Министерство внутренних дел Российской Федерации

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

Кафедра экономики, финансового права и информационных технологий в деятельности ОВД

# ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

**на тему:** преступления в сфере использования компьютерной информации: основные проблемы правоприменительной практики

Выполнил: Романова Екатерина Владимировна, правоохранительная деятельность, 2013 год набора, 032 учебная группа

Руководитель: преподаватель, Каримов Адель Миннурович

Рецензент: Начальник ОП 10 УМВД России по г.Казани, подполковник полиции Охотников Павел Николаевич

К защите Допущена 18.06.18г.
(допущена, дата)

Начальник кафедры: Шевко Наиля Рашидовна

Дата защиты: "___" июля 2018 г. Оценка _____

Казань 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ ..... 3
1 УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СФЕРЕ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ..... 8
1.1 Становление и развитие российского уголовного законодательства в сфере использования компьютерной информации ..... 8
1.2 Компьютерная информация как предмет преступления, объективные и субъективные признаки ..... 17
1.3 Классификация киберпреступлений ..... 30
2 ОСОБЕННОСТИ ВЫЯВЛЕНИЯ, РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РФ: ПРОБЛЕМЫ НОРМОТВОРЧЕСТВА И ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ ..... 43
2.1 Специфика подготовки и проведения осмотра места происшествия и обыска ..... 43
2.2 Взаимодействие служб и подразделений ОВД при выявлении, раскрытии и расследовании преступлений в сфере использования компьютерной информации ..... 45
2.3 Использование специальных познаний при расследовании преступлений в сфере использования компьютерной информации ..... 48
3 ТЕНДЕНЦИИ РАЗВИТИЯ МЕТОДОВ И СПОСОБОВ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ..... 53
3.1 Мировой опыт борьбы с кибепреступностью ..... 53
3.2 Проблемы правоприменительной практики расследования преступлений в сфере использования компьютерной информации и способы их решения на примере ..... 58
ЗАКЛЮЧЕНИЕ ..... 64
СПИСОК ЛИТЕРАТУРЫ ..... 67
ПРИЛОЖЕНИЯ ..... 81

# ВВЕДЕНИЕ

Актуальность темы исследования. История развития человеческой цивилизации всегда была связана с накоплением и последующим использованием общественно-полезной информации. По мере появления новых технологий все острее встает вопрос защиты интересов граждан и государства в сфере компьютерной информации и высоких технологий, особенно на фоне постоянного увеличения преступлений в сфере использования компьютерной информации. Так, в 2013 году было совершено 693 мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ), в 2016 году их количество увеличилось до 4 329. Также немало совершено преступлений, предусмотренных ст. 272 (Неправомерный доступ к компьютерной информации) и 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ) – 1151 и 585 преступлений соответственно[1].

В наши дни жертвами преступлений в сфере использования информационных технологий становятся не только руководители высшего звена и правительственные организации, но и простые граждане.

В настоящее время необходимость дальнейшего совершенствования мер борьбы с компьютерной преступностью признана как на национальном, так и на международном уровне. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 05.12.2016 г. № 646) отмечает возрастание масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в т.ч. в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. В свою очередь, Организация Объединенных Наций предлагает государствам опробовать конкретные

[1] Официальный сайт МВД РФ. URL: //www.мвд.рф (дата обращения: 08.05.2018).

меры, направленные на создание защищенной и устойчивой киберсреды, предупреждать и пресекать преступную деятельность, осуществляемую с помощью Интернета.

Количество преступлений, совершаемых в сфере компьютерной информации и высоких технологий увеличивается соразмерно росту пользователей компьютерных сетей. Об этом, в частности, свидетельствуют отдельные электронные ресурсы, разработанные правительствами некоторых стран мира для приема заявлений граждан на преступления, совершенные в телекоммуникационной сети «интернет». Так запущенный в мае 2000 года как виртуальный центр для приема жалоб граждан США на «интернет – преступления» сайт «InternetComplain Center» получил своего миллионного заявителя спустя семь лет после создания (июнь 2007 года). В ноябре 2010 года было зарегистрировано два миллиона жалоб на «интернет – преступления». В 2014 году количество заявлений достигло трёх миллионов. Ежегодно, начиная с 2010 года количество заявлений граждан США на совершенные в отношении них в телекоммуникационной сети «интернет» преступления приближается к отметке в 300 тысяч (2010 – 303,809; 2011 – 314,246; 2012 – 289,974; 2013 – 262,813; 2014 – 269,422; 2015 – 288,012). По сообщениям интернет пользователей общие потери от киберпреступности за 2015 год составили 1,070,711,522 долларов США[2].

