституционные права граждан и процессуальные нормы. Изъятию подлежит только та компьютерная техника и носители информации, которые могут содержать имеющую значение для уголовного дела информацию. При последующем анализе изъятых данных должна быть обеспечена конфиденциальность личной информации, не имеющей отношения

---

[1] Александрова И. В. Указ соч. С. 211.

к расследуемому преступлению. Допрос является одним из ключевых следственных действий, позволяющих получить вербальную информацию от участников уголовного судопроизводства – подозреваемых, обвиняемых, потерпевших и свидетелей. В условиях расследования преступлений, совершенных с использованием информационных технологий, специфика допроса заключается в необходимости адаптации методик и вопросов для выяснения обстоятельств, связанных с цифровыми следами и техническими аспектами деяния.

При допросе подозреваемых и обвиняемых критически важно учитывать их уровень компьютерной грамотности. Следователю необходимо использовать понятные термины, избегая чрезмерного технического жаргона, чтобы обеспечить адекватное восприятие вопросов и получение правдивых показаний. Основное внимание уделяется выяснению мотивов, целей, конкретных способов и механизмов совершения преступления в цифровой среде, а также установлению роли каждого участника преступной группы, если таковая имелась.

Допрос потерпевших направлен на получение детальной информации о характере и обстоятельствах причинения вреда, виде и размере понесенного ущерба (включая, при необходимости, упущенную выгоду). Важно выяснить, какие именно технические средства использовались потерпевшим (компьютеры, смартфоны, аккаунты, сервисы), какие меры безопасности были им предприняты до и в момент совершения преступления, и как он обнаружил факт противоправного воздействия.

Сведения от свидетелей могут касаться действий подозреваемых, используемых ими технических средств, обстоятельств подготовки или совершения преступления, а также поведения потерпевшего до и после инцидента. Свидетели могут предоставить информацию, подтверждающую или опровергающую информацию, или уточняющую технические детали, которые могли быть ими замечены.

Особое значение имеет допрос специалистов, обладающих специальными знаниями в области информационных технологий. Они могут предоставить

следователю квалифицированные разъяснения по сложным техническим вопросам, связанным с работой компьютерной техники, сетевыми протоколами, спецификой программного обеспечения, методами защиты информации и способами осуществления несанкционированного доступа, что необходимо для правильного понимания механизма преступления и оценки доказательств.

4. В процессе расследования преступлений, совершенных в сфере информационных технологий, ключевое значение приобретает назначение и производство судебных экспертиз. Главным инструментом здесь выступает компьютерная экспертиза, целью которой является исследование компьютерной техники, программного обеспечения и цифровых данных для установления обстоятельств, имеющих существенное значение для уголовного дела[1]. Компьютерно-техническая экспертиза включает в себя несколько специализированных видов: экспертизу компьютерной техники (исследование аппаратной части), экспертизу программного обеспечения (анализ программного кода и функционала), экспертизу компьютерной информации (поиск, извлечение и анализ данных), сетевую экспертизу (исследование сетевой активности и соединений) и экспертизу по восстановлению данных (работа с удаленной или поврежденной информацией). Эффективность проведения указанной экспертизы во многом зависит от правильной постановки вопросов эксперту, которые должны быть четкими, конкретными и относиться к его технической компетенции.

При расследовании преступлений в сфере компьютерной информации активно применяются и другие следственные действия, адаптированные к специфике предмета доказывания. К ним относятся контроль и запись

---

[1] Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации (вместе с «Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», «Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации») [Электронный ресурс] : приказ МВД России от 29 июня 2005 № 511 . Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

переговоров (при использовании цифровых каналов связи), получение информации о соединениях между абонентами и устройствами (анализ метаданных коммуникаций), опознание (включая, при необходимости, идентификацию цифровых объектов или закономерностей) и следственный эксперимент (для проверки технических возможностей или воспроизведения цифровых действий). Комплексное и грамотное применение этих экспертиз и следственных действий позволяет эффективно собирать, анализировать и закреплять цифровые доказательства, необходимые для установления истины по делу.

При изучении материалов уголовных дел и на основании обстоятельств уголовного дела: неустановленное лицо путем осуществления входа в сеть «Интернет» посредством соединения с сервером провайдера, незаконно воспользовавшись аккаунтом на портале «Госуслуги» и паролем, принадлежащим гражданину, получило неправомерный доступ к охраняемом законом компьютерной информации, что повлекло блокирование личного кабинета на указанном портале, было принято решение о проведении такого следственного действия, как получение информации о соединениях между абонентами и устройствами. Однако прежде требовалось получение судебного решения, тем самым следователем выло вынесение проставление с согласование руководителя следственного органа о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами (Приложение 2).

Таким образом, анализ особенностей производства отдельных следственных действий по преступлениям в сфере компьютерной информации показывает, что нематериальная природа цифровых доказательств и специфика их хранения и передачи требуют существенной адаптации традиционных следственных методов, применения специализированных технических средств и привлечения экспертов для эффективного сбора, фиксации и исследования электронных данных.

