МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего
образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра уголовного процесса, криминалистики и судебных экспертиз

Особенности расследования и раскрытия преступлений в сфере компьютерной информации

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 3 курса 365 группы
направления подготовки 40.04.01«Юриспруденция»
юридического факультета

Васячкиной Алеси Павловны

Научный руководитель
Профессор, д.ю.н., доцент _____ Л.Г. Шапиро

Зав. кафедрой уголовного процесса,
криминалистики и судебных экспертиз
к.ю.н., доцент _____ С.А. Полунин

Саратов 2022

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы заключается в том, что она обусловлена практической и теоретической значимостью вопросов, связанных со становлением и развитием механизмов обеспечения информационной безопасности в России. Число совершенных киберпреступлений возрастает и охватывает все новые и новые деяния. Преступления такого рода характеризуются высоким уровнем скрытности, быстротой совершения и глобальностью последствий, что ставит перед правоохранительными органами задачу разработать новые подходы к раскрытию и расследованию таких деяний. Нормативно-правовая база также требует постоянного обновления и совершенствования, чтобы своевременно реагировать на новые угрозы. По своему механизму, способам совершения и сокрытия следов, эти преступления имеют свои особенности и характеризуются большой латентностью. Одной из причин возникновения компьютерной преступности явилось информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных.

Целью настоящей работы является в комплексном уголовно-правовом и криминологическом научном исследовании состояния, тенденций, характерных черт преступлений в сфере компьютерной информации в Российской Федерации.

Для достижения указанной цели была предпринята попытка решить следующие **задачи**:

- исследовать проблемы квалификации преступления и проблемы привлечения к уголовной ответственности;

- раскрыть основные причины и условия, способствующие совершению преступления в сфере компьютерной информации;

- изучить особенности и проблемы в раскрытии и расследовании преступлений в сфере компьютерной информации;

- проанализировать нормы права, устанавливающие уголовную ответственность за преступления в сфере компьютерной информации.

Объектом исследования является общественные отношения, в части правомерного и безопасного использования компьютерной информации и информационных ресурсов.

Предмет изучения является преступность в сфере компьютерной информации, ее состояние, структура и динамика; методы, особенности расследования преступлений в сфере компьютерной информации; совокупность мер по предупреждению компьютерных преступлений.

Степень научной разработанности. Тема выпускной квалификационной работы носит комплексный подход к изучению. Достижение поставленной в диссертационном исследовании цели, потребовало обращения к трудам ученых, специализировавшихся в области изучение преступности в сфере компьютерной информации, таких процессуалистов, как В.И. Алексеровым, О.Н. Колокольчиковой, Ю.М. Батуриным, В.В. Гончарым, В.Ю. Агибаловым, М.А. Бабаковой, В.Б. Веховым, А.С. Вражновым, А.А. Васильевым, Ю.В. Гаврилиным, В.В. Крыловым, В.А. Мещеряковым, Д.А. Илюшиным, В.В. Степановым, А.И. Семикаленовой, А.И. Усовым и др. Авторами исследовались вопросы как предварительного расследования, так и судебного рассмотрения уголовных дел в сфере компьютерной информации.

Методологическую основу работы составляют общенаучные и частнонаучные методы исследования: анализ изучаемого объекта, синтез полученных при анализе объекта данных в систему, аксиоматический подход к рассмотрению положений нашего законодательства, а также комплексный подход к изучению объекта исследования.

Теоретическую основу работы составляют труды российских ученых в области преступности в сфере компьютерной информации.

Правовая основа работы сформирована на основе Конституции Российской Федерации, федеральных законов, законов Российской Федерации, и др.

Научная новизна магистерской работы определяется также его комплексным характером, углубленным исследованием процессов раскрытия дел в сфере компьютерной информации, развития и реализации преступности в сфере компьютерной информации.

Эмпирическую основу работы составили материалы периодической печати, социологических исследований, данные размещенные в сети Интернет по теме выпускной квалификационной работы.

Положения, выносимые на защиту:

1. Преступления в сфере компьютерной информации – это совершаемые посредством ЭВМ предусмотренные уголовным законом и запрещенные им под угрозой наказания виновные общественно опасные деяния, посягающие на общественные отношения, возникающие в сфере обеспечения безопасности компьютерной информации и систем обработки, приема и передачи компьютерной информации, состоящие в противоправном воздействии на компьютерную информацию и причиняющие вред личности, обществу или государству.

