Министерство внутренних дел Российской Федерации

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

Кафедра криминалистики

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему «Особенности выявления и расследования преступлений в сфере компьютерной информации»

Выполнил: Козонков Константин Юрьевич ___
(фамилия, имя, отчество)
40.05.02- Правоохранительная деятельность
(специальность, год набора, № группы)
__2015 г._№352_____

Руководитель:
Профессор кафедры криминалистики д.п.н.,
(ученая степень, ученое звание, должность)
профессор Казанцев Сергей Яковлевич
(фамилия, имя, отчество)

Рецензент: Заместитель начальника ОМВД России по Алексеевскому району РТ – начальник следственного отделения, подполковник юстиции
Хайбуллин Руслан Харисович

Оценка _____

Дата защиты:
"___" _____2021г.

Казань 2021

СОДЕРЖАНИЕ

ВВЕДЕНИЕ ……..….....…3
ГЛАВА 1. УГОЛОВНО – ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ
§1. Компьютерная информация как объект криминалистического исследования…….……7
§2. Уголовно-правовая характеристика преступлений в сфере компьютерной информации ……..…9
§3. Вредоносные компьютерные программы как один из элементов криминалистической характеристики ……17
§4. Иные элементы криминалистической характеристики преступлений, совершаемых в сфере компьютерной информации ……..……30

ГЛАВА 2. ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ И ВЗАИМОДЕЙСТВИЯ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§1. Особенности производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации…….....40
§2. Особенности следователя с органами дознания и специалистами ……50

ЗАКЛЮЧЕНИЕ…….…....54
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ…….……58
ПРИЛОЖЕНИЯ ……65

ВВЕДЕНИЕ

Актуальность темы. Быстрое развитие высокой технологии обеспечивает общество наравне с комфортной жизнедеятельностью всех членов проблемой, связанной с возникновением и последующим развитием новейших типов преступности. Один из данных типов – это преступность в области компьютерной информации, образованная деяниями, указанными в ст. ст. 272-274.1 Уголовного кодекса Российской Федерации (далее УК РФ)[1].

На основании данных официальной статистики МВД России, на данный момент времени, возможно, наблюдать значительное сокращение количества преступлений, которые совершают в области компьютерной информации. Например, в 2014 году их зарегистрировано 1739, в 2015 году – 2382 в 2020 году зарегистрировано 2346 преступлений[2]. Является понятным, что указанный показатель говорит не об уменьшении числа совершенных компьютерных преступлений, а о высокой латентности, о том, что выявлять их становится все труднее и труднее.

Согласно данным Судебного департамента при Верховном суде РФ по ст.272-274.1 УК РФ в 2017 году осуждено – 203, в 2018 – 129, в 2019 – 165, в 2020 – 137 человек. [3]

Однако ущерб от действий киберпреступников ежегодно исчисляется в России миллиардами рублей.

Одна из причин такого положения – это совершенствование противодействия проводимому расследованию этого типа преступлений со стороны, как виновного лица, так и других заинтересованных в сокрытии истины субъектов. На эффективность оказываемого расследованию противодействия

---

[1]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2017) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

[2]Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – URL: http://www.mvd.ru/presscenter/statistics/reports (дата обращения 15.03.2017)

[3]Официальный сайт Судебного департамента при ВС РФ режим доступа свободный http://www.cdep.ru/index.php?id=79&item=5669 (дата обращения 2.08.2021)

указывает падение раскрываемости преступлений в области компьютерной информации. Например, в 2015 году раскрываемость снижается на 39,8 процентов, а за 2016 году составила 61,2% в 2020 – 45%. [1].

Эффективное противостояние преступлениям в сфере компьютерной информации, защита прав и законных интересов граждан, а также обеспечение информационной безопасности государства и юридических лиц возможно только на базе постоянно изменяемого комплекса всех мер защиты, включая и формирование криминалистических средств.

Теоретической основой исследования стали основные труды ученых-процессуалистов в данной области: Андреев Б.В.,[2] Вехов В.Б.[3], Воробьев В.В.,[4] Головин А.Ю.,[5] Голубев В.А.,[6] Дворецкий М.Ю.,[7] Номоконов В.А.,[8] Селиванов Н. А.,[9] Черкасов В.Н.[10] и другие. Данными авторами было подробно изучены особенности выявления и расследования преступлений в сфере компьютерной информации, отдельные проблемы его реализации в практической деятельности

---

[3]Там же.

[2]Андреев Б.В., Пак, П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации: учебное пособие // Б.В. Андреев., П.Н. Пак, В.П. Хорс. – М.: Юрлитинформ, 2012. – 152 с.

[3]Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации: учебное пособие // В.Б. Вехов, В.В Попова, Д.А.Илюшин., 2014. – 289 с.

[4]Воробьев В. В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Дис. … канд. юрид. наук. – Н. Новгород, 2010. – 200 с.

[5]Головин А. Ю. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации//http://www.crime-research.org (дата обращения: 15.03.2021).

[6]Голубев В.А. Вопросы международного сотрудничества в борьбе с транснациональной компьютерной преступностью // В.А. Голубев. – Режим доступа: http://www.crime-research.ru/articles/2011/ (дата обращения: 15.03.2021).

[7]Дворецкий М.Ю. Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ: учебное пособие // М.Ю. Дворецкий А.Н. Копырюлин. – Уголовное право, 2012. — №4. – 34 с.

[8]Номоконов В.А. Новые информационные технологии в борьбе с преступностью / В.А. Нимоконов. – Российский криминологический взгляд, 2012. – № 1. – 94 с.

[9]Селиванов Н. А. Проблемы борьбы с компьютерной преступностью: учебное пособие / Н.А. Селиванов. – Законность, 2013. – № 8. 37 с.

[10]Черкасов В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий: учебное пособие / В.Н. Черкасов. – Саратов, 2015. – 81 с.

правоохранительных органов РФ и зарубежных стран.

Объектом исследования выступают общественные отношения, возникающие в связи с выявлением и расследованием компьютерных преступлений.

Предметом исследования являются закономерности механизма преступной деятельности, реализуемой в сфере компьютерной информации, закономерности обнаружения, фиксации, исследования, оценки и использования следов данного вида преступной деятельности.

Целью настоящего исследования является выявление закономерностей механизма преступной деятельности, реализуемой при совершении преступлений в сфере компьютерной информации и разработка на этой основе соответствующей методики расследования

Для ее достижения были поставлены следующие **задачи:**

- раскрыть понятие компьютерной информации как объекта криминалистического исследования;
- исследовать уголовно-правовую характеристику;
- рассмотреть криминалистическую характеристику преступлений, совершаемых в сфере компьютерной информации;
- изучить вредоносные программы и компьютерные вирусы.
- раскрыть особенности производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации,
- рассмотреть особенности взаимодействия сотрудников оперативных с подразделениями оперативно-технических мероприятий (далее ОТМ) органов внутренних дел (далее ОВД) в ходе производства оперативно-розыскных мероприятий и следственных действий;

Методологической основой исследования является диалектический метод научного познания. В процессе исследования также применялись частно-научные методы: сравнительно-правовой, системно-структурный, логический, конкретно-социологический, исторический, статистические методы с приемами анализа и синтеза, описания и др.

Практическая значимость выпускной квалификационной работы состоит в возможности использования содержащихся в ней выводов, предложений и рекомендаций в практической деятельности следственных подразделений органов внутренних дел.

Выпускная квалификационная работа структурно содержит введение, две главы, объединяющие шесть параграфов, заключение и список использованной литературы, приложения.

ГЛАВА 1. УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§1. Компьютерная информация как объекта криминалистического исследования

Компьютеризация различных слоев населения – это социально значимое явление, ее достижения используют не только в хороших целях. Но во время совершения преступлений компьютерного направления. У компьютерных преступлений специфический вид, на данный момент времени – это новация системы уголовного права. Способ совершения компьютерного преступления может быть многогранен и иметь изощренный вид, что документирование и раскрытие этого типа преступлений иногда вызывает некоторые трудности. На основании этого разрабатывают и внедряют новейшие формы, а также методы оперативной розыскной деятельности.

Необходимо заметить, что одним из важнейших составляющих элементов криминалистической характеристики методики раскрытия компьютерных преступлений является субъективная особенность личности преступника, которая на начальном этапе раскрытия преступлений представляется лишь скудной информацией, в связи с чем необходимо учитывать такие составляющие, как пол, возраст, социальное происхождение, уровень образования, род занятий, наличие специальности, семейное положение, социальный статус, уровень материальной обеспеченности, место жительства, а также места проведения досуга и возможная принадлежность к определенной субкультуре. Иными словами, важное значение в раскрытии любого вида компьютерного преступления играют психологические особенности личности преступника.

В действующем уголовном законе на данный момент находится под защитой не только документированная информация, но и ее разновидности, что расширило возможность своевременного изобличения граждан, которые

совершают преступление данного направления. Из проведенного анализа УК РФ можно сказать о том, что отношения, которые возникают в сфере компьютерной информации, на данный момент находятся под специальной охраной.

В главе 28 УК РФ[1] о преступлениях в области компьютерной информации ввели понятия, которых раньше не содержалось в уголовной правовой терминологии, а также в законодательстве, регулировавшем информационные отношения.

Основной предмет посягательств – это компьютерные сведения, определяемые в качестве документированных сведений о лицах, предмете, факте, событии, явлении и процессе, которые хранятся на машинном носители, в электронно-вычислительной машине (далее ЭВМ), системе либо сети ЭВМ, или управляющие ЭВМ.[2]

Понимая под системой любой объект, элементы которого находятся в упорядоченной взаимосвязи, систему ЭВМ можно определить как комплекс, в котором хотя бы одна ЭВМ является элементом системы, либо несколько ЭВМ составляют систему.

Целью системы является повышение эффективности работы ЭВМ. Сетью ЭВМ являются компьютеры, объединенные между собой линиями (сетями) электросвязи, т. е. технологическими системами, обеспечивающими один или несколько видов передач (телефонную, телеграфную, факсимильную передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радиои проводного вещания). К машинным носителям компьютерной информации относятся устройства памяти ЭВМ, периферийные устройства связи, сетевые устройства и сети электросвязи.

Понятие «компьютерная информация» - не менее многозначное, чем

---

[1]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

[2]Карчевский Н. В. Компьютерные преступления: определение, объект и предмет. - /Карчевский Н. В. - Режим доступа: http://www.ifap.ru/pi/05/karchev.htm (дата обращения: 15.03.2021).

понятие «информация». Ее роль в системе правовых нарушений, которые возникают в информационной сфере, до данного момента предмет научной дискуссии, которую пока не завершили формированием общепризнанного научного и законодательного определения, так как многообразие толкований отображает довольно сложный тип реального мира.

Компьютерные сведения могут быть массовыми, если они предназначены для неограниченного числа лиц, либо конфиденциальными, когда принадлежат определенным собственникам, либо их распространение и доступ, ограниченные специальными нормами права, допустим персональные сведения о субъекте, государственной, коммерческой, врачебной тайне и так далее.

Доступ к данным сведениям ограничивают, и требуется специальный допуск. В иных случаях доступ к данным сведениям будет неправомерным.

На основании этого при учете представленных позиций авторов понятие «компьютерная информация» в качестве предмета преступления, возможно, сформулировать в качестве организационно упорядоченной совокупности информации (сообщений, данных), которые зафиксированы на машинных носителях или в информационно-телекоммуникационных сетях с реквизитами, позволяющими идентифицировать, имеющих собственников или иных законных владельцев.

Следовательно, уголовной правовой защите будет подлежать различная информация, неправомерное обращение с которой наносит ущерб собственниками (владельцам, пользователям).

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

Глава №28 УК РФ «Преступления в сфере компьютерной информации» содержит следующие составы преступлений:

- Статья 272. Неправомерный доступ к компьютерной информации

- Статья 273. Создание, использование и распространение вредоносных компьютерных программ
- Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно телекоммуникационных сетей
- Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Не всякий неправомерный доступ образует состав преступления, а лишь такой, при котором наступили вредные последствия для правообладателя информации, затруднившие или сделавшие невозможным для потерпевшего использование информации:

- уничтожение;
- блокирование;
- модификацию;
- или копирование информации.[1]

Одно из определений компьютерной программы – последовательность инструкций, которая предназначена для выполнения устройством управления вычислительного аппарата. В примечании 1 к ст. 272 УК РФ[2] дается определение понятию компьютерной информации. Корректировка и изменения существующих программ по своей сути и есть модификация уже созданного кода программы. Таким образом, формулировка «создание другой компьютерной информации» подразумевает также внесение изменений и корректировок в программу. Причем лицо, создавшее вредоносный код, но при этом не добавившее его в существующую программу, в рамках прошлой редакции статьи не привлекалось к уголовной ответственности, однако в соответствии с новой – подлежит ответственности.

