МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Кафедра «Уголовное право и процесс»
(наименование)

40.03.01 Юриспруденция
(код и наименование направления подготовки /специальности)

Уголовно-правовой
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему «Методика расследования преступлений в сфере компьютерной информации»

Обучающийся В.В. Голенкова
(Инициалы Фамилия) (личная подпись)

Руководитель К.А. Корчагина
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2024

Аннотация

В сегодняшнем быстро развивающемся цифровом мире интеграция технологий во все аспекты жизни общества привела к значительным изменениям. Хотя эти достижения предлагают многочисленные преимущества, они также создают серьезные проблемы, особенно в области кибербезопасности. Растущую обеспокоенность вызывает рост киберпреступлений, которые в настоящее время составляют значительную долю всей преступной деятельности.

Эксперты прогнозируют, что киберпреступления, особенно те, которые совершаются через Интернет, будут все больше выступать в качестве движущей силы более широкого спектра глобальной преступной деятельности. Эта растущая угроза подчеркивает настоятельную необходимость в разработке и совершенствовании методов расследования для эффективного противодействия этим преступлениям.

Необходимость развития надежных методов расследования в сфере киберпреступности имеет решающее значение и не может быть недооценена. В данной работе основное внимание уделяется изучению и анализу различных методологий, используемых при расследовании компьютерных преступлений.

Структура данной работы состоит из введения, в котором показана сфера обсуждения. Затем идут три главы, каждая из которых рассматривает конкретные аспекты исследовательских методологий, относящихся к расследованию киберпреступности. Исследование завершается заключением и списком используемой литературы и используемых источников в котором перечислены все соответствующие источники и литература, использованные в ходе исследования.

Оглавление

Введение

Стремительное развитие технологий открыло эру возросшей компьютеризации, глубоко повлияв на различные аспекты современного общества. Поскольку учреждения и организации все больше зависят от компьютерных сетей и систем управления данными, возникла насущная проблема: рост преступлений, связанных с компьютерной информацией. Операционный успех современных учреждений, будь то государственные или частные, все больше зависит от эффективной обработки, хранения и безопасности данных.

Определяющей чертой этой технологической эпохи является бесшовная интеграция отдельных локальных сетей в обширную глобальную систему, чему способствуют сложные цифровые телекоммуникации. Эта взаимосвязанная сеть особенно важна в секторах стратегического значения, таких как национальная оборона и экономика. В этих областях автоматизированные системы, работающие на микропроцессорных устройствах и интегральных схемах, необходимы для управления, мониторинга, прогнозирования и обеспечения безопасности.

Однако распространение цифровых инструментов и широкая доступность телекоммуникационных ресурсов непреднамеренно подстегнули всплеск преступной деятельности в этой области. Анонимность, часто связанная с огромными объемами информации, обрабатываемой компьютерами, сделала этот сектор особенно уязвимым для преступной эксплуатации. Хотя текущая статистика из Российской Федерации указывает на то, что преступления, связанные с компьютерами, по-прежнему составляют относительно небольшую долю от общего числа зарегистрированных преступлений, быстрый рост таких инцидентов вызывает тревогу. Эта тенденция свидетельствует о том, что компьютерные преступления находятся на грани превращения в значительный элемент преступной деятельности,

требуя немедленного и постоянного внимания со стороны правоохранительных органов и политиков.

Растет убеждение, что преступления, связанные с компьютерной информацией, особенно те, которые совершаются в сети, вскоре станут движущей силой большинства видов преступной деятельности. Интернет, в частности, стал рассадником компьютерных преступлений. Развитие компьютерных технологий и ИТ-образования позволило разработать новые методы совершения преступлений против собственности, нарушений прав интеллектуальной собственности и даже государственной измены.

Одним из наиболее существенных аспектов компьютерных преступлений является их способность совершаться через национальные границы с минимальными усилиями. Эта транснациональная способность значительно усиливает угрозу, которую они представляют для общественной безопасности. Ситуация еще больше осложняется относительно неразвитой теоретической и правовой базой, окружающей компьютерные преступления.

Расследование и предотвращение компьютерных преступлений представляют собой уникальные проблемы из-за их технической сложности. Сотрудники правоохранительных органов часто испытывают трудности с выполнением этих задач, поскольку им может не хватать специальных знаний в области ИТ, необходимых для проведения всесторонних расследований. Этот пробел в знаниях может затруднить обеспечение тщательности расследований и проведение справедливых и законных судебных разбирательств. Такие технические проблемы и недостатки в экспертизе имеют потенциал.

Преступления, связанные с компьютерами, являются проблемой не только для высоко-компьютеризированных и развитых стран. Они также затрагивают страны с менее развитой технологической инфраструктурой и слабыми промышленными и социальными отношениями. Поскольку общество продолжает цифровизироваться, борьба с ростом компьютерных преступлений и повышение квалификации правоохранительных органов в

этой области будут иметь решающее значение для поддержания безопасности и правосудия в информационную эпоху.

Цель выпускной работы заключается в том, чтобы изучить особенности методики расследования преступлений в сфере компьютерной информации.

Растущая угроза киберпреступности представляет собой серьезную проблему для правоохранительных органов во всем мире. Главным препятствием для эффективного противодействия этим преступлениям является недостаточная профессиональная подготовка персонала, ответственного за расследование киберинцидентов. Значительное число этих специалистов не имеют необходимого опыта в таких критически важных областях, как информационные технологии, кибербезопасность и управление специализированным программным обеспечением и компьютерными информационными системами. Этот недостаток образования серьезно ограничивает их способность эффективно реагировать на киберпреступную деятельность.

Более того, крайне важно, чтобы эти специалисты не только получили базовое образование, но и участвовали в непрерывном обучении и повышении квалификации. Поскольку киберпреступники постоянно совершенствуют свои методы и расширяют свои технологические возможности, сотрудники правоохранительных органов также должны повышать свои навыки, чтобы идти в ногу со временем. Постоянное профессиональное развитие имеет важное значение для обеспечения того, чтобы правоохранительные органы могли быстро и эффективно реагировать на постоянно меняющуюся сферу киберпреступности. Регулярное профессиональное развитие имеет решающее значение для того, чтобы идти в ногу с этими динамичными и постоянно меняющимися угрозами, гарантируя, что те, кто находится на передовой борьбе с киберпреступностью.

Этот непрерывный процесс обучения необходим для обеспечения того, чтобы правоохранительные органы могли эффективно противодействовать изощренным тактикам, используемым компьютерными преступниками.

Важность, актуальность, теоретическая и практическая значимость исследования компьютерных информационных преступлений подчеркивают необходимость всесторонних и обновленных программ обучения.

Объектом исследования является оперативно-розыскная деятельность правоохранительных органов по расследованию компьютерно-информационных преступлений.

Предметом исследования являются криминалистическая характеристика этих преступлений и производство отдельных следственных действий.

Цель работы - изучить методологии расследования преступлений в сфере компьютерной информации.

Цель решается через поставленные задачи:

- рассмотреть основные элементы криминалистической характеристики субъективной стороны преступлений в сфере компьютерной информации;
- проанализировать криминалистическую характеристику объективной стороны преступлений в сфере компьютерной информации;
- изучить особенности и методы расследования преступлений в сфере компьютерной информации.

В этом контексте методология расследования понимается как комплексная система, которая объединяет научные принципы, технические инструменты, тактические стратегии и методические указания.

Структура работы начинается с введения, в котором описывается область обсуждения, за которым следуют три главы, в которых рассматриваются конкретные аспекты исследовательских методологий, связанных с расследованием киберпреступлений. Работа завершается заключением и списком используемой литературы и используемых источников.

Глава 1 Основные элементы криминалистической характеристики субъективной стороны преступлений в сфере компьютерной информации

1.1 Типологические данные о субъектах преступлений в сфере компьютерной информации

Стремительное развитие технологий породило новый и сложный ландшафт преступной деятельности, особенно в сфере киберпреступности. Среди наиболее выдающихся фигур в этой области - хакеры, чьи знания и действия оказали глубокое влияние на характер и развитие компьютерных преступлений. Понимание роли хакеров в цифровом преступном мире имеет важное значение для разработки эффективных стратегий борьбы с киберпреступностью. Проблема заключается не только в их техническом мастерстве, но и в их способности постоянно адаптироваться и развиваться, создавая значительные препятствия для правоохранительных органов по всему миру.

В сфере компьютерных преступлений феномен «хакеров» часто рассматривается как тесно переплетенный с истоками и развитием этих правонарушений. Термин «хакер» относится к лицам с передовыми знаниями в области компьютерных технологий, электронного документооборота (EDM), криптографии и смежных областях. Их неустанное стремление к новым знаниям и навыкам представляет собой значительную проблему для тех, кому поручено расследование этих преступлений. Хакеров, как правило, можно отнести либо к категории компьютерных нарушителей, либо, в более серьезных случаях, к категории компьютерных преступников. Статистика показывает, что значительная часть молодых специалистов в области компьютерных технологий тянется к хакерской деятельности. Привлекательность часто заключается в чувстве свободы и волнения, связанных с участием в запрещенных действиях.

Хакеров можно характеризовать как «пользователей электронно-вычислительных машин, систем ЭВМ, сети таких ЭВМ, деятельность которых заключается в несанкционированном доступе к охраняемой законом компьютерной информации» [12, с. 210].

Правительственные инициативы по укреплению систем безопасности часто служат мотивацией для хакеров доказать свою способность обходить эти защиты, независимо от того, нацелены ли они на государственные учреждения, частные организации или личную информацию отдельных граждан. Хакеры часто действуют группами, поддерживают присутствие в печатных СМИ и управляют веб-сайтами и порталами в глобальном Интернете. Интернет стал основной платформой для сообщества, вовлеченного в компьютерные и информационные преступления. Многочисленные незаконные сайты облегчают обмен знаниями между хакерами, позволяя им вербовать новых членов для преступной деятельности и рекламировать свои незаконные услуги.

Некоторые онлайн-ресурсы специально созданы для того, чтобы объединять людей, стремящихся заниматься преступной деятельностью, тем самым способствуя созданию среды, благоприятствующей распространению компьютерных преступлений. Эти нерегулируемые взаимодействия с преступным миром усугубляют и без того сложную ситуацию, делая предотвращение компьютерных преступлений еще более сложным. Хакеры также участвуют в форумах для обмена опытом и продвижения своих услуг, что не только вовлекает молодежь в незаконную деятельность, но и служит формой профессионального развития как для новичков, так и для опытных преступников. В этой цифровой экосистеме преступники обмениваются методами совершения и сокрытия преступлений, связанных с ИТ.

Кроме того, существует существенное сотрудничество между российскими хакерами и их международными коллегами, что способствует обмену опытом и знаниями. Это трансграничное сотрудничество еще больше усложняет усилия по борьбе с компьютерными преступлениями.

Криминологические исследования часто подчеркивают важность понимания личности преступника. В контексте киберпреступности определение типологии и характеристик преступников имеет важное значение для разработки всеобъемлющего криминологического профиля. Этот профиль играет решающую роль в формулировании эффективных стратегий как для предотвращения, так и для расследования киберпреступлений.

В криминологии анализ черт личности киберпреступников традиционно фокусируется на атрибутах, которые помогают правоохранительным органам предотвращать и сдерживать преступную деятельность. Однако этот узкий подход может упускать из виду другие критические характеристики, которые могут быть полезны для идентификации и задержания киберпреступников, тем самым усложняя обнаружение и раскрытие киберпреступлений.

Самый большой пробел – «это оставление без внимания особых навыков преступников, которые говорят нам об определенных способах совершения этих преступлений, которые в свою очередь формируют так называемый почерк преступника. Именно этот почерк и личностные особенности совершения и сокрытия преступлений и содержит большую часть «следов личности», совершившего преступление в сфере IT» [22, с. 7].

