МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

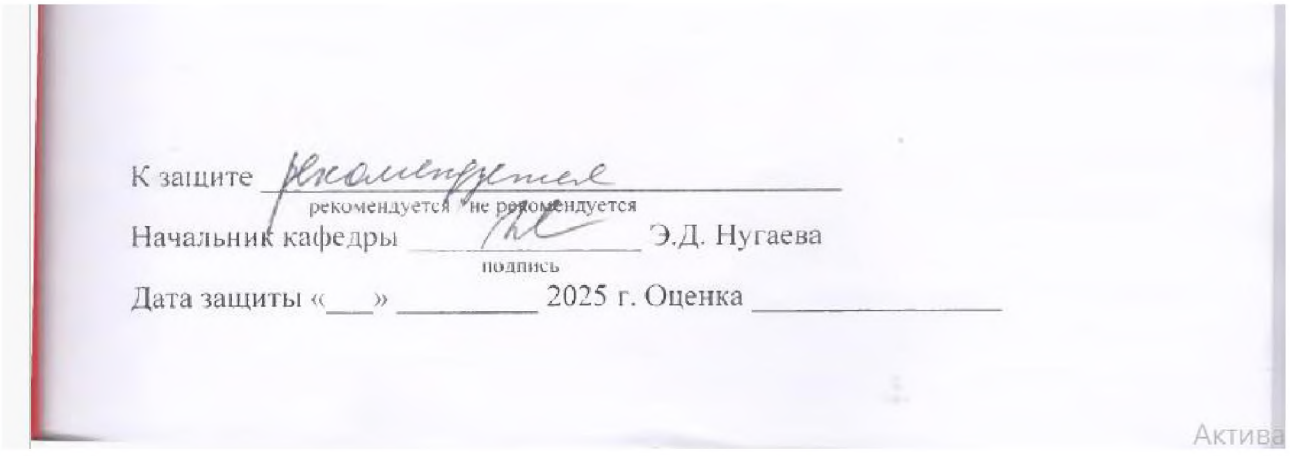
Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему **«ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнил
Хидиятуллин Даян Рустемович
обучающийся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2020 года набора, 011 учебного взвода

Руководитель
старший преподаватель
кафедры криминалистики
Гилязов Руслан Рэлифович



ПЛАН

ВВЕДЕНИЕ

Развитие информационных технологий в последние годы привело к увеличению преступлений в сфере компьютерной информации. На территории Российской Федерации в 2024 году увеличилось количество зарегистрированных преступлений, совершенных с использованием информационно–телекоммуникационных технологий, в сравнении с 2023 годом[1]. Ущерб от такого рода преступлений составляет сотни миллиардов, что является существенным для государства в целом.

Сегодня ни одно учреждение и организация не обходятся без применения в своей деятельности сети Интернет, системы учёта и т.д. именно уровень безопасности данных процессов определяет защищённость государства, обеспечивает нормальную жизнедеятельность человека в обществе. Локальные сети объединены в систему общемировой глобальной сети посредством телекоммуникационных технологий.

Во всех стратегически важных сферах хозяйства и, самое главное, в сфере обороны страны, применяются системы автоматизации управления, контроля (мониторинга), а также прогнозирования, охраны и защиты объектов с помощью устройств, основанных на разнообразных микропроцессорных устройствах (интегральных микросхемах).

Согласно статистическим данным процент преступлений в области компьютерной информации в общей массе зарегистрированных преступлений небольшой, однако, данный вид преступлений с каждым годом набирает обороты и растёт, что ставит под угрозу информационную безопасность государства.

Развитие сферы информационно-телекоммуникационных технологий (далее ИТТ) порождает возникновение новых способов совершения преступных посягательств на собственность и иные объекты уголовно–правовой охраны.

---

[1] Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://xn—b1aew.xn—p1ai/reports/item/60248328/ (дата обращения 01.03.2025).

Несколько усугубляется положение в связи с плохо разработанной правовой базой в данной области, неимением необходимых навыков работы в указанной области сотрудниками правоохранительных органов при расследовании преступлений в области компьютерных технологий. Отсутствует должное обучение сотрудников правоохранительных органов в сфере информационных технологий, специальных программ ЭВМ, защиты от вредоносных вирусов, современных компьютерных программ, а также баз данных компьютерной информации. Более того дополнительно сотрудники должны проходить переподготовку в данной области, так как технические возможности постоянно совершенствуются, поэтому необходима должная подготовка для соответствия профессиональной подготовке компьютерных преступников.

По данным МВД России в 2024 году общее количество, зарегистрированных на территории Российской Федерации преступлений снизилось на 1,8 %. Однако, 40 % из общего количества зарегистрированных преступлений составляют преступления, совершённые с применением информационных технологий. Противоправных деяний такого рода зарегистрировано на 13,1 % больше нежели в 2023 году[1].

В ходе прохождения преддипломной практики в ОМВД России по Кунашакскому району Челябинской области изучены статистические сведения по преступлениям в области ИТТ за период с 2021 по 2024 годы (рис. 1.1)[2]. Представленные показатели свидетельствуют о положительной динамике снижения, зарегистрированных преступлений в сфере ИТТ в анализируемый период. Однако, данного нельзя сказать о общем количестве, зарегистрированных преступлений, которое в последние три года практически не изменяется.

---

[1] Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/ (дата обращения 01.03.2025).

[2] Статистические данные ОМВД России по Кунашакскому району Челябинской области.

Год	Зарегистрировано преступлений всего	Зарегистрировано преступлений в сфере ИТТ
2021	391	50
2022	455	56
2023	456	54
2024	455	45

Рис. 1.1 «Динамика общего количества преступлений и преступлений в сфере ИТТ, зарегистрированных в ОМВД России по Кунашакскому району Челябинской области за период с 2021 по 2024 год».

Следственная практика показывает, что при расследовании компьютерных преступлений возникает много проблем и пробелов, имеет место большая разобщенность в действиях следственных органов по обмену и проверке информации по обстоятельствам, подлежащим установлению и проверке.

Возможности экспертно – криминалистических подразделений не применяются в полной мере для обнаружения, фиксации, исследования и изъятия специфических вещественных доказательств. Вышеизложенное указывает на важность, актуальность, практическую и теоретическую значимость темы дипломного исследования.

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

Для достижения поставленной цели необходимо решить следующие задачи:

– определить основные элементы криминалистической характеристики преступлений в сфере компьютерной информации;

– провести анализ обстоятельств, подлежащих установлению и доказыванию;

– выявить особенности производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации;

– выявить современные проблемы расследования и раскрытия преступлений в сфере компьютерной информации и пути их решения.

Объектом исследования настоящей выпускной квалификационной работы является деятельность правоохранительных органов по расследованию преступлений в сфере компьютерной информации.

Предметом исследования являются криминалистическая характеристика данного состава преступления и производство отдельных следственных действий.

Структуры выпускной квалификационной работы составляет введение, две главы, объединяющих четыре параграфа, заключение, список использованной литературы.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Уголовно-правовая характеристика преступлений в сфере компьютерной информации

Родовым объектом такого преступления как неправомерный доступ к компьютерной информации является совокупность общественных отношений, составляющих содержание общественной безопасности и общественного порядка.

Видовым объектом преступного посягательства, то есть критерием по которому компьютерные преступления могут быть собраны в одной главе Уголовный кодекс Российской Федерации (далее УК РФ) являются общественные отношения в части правомерного и безопасного использования компьютерной информации и информационных ресурсов.

Объектом же рассматриваемого преступления выступают общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы электронной вычислительной машины, системы электронно–вычислительной машины или их сети.

Что касается факультативного объекта неправомерного доступа к компьютерной информации, то стоит подчеркнуть, что о его наличии следует судить только исходя из причинённого преступлением вреда. Следовательно, при наличии факультативного (дополнительного) объекта общественная опасность преступления повышается, что необходимо принимать во внимание при назначении наказания.

Объекта преступления выступает основным элементом состава преступления, поэтому при его отсутствии состава преступления не будет.

Предмет такого преступления как неправомерный доступ к компьютерной информации служит основным показателем разграничения компьютерных преступлений от остальных преступлений, имеющихся в УК РФ.

По мнению ряда научных деятелей, предметом преступлений в сфере неправомерного доступа к компьютерной информации является персональный компьютер – носитель информации[1]. Однако, следование такой трактовке позволяет умышленно расширить границы уголовной ответственности за совершение данного преступления, что является несправедливым. Более того отнесение персонального компьютера к предмету преступления свидетельствует о наличии иной группы преступлений, а именно преступлений против собственности.

Здесь к предмету преступления следует относить компьютерную информацию, базы данных или информационные ресурсы, которые находятся в персональном компьютере. Так как при совершении компьютерного преступления лицо посягает именно на данные ресурсы, а также ставит под угрозу своими действиями безопасность и защиту такого рода информации, нормальную работу с персональным компьютером или сети электронной вычислительной машины.

Следует подчеркнуть, что здесь рассматривается именно информация, которая находится под охраной законодательства Российской Федерации (далее РФ), иными словами, это не любая компьютерная информация, а только определённая УК РФ.

Доступ к такого рода информации имеют только определённые лица, имеющие особый статус, регламентированный законодательством РФ и субъектов. Такая информация может касаться безопасности государства и общества, затрагивать жизнедеятельность отдельных членов общества, сведения о вооружении, космосе и т.д.

Охраняемая законом информация принадлежит не отдельно взятому гражданину, а государству, следовательно, её распространение может нанести ущерб безопасности Российской Федерации.

---

[1] Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. М.: Новый юрист. 2020. с. 210.

Сюда же следует относить информацию, содержащую коммерческую тайну. Это может быть коммерческая информация, но и любая другая, содержащая банковскую или служебную тайну. Такая информация регламентирована ГК РФ[1] и УК РФ[2].

Специфическим видом информации являются сведения, относящиеся к авторскому праву, их правовой статус регламентирован Конституцией РФ[3].

Что же касается частной информации, стоит отметить, что Конституция РФ провозглашает неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Именно данный закон дает с одной стороны свободу выбора в пользовании информации о своей личности (персональной информации), а с другой стороны ограничивает это же право, тем самым защищая права иных лиц.

УК РФ предусматривает ответственность за незаконное разглашение информации любого плана, содержащую сведения о личной тайне конкретного гражданина.

Так ст. 155 УК РФ[4] предусмотрена ответственность за разглашение тайны усыновления или удочерение, так как информация такого рода относится к личной тайне конкретно взятой семьи.

Вместе с этим, органы ЗАГС также не имеют права на разглашение информации такого рода посредством выдачи дубликата свидетельства об усыновлении, в том числе усыновленному лицу. Такой документ имеют право получить только родители указанного лица.

К семейной – личной информации относятся сведения, касающиеся семейного положения, состояния здоровья, денежного положения и т.д.

---

[1] Гражданский кодекс Российской Федерации: федер. закон от 30 ноября 1994 г. № 51–ФЗ. URL: http:// www.pravo.gov.ru (дата обращения: 20.12.2024).

[2] Уголовный кодекс Российской Федерации: федер. закон от 13 июня 1996 г. № 63–ФЗ. URL: http:// www.pravo.gov.ru (дата обращения: 20.12.2024).

[3] Конституция Российской Федерации. URL: http://pravo.gov.ru (дата обращения: 20.11.2024).

[4] Уголовный кодекс Российской Федерации: федер. закон от 13 июня 1996 г. № 63–ФЗ. URL: http:// www.pravo.gov.ru (дата обращения: 20.12.2024).

Однако, не все сведения, относящиеся к частной жизни человека, являются охраняемой законом информацией, данный вопрос решается судом в каждом конкретном случае индивидуально, принимая во внимание все обстоятельства совершенного преступного деяния.

Федеральный закон «Об оперативно–розыскной деятельности[1]» гарантирует сохранение тайны имени лиц, внедренных в организованные преступные группы, штатных негласных сотрудников органов, осуществляющих оперативно–розыскную деятельность, а также лиц, оказывающих или оказавших содействие этим органам на конфиденциальной основе.