2. В целях более четкого изложения диспозиции ч. 1 ст. 272 УК РФ при описании предмета преступления предлагается вместо термина «охраняемая законом компьютерная информация» использовать термин «компьютерная информация ограниченного доступа».

3. Заключение, основанное на дефиниции ч. 2 ст. 24 УК РФ, о возможности совершения преступления, предусмотренного ст. 272 УК РФ, как умышленно, так и по неосторожности.

4. В целях дифференциации уголовной ответственности предложение о выделении в качестве особо квалифицирующего признака совершение преступления организованной группой.

5. Вывод о признании субъектом преступления, предусмотренного ч. 2 ст. 272 УК РФ (по признаку «лицом с использованием своего служебного положения»), как должностных, так и не должностных лиц, перечень которых содержится в примечаниях к ст. 285 и 201 УК РФ, чьи служебные обязанности

позволяют совершать доступ к охраняемой законом компьютерной информации или влиять по службе на лиц, имеющих такой доступ.

6. Тезис о том, что местом совершения преступления, предусмотренного ст. 272 УК РФ, следует признавать Россию независимо от того, где началось/закончилось это преступление, если хотя бы какая-то его часть была совершена на территории Российской Федерации.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы, анализируется ее научная разработанность, определяются объект и предмет исследования, цели работы и комплекс решаемых задач, отмечаются теоретико-методологическая основы исследуемой проблемы, раскрываются использованные в исследовании источники, формулируются научная новизна диссертационного исследования, положения, выносимые на защиту и подтверждающие теоретическую и практическую значимость работы, излагаются результаты апробации проведенного исследования.

Глава первая: «Сущность и развитие преступлений в сфере компьютерной информаци и» посвящена понятиям и видам преступлений в сфере компьютерной информации (§1.1); истории создания Управление «К», как одно из подразделений по борьбе с компьютерными преступлениями в структуре МВД России (§1.2); информации как основному элементу при раскрытии преступлений (§1.3).

В первой параграфе исследован вопрос о соотношении понятий компьютерные преступления и преступления в сфере компьютерной информации.

В ходе исследования было определено, что есть несколько позиций относительно определения понятия преступлений в сфере компьютерной информации. Л.Е. Шведова, В.А. Номоконов, к таковым преступлениям относят преступные деяния, в которых объектом или оружием преступления выступает компьютер. С данной точкой зрения сложно согласиться, по той причине, что с

помощью компьютера или цифровых технологий могут быть связаны и иные преступления, которые не относятся к рассматриваемой группе преступных посягательств.

Так, например, Ю.И. Ляпунов отмечает, что компьютер может выступать предметом таких преступления, как хищение, повреждение, которые направлены против собственности, и соответственно представляют собой иную группу преступлении.

Н.Н. Коротких, М.Д. Останин рассматривая соотношений этих двух понятий отмечают, что понятие «компьютерные преступления» шире чем понятие ««преступления в сфере компьютерной информации». Мы полагаем необходимым согласиться с этим мнением, поскольку как уже отмечали ранее, преступления, которые совершены с применением компьютеров компьютерных технологий, не всегда направлены на компьютерную информацию.

В.И. Белоножкин в своей работе отмечает, что одни авторы к преступлениям в сфере компьютерной информации относят только те преступные деяния, которые затрагивают сферу обращения информации, распространяемой в информационно-телекоммуникационных системах, другие же определяют компьютерные преступления, как информационные преступные деяния.

Известны также точки зрения, согласно которым предметом исследуемой группы преступлений следует считать не только компьютер или компьютерную информацию, но также и компьютерные систему и сеть. Сторонниками такой позиции являются Г.Н. Борзенков, В.С. Комиссаров.

Как мы видим, единого мнения по вопросу природы и понятия преступлений в сфере компьютерной информации в научной среде не достигнуто.

В то время как в научной литературе ведутся споры по вопросам содержания рассматриваемой группы преступлений, законодатель не дает определений понятию преступлений в сфере компьютерной информации, закрепляя лишь их перечень в уголовном законе России.

Уголовный закон России к рассматриваемой группе преступлений предусматривает термин «преступления в сфере компьютерной информации».