Вещественные доказательства, обнаруженные на месте преступления, могут дать ценную информацию о различных аспектах личности подозреваемого. Эти доказательства могут раскрыть важные детали, такие как профессиональный опыт человека, специальные знания, пол, возраст и характер его отношений с жертвами. Благодаря тщательному анализу таких доказательств следователи могут разработать подробный профиль, который охватывает как общие, так и конкретные черты личности преступника.

Это тонкое понимание позволяет экспертам-криминалистам создавать всеобъемлющий профиль киберпреступников, что значительно повышает способность правоохранительных органов выявлять преступников и предотвращать будущие киберпреступления. Расширяя область анализа черт личности, криминологи могут предложить более глубокие идеи, которые

способствуют более эффективным уголовным расследованиям и стратегиям сдерживания.

«Информацию, имеющую значение для криминалистов, можно классифицировать по нескольким основаниям» [14, с. 85].

При изучении киберпреступности необходимо анализировать информацию о личностях предполагаемых преступников. Эту информацию можно разделить на две отдельные группы:

- начальная следственная информация: эта группа состоит из данных, собранных на месте преступления, и информации, полученной от свидетелей, если таковая имеется. Эта ранняя информация имеет решающее значение для начальных этапов расследования, предоставляя зацепки, которые могут привести к задержанию преступника. Часто эти данные помогают сузить поиск до определенной группы потенциальных преступников, а иногда они могут точно указать на человека и выделить его уникальные личные черты. Эта информация бесценна для сравнительного анализа и составления статистических выводов о демографических характеристиках типичных киберпреступников, которые впоследствии могут быть использованы при разработке стратегий профилактики преступлений;
- информация, полученная в ходе допроса: эта группа включает данные, полученные в ходе допроса подозреваемых или обвиняемых лиц в соответствии с уголовно-процессуальным законодательством. В то время как первоначальная следственная информация дает общий профиль, данные, полученные в ходе допроса, позволяют проводить подробную типизацию и классификацию киберпреступников. Эта информация играет важную роль в понимании конкретных методов, используемых для совершения преступлений, и дает представление о предотвращении будущих правонарушений. Кроме того, она способствует установлению

взаимопонимания между сотрудниками правоохранительных органов и подозреваемыми, что имеет решающее значение для проведения правдивых допросов и получения признаний или доказательств вины.

Всесторонне анализируя эти две группы информации, следователи могут составить подробный профиль киберпреступников, что позволит повысить как раскрываемость киберпреступлений, так и разработку эффективных мер профилактики.

Выше было сказано о возможности типизации (классификации) преступников в сфере компьютерных преступлений, что необходимо для создания так называемых «типовых моделей преступников» [8, с. 273].

«Если анализировать случаи совершения данных преступлений ни отдельным взятым преступником, а группой лиц, то есть преступных сообществом, то предметом изучения становится информация, которая будет описывать именно эту группу. Для групп лиц одним из главных элементов изучения является ее структура, т.е. организация и порядок взаимодействия разных участников данного преступного сообщества. Но даже в данном случае изучаются участники группы как личности, их особенности, а также функционал в данном сообществе, так как преступное сообщество имеет свою иерархию и свои правила взаимодействия между ее участниками» [9, с. 94].

Изучение профилей киберпреступников имеет решающее значение для понимания и борьбы с преступлениями в цифровой сфере. Анализируя характеристики этих групп или сообществ, следователи могут лучше идентифицировать и задерживать всех участников преступных сетей и понимать основные преступные эпизоды.

С точки зрения криминологии киберпреступников можно разделить на несколько отдельных групп в зависимости от черт личности:

– профессиональные ИТ-преступники: в эту группу входят лица, которые проявляют своего рода фанатизм в своей незаконной деятельности. Эти преступления дают им чувство

профессионального достижения и личного удовлетворения. Вызов и волнение от совершения киберпреступлений мотивируют этих лиц постоянно совершенствовать свои методы как для совершения, так и для сокрытия своих преступлений. Основной характеристикой этой группы является четкое и преднамеренное намерение совершать преступления как средство демонстрации своей компетентности и утверждения своих навыков. «Постоянное совершенствование защиты приводит к постоянному совершенствованию преступников, что является причиной для улучшения алгоритма преступных действий и процессов» [1, с. 7]. Обязательно стоит отметить тот факт, что «данные преступники не имеют необходимой подготовки к совершаемому преступлению, способ совершения отличается оригинальностью и новизной свершения, а также отсутствуют меры для сокрытия совершаемого преступления» [23, с. 40];

- лица с психологическими расстройствами, связанными с информацией: эта менее изученная группа состоит из лиц, страдающих от таких психологических состояний, как информационные заболевания или компьютерные фобии. «Главными причинами в литературе называют систематические нарушения информационного режима индивидуума. Составляющих такого нарушения много, к ним можно отнести и «информационный голод», и «информационный перегруз», также незапланированные срочные и частые переключения с одного процесса на другой в информационной сфере, а также так называемый «информационный шум». Именно анализом этого заболевания, изучением причин появления и способов лечения занимается новая отрасль – информационная медицина» [27, с. 180];
- профессиональные преступники с эгоистичными мотивами («Профи»): в отличие от предыдущих групп, эти лица совершают повторные преступления в сфере компьютерной информации, всегда

заботясь о том, чтобы замести следы. Они обладают высоким уровнем преступных навыков и часто работают в составе организованных групп, оснащенных передовыми технологиями. В эти группы обычно входят не только программисты-преступники, но также юристы и экономисты, что делает их значительной угрозой для информационной безопасности. Члены этой группы обычно занимают должности, которые предоставляют им особый доступ к конфиденциальной информации и компьютерным системам, например, управленческий персонал или ключевые сотрудники в различных отраслях. Их законный доступ к защищенной информации отличает их, поскольку они используют свое положение для совершения киберпреступлений без каких-либо очевидных психологических отклонений. «Именно рост преступлений, совершенных преступными группами, и показывает статистика в последние годы» [29, с. 28].

Эта классификация распространяется и на характер доступа этих преступников к компьютерной информации. Они делятся на:

- внешние пользователи: лица, которые атакуют системы из-за пределов организации;
- внутренние пользователи: Инсайдеры, которые используют свой привилегированный доступ для совершения преступлений.

Понимание этих категорий, а также глубинных мотивов и методов киберпреступников имеет важное значение для правоохранительных органов. Это помогает разрабатывать целевые стратегии для предотвращения и расследования компьютерных преступлений, в конечном итоге усиливая меры кибербезопасности и сокращая количество таких правонарушений.

Необходимо дать определение внешнему пользователю – «это лицо, которое для получения информации обращается либо к посреднику, либо к ЭВМ» [7, с. 220].

При анализе киберпреступности крайне важно понимать классификацию преступников на основе их правового статуса и типа доступа к компьютерным системам и информации. Эта классификация помогает точно определить источники преступной деятельности и эффективно адаптировать стратегии предотвращения. Юридически зарегистрированные и незарегистрированные пользователи: киберпреступников можно классифицировать на основе того, являются ли они юридически зарегистрированными пользователями компьютерной системы или нет. Статистические данные показывают важную тенденцию: почти 95% компьютерных преступлений совершаются внутренними пользователями - теми, кто имеет разрешение или законный доступ к системе. Напротив, преступления, совершаемые внешними пользователями, относительно редки.

Категории, основанные на методологии доступа и преступности:

- преступления с использованием специализированного программного обеспечения: эта группа включает лиц, которые совершают киберпреступления, используя определенные программные инструменты. Эти преступники часто имеют технические роли, такие как программисты, ИТ-специалисты, системные администраторы, кассиры, бухгалтеры или даже операторы заправочных станций. Их опыт в использовании или манипулировании программными инструментами позволяет им осуществлять свою незаконную деятельность;
- преступления с использованием оборудования: Другая категория включает преступников, которые используют компоненты оборудования для совершения преступлений. Эта группа может включать операторов связи, сигналистов и подобных специалистов, которые используют оборудование для содействия своим преступным действиям;
- преступления через косвенный доступ: Эти лица получают доступ к компьютерным системам и информации косвенными способами,

часто манипулируя своими ролями в управлении или организационными должностями. Они используют свой доступ для совершения своих преступлений без прямого взаимодействия с системой.

Хотя характеристики внешних пользователей признаются, они менее актуальны для детального расследования и предотвращения компьютерных преступлений. Внешними преступниками могут быть любые лица, и они с меньшей вероятностью предоставят существенную информацию для совершенствования следственных процедур или улучшения стратегий предотвращения. Поэтому основное внимание уделяется внутренним пользователям, чей существенный доступ и особые роли вносят более непосредственный вклад в распространенность киберпреступлений.

Понимание этих классификаций помогает в разработке эффективных методов расследования и превентивных мер, рассматривая различные методологии и уровни доступа киберпреступников. Такой подход повышает способность более точно нацеливать вмешательства и меры безопасности, снижая вероятность будущих киберпреступлений.

1.2 Сведения об обстановке и типичных мотивах их совершения преступлений в сфере компьютерной информации

Анализ среды, в которой происходит преступление, играет ключевую роль в уголовном праве и процессе. Эту среду можно рассматривать как с широкой, так и с узкой точки зрения, каждая из которых предлагает уникальное понимание характера и обстоятельств преступления. Понимание конкретного контекста преступления имеет важное значение для его тщательного расследования.

Широкое и узкое определения ситуаций преступления:

– широкое определение: в широком смысле окружающая среда относится к современным общественным условиям и стадии

развития, влияющим на динамику преступности. Эта перспектива подчеркивает, как текущие социальные изменения и достижения влияют на распространенность и характер преступлений. Она подчеркивает, что преступная среда непрерывно развивается и формирует преступное поведение;

- узкое определение: в более конкретном смысле окружающая среда относится к непосредственным условиям, окружающим конкретное преступление. Это включает в себя прямые факторы, влияющие как на жертву, так и на преступника. Узкое определение фокусируется на ситуативном контексте, который напрямую влияет на преступление, включая физические и социальные условия во время преступления.

Если говорить об этой величине в узком смысле слова понимается «определенная группа факторов, позволяющие судить об особенностях влияния этой системы на содержание преступного события» [13, с. 305].

Подробный ситуационный анализ является неотъемлемой частью судебной характеристики любого преступления. Тщательно изучая окружающую среду, следователи могут выдвигать обоснованные гипотезы и делать значимые выводы о различных аспектах преступления. Это всестороннее исследование не только проливает свет на природу преступного деяния, но и помогает выявить критические компоненты инцидента [6], повышая общую эффективность расследования:

- потенциальные криминальные черты, характеристики предполагаемого преступника;
- методы преступления, как было совершено преступление;
- сопутствующие обстоятельства, факторы, которые способствовали или способствовали совершению преступления.

Расследование конкретных обстоятельств преступления повышает эффективность поисковых мероприятий и имеет решающее значение для задержания подозреваемых. Оно дает критически важное представление об

условиях, которые позволили преступлению произойти, и помогает в разработке стратегий по предотвращению подобных правонарушений.

Субъективные аспекты киберпреступности:

При анализе субъективной стороны киберпреступлений необходимо учитывать несколько компонентов:

- вина: признание преступником своей вины и чувство ответственности за совершенное преступление;
- мотив: причины преступного поведения;
- цель: конечная цель или задача, определяющая преступление.

Понимание этих субъективных элементов дает всестороннее представление о мышлении преступника. Мотив преступления часто определяет решение человека совершить правонарушение, подчеркивая личные или внешние факторы, влияющие на его поведение.

Мотивы совершения киберпреступлений различаются у разных преступных групп. У каждой группы есть свои цели и причины для своих действий, на которые влияют их конкретные обстоятельства и намерения. Распознавание этих мотивов имеет важное значение для разработки целевых подходов к расследованию и превентивных мер.

«Именно эти различные мотивы (корысть, месть, доказывание своих профессиональных и преступных навыков и т.д.) в первую очередь влияют на способ совершения конкретно взятого преступления, а главное на выбор объекта как потерпевшего» [14, с. 208].