Еще одним определением компьютерной программы является написание

[1]Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. - М., 2012. С.112.
[2]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2017) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

программного кода, а также его преобразование в программу, которая выполняет отрицательные действия. Создание другой компьютерной информации подразумевает любые действия, в результате которых приобретается вредоносный программный код.

Распространением признается совершение действий, приводящих к внедрению программы в гражданский оборот (дарение, продажа), или организация доступа к программе (размещение на незащищенном сервере). Под применением программы понимается самостоятельное использование ее владельцем по прямому назначению. Данные действия должны предназначаться для несанкционированного уничтожения, модификации, копирования, блокирования компьютерной информации и/или нейтрализации защитных средств компьютерной информации.

Уничтожением компьютерной информации считаются действия, результатом которых является потеря возможности отображения этой информации с определенного носителя. Уничтожение возможно реализовать посредством уничтожения электронной копии документа (к примеру, удаление с жесткого диска определенного файла) либо непосредственного повреждения носителя такой копии, что делает невозможным считывание информации (к примеру, повреждение диска). В этом случае квалификация действия будет зависеть от цели умысла злоумышленника либо на уничтожение именно информации, либо на уничтожение самого носителя этой информации. При выяснении умысла только на повреждение или уничтожение носителя информации, деяния лица не образуют состав преступления, предусмотренного ст. 273 УК РФ.[1]

Под блокированием компьютерной информации подразумеваются действия, результатом которых является лишение возможности доступа к определенной информации для законного владельца, причем в таком случае сама информация не повреждается и не уничтожается (к примеру, установка пароля

[1]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

для открытия файла).

Под модификацией компьютерной информации подразумевается внесение изменений, которые повлекли искажение этой информации, при этом собственник не давал своего согласия.

Под копированием компьютерной информации подразумеваются действия, которые направлены на незаконное создание аналогичной версии (дубликата) информации.

К средствам защиты компьютерной информации относят технические, программные, криптографические и любые другие средства, которые предназначены для защиты этой информации. Также к ним относятся средства реализации и контроля над эффективностью защиты информации. Существует и понятие нейтрализации описанных выше средств защиты информации. К ним относятся такие действия, в результате которых средства защиты компьютерной информации не могут выполнять свои функции по защите.

Согласно российскому уголовному законодательству выделяют четыре состава преступлений в сфере компьютерной информации (ст. 272-274.1 УК РФ). Однако существует гораздо больше преступлений, которые совершаются посредством компьютерных технологий. При этом возможности использования данных технологий при совершении преступлений иногда бывают прямо оговорены в законодательстве. Закрепление de-jure применения компьютерных технологий реализуется законодателем через введение в отдельные ст. УК РФ дополнительных статей и квалифицирующих признаков, которые устанавливают ответственность за конкретные деяния, которые являются частными случаями применения информационных технологий в незаконной деятельности.

В качестве примеров применения законодателем указанных методов реагирования на изменяющиеся преступные реалии можно рассматривать новые нормы УК РФ, которые содержат такой квалифицирующий признак, как использование при совершении преступления информационно-телекоммуникационных или электронных сетей (в том числе и сеть интернет) в некоторых статьях УК РФ (ч. 1 ст. 171.2, ч. 1 ст. 185.3, п. «б» ч. 2 ст. 228.1, п. «б»

ч. 3 ст. 242, п. «г» ч. 2 ст. 242.1, п. «г» ч. 2 ст. 242.2 УК РФ)[1], а также введение в УК РФ ст. 159.6 – «Мошенничество в сфере компьютерной информации»[2] и ст. 159.3 – «Мошенничество с использованием платежных карт». [3]

Цель законодателя ясна – противодействовать постоянному возникновению новых видов преступлений, которые совершаются при помощи современных технологий.

Понятны и задачи – использовать потенциал уголовного законодательства для достижения указанной цели.

Однако также очевидно как отсутствие комплексного представления о возможных средствах достижения указанной цели, так и отсутствие реализации поставленных задач. В первую очередь, выделяется отсутствие четкого представления обо всех возможностях уголовного законодательства для качественного противодействия новым видам преступной деятельности, о круге преступных деяний, которые в будущем будут чаще совершаться с помощью компьютерных технологий. Также проблемой остается противоречивое и недостаточное правовое закрепление в уголовном законодательстве терминов технического характера.[4]

Отмеченные обстоятельства вероятнее всего приведут к трудностям практического использования названных правовых новелл, и в результате вызовут очередные законодательные преобразования. Достаточно реальной в этой связи представляется печальная перспектива – дальнейшее применение в процессе правотворчества печально известного метода «проб и ошибок». Таким образом, предполагая дальнейшее совершенствование УК РФ в части ответственности за совершение преступлений посредством компьютерных технологий, достаточно разумно будет внедрение новелл в канву уголовного закона лишь после особо тщательного мониторинга среды, которая генерирует

---

[1]Там же.
[2]Там же.
[3]Там же.
[4]Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. - М.: Юрлитинформ, 2012. – С.112.

преступные проявления, анализа действующей возможности правоприменительных структур регулировать эту среду, учитывая предлагаемые законодательные нововведения, с помощью максимального учета всех возможных последствий использования потенциала уголовного закона при противодействии нежелательным для общества и государства проявлениям в сфере использования компьютерных технологий.

К сожалению, невозможно лишь положительно оценить уже реализованные законодательные преобразования в данной сфере. Попытка адаптировать правовую базу к требованиями информационного сообщества, безусловно, является серьезным позитивным импульсом. Но внесенные изменения не до конца продуманы, в целом носят незавершенный характер, а также на данный момент нуждаются в корректировке. Особый интерес для изучения представляет конструкция норм права, которые устанавливают ответственность за мошенничество посредством платежных карт (ст. 159.3 УК РФ)[1] и мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ).[2]Данные правовые нормы являются безусловными новеллами российского уголовного законодательства, аналогов которым до настоящего времени не имелось.

Необходимость подобных законодательных преобразований социально обусловлена. Ежегодный ущерб от преступных действий с электронными платежами составляет приблизительно 6 миллиардов долларов. Осознавая необходимость особого уголовного правового урегулирования данной области общественных отношений, ФЗ от 29.11.2012 г. «О внесении изменений в УК РФ и определенные законодательные акты РФ»[3] в УК РФ было введено шесть специальных составов мошенничества, и прежде всего мошенничество с

---

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

[2] Там же.

[3] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации от 29 ноября 2012 г № 207-ФЗ (с изменениями и дополнениями от 03.07.2021) // Собрание законодательства РФ. – 03.12.2012. – № 49. – ст. 6752.

применением платежной карты (ст. 159.3 УК РФ),[1] а помимо этого мошенничество в области компьютерных сведений (ст. 159.6УК РФ).[2]

Следует иметь в виду, что правомерный доступ к компьютерному оборудованию не означает правомерности доступа к компьютерной информации, которая предназначается для определенных лиц и выполнения ими соответствующих функций.

Основными средствами неправомерного доступа и преодоления информационной защиты являются:

- ✓ хищение ключей и паролей, использование несовершенства защиты информации,
- ✓ использование визуальных, оптических и акустических средств наблюдения за ЭВМ,
- ✓ использование недостатков программного обеспечения, операционных систем,
- ✓ несанкционированное подключение к основной и вспомогательной аппаратуре ЭВМ, внешним запоминающим устройствам, периферийным устройствам, линиям связи и пр.

В основном для совершения преступления используются программные (55% случаев) либо комбинированные (программные и технические носители) средства.[3]

Физическая деятельность субъектов при создании, использовании и распространении вредоносных программ для ЭВМ (ст. 273 УК РФ)[4] заключается в постановке задачи, определении цели программы, в выборе средств и языка реализации программы, написании текста программы, ее отладке и запуске, а также в ее использовании, т. е. в создании вредоносной программы.

---

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.
[2] Там же.
[3] Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – URL: http://www.mvd.ru/presscenter/statistics/reports (дата обращения 15.03.2021)
[4] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

Вредоносными являются любые программы, специально разработанные либо модифицированные для несанкционированного собственниками информационных систем уничтожения, блокирования, модификации либо копирования сведений, нарушения привычной работы ЭВМ. Создание программы возможно производить непосредственно на ЭВМ в подвергающейся воздействию компьютерной системе, а помимо этого в других местах, где субъекты обладают доступом к персональным компьютерам и имеют нужное для разработки программ оборудование, время и средства.[1]

Наиболее ярким примером этого могут являться хищения путем незаконного электронного перевода денежных средств со счетов граждан путем использования номеров их банковских счетов с обналичиванием денег через подставных лиц. Выявление компьютерных преступлений не всегда означает автоматическое выяснение места его совершения.

Между выявлением и поимкой преступника могут существовать барьеры в виде национальных границ между государствами с разными правовыми системами, в которых по-разному определяется понятие компьютерного преступления, и тогда возмездие за содеянное может не наступить.

Таким образом, в соответствии с российским уголовным законодательством выделяется четыре состава преступлений в сфере компьютерной информации (ст. 272-274.1 УК РФ).[2] Тем не менее, существует намного больше преступлений, совершаемых через компьютерные технологии. И даже иногда возможности использования подобных технологий при совершении преступлений прямо оговорены в законодательстве. Закрепление de- jure применения компьютерных технологий реализуется законодателем через введение в отдельные ст. УК РФ дополнительных статей и квалифицирующих признаков, которые устанавливают ответственность за совершение определенных деяний, являющихся частными случаями

[1]Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. - М.: Юрлитинформ, 2012. – С.112.

[2]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

применения компьютерных технологий в преступной деятельности.

§3. Вредоносные компьютерные программы как элемент криминалистической характеристики

Вместе с тем основная сложность расследования данного рода преступления заключается, прежде всего, в необходимости доказывания факта « вредоносности программ». Отметим, что на сегодняшний момент отсутствует четкое законодательное определение данного понятия, доктринальное его толкование довольно противоречиво.

Во время расследования преступления, связанного с созданием, а помимо этого использованием вредоносной программы, главные задачи расследования состоят в следующем.

1. Определение фактов и способов создания вредоносных компьютерных программ, их использование и распространение.

На практике установление фактов создания вредоносных программ либо компьютерных вирусов очень сложный процесс и зачастую, это возможно сделать только после фактического определения результата их применения.

Само по себе направление действия данной вредоносной программы, равно как и цели ее создания, это проникновение в защищенную компьютерную сеть, повреждение ее либо похищение важных компьютерных сведений. Именно на основании этого практически во всех фактах расследования неправомерного доступа к компьютерным сведениям, возможно, говорить о преступлениях, предусмотренных ст. 273 УК РФ.[1]

Факты применения вредоносных программ, зачастую выявляют антивирусные программы, в случаях их отсутствия в качестве признаков

[1]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2017) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

преступлений выступает сбой работы систем и ПО, повреждение информации и так далее.

Следовательно, чаще всего преступления выявляют сами пользователи компьютера и потерпевшие.

2. Определение лиц, виновных в совершении преступлений.

В профессиональном плане чрезвычайно широк круг преступников, которые совершают преступления с помощью компьютерных технологий. Это различные и достаточно отличные друг от друга категории специалистов: инженеры, программисты, системные администраторы, бухгалтеры, банковские служащие, финансисты, руководители, юристы. Тем не менее, их всех можно разделить на две группы. Критерий разделения в этом случае – возможность неограниченного доступа к компьютерным технологиям:

1. Внешний пользователь.
2. Внутренний пользователь.

В предложенной классификации пользователь определяется как лицо, которое имеет доступ к системе для получения соответствующей информации с целью ее использования. Пользователи также подразделяются на две другие категории:

- санкционированные пользователи, которые имеют право доступа к информации.

- несанкционированные пользователи, которые получают доступ незаконно.