Во втором параграфе автор выявил, что изменения начали происходить в 90-е годы, когда компьютеры стали более распространены, а интернет начал активно развиваться. В этот период в России произошли первые значительные случаи киберпреступлений, связанные с мошенничеством и кражей конфиденциальных данных. Одним из самых известных инцидентов стала кража уникального программного обеспечения для банковской системы «Финам» в 1995 году.

Таким образом, переход от игнорирования киберпреступлений к осознанию их опасности и необходимости их пресечения стал важным этапом в развитии правоприменительной практики и законодательства в данной сфере.

В девяностых годах процесс компьютеризации продолжал набирать обороты, что способствовало возникновению новых форм преступлений, связанных с компьютерами. Одним из самых распространенных видов стало интернет-мошенничество. Злоумышленники применяли различные техники обмана, такие как фишинг, а также создавали поддельные интернет-магазины, чтобы вводить в заблуждение пользователей.

В связи с этим, первым этапом борьбы с злом явилась разработка нового Уголовного кодекса Российской Федерации, который вступил в силу с января 1997 года.

В Уголовный кодекс Российской Федерации была включена Глава 28 «Преступления в сфере компьютерной информации», предусматривающая три состава преступления:

1. незаконный доступ к информации ЭВМ, их систем и сетей (ст. 272 УК РФ);
2. создание, распространение и использование вредоносных программ для ЭВМ (ст. 273 УК РФ);
3. нарушение правил эксплуатации ЭВМ, их систем и сетей (ст. 274 УК РФ).

В 1986 году с целью обеспечения радиоэлектронной безопасности для органов внутренних дел, а также для выявления специальных технических устройств, предназначенных для тайного сбора информации и предотвращения несанкционированного доступа к компьютерным сетям, в структуре МВД СССР было создано Управление радиоэлектронной борьбы, также известное как Управление «Р».

7 октября 1998 года Управление «Р» было преобразовано в Управление по борьбе с преступлениями в сфере высоких технологий (УБПСВТ). В его структуре были выделены три направления деятельности:

1. Борьба с преступлениями в сфере компьютерной информации.
2. Борьба с преступлениями в сфере телекоммуникаций.
3. Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

В территориальных подразделениях МВД Республик, УВД, ГУВД областей до 1999 года были созданы аналогичные структурные подразделения – отделы БПСВТ (ОБПСВТ).

В 2002 году это управление было расформировано, а его функции переданы Главному Управлению Специальных Технических мероприятий МВД России. После ряда реформ название подразделения изменилось на современное – Управление «К» БСТМ МВД России, а также были учреждены отделы «К» на уровне территориальных подразделений МВД.

В третьем параграфе было установлено, что с каждым годом человечество все больше погружается в мир технологий. Это, безусловно, приносит множество положительных изменений, однако, к сожалению, некоторые люди используют эти достижения в корыстных целях.

Поскольку преступления в сфере компьютерной информации является сравнительно новым и уникальным видом правонарушений, их расследование представляет собой ряд сложностей. Чтобы эффективно выявить и предотвратить подобные деяния, работникам подразделений «К» необходимо

разрабатывать и внедрять новые методы и подходы в оперативно-розыскной деятельности.

На данный момент уголовное законодательство включает нормы, которые обеспечивают защиту самых различных видов информации, включая как документированную, так и иную. Таким образом, правоотношения, возникающие в контексте компьютерной информации, должны находиться под охраной закона.

Проанализировав нормы отраслей права, можно сделать ряд выводов :

1. Информация представляет собой сведения (сообщения, данные) независимо от формы их представления.
2. Любая документированная информация, т.е. информация, облеченная в форму, которая позволяет ее идентифицировать полежит правовой защите.
3. Любая информация, которая задокументирована, имеет собственника, а, следовательно, является объектом гражданских прав.
4. Ограничения использования информации устанавливаются законом или собственником информации, которые объявляют уровень ее конфиденциальности.
5. Любая форма завладения и пользования конфиденциальной документированной информацией без прямо выраженного согласия ее собственника является нарушением его прав, т.е. неправомерным деянием.

Анализ уголовного права в сфере преступлений, связанных с компьютерной информацией, невозможен без чёткого понимания понятия «информация». Информация выступает как относительно новый объект исследования и правового регулирования. Поэтому требуется изучение как законодательных, так и научных определений информации.