В России подобные электронные ресурсы пока не введены в действие, а официальная статистика сообщает о не значительном количестве киберпреступлений. К тому же последние традиционно ограничиваются составами, перечисленными в 28 главе УК РФ. Так по данным отчета о состоянии преступности, ежегодно размещаемого на сайте Министерства внутренних дел, в России за 2016 год было зарегистрировано 1748 преступлений в сфере компьютерной информации, что на 26,6 % меньше чем за аналогичный период в 2015 году. 1503 преступления было выявлено

[2] Официальный сайт ФБР США – Центр интернет-мониторинга жалоб на преступления в электронной сети. URL: //www.ic3.gov (дата обращения: 08.05.2018).

сотрудниками ОВД. Из преступлений, дела и материалы о которых находились в производстве, было раскрыто 903 деяния[3].

Объектом исследования являются общественные отношения, возникающие в процессе использования компьютерной информации, в частности ситуации, когда она становиться предметом преступных посягательств.

Предмет дипломной работы составляют правовые нормы, предусматривающие уголовно-правовую и иную ответственность за совершение преступлений, в сфере использования компьютерной информации.

Цель работы заключается в исследовании особенностей совершения преступлений в сфере использования компьютерной информации, их предупреждения, выявлению, раскрытия и расследования. Для достижения поставленной цели были определены следующие задачи:

1. рассмотреть становления и развитие российского уголовного законодательства в сфере использования компьютерной информации,

2. определить компьютерную информацию как предмет преступления, объективные и субъективные признаки,

3. провести классификацию киберпреступлений,

4. исследовать организацию процесса расследования преступлений в сфере использования компьютерной информации,

5. изучить вопросы взаимодействия служб и подразделений ОВД при выявлении, раскрытии и расследовании преступлений в сфере использования компьютерной информации,

6. выявить особенности использования специальных познаний при расследовании преступлений в сфере использования компьютерной информации,

7. раскрыть мировой опыт борьбы с киберпреступностью,

[3] Официальный сайт МВД РФ. URL: //www.мвд.рф (дата обращения: 08.05.2018).

8. проанализировать проблемы правоприменительной практики расследования преступлений в сфере использования компьютерной информации и способы их решения на примере РТ.

Проблемам компьютерной преступности в настоящее время посвящено значительное количество научных трудов. Большая часть исследований затрагивает вопросы уголовно-правовой характеристики компьютерной преступности. Особое внимание данной проблематике в своих работах уделяют Р. М. Айсанов, Р.С. Атаманов, И. Р. Бегишев, Е. В. Беспалова, Д. С. Будаковский, В. И. Быков, В. Б. Вехов, А. Г. Волеводз, М. Гаврилов, М. Герке, В. В. Голубев, О. В. Григорьев, М. В Демьянец, К.Н. Евдокимов, Н. А. Егиазарян, М. А. Ефремова, А. Иванов, И. А Каримов А.,Клепицкий, А. Н. Копырюлин, В. Н. Кудрявцев, Е. Б. Кургузкина, А. И. Маляров, И. М. Рассолов, Н. Д. Ратникова, М.Е. Репин, О. М. Сафонов, Н. А. Сивицкая, П. Г. Смагин, В. Г. Степанов-Егиянц, А. И. Халиуллин, В. В. Хилюта, З. И. Хисамова, И. Г. Чекунов, В. Н. Черкасов, В. А. Широков, В. Н. Щепетильников, С.А. Янин и др.

Методологическую основу исследования составляют общенаучные методы – диалектический, формальной логики, анализа и синтеза; частнонаучные методы – логико-юридический, сравнительно-правовой, системно-структурный, анализа документов, статистические методы.

Нормативно-правовую базу исследования составляют Конституция Российской Федерации, международно-правовые акты, Уголовный кодекс Российской Федерации (далее – УК РФ), Уголовно-процессуальный кодекс Российской Федерации (далее – УПК РФ), федеральные законы, акты Президента и Правительства Российской Федерации, другие отечественные и зарубежные нормативные правовые акты.

Теоретическая значимость исследования состоит в том, что в нем комплексно освещаются понятие и виды преступлений в сфере обращения компьютерной информации, а также обосновываются предложения по

дополнению, совершенствованию и повышению эффективности уголовного законодательства об ответственности за данные преступления.