Понимание мотивов преступных действий необходимо для понимания как используемых методов, так и инструментов, используемых при совершении преступлений, особенно в контексте киберпреступности. Хотя мотив не является обязательным компонентом для установления совершения преступления, он имеет важное значение в уголовных расследованиях. Анализируя мотив, следователи могут получить ценную информацию о характере и целях преступления, улучшая свое понимание намерения преступника и общей цели преступления.

Мотив является ключевым фактором в определении подхода, методов и инструментов, используемых преступниками. Выявив мотив, правоохранительные органы могут сформулировать гипотезы о потенциальных преступниках и их конкретных целях. Это, в свою очередь, способствует проведению целенаправленных расследований и более эффективному поиску подозреваемых.

Типы мотивов киберпреступности:

- эгоистичные цели: многие киберпреступления мотивированы личной выгодой. Преступники, мотивированные финансовой или материальной выгодой, часто демонстрируют высокий уровень изощренности как в совершении, так и в сокрытии своих преступлений;
- политические цели: преступления с политическими мотивами характеризуются сложностью и стратегическим планированием. Эти преступления часто тщательно организованы для продвижения политических планов или создания беспорядков;
- месть: некоторые киберпреступники действуют из желания отомстить. Их действия обычно направлены на причинение вреда или смущения определенным лицам или организациям;
- хулиганство: эта категория включает в себя действия, вызванные желанием нарушить порядок или совершить акт вандализма без какой-либо конкретной цели личной выгоды или политических изменений. Такие преступления часто отражают импульсивное или безрассудное поведение;
- профессиональный или исследовательский интерес: некоторые люди совершают киберпреступления в рамках своего профессионального или интеллектуального любопытства. Эти преступники часто мотивированы вызовом проверки своих навыков или открытием новых методов атаки.

Отличительные черты мотивов:

– политически мотивированные и финансовые преступления: преступления, мотивированные политическими мотивами или финансовой выгодой, часто более изощренные, с использованием передовых методов, чтобы избежать обнаружения. Эти преступления требуют высокого уровня планирования и экспертизы;
– преступники-любители: Непрофессиональные преступники, или любители, обычно занимаются киберпреступностью без злого умысла. Для них компьютер - это инструмент для экспериментов и проверки навыков, а не средство достижения конкретных незаконных целей. Их деятельность часто включает в себя исследование новых методов взлома или манипулирования данными, которые впоследствии могут быть приняты более опытными преступниками;
– информационная болезнь: уникальная категория включает людей, страдающих от «информационных болезней», когда акт повреждения или уничтожения компьютеров служит формой психологического освобождения. Для этих людей компьютер сам по себе становится целью из-за его символической роли в их психическом расстройстве.

Понимание мотива киберпреступления необходимо для разработки эффективных стратегий расследования и превентивных мер. Анализируя намерения преступника, правоохранительные органы могут получить представление об используемых методах и приемах, выявить потенциальных подозреваемых и разработать целевые подходы для рассмотрения и смягчения таких преступлений. Это всестороннее понимание помогает в формулировании подробного профиля преступника, в конечном итоге повышая эффективность усилий по предупреждению и разрешению преступлений.

В сфере киберпреступности условия, при которых происходят эти преступления, существенно влияют на характер самих преступлений. Часто

киберпреступления совершаются лицами, которые испытывают повышенные эмоциональные состояния или психическую неустойчивость. Понятие «среды компьютерной преступности» охватывает широкий спектр факторов, начиная от физического рабочего пространства и заканчивая социальными и материальными условиями, которые влияют на поведение преступника. Эти элементы среды имеют решающее значение для формирования как мотивации, так и совершения киберпреступлений [28, с 10]. Глубокое понимание этих влияний необходимо для разработки более эффективных стратегий предотвращения и расследования киберпреступлений.

Факторы окружающей среды, влияющие на компьютерные преступления:

Объективные условия: они относятся к материальным аспектам окружающей среды жертвы, таким как:

- вид деятельности: это характер работы жертвы и ее роль в организации;
- форма собственности: это является ли жертва физическим или юридическим лицом, а также связанные с этим правовые последствия;
- доступность информации: это степень доступности информации жертвы;
- обеспечение ресурсами: это наличие материальных и человеческих ресурсов, необходимых для деятельности жертвы.

Субъективные условия: это внутренние, часто эксплуатационные факторы, в том числе:

- процедурные отклонения: это любые нарушения в том, как обрабатывается или управляется информация;
- эксплуатационные проблемы: это проблемы с обработкой и защитой компьютерных систем и информации;
- практики документирования: это степень интеграции ручных процессов с автоматизированными системами;

– контроль и надзор: это наличие или отсутствие мер надзора и межличностной динамики внутри организации.

Влияние на динамику преступности:

Взаимодействие этих факторов существенно влияет на различные аспекты компьютерного преступления:

– выбор жертвы: это как и почему конкретное лицо или организация выбираются в качестве цели;
– методы исполнения: это конкретные приемы и подходы, используемые для совершения преступления;
– участие сообщников: это были ли другие лица завербованы или вовлечены в планирование или совершение преступления;
– стратегии сокрытия: это методы, используемые для сокрытия улик и избежания обнаружения;
– более широкая преступная деятельность: это дополнительные незаконные действия, это связанные с основным компьютерным преступлением, такие как финансовые кражи.

Важность ситуационного анализа:

Анализ ситуационного контекста компьютерного преступления необходим для понимания того, как и почему произошло преступление. Изучая как объективные, так и субъективные факторы, следователи могут получить представление о:

– возможности для совершения преступлений: это как определенные условия могут способствовать или препятствовать преступной деятельности;
– преступное поведение: это как условия окружающей среды влияют на методы и мотивы преступников.

Всестороннее изучение этих факторов имеет жизненно важное значение для разработки эффективных стратегий расследования и превентивных мер. Понимание полного контекста, в котором происходят компьютерные преступления, позволяет правоохранительным органам лучше решать

проблемы, связанные с этими сложными преступлениями, и повышать безопасность компьютерных информационных систем.

В заключение следует отметить, что криминалистические характеристики субъективной стороны преступлений в сфере компьютерной информации являются неотъемлемой частью понимания и рассмотрения этих сложных правонарушений. В этой главе были исследованы основные элементы, которые вносят вклад в субъективное измерение компьютерных преступлений, подчеркивая роль мотивов, психологических состояний и поведенческих моделей в преступной деятельности.

Всесторонний анализ показывает, что субъективные аспекты компьютерных преступлений многогранны и тесно переплетены как с индивидуальными, так и с контекстуальными факторами. Ключевые элементы, такие как мотивы преступника от личной выгоды и политических планов до психологических условий играют решающую роль в формировании его действий и методов. Понимание этих мотивов не только помогает в профилировании и идентификации преступников, но и дает представление об их процессах принятия решений и конкретной тактике, которую они используют.

Влияние психологических состояний, таких как страсть или психическая нестабильность, подчеркивает необходимость тонкого подхода к расследованию компьютерных преступлений.

Глава 2 Криминалистическая характеристика объективной стороны преступлений в сфере компьютерной информации

2.1 Предмет и объект посягательства при совершении преступлений в сфере компьютерной информации

«Уголовно-правовая квалификация преступления состоит в установлении совпадения типичных обстоятельств конкретного общественно-опасного, противоправного деяния признакам, определенного в УК РФ состава преступления» [15, с. 55].

Понимание основных компонентов преступления имеет решающее значение в области уголовного правосудия, особенно при рассмотрении преступлений, связанных с компьютерной информацией. В этой главе рассматриваются основные элементы, определяющие эти преступления, с упором на объект и субъект преступных атак. Анализируя эти аспекты, мы можем лучше понять, как идентифицировать и отличать компьютерные преступления от других связанных с ними преступлений. Это имеет решающее значение не только для обеспечения соблюдения закона, но и для усиления мер кибербезопасности.

Всесторонний анализ любого преступления начинается с определения его объекта и субъекта. Объект относится к общественным отношениям и ценностям, которые нарушает преступление, в то время как субъект включает в себя субъектов, на которых направлено преступное деяние. После того, как эти компоненты установлены, мы можем перейти к изучению объективной стороны преступления, которая охватывает фактические элементы и обстоятельства, при которых было совершено преступление.

Для полного понимания объективной стороны компьютерных преступлений необходимо проанализировать конкретные элементы, составляющие неправомерный доступ к компьютерной информации. Согласно статье 9 Уголовного кодекса Российской Федерации, эти

преступления подпадают под более широкую категорию преступлений против общественной безопасности и общественного порядка. Такая классификация подчеркивает общественное воздействие таких преступлений, подчеркивая их потенциальную возможность нарушить не только частную жизнь личности, но и общественное доверие к цифровым системам.

При буквальном толковании закона объектом компьютерных преступлений являются общественные отношения, обеспечивающие безопасность и надлежащее функционирование компьютерных информационных систем. Эти отношения являются неотъемлемой частью поддержания целостности и надежности цифровой информации, что имеет решающее значение в условиях все более цифровизированного общества.

В зависимости от степени вреда, причиненного преступлением, может также присутствовать необязательный, необязательный дополнительный объект. Этот аспект допускает гибкость в юридической квалификации, гарантируя, что тяжесть преступления может быть адекватно рассмотрена на основе его воздействия.

Процедура определения объекта и субъекта преступления, а также анализ его объективной стороны являются основополагающими для установления четкой связи между преступным деянием и признаками, предусмотренными Уголовным кодексом Российской Федерации. Данный процесс имеет существенное значение для отграничения компьютерных преступлений от иных схожих правонарушений, обеспечения правильной юридической квалификации и адекватности мер наказания.

«Факт наличия факультативного объекта повышает степень общественной опасности данного преступления, что необходимо учитывать при назначении наказания виновному лицу» [10, с. 18].

Объект преступления относится к общественным отношениям и ценностям, которые нарушает преступление. Напротив, предмет преступления, особенно в случаях незаконного доступа к компьютерной информации, служит ключевым фактором для различения компьютерных

преступлений от других видов правонарушений. Это различие имеет жизненно важное значение для точной юридической классификации и эффективного применения закона.

Существует мнение ученых, что «предметом в данном случае будет являться именно ПК, как носитель информации, путеводитель в информационную систему» [16, с. 110].

Сторонники вышеупомянутой теории полагают, что несанкционированный доступ к ПК и его незаконное использование следует классифицировать как компьютерные преступления. Однако этот упрощенный подход широко расценивается как ошибочный. Большинство экспертов-юристов утверждают, что рассмотрение самого ПК в качестве субъекта смешивает компьютерные преступления с имущественными преступлениями, тем самым усложняя правовые различия.

Поэтому можно сделать верный вывод, что «предметом в указанном преступлении будет именно компьютерная информация, базы данных или информационные ресурсы, которые содержатся в материальном носители, которым и является ПК» [3, с. 65].

Когда преступник совершает противоправные действия, направленные на компьютерные системы, он ставит под угрозу безопасность и защиту конфиденциальной информации. Такие действия также нарушают нормальное функционирование персональных компьютеров и компьютерных сетей. Этот конкретный вид преступной деятельности относится к категории компьютерных преступлений из-за его прямого воздействия на информационные ресурсы и работу систем.

Объект компьютерного преступления охватывает общественные ценности и отношения, которым преступление угрожает. Напротив, субъект относится к непосредственной цели преступного деяния. В случае незаконного доступа к компьютерной информации субъектом обычно является сама информация, а не физический компьютер.

«Это логично, так как ЭВМ как техника, в отличии от информации овеществлена и материальна, имеет цены, а главное является именно вещью, причем чужой для преступника, что характерно для преступлений определенных 21 главой Особенной части УК РФ» [20, с. 273].

Похитить чужие средства можно и без карты, например, с помощью чужого «мобильного банка» или системы интернет-платежей, обманув владельца. Это кража, но, если при этом виновный незаконно не влиял на программное обеспечение серверов, компьютеров или сами сети. Это разъясняет п. 21 Постановления № 48 [25].