Прогресс в области технологии дал злоумышленникам новые возможности для неправомерного доступа к данным. Таким образом, на начальной стадии расследования важно своевременно получать информацию о

совершенном или готовящемся преступлении для выбора правильной стратегии действий оперативных сотрудников. Это позволит быстрее установить личности преступников с закреплением, полученных в ходе документирования доказательств.

Глава вторая «Криминалистическая характеристика преступлений, совершаемых в сфере компьютерной информации» посвящена неправомерному доступу к компьютерной информации (ст. 272 УК РФ) (§2.1), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) (§2.2), а также нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-коммуникационных сетей (ст. 274 УК РФ) (§2.3).

В первом параграфе автором установлено, что неправомерный доступ к компьютерной информации – это одно из самых распространенных преступлений в сфере информационных технологий. Этот вид преступления, определенный статьей 272 Уголовного кодекса Российской Федерации, является угрозой безопасности информации, которая имеет критическое значение для различных сфер жизни общества, включая экономику, государственные органы, предприятия и частных граждан. Важно отметить, что данное преступление может быть совершено как с применением традиционных методов взлома, так и с использованием более сложных технических средств и методов.

Неправомерный доступ в контексте данной статьи подразумевает любые действия, направленные на незаконное проникновение в систему, программу или базу данных с целью получения доступа к компьютерной информации, хранимой или передаваемой с использованием информационно-коммуникационных технологий. Важно подчеркнуть, что такие действия, как правило, совершаются без согласия владельца или законного оператора информационных систем, что нарушает права и законные интересы граждан, организаций и государства.

Существует несколько типов неправомерного доступа к компьютерной информации, в зависимости от методов и инструментов, используемых для совершения преступления.

Так, использование программ для подбора паролей (например, с помощью атак перебора или социальных инженерных методов) с целью несанкционированного доступа к системам, защищенным паролями.

Вредоносные программы могут быть использованы для захвата данных пользователя, их скрытого использования или передачи третьим лицам. Применение таких программ часто связано с риском кражи личных данных, финансовой информации и других конфиденциальных сведений.

Взломы, основанные на найденных уязвимостях в программном обеспечении или операционных системах, также составляют часть преступления. Вредоносные лица могут использовать эти уязвимости для незаконного получения доступа к информации.

С помощью средств удаленного доступа злоумышленники могут проникать в системы организаций, используя слабые места в безопасности Интернет-соединений или неправомерный доступ к защищенным серверам.

Согласно статье 272 УК РФ, неправомерный доступ к компьютерной информации карается штрафом, обязательными работами, арестом или лишением свободы. В случае, если преступление повлекло за собой значительные материальные убытки или утечку конфиденциальной информации, наказание может быть более жестким. Лица, имеющие судимость или ранее осужденные за аналогичные преступления, могут быть подвергнуты более строгому наказанию.

Максимальная мера наказания за неправомерный доступ к компьютерной информации может включать лишение свободы на срок до 6 лет с возможным штрафом. В то же время, для лиц, совершивших это преступление по неосторожности, наказание может быть менее строгим.

Расследование преступлений, связанных с компьютерной информацией, представляет собой одну из самых сложных областей уголовного права и

криминалистики. Этот процесс включает в себя множество вызовов, с которыми сталкиваются правоохранительные органы, от сложностей доказательства до технических и юридических преград.

Одной из основных сложностей в расследовании компьютерных преступлений является сама природа доказательств, которые часто легко могут быть скрыты или удалены. В отличие от традиционных преступлений, где доказательства могут быть физическими объектами (например, оружие, следы на месте преступления), в сфере компьютерной информации доказательства часто существуют в цифровом виде, что приводит к нескольким проблемам.

Современные технологии требуют использования специализированных инструментов для сбора и анализа цифровых доказательств. Для извлечения данных из защищенных систем, таких как зашифрованные носители или системы с высокой степенью защиты, требуется наличие специализированных программ и аппаратных средств. Не все правоохранительные органы имеют доступ к таким ресурсам, что затрудняет процесс расследования. Современные инструменты для расследования компьютерных преступлений могут быть очень дорогими, что становится серьезным препятствием для многих правоохранительных органов, особенно в странах с ограниченным бюджетом.