Практическая значимость исследования заключается в том, что сформулированные в нем выводы, предложения и рекомендации могут быть применены в законотворческой деятельности по совершенствованию уголовного законодательства и иных нормативно-правовых актов; в правоприменительной деятельности при квалификации преступлений, посягающих на компьютерную информацию; в процессе преподавания уголовного права, правовых основ информационной безопасности и правовой защиты информации в юридических вузах и на курсах повышения квалификации.

Структура работы обусловлена целью и задачами и состоит из введения, трех глав, включающих восемь параграфов, заключения, списка литературы.

# 1 УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СФЕРЕ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

## 1.1 Становление и развитие российского уголовного законодательства в сфере использования компьютерной информации

Развитие информационного общества основывается на расширении применения информационных технологий, облегчающих доступ к любой информации для всех лиц. Вопрос компьютерных преступлений имеет международный масштаб.

Термин «киберпреступление» стал активно употребляться в начале 60х годов 20 века. В настоящее время значение термина возросло, о чем говорит его активное использование в деятельности правоохранительных органов. Новые информационные технологии создали основу для появления новых способов посягательства на общественные отношения, охраняемые законом. Возникла проблема обеспечения надежной защиты информации от неправомерного доступа третьих лиц.

В. Б. Вехов верно отметил, что отсутствие четкого уголовно-правового определения компьютерной информации, единого понимания ее сущности как предмета преступного посягательства значительно затрудняет выработку общей концепции борьбы с компьютерными преступлениями[4].

Такое положение дел привело к тому, что различные ученые трактуют понятие «компьютерная информация» по-разному. Так, например, В. А. Мещеряков под компьютерной информацией понимает информацию, представленную в специальном виде[5].

[4] Вехов В. Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // Уголовное право. 2014. № 4. С. 15.

[5] Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж : Изд-во Воронеж. гос. ун-та, 2002. С. 46. // СПС «КонсультантПлюс», 2018.

Аналогичную точку зрения высказывает и М. В. Старичков[6], который под компьютерной информацией понимает зафиксированные на материальном носителе сведения, представленные в виде, пригодном для обработки с использованием компьютерных устройств, и предназначенные для использования в таких устройствах.

В трудах представителей уголовно-правовой науки содержатся и другие определения понятия «компьютерная информация». Так, Н. А. Зигура утверждает, что компьютерная информация – это сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации[7]. Однако представляется, что включение в определение компьютерной информации термина «создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации» является неоправданным. Это связано с тем, что создание компьютерной информации средствами фиксации и передачи информации невозможно, т. к. они являются только дополнительными элементами любой информационной системы. В связи с этим более уместным было бы говорить об аппаратных средствах создания и обработки информации, т. е. компьютерах, а в общем смысле об информационно-телекоммуникационных устройствах, которые, как правило, и создают компьютерную информацию. Более того, Н. А. Сивицкая[8] и Р. М. Айсанов[9] считают, что уголовно-правовой защите помимо собственно сведений должна подлежать информация в виде баз данных и программ.

---

[6] Старичков М. В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. 2014. № 1. С. 20.

[7] Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис. … канд. юрид. наук. Челябинск, 2010. С. 9. // СПС «КонсультантПлюс», 2018.

[8] Сивицкая Н. А. К вопросу об определении понятия «компьютерная информация» // Проблемы правовой информатизации. 2005. № 2. С. 35. // СПС «КонсультантПлюс», 2018.

[9] Айсанов Р. М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: автореф. дис. … канд. юрид. наук. М., 2006. С. 8. // СПС «КонсультантПлюс», 2018.

В то же время определение понятия «компьютерная информация» должно быть основано, прежде всего, на понятийном и нормативном аппарате российского информационного права[10].

Понятием «компьютерная информация», используемым уголовным законодательством, охватывается и управляющая, и смысловая информация, закрепленная на цифровом носителе и (или) передаваемая по телекоммуникационным сетям[11].

По нашему мнению, оригинальным и, в свою очередь, простым и точным представляется определение компьютерной информации, изложенное В. Б. Веховым, который предлагает под ней понимать сведения, находящиеся в памяти ЭВМ[12].