«Рассмотрение уголовного дела в суде первой инстанции в точном соответствии с установленным законом порядком, отвечающим критериям справедливого судебного разбирательства, служит надежной гарантией защиты прав и законных интересов лиц и организаций, потерпевших от преступлений, и защиты личности от незаконного и необоснованного обвинения, осуждения, ограничения ее прав и свобод» [26].

В одном случае суд первой инстанции не в полной мере учел представленные объяснения и квалифицировал действия А. Ербягина по пункту «ж» части 3 статьи 158 УК РФ, что касается «хищения с банковского счета, а равно в отношении электронных денежных средств». Ербягин использовал мобильный банкинг для перевода денежных средств с чужого счета на свой. Хотя точная сумма в судебных документах не разглашается, ущерб охарактеризован как «значительный». В результате Ербягин был приговорен по этой статье к двум годам лишения свободы.

Однако Красноярский краевой суд счел это наказание чрезмерно суровым, что отражено в определении № 22-993/2019. Рассмотрев апелляционную жалобу, суд установил, что преступление является «простым» крупным хищением, предусмотренным пунктом «в» части 2 статьи 158 УК РФ. Санкции по этой статье существенно мягче, чем по пункту «г» части 3. Суд подчеркнул, что хотя Ербягин и пользовался мобильным банкингом, но не вмешивался в работу программ, серверов и информационно-

телекоммуникационных сетей. В результате краевой суд снял более суровое обвинение и, учитывая иные смягчающие обстоятельства, сократил наказание до одного года исправительных работ с удержанием из заработной платы в размере 10%.

Напротив, дело Петра Звола, продавца в салоне сотовой связи «Мегафон», включало иную правовую трактовку в отношении несанкционированного доступа к компьютерным системам. Звол перерегистрировал абонентские счета и мошенническим путем перевел около 500 000 рублей из «МегаФона» путем манипулирования компьютерной базой данных лицевых счетов. Первоначально районный суд квалифицировал его действия как «мошенничество с использованием компьютерной информации» по части 1 статьи 159.6 УК, решив не добавлять дополнительное обвинение по части 3 статьи 272, которая касается «несанкционированного доступа к компьютерной информации с использованием служебного положения». Суд утверждал, что мошеннические действия Звола, направленные на хищение денег у «МегаФона», в достаточной степени охватываются более широким обвинением в мошенничестве.

Однако Самарский областной суд, ссылаясь на пункт 20 Постановления Пленума № 48, в котором даны указания по квалификации мошеннических действий, связанных с несанкционированным доступом к компьютерной информации или использованием вредоносных программ, постановил, что действия Звола следует также квалифицировать по статье 272 УК РФ. Поскольку он внес несанкционированные изменения в охраняемую законом информацию, дело было направлено на новое рассмотрение, о чем говорится в Постановлении № 226541.

«Может возникнуть проблема при квалификации, если предметом посягательства будет не только компьютерная информация, защищаемая законом, но и сам объект ЭВМ» [2, с. 129].

«Юридически охраняемая» информация относится к данным, защищенным российским законодательством. Это охватывает определенные

типы информации, которые по закону ограничены определенной группой лиц с особым правовым статусом. Такая информация часто касается национальной безопасности, государственной и общественной безопасности, а также жизненно важной деятельности отдельных граждан. Примерами могут служить данные об оружии, космосе и сведения, имеющие отношение к промышленному и сельскохозяйственному секторам страны.

«Юридически защищенная» информация относится к данным, которые защищены в соответствии с российским законодательством, ограничивающим доступ к ним лиц с определенными юридическими полномочиями. Эта категория информации обычно включает данные, имеющие решающее значение для национальной безопасности, общественной безопасности и основных общественных функций. Примерами таких данных являются информация, связанная с оружием, исследованием космоса и ключевыми промышленными и сельскохозяйственными секторами страны.

Доступ к юридически защищенной информации строго ограничен и регулируется законом. Он недоступен для широкой общественности, но ограничен лицами или организациями, имеющими необходимое юридическое разрешение. Этот правовой статус гарантирует, что только те, у кого есть соответствующий допуск, могут получить доступ к конфиденциальной информации, тем самым защищая ее от несанкционированного использования или раскрытия.

В сфере информационной безопасности значительная часть охраняемых законом данных принадлежит не частным лицам, а государству. К этой категории относится особо чувствительная информация, касающаяся военных операций, внешней политики, экономических стратегий, разведывательной, контрразведывательной и правоохранительной деятельности. Несанкционированное раскрытие таких данных представляет серьезную угрозу безопасности Российской Федерации, что подчеркивает необходимость защиты этой информации от возможных нарушений.

Хотя защита информации, связанной с государством, имеет решающее значение, не менее важно обеспечить безопасность коммерческих конфиденциальных данных. Хотя коммерческие секреты могут быть напрямую не связаны с национальной безопасностью, они имеют значительную экономическую ценность. Защита этих секретов жизненно важна для предотвращения промышленного шпионажа и сохранения конкурентного преимущества на рынке. Поэтому обе категории информации требуют строгих мер безопасности для предотвращения несанкционированного доступа и обеспечения их постоянной конфиденциальности.

«Это может быть информация, как коммерческая, так и содержащая служебную либо банковскую тайну» [5, с. 23].

Защита информации в правовых рамках имеет решающее значение для поддержания как государственной безопасности, так и личной неприкосновенности частной жизни. В России конкретные нормы, изложенные в Гражданском кодексе, Уголовном кодексе и Конституции, обеспечивают надлежащую защиту различных видов информации, тем самым защищая национальные интересы и личные права.

Правовой статус информации, находящейся под защитой государства, в России определяется положениями Гражданского кодекса и Уголовного кодекса Российской Федерации. К этой категории часто относятся материалы, защищенные авторским правом, закрепленным в статье 44 Конституции Российской Федерации. Нарушения этих прав рассматриваются в соответствии со статьей 272 Уголовного кодекса, которая предусматривает наказание за несанкционированный доступ к компьютерной информации.

Хотя защищаемая государством информация имеет решающее значение, защита частной информации, принадлежащей отдельным лицам, также требует детального рассмотрения. Конституция Российской Федерации, основной закон страны, прямо защищает личную неприкосновенность.

Статья 23 Конституции гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Еще больше усиливая эти меры защиты, статья 24 Конституции запрещает сбор, хранение, использование и распространение личной информации без согласия лица. Для обеспечения эффективности этих конституционных гарантий Уголовный кодекс устанавливает наказания за нарушение неприкосновенности частной жизни, включая незаконный перехват корреспонденции и другие нарушения права на неприкосновенность частной жизни. Эти правовые меры имеют решающее значение для сохранения конфиденциальности и безопасности как защищаемой государством, так и личной информации в Российской Федерации.

Уголовное право в России охватывает широкий спектр личной информации, гарантируя, что любые данные, касающиеся личной жизни человека, защищены от несанкционированного сбора и распространения. Это включает в себя семейные тайны, с конкретными положениями в Уголовном кодексе, такими как статья 155, которая карает разглашение тайны усыновления, тем самым защищая индивидуальную семейную тайну.

Правовая защита личной и конфиденциальной информации является важнейшим аспектом поддержания конфиденциальности и безопасности в обществе. Эта защита закреплена в различных законах и нормативных актах, гарантирующих защиту конфиденциальных данных от несанкционированного доступа и раскрытия. В России Гражданский кодекс, Уголовный кодекс и отдельные федеральные законы обеспечивают всеобъемлющую основу для защиты такой информации, уравновешивая необходимость конфиденциальности с требованиями государственной безопасности и общественного порядка.

«Семейная (личная) информация, имеющая статус конфиденциальности это и семейное положение, состояние здоровья, информация о денежном состоянии, счетах и вкладах в банках и т.д.» [19, с. 343].

Закон в России налагает строгие запреты на раскрытие конфиденциальной информации, охватывающей личные, частные и семейные данные. Например, информация об усыновлении надежно защищена; даже ЗАГС не может выдать дубликат свидетельства об усыновлении усыновленному. Этот документ доступен только усыновителям, что подчеркивает высокий уровень сохраняемой конфиденциальности.

Государственные и муниципальные органы также ограничены в запрашивании такой конфиденциальной информации, поскольку это нарушит права на неприкосновенность частной жизни и семьи отдельных лиц. Информация о частной жизни, религиозных убеждениях и мировоззрении человека считается защищенной, что отражает ее классификацию как личной тайны. Однако не вся личная информация подпадает под «защищенную законом информацию»; определение такого статуса зависит от оценки судом конкретных обстоятельств дела и тяжести потенциального вреда для жертвы.

Защита персональных данных, особенно в сфере правоохранительной деятельности и разведки, является важнейшим аспектом как национальной безопасности, так и прав на неприкосновенность частной жизни. Федеральный закон «Об оперативно-розыскной деятельности», принятый в 1995 году, определяет правовую основу управления такой информацией в России. Этот закон гарантирует конфиденциальность лиц, участвующих в следственных операциях, включая тайных агентов и осведомителей. Несанкционированное раскрытие этой конфиденциальной информации влечет за собой уголовное преследование.

В соответствии с этим законодательством статья 272 Уголовного кодекса Российской Федерации относит нематериальные активы, такие как охраняемая законом компьютерная информация, к объектам преступной деятельности. К ним относятся конфиденциальные персональные данные, служебная тайна, коммерческая и банковская информация, государственная

тайна, интеллектуальная собственность. Напротив, несанкционированный доступ к общедоступной компьютерной информации, которая не охраняется законом и предназначена для всеобщего доступа, не подпадает под уголовную ответственность, предусмотренную статьей 272. Различие между охраняемыми и незащищенными данными имеет решающее значение для определения правовых последствий доступа к такой информации.

Тщательный анализ субъекта и объекта преступления необходим для точной классификации и понимания правонарушения. Преступления, связанные с компьютерной информацией, которые не оказывают прямого влияния на безопасность таких данных или нормальную работу компьютерных систем, не подпадают под действие анализируемого правового положения. Неправильное толкование взаимосвязи субъекта и объекта может привести к ошибкам в классификации преступлений, что может подорвать принципы законности и справедливости в уголовном праве.

В заключение следует отметить, что защита конфиденциальной и юридически защищенной информации является краеугольным камнем законов о конфиденциальности и безопасности в России. Строгие правила и правовые рамки гарантируют, что персональные, частные и конфиденциальные данные защищены от несанкционированного доступа и раскрытия. Понимание юридических нюансов такой защиты имеет решающее значение для точной классификации преступлений и соблюдения принципов справедливости и законности.

2.2 Способы совершения и сокрытия преступлений в сфере компьютерной информации

Объективная сторона преступления, предусмотренного частью 1 статьи 272 УК РФ, заключается в неправомерном доступе к охраняемой законом компьютерной информации. Уголовно-наказуемым деяние становится, если оно приводит к уничтожению, блокированию, изменению,

копированию данных либо нарушению работы ЭВМ, системы ЭВМ или сети ЭВМ. Для привлечения к ответственности по данной статье необходимо установить факт совершения противоправного действия. Это действие должно быть умышленным и инициативным, в отличие от иных форм преступного поведения, которые могут быть сопряжены с бездействием.

Как говорилось ранее «для привлечения к ответственности необходимо наличие всего состава преступления, согласно норме УК РФ» [23, с. 42].

Статья 272 Уголовного кодекса специально нацелена на лиц, которые незаконно получают доступ к защищенной информации или ресурсам. Ключевым аспектом этого преступления является незаконный характер доступа к таким защищенным данным. Хотя метод, используемый для получения доступа, не меняет фундаментальной юридической классификации преступления, различные используемые методы требуют тщательного рассмотрения из-за их влияния на правовую оценку.

Один из известных методов несанкционированного доступа включает применение насилия или угроз. Этот подход особенно актуален, когда у преступника нет технических знаний, необходимых для прямого доступа. В таких случаях преступник может принудить владельца информации или его законного представителя, обладающего необходимыми навыками и знаниями, совершить преступление от его имени.