ГЛАВА 3. АКТУАЛЬНЫЕ ПРОБЛЕМЫ И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ МЕТОДИКИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Проблемные аспекты методики расследования преступлений в сфере компьютерной информации

Методика расследования преступлений в сфере компьютерной информации, несмотря на развитие технологий и накопленный опыт, сталкивается с рядом серьезных проблем. Проблемы обусловлены спецификой цифровой среды, природой цифровых доказательств и особенностями самих киберпреступлений. Основные проблемы методики расследования преступлений данного вида характеризуются следующими особенностями:

1. Одной из ключевых криминалистических проблем при расследовании преступлений в сфере компьютерной информации является специфическая природа цифровых доказательств. В отличие от традиционных материальных доказательств, цифровые следы (логи, файлы, сетевой трафик и пр.) не обладают физической формой, они существуют в виде электронных сигналов и записей. Их нематериальность и высокая изменчивость (способность к быстрому изменению, удалению или уничтожению) требуют применения специфических методов и инструментов для их обнаружения, фиксации и сохранения, значительно отличающихся от работы с физическими объектами. Кроме того, одной из характерных особенностей является огромный объем генерируемых компьютерными системами и сетями данных, что

2. Создает проблему, часто описываемую, как поиск «иголки в стоге сена», поскольку выявление действительно значимой для расследования информации среди терабайтов цифровых записей является чрезвычайно трудоемкой задачей, требующей использования специализированного программного обеспечения и аналитических навыков. Техническая сложность работы с цифровыми

доказательствами обусловлена необходимостью глубоких знаний в области информационных технологий, сетевых протоколов, операционных систем и криптографии. Данный вопрос делает обязательным привлечение квалифицированных экспертов-криминалистов в области компьютерных технологий для корректного сбора, анализа и интерпретации полученных данных, что усложняет процесс расследования. Не менее важным аспектом является обеспечение юридической значимости и допустимости цифровых доказательств. Процесс их обнаружения, изъятия, фиксации и исследования должен строго соответствовать процессуальному законодательству, поскольку любые нарушения установленных процедур могут привести к признанию таких доказательств недопустимыми в суде, тем самым подрывая доказательственную базу по делу. Наконец, проблема трансграничности цифровых доказательств, которые могут храниться на серверах в других юрисдикциях, создает значительные трудности с точки зрения их обнаружения, получения и правового оформления, что требует активного использования механизмов международного сотрудничества и правовой помощи, что зачастую является длительным и сложным процессом. Таким образом, уникальные характеристики цифровых доказательств требуют выработки и применения специфических криминалистических методик и тактик, отличающихся от традиционных подходов к работе с материальными следами преступления.

3. Одной из наиболее острых криминалистических и правовых проблем, связанных с расследованием преступлений в сфере компьютерной информации, является их выраженный транснациональный характер, который непосредственно порождает сложные вопросы юрисдикции. Данная сложность во многом обусловлена анонимностью и удаленностью преступников. Киберпреступники активно используют различные технологии анонимизации, такие как VPN, Tor и прокси-серверы, позволяющие скрывать свое реальное местоположение и личность. Более того, специфика киберпространства позволяет злоумышленникам действовать практически из любой точки мира,

находясь на значительном географическом удалении как от жертвы, так и от места нахождения цифровых следов, что делает установление их фактического местонахождения и идентификацию крайне затруднительным для правоохранительных органов одной страны. Следствием этого является острая необходимость в международной кооперации и правовой помощи. Расследование трансграничных киберпреступлений практически всегда требует активного взаимодействия с правоохранительными органами других государств, направления запросов о международной правовой помощи для получения доступа к цифровым доказательствам, идентификации подозреваемых, проведения следственных действий или изъятия серверов, расположенных за рубежом. Однако процесс международного сотрудничества зачастую является длительным, бюрократичным и сопряжен с различиями в законодательстве разных стран в сфере киберпреступности и процессуальных процедурах, что существенно замедляет или даже блокирует ход расследования. Не менее важным аспектом является фундаментальная проблема определения места совершения преступления в киберпространстве. В силу распределенной природы цифровых систем – когда серверы, компьютеры преступников, жертв и цифровые следы могут находиться в разных юрисдикциях одновременно – однозначно определить «место» совершения киберпреступления становится чрезвычайно сложной задачей, что порождает значительные трудности в определении подсудности уголовного дела (какое государство имеет право осуществлять уголовное преследование) и применимого права, создавая так называемые «юрисдикционные пробелы» или, наоборот, «конфликты юрисдикций». Таким образом, транснациональный характер киберпреступности порождает комплексные вызовы, требующие не только совершенствования национального законодательства и криминалистических методик, но и углубления международного сотрудничества для эффективного противодействия этим видам преступлений.