Наибольшая опасность компьютерного преступления исходит именно от внутренних пользователей информационной системы. Соотношение преступлений следующее: около 6% подобных преступлений совершается внешними пользователями; около 94%– внутренними. При этом клиентами и пользователями компьютерных систем является, как правило, 70% преступных лиц; 24% злоумышленников – обслуживающий персонал; 6% -

другие лица.[1] Также исследователями выделяются наиболее распространенные мотивы противоправного поведения:

- корысть (53%);
- политические мотивы (17%);
- хулиганские побуждения (15%);
- жажда мести (9%);
- иные мотивы (6%).[2]

К последним могут также относиться: интеллектуальный вызов исследовательский интерес и т.п. Вместе с тем в 52% случаев происходит хищение денег или иного ценного имущества; в 16% преступлений – уничтожение и повреждение компьютерной информации; в 12% случаев – подмена данных; в 10% случаев – хищение ПО или охраняемой информации; оставшиеся 10% случаев приходятся на противоправную активность, направленную на хищение оказываемых услуг.[3]

3. Установление вреда, причиненного данным преступлением.

Данное преступление отнесено законодателем к категории тяжких. Тяжесть последствий — это оценочная категория, устанавливаемая правоприменителем в каждой конкретной ситуации. Примерами тяжких последствий могут служить существенные сбои в работе транспортных, коммунальных и иных организаций, аварии и повреждения на социально значимых объектах инфраструктуры, причинение лицу вреда здоровью или смерти. При этом следует учесть возможные сложности при определении тяжести последствий. Так информация, в отличие от материальных объектов, не имеет объективной цены производства и потребительской стоимости. Таким образом, стоимость информации для нескольких лиц может быть различна. Это может привести к тому, что цена информации в случае кражи

[1]Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – URL: http://www.mvd.ru/presscenter/statistics/reports (дата обращения 15.03.2017)
[2]Там же.
[3]Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – URL: http://www.mvd.ru/presscenter/statistics/reports (дата обращения 15.03.2017)

(копирования) может измениться: как увеличиться, так и уменьшится. Для расчета тяжести последствий при отсутствии соответствующей практики Верховного суда РФ некоторые авторы предлагают использовать по аналогии практику расчета ущерба при нарушении авторских и смежных прав, поскольку, согласно ч.1 ст. 1259 ГК РФ[1], программы для ЭВМ относятся к объектам охраны авторских прав и охраняются как литературные произведения. Указанная точка зрения представляется нам не совсем верной, поскольку компьютерная информация является более широким понятием, и помимо программ для ЭВМ включает в себя иные объекты. Однако учитывая отсутствие законодательно закрепленных разъяснений высших судебных органов, она также имеет право на существование.

Значительные проблемы возникают при установлении признаков неправомерного доступа к компьютерной информации. Отсутствие единого понимания того, что следует относить к неправомерному доступу и отсутствие каких- либо разъяснений по этому вопросу со стороны Верховного суда РФ приводят к существенным затруднениям в оценке содеянного.

В судебной практике есть существенные проблемы, которые связаны с квалификацией незаконного доступа к информации, связанного с совершением других преступлений, к примеру, нарушений авторских прав, хищений и т.д. В основном это связано с недопониманием правоприменителями самой сути уголовно- правовой охраны компьютерной информации в качестве объекта посягательства. Например, Захаровский районный суд Рязанской области вынес приговор от 10.06.2011г.,[2] в соответствии с которым установлены следующие обстоятельства противоправного деяния: обвиняемый незаконным путем получил доступ к персональным учетным данным абонентов ОАО « ЦентрТелеком» и,

[1]Там же.

[2]Приговор Захаровского районного суда Рязанской области от 10.06.2011г. в отношении Захарова П.В. // РосПравосудие: [сайт]. URL: https://rospravosudie.com/court-zaxarovskij-rajonnyj-sud-ryazanskaya-oblast-s/act-100404151/ (дата обращения: 15.03.2017).

используя одну из учетных записей, подключился к сети интернет. Данные действия квалифицированы судом в совокупности ч. 1 ст. 272 УК РФ и ч. 1 ст. 165 УК РФ.[1] УК называется, что подсудимый незаконно подключался к сети интернет, получал там информацию, используя при этом трафик в количестве 10.511,66 Мбайт. Юридически оценивая деяния подсудимого, суд провел квалификацию его действий отдельно по каждому из 111 эпизодов совершенных им 91 преступлений, предусмотренных ч. 1 ст. 272 УК РФ,[2] как неправомерный доступ к охраняемой законом компьютерной информации, и одного длящегося преступления, предусмотренного ч. 1 ст. 165 УК РФ,[3] как причинение имущественного ущерба собственнику путем обмана при отсутствии признаков хищения. По нашему мнению, квалификация причинения имущественного ущерба как единого деяния ошибочна, и данные действия следовало бы квалифицировать как отдельные эпизоды, в каждом случае, когда в результате неправомерного доступа потерпевшему причинялся материальный ущерб.

4. Определение обстоятельств, которые способствовали совершению
расследуемых преступлений.

Как и в случаях неправомерного доступа к компьютерным сведениям, разрешение данной задачи поможет наиболее верно квалифицировать деяния, хоть по значению она второстепенная.

Помимо всего вышесказанного возникает проблема в признании статус « вредоносной» экспертом компьютерной программы.

При разработке компьютерной программы или другой компьютерной информации умысел бывает косвенным или прямым. Косвенный умысел возможен тогда, когда лицо создает, к примеру, программу, которая предназначается для демонстрации введенного пользователем пароля. Главная

[1]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.
[2]Там же.
[3]Там же.

цель программы – напомнить пароль владельцу, но создатель программы понимает возможность незаконного использования этой программы. Преступление с прямым умыслом подразумевает, что лицо полностью осознает, что созданная компьютерная программа либо иная компьютерная информация предназначается для несанкционированного уничтожения, модификации, копирования, блокирования компьютерной информации и/ или нейтрализации средств защиты этой информации. Помимо этого преступник предвидит возможность и/ или неизбежность наступления вредных последствий при ее использовании, а также желает их наступления.

При использовании или распространении компьютерной информации имеет место только прямой умысел. Лицо в любом случае осознает, что используемая или распространяемая им программа либо другая компьютерная информация предназначена для несанкционированного уничтожения, модификации, блокирования компьютерных сведений или нейтрализации их средств защиты, предвидит появление опасного последствия и хочет этого. Цели и мотивы не являются обязательными признаками состава данных преступных действий и не станут влиять на их квалификацию. Помимо этого совершение преступлений, которые предусмотрены в ст. 273 УК РФ,[1] создают состав преступления лишь в случаях, когда подобная программа заведомо предназначается для несанкционированного уничтожения, модификации, копирования, блокирования компьютерных данных или нейтрализации их средств защиты.

Признак заведомости предполагает, что лицо при создании компьютерной программы или при внесении в нее изменений достоверно знает о ее вредоносности. Причем достаточно, чтобы данное лицо знало хотя бы о некоторых вредоносных свойствах программы, а не строго обо всех.

[1]Там же.

Например, достаточно спорным является вопрос о вменении статьи 273 УК РФ[1] в случае взлома компьютерных программ с применением « кейгенов» - специальных программ, генерирующих лицензионные ключи и позволяющих использовать программы без их покупки. Так, приговор мирового судьи судебного участка № 48 Самарской области от 06.06.2011г.[2] содержит следующую квалификацию деяний: Подсудимый предоставил любому пользователю возможность скопировать контрафактный экземпляр ПО Microsoft Windows XP:« Microsoft Office (далее по тексту МО) 2003»,« МО Excel», « МО Outlook», « МО Word», « МО Visio», « МО Power Point», « МО Access» посредством размещения в файлообменнике ссылок для их загрузки. При этом файлы имели признаки контрафактности, а также характеризовались отсутствием защиты от нелицензионного копирования, предусмотренной производителем.

В отличие от лицензионных продуктов, файлы, не предусматривали введения лицензионного кода при установке. Исходя из диспозиции статьи 273 УК РФ,[3] в действиях подсудимого содержались признаки распространения программ с внесенными изменениями, заведомо приводящими к несанкционированной модификации информации. Однако суд признал подсудимого виновным в совершении только преступления, предусмотренного ч. 2 ст. 146 УК РФ.[4] Вопрос привлечения к ответственности по ст. 273 УК РФ даже не рассматривался, что, по нашему мнению, является судебной ошибкой. Приговор Советского районного суда г. Томска от 10.03.2011г.[5] содержит такие выводы, касающиеся квалификации действий

---

[1]Там же.

[2]См.: Приговор мирового судьи судебного участка N 48 Самарской области от 06.06.2011г. в отношении Мордвинцева. // РосПравосудие: [сайт]. URL: https://rospravosudie.com/court-sudebnyj-uchastok-48-samarskoj-oblasti-s/act-200780468/ (дата обращения: 15.01.2017).

[3]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2017) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

[4]Там же.

[5]Приговор Советского районного суда г. Томска от 10.03.2011г. в отношении Регнера И.В. // РосПравосудие: [сайт]. URL: https://rospravosudie.com/court-sovetskij-rajonnyj-sud-g-tomska-tomskaya-oblast-s/act-100402140/ (дата обращения: 15.03.2017).

виновного: Регнер И.В. незаконно пользовался объектами авторского права программных продуктов: « MO 2007», « AutoCAD», « Microsoft Windows XP», «1С: Предприятие», осуществляя их установку на жесткий диск клиента за вознаграждение. Причем, при установке ПО он пользовался программой « MSOE2007KG», которая предназначена для случайной генерации лицензионных ключей для программы « MO 2007», а также программу « AutoCAD – 2008- keygen», для генерации лицензионных ключей программы « AutoCAD». Действия Регнера И.В. суд квалифицировал по ч. 2 ст. 146 УК РФ,[1] как незаконное использование объектов авторского права совершенные в крупном размере.

Представляют определенный интерес для исследования выводы суда в части привлечения подсудимого к ответственности за совершение деяний, предусмотренных ст. 272 и ст. 273 УК РФ.[2] В приговоре указано, что, в соответствии с заключением экспертизы, программы « MSOE2007KG» и « AutoCAD-2008- keygen» предназначены для генерации кода активации. При использовании этих программ не происходит модификации информации.

Следовательно, по факту использования упомянутых программ суду не были предоставлены доказательства наличия необходимого элемента объективной стороны этого преступления – возникновения последствия, предусмотренного ч. 1 ст. 272 УК РФ,[3] - модификации компьютерной информации. Также суд оправдал Регнера И.В. в совершении предусмотренных ч. 1 ст. 273 УК РФ[4] действий, постановив, что диспозиция статьи 273 УК РФ[5] предусматривает ответственность за использование программ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ,

[1]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2017) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.
[2]Там же.
[3]Там же.
[4]Там же.
[5]Там же.

системы ЭВМ или их сети. Учитывая, что в заключении экспертизы указано, что программы « MSOE2007KG» и « AutoCAD – 2008- keygen» не модифицируют программный код, а лишь обманывают систему защиты, данные обстоятельства свидетельствуют об отсутствии в действиях подсудимого необходимого элемента объективной стороны несанкционированной модификации компьютерной информации. Как видно, суд признал использование « кейгенов» действиями, не содержащими состава предусмотренного ст. 273 УК РФ[1] деяния.

В то же время, Приговором Октябрьского районного суда г. Кирова от 24.12.2013г.[2] дается иная квалификация при сходных обстоятельствах. Как установлено судом, Сиков Д.В. скопировал из сети Интернет программные продукты « Autodesk 3ds Max 2012», « Autodesk 3ds Max 9», « CorelDRAW» и установил их на персональный компьютер, предоставленный сотрудниками отдела «К». Указанные действия получили квалификацию по ч. 2 ст. 146 УК РФ,[3] как незаконное использование объектов авторского права. Кроме того, суд установил наличие в действиях подсудимого состава преступления, ответственность за которое предусмотрена ч. 1 ст. 272 УК РФ,[4] обосновав свою позицию следующим: Сиков Д.В. при активации программного продукта « Autodesk 3ds Max 2012» осуществил запуск специальной программы « xf- adesk2012x32. exe», и с помощью данной программы перехватил механизм генерации активационного кода программного продукта « Autodesk 3ds Max 2012», модифицировав память персональной ЭВМ, содержащую исполняемый код программного продукта « Autodesk 3ds Max 2012», что привело к блокированию исходных функций проверки

[1]Там же.
[2]Приговор Октябрьского районного суда г. Кирова от 24.12.2013 г. в отношении Сикова Д.В. // РосПравосудие [сайт]. URL: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-445968591/ (дата обращения: 15.01.2017)
[3]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2017) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.
[4]Там же.

корректности кодов активации данного программного продукта и незаконной выдаче кода активации программного продукта « Autodesk 3ds Max 2012».

После чего им вводится незаконно полученный код активации в соответствующее окно запросов программы « Autodesk 3ds Max 2012», а следовательно умышленно осуществляется нейтрализация средств защиты.