Во втором параграфе рассмотрено создание вредоносных программ, или, другими словами, разработка программного обеспечения с намерением нанести вред системе, считается тяжким преступлением. Вредоносное ПО может быть использовано для различных целей: от простых вирусов, наносящих ущерб данным, до сложных программ, с помощью которых можно красть личные данные, получить несанкционированный доступ к компьютерным системам или организовывать масштабные кибератаки.

Программисты, занимающиеся созданием вредоносных программ, используют различные методы, такие как внедрение скрытого кода в легитимное программное обеспечение, использование уязвимостей в операционных системах и приложениях, а также создание программ, которые скрываются от антивирусных программ. Вредоносные программы могут быть

специально настроены для того, чтобы не обнаруживаться или запускаться только при определенных условиях, что значительно усложняет их детекцию.

Зачастую цель создания таких программ заключается в получении незаконного доступа к личной или корпоративной информации, вмешательстве в работу государственных или коммерческих учреждений, повреждении файлов и баз данных или в проведении хакерских атак. Программы могут использоваться для установки шпионских программ, «захвата» ПК для проведения атак (ботнеты) или криптоджекинга, а также для осуществления мошеннических действий через фишинг и подмену данных.

Они могут варьироваться по своей функциональности, целям и способам распространения. Использование вредоносных программ предполагает их применение с целью достижения преступных намерений. Такие программы могут использоваться для различных целей, включая кражу данных, захват систем, саботаж и многое другое.

Злоумышленники могут использовать вредоносное ПО для получения несанкционированного доступа к компьютерным системам или сетям. Например, использование троянских программ может дать хакеру полный контроль над системой жертвы, включая доступ к личным и финансовым данным.

Вредоносные программы, такие как шпионские вирусы, могут быть использованы для сбора конфиденциальной информации о пользователе – паролей, логинов, финансовых данных, истории веб-серфинга и других данных, которые могут быть использованы для мошенничества, кражи денег и других преступлений.

Также они могут использоваться для проведения шпионских операций, включая кражу интеллектуальной собственности, корпоративных данных или государственных секретов. Это особенно актуально для киберпреступлений, связанных с промышленным шпионажем.

Для защиты от вредоносных программ используются антивирусные и антишпионские программы, системы защиты от вторжений, шифрование

данных и другие технологии информационной безопасности. Обновления программного обеспечения, регулярное тестирование на уязвимости и использование безопасных систем хранения данных являются важными элементами профилактики.

Обучение пользователей безопасному поведению в интернете, включая осторожность при открытии подозрительных электронных писем, скачивании файлов и переходе по ссылкам, может существенно снизить риски заражения вредоносными программами.

В третьем параграфе рассмотрена роль ст. 274 Уголовного кодекса Российской Федерации (УК РФ), которая регулирует ответственность за преступления, связанные с нарушением правил эксплуатации информационных систем, которые обеспечивают хранение, обработку или передачу данных. Эти преступления наносят вред информационным ресурсам, нарушают нормальное функционирование систем и могут повлечь серьезные последствия, такие как утечка данных, нарушение работы предприятий и организаций, а также угрозу национальной безопасности.

Нарушения правил эксплуатации информационных систем могут привести к значительным убыткам для компаний и организаций. Одним из главных рисков является утрата критически важной информации. Это может быть связано с отсутствием резервного копирования или неправильной настройкой систем хранения данных. Такие потери затрудняют работу и нередко требуют длительного восстановления.

Любой сбой в работе информационных систем, вызванный неправильной эксплуатацией, может привести к остановке производственных линий, срыву деловых операций или задержке выполнения заказов.

Компании несут убытки не только из-за потери данных или простоев, но и из-за штрафов за несоблюдение стандартов информационной безопасности. Кроме того, затраты на восстановление работы системы, судебные разбирательства и компенсацию клиентам могут оказаться значительными.

Во-вторых, нарушение правил эксплуатации может нести угрозу для национальной безопасности. Если сбой происходит в системах, связанных с энергетическими объектами, транспортными сетями, здравоохранением или другими важными отраслями, это может привести к масштабным кризисам. Например, атака на информационные системы энергокомпаний может оставить целые регионы без электричества, а нарушение транспортных систем – парализовать работу логистики.

Третий аспект касается защиты данных граждан. Нарушение правил эксплуатации часто приводит к утечке конфиденциальной информации пользователей. Это могут быть паспортные данные, сведения о банковских картах, адреса или другая информация. Такая утечка создает возможности для мошенничества, кражи личности или иных преступлений.