4. Исключительная скорость совершения и распространения преступлений данного вида создает следующую проблему, которая требует

принципиально иного подхода к оперативному реагированию. В отличие от традиционных форм преступности, атаки в компьютерной сфере обладают способностью к практически мгновенному, экспоненциальному распространению. Вредоносное программное обеспечение или иные виды атак могут поражать тысячи и даже миллионы информационных систем за считанные минуты или часы, пересекая географические и юрисдикционные границы без каких-либо физических препятствий. Такая скорость распространения делает жизненно важным максимально оперативное реагирование со стороны служб информационной безопасности и правоохранительных органов для локализации атаки, минимизации ущерба и предотвращения дальнейшего заражения. Любое промедление может привести к катастрофическим последствиям. Более того, в процессе расследования время играет критически важную роль. Цифровые следы преступления – лог-файлы, временные метки, данные в оперативной памяти, временные файлы, резервные копии – являются чрезвычайно волатильными и могут быть легко изменены, уничтожены или перезаписаны, как автоматически (например, в результате работы системы), так и целенаправленно преступником, стремящимся замести следы. Преступники, осознавая уязвимость цифровых улик, часто принимают меры для их сокрытия или уничтожения сразу после совершения деяния или даже в процессе атаки. Следовательно, промедление в начале расследования и сборе цифровых доказательств может привести к их безвозвратной утрате, что существенно затруднит или сделает невозможным установление всех обстоятельств преступления, идентификацию виновных и привлечение их к ответственности. Таким образом, необходимость оперативного реагирования на сам факт атаки и быстрота сбора и фиксации цифровых доказательств являются решающими факторами успеха в расследовании киберпреступлений, что требует постоянного совершенствования методик, технического оснащения и организационных процедур в правоохранительных органах.

§ 2. Актуальные направления совершенствования методики расследования преступлений в сфере компьютерной информации

Актуальные направления совершенствования методики расследования преступлений в сфере компьютерной информации определяются динамичным развитием самих информационных технологий и постоянной адаптацией преступниками своих методов и средств совершения противоправных деяний. Одним из главных векторов является необходимость постоянной адаптации методик к появлению новых видов информационных систем, сервисов и технологий, таких как облачные вычисления, искусственный интеллект, интернет вещей, распределенные реестры (блокчейн) и криптовалюты. Расследование преступлений, связанных с этими технологиями, требует разработки специфических подходов к обнаружению, сбору и анализу цифровых следов, которые могут существенно отличаться от традиционных. Параллельно критически важным становится повышение уровня профессиональной подготовки сотрудников правоохранительных органов, включающее не только углубленное знание технических аспектов функционирования современных информационных-систем, но и развитие навыков работы с большими объемами данных, понимание принципов криминалистического анализа цифровой информации
и основ информационной безопасности. Не менее значимым направлением является укрепление межведомственного и международного взаимодействия, поскольку киберпреступность по своей природе трансгранична и успешное расследование часто зависит от оперативного обмена информацией и координации действий между различными службами внутри страны и за ее пределами. Кроме того, совершенствование требует разработки и внедрения специализированного программного и аппаратного обеспечения для автоматизации процессов сбора, анализа и визуализации цифровых доказательств, а также актуализации нормативно-правовой базы для обеспечения законности и допустимости использования полученных данных в уголовном

процессе. В совокупности эти направления призваны обеспечить адекватное и эффективное противодействие растущим вызовам киберпреступности.

Указанные направления обусловлены как стремительным развитием информационных технологий, так и постоянной эволюцией методов совершения таких преступлений.

Одним из ключевых аспектов совершенствования методик расследования преступлений, предусмотренных главой 28 УК РФ, является их адаптация к вызовам, порождаемым новыми и развивающимися технологиями. Стремительное развитие облачных вычислений, Интернета вещей, технологий распределенных реестров (криптовалют), искусственного интеллекта, а также эволюция мобильных платформ и использование анонимных сетей существенно меняют способы совершения преступлений и усложняют процесс сбора и анализа цифровых доказательств. Преступники активно используют эти технологии для обеспечения анонимности, автоматизации атак, хранения и передачи данных, что требует пересмотра традиционных подходов к поиску, фиксации и извлечению цифровых следов. Эффективное противодействие necessitates разработку специализированных методик, учитывающих специфику получения и анализа данных, хранящихся в распределенных и облачных средах, извлекаемых из множества разнородных устройств с ограниченными ресурсами, связанных с псевдоанонимными транзакциями в блокчейне, а также полученных с современных, сильно защищенных мобильных устройств и из сложно отслеживаемых анонимных сетей, что влечет за собой потребность в постоянном обновлении технического инструментария, освоении новых аналитических методов (включая применение возможностей искусственного интелекта в самом расследовании) и непрерывном повышении квалификации сотрудников, специализирующихся на расследовании высокотехнологичных преступлений, что делает процесс адаптации непрерывным и критически важным для обеспечения эффективности правоприменения в цифровой среде.