Из содержания норм данного федерального закона мы видим, что сведения, указанные выше являются охраняемой законом информацией, за распространение которой наступает уголовное наказание.

Таким образом, предметом преступления, предусмотренного ст. 272 УК РФ[2] являются нематериальные ценности, в частности, компьютерная информация, охраняемая законом, такие как конфиденциальные сведения о персональных данных, сведения, составляющие служебную, коммерческую, банковскую или государственную тайну, информация, являющаяся объектом авторского права.

Неправомерное завладение компьютерной информацией общего пользования, не находящейся под защитой законодательства РФ не образует состава преступления, предусмотренного ст. 272 УК РФ[3].

Также стоит учитывать, что анализ предмета преступления в разрезе от объекта посягательства не дает определить отношение, которому наносится ущерб, что, в свою очередь, может порождать ошибки при квалификации

---

[1] Об оперативно–розыскной деятельности: федер. закон от 12 августа 1995 г. № 144–ФЗ. URL: http:// www.pravo.gov.ru (дата обращения: 20.12.2024).

[2] Уголовный кодекс Российской Федерации: федер. закон от 13 июня 1996 г. № 63–ФЗ. URL: http:// www.pravo.gov.ru (дата обращения: 20.12.2024).

[3] Уголовный кодекс Российской Федерации: федер. закон от 13 июня 1996 г. № 63–ФЗ. URL: http:// www.pravo.gov.ru (дата обращения: 20.12.2024).

преступлений и, следовательно, ведет к несоответствию с основополагающими принципами уголовного права: законности и справедливости.

Объективная сторона преступления, предусмотренного ч. 1 ст. 272 УК РФ, выражается в неправомерном доступе к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы Электронно-вычислиительной машиины (далее ЭВМ), системы ЭВМ или их сети.

Для привлечения лица к ответственности по указанной статье необходимо установить факт неправомерного действия, выраженный именно в активных действиях. Данное свидетельствует о том, что обязательным элементом объективной стороны рассматриваемого преступления является неправомерность доступа к защищённой законом информации. Однако, способ совершения преступления на правовую оценку преступления не влияет.

Одним из способов совершения неправомерного доступа к компьютерной информации является его совершение с применением насилия над личностью либо с угрозой его применения.

Данное характерно, например, для ситуаций, когда преступник не владеет знаниями в области информационных технологий и применяет насилие над владельцем информации, чтобы последний совершил преступление в отношении имеющей для него значение информации.

Так диспозиция ст. 272 УК РФ не охватывает насилие, следовательно, в данном случае преступление будет квалифицировано по совокупности с преступлением против личности.

При такой квалификации действия лица, которого заставили совершить преступление находятся под сомнением. Так в случае нахождения последнего в состоянии крайней необходимости его действия будут квалифицированы по ст. 39 УК РФ. Однако, могут быть случаи квалификации таких действий и как соучастника, и по совокупности преступлений.

Однако, квалифицировать действия третьего лица в качестве соучастника можно лишь в случае не нахождения его в состоянии крайней необходимости и направления в его адрес угроз легкого вреда либо побоев.

Уголовное законодательство РФ не предусматривает квалифицированных составов преступлений против компьютерной информации. Но необходимо иметь ввиду, что компьютерные преступления не всегда являются самостоятельными преступлениями, а могут выступать способом совершения другого противоправного деяния. Так, например, посредством доступа к определённой компьютерной информации может быть совершено преступление против собственности. Здесь персональный компьютер выступает в качестве орудия совершения преступления против собственности. Следовательно, в данном случае преступления здесь будут квалифицироваться по совокупности.

При расследовании рассматриваемого рода преступлений у правоохранительных органов возникает ряд сложностей по определению места совершения преступления, так как в большинстве случаев преступник совершает преступление посредством ЭВМ в одном месте, а последствия и потерпевшие лица находятся в другом месте, иногда и в другой стране.

Так считаем необходимым детально рассмотреть место и время совершения преступления, направленного против компьютерной информации.

Если рассматривать время совершения преступления, то необходимо обратиться к ст. 9 УК РФ, где определено, что временем совершения преступления является время действий или бездействий преступника, иными словами, законодатель не акцентирует внимание на последствиях, следовательно, их наступление или не наступление совершенно не важно.

Что нельзя сказать о месте совершения преступления, здесь дела обстоят несколько иначе, определение места совершения компьютерных преступлений сегодня является спорным в правовом поле.

Первая точка зрения состоит в том, что местом совершения преступления является та территория и государство, где таковое было закончено. Состав

преступления рассматриваемых преступлений может считаться полным только при наличии вредных последствий, так как данный раздел подразумевает только материальные составы по смыслу уголовного законодательства.

Вторая точка зрения является совершенно иной, так как полностью отличается от предыдущей, согласно этого мнения ответственность должна наступать в месте совершения преступного деяния, не зависимо от места наступления последствий от совершенного преступного деяния. По нашему мнению, такой подход не будет верным, по причине того, что в случае совершения преступления территориально в разных местах, на основании уголовного законодательства ответственность наступает в месте окончания преступления, а, следовательно, и наступления вредных последствий. Иными словами, место нахождения участников преступления не имеет значения для наступления ответственности, так как она наступает по законодательству того государства, к котором преступное деяние было окончено.

Также необходимо иметь ввиду, что законодательство далеко не всех стран мира регламентирует ответственность за совершение рассматриваемого состава преступления, в случае если преступники пытаются применить в своих целях данный пробел, то им стоит иметь ввиду, что в случае направления преступления на интересы представителей страны, имеющей в своём законодательстве вышеизложенные составы, то ответственность будет применяться именно того государства в котором было окончено преступное деяние и наступили общественно–опасные последствия.

Согласно действующему уголовному законодательству РФ наличие последствий преступного деяния в рассматриваемом составе преступления обязательно, также обязательным признаком состава преступления здесь является и причинно–следственная связь между действием и последствиями данного преступного действия.

Говоря о общественно–опасных последствиях рассматриваемого вида преступлений, обратимся к судебной практике. Согласно апелляционной жалобе, поданной адвокатом гр. К в защиту осужденного гр. Л

по ч.1 ст. 183 УК РФ и ч. 3 ст. 272 УК РФ, адвокат считает, что выводы суда о виновности осужденного основаны на предположениях. В приговоре не установлены общественные опасные последствия от преступления, предусмотренного ст. 272 УК РФ, какой вред причинен потерпевшей стороне. Однако, суд приходит к выводу, что вина гр. Л. в совершении преступлений, обоснованно подтверждается совокупностью доказательств, содержащихся в материалах уголовного дела, которые полно, всесторонне исследованы судом. Таким образом, апелляционная жалоба адвоката оставлена без удовлетворения[1].

Далее перейдём к анализу причинно–следственной связи между проступком и последствиями в виде копирования, уничтожения и т.д., так как наличие причинно–следственной связи обязательно для преступления, направленного против компьютерной информации.

Под причинно–следственной связью в уголовном праве РФ понимается явление, при котором причина обоснованно порождает следствие. Применительно к рассматриваемому виду преступлений неправомерный доступ к защищаемой законом компьютерной информации влечёт такие негативные последствия как – копирование, уничтожение, блокирование и иное, регламентированное ст. 272 УК РФ.

§ 2. Основные элементы криминалистической характеристики преступлений в сфере компьютерной информации

Появление преступлений в компьютерной сфере очень тесно связано с таким явлением как «хакеры». Хакерами выступают пользователи электронно–вычислительных машин, систем ЭВМ, сети таких ЭВМ, деятельность которых направлена на несанкционированный доступ к охраняемой законом компьютерной информации.

---

[1] Аппеляционное постановление Московского областного суда от 20.08.2024 г. ULR: https://sudact.ru/regular/doc/dWgQxopbXPrj/ (дата обращения 17.03.2025).

Именно хакеры имеют высокие знания и навыки в сфере компьютерных технологий, которые постоянно совершенствуются, что делает деятельность правоохранительных органов по расследованию преступлений в области компьютерных технологий наиболее сложной. Хакеры в широком смысле этого слова – это компьютерные правонарушители, а иногда и преступники.

Всех лиц, обладающих определенными познаниями в области компьютерных технологий в той или иной мере, объединяет сеть Интернет, где они получают возможность воспользоваться запрещёнными сайтами, с целью получения или обучения новым знаниям, вербовки друг друга на выполнение преступных действий, рекламы услуг преступной направленности.

В сети интернет хакер может иметь доступ к электронных ресурсам, позволяющим удалённо найти исполнителя для своих преступных целей, что является благоприятной средой для распространения преступлений в сфере компьютерных технологий.

Данное способствует вовлечению молодых слоёв общества в противоправную деятельность в области компьютерных технологий.

Сеть Интернет позволяет преступникам в сфере информационных технологий обмениваться опытом совершения и сокрытия преступлений в области информационных технологий. Более того взаимодействие здесь происходит не только с отечественными преступниками, но и с зарубежными коллегами.

Объектом криминалистической исследования преступлений в сфере компьютерных технологий является личность преступника. Следует отметить, что исследование криминологами особенностей личности данных преступников охватывает лишь их черты, которые будут способствовать профилактике рассматриваемого вида преступлений. В свою очередь, такое ограниченное изучение личности преступника не способствует раскрытию преступлений, так как ряд особенностей личности преступника остаются неисследованными криминологами.

Здесь прежде всего, стоит отметить оставление без внимания особых навыков преступников, которые свидетельствуют о способе совершения преступления и являются почерком преступника. Именно это позволяет при расследовании преступлений в области компьютерных технологий наиболее оперативно выявить следы преступника на месте преступления[1].

Все найденные на месте преступления вещественные доказательства и иные следы преступления позволяют судить о личности преступника, о его навыках и профессиональном опыте, взаимоотношении с потерпевшим и т.д.

В криминалистике «компьютерных преступников» принято классифицировать на несколько групп:

1) Профессиональные преступники в сфере информационных технологий. Преступники данной группы совершением преступления самоутверждаются именно это толкает человека на совершение преступления.

Преступники данной группы очень умны, наделены особыми интеллектуальными данными, позволяющими обходить различные средства защиты при проникновении в электронную вычислительную машину.

Так называемым катализатором преступных намерений такого рода преступников является любого рода улучшение и совершенствование компьютерных систем и защиты данных в сети Интернет, которое мотивирует преступника на совершение преступления, так как последний должен показать своё превосходство над системой.

Большое значение здесь имеет тот факт, что преступники данной группы не имеют профессиональной подготовки для совершения преступления, так как способу совершения преступления характерна оригинальность и новизна совершения, более того методы по сокрытию преступления чаще всего не применяются[2].

---

[1] Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. М.: Норма. 2020. С. 7.

[2] Панфилова Е. И. Компьютерные преступления: учеб. пособ., 2020. С. 69.

2) Лица, имеющие психическое заболевание такое как – информационная болезнь, а также компьютерные фобии.

Информационная болезнь – является одним из новых видов психических заболеваний изучением которого занимается новая отрасль – информационная медицина[1].

Развитие информационных технологий пришло к тому, что практически каждый человек на своём рабочем месте вынужден работать на персональном компьютере, так как это способствует эффективности производимых им манипуляций, в связи с этим, очень много работников подвергаются информационному давлению, что создает для них стрессовые ситуации, которые могут послужить источником фобии в дальнейшем. Таким образом, персональный компьютер выступает в качестве источника профессионального заболевания.

Преступники данной группы преступлений совершают преступления, как правило, при частичной или полной потере контроля над своими действиями, поэтому при расследовании компьютерных преступлений в случае подтверждения факта страдания лицом, указанным заболеваем следует в обязательном порядке назначить судебную психиатрическую экспертизу.

3) Профессиональные преступники в области компьютерной информации, преследующие корыстные цели. Особенность преступников данной группы преступлений состоит в многократности совершения преступлений и обязательном сокрытии его следов. Для таких преступников характерно наличие высоких преступных навыков.