Помимо этого суд привлекает лицо к ответственности по ч. 1 ст.273 УК РФ[1] за распространение и применение компьютерных программ, которые заведомо предназначены для несанкционированного блокирования, модификации компьютерных данных, а также нейтрализации средств защиты компьютерных данных. Сходная аргументация при соответствующих обстоятельствах совершенного деяния содержится и в Приговоре Октябрьского районного суда г. Кирова от 11.12.2013 г.[2] В Постановлении мирового судьи судебного участка № 49 г. Находка от 16.01.2014 г.[3] при сходных обстоятельствах совершенного деяния суд вообще не исследовал вопрос наличия признаков предусмотренных ст. 272, ст. 273 УК РФ[4] преступлений в действиях подсудимого. Подсудимый загрузил на собственный персональный компьютер контрафактное ПО – программу « MicrosoftWindows 7» и программы « КОМПАС- 3D», « КОМПАС- Электрик» и « КОМПАС- Электрик V14» с целью последующего сбыта, после чего незаконно реализовал их путем установки на персональный компьютер третьего лица. Руководствуясь ст. 25 УПК РФ,[5] суд прекратил уголовное дело в отношении подсудимого, обвиняемого в совершении преступления,

---

[1]Там же.

[2]Приговор Октябрьского районного суда г. Кирова от 11.12.2013г. в отношении Пленкина А.А. //РосПравосудие: [сайт]. URL: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-447482174/ (дата обращения: 15.03.2021).

[3]Постановление и.о. Мирового судьи судебного участка № 49 г. Находка от 16.01.2014г. // РосПравосудие: [сайт]. URL: https://rospravosudie.com/court-sudebnyj-uchastok-49-g-naxodka-s/act-213736047/ (дата обращения: 15.03.2017).

[4]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

[5]Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (в редакции от 16.03.2017) // Собрание законодательства РФ. – 24.12.2001. – № 52. – ст. 4921.

предусмотренного ч. 2 ст. 146 УК РФ,[1] в связи с примирением с потерпевшими. Как представляется, такое обстоятельство, как примирение с потерпевшим не освобождает суд от обязанности установления всех обстоятельств дела и наличия в действиях лица иных составов преступления. Также отсутствие единства судебной практики, приводящее к совершению судом ошибок при квалификации рассматриваемой группы деяний характерно проявилось в Приговоре Егорьевского городского суда Московской области от 26.10.2011 г.[2] Суд установил, что Миленин А.С. незаконно приобрел, путем загрузки из сети « Интернет», список IP- адресов, используемых компьютерами удаленных пользователей, ввел их в установленную на своем компьютере вредоносную программу, предназначенную для подбора паролей и логинов, с помощью которой получил логин и пароль, используемые компьютером потерпевшего.

Указанные действия суд квалифицировал как преступление, которое предусматривается в ч. 1 ст. 273 УК РФ,[3] - незаконное использование программы, которая заведомо приводит к незаконному копированию информации о логине и пароле, используемых компьютером; с использованием этой информации впоследствии был осуществлен неправомерный доступ в компьютер, содержащий конфиденциальную информацию. Необходимо отметить, что логин и пароль жертвы данного преступления относятся к охраняемой законом компьютерной информации, поэтому совершение подобных действий должно быть квалифицировано как совокупность предусмотренных ст. 272 и ст. 273 УК РФ[4] деяний. Однако данная квалификация не произведена, что является ошибкой. После суд

---

[1]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

[2]Приговор Егорьевского городского суда Московской области от 26.10.2011г. в отношении Миленина А.С. // РосПравосудие: [сайт]. URL: https://rospravosudie.com/court-egorevskij-gorodskoj-sud-moskovskaya-oblast-s/act-105695669/ (дата обращения: 15.03.2021).

[3]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

[4]Там же.

установил, что А.С. Миленин, используя полученный логин и пароль, осуществил через интернет со своего компьютера незаконный доступ к компьютеру жертвы преступления, тем самым считается, что он совершил незаконный доступ к охраняемой компьютерной информации. Затем преступник, обнаружив на компьютере программу платежной системы, предпринял попытку подободрать пароль, чтобы получить доступ к ней, но перестал пробовать, когда не получил желаемого. Следовательно, А.С. Миленин совершил преступление, которое предусматривает ч. 1 ст. 272 УК РФ.[1] Подобные действия необходимо оценивать не только как незаконный доступ к компьютерной информации, охраняемой законом, но и как применение вредоносных компьютерных программ (ст. 273 УК РФ),[2] так как использовалась программа, которая осуществляет подбор пароля для платежной системы. Также следует рассматривать данное деяние как покушение на кражу денег, находящихся в упомянутой платежной системе (ст. 159 УК РФ).[3] Затем суд постановил, что А.С. Миленин со своего компьютера через интернет совершил незаконный доступ к компьютеру жертвы преступления, т.е. совершил незаконный доступ к компьютерной информации, охраняемой законом, после чего он попытался подобрать пароль к установленной на том компьютере программе платежной системы, но, не сумев, установил вредоносную программу на компьютер потерпевшего.

Следовательно, подсудимый совершил преступление, которое предусматривается в ч. 1 ст. 272 УК РФ.[4] Попытка подобрать пароль к платежной системе и в этом случае должна быть оценена как применение вредоносных компьютерных программ так же, как и установление вредоносной программы на чужом компьютере отвечает признакам деяния,

[1]Там же.
[2]Там же.
[3]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.
[4]Там же.

которое предусматривается в ст. 273 УК РФ.[1] Указанная квалификация не дана судом этому деянию, что является ошибкой. И наконец, суд постановил, что А.С. Миленин осуществил через интернет незаконный доступ к чужому компьютеру, затем подобрал пароль к установленной программе платежной системы, зашел в программу и осуществил операции перечисления денежных средств потерпевшего с электронного кошелька в платежной системе « Рапида» на счет своего мобильного телефона в сумме 50 рублей, а также на принадлежащий ему электронный кошелек в сумме 402 690 рублей. Т.е. он тайно похитил денежные средства и распорядился ими в собственных целях, чем причинил ущерб на общую сумму 402 740 рублей, которая является крупной. Этот эпизод суд квалифицировал как преступление, по которому предусмотрена ответственность в соответствии с п. «в» ч. 3 ст. 158 УК РФ[2] – кража.

Можно сделать вывод, что вменение кражи в этом случае следует осуществлять по совокупности со ст. 272 УК РФ,[3] так как налицо незаконный доступ к компьютерной информации, охраняемой законом, а именно данным электронного кошелька жертвы преступления. Но суд не квалифицировал таким образом преступление, что является судебной ошибкой. Таким образом, для рассмотренных судебных решений характерно наличие противоречивой квалификации деяний, совершенных при похожих обстоятельствах. На основе проведенного анализа, можно сделать вывод, что существующая судебная практика по данной категории дел не отвечает критерию единства, а подчас является взаимоисключающей. Приведенные примеры также свидетельствует о необходимости скорейшего принятия Пленумом Верховного суда РФ, специального постановления, разъясняющего наиболее острые и спорные вопросы правоприменительной деятельности в

[1]Там же.
[2]Там же.
[3]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

части оценки деяний, посягающих на безопасность компьютерных систем, в том числе в части соотношения с другими преступлениями.

§4. Иные элементы криминалистической характеристики преступлений, совершаемых в сфере компьютерной информации

Анализ свойств, а помимо этого признаков преступности с применением компьютерной технологии довольно сложный по определенным причинам. Первая и основная из них – это отсутствие в науке одного, устоявшегося терминологического аппарата для этой области противоправных деяний. В качестве еще одной причины выступает довольно высокая степень латентности преступности в целом, в том числе с применением компьютерной технологии. Степень латентной преступности на данный момент составила, 70-80 процентов от реальной преступности к судебной уголовной ответственности при этом привлекают примерно пять процентов лиц, которые реально совершили преступление[1].

По данным проведенных опросов 85,71% пострадавших от компьютерных преступников не заявляют об этом в правоохранительные органы.[2] Как правило, причинами этого является отсутствие существенного ущерба, разрешение вопроса иными средствами, неверие в способность правоохранительных органов раскрыть такое преступление и т.п. Структура компьютерных преступлений, которые совершаются на территории РФ, достаточно разнородна, данные о ней отрывочны, а также не систематизированы даже как минимум в пределах десяти лет.

Общий размер материального ущерба составил 3 млн. 945 тыс. 557 долларов США и 32 цента (по курсу ЦБ РФ на 06.03.2017: 1 USD = 56,62

[1]См.: Селиванов Н. А. Проблемы борьбы с компьютерной преступностью // Законность. 2013. № 8. С. 37.

[2]Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. – URL: http://www.mvd.ru/presscenter/statistics/reports (дата обращения 15.03.2021)

RUB)[1].

Ниже представлена статистика по способам выявления компьютерных преступлений к общему числу официально зарегистрированных (рис.1.1):

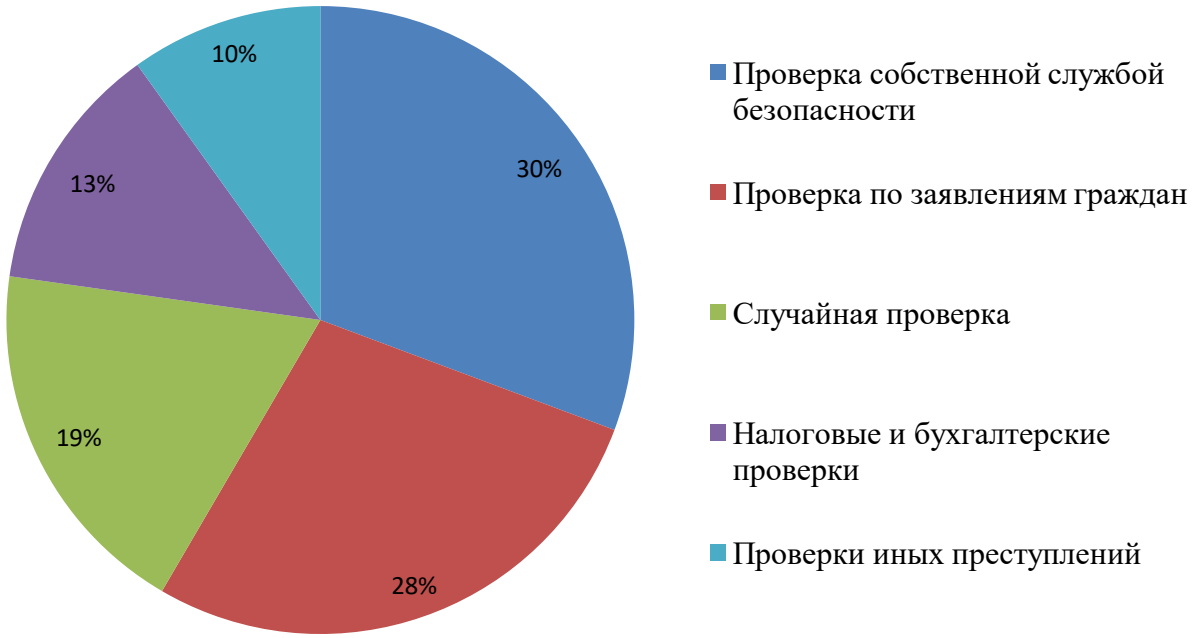

Рис. 1.1. Статистика выявления компьютерных преступлений

Проанализировав приведенные данные, можно сделать следующий вывод:

- основным противоправным деянием является неправомерный доступ. Мошенничество, которое составляет основу всей преступной деятельности с компьютерными технологиями, занимает в официальной статистике долю около 2%;

- примерно 60% фактов совершения преступлений в сфере компьютерных технологий расследуются после заявлений потерпевших либо

[1]Черкасов В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий. Саратов, 2015. С. 81.

свидетелей.

Следовательно, можно утверждать, что, как правило, жертвы компьютерных преступлений скрывают или игнорируют факт информационных или финансовых потерь.