Кроме того, В. Б. Вехов указывает на основания классификации компьютерной информации как предмета совершения преступления:

– по юридическому положению (документированная и недокументированная);

– по категории доступности (общедоступная либо охраняемая законом – конфиденциальная информация или государственная тайна);

– по форме представления (электромагнитный сигнал, документальное сообщение, файл, программа для ЭВМ, база данных).

Существует ряд иных сходных понятию «компьютерная информация» терминологических оборотов. Так, например, «электронная информация», «цифровая информация, которые, несомненно, представляют определенный научный интерес и научную ценность.

Так, А. В. Геллер, исследуя уголовно-правовые аспекты обеспечения защиты электронной информации, приходит к выводу, что электронная

---

[10] Гребеньков А. А. Общие подходы к определению понятия «компьютерная информация» в уголовно-правовой теории // Известия Юго-Западного государственного университета. Серия: История и право. 2013. № 1-2. С. 138.

[11] Кургузкина Е. Б., Ратникова Н. Д. Место совершения компьютерных преступлений // Вестник Воронежского института ФСИН России. 2016. № 1. С. 81.

[12] Вехов В. Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // Уголовное право. 2004. № 4. С. 17. // СПС «КонсультантПлюс», 2018.

информация в рамках состава преступления представляет различные ее элементы (предмет и способ совершения преступления)[13].

По мнению В. Н. Щепетильникова, при формулировании объективной стороны преступлений гл. 28 «Преступления в сфере компьютерной информации» УК РФ целесообразно использовать выражение «электронная информация»[14]. Аналогичного мнения придерживается Е. Г. Титарева[15]. Мы поддерживаем такую точку зрения.

Интересные предложения выдвигает П.Г. Смагин, который, основываясь на определении понятия «компьютерная информация», предложенном О. Г. Григорьевым[16], вводит свою дефиницию «электронная информация». Он пишет, что если информация была создана не на компьютере, а, к примеру, на цифровом фотоаппарате, то она уже не является компьютерной, но все равно она зафиксирована в цифровом виде и при передаче ее на компьютер никакого искажения не произойдет. Он считает, что с появлением огромного количества цифровых устройств (сотовых телефонов, цифровых диктофонов) понятие «компьютер» необходимо исключить из оборота в соответствующих законах, в том числе в УК РФ и иных нормативно-правовых актах, т. к. можно говорить только о цифровом устройстве[17]. Считаем, с этой точкой зрения следует согласиться.

А. А. Нагорный под электронной информацией предлагает понимать сведения (сообщения, данные), представленные в цифровой форме и содержащиеся в информационно-телекоммуникационных устройствах, их системах и сетях. Он считает, что данное определение не лишено

---

[13] Геллер А. В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета: автореф. дис. … канд. юрид. наук. М., 2006. С. 7. // СПС «КонсультантПлюс», 2018.

[14] Щепетильников В. Н. Уголовно-правовая охрана электронной информации: автореф. дис. … канд. юрид. наук. Елец, 2006. С. 7. // СПС «КонсультантПлюс», 2018.

[15] Титарева Е. Г. Мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий // Научный альманах. 2015. № 7. С. 1160.

[16] Григорьев О. В. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: автореф. дис. … канд. юрид. наук. Омск, 2007. С. 8. // СПС «КонсультантПлюс», 2018.

[17] Смагин П. Г. О понятии «компьютерной информации» и особенностях ее использования при расследовании преступлений в ОВД // Вестник Воронежского института МВД России. 2008. № 1. С. 80. // СПС «КонсультантПлюс», 2018.

недостатков, однако оно способно наиболее полно отразить суть рассматриваемого явления[18].

По мнению О. С. Герасимовой, не существует информации вообще, на каких бы носителях она не закреплялась, и с помощью каких бы технических средств она не хранилась и не передавалась. Это чисто теоретическое понятие. Практически существуют сведения конкретного содержания[19].

На наш взгляд, предметом преступления, посягающего на информацию в телекоммуникационных устройствах, их системах и сетях, следует признавать не компьютерную, а цифровую информацию. Под информацией в цифровой форме понимается информация в виде цифровой последовательности сигналов.

Следует отметить, что существует точка зрения, заключающаяся в необходимости использования в ст. 272 УК РФ термина «электронно-цифровая информация», предложенного А. И. Маляровым[20]. Однако данное определение не совсем точно, т. к. цифровая информация является цифровой последовательностью по форме, но по виду изменяется в зависимости от среды распространения, т. е. от линии связи и канала передачи информации. Например, если цифровая информация передается в радиолинии связи, то такая информация носит название электромагнитно-цифровой. Если по волоконно-оптической линии связи, то это оптико-цифровая информация. Очевидно, что электронно-цифровой информацией будет называться информация, передаваемая по проводным или кабельным линиям связи. Предложенный А. И. Маляровым к использованию термин «электронно-цифровая информация» не учитывает волоконно-оптические линии и радиолинии связи, в которых также циркулирует цифровая информация и иные объекты.