Преступники профессионалы, как правило, реализовывают свой преступный умысел в составе группы, где обязательно есть программисты, юристы, экономисты, что создает наибольшую опасность для компьютерной информации.

---

[1] Сальников В. П. Компьютерная преступность: учеб. пособ., 2020. С. 126.

Особенность преступников данной группы состоит в том, что они являются наёмными сотрудниками из числа руководящих должностей и имеющие доступ к информации и электронной вычислительной машине. В качестве таковых преступников могут быть как наёмные сотрудники автозаправочных станций, так и сотрудники банков.

Далее справедливо перейти к рассмотрению обстановки и мотивов совершения компьютерных преступлений.

Под обстановкой преступления принято понимать конкретные условия, оказывающие влияние на субъект и на объект преступления. С помощью подробного изучения обстановки преступления можно сделать выводы о личности преступника, способе совершения преступления. Более того, изучение обстановки преступного события позволяет определить обстоятельства, способствующие совершению преступления.

Рассмотрение любого преступления, в частности, преступления в области компьютерной информации нельзя не обратиться к изучению вины, мотивов, цели преступного поведения. Так как именно посредством анализа именно этих составляющих сотрудники правоохранительных органов получают возможность увидеть целостную картину психического состояния конкретного преступника.

Человек не имеющий цели на совершение преступления, не может иметь мотив, а, следовательно, и желание совершить преступление. Мотив является движущим элементом для совершения преступления лицом.

В зависимости от вида преступника их мотив будет отличаться. Именно мотив оказывает влияние на то каким способом будет совершено преступление.

Вместе с этим, мотив определяет и то какие средства и действия следует применять преступнику при совершении преступления. Мотив имеет важную роль при расследовании преступлений в области компьютерной информации, хотя и не является обязательным элементом состава преступления.

Наиболее распространёнными мотивами совершения преступлений в области компьютерной информации являются – с корыстной целью,

преследующие политические цели, месть, хулиганские соображения, а также преследующие только профессиональный (исследовательский) интерес.

Анализ мотивов позволяет судить о том, что преступления, совершённые с политическим мотивом и с целью материальной выгоды, отличаются наиболее изощрёнными методами совершения и сокрытия компьютерных преступлений.

Преступники непрофессионалы чаще всего совершают преступление, не имея на то определённой цели, именно они по большей мере являются изобретателями и первопроходцами способов совершения и сокрытия компьютерных преступлений, так как компьютер для них служит предметом для игр и анализа своих способностей.

Основная цель преступников, относящихся к группе лиц, имеющих информационное заболевание – это уничтожение ЭВМ, которая выступает для них раздражителем. Как правило, преступника данной группы совершают преступление в составе аффекта либо невменяемости.

Обстановка совершения преступления в области компьютерной информации включает в себя такие факторы как – производственные, социальные, материальные.

Рассмотрение причинно–следственной связи между действием и последствиями совершения компьютерных преступлений следует начать с анализа и классификации способов и видов преступлений, совершенных в отношении компьютерной информации.

Незаконное копирование информации один из наиболее распространённых способов совершения компьютерных преступлений, для которого характерно перемещение информации с одного электронного носителя информации на другой.

Следующий способ – это уничтожение и блокирование защищаемой законом информации, которое влечёт бесследное исчезновение защищаемой информации и её недоступность по причине закрытия донного допуска посредством технических средств.

Незаконное модифицирование защищаемой законом информации – это способ совершения преступления, состоящий в таком изменении имеющейся информации при котором её сущность не меняется.

Из изложенного следует, что в качестве вредных последствий совершения рассматриваемого вида преступления могут быть:

– нарушение работы компьютерной техники;

– вывод ЭВМ путём модификации или иного нарушения компьютерной информации;

– нарушение целой сети персональных компьютеров путём незаконной модификации файлов операционной системы ЭВМ.

Наступление одного из выделенных вредных последствий является основанием для утверждения об окончании преступления против компьютерной информации.

Что касается приготовления к преступлению против компьютерной информации то здесь стоит отметить, что за такие действия уголовная ответственность не предусмотрена по причине небольшой тяжести преступления.

Необходимо подробно остановиться на рассмотрении способов совершения преступлений, направленных против компьютерной информации.

Первым способом совершения рассматриваемого вида преступления является непосредственный доступ к компьютерной информации, а также дистанционный.

Первый способ совершения преступления, как правило, сопряжен с совершением иных преступлений, так как требует непосредственного доступа к ЭВМ, которая должна быть изъята у правообладателя. В результате совершения преступления таким способом могут быть оставлены следы взлома, повреждения или уничтожения охранной сигнализации и т.д.

При дистанционном методе совершения преступления применяются промежуточные средства связи, персональные компьютеры с помощью которых происходит посягательство на защищаемую законом информацию. Для данного

способа также характерно применение специальных компьютерных программ, вирусов, средств подбора пароля и т.д. Следами преступления, совершённого таким способом могут быть информация, полученная с помощью регистрирующих и пеленгующих средств связи и др.

Ещё одним способом является фальсификация данных для замены доступа и дальнейшего управления информацией или её носителями. Данный способ имеет большое распространение в области экономических преступлений, совершаемых в целях получения денежных средств посредством доступа к банковским счетам. Оставленными следами в данном случае могут быть несовпадения первичных данных.

Способ, посредством которого осуществляется уничтожение и блокирование информации – создание вредоносных программ. В том числе, метод незаконного распространения носителей защищаемой законом компьютерной информации. Следами преступления могут быть – сбои и иные нарушения в работе ЭВМ или сети ЭВМ, изменение или модификация, блокировка информации, расположенной на машинном носителе и др.

Пятая группа способов совершения рассматриваемого вида преступлений выражается в форме распространения, продажи, проката, аренды, а также создания условий для распространения программ для ЭВМ или носителей информации, являющихся контрафактными, содержащими запрещённую уголовным правом информацию или нарушающими авторские права.

Вместе с этим, указанные методы могут быть применены злоумышленником в комплексе, данное будет зависеть от цели преступления.

При расследовании преступлений, совершенных с применением комплексного использования методов, стоит иметь ввиду, что всегда один метод будет доминировать над другим, то есть первый наиболее подходящий, а второй используемый для реализации отдельных целей.

Личность преступника, совершающего неправомерный доступ к компьютерной информации, обладает рядом специфических черт. Преимущественно это мужчины в возрасте от 19 до 25 лет, характеризующиеся

высоким интеллектуальным уровнем, нестандартностью мышления, профессионализмом и скрытностью. Они являются уверенными пользователями компьютерной техники и обладают специальными познаниями в области информационных технологий, включая языки программирования, программное обеспечение и аппаратную часть устройств, часто применяя для общения профессиональный жаргон, обеспечивающий латентность их действий для непосвященных.

Преступник, как правило, имеет техническое образование, беспрепятственный доступ к компьютерам и сети Интернет, а также владеет набором программно–аппаратных методов, облегчающих совершение преступления. В случаях преступлений против юридических лиц исполнителем или пособником нередко выступает сотрудник организации (например, инженер–программист, системный администратор), имеющий легальный доступ к служебным системам.

Особого внимания заслуживает классификация преступников по степени вовлеченности:

– Начинающие (18–30 лет) обладают средним достатком, техническим образованием и существенными познаниями в ИТ.

– Устойчивые (20–25 лет) имеют высшее или неоконченное высшее техническое образование, доход средний или выше среднего, глубокие системные знания в сфере компьютерных технологий[1] и программирования; они часто работают в ИТ–сфере, что может облегчить доступ к данным жертвы.

– Профессиональные (старше 25 лет) обладают экспертной подготовкой, навыками программирования на нескольких языках, глубокими знаниями ПО, нередко имеют второе образование (юридическое или экономическое) и связи в государственных структурах; их легальная работа (часто в ИТ–отделах крупных компаний или госорганов) служит прикрытием (алиби), тогда как основной доход получается в полукриминальной или криминальной среде.

---

[1] Федотов Н. Н. Форензика – компьютерная криминалистика. М. 2012. С.16.

Для профессионалов характерно постоянное совершенствование методов противоправной деятельности. Мотивация преступников ярко выражена как корыстная, а сами преступления часто совершаются устойчивыми группами с четким распределением ролей, высокой мобильностью, технической оснащенностью и продуманной системой сокрытия следов. При этом современное развитие информационной сферы привело к тому, что преступнику не всегда требуются глубокие познания – порой достаточно общих навыков, подкрепленных инструкциями из сети и несоблюдением мер безопасности жертвой.

Механизм следообразования при неправомерном доступе к компьютерной информации обладает значительной спецификой. Следы преступления являются прежде всего результатом изменений, вносимых преступниками в охраняемую законом информацию в процессе ее уничтожения, модификации, копирования или блокирования.

Ключевое значение имеют цифровые следы – зафиксированные в виде цифрового образа изменения состояния информации в памяти электронных устройств, вызванные алгоритмом ПО и связанные с событием преступления.

В отличие от традиционных, цифровые следы легко уничтожаются (умышленно или случайно), воспринимаются только через систему аппаратно–программных средств (что затрудняет их демонстрацию в суде), и их неизменность не всегда может быть гарантирована из–за методов хранения со сменой носителей, программных сбоев или технических ошибок.

Характерной чертой является их географическая распределенность: следы часто обнаруживаются одновременно в разных местах, удаленных друг от друга (например, на рабочем месте жертвы, сервере, месте хранения резервных копий).

Процесс следообразования включает стадии:

1) физическое проявление свойств следообразующих объектов (данные, изображение, звук, время);

2) предварительную обработку, передачу и хранение цифровой информации;

3) изъятие информации на электронный носитель. Типичные следообразующие действия и оставляемые следы разнообразны. При осуществлении DoS/DDoS–атак (вызывающих «зависание» или «обрушение» сайта/сервера, что является блокированием информации) на компьютере преступника остается специализированное ПО для атак и следы его эксплуатации (логи, кэш).

Взлом сайтов, электронной почты или хранилищ данных (с целью модификации или уничтожения информации) путем поиска уязвимостей оставляет следы вмешательства на атакованной системе, а на ПК злоумышленника – измененную страницу, ПО для поиска уязвимостей и взлома со следами использования.

Для сокрытия своей деятельности преступники применяют вымышленные электронные адреса, ремейлеры, анонимайзеры (изменяющие данные об отправителе) или используют второй почтовый ящик; следы этих действий – конфигурации ПО и логи подключений (часто позволяющие, несмотря на анонимизацию, установить реальный IP–адрес компьютера отправителя).

К материальным следам относятся рукописные записки, распечатки, свидетельствующие о подготовке, а также следы пальцев рук и микрочастицы на компьютерной технике и носителях.

Идеальные следы представляют собой отражение события преступления и его механизма в сознании и памяти людей (психофизиологической природы), проявляющееся в виде мысленных образов.

Личность потерпевшего (обладателя информации) при неправомерном доступе к компьютерной информации может быть представлена как физическим лицом (гражданином), так и юридическим лицом, Российской Федерацией, субъектом РФ или муниципальным образованием (от их имени права осуществляют госорганы и органы местного самоуправления).

Обладатель информации вправе разрешать или ограничивать к ней доступ, определять порядок и условия такого доступа, защищать свои права законными

способами, но и обязан принимать адекватные меры по ее защите. Степень защиты конфиденциальной информации должна соответствовать ее ценности для обладателя; меры признаются достаточными, если исключают доступ к информации без согласия владельца. Эти меры включают организационные, юридические и специальные технические решения, затрудняющие доступ третьих лиц. Несоблюдение данных требований безопасности со стороны потерпевшего часто облегчает задачу преступнику.