Понятие компьютерного преступления неразрывно связано с определением лица, которое совершает данное преступление. Исследуя личность компьютерного преступника необходимо обратить внимание на специфические особенности, характерные для лиц, использующих высокие технологии в своей преступной деятельности. Это касается мировоззрения и некоторых особенностей взаимодействия участников преступной среды, что накладывает отпечаток на виды и методы совершения лицом незаконных действий.[1]

Трактовка этого понятия тесно связана со смыслом, заложенным в нем исследователем. Поэтому рассмотрение компьютерного преступника возможно как в широком, так и в узком смысле. В узком смысле, компьютерный преступник – это человек, который совершил как минимум одно из преступлений в сфере компьютерной информации, перечисленных в УК. Такое определение значительно ограничивает круг лиц, которые относятся к компьютерным преступникам. В этом случае личностные характеристики, как правило, будут зависеть от противоправного деяния, которое лицо совершило. В главе 28 УК РФ законодатель первой установил ответственность за незаконный доступ к компьютерной информации (ст. 272 УК РФ).[2]

Незаконный доступ к информации – это получение возможности достать компьютерную информацию вне ведома ее владельца и без его разрешения. Преступник, который совершает подобное деяние, как правило,

---

[1]Карчевский Н. В. Компьютерные преступления: определение, объект и предмет. - / Карчевский Н. В.- Режим доступа: http://www.ifap.ru/pi/05/karchev.htm (дата обращения: 15.03.2017).

[2]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2017) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

всегда технически подготовлен, обладает определенными программно-аппаратными методами и навыками, которые позволяют облегчить совершение преступления. Зачастую, это лицо, которое имеет техническое образование. Преступник обладает беспрепятственным доступом к компьютерным технологиям и сети интернет. Вместе с тем, современное развитие информационной среды предоставило дополнительные возможности для преступления – преступнику уже не обязательно иметь глубокие познания о компьютерных технологиях. Как правило, базовых навыков работы за компьютером бывает достаточно, особенно, если они подкреплены подробными инструкциями, которые легко можно найти в интернете, и недостаточным выполнением жертвой требований.

Существующие границы возраста злоумышленника: 18–45 лет. Соотношение преступников, которые совершают незаконный доступ к охраняемой компьютерной информации, представлено на рис. 1.2. Разделение сделано по принципу приобретения соответствующих навыков для совершения преступления. Рис. 1.2. Соотношение преступников в зависимости от получения соответствующих навыков для совершения преступления[1].

[1]Карчевский Н. В. Компьютерные преступления: определение, объект и предмет. - / Карчевский Н. В.- Режим доступа: http://www.ifap.ru/pi/05/karchev.htm (дата обращения: 15.03.2017).

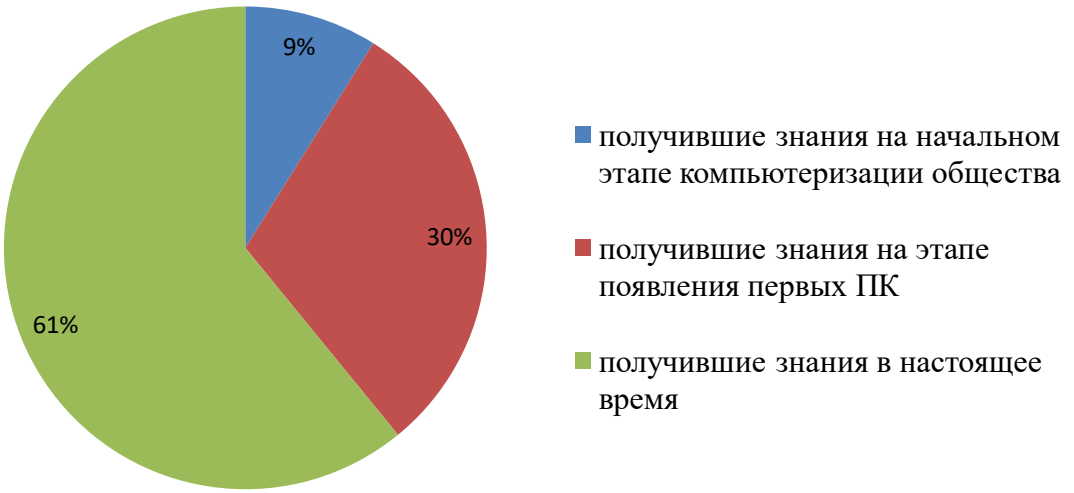

Рис. 1.2. – Соотношение преступников в зависимости от получения соответствующих навыков для совершения преступления.

Таким образом, можно классифицировать преступников, которые совершают предусмотренное ст. 272 УК РФ[1] деяние, в зависимости от степени вовлеченности в запрещенную законом деятельность (таблица 1):

Таблица 1

Классификация компьютерных преступников

Группа	Возраст	Пол	Образование	Уровень достатка	Навыки
1	2	3	4	5	6
а) Начинающие	18-30	Преобладает «мужской»	среднее, среднее специальное или высшее (иногда неоконченное)	средний	существенные познания в области компьютерных технологий, включая языки программирования, а также программно-

[1]Там же.

					аппаратных частей компьютерных устройств
б) Устойчивые	20-25	Преобладает «мужской»	высшее либо незаконченное высшее техническое образование	средний и выше среднего	глубокие и системные знания в сфере компьютерных технологий, языков программирования, а также программно-аппаратной части компьютерных систем
в) Профессиональные	более 25	Преобладает «мужской»	высшее техническое образование, второе высшее образование, преимущественно по юридическим или экономическим специальностям	выше среднего	высокий уровень знаний в области компьютеров и компьютерных технологий; навыки программирования на нескольких языках, глубокие знания в области программных средств и устройства аппаратной части компьютерных систем

Далее более подробно рассмотрим представленные в таблицы группы.

а) Начинающие.

Эти лица, как правило, не имеют постоянную работу или они работают с компьютерными технологиями (специалисты компьютерных фирм, администраторы баз данных и т.п.). Для их личности характерно увлечение компьютерными технологиями. Незаконную деятельность они зачастую начинают, не задумываясь, что их деяния – преступные. Целенаправленное преступное поведение появляется внезапно, как правило, под влиянием череды удачных взломов лицензионных программ на собственном компьютерном устройстве и/ или принадлежащих другим лицам устройствах. Зачастую их деятельность также связана с незаконным распространением и выкладыванием на сервер в открытый доступ взломанных программных

продуктов.

б) Устойчивые.

В этой группе наблюдается тенденция к росту активности женщин: в настоящее время их доля составляет около 5%. Представители этой группы в преступной деятельности осознано применяют заранее подготовленные программно- аппаратные инструменты, которые они самостоятельно разработали или нашли в интернете.

в) Профессиональные.

В этой группе доля женщин составляет уже около 8%. Представители этой группы имеют профессиональные навыки работы с множеством компьютерных платформ, большинством пакетов специализированного программного обеспечения (далее по тексту – ПО) (офисное, сетевое ПО, пакеты разработки приложений) и с главными операционными системами. Также они владеют полной информацией о главных системах электронных коммуникаций (сетевых протоколах, сотовой связи, защищённой связи, систем и способов защиты информации) и используют данные знания в незаконной деятельности.

Мотивация преступного поведения формируется, как правило, на стадии изучения информационных технологий и сначала подкрепляется только желанием продемонстрировать интеллектуальное превосходство, а не стремлением получить выгоду. Преступники зачастую имеют связи, в том числе, в государственных структурах и используют их при необходимости. У них есть легальная работа, в основном для алиби, как правило, в отделе информационных технологий в крупной организации: банк, зарубежная компания и государственный орган. И вместе с тем основным заработком выступает деятельность в полулегальной, а также криминальной среде. Преступники постоянно совершенствуют свои знания в области средств противоправной деятельности, зачастую сами их и разрабатывают.

Таким образом, личностные признаки преступника ограничены самой сущностью компьютерной программы – программный код, являющийся

набором команд для компьютерного устройства, в результате которых появляются какие- либо вредные последствия для пользователя или самого устройства. Следовательно, для написания такого программного кода злоумышленник должен обладать знаниями языка программирования, а также опытом по написанию компьютерных программ. Поэтому вывод следующий – автор вредоносной компьютерной программы является квалифицированным компьютерным специалистом.

Для большинства лиц, которые совершают преступления посредством компьютерных технологий, характерен высокий уровень интеллекта[1]. Доля их составляет около 77%. Для 21% преступников характерно развитие интеллекта выше среднего. Только у 2% лиц установлен более низкий уровень.

Приведем примеры из практики.

Так, Низамов Н.В. совершил неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно- вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это повлекло копирование информации при следующих обстоятельствах.

В начале 2010 года Низамов Н.В., владеющий компьютерной техникой и имеющий опыт работы в области высоких технологий, по личной просьбе сотрудников УИИ № был допущен к служебным компьютерам инспекции для установки антивирусной программы и последующего обновления данной программы до декабря 2010 года.

В июле 2010 года Низамов Н.В., находясь в помещении кабинета № УИИ №, имея неограниченный доступ к служебному компьютеру УИИ №, неправомерно осуществил копирование охраняемой законом компьютерной информации, а именно баз данных « АКУС» (автоматизированный картотечный учет спецконтингента) и « Паспорта 2007», с использованием

[1]Криминалистика: Учебник / Под ред. Р. С. Белкина. М., 2019. С. 950 - 951.

съемного электронного носителя. При этом Низамов Н.В. неправомерно установил программу « клавиатурный шпион»- ActualSpy (фактический шпион), с помощью которой он получил пароли доступа к незаконно скопированной им компьютерной информации. После чего Низамов Н.В. разместил указанную незаконно полученную компьютерную информацию в сети Интернет на сайте www. ksivi. ru.

Подсудимый с предъявленным обвинением согласился полностью, и в присутствии защитника и после консультации с ним, ходатайствовал о постановлении приговора в особом порядке, без проведения судебного разбирательства.

Деяние Низамова Н.В. суд квалифицирует по части 1 статьи 272 УК Российской Федерации /в редакции Федерального закона от ДД. ММ. ГГГГ № 81- ФЗ\- неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло копирование информации[1].

Так, Курочкин К.А. был признан виновным в том, что с 20 часов 16 минут 07 июня 2010 года до 19 часов 37 минут 08 июня 2010 года, применяя персональный компьютер, при помощи незаконного применения регистрационной информации (логина и пароля), которые принадлежали ФИО2 где он работал, незаконно осуществляет неправомерный доступ при помощи сети « Интернет» к компьютерным данным ФИО2 что приводит к блокированию доступа законного пользователя сети (работников ФИО2) к внутреннему ресурсу организации, копированию сведений, принадлежащих ФИО2, модифицированию сети ЭВМ: смене паролей системных администраторов, администраторов программы «1С- Бухгалтерия».

Во время судебного заседания Курочкин К.А. вину признает в полном объеме и заявляет ходатайство о проведении особенного порядка судебного

[1]Приговор Авиастроительного районного суда г. Казани от 17 апреля 2012 года // Архив Авиастроительного районного суда г. Казани

разбирательства, поясняя, что осознал характер и последствия заявленного ходатайства, которое он заявил добровольно после консультаций со своими защитниками.

Проверив материалы уголовного дела, обсудив доводы кассационной жалобы, судебная коллегия сочла, что приговор суда в отношении Курочкина К.А. законный, обоснованный и справедливый.

Рассмотрев уголовное дело в особенном порядке принятия судебного решения, суд действия Курочкина К.А. квалифицирует по ч. 1 ст. 272 УК РФ,[1] в качестве неправомерного доступа к охраняемых законом компьютерным сведениям, то есть сведениям на машинных носителях, в электронно- вычислительных машинах (ЭВМ), системах ЭВМ либо их сетях, когда данные деяния влекут уничтожение, блокирование, модификацию, нарушение работы ЭВМ, систем ЭВМ либо их сетей[2].

Таким образом, следует сказать о то, что применение компьютерной технологии во время совершения преступления – это особенная разновидность общественно опасной, а кроме этого противоправной деятельности, на данный момент времени которая получила наибольшее распространение в глобальном масштабе, а помимо этого в определенных странах и в том числе в РФ. Рассматриваемый тип преступлений обладает следующими, объясняющими возросшую стремительным темпом « популярность» в криминальной среде, чертами: высоким уровнем латентности, объясняющимся в качестве всеобъемлемой компьютеризацией общественной и личной жизни, а также трансграничным типом преступной деятельности и связанной с этим неуловимостью компьютерных преступников, а помимо этого сравнительная простота совершения преступления.

---

[1]Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (редакции от 30.03.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.

[2]Кассационное определение Верховного Суда Республики Татарстан по делу № 22-6848 от 02 ноября 2010 года // Архив Верховного Суда Республики Татарстан

ГЛАВА 2. ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ И ВЗАИМОДЕЙСТВИЯ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

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

Организация начального этапа расследования зависит от того, какая следственная ситуация сложилась к моменту возбуждения уголовного дела.