Проблема в том, что «диспозиция данного состава преступления не охватывает своим содержанием указанный способ его совершения. На основании этого квалификация преступления только лишь по ст. 272 УК РФ будет некорректной, так как посягательство в данном случае не только на общественные отношения, связанные с компьютерной информацией, но и затрагивает безопасность жизни и здоровья личности и человека. В вышеуказанном примере суду необходимо будет проводить квалификацию содеянного преступления в сфере компьютерной информации по совокупности с преступлением против личности» [24, с. 105].

Сложный юридический вопрос возникает при рассмотрении ответственности лиц, принуждаемых к совершению противоправных действий. Например, если исполнитель принуждает третье лицо, будь то потерпевший или его представитель, к совершению противоправных действий под принуждением, основная юридическая ответственность обычно возлагается на исполнителя. Согласно статье 39 Уголовного кодекса Российской Федерации, если принуждаемое лицо действовало в состоянии крайней необходимости, основную ответственность за преступление несет принуждающий.

Однако если лицо не находилось в состоянии крайней необходимости, вступают в действие правовые принципы соучастия. Это означает, что как принуждаемое лицо, так и принуждающий могут нести совместную ответственность в зависимости от конкретных обстоятельств. Для точного определения правового статуса принуждаемой стороны может потребоваться тщательный анализ ситуации и связанных с ней преступлений.

Понимание правил соучастия, определенных Уголовным кодексом, в таких случаях имеет важное значение. Лицо считается соучастником только тогда, когда оно действовало не в состоянии крайней необходимости. Например, если кому-либо угрожают причинением незначительного вреда или нанесением телесных повреждений, а степень угрозы не оправдывает противоправные действия, суд может привлечь его к ответственности как соучастника. Согласно статьям 272 и 119 Уголовного кодекса Российской Федерации, если лицо принуждает оператора ЭВМ к незаконному доступу к защищенной информации под угрозой убийства, принуждающий несет полную ответственность за преступление.

Уголовный кодекс Российской Федерации не содержит четкого определения квалифицированного персонала для работы с компьютерной информацией и системами. Важно отметить, что неправомерный доступ к компьютерной информации не всегда является самостоятельным преступлением. Часто он служит средством достижения другой преступной

цели. Например, преступник или преступная группа могут использовать дополнительные хакерские программы для получения экономической выгоды, делая несанкционированный доступ методом совершения имущественных преступлений.

Из вышесказанного делаем вывод, что «данный преступный поступок необходимо будет судом квалифицировать по совокупности данных преступлений, предусмотренных разными главами УК РФ» [17, с. 9].

Персональные компьютеры и электронные устройства используются не только для нацеливания на защищенную компьютерную информацию, но и как инструменты в преступлениях против собственности. Такое двойное использование технологий усложняет задачу для сотрудников правоохранительных органов, которым необходимо точно определить ключевые элементы преступления, такие как его место и время.

Значительная проблема возникает, поскольку место преступления часто отличается от того, где ощущаются пагубные последствия. Благодаря достижениям в области хакерства и компьютерных технологий преступники могут совершать преступления из одной страны, в то время как жертвы и последствия находятся в совершенно разных регионах.

Действующее законодательство, как определено в статье 9 Уголовного кодекса Российской Федерации, определяет, что временем преступления является исключительно момент совершения преступного действия или бездействия. Последующее время наступления последствий, хотя и имеет практическое значение, не влияет на юридическое определение преступления.

Не все страны признают конкретные киберпреступления, обсуждаемые здесь. Если преступники используют эти правовые пробелы, они должны помнить, что ответственность будет применяться в соответствии с законами государства, где ощущались последствия преступления. Это особенно актуально, когда преступление затрагивает отдельных лиц или интересы в стране, которая признает такие элементы в своей правовой системе.

Важнейшим аспектом преследования преступлений против компьютерной информации является установление причинно-следственной связи между преступным деянием и его последствиями. Эта связь является обязательным признаком объективной стороны таких преступлений, согласно действующему уголовному законодательству. Понимание этой связи имеет жизненно важное значение для обеспечения точной классификации и преследования киберпреступлений.

Незаконное копирование информации подразумевает перенос данных, защищенных законом, с одного электронного носителя на другой, например, на USB-накопитель. Это действие является явным нарушением, когда скопированная информация предназначена для неправомерного использования или распространения без разрешения. Это представляет собой прямое нарушение мер безопасности, принятых для защиты конфиденциальных данных.

Уничтожение защищенной информации подразумевает полное стирание данных, так что они больше не существуют ни в какой форме. Этот тип преступного деяния может иметь серьезные последствия, особенно если данные имеют решающее значение для национальной безопасности или функционирования ключевых инфраструктур. Блокирование информации, с другой стороны, подразумевает, что данные становятся недоступными с помощью технических средств, тем самым препятствуя их законному использованию. Оба действия нарушают целостность и доступность важной информации.

Незаконное изменение относится к изменению юридически защищенной информации таким образом, что изменяется ее форма, но не ее фундаментальная сущность. Такие изменения могут быть едва заметными, но значительными, влияющими на точность и надежность данных. Этот тип преступного деяния может ввести в заблуждение пользователей и системы, что приведет к ошибочным решениям и действиям, основанным на измененной информации.

Не все случаи взаимодействия с защищенной информацией представляют собой незаконное копирование. Например, простое получение доступа или ознакомление с информацией без переноса ее на другой носитель не подпадает под незаконное копирование. Такие действия могут иметь место в ходе подготовки к другому преступлению, когда полученная информация служит предвестником или средством для облегчения последующего незаконного действия.

Можно сделать вывод, вредными последствиями являются:

- «нарушение работы компьютерной техники (персональный компьютер, система ЭВМ, сеть ЭВМ и т.д.);
- вывод ЭВМ путём модификации или иного нарушения компьютерной информации;
- нарушение целой сети персональных компьютеров путём незаконной модификации файлов операционной системы ЭВМ. Именно наступление хоть одного из данных вредных последствий и является основанием для утверждения об окончании преступления против компьютерной информации. На данный вид преступлений распространяются нормы уголовного законодательства о покушении (ст. 30 УК РФ) [32], данное условие применяется для случаев, когда незаконное действие в отношении информации было совершено, но было пресечено третьей стороной до наступления вышеуказанных последствий» [4, с. 80].

«Вернёмся к вопросу, который мы поставили перед собой в рамках данного исследования, к вопросу причинно-следственной связи между действием (так как преступное деяние в данном случае не может быть выражено в бездействии) преступника и негативными последствиями данного проступка» [30, с. 217].

В контексте российского уголовного права причинно-следственная связь определяется как прямая связь, при которой определенная причина влечет за собой определенное следствие. Для преступлений в сфере

компьютерной информации это означает, что неправомерный доступ к защищаемым данным должен непосредственно приводить к неблагоприятным последствиям, таким как копирование, уничтожение или изменение, как указано в статье 272 УК РФ.

Без этой прямой связи между противоправным деянием и его последствиями подрывается правовая основа для преследования. Таким образом, установление этой связи имеет решающее значение для определения наличия преступления и обеспечения того, чтобы судебный процесс соответствовал правовым нормам. Любое отклонение от этого требования поставило бы под угрозу целостность правовой системы.

Понимание методов, используемых для совершения компьютерных преступлений, помогает в классификации и эффективном противодействии этим правонарушениям. Основные методы включают:

- прямой доступ к компьютерной информации, этот метод подразумевает физический доступ к компьютерным носителям информации, например, прямое взаимодействие с компьютером или его устройствами хранения. Часто он требует от преступника физического взаимодействия с оборудованием, что может включать в себя кражу или вмешательство в работу систем безопасности. Следовательно, доказательства в таких случаях могут включать признаки взлома, повреждения охранной сигнализации или другие физические следы;
- удаленный или телекоммуникационный доступ происходит, когда преступник получает несанкционированный доступ к компьютерной информации на расстоянии. Это может быть достигнуто с помощью промежуточных каналов связи или других компьютеров. Такие методы, как развертывание вредоносного программного обеспечения, вирусов или инструментов, предназначенных для взлома паролей, обычно используются в удаленных атаках. Эти методы обычно включают доступ к целевой информации через сеть

или через Интернет, минуя необходимость физического взаимодействия с исходным носителем информации;

- подделка данных подразумевает изменение или манипулирование информацией с целью введения в заблуждение или контроля использования данных. Этот метод может включать изменение данных или структуры их носителя для воздействия на их целостность или функциональность. Такие изменения могут использоваться для обмана пользователей или систем, часто для содействия дальнейшей преступной деятельности;
- создание и развертывание вредоносного ПО - еще один метод, используемый для нарушения, уничтожения или блокировки доступа к компьютерной информации. Это может включать создание вирусов или другого вредоносного ПО, предназначенного для повреждения или порчи данных. Кроме того, несанкционированное распространение защищенных данных или носителей может происходить, когда преступники незаконно делятся или распространяют конфиденциальную информацию.

Методы, используемые в компьютерных преступлениях, могут быть сложными и многогранными, часто включающими как прямые, так и дистанционные методы. Анализируя конкретные используемые подходы, правоохранительные органы могут лучше решать проблемы, связанные с компьютерными преступлениями, и обеспечивать отправление правосудия в рамках установленных правовых принципов.

«Комплексные методы, как уже говорилось, состоят из нескольких методов, причём один из них будет являться основным, то есть доминирующий метод, более подходящий и второстепенный необходимый для выполнения отдельных целей и задач в рамках компьютерного преступления» [18, с. 198].

Методы, выбранные для совершения компьютерных преступлений, во многом определяются уровнем специальных знаний и технической

подготовки преступника. Кроме того, цели и мотивы преступления играют важную роль в формировании используемых методов. Например, опытный хакер с передовыми навыками может использовать сложные инструменты, тогда как менее опытный человек может прибегнуть к более элементарным методам.

В заключение следует отметить, что криминалистические характеристики объективной стороны компьютерных преступлений выявляют сложное взаимодействие между методами, используемыми преступниками, и характером совершенных преступлений. Объективная сторона таких преступлений охватывает ряд незаконных действий, включая несанкционированный доступ, кражу данных, уничтожение и изменение компьютерной информации. Понимание этих действий требует тонкого подхода, который учитывает используемые технические методы, конкретный тип целевой информации и итоговое воздействие как на жертв, так и на задействованные системы.

Изучение криминалистических характеристик в этой области имеет решающее значение по нескольким причинам. Оно помогает очертить конкретные действия, составляющие преступление, тем самым устанавливая четкую связь между поведением преступника и полученным вредом. Эта ясность необходима для точного определения элементов преступления, что, в свою очередь, дает информацию для правовой оценки и соответствующего судебного реагирования.

Анализируя используемые методы и их воздействие, эксперты-криминалисты могут лучше отслеживать действия преступников, восстанавливать последовательность событий и в конечном итоге способствовать обеспечению правосудия и повышению кибербезопасности.

В целом, криминалистические характеристики объективной стороны компьютерных преступлений подчеркивают необходимость постоянной адаптации следственных и правовых рамок для того, чтобы идти в ногу с развивающимися технологическими угрозами.

Глава 3 Особенности и методы расследования преступлений в сфере компьютерной информации

3.1 Обстоятельства, подлежащие установлению и доказыванию

В сфере современного уголовного правосудия проблема незаконного доступа к компьютерной информации стала особенно актуальной и динамичной проблемой. Этот тип преступлений, хотя и является относительно новым, быстро приобретает известность благодаря бурно развивающимся достижениям в области компьютерных технологий и ИТ-образования. Эти разработки не только способствуют инновационным методам совершения имущественных преступлений, но и распространяются на более сложные нарушения, такие как нарушение авторских прав и нарушение национальной безопасности.