Особую группу потерпевших составляют владельцы банковских счетов и карт. Совместный анализ данных кредитных организаций, проведенный специалистами служб информационной безопасности банков, психологами и представителями Банка России, позволил выделить пять основных типов жертв[1]:

1) Индивидуалисты – финансово благополучные лица, легко тратящие деньги на себя и удовольствия, излишне доверяющие новым технологиям;

2) Школьники, студенты, лица с особенностями социальной адаптации – доверчивые, расточительные, импульсивные, склонные к риску, с противоречивой самоидентификацией;

3) Бюджетораспорядители семей с невысоким уровнем дохода и высокой финансовой нагрузкой – целеустремленные, высоко ценящие семейные и дружеские связи, ответственные;

4) Домохозяйки – уступчивые, доверчивые, с выраженным внешним локусом контроля (ориентированные на внешние обстоятельства);

5) Пенсионеры[2];

Таким образом, проведённый анализ показывает эффективные способы совершения; личность преступника; механизм следообразования; личность потерпевшего; рассматриваемого вида преступления необходимо, прежде всего,

---

[1] Валькова Т. В., Шуин В. Э., Долгаев В. В. Методика расследования преступлений против собственности: метод. рекомен. СПб.: Издат. СПб ун-та МВД России. 2020. С. 18.

[2] Информация Банка России от 28.09.2020 г. «Основные направления развития информационной безопасности в кредитно-финансовой сфере на период 2019-2021 гг.». URL: https://www.garant.ru/products/ipo/prime/doc/74615166/ (дата обращения: 21.04.2025).

для того, чтобы в процессе самого расследования преступления установить имеющие значение для расследования преступления обстоятельства.

Все эти факторы могут оказывать влияние на способы и условия совершения преступления, определять уровень доступа к компьютерной информации, возможность совершения преступления.

Таким образом, в криминалистическую характеристику компьютерных преступлений входят такие составные элементы как – личность преступника, его мотив, цель, способы совершения, а также обстановка совершения преступления.

ГЛАВА 2. ОСОБЕННОСТИ И МЕТОДЫ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Обстоятельства, подлежащие установлению и доказыванию

Преступления, связанные с компьютерной информацией, являются новыми, но в то же время имеют большое распространение в нынешних реалиях, в связи с развитием сферы ИТТ, которое способствует появлению различных способов и методов совершения преступлений рассматриваемого вида, а также иных преступлений.

Уголовное законодательство РФ объединяет все преступления в области информационных технологий в главе 28 «Преступления в сфере компьютерной информации», данная глава содержит общественно–опасные деяния, предусмотренные ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации»[1].

Однако, проведенный опрос среди следователей и дознавателей показал, что чаще всего приходится расследовать такие преступления в сфере информационных технологий как – мошенничество в сфере компьютерной информации (ст.159.6 УК РФ), кража (ст. 158 УК РФ), неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ (ст. 242 УК РФ)[2].

---

[1]Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63–ФЗ. – Текст: электронный // Официальный интернет–портал правовой информации: – URL: http:// www.pravo.gov.ru (дата обращения: 20.12.2024).

[2] Там же ст. 242 УК РФ.

В широком смысле киберпреступление – это любое преступление, совершенное в электронной среде[1].

Наряду с этим стоит отметить, что в последние годы все чаще совершаются мошенничества с использованием средств связи. На практике существенной проблемой здесь является своевременность принятия решения по сообщениям о данного вида преступлениях. По причине того, что звонки потерпевшему могут поступить от преступника, находящегося в любом из субъектов РФ, имеет место быть затягивание принятия решения по материалу проверки, так как материалы переправляются по разным субъектам, тем самым происходит нарушение права заявителя на своевременное и оперативное рассмотрение поданного им заявления[2].

Одной из основных причин высокой общественной опасности преступлений, направленных на компьютерную информацию, является именно территориальная свобода совершения преступлений.

Ситуация несколько усугубляется в связи с отсутствием разработанной нормативной базы в области компьютерных преступлений, как выше отмечалось, рассматриваемые составы преступлений являются новыми и в законодательстве они появились с момента вступления в законную силу Уголовного кодекса 1997 года.

Стоит отметить, что действующий уголовный закон РФ защищает частные права граждан на защиту информации, так как до 01.01.1997 года законом защищалась исключительно государственная тайна.

Также следует отметить, что специфичность преступлений, направленных на компьютерную информацию состоящая в особенностях технического характера не делает указанный вид преступлений наиболее простым для расследования и предотвращения. Так как зачастую, сотрудники

---

[1] Шевко Н. Р., Каримов А. М., Турутина Е. Э. Преступления, совершаемые с использованием высоких технологий и коммуникаций: учеб. посо. Казань. 2020. С. 18.

[2] Теппеев А. А.. Особенности расследования преступлений, связанных с мошенническими действиями, совершёнными с использованием средств сотовой телефонной связи: учеб. посо. Краснодар. 2021. С. 46.

правоохранительных органов не обладают достаточными знаниями в области ИТТ.

В частности, преступления, посягающие на компьютерную информацию, как правило, совершаются в совокупности с иными. Для подтверждения такового обратимся к Апелляционному постановлению Верховного Суда Республики Крым, поданному защитником Н на постановление Киевского районного суда г. Симферополь о замене меры пресечения в отношении гр. А. Согласно данному, гр. А. обвиняется в распространении заведомо ложных сведений, порочащих честь и достоинство других лиц и подрывающих их репутацию, а именно заместителя председателя Совета Министров Республики Крым гр. Б и главного врача ГБУЗ РК «Республиканской клинической больницы» гр. В, совершённом публично с использованием информационно–телекоммуникационных технологий, соединённое с обвинением последних в совершении тяжких и особо тяжких преступлений. Таким образом, по данному факту в отношении гр. А возбуждено уголовное дело по ч. 5 ст. 128.1 УК РФ.

В частности, гр. А. был совершен неправомерный доступ к защищаемой законом компьютерной информации, содержащейся в системе электронного документооборота Министерства здравоохранения Республики Крым, в связи с этим в отношении последней возбуждено уголовное дело по признакам преступления, предусмотренного ч. 3 ст. 272 УК РФ[1].

Следующим примером является Приговор Балашихинского городского суда в рамках которого гр. Г. Признан виновным в собирании сведений, составляющих банковскую тайну, путем обмана, а также в неправомерном доступе к охраняемой законом компьютерной информации, повлекшей копирование компьютерной информации, совершенным лицом с использованием своего служебного положения. Таким образом, в отношении гр. Г. Было выдвинуто обвинение по признакам преступлений, предусмотренных

[1] Апелляционное постановление №22К – 2839/ 2024 от 30.08.2024 г. URL: https://sudact.ru/regular/doc/hv3CZjqqBRJl/ (дата обращения 17.03.2025).

ч. 1 ст. 183 УК РФ и ч. 3 ст. 272 УК РФ[1].

Таким образом, выше изложенные сложности приводят к проблемам расследования преступлений в области компьютерной информации, а также к необратимым последствиям нарушения принципов справедливости и законности судопроизводства на этапе судебного процессе.

Первая глава дипломного исследования содержит все обязательные элементы состава преступления, направленного на компьютерную информацию, а, чтобы доказать наличие того или иного элемента состава преступления необходимо доказать ряд обстоятельств.

Наиболее важным из таковых является – доказывание самого факта совершения преступления. Возможны случаи, когда негативные обстоятельства могут наступить не в результате преступления, а в результате поломки в таком случае состав преступления будет отсутствовать. Иными словами, первостепенно необходимо выявить было ли в отношении компьютерной информации совершено противоправное деяние.

После установления и доказывания факта преступного воздействия на охраняемую законом компьютерную информацию, необходимо установить, действительно ли посягательство совершено на информацию, находящуюся под охраной закона. Основное обстоятельство – это содержание и назначение информации, на которую произведено посягательство. К какой именно категории отнесена информация такого рода – общедоступная или же, находящаяся под охраной закона.

Правоохранительные органы устанавливают форму предоставления информации, её индивидуальные признаки и признаки, указывающие на носитель информации, в отношении которой совершено преступное посягательство.

Вместе с этим следует установить статус и содержание информации, содержащейся на машинном носителе и предмет преступного посягательства.

---

[1] Приговор Балашихинского гор. суда от 23.02.2024 г. ULR: https://sudact.ru/regular/doc/dWgQxopbXPrj/ (дата обращения 17.03.2025).

Что касается времени и места совершения преступления то оно определяется на основании норм уголовного права, что было описано в первой главе данной работы.

В каждом случае расследования преступления следует определить способ совершения, в рамках чего подлежит анализу способ доступа к предмету, способ обхода защиты предмета, метод воздействия, который был объектом исследования ранее.

В силу того, что преступление в отношении компьютерной информации было совершено нужно провести анализ режима работы с информацией такого вида, определить используемые способы её защиты, выявить причину нарушения безопасности, которая способствовала совершению преступления.

Не лишним также будет установление предмета с помощью которого было совершено преступление, а именно кода, шифра и др.

При расследовании преступлений рассматриваемого вида существенным будет выявление фактов утечки конфиденциальной информации от сотрудников. Данное необходимо для того, чтобы исключить участие должностных лиц потерпевшей стороны в совершении расследуемого преступления.

Отдельного внимания заслуживает вопрос об определении размера материального ущерба, причинённого в результате совершения преступления в сфере компьютерной информации. В данном случае размер материального ущерба определяется исходя не только из стоимости охраняемой законом информации, но и стоимости системы, средств, затраченных на защиту, стоимость самого машинного носителя предмета преступления. Также в сумму материального ущерба входит суммы недополученной прибыли, в виду невозможности применять информацию, на которую осуществлено преступное посягательство.

Если же был причинён не материальный ущерб, то необходимо установить кому именно, кем и как будет возмещён.

После установления, всего выше перечисленного сотрудники правоохранительных органов переходят к определению наличия или отсутствия квалифицирующих признаков преступления, а именно:

– в совершении преступления участвовала группа лиц по предварительному сговору или организованная группа;

– в совершении преступления подозревается лицо, совершившее последнее с использованием своего служебного положения;

– преступление совершено лицом, располагающим доступом к ЭВМ, системе ЭВМ или их сети;

– преступление повлекло наступление тяжких последствий по неосторожности.

Далее сотрудники переходят к установлению сведений о личности преступника, а именно анкетные данные, сведения о семейном положении, окружении, вид трудовой деятельности, были ли ранее совершены им преступления и т.д. Также следует определить физические и физиологические данные преступника – рост, особые признаки внешности человека, особые приметы, как одевается и т.д. Отдельное внимание необходимо обратить уровню психологического развития преступника, уровень его знаний, навыков, умений, наличие фобий, склонностей к чему либо и т.д. Далее следует определить соучастников преступления.

Если установлено, что преступление совершено организованной группой, то необходимо установить её признаки – когда была организована, какой период уже существует, распределение ролей между членами организованной преступной группы, какова основная цель организованной преступной группы.

После этого устанавливаются отношения внутри организованной преступной группы между её участниками, а именно имеются ли какие–либо поощрения, наказания, общие денежные и иные материальные средства, наличие технической оснащённости, вооружения.

Имеются ли коррумпированные связи с правоохранительными органами и иными силовыми структурами, покровители.

Цель и мотив совершения преступления организованной преступной группой являются обязательными к установлению.

Далее проводится работа с потерпевшим, устанавливаются в все сведения о нём, имеющие значение к расследуемому преступлению.

Если потерпевшим является юридическое лицо, то установлению подлежит: название; адрес; форма собственности; вид хозяйственной деятельности; сведения о руководителе (–ях) и главном бухгалтере; данные о лице, ответственном за получение, хранение, обработку, передачу, уничтожение или защиту компьютерной информации, подвергшейся преступному воздействию, либо ее машинных носителей.

Если же физическое: анкетные; учетные; физические; физиологические; психолого–психические; оформление внешности; круг связей лица.

Далее следует доказать виновность лица в совершении конкретного преступления в области компьютерной информации.

В случае не установления причастного к совершению преступления лица необходимо акцентировать внимание на выявлении информации о преступлениях в области компьютерной информации, совершённых ранее аналогичным способом, о лицах причастных к данным преступлениям и т.д.

Выявление перечисленных выше обстоятельств расследуемого уголовного дела реализуется правоохранительными органами путем проведения следственных действий, оперативно– розыскных и иных мероприятий.