Под следственной ситуацией понимается объективная криминалистическая категория, отражающая положение в определенный момент расследования, характеризующаяся содержанием криминалистически значимой информации и степенью достаточности ее для принятия решений следователем или прокурором.

Во время проведения начального этапа расследования организацию сводят, прежде всего, к работе с информацией - к ее восприятию, анализу, переработке, оценке, систематизации, синтезу.

На основании результата обработки исходных сведений выдвигают версию, определяют задачи расследования, следователи принимают решения, организуют их исполнение и осуществляют контроль за выполнением каждым участником процесса.

В результате они получают новые сведения, которые, в свою очередь, воспринимаются, анализируются, перерабатываются, синтезируются, что приводит к постановке новейших задач и принятию новейших управленческих решений и корректировке предыдущих.

Все время по ходу данного процесса следователи прогнозируют расследование, в общем, поведение подозреваемых, обвиняемых, заявителей о компьютерных преступлениях, свидетелей, иных участников расследования, а помимо этого возможное недобросовестное противодействие со стороны

защиты.

Организация расследования осуществляется с использованием программно- целевого метода, метода мысленного моделирования, криминалистического факторного анализа и комплексного подхода. Для начального этапа расследования компьютерных преступлений наиболее типичны следующие ситуации:

- собственник или правообладатель компьютерной информации самостоятельно выявил факт преступления и обнаружил лицо, его совершившее;
- собственник или правообладатель компьютерной информации самостоятельно выявил факт преступления, но преступник не известен;
- преступление выявлено органом дознания в результате проведенной оперативно- розыскной деятельности.

Анализ исходной информации, независимо от ситуации, осуществляется на основе обобщения имеющихся в материале сведений о криминалистических признаках, указывающих на совершение компьютерного преступления. Это могут быть следующие признаки:

- сбои в работе ЭВМ, системе ЭВМ или локальной вычислительной сети собственника или правообладателя;
- уничтожение, блокирование, модификация или копирование компьютерной конфиденциальной информации;
- утрата значительных массивов информации или баз данных; необычные проявления в работе ЭВМ:
- замедленная или необычная загрузка операционной системы, замедление работы машины с внешними устройствами, неадекватные реакции ЭВМ на команды пользователя и пр.;
- копии чужих файлов в файловой системе правообладателя;
- файлы с вредоносными программами; наличие программного обеспечения подбора паролей для неправомерного доступа в Интернет либо

иного проникновения в компьютерные сети, а также содержащего функции по уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

- внесение в конструкцию компьютера встроенных устройств, дополнительных жестких дисков, устройств для расширения оперативной памяти, считывания оптических дисков и т. д.; наличие нестандартных периферийных устройств;
- изменения в оперативном запоминающем устройстве, зафиксированные при задержании подозреваемого с поличным в момент работы на компьютере при совершении неправомерного доступа к компьютерной информации; улики поведения подозреваемого;
- другие признаки.[1]

Анализируя указанные признаки, следователь выдвигает общие и частные типовые версии.

Основными из них являются следующие:

✓ имело место компьютерное преступление, правообладатель правильно отразил в заявлении его обстоятельства; совершено иное преступление, сбой компьютерного оборудования применен для запутывания следов преступления;

✓ имеет место оговор или ложное заявление о преступлении с целью отвести подозрение от себя или избавиться от нежелательного лица;

✓ имеет место заблуждение или ошибка заявителя.

Одновременно выдвигаются типовые частные версии по каждому из обстоятельств, подлежащих доказыванию, в зависимости от того, какие из них не установлены к данному моменту. После этого в результате сопоставления обстоятельств, подлежащих установлению и уже установленных, формулируются задачи расследования и определяются средства их решения, т. е. те следственные действия и иные мероприятия, в

[1]Федоров В. Компьютерные преступления: выявление, расследование и профилактика. // Законность. 2011, № 6. - С.45.

результате проведения которых предполагается установить не известные еще обстоятельства совершения преступления.

Таким образом, формируется план расследования по делу в целом, отдельным эпизодам и обстоятельствам. По мере его выполнения и получения новой информации вносятся коррективы в имеющийся план, и вновь проводится анализ и формулирование дальнейших задач расследования. Наиболее важными следственными действиями на начальном этапе расследования компьютерных преступлений являются осмотр места происшествия, компьютерного оборудования и информации, обыск и выемка с целью обнаружения, фиксации и изъятия компьютерной информации и компьютерных средств, относящихся к расследуемому событию. Это ключевой момент расследования, поскольку компьютерная информация является предметом посягательства, неправомерный доступ к ней должен быть своевременно процессуально зафиксирован. Тем более что компьютерная информация может быть легко изменена или уничтожена, что повлечет утрату следов преступления.

Если у следствия есть основания полагать, что цифровая информация может являться доказательством по уголовному делу, то она должна изыматься только процессуальными способами, предусмотренными законом: в процессе производства осмотра, обыска, выемки. Выбор конкретного следственного действия зависит от решения следователя, которое, как правило, обусловлено конкретной ситуацией расследования на момент необходимости изъятия цифровой информации.

В бесконфликтной ситуации с собственником или владельцем цифровой информации, когда гражданин или организация потерпели от правонарушения и готовы оказать помощь в установлении истины, целесообразно проводить выемку или осмотр. Такая ситуация чаще всего складывается с организациями, подвергшимися неправомерному доступу к

компьютерной информации[1].

В конфликтной ситуации, особенно при расследовании преступлений в сфере экономики, целесообразно проводить обыск, поскольку гражданин и организация могут оказывать явное или скрытое противодействие, вплоть до преграждения доступа и уничтожения информации и ее носителей. Возможно привлечение специалиста для обыска. В том, числе эксперта отдела компьютерно- технической экспертизы.

Задачи подготовительной стадии:

- получить наиболее полное представление о характере деятельности объекта, где могут находиться следы преступления и другие объекты, относящиеся к расследуемому делу, изучить обстановку в организации: отрасль хозяйствования, порядок учета, документооборот, структуру, особенности используемых технологий;
- изучить коммуникативные, а также другие тактико- технические характеристики применяемой компьютерной техники и ПО;
- рассмотреть организацию охраны объекта конкретной компьютерной информации;
- изучить служебные обязанности лиц, которые имеют доступ к охраняемой компьютерной информации, в том числе их косвенное или прямое отношение к имуществу, которое стало предметом правонарушения.

Для полного и объективного исследования всех обстоятельств преступления необходимо получить ответы на множество вопросов, которые касаются обстановки в организации:

1. Количество компьютеров в организации, где они располагаются (в каких отделах, филиалах, подразделениях, службах и пр.)?
2. Есть ли локальная сеть (их количество)? Размерность сети (количество ПЭВМ, объединенных сетью, где они расположены)?

---

[1]Гудзь Е.Г. Актуальность проблемы ведения борьбы с преступлениями в сфере высоких технологий // Сб. докладов науч.-практ. семинара «Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств», М., 2012. С.62.

3. Есть ли у организации представительства и филиалы, каковы их адреса, подсоединены ли к локальной сети их компьютеры? Их сети связаны с сетью головной организации?

4. Имеются ли компьютеры в организации, которые имеют выход в интернет? Где они располагаются? Через какой провайдер осуществляется выход в интернет?

5. Какие средства телекоммуникаций и связи используются для работы вычислительной техники и для информационного обмена (какой тип, конфиденциальные или общедоступные, абонентские номера, ключи (коды) доступа)?

6. Какова система охраны? Какая организация предоставляет охранные услуги?

7. Категория обрабатываемой информации (есть ли данные, являющиеся государственной тайной, конфиденциальная информация, личные данные)?

8. Используемые источники электропитания (электросеть, бесперебойные, комбинированные, автономные)?

9. Какое ПО и какая операционная система используется в сети?

10. Используемые средства защиты доступа в локальной сети (пароли, шифры, программные средства, коды и пр.)?

11. Какая ведется документация в организации о функционировании локальной сети? Кто является ответственным за ее ведение?

12. Сколько информации о бухгалтерском учете (какие учетно-хозяйственные операции проводятся) фиксируется посредством локальной сети и где хранятся результаты обработки?

13. Иные вопросы.[1]

Для получения ответов на выше поставленные вопросы проводят ряд

[1]Гудзь Е.Г. Актуальность проблемы ведения борьбы с преступлениями в сфере высоких технологий // Сб. докладов науч.-практ. семинара «Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств», М., 2012. С.62.

следственных действий, а также иных мероприятий, к примеру:

- изучение схемы документооборота на предприятии, которая утверждена приказом руководителя в рамках интересующего следствие периода;
- выемка и изучение документации по локальной сети, в которых указывается количество помещений, охваченных локальной сетью; количество подключенных к сети ПЭВМ в этих помещениях; схемы всех мест подключения в помещениях; место расположения сервера; тип машины, планируемой для использования в качестве сервера, ее технические характеристики;
- анализ и сопоставление показаний свидетелей, подозреваемых, обвиняемых, потерпевших;
- выемка и изучение актов проверок независимых органов контроля: финансовых, экологических, налоговых, аудиторских, санитарных, аварийных, а также пожарных проверок и иных документов.

Свидетельскую базу необходимо расширить. Она должна быть представлена следующими свидетельскими группами:

- заказчики локальной сети;
- менеджер сети;
- проектировщики;
- операторы и лица, которые работают непосредственно с рабочими станциями и сервером, и др.

В этот период необходимо тактически правильно определить как места проведения следствия, так и время возможного доступа к компьютерной информации, оказания противодействия группе следствия со стороны нарушителей правопорядка, полноты загрузки мощностей функционирующего компьютерного оборудования или его отключения и т.п.

Обязательно нужно составить план будущего следственного действия, где учитываются и обоснованно используются собранные данные об обстановке в сомнительной организации. Именно на основании «

разведывательных данных» следователь устанавливает место, время проведения следствия, его участников, техническое обеспечение и т.д..[1]

Важно наличие технического плана локальной вычислительной сети. Состав оперативно- следственной группы планируется в зависимости от обстановки на предприятии.

В процессе следственного действия имеют право присутствовать:

- собственник жилого помещения и проживающее в нем лицо (если следствие проводится в жилище);
- уполномоченные представители предприятия, в котором проводится следствие: администрация;
- службы безопасности;
- персонал, который обслуживает носители цифровой информации;
- специалисты (операторы ЭВМ, контролеры, технологи, бухгалтеры и другие);
- иные лица.

Техническая подготовка подразумевает обеспечение транспортом, научно- техническими средствами широкого назначения, упаковочными материалами, достаточным количеством носителей для копирования информации[2].

Целесообразно иметь при себе:

- портативный компьютер (ноутбук) и соединительные кабели с различными разъемами и/ или с комбинированным разъемом;
- ПО для копирования информации в месте проведения следствия;
- сервисные программы для установления технических характеристик изучаемых компьютеров, исправности внешней памяти и некоторых устройств, в том числе антивирусные программы;

---

[1]Чернышева В.О. Интернет и преступность // Реагирование на преступность: концепции, закон, практика. М., 2012. С. 144-148.

[2]Гудзь Е.Г. Актуальность проблемы ведения борьбы с преступлениями в сфере высоких технологий // Сб. докладов науч.-практ. семинара «Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств», М., 2012. С.62.

- комплект чистых дисков (CD- RW или CD-R) для копирования небольшого объема информации (при необходимости).

Для того, что бы избежать ошибок во время проведения следственных действий в период начального этапа расследования, которые могут привести к потере либо искажению компьютерных сведений, нужно придерживаться определенных предохранительных мер.

Рекомендация 1.

Прежде всего, стоит сделать резервные копии информации.

Во время обысков и выемки, которые связаны с изъятием компьютеров, магнитных носителей и сведений, появляются общие проблемы, которые связаны со спецификой изымаемого технического средства. Прежде всего, нужно предусмотреть меры безопасности, совершаемые преступником для уничтожения компьютерных сведений. Он, допустим, может применять специальное оборудование, в критическом случае которое образует большое магнитное поле, стирающее магнитную запись.

Во время обыска электронное доказательство, которое находится в компьютерах или в компьютерных системах нужно собирать так, чтобы его потом признал суд. Из мировой практики можно увидеть, что чаще всего под давлением представителя защиты в судебном заседании электронное доказательство не принимают во внимание. Чтобы гарантировать его признание в виде доказательства, нужно строго придерживаться уголовного процессуального законодательства, а помимо этого стандартных приемов и методов его изъятия.

Рекомендация 2.