Критическим фактором успешности борьбы с высокотехнологичной преступностью является не только адаптация следственных методик и наличие технического оснащения, но и, прежде всего, уровень профессиональной подготовки и специализации сотрудников правоохранительных органов, непосредственно занимающихся расследованием данной категории дел. Эффективное расследование требует от следователей, оперативных сотрудников и экспертов-криминалистов выхода за рамки традиционных юридических знаний; необходимо глубокое техническое образование, включающее понимание принципов функционирования компьютерных систем, сетей, протоколов передачи данных, операционных систем и различных типов программного обеспечения, что позволяет квалифицированно оценивать цифровую среду преступления. Особое значение приобретает развитие практических навыков цифровой криминалистики, подразумевающее обучение работе со специализированным программным и аппаратным обеспечением для квалифицированного извлечения, анализа и надежного сохранения цифровых доказательств при неукоснительном соблюдении процессуальных норм, обеспечивающих их допустимость в качестве доказательств в суде. Учитывая специфику и сложность преступлений данного вида, целесообразным является формирование специализированных подразделений или групп, сотрудники которых могут сосредоточиться исключительно на расследовании таких дел, накапливая уникальный опыт и углубляя свои компетенции в этой узкой, но динамично развивающейся области. При этом, скорость изменений в сфере информационных технологий делает систему непрерывного обучения и профессионального развития сотрудников абсолютно необходимой, требуя регулярного обновления знаний, освоения новых инструментов и обмена опытом для поддержания высокого уровня квалификации. Реализация этих мер является фундаментальным условием для формирования компетентного кадрового потенциала, способного адекватно реагировать на вызовы высокотехнологичной преступности и обеспечивать успешное расследование таких дел в современных условиях.

Ключевым фактором, определяющим эффективность расследования высокотехнологичных преступлений в условиях непрерывного технологического прогресса, является активная разработка и внедрение современного криминалистического программного и аппаратного обеспечения. Масштабы и сложность цифровых данных требуют перехода к автоматизации процессов сбора и анализа информации. Современные инструменты позволяют осуществлять автоматизированное извлечение данных с широкого спектра источников – от традиционных персональных компьютеров и серверов до мобильных устройств и облачных хранилищ. Они включают функции парсинга, способные извлекать структурированную и значимую информацию из неструктурированных данных, а также возможности анализа больших объемов данных, что критически важно при работе с петабайтами информации, генерируемой в ходе киберпреступлений. Для преодоления сложности и наглядности представления взаимосвязей в массивах цифровых доказательств незаменимыми становятся средства визуализации данных. Эти инструменты трансформируют сложные таблицы и логи в интуитивно понятные графики, схемы и диаграммы, позволяя наглядно представить связи между объектами, участниками и событиями, построить хронологию действий, визуализировать сетевую активность или потоки транзакций, тем самым значительно ускоряя процесс понимания картины преступления следователем. Учитывая постоянное появление новых технологий, используемых преступниками, возникает острая потребность в инструментах для работы с новыми технологиями. Это специализированное программное обеспечение для анализа данных распределенных реестров, инструменты для извлечения и анализа данных из устройств Интернета вещей, а также средства для анализа оперативной памяти и сетевого трафика, в том числе в реальном времени, что позволяет обнаруживать временные или скрытые следы. Наконец, для получения доступа к зашифрованной или защищенной информации, необходимой для доказательной базы, требуется наличие легальных инструментов и методик для обхода защитных механизмов, таких как шифрование, пароли. Разработка и применение

таких средств, осуществляется в строгом соответствии с процессуальными нормами является необходимым условием для обеспечения полноты собранных доказательств. Таким образом, непрерывное обновление и совершенствование технологической базы правоохранительных органов становится фундаментальным элементом успешной борьбы с высокотехнологичной преступностью.

Совершенствование нормативно-правовой базы и процессуальных аспектов работы с цифровыми доказательствами. Эффективность противодействия высокотехнологичной преступности в значительной степени зависит от адекватности существующей нормативно-правовой базы и разработанности процессуальных механизмов работы с цифровыми доказательствами. В условиях стремительного развития информационных технологий критически важным является актуализация законодательства, что предполагает внесение существенных изменений в УПК РФ и другие нормативные акты с целью четкого учета специфики сбора, фиксации, хранения и представления в суде цифровых доказательств. Особое внимание должно быть уделено правовому регулированию получения доступа к данным, находящимся за пределами национальной юрисдикции или размещенным в «облачных» хранилищах, что требует разработки механизмов международного сотрудничества и адаптации национального законодательства к трансграничному характеру цифровой информации. Параллельно с этим возникает острая необходимость в детальной регламентации процессуальных действий. Требуется четкое определение порядка проведения осмотра компьютерной информации на различных носителях, процедуры законного получения удаленного доступа к информационным системам, стандартизации методик проведения компьютерно-технических экспертиз и, что особенно важно для сохранения целостности доказательств, обеспечения надлежащей «цепочки хранения» цифровых данных с момента их обнаружения до представления в суде. Это позволит минимизировать риски утраты, изменения или оспаривания подлинности доказательств. Наконец,

для обеспечения справедливости судебного процесса и предотвращения злоупотреблений необходимо выработать единые подходы к оценке допустимости цифровых доказательств. Это включает установление критериев оценки законности методов и инструментов, использованных для их получения, а также стандартов документирования процесса сбора и анализа, что обеспечит прозрачность и проверяемость каждого этапа работы с цифровой информацией и повысит доверие суда к представленным материалам.