Вместе с этим, большое значение в уголовно–процессуальном доказывании преступлений, связанных с посягательством на компьютерную информацию, имеет использование информации, содержащейся на электронных носителях.

К сожалению, практика применения уголовно–процессуальных положений законодательства в части собирания доказательств на электронных носителях информации указывает на наличие проблем. Наиболее типичными из которых являются следующие:

– определение оснований для изъятия электронных носителей информации в ходе производства следственных действий;

– законодательно закрепленное императивное требование участия специалиста;

– обеспечение реализации права на копирование информации, содержащейся на изъятых электронных носителях.

Для более подробного понимания выдвинутых проблем необходимо обратиться к практике применения уголовно–процессуального законодательства в рассматриваемой области.

Изъятие электронных носителей информации по общему правилу по уголовным делам в сфере экономической и предпринимательской деятельности не допускается, однако, есть исключения.

1) произвести изъятие электронных носителей информации в рамках следственного действия по уголовному делу возможно, но только в случае вынесения постановления о назначении в отношении электронных носителей информации судебной экспертизы. Однако, данное основание очень плохо реализуется на практике, так как при назначении судебной экспертизы и составлении постановления о назначении таковой все объекты, предоставляемые на исследование специалисту должны быть уже изъяты и быть в распоряжении следователя, а в данном случае получается. Более того согласно нормам УПК РФ, все заинтересованные лица по уголовному делу должны быть ознакомлены с постановлением о назначении экспертизы до её производства (ч. 3 ст. 195 и ч.1 ст. 198 УПК РФ).

2) Электронные носители информации могут быть подвергнуты изъятию на основании судебного решения. Таковыми судебными решениями могут быть, указанные в п.5 ст. 29 УПК РФ, то есть о производстве обыска и (или) выемки в жилище в процессе которых производится изъятие электронных носителей информации, а также указанные в п. 7 ст. 29 УПК РФ.

Указанное подтверждается судебной практикой рассмотрения жалоб на действия следователя при изъятии и осмотре информации с мобильных

телефонов, которые могут содержать сведения, относящиеся к охраняемой законом тайне.

Согласно Кассационному определению Омского областного суда ст. 13 УПК РФ предусмотрено, что ограничение права на тайну переписки, телефонных и иных переговоров возможно исключительно на основании решения суда. Право на тайну переписки гарантировано Конституций РФ, а именно ст. 23. Также ст. 8 Конвенции о защите прав человека и основных свобод определяет, что каждый гражданин имеет право на уважение его личной и семейной жизни, жилища и корреспонденции. Несмотря на то, что гл. 25 УПК РФ прямо не указывает на получение судебного решения следователем на осмотр SMS–переписки гражданина, данная обязанность предусмотрена вышеперечисленными нормативными актами[1].

Наряду с этим, определение Конституционного Суда РФ от 28.02.2017 года №338–О гласит, что если владелец мобильного телефона не возражает против производства осмотра информации, находящейся в его мобильном устройстве, сам сообщает пароль от него, то в данном случае нарушение конституционного права не усматривается[2]. Следовательно, если последний возражает на производство исследования его устройства без судебного решения, имеет место быть нарушение конституционного права.

В данном контексте заслуживает особого внимания позиция Конституционного Суда Российской Федерации, выразившаяся в определении от 25.01.2018 № 189–О, в котором указано, что проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения. Если же

---

[1] Кассационное определение № 22–2225/12 Омского обл. суда от 24.05.2012 по делу № 22–2225/12. ULR: https://sudact.ru/regular/doc/wLdgQxozbRPrj/ (дата обращения 17.03.2025).

[2] Об отказе в принятии к рассмотрению жалобы гражданина Попова Анатолия Николаевича на нарушение его конституционных прав статьями 176 и 177 УПК РФ: опр. Конст. Суда РФ от 28 февраля 2017 г. № 338–О.

лица полагают, что проведение соответствующих следственных действий и принимаемые при этом процессуальные решения могут причинить ущерб их конституционным правам, в том числе праву на тайну переписки, почтовых, телеграфных и иных сообщений, они могут оспорить данные процессуальные решения и следственные действия в суде в порядке, предусмотренном ст. 125 УПК РФ[1].

Таким образом, электронные носители информации могут быть изъяты в соответствии с п. 2 ч. 1 ст. 164.1 УПК РФ только при проведении следственных действий, перечень которых приведен в ст. 29 УПК РФ. Однако, законодателю целесообразно уточнить свою позицию относительно смысла п. 2 ч. 1 ст. 164.1 УПК РФ.

3) Электронные носители информации содержат информацию полномочиями на хранение и использование которой владелец данного носителя не обладает.

В данном случае законодательство позволяет изымать электронные носители у лиц не причастных к расследуемому преступлению, однако, обладающих сведениями, находящимися на электронном носителе.

4) Сведения, содержащиеся на электронном носителе, могут быть применены для совершения новых преступлений.

Так, в ходе проведения обыска в квартире подозреваемого в совершении преступлений, предусмотренных ч. 2 ст. 273 УК РФ, ч. 4 ст. 159.6 УК РФ было обнаружено 23 мобильных телефона, 6 ноутбуков и иная техника, используемая для хищения денежных средств с дебетовых и кредитных банковских карт, лицевых счетов абонентских номеров[2].

---

[1] Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 УПК РФ: опр. Конст. Суда РФ от 25 января 2018 г. № 189–О.

[2] Приговор Московского районного суда г. Чебоксары Чувашской Республики от 03.08.2018 г. по делу 1–180/2018. ULR: https://sudact.ru/regular/doc/gLdwQxodabDPjd/ (дата обращения 17.03.2025) .

5) Копирование сведений, содержащихся на электронном носителе по заявлению специалиста может повлечь её утрату или искажение.

Исходя из содержания ч. 2 ст. 164.1 УПК РФ при производстве любого следственного действия, производимого следователем или органом дознания, участие специалиста обязательно в случае изъятия флэш–носителей, ноутбуков (нетбуков, ультрабуков), видеорегистраторов, системных блоков, сотовых телефонов, смартфонов всех видов и типов, планшетных устройств, компьютерных блоков (моноблоков) и других менее распространенных электронных носителей информации. Сказанное касается как проведения следственных действий с участием как подозреваемых (обвиняемых), так и свидетелей (потерпевших)[1].

Таким образом, анализ обстоятельств, подлежащих установлению при расследовании преступлений в области компьютерной информации показал, что установление перечисленных в данном параграфе обстоятельств совершенного преступления обязательно, прежде всего, для того, чтобы полно, всесторонне и объективно расследовать уголовное дело, и как следствие, привлечь виновных к установленной законом ответственности.

Требование об обязательном участии специалиста при изъятии электронного носителя информации считаем излишним, целесообразно предоставить право выбора лицу, производящему следственное действие.

Копирование сведений, находящихся на электронных носителях информации следует применять при расследовании всех преступлений в области компьютерной информации, установив следующие основания изъятия:

– отсутствие возможности исследования информации в ходе следственного действия;

– информация на электронном носителе отвечает требованиям, предъявляемым ч. 1 ст. 81 УПК РФ;

---

[1] Гаврилина Ю. В., Победкина А. В. Использование информации, содержащейся на электронных носителях, в уголовно–процессуальном доказывании: учеб. пособ. 2021. М. С. 120.

– на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение.

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

Основным правилом проведения следственных действий в ходе расследования преступлений является четкое следование нормам уголовно–процессуального закона при совершении различных действий на всех этапах осуществления. Именно соблюдение данного правила позволяет использовать результаты следственных действий, в противном случае, последние будут признаны недопустимыми доказательствами по уголовному делу и не подлежащими к использованию в уголовном деле.

Уголовно–процессуальное законодательство строго определяет виды следственных действий, остановимся наиболее подробно на более значимых особенностях проведения отдельных следственных действий при расследовании компьютерных преступлений.

Одним из наиболее значимых и позволяющих получить, имеющую значение для расследования преступления связанного с компьютерными технологиями информацию является следственный осмотр, не смотря на законодательную регламентацию проведения такового следственного действия в практической деятельности возникают неоднозначные вопросы, в этой связи, считаем необходимым остановиться на рассмотрении тактических

особенностей проведения осмотра места происшествия при расследовании компьютерных преступлений[1].

Осмотр места происшествия позволяет обнаружить на месте преступления помимо следов преступного деяния, также и компьютерные устройства, различные носители информации (диски, флешки и тд.), которые могут быть важны для расследования преступления рассматриваемого вида.

Как отмечалось в предыдущей главе компьютерное преступление может быть совершено сразу в нескольких местах, поэтому необходимо осмотреть несколько мест происшествия. Так осмотру подлежат: технические устройства, место обработки информации злоумышленником, устройства внутреннего и внешнего хранения или резервирования информации, место применения технических средств, для незаконного доступа к защищаемой компьютерной информации (таковое может быть расположено совершенно в другом месте, но при этом являться рабочим, даже в другой стране), устройство или место на котором была совершена подготовка к преступлению или была применена, полученная информация, например, программа посредством которой был открыт доступ к защищаемой информации. В практической деятельности правоохранительных органов возникают вопросы именно при получении информации с удаленного персонального компьютера. Зачастую следователь сталкивается с ситуацией, когда ЭВМ работает в режиме удаленного рабочего места. В данной ситуации может сложиться два варианта развития событий:

– следователь может сам провести осмотр места происшествия по месту нахождения управляемого персонального компьютера, однако, в данной ситуации может быть потеряно время, в процессе которого будет установлен персональный компьютер, а злоумышленник за это время может просто удалить нужную информацию, что поставит следствие в тупик;

---

[1] Лебедев В. С. Тактические особенности осмотра места происшествия при расследовании компьютерных преступлений. URL: https://elibrary.ru/download/elibrary_80013310_21240060.pdf (дата обращения 25.02.2025).

– поручить проведение следственного осмотра в порядке ч. 1 ст. 152 УПК РФ[1], уполномоченным должностным лицам.

К сожалению, в практической деятельности правоохранительных органов иногда возникают сложности с установлением времени и места совершения компьютерного преступления. Временные атрибуты файла могут быть подвергнуты фальсификации посредством применения специальных программ или перевода часов вперед или назад[2]. Всё это несколько затрудняет объективную оценку достоверности сведений, которые находятся в файле документа, следовательно, таковые не могут служить по уголовному делу доказательствами.

Особое внимание при расследовании компьютерных преступлении уделяется привлечению специалиста для производства осмотра места происшествия. В качестве специалиста здесь может принимать участие программист, инженер по средствам связи или системный аналитик. Основная задача специалиста на осмотре места происшествия сводится к обнаружению, фиксации и изъятии следов преступного посягательства. Вместе с этим, специалист способствует обеспечению доступа к компьютерным данным, которые могут находиться в зашифрованном состоянии и иметь значение для расследования уголовного дела. Стоит иметь ввиду, что по причине сложности цифровых следов, данные, находящиеся в них могут быть получены в подлинном виде только с использованием специальных познаний. В ходе изъятия цифровых следов необходимо руководствоваться правовой регламентацией, а именно ст. 164.1 УПК РФ[3], однако, данная не регламентирует возможность удаленного обследования места происшествия.

---

[1] Уголовно–процессуальный кодекс Российской Федерации: ФЗ от 18 декабря 2001 г. № 174–ФЗ: электрон // Официальный интернет–портал правовой информации URL: http: // www.pravo.gov.ru (дата обращения: 02.12.2024).

[2] Першин А. Н. Временные следы при расследовании преступлений, совершаемых с использованием компьютерных технологий // Преступность в сфере ИТТ: проблемы предупреждения, раскрытия и расследования преступлений. М. 2022. № 1. С. 46–51.

[3] Уголовно–процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174–ФЗ: электрон // Официальный интернет–портал правовой информации. URL: http: // www.pravo.gov.ru (дата обращения: 02.12.2024).

Преступления в области компьютерных технологий очень разнообразны, иногда настолько сложны, что следователь не может определиться какой квалификации специалиста привлечь для производства осмотра места происшествия[1].