Наконец, важно учитывать репутационные последствия. Когда компания или государственная структура допускает утрату данных или сбой работы систем, это приводит к потере доверия со стороны клиентов, партнеров и граждан. Репутация, которая создавалась годами, может быть разрушена за считанные дни. Например, клиенты банка, пострадавшие от утечки данных, могут перейти к конкурентам, а граждане утратят веру в безопасность государственных сервисов.

Таким образом, статья 274 УК РФ является важным инструментом для обеспечения ответственности за нарушения в сфере эксплуатации информационных систем.

Глава 3. Особенности расследования и раскрытия преступлений в сфере компьютерной информации глава посвящена преступлениям в области компьютерной информации, которые имеют ряд особенностей и затруднений их обнаружение и расследование. Одной из ключевых характеристик является несовпадение места, где осуществляются противоправные действия, с местом наступления общественно опасных последствий. Это связано с дистанционным характером преступлений, которые совершаются с использованием информационных технологий.

Чаще всего такие преступления происходят в профессиональной среде, связанной с интеллектуальной деятельностью. Преступники пользуются знаниями и навыками, полученными во время профессиональной подготовки, и применяют специализированное оборудование. Это предполагает осведомленность нарушителей о механизмах работы информационных систем, их уязвимостях и возможных нарушениях правил эксплуатации.

Спецификой данного типа преступлений является необходимость привлечения квалифицированных специалистов. Они помогают правильно интерпретировать технические данные и выявить следы вмешательства в работу системы.

Признаки неправомерных действий с компьютерной информацией, как правило, фиксируются сотрудниками, обслуживающими систему, или ее пользователями. Эти признаки могут быть как явными, так и косвенными.

Если преступник задержан на месте совершения преступления или сразу после него, следственные действия включают изъятие технических устройств, документов и других предметов, связанных с преступлением, уточнение мотивов, способа вторжения и других обстоятельств преступления и выявление доказательств подготовки и совершения преступления, включая аппаратуру и документацию.

Если подозреваемое лицо отсутствует, следователь сосредотачивается на сборе и фиксации доказательств с помощью собственника системы и розыске виновного лица и места, откуда совершалось вторжение.

Важной особенностью расследований в данной области является тесное сотрудничество следователя со специалистами в области компьютерной техники. Специалисты помогают анализировать технические данные, определять способы проникновения, фиксировать состояние систем и носителей и выстраивать технологическую цепочку действий злоумышленника.

Глава 4. Расследование и раскрытие компьютерных преступлений: проблемы и пути совершенствования глава посвящена стремительному развитию информационных технологий, которое привело к существенным

изменениям в характере преступности. Одним из самых сложных и быстрорастущих видов преступлений являются **компьютерные преступления**. Эти преступления охватывают широкий спектр действий, включая взломы информационных систем, кражу данных, распространение вирусов, мошенничество с использованием интернета и т.д. Расследование таких преступлений сталкивается с рядом проблем, связанных с техническими, правовыми и организационными аспектами. В этом контексте важно рассмотреть основные трудности, возникающие при расследовании компьютерных преступлений, а также пути их преодоления.

Одной из главных проблем, с которыми сталкиваются правоохранительные органы при расследовании компьютерных преступлений, является высокая сложность технической стороны этих дел. Компьютерные преступления могут быть совершены с использованием сложных программных средств, криптографических методов и анонимных каналов связи, что затрудняет сбор доказательств, а также установление точной последовательности событий. С развитием технологий преступники все чаще применяют новые способы уклонения от расследования, включая использование шифрования для скрытия своих действий, создания вредоносного ПО, взлома систем защиты данных и применения методов анонимизации в сети. Это приводит к тому, что традиционные методы расследования, которые применяются для анализа физических доказательств, становятся неэффективными в виртуальной среде.

Одним из ярких примеров является использование криптографических технологий для шифрования данных. Когда преступники применяют шифрование, это может серьезно затруднить доступ правоохранительных органов к информации, необходимой для раскрытия преступления. Для расшифровки данных часто требуется значительный объем вычислительных ресурсов и знания в области криптографии, которых могут не быть у сотрудников, работающих над делом. Также важным аспектом является использование вредоносных программ, таких как вирусы, трояны или руткиты,

которые могут скрывать или удалять следы преступной деятельности, либо делать их недоступными для обычных методов анализа.