Таким образом, указанные направления взаимосвязаны и требуют комплексного подхода для совершенствования методики расследования преступлений в сфере компьютерной информации, предусмотренным гл. 28 УК РФ. Совершенствование по каждому из них напрямую влияет на эффективность расследования, собираемость доказательств и, как следствие, на неотвратимость наказания.

ЗАКЛЮЧЕНИЕ

Настоящая работа посвящена комплексному исследованию понятия, видов и особенностей методики расследования преступлений, совершаемых в сфере компьютерной информации. Актуальность выбранной темы обусловлена неуклонным ростом числа преступлений данного вида, их трансграничным характером, высокой латентностью, а также постоянным усложнением способов их совершения, что диктует необходимость непрерывного совершенствования правовой базы и, главное, криминалистических подходов к их раскрытию и расследованию.

В ходе проведенного исследования сделан вывод, что преступления в сфере компьютерной информации представляют собой общественно опасные посягательства, совершаемые в цифровой среде с использованием или в отношении средств вычислительной техники, информационных систем и телекоммуникационных сетей (включая критическую информационную инфраструктуру), и направленные на нарушение установленного порядка обращения с компьютерной информацией, ее конфиденциальности, целостности, доступности, а также на дезорганизацию нормального функционирования информационных систем и сетей, что влечет причинение вреда охраняемым законом интересам личности, общества и государства.. Классификация этих преступлений, представленная в работе, позволяет более четко структурировать подходы к их расследованию, исходя из особенностей предмета посягательства и используемых инструментов. Определенно, что нематериальная природа цифровых доказательств и специфика их хранения и передачи требуют существенной адаптации традиционных следственных методов, применения специализированных технических средств и привлечения экспертов для эффективного сбора, фиксации и исследования электронных данных.

Проведенный анализ показал, что эффективное расследование преступлений в сфере компьютерной информации сдерживается рядом объективных трудностей. К ним относятся: высокая скорость развития

информационных технологий и, как следствие, постоянное появление новых способов совершения преступлений, легкость сокрытия следов и достижения анонимности в сети «Интернет», трансграничный характер многих киберпреступлений, порождающий сложности взаимодействия между правоохранительными органами разных государств, большие объемы цифровой информации, требующие анализа, недостаток квалифицированных специалистов, обладающих необходимыми знаниями и навыками в области цифровой криминалистики.

Таким образом, развитие вопросов цифровизации в сфере уголовного судопроизводства и криминалистики представляет собой стратегическое направление, требующее системного подхода. В контексте расследования уголовных дел, особенно касающихся преступлений в сфере компьютерной информации, наблюдается выраженная специфика, детерминирующая потребность в специализированных знаниях и навыках у субъектов расследования. Для эффективного противодействия данной категории преступлений необходимо:

обеспечить комплексное обучение и регулярное повышение квалификации сотрудников следственных подразделений, направленное на формирование углубленных компетенций в области цифровых технологий и особенностей их применения в уголовном процессе;

разработка и внедрение методик, позволяющих всесторонне осмыслить специфику расследования преступлений в сфере компьютерной информации.

обеспечение способности следователей к надлежащему производству следственных действий в условиях цифровой среды;

оптимизировать механизмы межведомственного и внутриведомственного взаимодействия с профильными подразделениями и службами, что является ключевым фактором успешного раскрытия и расследования преступлений данного вида.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: принята всенародным голосованием 12 дек. 1993 г. с учетом поправок, внесенных Законами Рос. Федерации о поправках к Конституции Рос. Федерации от 30 дек. 2008 г. № 6-ФКЗ, от 30 дек. 2008 г. № 7-ФКЗ, от 5 февр. 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ, от 4 октября 2022 г. № 5-ФКЗ, от 4 октября 2022 г. № 6-ФКЗ, от 4 октября 2022 г. № 7-ФКЗ, от 4 октября 2022 г. № 8-ФКЗ // Рос. газ. – 2020. – 4 июля.

2. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13 июня 1996 г. № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

3. Уголовно-процессуальный кодекс Российской Федерации: федер. закон Рос. Федерации от 18 декабря 2001 г. № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 нояб. 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 дек. 2001 г. // Рос. газ. – 2001. – 22 декабря.

4. О связи: федер. закон Рос. Федерации от 7 июля 2003 № 126-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 18 июн. 2003 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 25 июн. 2003 г. // Собр. законодательства Рос. Федерации. – 2003. – № 28, ст. 2895.

5. О персональных данных: федер. закон Рос. Федерации от 27 июля 2006 г. № 152-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июл. 2006 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июл. 2006 г. // Собр. законодательства Рос. Федерации. – 2022. – № 29, ст. 5233.

6. Об информации, информационных технологиях и о защите информации: федер. закон Рос. Федерации от 27 июля 2006 № 149-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 8 июл. 2006 г.: одобр. Советом

Федерации Федер. Собр. Рос. Федерации 14 июл. 2006 г. // Собр. законодательства Рос. Федерации. – 2006. – № 31, ст. 3448.

7. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 12 июл. 2017 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 19 июл. 2017 г. // Собр. законодательства Рос. Федерации. – 2017. – № 31, ст. 4736.

8. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации (вместе с «Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», «Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации») [Электронный ресурс] : приказ МВД России от 29 июня 2005 № 511 . Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

II. Учебная, научная литература и иные материалы

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

2. Багдасарян А. В. Способы совершения компьютерных преступлений // Инновационная наука. 2022. №12-2. URL: https://cyberleninka.ru/article/n/sposoby-soversheniya-kompyuternyh-prestupleniy-1 (дата обращения: 20.01.2025).

3. Банюкова Д. В. Правовое регулирование преступлений в сфере информационных технологий // E-Scio. 2022. № 7 (70). URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-prestupleniy-v-sfere-informatsionnyh-tehnologiy (дата обращения: 12.05.2025).

4. Белевский Р. А. Методика расследования преступлений, связанных с неправомерным доступом к компьютерной информации в сетях ЭВМ : дис. ... канд. юрид. наук. Санкт-Петербург, 2006. 176 с.

5. Белкин Р.С. Курс криминалистики: учебное пособие для студентов вузов, обучающихся по юрид. специальностям. М. : Юнити, 2001. 837 с.

6. Беришвили Р. Ш. Компьютерные преступления // Символ науки. 2021. № 12-1. URL: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya (дата обращения: 20.01.2025).

7. Гайнельзянова В. Р. Криминалистический аспект рассмотрения осмотра места происшествия в ходе расследования преступлений в сфере компьютерной информации // Государственная служба и кадры. 2022. № 2. URL: https://cyberleninka.ru/article/n/kriminalisticheskiy-aspekt-rassmotreniya-osmotra-mesta-proisshestviya-v-hode-rassledovaniya-prestupleniy-v-sfere-kompyuternoy (дата обращения: 20.01.2025).

8. Григорян С. А. Особенности личности современного «киберпреступника» // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2022. № 8 (147). С. 103-106. URL: https://elibrary.ru/seyfyc (дата обращения: 20.01.2025).

9. Егорышев, А. С. Расследование и предупреждение неправомерного доступа к компьютерной информации : дис. ... канд. юрид. наук. Уфа, 2004. 230 с.

10. Жижина М. В., Завьялова Д.В. Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах. М.: Проспект, 2023. 136 с. URL: https://elibrary.ru/oimenm (дата обращения: 20.01.2025).

11. Зеленкина О. Ю. Особенности расследования преступлений в сфере компьютерной информации // Сибирские уголовно-процессуальные и криминалистические чтения. 2019. № 2 (24). URL: https://cyberleninka.ru/article/n/osobennosti-rassledovaniya-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения: 20.01.2025).

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

13. Мартынова Н. В. Некоторые аспекты криминологической характеристики личности киберпреступника // Студенческий вестник. 2022. № 17-5 (209). С. 7-10. URL: https://elibrary.ru/jgqysk (дата обращения: 20.01.2025).

14. Марьясис И. В. Криминалистические характеристики компьютерных преступлений // Инновационная наука. 2021. № 12-2. URL: https://cyberleninka.ru/article/n/kriminalisticheskie-harakteristiki-kompyuternyh-prestupleniy (дата обращения: 20.01.2025).

15. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : дис. ... док. юрид. наук. Воронеж, 2001. 387 с.

16. Могунова М. М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) // Вестник Саратовской государственной юридической академии. 2020. № 4 (135). С. 135-141. URL: https://doi.org/10.24411/2227-7315-2020-10110, https://elibrary.ru/hfbjrg (дата обращения: 20.01.2025).

17. Петрова И. А., Лобачев И. А. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств // Журнал прикладных исследований. 2020. № 1. URL: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-kompyuternoy-tsifrovoy-informatsii-diskussionnye-voprosy-opredeleniya-ponyatiya-obekta-ugolovno-pravovoy-ohrany (дата обращения: 20.01.2025).

18. Попов А. М., Дубовицкий А. И. Особенности производства осмотра по преступлениям в сфере компьютерной информации // Вестник экономической безопасности. 2020. № 1. URL: https://cyberleninka.ru/article/n/osobennosti-proizvodstva-osmotra-po-prestupleniyam-v-sfere-kompyuternoy-informatsii (дата обращения: 20.01.2025).

19. Попов А. Н. Преступления в сфере компьютерной информации : учебное пособие. СПб: Университета прокуратуры Российской Федерации, 2018. 68 с.

20. Савченко М. Ю. Способы совершения преступлений в сфере компьютерной информации и меры по их профилактике // Вестник КРУ МВД России. 2024. № 2 (64). URL: https://cyberleninka.ru/article/n/sposoby-sovershеniya-prestupleniy-v-sfere-kompyuternoy-informatsii-i-mery-po-ih-profilaktike (дата обращения: 20.01.2025).

21. Тарчоков Б. А. Тенденции развития киберпреступности в глобальном информационном пространстве // Проблемы экономики и юридической практики. 2021. Т. 17. № 1. С. 198-201.