При расследовании преступлений в области информационных технологий очень часто информацию о способе совершения преступления содержат цифровые (виртуальные) следы. Следы такого рода не являются ни идеальными, ни материальными, в этой связи, в научных кругах решается вопрос о отнесении данных к отдельной группе[2]. Так, например, Бахтеев Д.В. считает, что цифровые следы имеют схожесть с материальными следами преступления, а именно в том, что они имеют характеристики носителя информации (уровень намагниченности участка поверхности жесткого диска или электрический заряд в транзисторах твердотельных накопителей)[3].

Наиболее распространёнными цифровыми следами являются – дампы оперативной памяти и дампы трафиков, файлы и их обрывки, информация о данных файлах. Не понимание особенностей цифровых следов порождает возникновение проблемы в ходе осмотра места происшествия, состоящей в частичной либо в полной утрате доказательств по уголовному делу. В этой связи, имеет место быть необходимость в изучении практики цифровых следов и разработки на её основе тактики обнаружения, изъятия, фиксации цифровых следов в ходе осмотра места происшествия.

Сегодня всё чаще можно услышать о цифровой тени, данное понятие очень бурно обсуждается в научных кругах. Цифровая тень – это активные действия

---

[1] Семикаленова А. И., Рядовский И. А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2020. № 6 (103). С. 178–185.

[2] Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: дис. … д–ра юрид. наук. Воронеж, 2021. С. 166-169.

[3] Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юр. журнал. 2020. № 6 (129). С. 61–68.

третьих лиц в отношении определённого субъекта, когда как цифровой след – это действия субъекта[1].

Роскомнадзор предложил рассматривать цифровой след как результат цифрового присутствия, а цифровую тень как цифровое присутствие, осуществляющееся без участия самого субъекта за счет деятельности и устройств третьих лиц[2]. То есть цифровая тень – это разновидность цифрового следа, но об оставлении, которого субъект не знает. Например, цифровой тенью является система «Безопасный город», цель которой наблюдение с помощью камер за улицами городов, однако, о таком наблюдении большое количество людей не знает. Система «Безопасный город» была очень эффективна в период пандемии, посредством неё даже правонарушители привлекались к ответственности за нарушения различного рода.

В ходе осмотра места происшествия и иных следственных действий цифровые следы могут быть изъяты с материальным носителем, при этом собственник последних имеет право произвести копирование информации. Однако, УПК РФ устанавливает случаи, когда материальные носители не могут быть изъяты в процессе следственного действия, а информация подлежит копированию (ст. 164.1 УПК РФ[3]). При наличии случаев, установленных УПК РФ информация копируется с электронного носителя информации, при этом в протоколе следственного действия об этом делается пометка о носителе информации с которого производилось копирование, и на который записывается, оригинал носителя остается у собственника, а копия приобщается к протоколу.

Таким образом, с помощью осмотра места происшествия следователь получает наиболее широкую базу для проведения дальнейшего расследования

---

[1] Гапанович А. В. Цифровые следы и цифровые тени: правовая квалификация // Юрист. 2022. № 6. С. 2 – 7.

[2] Методические рекомендации по организационной защите физическим лицом своих персональных данных. URL: https://pd.rkn.gov.ru/library/p195/ (дата обращения: 30.01.2025).

[3] Уголовно–процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174–ФЗ: электрон // Официальный интернет–портал правовой информации. URL: http: // www.pravo.gov.ru (дата обращения: 02.12.2024).

по преступлению в сфере информационных технологий. Однако, развитие информационных технологий не стоит на месте и требует совершенствования тактики осмотра места происшествия при расследовании преступлений рассматриваемого вида.

Следующим следственным действием является следственный эксперимент, его цель состоит в проверке полученной от участников уголовного процесса информации опытным способом, также предположений, возникающих в процессе следствия, боле того результатом его проведения может быть получение новой информации о навыках и способностях подозреваемого.

При проведении следственного эксперимента необходимо соблюдать следующие условия:

– создание условий проведения такового не унижающих честь и достоинство участников следственного эксперимента;

– наличие понятых;

– при необходимости наличие защитников обвиняемого или подозреваемого;

– наличие потерпевшего и свидетеля, при необходимости.

Ещё раз подчеркнём, что все следственные действия проводятся строго на основании норм УПК РФ, следовательно, согласно этому ход и результаты проведения следственного эксперимента фиксируются в протоколе, в котором отражены все условия его осуществления.

В ходе проведения данного следственного действия должны быть установлены возможности наступления вредных последствий при нарушении определённых правил.

Следственный эксперимент проводится с применением копий исследуемой информации и по возможности на той же ЭВМ или ПК, при работе на которой или котором нарушены правила.

Немаловажным следственным действием является допрос, при расследовании компьютерных преступлений на допросе такого участника уголовного дела как подозреваемый необходимо установить наличие

специальных навыков в части работы с ПК и ЭВМ, а также выяснить как он получил данные навыки.

После этого следует установить должность и место работы допрашиваемого, а также входит ли в его обязанности по должностной инструкции работы с ПК, при наличии положительного ответа, следует установить информацию о наличии/ отсутствии допусков к определённым программам, какие операции им выполняются в ходе работы на рабочем месте.

Более того большое значение имеет установление информации о том, имеет ли допрашиваемый доступ к сети Интернет, закреплены ли за ним коды и пароли, необходимые для работы в сети.

Вместе с этим, стоит иметь ввиду, что на допросе подозреваемые, обвиняемые, как правило, занимают конфликтующую позицию и пытаются оказать любое посильное противодействие следователю. Для наглядного понимания специфики допроса подозреваемого, обвиняемого при расследовании преступлений, посягающих на компьютерную информации, считаем целесообразным обратиться к примеру судебной практики. Рассмотрим конкретный пример совершения преступления в сфере компьютерной информации в крупном размере и определим какие вопросы необходимо задать подозреваемому на первоначальном допросе. Так, гр. В. с целью личного обогащения посредством ввода модификации компьютерной информации и вмешательства в функционирование средств хранения, являясь осведомленным о порядке и правилах доступа к автоматизированной услуге «мобильный банк» ПАО «Сбербанк» и о возможности перевода денежных средств без использования самой карты, применяя SIM–карту, отправил SMS–сообщение на незнакомый абонентский номер, принадлежащий гр. Г. с текстом «Ваша карта заблокирована, информация № 752». Гр. Г., введенный в заблуждение, перезвонил на номер В, который представился сотрудником банка. Далее гр. В. путем обмана получил сведения о номере банковской карты и кодовом слове, после этого посредством неустановленной техники получил

доступ к лицевому счёту гр. Г. И перевел денежные средства на подконтрольный ему счёт[1].

Итак, определим вопросы, которые необходимо поставить перед гр. В:

– выяснить личные данные, в частности, наличие судимостей, стоит ли на каких–либо учётах, уровень образования, а также любая иная информация, свидетельствующая о наличии у допрашиваемого специальных знаний и умений;

– все обстоятельства совершения преступного деяния, в частности, каким образом производил звонки потерпевшим, если по наводке, то кто именно навел, где и как была куплена сим–карта, где хранится телефон, через который производился звонок потерпевшему;

– где, на чье имя открыт счет куда переводились денежные средства, имеются ли иные счета или это единственный;

– где и (или) у кого было приобретено техническое средство с помощью которого был осуществлен неправомерный доступ, где они на данный момент находится;

– каким образом были использованы денежные средства, полученные от реализации преступного умысла;

– все преступные действия были совершены В. в одиночку или в составе преступной группы;

– имеет ли отношение к совершению иных преступных эпизодов или это единственный.

Это основные вопросы, ответы на которые необходимо установить при допросе гр. В, однако, данные перечень не является исчерпывающим.

Позиция следователя на допросе в конфликтной ситуации должна быть несколько иной, более избирательной. Необходимо помнить, что не стоит упоминать о ненадежных доказательствах. Наиболее эффективными приёмами допроса подозреваемого (обвиняемого) в конфликтной ситуации являются:

---

[1] Приговор суда по ч. 3 ст. 159.6 УК РФ № 1–144/2017 г: электрон путеводитель. URL: https://advocate-service.ru/sud-praktika/ugolovnye-dela/prigovory-sudov-po- ch.-3-st.-159.6-uk-rf--1-1442017 (дата обращения: 02.12.2024).

доведение до допрашиваемого информации, которая на самом деле не является полностью достоверно известной, иными словами, необходимо создать впечатление допрашиваемому о наибольшей осведомленности о преступном событии; постоянное акцентирование внимание допрашиваемого на одном и том же вопросе, но задавая при этом данный в различных вариантах, данное может привести к проговору; предъявление доказательств в процессе допроса; маскировка основного вопроса среди второстепенных; доведение до допрашиваемого мер ответственности за совершенное им преступление; разъяснение мер смягчения наказания за содействие следствию[1].

Стоит иметь ввиду, что при расследовании преступлений, посягающих на компьютерную информацию, защищаемую законом, на первый взгляд, установить подозреваемого проще, когда доступ к предмету преступления очень сложен и требует специальных познаний, так как круг специалистов, наделённых необходимыми для этого способностями несколько ограничен. Однако, зачастую профессиональные хакеры специально таким образом подставляют третье лицо с целью запутывания следствия. В данном случае хакер выбирает лицо, имеющее доступ к информации необходимой для совершения преступления, трудоустроенное официально в организации, являющейся потерпевшей.

Виновность лиц, осуществляющих неправомерный доступ к компьютерной информации может быть доказана только по результатам всего расследования.

Основополагающими в данном случае будут показания свидетелей, подозреваемых, обвиняемых, потерпевших, заключения судебных экспертиз (информационно–технологических, информационно– технических), результаты обысков.

На стадии выявления обвиняемого, в процессе его допроса следует установить все этапы совершения преступления с начала подготовки в случае

[1] Бердникова О. П., Дерюгин Р. А. Особенности расследования мошенничества в сфере компьютерной информации: учеб. пособ.. Екатеринбург. 2021. С. 64.

с вредоносной программой необходимо установить алгоритм её действия и ту часть информации, которую она поражает.

Именно при наличии вредоносной программы установить причинённый преступным деянием вред и размер ущерба очень сложно, в связи с тем, что вирус размножается очень быстро и в большом количестве, поражая всю компьютерную сеть потерпевшего.

Однако, необходимо учитывать, что огромный ущерб для потерпевшего может наступить не только применением вирусных атак, но и нарушением требований использования ЭВМ, так как именно это по итогу влечёт нарушение работы всего учреждения.

Расследование преступлений, совершенных данным методом требует изучения всех нормативных документов организации–потерпевшей, а также привлечение незаинтересованного специалиста, который сможет дать ответы на многие вопросы расследования.

Первостепенно при расследовании необходимо определить место нахождение станции, эксплуатация которой была нарушена. Данное может быть решено посредством проведения информационно–технической экспертизы.

Также необходимо установить время и место совершения преступления, как уже отмечалось выше, временем будет момент наступления вредных последствий. Данное также могут определить лишь специалисты в рамках экспертного исследования. Также этому может помочь служебное расследование, материалы которого положены в основу всего расследования, допрос участников расследования, а также осмотр места происшествия.

Нарушение правил эксплуатации ЭВМ может быть выражено как в активных действиях, например, совершении несанкционированных операций, так и пассивных, например, невыполнение определённых требований информационной безопасности.

Информация о способе нарушения правил эксплуатации ЭВМ может быть получена следователем в результате проведения таких следственных действий, как допрос, судебная–компьютерная экспертиза, следственный эксперимент.

Чтобы следственный эксперимент прошел эффективно необходимо использовать именно ту технику, с применением которой были нарушены правила эксплуатации.

Одной из основных задач расследования рассматриваемого вида преступлений является установление лица, допустившего нарушение правил работы с ЭВМ, предусмотренное ст. 274 УК РФ, так как данным может быть далеко не любое лицо. Нарушителем может быть только лицо, имеющее необходимый допуск к компьютерной информации.