Кроме того, значительные трудности при расследовании создают анонимные каналы связи, через которые преступники могут скрывать свое местоположение и личность. Использование средств анонимизации, таких как VPN (виртуальная частная сеть), прокси-серверы или анонимные сети типа Tor, позволяет хакерам скрывать свой IP-адрес, что затрудняет установление их точного местоположения. Эти технологии позволяют преступникам проводить свои действия в интернете практически без следов, что усложняет идентификацию подозреваемых. В случае с международными преступлениями, когда преступники могут действовать из разных стран, проблема анонимности усложняется еще больше. Это требует от правоохранительных органов тесного сотрудничества с коллегами из других государств, а также учета различий в законодательных системах разных стран. Раскрытие таких преступлений может потребовать времени и усилий для сбора доказательств в разных юрисдикциях, что увеличивает сроки расследования и может влиять на его успешность.

Несмотря на наличие специалистов в области информационных технологий, правоохранительные органы часто сталкиваются с нехваткой кадров, обладающих достаточным уровнем знаний в области компьютерных наук и криминалистики. В результате этого недостатка квалифицированных кадров, расследования компьютерных преступлений часто неэффективны, а также могут возникать проблемы с правильной интерпретацией полученных данных. Учитывая скорость развития технологий, отсутствие квалифицированных специалистов может привести к тому, что расследования будут затягиваться, а в некоторых случаях — не приводить к успешному завершению дела. Это также может привести к недооценке угроз и неправильной оценке степени опасности, исходящей от киберпреступников.

Важной проблемой является также то, что законодательство в ряде случаев не успевает за быстрым развитием информационных технологий. Многие аспекты, связанные с компьютерными преступлениями, такими как

защита данных, вопросы конфиденциальности, криптография и межгосударственное сотрудничество, остаются без должного правового регулирования. В некоторых странах законы не охватывают новые виды преступлений, такие как кибертерроризм, интернет-мошенничество, распространение фальшивых новостей, кражу личных данных и т.д. Это создает правовые пробелы, которые могут затруднить не только расследование, но и привлечение преступников к ответственности. Например, законодатели часто не успевают оперативно реагировать на новые угрозы и не могут обеспечить достаточно жесткие наказания для преступников, которые используют новые технологии.

Еще одним важным инструментом является аналитика трафика в сети. Программы для анализа сетевых пакетов и протоколов могут помочь выявить аномалии в трафике, такие как утечку данных, попытки взлома или связи с удаленными серверами. Эти инструменты позволяют детально отслеживать передвижение данных по сети, анализировать пакеты, их размер, источник и назначение, что может помочь установить связь между преступными действиями и конкретными пользователями. Также стоит обратить внимание на возможность мониторинга анонимных сетей, таких как Tor, которые часто используются для сокрытия преступной деятельности в Интернете. Разработка технологий для анализа анонимных соединений и выявления реальных IP-адресов преступников в этих сетях крайне важна для успешного расследования.

Кроме того, нужно совершенствовать взаимодействие между государственными структурами и частными компаниями, занимающимися безопасностью данных. Многие компании разрабатывают системы защиты от киберугроз и обладают важной информацией о хакерских атаках и уязвимостях в системах. Обмен такой информацией с правоохранительными органами позволит оперативно реагировать на угрозы и предотвращать преступления. Важно создать механизмы для защиты конфиденциальности при обмене информацией между государством и частными компаниями, чтобы избежать

утечек данных, и обеспечить эффективное использование этой информации для раскрытия преступлений.

Таким образом, расследование и раскрытие компьютерных преступлений представляет собой сложную задачу, которая требует постоянного совершенствования методов, инструментов и подходов. Только с помощью активного обучения специалистов, международного сотрудничества, разработки новых технологий и правового регулирования можно создать эффективную систему борьбы с киберпреступностью. Важно отметить, что успешное раскрытие таких преступлений невозможно без тесной кооперации между государственными и частными структурами, а также без применения новейших достижений в области информационных технологий.

В **Заключении** подводятся итоги, формулируются выводы и предложения диссертанта. Освещены основные проблемы, связанные с раскрытием преступлений в сфере компьютерной информации и пути их совершенствования.

По теме диссертации автором опубликованы статьи:

- в Международном научном журнале «Молодой ученный №22»;
- в Международном научном журнале «Молодой ученный №26».