Существенным аспектом угрозы, которую представляют собой компьютерные преступления, является их неотъемлемая способность выходить за рамки национальных границ. Глобальный охват этих преступлений подчеркивает неадекватность существующих правовых и теоретических рамок, которые с трудом поспевают за быстрым развитием технологий. Действующий Уголовный кодекс Российской Федерации, вступивший в силу с 1 января 1997 года, ознаменовал собой кардинальный сдвиг, расширив правовую защиту за пределы государственной тайны и включив в нее индивидуальные права на неприкосновенность частной жизни и информационную безопасность. Однако сложность этих преступлений и техническая экспертиза, необходимая для их расследования, представляют собой существенные проблемы для правоохранительных органов.

Отсутствие специализированных знаний в области ИТ у следователей усложняет процесс раскрытия преступлений и может поставить под угрозу справедливость и законность судебного разбирательства. Эти технические проблемы усугубляются относительной новизной законодательства о

компьютерных преступлениях, которое начало решать эти проблемы комплексно только с принятием действующего Уголовного кодекса.

Ранее мы провели глубокий анализ субъективных и объективных элементов, составляющих компьютерные преступления. В этом исследовании были выяснены условия, при которых возникает уголовная ответственность, и определены конкретные компоненты, изложенные в уголовном праве. Установление факта совершения преступления требует тщательного расследования всех соответствующих обстоятельств. Первоочередной целью любого расследования является определение того, действительно ли имело место противоправное деяние. Если выясняется, что инцидент является результатом технических неисправностей или внешних факторов, а не преднамеренного преступного поведения, он не может быть классифицирован как преступление. Следовательно, начальный этап следственного процесса сосредоточен на проверке того, имела ли место противоправная деятельность с использованием компьютерной информации.

После подтверждения факта совершения преступления фокус переключается на определение характера затронутой информации. Это подразумевает разграничение информации, которая находится в открытом доступе, и информации, защищенной законом. Классификация информации как защищенной законом или иной определяет применимость конкретных федеральных законов и влияет на юридическое рассмотрение дела.

Можно сказать, что сложность расследования компьютерных преступлений требует глубокого понимания как технических аспектов, так и соответствующих правовых рамок. Поскольку технологии продолжают развиваться, то же самое должны делать методы расследования и правовые положения для эффективного устранения и смягчения этих новых угроз.

Следователи должны начать с анализа того, как представлена информация, вовлеченная в киберпреступление, сосредоточившись как на ее качественных, так и количественных аспектах. Это включает в себя изучение конкретных характеристик компьютерных носителей информации,

вовлеченных в преступление. Понимание этих деталей имеет жизненно важное значение для оценки характера данных и потенциальных последствий их компрометации.

Кроме того, статус и содержание информации, хранящейся на затронутых носителях, должны быть тщательно проверены. Этот процесс включает определение юридической классификации данных и их релевантности преступлению. Правильная классификация помогает обеспечить применение правильных правовых положений и проясняет масштаб преступной деятельности.

Для расследования важно учитывать время и место преступления в соответствии со стандартами уголовного права. Как упоминалось ранее, эти факторы являются основополагающими для установления контекста преступления и обеспечения того, чтобы судебный процесс точно отражал временные и пространственные реалии преступления.

Для каждого конкретного компьютерного преступления важно определить метод совершения. Это включает анализ того, как было совершено преступление, включая технику, использованную для доступа к информации, обхода мер безопасности и совершения преступного деяния. Понимание этих методов помогает выявлять уязвимости и улучшать профилактические меры.

Следователи также должны изучить процедуры и методы, используемые для защиты информации. Это включает изучение действующих мер безопасности и определение причины нарушения безопасности. Определение того, как была нарушена безопасность, является ключом к пониманию преступления и предотвращению будущих инцидентов.

Кроме того, расследование должно прояснить технические детали, связанные с преступлением, такие как любые коды, шифры или использованные инструменты взлома. Эти детали имеют решающее значение для понимания сложности атаки и для судебно-медицинского анализа.

Ключевым элементом расследования киберпреступлений является оценка того, была ли скомпрометирована конфиденциальная информация.

Этот процесс включает в себя проверку того, были ли инсайдеры, такие как сотрудники или лица со специальными знаниями, вовлечены в нарушение. Определение того, сыграли ли должностные лица, имеющие доступ к конфиденциальным данным, свою роль, имеет решающее значение, поскольку их участие может существенно повлиять как на расследование, так и на последующее судебное преследование.

Правовые рамки, такие как Постановление Пленума № 51, определяют различия между мошенничеством, связанным со злоупотреблением служебным положением, и другими видами преступной деятельности. Мошенничество может иметь место, когда лица используют свое официальное положение или административную роль для причинения вреда. Признание этих различий важно для точной классификации и рассмотрения преступления в рамках правовой системы.

Например, Оренбургский областной суд подчеркнул необходимость четкого определения преступных деяний в деле Игоря Перепелкина. После детального рассмотрения подсудимый смог добиться смягчения приговора, что продемонстрировало важность точной юридической квалификации для достижения справедливых результатов.

«Районный суд приговорил его к 2,5 годам в колонии общего режима и штрафам в общей сумме на 750000 руб. Перепелкина признали виновным в уклонении от уплаты налогов (ч. 1 ст. 199 УК) и покушении на мошенничество в особо крупном размере с использованием своего служебного положения (ч. 3 ст. 30, ч. 4 ст. 159 УК).

Как установило следствие, фактический руководитель ООО оформлял фиктивные поставки и пытался возместить из бюджета более 3 млн руб. НДС.

Первая инстанция решила, что Перепелкин совершил мошенничество с использованием служебного положения, потому что он распорядился учредить эту фирму и фактически управлял ею (бизнес был оформлен на родственницу лишь номинально).

Иного мнения оказался Оренбургский областной суд. Он применил более формальный подход. По документам осужденный в компании никто и никаких полномочий не имеет. «Суд не указал в приговоре, какими служебными полномочиями был наделен Перепелкин и какие он использовал при совершении преступления», – излагается в определении № 22-680/2019. Придя к таким выводам, апелляция уменьшила штраф на 250000 рублей» [21].

При расследовании компьютерных преступлений определение размера материального ущерба имеет решающее значение. Такая оценка должна охватывать несколько факторов:

Во-первых, количественная оценка материального ущерба.

Расчет материального ущерба выходит за рамки оценки стоимости самой скомпрометированной информации. Он включает в себя стоимость, связанную со следующими элементами:

- защищенная информация: внутренняя ценность данных, являющихся объектом преступления;
- системы безопасности: расходы на системы и меры, реализуемые для защиты информации;
- носители информации: стоимость оборудования, используемого для хранения скомпрометированных данных;
- упущенная выгода: финансовые последствия, возникающие в результате невозможности доступа к информации или ее эффективного использования.

Помимо материального ущерба, важно оценить любой нематериальный ущерб. К ним могут относиться репутационный ущерб, потеря доверия клиентов или другие нематериальные последствия. Понимание того, кто понес эти убытки и как их можно компенсировать, имеет важное значение для всестороннего расследования.

Во-вторых, определение квалифицирующих признаков преступления.

Правоохранительные органы должны определить, содержит ли преступление какие-либо из следующих квалифицирующих характеристик:

- групповая деятельность: было ли преступление совершено группой лиц, действующих сообща, или организованной преступной группой;
- злоупотребление полномочиями: было ли преступление совершено лицом с использованием своего служебного положения;
- доступ к системам: было ли преступление совершено лицом, имеющим санкционированный доступ к компьютеру, компьютерной системе или сети;
- халатность и последствия: привело ли преступление к значительному ущербу из-за халатности, например, к потере критически важных данных, системным сбоям, влияющим на основные технологические процессы, или несчастным случаям, повлекшим за собой человеческие травмы или катастрофы.

В-третьих, анализ деталей предмета.

Расследование должно быть сосредоточено на сборе подробной информации о подозреваемых, включая:

- персональные данные: такие данные, как имена, звания, семейное положение и другие личные аспекты;
- криминальное прошлое: любые предыдущие уголовные деяния или судимости, имеющие отношение к делу;
- физические характеристики: такие характеристики, как рост, отличительные физические черты, отпечатки пальцев, группа крови и общий внешний вид, включая стиль одежды и опознавательные знаки.

В-четвертых, оценка психологических и умственных качеств

Понимание психологического и ментального профиля подозреваемых имеет решающее значение. Это включает оценку:

- знания и навыки: Техническая компетентность и профессионализм подозреваемого в соответствующих областях;

– самооценка и тенденции: понимание своего самовосприятия, склонностей и потенциальных фобий.

В-пятых, расследование сообщников и организационной структуры

Если в преступлении участвует группа лиц, необходимо провести расследование:

– динамика группы: формирование, устойчивость и продолжительность деятельности организованной преступной группы;
– экономическая мотивация: была ли группа создана с целью получения экономической выгоды;
– распределение ролей: как распределяются роли и обязанности внутри группы;
– управление и дисциплина: структура руководства, методы мотивации, методы наказания и распределение ресурсов, включая финансовые, транспортные и технические активы.

Тщательное изучение материального ущерба, характеристик преступления и профилей подозреваемых имеет важное значение для всестороннего расследования компьютерных преступлений. Понимание этих элементов не только помогает раскрыть преступление, но и предотвратить будущие инциденты и обеспечить справедливость.

В сфере уголовного процесса, особенно связанных с коррупцией и киберпреступностью, решающее значение имеет тщательный и методичный подход. Следователи должны рассмотреть несколько ключевых элементов, чтобы раскрыть правду и обеспечить справедливость. Этот процесс включает не только проверку потенциальных связей между подозреваемым и правоохранительными органами или влиятельными лицами, но и установление объективных аспектов преступления, включая мотивы и цели преступника.

Важнейшим шагом в любом расследовании является определение того, есть ли у подозреваемого какие-либо связи с правоохранительными органами,

службами безопасности или влиятельными лицами, которые могли бы выступать в качестве покровителей. Выявление этих связей может дать представление о возможных мотивах и масштабах преступления.

Одновременно следователи должны установить элементы объективной стороны преступления. Это включает в себя понимание цели и мотивов преступной деятельности. Необходимо собрать исчерпывающую информацию о жертве, будь то физическое или юридическое лицо:

Для юридического лица:

- имя и адрес;
- вид собственности и хозяйственная деятельность;
- данные о руководителе(ях) и главном бухгалтере;
- информация о лице, ответственном за обработку и защиту компьютерной информации или носителей информации, затронутых преступлением.

Для частного лица:

- личные данные, такие как физический и психологический профиль;
- внешний вид и связи;
- профессиональный и социальный опыт.

Установление виновности подозреваемого в соответствии с конкретными положениями Уголовного кодекса Российской Федерации имеет существенное значение. В случае, когда виновный неизвестен, расследование должно быть расширено за счет:

- подробности аналогичных прошлых преступлений;
- информация о лицах, причастных к этим преступлениям;
- записи о любых нарушениях должностных инструкций или других соответствующих факторов.

Кроме того, необходимо выявить и оценить недовольных сотрудников в организации-жертве. Это включает отслеживание их местонахождения во время преступления.

Расследование включает в себя совокупность следственных действий, оперативно-розыскных мероприятий и стратегического планирования. Эти элементы, а также их реализация будут подробно рассмотрены в следующем разделе работы.

3.2 Особенности производства некоторых следственных действий при расследовании преступлений в сфере компьютерной информации

В системе уголовного правосудия возбуждение уголовного дела знаменует начало этапа предварительного расследования. На этом критическом этапе сотрудники правоохранительных органов и следователи тщательно изучают обстоятельства преступления. Основная цель этого этапа — раскрыть подробности преступления, установить все соответствующие факты и привлечь виновных к ответственности в соответствии с законом.

- предварительное расследование преследует несколько основных целей;
- детализация преступления: расследование направлено на раскрытие всех аспектов совершенного преступления, чтобы не оставить камня на камне;
- формирование уголовного дела: выводы, полученные на этом этапе, объединяются в комплексное уголовное дело, которое затем направляется в суд для дальнейшего разбирательства;
- выявление причин и условий: ещё одной важной задачей является выявление основных причин и условий, способствовавших совершению преступления, с целью предотвращения подобных преступлений в будущем.