Здесь стоит отметить, что наряду с общими данными у таких лиц, необходимо установить их профессиональный уровень, уровень образования, например, стаж работы, перечень должностей ранее им замещаемых. Но главной информацией является уровень допуска к охраняемой информации, наличие обязанностей по защите компьютерной информации, участие в разработках программных систем, доступ к базам данных и иное .

Преступления, связанные с компьютерными технологиями, являются специфическим видом, поэтому их успешное раскрытие и расследование зависит от эффективного применения специальных знаний в данной области, а именно назначения и производства судебных компьютерных экспертиз. Низкий уровень проработанности методических рекомендаций по назначению и производству судебных компьютерных экспертиз порождает возникновение процессуальных и организационно–тактических проблем. Проведенное исследование материалов судебной и следственной практики показало, что на сегодняшний день у следователя очень часто возникают сложности при назначении судебных компьютерных экспертиз. Указанное возникает в связи с тем, что имеет место быть неполнота и недостаточность представляемых на исследование объектов, некорректное изложение вопроса, адресованного эксперту, неправильный выбор экспертного учреждения или специалиста и т.д.

С целью минимизации возникающих проблем необходимо провести их детальный анализ, а для начала определить понятие, виды и задачи судебной компьютерной экспертизы. На основании п. 11.1 Перечня видов судебных

экспертиз, утвержденного приказом МВД России от 29 июня 2005 г. № 511[1] видом судебной компьютерной экспертизы, является исследование компьютерной информации. Из этого следует, что основная цель рассматриваемого вида экспертизы направлена на исследование объектив, содержащих компьютерную информацию и исследование самой информации, имеющей значение для расследуемого уголовного дела.

По мнению, А.Б. Соколова и А.Р. Сысенко судебная компьютерная экспертиза – это исследование в области выявления закономерностей возникновения и сокрытия электронно–цифровых следов, проводимое компетентным лицом на основании норм уголовно–процессуального законодательства[2]. Согласно данному понятию основная цель судебно–компьютерной экспертизы состоит в получении информации в электронно–цифровом виде. Объектами же исследование такого вида экспертизы может компьютерная информация, а также различные программные обеспечения. В результате проведения экспертного исследования перечисленных объектов следователь получает информацию о механизме совершения преступления и на его основе определяет данные имеющие значение для расследования уголовного дела[3].

Объектами исследования судебно–компьютерной экспертизы не являются компьютерное оборудование, компьютерные системы, так как данные характерны для исследования в рамках компьютерно–технической экспертизы, где указанные изучаются на предмет определения фактов и обстоятельств их применения при совершении расследуемого преступления. Когда как

---

[1] Вопросы организации производства судебных экспертиз в экспертно–криминалистических подразделениях органов внутренних дел РФ: приказ МВД России от 29.06.2005 № 511 // «КонсультантПлюс».

[2] Соколов А. Б., Сысенко А. Р. Назначение и производство компьютерной экспертизы при расследовании преступлений, совершенных с использованием сети Интернет: проблемы теории и практики // Криминалистика: вчера, сегодня, завтра. 2023. № 1 (17). С. 128.

[3] Гайнельзянова В. Р. Возможности судебной компьютерно–технической экспертизы при расследовании преступлений в сфере компьютерной информации // Вестн. УЮИ МВД России. 2022. № 1 (91). С. 146.

основным объектом судебно–компьютерной экспертизы является информация, представляемая на исследование на каком–либо носителе.

Задачами компьютерной экспертизы являются: поиск, анализ и оценка компьютерной информации, расположенной на определенном носителе. При этом выделяют идентификационные задачи экспертного исследования, к которым можно отнести исследование информации на предмет определения автора программного продукта, части и целого и т.д. Более того, имеют место быть диагностические задачи экспертного исследования такого рода, где решаются вопросы о наличии заражения вирусом, наличии факта уничтожения информации злоумышленником и т.д.

Безусловно, качественное проведение судебной–компьютерной экспертизы зависти от её грамотной организации, подготовки и назначения, несколько осложняет данное специфичность такого рода экспертиз, своеобразие её объектов поэтому значение подготовки здесь ещё более возрастает.

Назначение судебно–компьютерной экспертизы проходит в несколько этапов:

- определение оснований назначения экспертного исследования;

– определение рода и вида экспертизы;

– определение учреждения, где будет проведено исследование или конкретного эксперта;

- подготовка объектов для исследования;

- формулировка вопросов эксперту;

- вынесение постановления о назначении экспертизы;

– ознакомление участников уголовного дела с постановлением, на основании УПК РФ;

– направление постановления о назначении исследования и объектов для проведения экспертизы в учреждение.

Необходимо детально изучать задачи судебно–компьютерной экспертизы, так как имеют место быть случаи, когда вопрос поставленный на исследование

эксперту можно решить посредством привлечения специалиста в рамках следственного действия, например, осмотра места происшествия.

После определения оснований назначения судебно–компьютерной экспертизы следователь должен решить вопрос о её виде. Выбор вида экспертного исследования зависит от целей, задач планируемого исследования, однако, все индивидуально для каждого конкретного случая. Согласно Приказа МВД России от 29 июня 2005 года №511 компьютерная экспертиза проводится в экспертно–криминалистических подразделениях органов внутренних дел[1]. Когда как такая экспертиза как «компьютерно–техническая» проводится в учреждении системы Министерства юстиции Российской Федерации[2].

Выбор экспертного учреждения может зависеть от следующих обстоятельств:

– ведомственная принадлежность и территориальное расположение экспертного учреждения;

– сроки проведения конкретного исследования;

– наличие и возможность проверки документов, подтверждающих статус эксперта;

– возможность проверки компетентности эксперта и т.п.

При выборе экспертного учреждения и эксперта необходимо учитывать положения ст. 61 УПК РФ, а именно исключать основания, препятствующие проведению экспертного исследования конкретному эксперту. Практика показывает, что одной из основных проблем сегодня является отсутствие квалификационных требований, предъявляемых эксперту негосударственных учреждений, определяющих компетентность последнего. Данное имеет большое значение, так как основная доля судебно–компьютерных экспертиз проводится

---

[1] Вопросы организации производства судебных экспертиз в экспертно–криминалистических подразделениях органов внутренних дел РФ : приказ МВД России от 29.06.2005 № 511 // «КонсультантПлюс».

[2] Об утверждении инструкции по организации производства судебных экспертиз в судебно–экспертных учреждениях системы Министерства юстиции РФ: приказ Минюста России от 20.12.2002 № 347 // «КонсультантПлюс».

именно экспертами негосударственных учреждений. Вместе с этим, зачастую эксперты данных учреждений не имеют экспертного образования, необходимое для проведения судебно–компьютерной экспертизы. Следовательно, эксперты такого рода очень часто не знают процесс судопроизводства, а также не отдают отчет в правовых последствиях даваемых ими заключениях. Нередко такие эксперты выходят за рамки своей компетенции, решают вопросы правового характера. Имеют место быть также нарушения правил работы с объектами исследования, что может повлечь уничтожение, содержащейся на них информации.

Однако, даже высококвалифицированный специалист не всегда компетентен в вопросах работы компьютерных программ и приложений, что делает разрешение вопросов, поставленных на исследование невозможным.

Для обеспечения правильного проведения экспертного исследования следует подготовить объекты, подвергаемые исследованию. Экспертное исследование в рамках проведения компьютерной экспертизы заключается в работе с таким объектом как компьютерная информация. Однако, по словам сотрудников экспертных подразделений системы МВД России в практической деятельности последние сталкиваются с исследованием и иных смежных объектов, по причине того, что информация на компьютере может касаться и аппаратных, программных объектов. Также компьютерная информация предоставляется на исследование на электронном носителе.

Специфичность объекта исследования компьютерной экспертизы требует соблюдения правил его упаковки и изъятия, участие специалиста в области компьютерных технологий при этом принесёт положительный результат, более того на основании ст. 164.1 УПК РФ[1] участие специалиста при изъятии электронных носителей информации обязательно. В случае изъятия средств

[1]Уголовно–процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174–ФЗ. – Текст: электрон // Официальный интернет–портал правовой информации: URL: http: // www.pravo.gov.ru (дата обращения: 02.12.2024).

компьютерной техники необходимо принимать меры к сохранности, находящейся на них информации, комплектующих деталей.

Наряду с компьютерными экспертизами при расследовании преступлений рассматриваемого вида могут быть назначены и традиционные виды экспертиз, например, дактилоскопическая, тератологическая, почерковедческая и т.д. Данное связано, прежде всего с тем, что расследование преступлений в сфере компьютерной информации предполагает не только изъятие компьютерного оборудования и информации, но и различные традиционные следы, оставленные преступником и требующие проведения других видов экспертного исследования[1].

В области обязательного участия специалиста при изъятии электронных носителей информации в научных кругах возникают споры. Так как к электронным носителям информации относятся совершенно различные объекты. Например, безусловно участие специалиста обязательно при осуществлении поиска и копирования информации на электронных носителях. Однако, при изъятии таких объектов, относящихся к носителям информации как CD–диски, сотовые телефоны и т.п. обязательное участие специалиста ставится под сомнение. Несколько больше вопросов возникает и при рассмотрении вопроса об обязательном участии специалиста в ходе изъятия бытовых приборов, составляющими которых являются исполнительные модули, относящиеся к электронным носителям информации (холодильники, посудомоечные машины, стиральные машины, микроволновки).

Решение вышеперечисленных споров судами было осуществлено посредством выработки позиции о том, что изъятие электронных носителей информации в ходе следственного действия может быть произведено без участия специалиста в случае, если для этого не требуются копирование информации с данного носителя, а также изъятие не является сложным и не требует специальных знаний и навыков. Более того судами следователю даётся выбор

[1] Рясов А. А. Методика расследования мошенничества в сфере компьютерной информации: учеб. пособ. Краснодар. 2021. С. 18.

на привлечение или не привлечение специалиста для производства следственного действия[1].

Следует иметь ввиду, что для полноты и качества проведения судебной компьютерной экспертизы эксперту иногда могут потребоваться данные технической документации, имеющей отношение к исследуемым объектам, материалы уголовного дела, содержащие пароли и логины, информацию о средстве защиты и т.п.

Полнота проведения экспертного исследования, вместе с вышеизложенным, зависит от правильности постановки перед экспертом вопросов, которые эксперт должен решить.

Сложность формулировки вопросов следователем состоит в том, что компьютерная экспертизы, требует знания большого количества технической терминологии, поэтому участие специалиста здесь необходимо. Наиболее распространённой ошибкой следователя является формулировка правовых вопросов, что недопустимо по причине процессуальных требований.

Вопросы, адресованные эксперту должны соответствовать следующим критериям:

– применение правильной терминологии при изложении вопроса, недопустимо применение жаргонных понятий, например, «гаджет»;

– вопросы не могут затрагивать этапы экспертного исследования;

– не допустимо использование абстрактных фраз, которые могут трактоваться двойственно;

– вопрос не может быть правовым или носить справочный характер должен быть адресован строго конкретному эксперту;

– вопрос должен быть конкретным и отвечать уровню подготовки эксперта;

---

[1] Апелляционное постановление Судебной коллегии по уголовным делам Московского городского суда от 07.10.2013 по делу № 10–9861 // Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/Emr OjKn4X5Zm (дата обращения: 07.03.2025).

– постановление о назначении экспертизы должно содержат информацию о объектах, направляемых на исследование и их количестве.

Таким образом, процесс подготовки и проведения судебной компьютерной экспертизы очень трудоёмкий, требующий от следователя чёткого понимания целей и задач проводимого исследования. Эффективность проведения судебно–компьютерной экспертизы сложно представить без организации взаимодействия со специалистами на всех стадиях работы по подготовке и назначению экспертизы[1].

При расследовании преступлений, посягающих на компьютерную информацию особое значение, стоит уделять проведению таких следственных действий как осмотр места происшествия, допрос, следственный эксперимент экспертные исследования и др. при необходимости. Вместе с этим, в настоящее время имеют место быть некоторые сложности в определении вопросов, касающихся обязательного участия специалиста при проведении осмотра места происшествия, изъятия цифровых следов преступления, определения времени и места совершения преступления, назначения судебной–компьютерной экспертизы.