Найти и сделать копию временного файла.

Множество текстовых редакторов и программ управления базой данных создают временный файл в качестве побочного продукта нормальной деятельности ПО. Многие пользователи компьютеров не осознают значимости создания данного файла, так как чаще всего он уничтожается программами в конце сеансов работы. Но, при этом данные, которые

находятся внутри данного уничтоженного файла, оказываются самыми полезными. И прежде всего, когда исходные файлы кодированы либо документы подготовки текста напечатали, но никогда не сохраняли на дисках, данный файл можно восстановить.

Рекомендация 3.

Нужно непременно проверять SwapFile.

Популярность Microsoft Windows приносит ряд дополнительных средств, которые касаются анализа компьютерных сведений. SwapFileработает в качестве дисковой памяти, огромной базы данных и множества различных временных фрагментов информации. В этом SwapFile можно обнаружить даже полный текст документов.

Рекомендация 4.

Нужно сравнить дубли текстового документа.

Часто дублей текстового файла, возможно, найти на жестких или гибких магнитных дисках. Это может быть незначительное изменение между версиями одного документа обладающие доказательным значением. Расхождение возможно идентифицировать при помощи самых новых текстовых редакторов.

Когда есть доступ к компьютерам и исключаются нежелательные ситуации, можно приступить к осмотру. При этом следователи и специалисты должны точно объяснить свои действия понятым.

Во время осмотра нужно установить:

- конфигурацию компьютеров с точным и подробным описанием различных устройств;
- номер модели и серийный номер устройств;
- инвентарный номер, присвоенный в бухгалтерии во время постановки оборудования на баланс предприятия;
- иные сведения фабричного ярлыка. Данные сведения вносят в протоколы осмотра вычислительной техники, и они могут быть важными для следствия.

Рекомендация 5.

Фотографирование, а помимо этого маркировка элементов компьютерных систем.

Фотографирование, а помимо этого маркировка элементов компьютерных систем является важным первым шагом подготовки системы к транспортировке. Документирование состояния систем на этом этапе нужно для точной сборки и подключения различных элементов систем при условиях лабораторий. Во время фотографирования нужно выполнять снимок систем крупным планом передней части и задней части. Фотографирование, а помимо этого маркирование элементов изымаемых компьютерных систем дает возможности точно воссоздавать состояние компьютерной техники в лабораторных условиях анализа. Некоторое оборудование такое как внешний модем может содержать много маленьких переключателей, которые фиксируют состояние при транспортировке которые могут изменяться, что создает дополнительную проблему для экспертов.

Таким образом, необходимый набор сервисных программ следователь или специалист формирует по своему усмотрению в зависимости от категории расследуемых дел, используемого ПО и оборудования в данном регионе в данный момент времени.

§2. Особенности взаимодействия следователя с органами дознания и специалистами.

Новым следственным действием для российского уголовно-процессуального закона является допрос специалиста, который позволяет не процессуальную форму участия специалиста в расследовании (например, консультации) перевести в процессуальную, закрепив ее в материалах дела посредством показаний.

Заключения экспертов по изучаемому типу дел – это одно из важных

источников доказательства[1].

Расследование инцидентов (включая расследование преступлений в информационной сфере) - хорошо известный раздел информационной безопасности. Как правило, цели таких расследований одинаковы вне зависимости от типа киберпреступления:

- доказательство, что преступление/ инцидент произошли;
- восстановление событий, окружающих инцидент;
- идентификация правонарушителей;
- доказательство причастности и ответственности правонарушителей;
- доказательство нечестных намерений со стороны правонарушителей.

Расследование, как правило, проводится с огромным количеством данных, которое сейчас исчисляется десятками терабайтов, для их исследования назначается и проводится сравнительно новая копьютерно-технической экспертиза.

Целями компьютерно - технических экспертиз является:

- восстановление сведений, которые, возможно, удалили;
- восстановление события, которое произошло внутри либо вне цифровой системы, связанной с происшествием;
- идентификация пользователя цифровой системы;
- обнаружение вируса и иного вредоносного ПО;
- обнаружение незаконного материала и программы;
- взлом пароля, ключа шифрования и кода доступа.

Существует несколько моделей, описывающих процесс анализа цифровых данных для судебных целей. Было предложено порядка 12 разных моделей, но в настоящее время одной из наиболее общепринятых является

[1]Приказ МВД РФ от 10.02.2006 № 70 «Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации» // Первоначальный текст документа опубликован не был.

так называемая улучшенная модель цифрового процесса, предложенная Брайаном Керером и Юджином Паффаром в 2003 г.

Компьютер, цифровые устройства, мобильные телефоны, iPad, iPod и так далее рассматриваются как отдельное место преступления. После того, как вы извлекли и сохранили данные, хранящиеся на этих устройствах, вы точно так же проводите изначальный анализ того, что же находится на жестком диске или в мобильном телефоне, документируете и после этого определяете зоны дальнейшего осмотра, которые уже углубленно изучаются.

Но, при этом есть ряд проблем. На данный момент объем жесткого диска постоянно увеличивают, помимо этого, одни и те же операционные системы Windows XP существуют как минимум семь лет, это дает возможность эксперту вырабатывать стандартную методику анализа системы, которая может быть изучена на протяжении короткого времени. На данный момент есть восемь различных операционных систем для мобильного устройства, которые активно противодействуют тому, чтобы из него извлекли сведения, и самое сложное, что версию данной операционной системы все время обновляют, что делает проблематичным разработку стандартного метода изучения данной системы.

Облачный сервис, заменяющий автономное цифровое устройство, должен обеспечивать необходимый уровень криминалистической подготовки. Но при этом это нуждается в преодолении проблем, которые связаны с объединением ресурсов, мультиарендой и эластичностью инфраструктуры облачного исчисления. Нужен высокий уровень взаимодействия с органом внутренних дел и корпорацией являющейся провайдером облачного сервиса.

Еще одна проблема состоит в том, что если информация находится на компьютерах, то хакеры либо вредоносное ПО, попадающее в системы, может ее увести и передавать тем, кто будет ее применять в нечестных целях. На основании этого число сведений, которые хранятся именно на компьютерах, тоже начинают снижать. Помимо этого, преступники начинают намного аккуратнее, при этом стараясь оставлять как можно меньше следов

в персональных компьютерах и мобильном телефоне.

Помимо этого, из систем с полной шифровкой жестких дисков, если ее выключили, но при этом нет паролей, тяжело извлекать сведения, на основании этого расследование данное системы возможно, если данные системы находятся на месте преступлений в включенном виде. Проблемы еще и в том, что почти все сотрудники оперативной группы не имеют специального образования и они нуждаются в помощи специалиста, а их число ограничено, что нуждается в широкого обучения оперативника именно на уровне извлечения сведений из живого компьютера[1].

Таким образом, в ходе допроса специалиста могут выясняться и закрепляться не только обстоятельства, требующие оценки лицом, обладающим специальными знаниями, но и разъяснение специалистом сущности своего заключения, данного в письменном виде.

[1]Маляров А.И Объект преступления в сфере электронно-цифровой (компьютерной) информации и вопросы квалификации (российский и зарубежный опыт) / А.И. Маляров // Общество и право. — 2008.— N 2. – С. 22-25.

ЗАКЛЮЧЕНИЕ

Итак, в результате проведенного научного исследования мы можем сформулировать следующие основные выводы:

1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. В действующем Уголовном кодексе РФ закреплено четыре состава преступлений в сфере компьютерной информации: статья 272. Неправомерный доступ к компьютерной информации; статья 273. Создание, использование и распространение вредоносных компьютерных программ; статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно телекоммуникационных сетей; статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Наибольшее распространение на практике получила статья 272, где элементы состава следующие: 1) объект: основной - общественный отношения, связанные с обеспечением общественной безопасности, в части касающейся безопасного использования компьютерной информации, дополнительный - общественные отношения, связанные с обеспечением безопасности конкретного вида информации, например, государственная тайна, коммерческая тайна, банковская тайна, тайна усыновления и т.п., а также экономические отношения, непосредственный - общественные отношения, обеспечивающие информационную безопасность конкретного субъекта; 2) объективная сторона: действие, заключающееся в неправомерном доступе к охраняемой законом информации, хранящейся в электронно- вычислительных машинах. Способ совершения такого действия может быть любой, например, взлом компьютерных систем, компьютерных программ, установка в компьютерных системах специализированных программ, которые обеспечивают возможность такого неправомерного доступа, неправомерный

сбор компьютерной информации, неправомерное копирование или записывание компьютерной информации с одного материального носителя на другой и т.п. Бездействие в данном случае не может характеризовать объективную сторону, так как доступ путем бездействия в принципе не возможен; 3) субъект преступления: общий - физическое вменяемое лицо, достигшее возраста 16- ти лет; 4) субъективная сторона: вина в форме умысла (как прямого, так и косвенного). Преступление имеет материальный состав, так как считается оконченным с момента наступления одного из следующих последствий: - уничтожение информации - прекращение существования информации, при котором ее восстановление невозможно ни при каких условиях и обстоятельствах; - блокирование информации - невозможность (отсутствие возможности) доступа к информации, иными словами, отсутствие возможности сбора, обработки, пользования, хранения и совершения иных действий в отношении информации; - модификация информации - любое изменение информации, например, искажение исходных данных, добавление нового содержания информации, частичное уничтожение первоначальной (исходной информации); - копирование информации - создание аналога информации на материальных носителях путем перенесения данных от исходной информации, но с сохранением ее первоначального содержания.

3. Вредоносная программа - любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, владельцу ЭВМ, сети ЭВМ, путём копирования, искажения, удаления или подмены информации. Многие антивирусы считают крэки (кряки), кейгены и прочие программы для взлома приложений вредоносными программами, или потенциально опасными. Один из наиболее известных компьютерных вирусов (вирус-вымогатель) «wannacry» в 2017 году вывел из строя более миллиона компьютеров в России, Украине Индии и других государствах, через сеть Интерет.

4. Способы совершения преступлений в сфере компьютерной информации связаны с использованием компьютерных программ. Чаще всего эти программ возможно скачать на сайтах в Интернете и далее с их помощью получить неправомерный доступ к чужим почтовым ящикам, аккаунтам в социальных сетях, фотографиям и видеозаписям. Тоже касается вредоносных программ. Большинство преступников не являются авторами этих программ., они их просто используют.

Обстановка совершения данных преступлений характеризуется массовостью аудитории потенциальных жертв, территориальной удаленности жертвы и преступника, круглосуточности преступного воздействия, отсутствия непосредственного контакта между потенциальной жертвой и преступником, больших возможностях по анонимизации преступных действий, а также обеспечении временного разрыва между началом активных действий и наступлением последствий.

Преступления совершаются преимущественно с корыстным мотивом, также незначительная часть из хулиганских побуждений.

Личность преступника характеризуется следующим образом – 95% случаев это мужчина в возрасте 18-30 лет, ранее не судимый, имеющий навыки в сфере компьютерных технологий, образованный, и т.п. То есть внешне вполне благополучный и вызывающий никаких подозрений у окружающих. Не имеет отношения к общеуголовной преступности.

5. Уголовное дело чаще всего возбуждается по заявлению потерпевшего. Типичные следственные ситуации: 1. Подозреваемый не известен; 2. Подозреваемый или место его нахождения установлено, требуется задержание; 3. Подозреваемый задержан.

На первоначальном этапе расследования, характерны следующие следственные действия: осмотр места происшествия и компьютерной техники потерпевшего, допрос потерпевшего, назначение компьютерной экспертизы, поручение органам дознания (подразделению «К» при Бюро специальных технических мероприятий) на установление личности и задержание

подозреваемого, допросы свидетелей, запросы в компании Интернет-провайдеры.

6. К особенностям следует отнести привлечение специалиста в сфере компьютерной информации к проведению следственных действий. Это допросы, обыски, выемки и назначение компьютерной экспертизы. Так же допрос самого специалиста.