Предварительное следствие может осуществляться как следователями, так и дознавателями в зависимости от объема их полномочий. Согласно процессуальному законодательству, дела могут быть переданы следственным

органам по решению суда или прокурора, даже если они изначально относились к подследственности дознавателя.

Важнейшим компонентом следственного процесса является строгое соблюдение правовых протоколов на каждом этапе, включая подготовку, исполнение и документирование. Соблюдение этих правовых стандартов имеет жизненно важное значение для гарантии того, что результаты следственных действий являются действительными и допустимыми в суде.

Одной из важнейших следственных процедур является допрос потерпевших и свидетелей. Этот процесс, регламентируемый Уголовно-процессуальным кодексом Российской Федерации, направлен на сбор необходимой информации, которая может оказать существенную помощь в расследовании.

Каждое следственное действие, включая допрос, играет важную роль в построении надежного дела и содействует общей эффективности процесса уголовного правосудия.

Обычно допросы проводятся на месте предварительного расследования. Однако при определенных условиях, таких как медицинские или материально-технические ограничения, допросы могут проводиться по месту жительства или в лечебном учреждении субъекта.

Повестка используется для вызова лиц на допрос. Этот документ либо вручается лично и подписывается, либо отправляется по каналам связи. Если допрашиваемому лицу меньше 16 лет, повестка направляется его законным представителям.

Допросы регламентируются строгими временными рамками: они не могут превышать восьми часов в день, с обязательными часовыми перерывами после первых четырех часов. Для обеспечения справедливости следователь или допрашивающий должен предъявить свои полномочия и разъяснить законные права и обязанности допрашиваемого.

Допросы должны проводиться законно, без принуждения и наводящих вопросов. Для обвиняемого допрос начинается с вопроса о его признании

вины - признают ли они себя виновными - а затем переходит к допросу о деталях обвинений.

На ранних стадиях расследования преступлений, особенно тех, которые связаны с цифровыми доказательствами, осмотры и обыски имеют решающее значение. При изъятии предметов важно документировать их размещение относительно других предметов на месте преступления, чтобы точно реконструировать события.

Проблемы часто возникают при изъятии электронных устройств. Преступники могут применять меры по уничтожению доказательств, например, писать программы, удаляющие информацию, или использовать пароли для защиты данных. Поэтому эффективное изъятие и сохранение электронных доказательств требуют тщательного планирования и выполнения.

Исследование цифровых доказательств включает в себя различные криминалистические методы для обнаружения соответствующей информации. Первичные криминалистические анализы в таких случаях включают:

- судебная экспертиза оборудования и компьютеров: включает в себя проверку физических компонентов вычислительных устройств;
- криминалистическая экспертиза программного обеспечения: основное внимание уделяется анализу программных приложений и их взаимодействий;
- криминалистическая экспертиза информации: подразумевает поиск, обнаружение и оценку данных, созданных пользователем или программой;
- судебная компьютерная и сетевая экспертиза: изучает сетевые технологии и их функции в компьютерных системах.

Помимо этих специализированных методов судебной экспертизы, стандартный сбор вещественных доказательств, включая снятие отпечатков

пальцев, по-прежнему имеет решающее значение на протяжении всего расследования.

Следственный эксперимент - еще один важный процессуальный инструмент, используемый для проверки теорий в контролируемых условиях. Этот экспериментальный подход помогает подтвердить гипотезы о преступлении и дает практическое представление о том, как было совершено преступление.

Можно сказать, что соблюдение процессуальных норм и применение ряда методов расследования имеют важное значение для эффективного раскрытия преступлений и обеспечения правосудия. Каждый шаг, от допроса до обработки цифровых доказательств, играет важную роль в общем успехе расследования.

Инициатором данного действия могут быть многие участники уголовного процесса по делу.

«Целью данного следственного действия является проверка предположений, возникающих в процессе следствия, а также получение дополнительной информации, к примеру, об умениях и навыках подозреваемого, что необходимо для законного установления вины данного участника уголовного процесса» [11, с. 410].

В области уголовных расследований, особенно связанных с цифровыми преступлениями, крайне важно придерживаться определенных протоколов для обеспечения целостности и справедливости процесса. Одним из таких следственных действий является следственный эксперимент, который играет решающую роль в проверке обстоятельств преступления. Этот этап требует строгого соблюдения правовых норм, чтобы не ставить под угрозу достоинство всех участников и обеспечить точные и беспристрастные результаты.

Следственный эксперимент должен соответствовать нескольким обязательным условиям:

- уважение достоинства: процесс должен уважать честь и достоинство всех участников, включая обвиняемых, подозреваемых, свидетелей и потерпевших;
- присутствие свидетелей: Свидетели, включая законных представителей и защитников, должны присутствовать по мере необходимости;
- соблюдение протокола: согласно Уголовно-процессуальному кодексу Российской Федерации, «каждый этап следственного эксперимента тщательно документируется в протоколе, в котором фиксируются все процессуальные детали» [31].

В ходе следственного эксперимента крайне важно оценить потенциальные неблагоприятные последствия, которые могут возникнуть из-за любых процессуальных ошибок. В идеале эксперимент должен использовать копии рассматриваемых данных и, по возможности, проводиться на том же компьютере или в той же системе, где произошли нарушения. Такой подход помогает точно воспроизвести условия предполагаемого преступления.

Согласно статье 47 Уголовно-процессуального кодекса Российской Федерации, лицо официально становится обвиняемым с момента вынесения постановления о привлечении его в качестве обвиняемого. До предъявления обвинения лицо может быть признано подозреваемым, если оно задержано в соответствии со статьями 91 и 92, к нему применена мера пресечения в соответствии со статьей 100 или сообщено о подозрении в соответствии со статьей 223.1.

При допросе подозреваемого в делах, связанных с компьютерными преступлениями, крайне важно оценить его технические навыки работы с компьютерами и определить происхождение этих навыков. Следователи должны определить:

- сведения о занятости: должностные обязанности подозреваемого и необходимость использования компьютера в его должности;

- доступ и использование: информация о доступе подозреваемого к определенным программам и его оперативной деятельности, связанной с компьютерной информацией;
- доступ в Интернет и безопасность: имеет ли подозреваемый доступ в Интернет, а также располагает ли он паролями или кодами безопасности, имеющими отношение к его работе.

Хотя может показаться, что идентификация подозреваемого проще, если преступление связано со сложными методами и специальными знаниями, это не всегда так. Профессиональные хакеры с передовыми навыками могут намеренно подставлять других, чтобы ввести следствие в заблуждение. Эти хакеры часто выбирают людей в организации жертвы, которые имеют необходимый доступ для совершения преступления, тем самым создавая фасад причастности для других.

Можно сказать, что процесс расследования цифровых преступлений включает строгие процессуальные требования и тщательный анализ технических возможностей подозреваемых. Понимание и управление этими сложностями жизненно важно для обеспечения правосудия и эффективного раскрытия компьютерных преступлений.

В сфере цифровой криминалистики расследование несанкционированного доступа к компьютерным системам требует комплексного подхода. Цель состоит в том, чтобы отследить действия лиц, имеющих доступ к определенным программам, кодам и системам, и определить стороны, ответственные за поддержание и защиту этих цифровых активов. Этот процесс включает в себя подробный анализ доказательств и показаний для раскрытия мотивов, методов и последствий преступления.

Для эффективного противодействия несанкционированному доступу к компьютерной информации следователи должны сначала определить лиц, ответственных за управление и защиту компьютерных систем и сетей. Это включает понимание того, кто имеет допуск и доступ к различным цифровым ресурсам.

Определение вины и понимание мотивов во многом зависят от результатов полного следственного процесса. Ключевые компоненты этого процесса включают:

- свидетельские показания и показания свидетелей: заявления свидетелей, подозреваемых и потерпевших;
- судебная экспертиза: технический анализ, проводимый судебными экспертами, специализирующимися в области информационных технологий;
- результаты поиска: результаты поисков, проведенных в ходе расследования.

При установлении личности и допросе подозреваемого крайне важно восстановить весь процесс преступления, начиная с этапа подготовки. В случаях, связанных с вредоносным программным обеспечением, следователи должны проанализировать алгоритм вредоносного ПО и его влияние на затронутую информацию.

Атаки вредоносного ПО могут усложнить расследование из-за быстрого копирования вредоносного кода в сети жертвы. Этот широко распространенный ущерб может скрыть масштаб вреда и затруднить определение точного воздействия.

Более того, нарушения правил эксплуатации компьютеров могут быть столь же разрушительными, как и вредоносные программы, часто приводя к параличу организационных функций. Расследование таких нарушений требует тщательного изучения нормативных документов и правил эксплуатации организации, чтобы понять общую структуру и конкретные действующие руководящие принципы.

Для решения проблем, связанных как с вредоносным ПО, так и с нарушениями правил эксплуатации, важно привлекать специалистов, которые хорошо разбираются в этих областях, но остаются беспристрастными в расследовании. Эти эксперты помогают расшифровывать сложные технические проблемы и понимать их последствия.

Официальное расследование, которое выявляет нарушения правил эксплуатации, может предоставить ценную информацию и ответы на критические вопросы. Такие выводы часто информируют о разработке стратегии расследования и помогают в формулировании следующих шагов.

Наконец, определение местоположения скомпрометированной станции и ее отклонений от требований информационной безопасности имеет жизненно важное значение. Это может быть достигнуто посредством информационной и технической экспертизы в ходе расследования. Специалисты оценят эти аспекты, чтобы понять, как были нарушены протоколы безопасности, и выявить любые отклонения от стандартных практик.

Можно сказать, что расследование цифровых преступлений требует многогранного подхода, включающего тщательное документирование, экспертный анализ и глубокое понимание технической и нормативной среды. Каждый шаг, от сбора доказательств до консультаций со специалистами, имеет решающее значение для построения всеобъемлющего дела и обеспечения правосудия.

Чтобы точно определить время нарушения правил и вызванного им ущерба, следователи должны оценить, произошли ли вредные последствия преступления одновременно с нарушением или были отсрочены. Это различие имеет решающее значение, поскольку время наступления этих последствий может существенно повлиять на подход к расследованию.

Для установления этих временных рамок можно использовать несколько методов:

- экспертный анализ: специалисты, изучающие журналы сервера и системные протоколы, могут предоставить информацию о том, когда произошли нарушения;
- свидетельские показания: интервью с лицами, участвовавшими в эксплуатации затронутых компьютерных систем, также могут пролить свет на время нарушений;

– техническая экспертиза: Информационные и технические экспертные оценки могут помочь точно определить время и место инцидента.

Такие методы расследования, как официальные запросы, допросы и осмотры мест происшествия, играют решающую роль в раскрытии специфики преступления. Материалы официального расследования часто являются основой для понимания последствий нарушения. Кроме того, допросы всех соответствующих участников могут раскрыть последовательность событий и любые нарушения нормативных требований.

Для выяснения способа нарушения следователям необходимо проводить подробные допросы, привлекать специалистов по криминалистическим экспертизам и следственным экспериментам. Эти методы помогают уточнить последовательность операций и оценить потенциальный вред, причиненный нарушениями.

Следственные эксперименты включают использование реального компьютерного оборудования или носителей информации, где произошло нарушение. Целью этих экспериментов является воспроизведение условий нарушения и понимание его влияния. Результаты помогают оценить масштаб ущерба и вероятность пагубных последствий, возникающих в результате нарушения правил.

Определение лица, ответственного за нарушения, предусмотренные статьей 274 УК РФ, является сложной задачей. Поскольку не все лица, имеющие доступ к системе, имеют необходимые допуски или опыт для совершения этих преступлений, крайне важно сосредоточиться на тех, кто имеет законный доступ и разрешения.

Для эффективного расследования таких случаев следователи должны собрать подробную информацию об этих лицах, включая:

– персональные данные: основные идентификационные данные и должностные обязанности;

- профессиональный опыт: образование, опыт работы и предыдущие должности;
- права доступа: уровень доступа к защищенной информации, обязанности по обеспечению информационной безопасности и участие в разработке программного обеспечения.