[1] Звягин И. С. Особенности подготовки и назначения судебной компьютерной экспертизы при расследовании преступлений//Вестн. Воронежского института МВД России. №2. 2023. С. 1–5.

ЗАКЛЮЧЕНИЕ

В XXI веке трудно представить жизнь без компьютера и информационных технологий, они сопровождает нас повсюду. Каждое рабочее место в офисе оснащено компьютером, различные управленческие и иные документы хранятся на компьютере, различные виды учётов также ведутся при помощи специальных программ, что существенно облегчает работу сотрудников, делая более автоматизированной, но в тоже время имеется высокая вероятность уязвимости информации, хранящейся на машинном носителе.

Информационное развитие общества способствует росту профессионалов в области компьютерных технологий, к сожалению, некоторые из них преследуют преступные цели, что в свою очередь ведёт к росту преступлений в области компьютерных технологий. Анализ статистических данных позволяет судить о значимости данного вопроса.

Исследование, проведенное в рамках дипломной работы, показало, что имеется ряд проблем при расследовании преступлений в сфере компьютерной информации, возникающих по причине неустойчивой судебной практики и отсутствия методических рекомендаций по расследованию преступлений такого вида. Практика показывает, что как правили преступления в области посягательств на компьютерную информацию расследуют следователи, не обладающие достаточными знаниями и опытом расследования уголовных дел в сфере компьютерных технологий.

Более того, сегодня правоохранительные органы страдают от острой нехватки кадров, специализирующихся на расследовании преступлений, связанных с использованием информационно–телекоммуникационных технологий, что напрямую влияет на качество и сроки расследования. Так, имеют место быть случаи, когда следователи вынуждены при расследовании, например, мошенничества в сфере компьютерной информации прибегать к помощи специалистов частных компаний,

осуществляющих деятельность в сфере компьютерной информации, так как иной возможности провести качественное экспертное исследование нет.

Вместе с этим, одним из пробелов, допускаемых при расследовании такого рода преступлений является некачественный анализ с особыми качествами преступников, которые могут свидетельствовать о способе совершения преступления, формирующем почерк преступника. Так как именно почерк преступника содержит большую часть следов человека, совершающего преступления в сфере информационных технологий.

Криминалистическая характеристика преступлений в сфере компьютерной информации – это совокупность таких элементов как, предмет преступного посягательства, способ совершения преступления, механизм следообразования, обстановка совершения преступления, личность преступника и потерпевшего. Данные элементы тесно связаны между собой и имеют свою специфику в части проявления в цифровой среде, именно это делает преступления, посягающие на компьютерную информацию отличительными от других и обеспечивает правильность выдвижения версий о преступном событии, о личности виновного лица, направление поиска и алгоритма действий лиц, расследующих данное преступление.

Производство следственных действий при расследовании преступлений рассматриваемого вида имеет свои особенности, обусловленные механизмом следообразования, особенностью работы с цифровыми следами (если данные имеются), способом совершения преступления, индивидуальными особенностями личности преступника.

Таким образом, компьютерные преступления представляют собой сложный и динамично развивающийся вид преступной деятельности, расследование которого сопряжено со значительными трудностями. Как показало исследование, эти трудности носят системный и взаимосвязанный характер: недостаточная специализация и нехватка кадров в правоохранительных органах, отсутствие устойчивой судебной практики и методических рекомендаций, проблемы с выявлением и работой с цифровыми

следами и "почерком" преступника, а также объективные сложности криминалистической характеристики преступлений в цифровой среде.

Успешное преодоление этих проблем требует комплексного подхода. Крайне важно понимать, что все элементы расследования – от выявления следов и анализа способа преступления до построения версий и оценки личности преступника – тесно взаимосвязаны и должны рассматриваться в едином ключе.

В этой связи необходимо активное привлечение специалистов в области информационных технологий на всех этапах расследования, особенно когда собственных ресурсов следствия недостаточно для проведения качественных экспертных исследований.

Не менее важна непрерывная подготовка и обучение самих следователей. Им необходимо систематически изучать и осваивать современные методы расследования киберпреступлений, особенности работы с цифровыми доказательствами, специфику ИТ–инфраструктуры и актуальные способы и методы, используемые злоумышленниками. Только сочетание профессиональной подготовки следователей и обязательного взаимодействия с высококвалифицированными ИТ–специалистами позволит обеспечить качество, оперативность и законность расследования.

Игнорирование этих факторов не только затрудняет раскрытие конкретных преступлений, но и создает серьезные риски для соблюдения основополагающих принципов уголовного судопроизводства – справедливости и законности – как на стадии расследования, так и в суде. Поэтому дальнейшее развитие законодательства, судебной практики и, что особенно важно, практических методик расследования с обязательным учетом необходимости специализированной подготовки и работы со специалистами, является важным условием для эффективного противодействия преступности в сфере компьютерной информации и защиты прав граждан и интересов общества в цифровую эпоху.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

I. Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации: [принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года]: электронный // Официальный интернет–портал правовой информации. URL: http://pravo.gov.ru (дата обращения: 20.11.2024).

2. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63–ФЗ: электронный // Официальный интернет–портал правовой информации. URL: http:// www.pravo.gov.ru (дата обращения: 20.12.2024).

3. Уголовно–процессуальный кодекс Российской Федерации: Федеральный закон от 18 декабря 2001 г. № 174–ФЗ: электронный // Официальный интернет–портал правовой информации. URL: http: // www.pravo.gov.ru (дата обращения: 02.12.2024).

4. Гражданский кодекс Российской Федерации: Федеральный закон от 30 ноября 1994 г. № 51–ФЗ: электронный // Официальный интернет–портал правовой информации. URL: http:// www.pravo.gov.ru (дата обращения: 20.12.2024).

5. Об оперативно–розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144–ФЗ: электронный // Официальный интернет–портал правовой информации. URL: http:// www.pravo.gov.ru (дата обращения: 20.12.2024).

6. Вопросы организации производства судебных экспертиз в экспертно–криминалистических подразделениях органов внутренних дел Российской Федерации: приказ МВД России от 29.06.2005 № 511. Документ опубликован не был. Доступ из справ.–правовой системы «Консультант Плюс».

7. Об утверждении инструкции по организации производства судебных экспертиз в судебно–экспертных учреждениях системы Министерства юстиции Российской Федерации: приказ Минюста России от 20.12.2002 № 347. Документ

опубликован не был. Доступ из справ.–правовой системы «Консультант Плюс».

II. Учебная, научная литература и иные материалы

1. Бахтеев Д. В., Смахтин Е. В. Криминалистические особенности производства процессуальных действий с цифровыми следами // Российский юридический журнал. 2020. № 6 (129). 14 с.

2. Бердникова О. П., Дерюгин Р. А. Особенности расследования мошенничества в сфере компьютерной информации: учебное пособие. Екатеринбург. 2021. 84 с.

3. Гаврилина Ю. В., Победкина А. В. Использование информации, содержащейся на электронных носителях, в уголовно–процессуальном доказывании: учебное пособие. 2021. Москва. 140 с.

4. Гайнельзянова В. Р. Возможности судебной компьютерно–технической экспертизы при расследовании преступлений в сфере компьютерной информации // Вестник Уфимского юридического института МВД России. 2022. № 1 (91). 146 с.

5. Гапанович А. В. Цифровые следы и цифровые тени: правовая квалификация // Юрист. 2022. № 6. 11 с.

6. Звягин И. С. Особенности подготовки и назначения судебной компьютерной экспертизы при расследовании преступлений // Вестник Воронежского института МВД России. №2. 2023. 9 с.

7. Коржов В. К. Право и Интернет: теория и практика: учебное пособие / В. К. Коржов. М.: Издательство БЕК. 2020. 236 с.

8. Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. М.: Новый юрист. 2020. 210 с.

9. Лебедев В. С. Тактические особенности осмотра места происшествия при расследовании компьютерных преступлений. Elibrary // URL: https://elibrary.ru/download/elibrary_80013310_21240060.pdf (дата обращения 25.02.2025).

10. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: дис. … д–ра юрид. наук. Воронеж, 2021. 387 с.

11. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: монография. М.: Норма. 2020. 432 с.

12. Панфилова Е. И. Компьютерные преступления: учебное пособие Феникс. 2020. 254 с.

13. Першин А. Н. Временные следы при расследовании преступлений, совершаемых с использованием компьютерных технологий // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. М. 2022. № 1. 109 с.

14. Рясов А. А. Методика расследования мошенничества в сфере компьютерной информации: учебное пособие. Краснодар. 2021. 293 с.

15. Сальников В. П. Компьютерная преступность: учебное пособие Приор, 2020. 192 с.

16. Семикаленова А. И., Рядовский И. А. Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2020. № 6 (103). 288 с.

17. Соколов А. Б., Сысенко А. Р. Назначение и производство компьютерной экспертизы при расследовании преступлений, совершенных с использованием сети Интернет: проблемы теории и практики // Криминалистика: вчера, сегодня, завтра. 2023. № 1 (17). 283 с.

18. Теппеев А. А.. Особенности расследования преступлений, связанных с мошенническими действиями, совершёнными с использованием средств сотовой телефонной связи: учебное пособие. Краснодар. 2021. 46 с.

19. Шевко Н. Р., Каримов А. М., Турутина Е. Э. Преступления, совершаемые с использованием высоких технологий и коммуникаций: учебное пособие. Казань. 2020. 18 с.

20. Федотов Н. Н. Форензика – компьютерная криминалистика. М. 2012.

21. Валькова Т. В., Шуин В. Э., Долгаев В. В. Методика расследования преступлений против собственности: метод. рекомен. СПб.: Издат. СПб ун–та МВД России. 2020. 124 с.

III. Эмпирические материалы

1. Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://мвд.рф/ (дата обращения 01.03.2025).

2. Портал Правовой статистики Генеральной Прокуратуры Российской Федерации. Показатели преступности России. Рейтинг. [Электронный ресурс]. URL: http://crimestat.ru/regions_chart_total (дата обращения 14.10.2024).

3. Аппеляционное постановление Московского областного суда от 20.08.2024 г. ULR: https://sudact.ru/regular/doc/dWgQxopbXPrj/ (дата обращения 17.03.2025).

4. Апелляционное постановление №22К – 2839/ 2024 от 30.08.2024 г. URL: https://sudact.ru/regular/doc/hv3CZjqqBRJl/ (дата обращения 17.03.2025).

5. Приговор Балашихинского городского суда от 23.02.2024 г. URL: https://sudact.ru/regular/doc/dWgQxopbXPrj/ (дата обращения 17.03.2025).

6. Статистические данные ОМВД России по Кунашакскому району Челябинской области.

7. Методические рекомендации по организационной защите физическим лицом своих персональных данных // URL: https://pd.rkn.gov.ru/library/p195/ (дата обращения: 30.01.2025).

8. Кассационное определение № 22–2225/12 Омского областного суда от 24.05.2012 по делу № 22–2225/12.

9. Об отказе в принятии к рассмотрению жалобы гражданина Попова Анатолия Николаевича на нарушение его конституционных прав статьями 176 и 177 Уголовно–процессуального кодекса Российской Федерации: определение Конституционного Суда РФ от 28 февраля 2017 г. № 338–О. Документ опубликован не был. Доступ из справ.–правовой системы «КонсультантПлюс».

10. Информация Банка России от 28.09.2020 г. «Основные направления развития информационной безопасности в кредитно–финансовой сфере на период 2019–2021 гг.». URL: https://www.garant.ru/products/ipo/prime/doc/74615166/ (дата обращения: 21.04.2025).

11. Официальный сайт Министерства внутренних дел Российской Федерации. URL: https://xn—b1aew.xn—p1ai/reports/item/60248328/ (дата обращения 01.03.2025).

Материал вычитан, цифры, факты, цитаты сверены с первоисточником. Материал не содержит сведений, составляющих государственную и (или) служебную тайну_____