7. Взаимодействие следователя ОВД при расследовании рассматриваемых преступлений происходит с сотрудниками подразделения «К» БСТМ, осуществляющими оперативное сопровождение расследования, экпертами-криминалистами подразделений компьютерных экспертиз, иными специалистами в данной сфере. Оно осуществляется в форме совместного проведения следственных действий, направления запросов, отдельных поручений о производстве оперативно-розыскных мероприятий и следственных действий.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Законы, нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года) // Консультант плюс электронный ресурс
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 01.07.2021) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (в редакции от 1.07.2021) // Собрание законодательства РФ. – 24.12.2001. – № 52. – ст. 4921.
4. Об информации, информационных технологиях и о защите информации от 27.07.2006 № 126 – ФЗ (последняя редакция) // Российская газета. – 29.07.2006. – № 165.
5. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (последняя редакция) // Собрание законодательства РФ. – 25.12.2006. – №52. – (часть 1) Ст.5496.
6. Приказ Генпрокуратуры России N 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 (ред. от 20.02.2014) «О едином учете преступлений (вместе с «Типовым положением о едином порядке организации приема, регистрации и проверки сообщений о преступлениях», «Положением о едином порядке регистрации уголовных дел и учета преступлений», «Инструкцией о порядке заполнения и представления учетных документов») (Зарегистрировано в Минюсте России 30.12.2005 № 733) // Российская газета. – 2006. – № 13.
7. Приказ МВД России от 01.06.1993 г №261 «О повышении эффективности экспертно-криминалистического обеспечения деятельности органов

внутренних дел» // Первоначальный текст документа опубликован не был.

8. Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях (зарегистрировано в Минюсте России 6 ноября 2014 г. № 34570): Приказ Министерства внутренних дел Российской Федерации от 29 августа 2014г. № 736 // Российская газета. – 2014. - № 6532
9. Приказ МВД РФ от 10.02.2206 № 70 «Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации» // Первоначальный текст документа опубликован не был.
10. Методические рекомендации об организации выполнения и защиты выпускных квалификационных (дипломных) работ для слушателей очной формы обучения по специальности 40.05.02 – Правоохранительная деятельность, специализация – уголовно-правовая; узкая специализация – уголовный розыск органов внутренних дел; квалификация – юрист.

Монографии, учебники, учебные пособия

11. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации: учебное пособие // Б.В. Андреев. П.Н. Пак, В.П. Хорс. – М.: Юрлитинформ, 2012. – 152 с.
12. Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев – Казань: Изд-во «Познане» Казанского инновационного университета, 2020 – 300 с. (Серия «Цифровая безопасность »).
13. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий : учебное пособие : в 2 ч. / [А. В. Аносов и др.]. – М. : Академия управления МВД России, 2019. – Ч. 1. – 208 с.

14. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебное пособие для вузов / С. В. Зуев [и др.] ; ответственные редакторы С. В. Зуев, В. Б. Вехов. — Москва : Издательство Юрайт, 2021. — 243 с.

Научные статьи, диссертации, авторефераты

15. Атаманов Р.С. Криминалистическая характеристика мошенничества в онлайн-играх // Р.С. Атаманов. – Российский следователь, 2011. – № 21. – 268 с.
16. Волженкин Б.В. Прозрачность правосудия и информационная безопасность. // Б.В. Волженкин. – Режим доступа: law.edu.ru/doc/document.asp (дата обращения: 15.03.2017).
17. Головин А. Ю. Криминалистическая характеристика лиц, совершающих преступления в сфере компьютерной информации//http://www.crime-research.org (дата обращения: 15.03.2017).
18. Голубев В.А. Вопросы международного сотрудничества в борьбе с транснациональной компьютерной преступностью // В.А. Голубев. – Режим доступа: http://www.crime-research.ru/articles/2011/ (дата обращения: 15.03.2017).
19. Гудзь Е.Г. Актуальность проблемы ведения борьбы с преступлениями в сфере высоких технологий // Е.Г. Гудзь. – Сб. докладов науч.-практ. семинара «Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств». – М., 2012. – 62 с.
20. Дворецкий М.Ю. Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ: учебное пособие // М.Ю. Дворецкий, А.Н. Копырюлин. – Уголовное право, 2012. — №4. – 34 с.
21. Завидов Б. Д., Ибрагимова З. А. Мошенничество в сфере высоких технологий: учебное пособие // Б.Д. Завидов, З.А. Ибрагимова. –

Современное право, 2011. – № 4. – 44 с.

22. Карчевский Н. В. Компьютерные преступления: определение, объект и предмет // Н.В. Карчевский. – Режим доступа: http://www.ifap.ru/pi/05/karchev.htm (дата обращения: 15.03.2017).
23. Компьютерная преступность и кибертерроризм: сборник научных статей // В.А. Голубева, Э.В. Рыжкова. – Запорожье: Центр исследования компьютерной преступности, 2012. – Вып. 3. – 448 с.
24. Крылов В. В. Расследование преступлений в сфере информации: учебное пособие // В.В. Крылов. – М., 2014. – 164 с.
25. Крылов В. В. Расследование преступлений в сфере компьютерной информации: учебное пособие // В.В.Крылов. – М., 2012. – 615 с.
26. Маляров А.И. Объект преступления в сфере электронно-цифровой (компьютерной) информации и вопросы квалификации (российский и зарубежный опыт) // А.И. Маляров. – Общество и право, 2008. — № 2. – 25 с.
27. Никифоров И., Уголовные меры борьбы с компьютерной преступностью: учебное пособие // И. Никифоров. – Защита информации, 2010. – № 5.
28. Номоконов В.А. Глобализация информационных процессов и преступность // В.А. Номоконов, - Режим доступа: http:// www.vkeys.kiev.ua/box/4/93.shtml (дата обращения: 15.03.2017).
29. Номоконов В.А. Новые информационные технологии в борьбе с преступностью/В.А. Номоконов. – Российский криминологический взгляд, 2012. – № 1. – 94 с.
30. Селиванов Н. А. Проблемы борьбы с компьютерной преступностью: учебное пособие / Н.А. Селиванов. – Законность, 2013. – № 8. 37 с.
31. Федоров В.Н. Компьютерные преступления: выявление, расследование и профилактика: учебное пособие / В. Федоров. – Законность, 2011, № 6. – 43 с.
32. Черкасов В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий: учебное пособие / В.Н. Черкасов.

– Саратов, 2015. – 81 с.

33. Чернышева В.О. Интернет и преступность / В.О. Чернышева. – Реагирование на преступность.– Концепции, закон, практика. – М., 2012. – 184 с.
34. Атаманов Р.С. Некоторые вопросы расследования мошенничества в сети Интернет // Р.С. Атаманов. – Актуальные проблемы российского права, 2010. – № 4 (17). – 496 с.
35. Бурлаков В.Н., Горшенков, Г.Н, Максина С.В., Шестаков Д.А. Средства массовой информации и преступность (криминология СМИ) // В.Н. Бурлаков, Г.Н. Горшенков, С.В. Максина. – Правоведение, 2012. – № 5. – 584 с.
36. Вестник ВИПК МВД России. 2012. № 3 (23). – 69 с.
37. Веб-технологии на службе правоохранительных органов. Режим доступа: http://www.crime-research.ru/news/16.03.2010/1870/(дата обращения: 15.01.2017).
38. Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации: учебное пособие // В.Б. Вехов, В.В Попова, Д.А.Илюшин., 2014. – 289 с.
39. Воробьев В. В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Дис. … канд. юрид. наук. – Н. Новгород, 2010. – 200 с.

Эмпирические материалы

(материалы судебной, следственной практики и т.д.)

40. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 27 декабря 2012 г. № 51 // Российская газета. – 2008. – № 4.
41. Кассационное определение Верховного Суда Республики Татарстан по

делу № 22-6848 от 02 ноября 2010 года // Архив Верховного Суда Республики Татарстан

42. Приговор мирового судьи судебного участка N 48 Самарской области от 06.06.2011г. в отношении Мордвинцева. // РосПравосудие: [сайт]. URL: https://rospravosudie.com/court-sudebnyj-uchastok-48-samarskoj-oblasti-s/act-200780468/ (дата обращения: 15.03.2017).
43. Постановление и.о. Мирового судьи судебного участка N 49 г. Находка от 16.01.2014г. // РосПравосудие: [сайт]. URL: https://rospravosudie.com/court-sudebnyj-uchastok-49-g-naxodka-s/act-213736047/ (дата обращения: 15.03.2017).
44. Приговор Захаровского районного суда Рязанской области от 10.06.2011г. в отношении Захарова П.В. // РосПравосудие: [сайт]. URL: https://rospravosudie.com/court-zaxarovskij-rajonnyj-sud-ryazanskaya-oblast-s/act-100404151/ (дата обращения: 15.03.2017).
45. Приговор Советского районного суда г. Томска от 10.03.2011г. в отношении Регнера И.В. // РосПравосудие: [сайт]. URL: https://rospravosudie.com/court-sovetskij-rajonnyj-sud-g-tomska-tomskaya-oblast-s/act-100402140/ (дата обращения: 15.03.2017).
46. Приговор Октябрьского районного суда г. Кирова от 11.12.2013г. в отношении Пленкина А.А. // РосПравосудие: [сайт]. URL: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-447482174/ (дата обращения: 05.03.2016).
47. Приговор Октябрьского районного суда г. Кирова от 24.12.2013 г. в отношении Сикова Д.В. // РосПравосудие [сайт]. URL: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-445968591/ (дата обращения: 15.03.2017)
48. Приговор Авиастроительного районного суда г. Казани от 17 апреля 2012 года // Архив Авиастроительного районного суда г. Казани
49. Приговор Егорьевского городского суда Московской области от 26.10.2011 года в отношении Миленина А.С. // РосПравосудие [сайт].

URL: https://rospravosudie.com/court-egorevski-gorodskoj-sud-moskovskaya-oblast-s/act-105695669/ (дата обращения: 15.03.2017)

50. Электронные ресурсы

51. Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс]. - URL: http://www.mvd.ru/presscenter/statistics/reports дата обращения 15.03.2017 г.
52. Официальный сайт Судебного департамента при ВС РФ режим доступа свободный http://www.cdep.ru/index.php?id=79&item=5669 (дата обращения 2.08.2021)

ПРИЛОЖЕНИЯ

Таблица №1

Количество лиц, осужденных за преступления ст.272-274.1 УК РФ в РФ

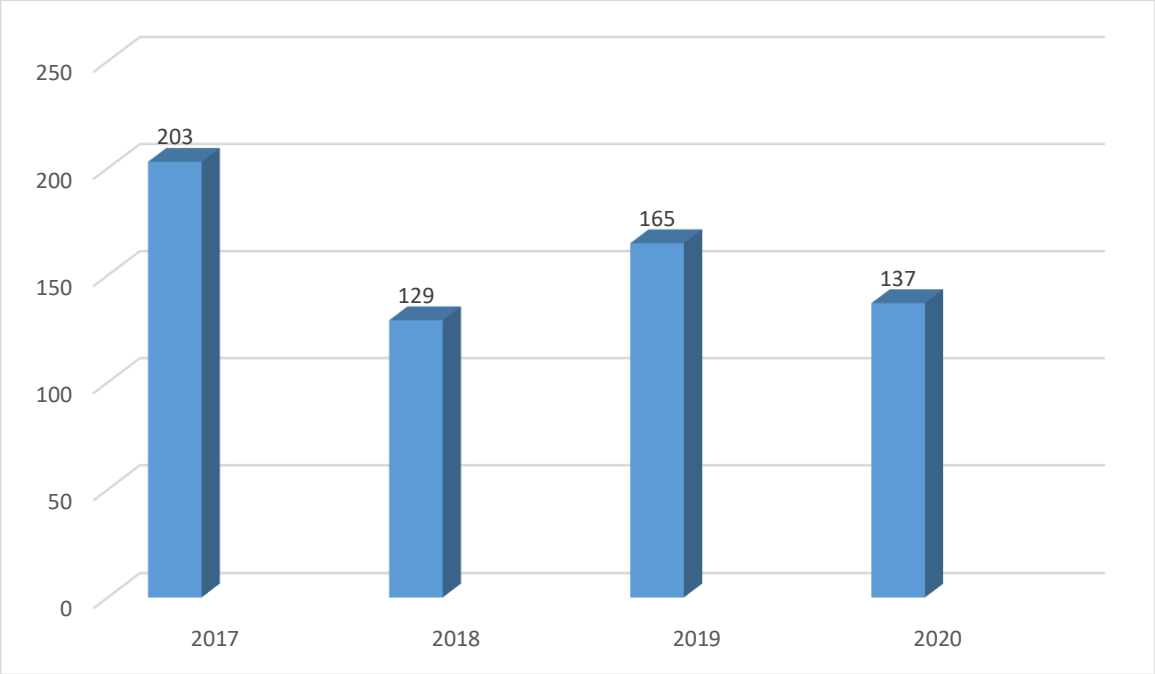

Таблица №2 Количество зарегистрированных преступлений в сфере компьютерной информации в РФ