22. Тарчоков Б. А., Хитиева А. Ж. Преступления в сфере компьютерной информации: виды и способы совершения // Журнал прикладных исследований. 2021. № 6. URL: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-kompyuternoy-informatsii-vidy-i-sposoby-sovershеniya (дата обращения: 20.01.2025).

23. Тарчоков Б. А., Хитиева А. Ж. Преступления в сфере компьютерной информации: виды и способы совершения // Журнал прикладных исследований. 2021. №6. URL: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-kompyuternoy-informatsii-vidy-i-sposoby-sovershеniya (дата обращения: 20.01.2025).

24. Ульянов М. В. Преступления в сфере компьютерной информации: возможности уголовно-правового воздействия и предупреждения // правопорядок: история, теория, практика. 2022. № 4 (35). URL: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-kompyuternoy-informatsii-vozmozhnosti-ugolovno-pravovogo-vozdeystviya-i-preduprezhdeniya (дата обращения: 20.01.2025).

25. Филиппова А. Г. Криминалистическая методика : учебник для вузов. М. : Юрайт, 2025. 339 с.

26. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие / Э. Д. Нугаева, С. Р. Низаева, В. Р. Гайнельзянова, З. И. Харисова. Уфа: Уфимский ЮИ МВД России, 2023. 96 с.

III. Эмпирические материалы:

1. 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» [Электронный ресурс] : постановление Пленума Верховного Суда РФ от 15 декабря 2022 № 37 . Документ опубликован не был. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Состояние преступности на территории Российской Федерации: официальный сайт МВД России. URL: https://мвд.рф/reports/item/60248328/ (дата обращения: 20.01.2025).

3. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) URL: https://www.consultant.ru/document/cons_doc_LAW_161817/ (дата обращения: 10.04.2025).

4. Приговор Ленинградского районного суда Краснодарского края № 1-20/2024 от 12 февраля 2024 г. URL: https://sudact.ru/regular/doc/AqzmSF1yIjWH/ (дата обращения: 10.04.2025).

5. Приговор Хасавюртовского городского суда Республики Дагестан 1-94/2024 от 27 февраля 2024 г. URL: https://sudact.ru/regular/doc/veqsKVcHL461/ (дата обращения: 10.04.2025).

6. Приговор Райчихинского городского суда Амурской области № 1-104/2024 от 7 мая 2024 г. URL: https://sudact.ru/regular/doc/pVmvLxn8r01/ (дата обращения: 10.04.2025).

7. Приговор Даниловского районного суда Ярославской области № 1-44/2024 от 13 июня 2024 г. URL: https://sudact.ru/regular/doc/XYf4UTzmlToW/ (дата обращения: 10.04.2025).

8. Приговор Заднепровского районного суда г. Смоленска № 1-199/2024 от 18 июня 2024 г. URL: https://sudact.ru/regular/doc/icBznkeWeDLq/ (дата обращения: 10.04.2025).

9. Приговор Центрального районного суда г. Сочи Краснодарского края № 1-482/2024 от 11 июля 2024 г. URL: https://sudact.ru/regular/doc/lR1ThzGEqYVT/ (дата обращения: 10.04.2025).

10. Приговор Сызранского городского суда Самарской области № 1-370/2024 от 25 июля 2024 г. URL: https://sudact.ru/regular/doc/IAumzEIDDmlX/ (дата обращения: 10.04.2025).

11. Приговор Курганского городского суда Курганской области № 1-1197/2024 от 1 сентября 2024 г. URL: https://sudact.ru/regular/doc/iO8awTPoNbN0/ (дата обращения: 10.04.2025).

12. Приговор Троицкого городского суда Челябинской области № 1-402/2024 от 11 сентября 2024 г. URL: https://sudact.ru/regular/doc/kW3bRTuiIMNE/ (дата обращения: 10.04.2025).

13. Приговор Неклиновского районного суда Ростовской области № 1-235/2024 от 17 сентября 2024 г. URL: https://sudact.ru/regular/doc/cr0FfHdCtaHj/ (дата обращения: 10.04.2025).

14. Приговор Нововятского районного суда г. Кирова № 1-169/2024 от 24 сентября 2024 г. URL: https://sudact.ru/regular/doc/AgxtDyNNi8d3/ (дата обращения: 10.04.2025).

15. Приговор Индустриального районного суда г. Барнаула Алтайского края № 1-670/2024 от 2 октября 2024 г. URL: https://sudact.ru/regular/doc/iS1uyIxQRj51/ (дата обращения: 10.04.2025).

16. Приговор Центрального районного суда № 1-781/2024 от 3 октября 2024 г. URL: https://sudact.ru/regular/doc/el2bC1Ssrnbq/ (дата обращения: 10.04.2025).