Эту информацию можно получить из различных источников, таких как записи сотрудников, протоколы допросов, анализы компьютерных систем и протоколов безопасности.

Кроме того, внутренние расследования, проводимые пострадавшей организацией, могут предоставить ценную информацию об обстоятельствах преступления. Эти выводы необходимы для понимания и доказательства незаконного доступа, создания и распространения вредоносного ПО и других нарушений правил эксплуатации компьютеров.

Заключение

В 21 веке компьютеры и цифровая информация стали неотъемлемой частью повседневной жизни и организационных операций. От офисных сред до индивидуальных предпринимателей персональные компьютеры, офисное оборудование, мобильные устройства и планшеты теперь повсеместны. Эти технологии упростили такие задачи, как бухгалтерский учет, управление и контроль запасов, значительно повысив эффективность. Однако эта обширная зависимость от цифровых инструментов также увеличивает уязвимость конфиденциальной информации, хранящейся на этих устройствах.

Эволюция компьютерных систем и их растущая сложность заставляют профессионалов постоянно повышать свою квалификацию, что, в свою очередь, способствует прогрессу в области информационных технологий. Эта всепроникающая компьютеризация влияет на ландшафт компьютерных преступлений, подчеркивая настоятельную необходимость в эффективных методах расследования.

Рост числа компьютерных преступлений подчеркивает важность понимания и решения этих проблем. Актуальность этой темы очевидна из статистики преступлений, которая отражает значительное количество правонарушений в сфере компьютерной информации. Эта тенденция побудила сосредоточить внимание в этой работе на изучении тонкостей расследования компьютерных преступлений.

Для тщательного изучения особенностей расследований компьютерных преступлений было поставлено несколько целей. Исследование было направлено на изучение методологий и особенностей, связанных с этими типами преступлений, и эти цели были всесторонне рассмотрены.

Исследование началось с анализа криминологических характеристик компьютерных преступлений, сосредоточившись как на субъективных, так и на объективных аспектах, изложенных в уголовном законодательстве. В

первых главах был представлен глубокий анализ этих элементов, с акцентом на следующие моменты:

- криминологические характеристики преступника: в первой главе был изучен профиль преступника, включая его особые навыки и методы. Эти факторы часто выявляют отличительные черты или «почерк», которые могут помочь в идентификации преступников;
- контекстуальные факторы: Расследование компьютерных преступлений также включает изучение среды, в которой произошло преступление. Этот аспект дает представление об условиях, которые способствовали или способствовали преступному деянию. Выявление этих ситуативных факторов имеет важное значение для понимания обстоятельств, которые способствовали преступлению.

Важным компонентом работы был анализ конкретного контекста каждого компьютерного преступления. Этот анализ помогает определить ключевые обстоятельства, которые позволили преступлению произойти. Изучая эти факторы, исследование стремится пролить свет на условия, которые сделали преступное деяние возможным, тем самым помогая в разработке более эффективных стратегий профилактики и расследования.

Можно сказать, что всестороннее изучение компьютерных преступлений и их расследования раскрывает сложность цифрового ландшафта и сложную природу этих преступлений. Понимание криминологических характеристик преступников, влияния их действий и задействованных факторов окружающей среды имеет решающее значение для совершенствования методов расследования и повышения общей эффективности профилактики преступлений в цифровую эпоху.

При изучении субъективной стороны компьютерных преступлений данное исследование выделяет ключевые элементы, такие как вина преступника, мотив и цель его действий. Мотив, хотя и не является обязательным компонентом преступления, играет решающую роль в формировании как метода, так и средств преступной деятельности. Он влияет

на то, как совершается преступление, и характеризует поведение преступника. Таким образом, понимание мотива имеет решающее значение для расследования и раскрытия этих преступлений, даже если оно может не требоваться явно для судебного разбирательства.

Вторая глава данной работы посвящена объективным элементам компьютерных преступлений. Это включает определение объекта и субъекта преступных деяний в этой области. Объектом таких преступлений, как это трактуется в юридических текстах, является защита общественных отношений, имеющих решающее значение для защиты компьютерной информации и обеспечения надлежащего функционирования компьютерных систем и сетей.

Когда несанкционированный доступ к компьютерной системе приводит к повреждению компьютерной информации, то это повреждение может рассматриваться как дополнительный элемент состава преступления в зависимости от его размера. Предметом такого преступления является охраняемая законом компьютерная информация, границы которой устанавливаются законодательством Российской Федерации.

Для привлечения к ответственности по российскому уголовному праву принципиально важно установить полный состав преступления, в том числе доказать, что действия были незаконными. Это предполагает акцент на активном противоправном поведении, а не на пассивном бездействии. В отличие от некоторых других видов правонарушений, компьютерные преступления требуют доказательства четкой причинно-следственной связи между противоправным деянием и его результатами, такими как копирование, уничтожение или изменение данных.

Для суда жизненно важно основывать свои решения на конкретных юридических доказательствах, а не на догадках. Тщательный анализ причинно-следственной связи между преступным деянием и его последствиями имеет важное значение для принятия обоснованных судебных решений.

В то время как начальные главы рассматривали субъективные и объективные аспекты компьютерных преступлений и условия уголовной ответственности, заключительная глава фокусируется на особенностях расследования таких преступлений. Это включает в себя подробное исследование методов расследования, адаптированных к сложностям компьютерных преступлений, подчеркивая необходимость специальных знаний и методологий для эффективного решения этих проблем.

Можно сказать, что это исследование представляет собой комплексное изучение элементов, задействованных в расследованиях компьютерных преступлений, подчеркивая важность понимания как субъективных, так и объективных компонентов. Анализируя эти аспекты, исследование направлено на повышение эффективности следственных практик и внесение вклада в более надежные правовые рамки для борьбы с компьютерными преступлениями.

В процессе расследования компьютерных преступлений первоначальный шаг включает в себя выявление и установление соответствующих обстоятельств, связанных с правонарушением. После этого проводятся конкретные следственные действия для обоснования этих выводов. В ходе таких расследований сотрудники правоохранительных органов, следователи и специалисты усердно работают над раскрытием всех соответствующих деталей преступления, стремясь установить четкое понимание фактов и привлечь виновных к ответственности. Этот этап имеет решающее значение для построения уголовного дела, которое затем представляется в суде.

Дополнительной целью этих расследований является выявление глубинных причин и условий, способствовавших совершению преступления. Понимая эти факторы, власти могут разрабатывать стратегии по предотвращению подобных преступлений в будущем.

Компьютерные преступления, как они определены в главе 28 Уголовного кодекса Российской Федерации, считаются серьезными угрозами

из-за их характера и воздействия. В отличие от традиционных преступлений, эти правонарушения тесно переплетены с технологическими достижениями, что представляет уникальные проблемы для следователей. Одной из существенных проблем является необходимость специальных знаний в области информационных технологий (ИТ).

Стремительное развитие технологий означает, что преступники постоянно совершенствуют свои методы и инструменты, что требует постоянного обучения и развития навыков для следователей. Текущие программы обучения специалистов часто не поспевают за этими достижениями, что может препятствовать эффективному расследованию и судебному преследованию.

Правовая система сталкивается с еще одной важной проблемой: предотвращение компьютерных преступлений. Существующая нормативная база в России не содержит достаточных положений для комплексного решения сложных проблем киберпреступности. Кроме того, наблюдается заметное отсутствие прозрачности в статистике преступлений, что еще больше усложняет усилия по предотвращению таких правонарушений.

Список используемой литературы и используемых источников

1. Анин Б. Ю. Защита компьютерной информации. СПб. : БХВ-Санкт-Петербург, 2000. 384 с.
2. Батурин Ю.М. Проблемы компьютерного права. М. : Юридическая литература, 1991. 272 с.
3. В.П. Тихомирова. Компьютерные преступления: Учебное пособие / Под ред. В.П. Тихомирова, А.В. Хорошилова. - М. : Финансы и статистика, 1996. 68 с.
4. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. Б.П. Смагоринского. - М. : Право и Закон, 1996. 182 с.
5. Викторов М. Законность в кредитно-банковской сфере // Законность. 2007. № 11. С. 23.
6. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): Автореферат дисс. канд. юрид. наук. Махачкала, 2004. 168 с.
7. Гульбин, Ю.А. Преступления в сфере компьютерной информации [Текст]: учебное пособие / Ю.А. Гульбин. – М. : Статут. 2007. 321 с.
8. Ермолович В.Ф. Научные основы криминалистической характеристики преступлений. Минск : Веды, 1999. 312 с.
9. Информатизация и информационная безопасность правоохранительных органов. М. : Академия управления МВД России, 2005. 94 с.
10. Кадников Н.Г. Квалификация преступлений (теория и практика). М. : БЧ интернешнл Лтд., 1999. 110 с.
11. Комментарий к Уголовному кодексу Российской Федерации / Под ред. В.М. Лебедева. - М. : Издательская группа ИНФРА-М - НОРМА, 2010. 640 с.
12. Коржов В.К. Право и Интернет: теория и практика [Текст]: учебное пособие / В.К. Коржов. – М. : Издательство БЕК, 2006. 236 с.

13. Криминология: Учебник / Под ред. В. Н. Кудрявцева, В.Е. Эминова. - М., Юристъ, 2008. 800 с.

14. Крылов В.В. Информационные компьютерные преступления [Текст]: учебное пособие / В. В. Крылов. – М. : Юрид. Лит., 2005. 240 с.

15. Куринов Б.А. Научные основы квалификации преступлений. М. : МГУ, 2004. 181 с.

16. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. М. 256 с.

17. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 9.

18. Максимов, В.Ю. Компьютерные преступления (вирусный аспект) [Текст]: учебное пособие / В.Ю. Максимов. – М. : АО «Центр ЮрИнфор», 2006. 210 с.

19. Научно-практический комментарий к Уголовному кодексу Российской Федерации. В 2 т. Т. 1. Нижний Новгород : Номос, 1996. 624 с.

20. Новое уголовное право России. Особенная часть: Учеб. пособие. М.: Зерцало, ТЕИС, 2006. 456 с.

21. Определение Ульяновского районного суда по делу № 22-680/2019 [Электронный ресурс] / Компания «Консультант Плюс». - Дата обращения 10.05.2019.

22. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. - М. : Норма, 2008. 432 с.

23. Панфилова Е.И. Компьютерные преступления [Текст]: учебное пособие / Е.И. Панфилова. – М. : Феникс, 2007. 254 с.

24. Пархомов В.А., Старичков М.В. О «троянском коне», хакере и уголовной статье // Правосудие в Восточной Сибири. 2003. № 2-3. С. 105.

25. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 г. Москва «О судебной практике по делам о мошенничестве, присвоении и растрате» / Компания «Консультант Плюс». - Дата обращения 10.05.2024.

26. Постановление Пленума Верховного Суда РФ от 19.12.2017 № 51 «О практике применения законодательства при рассмотрении уголовных дел в суде первой инстанции (общий порядок судопроизводства)» / Компания «Консультант Плюс». - Дата обращения 10.05.2024.

27. Сальников В.П. Компьютерная преступность [Текст]: учебное пособие / В.П. Сальников. – М. : Приор, 2004. 192 с.

28. Селиванов Н. А. Проблемы борьбы с компьютерной преступностью // Законность. 1993. № 8. С. 37.

29. Спирина С.Г. Криминологическая характеристика компьютерной преступности в России. Краснодар: Российский государственный торгово-экономический университет, 2009. 28 с.

30. Уголовное право. Общая часть: Учебник / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. - М. : НОВЫЙ Юрист, КноРус, 2007. 217 с.

31. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.05.2024) (с изм. и доп., вступ. в силу с 01.07.2024) [Электронный ресурс] Режим доступа URL: http://www.consultant.ru/ (дата обращения: 18.07.2024).

32. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 12.06.2024) (с изм. и доп., вступ. в силу с 06.07.2024) [Электронный ресурс] Режим доступа URL: http://www.consultant.ru/ (дата обращения: 18.07.2024).