ПРИЛОЖЕНИЕ 1

П О С Т А Н О В Л Е Н И Е № 124XXXXXXXXXXXXX
о возбуждении уголовного дела и принятии его к производству

с. Николо-Березовка хх хх 2024 года
16 часов 25 минут

Следователь СО отдела МВД России по Краснокамскому району капитан юстиции Х, рассмотрев сообщение о преступлении - неправомерного доступа к компьютерной информации, зарегистрированное в КУСП Отдела МВД России по Краснокамскому району за № хххх от хх.хх.2024,

У С Т А Н О В И Л:

хх.хх.2024 года около 11 час. 36 мин. неустановленное лицо, находясь в неустановленном месте, умышленно, путём осуществления входов в сети Интернет, посредством соединения с сервером провайдера, незаконно воспользовавшись аккаунтом на портале «Госуслуги» и паролем, принадлежащим гр. К., повлекло блокирование личного кабинета на портале «Госуслуги».

В результате преступных действий неустановленное лицо получило неправомерный доступ к охраняемой законом компьютерной информации, совершенное из корыстной заинтересованности.

Принимая во внимание, что имеются достаточные данные, указывающие на признаки преступления, предусмотренного ч. 1 ст. 272 УК РФ, руководствуясь ст. ст. 140, 145, 146 и ч.1 ст. 156 УПК РФ,

П О С Т А Н О В И Л:

1. Возбудить уголовное дело по признакам состава преступления, предусмотренного ч. 1 ст. 272 УК РФ.
2. Уголовное дело принять к своему производству и приступить к его расследованию.
3. Копию настоящего постановления направить в Прокуратуру Краснокамского района Республики Башкортостан.

Следователь СО отдела МВД России по Краснокамскому району
капитан юстиции

Копия настоящего постановления направлена в прокуратуру хх.хх.2024 в 17 часов 00 минут.

О принятом решении сообщено лицу, сообщившему о преступлении — гр. К.

Следователь СО отдела МВД России по Краснокамскому району
капитан юстиции

ПРИЛОЖЕНИЕ 2

«СОГЛАСОВАНО»
Руководитель следственного органа

–

Начальник СО Отдела МВД России
по Краснокамскому району
подполковник юстиции

«хх» хх 2024 года

ПОСТАНОВЛЕНИЕ
о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами

с. Николо-Березовка «04» апреля 2024 года

Следователь СО Отдела МВД России по Краснокамскому району капитан юстиции, рассмотрев материалы уголовного дела № 124ХХХ,

УСТАНОВИЛ:

Уголовное дело № 124ХХХ возбуждено хх.хх.2024 по признакам состава преступления, предусмотренного ч. 2 ст. 272 УК РФ.

Проведённым предварительным расследованием установлено, что В период с хх.хх.2023 по хх.хх.2024 неустановленное лицо, находясь в неустановленном месте, умышленно, путём осуществления входов в сети Интернет, посредством соединения с сервером провайдера, незаконно воспользовавшись аккаунтом на портале «Госуслуги» и паролем, принадлежащим гр. П., повлекло блокирование личного кабинета на портале «Госуслуги».

В результате преступных действий неустановленное лицо получило неправомерный доступ к охраняемой законом компьютерной информации, совершенное из корыстной заинтересованности.

В ходе предварительного следствия было установлено, что неустановленное лицо осуществляло звонок на абонентский номер потерпевшей +7987х.

С целью установления лица, причастного к совершению преступления, места и деталей его совершения, необходимо у оператора сотовой связи получить сведения о входящих и исходящих телефонных соединениях, SMS-сообщений, нулевых звонков в отношении абонента, зарегистрированного у оператора сотовой связи ПАО «МТС» (Ф.И.О., адреса проживания, номера абонента, время и дата выхода в эфир), использующего абонентский **+7987х** в период времени с хх.хх.2023 по хх.хх.2024, с обязательным указанием абонентских номеров собеседников,

номеров IMEI, базовых станций их местоположения, через которые происходило соединение.

В связи с вышеизложенным и руководствуясь ст.ст. 23, 25 Конституции РФ, ст. 64 Федерального закона от 07 июля 2003 года «О связи» № 126-ФЗ, ч. 1 ст. 144, ст.ст. 165, 186.1 УПК РФ,

ПОСТАНОВИЛ:

Ходатайствовать по уголовному делу № 124XXX возбужденному хх.хх.2024 по признакам состава преступления, предусмотренного ч. 2 ст. 272 УК РФ перед Краснокамским межрайонным судом о разрешении на получение сведений о входящих и исходящих телефонных соединениях, SMS-сообщений, нулевых звонков в отношении абонента, зарегистрированного у оператора сотовой связи сети ПАО «МТС» (Ф.И.О., адреса проживания, номера абонентов, время и даты выхода в эфир), использующего абонентский номер +7987х относящийся к емкости ПАО «Вымпелком» в период времени с хх.хх.2023 по хх.хх.2024, *и с момента вынесения данного постановления в течении шести месяцев по мере поступления информации, но не реже одного раза в неделю,* с обязательным указанием абонентских номеров собеседников, номеров IMEI, базовых станций их местоположения, через которые происходило соединение.

Следователь СО отдела МВД России по Краснокамскому району
капитан юстиции

Копия настоящего постановления направлена прокурору Краснокамского района Республики Башкортостан.

Следователь СО отдела МВД России по Краснокамскому району
капитан юстиции

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

Е.А. Микиев