---

[18] Нагорный А. А. Содержания понятия компьютерной информации как предмета компьютерных преступлений // Актуальные проблемы российского права. 2014. № 8. С. 1697.

[19] Герасимова О. С. Особенности преступлений в сфере компьютерной информации // Вестник ТГУ. 2007. № 12. С. 329. // СПС «КонсультантПлюс», 2018.

[20] Маляров А. И. Уголовно-правовые и криминологические аспекты международного сотрудничества в сфере защиты электронно-цифровой информации: автореф. дис. … канд. юрид. наук. Краснодар, 2008. С. 9. // СПС «КонсультантПлюс», 2018.

Как отмечает И. А. Юрченко, особенностью информации является то, что ее невозможно представить без какой-либо материальной основы, она является атрибутом (свойством) материи и неотделима от нее. Даже тогда, когда информация отражается сознанием человека, она существует лишь в единстве с определенными нейрофизиологическими процессами, т. е. имеет свой материальный носитель[21].

Мы солидарны с мнением Н. А. Иванова, указывающего на общепризнанность общественностью понятия «цифровая информация». Он отмечает, что информация, вводимая, обрабатываемая и хранящаяся в устройствах памяти средств компьютерной и иной микропроцессорной техники, или передаваемая по каким-либо каналам связи, имеет вид или зафиксирована (представлена) в виде дискретных сигналов, т. е. сигналов, имеющих конечное число значений. В средствах цифровой техники в подавляющем большинстве случаев используются сигналы только двух уровней. Поэтому информацию, представленную двумя уровнями дискретных сигналов, стали называть бинарной (двоичной). Наличие сигнала с определенными характеристиками стали считать за цифру «1», а сигнал другого уровня – за цифру «0». Соответственно информация, хранимая на машинных носителях, обрабатываемая средствами компьютерной или иной микропроцессорной техники и передаваемая по каким либо линиям связи, получила название «цифровая информация». Данное определение стало общепризнанным, и под ней сегодня никто не подразумевает запись, исполненную цифрами арабской, римской или иной системы исчислений[22].

Уголовный кодекс Российской Федерации содержит нормы, предусматривающие ответственность за совершение преступлений в сфере компьютерной информации. Они закреплены в следующих статьях УК РФ:

---

[21] Юрченко И. А. Информация конфиденциального характера как предмет уголовно-правовой охраны: автореф. дис. … канд. юрид. наук. М., 2000. С. 12. // СПС «КонсультантПлюс», 2018.

[22] Иванов Н. А. О понятии «цифровые доказательства» и их месте в общей системе доказательств // Проблемы профилактики и противодействия компьютерным преступлениям: материалы Международной научно-практической конференции (г. Челябинск, 30 мая 2007 г.) и «круглого стола» (г. Челябинск, 18 мая 2007 г.) / отв. ред. А. В. Минбалеев; Челябинский центр по исследованию проблем противодействия организованной преступности и коррупции. Челябинск, 2008. С. 96. // СПС «КонсультантПлюс», 2018.

ст.272 «Неправомерный доступ к компьютерной информации»; ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ»; ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»; ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Федеральным законом от 26 июля 2017 г. N 194-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"[23] вводится уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру РФ.

В частности, предусматривается уголовная ответственность за:

- создание, распространение и/или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации;

- неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру РФ, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре РФ;

- нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в

[23] Федеральный закон от 26.07.2017 N 194-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" // Собрание законодательства РФ. 2017. N 31 (Часть I). Ст. 4743.

критической информационной инфраструктуре РФ, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре РФ, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре РФ.

Нормы, закрепленные в статьях 272-274.1 УК РФ не способны полностью охватить все общественно опасные деяния в области информационных технологий. Компьютер рассматривается как предмет материального мира, что не позволяет отнести преступления относительно компьютера к компьютерным преступлениям. Но данное значение компьютера условно, так как его также можно рассматривать в качестве совокупности информационных и аппаратных структур. Информацию, в свою очередь, нельзя похитить из-за её нематериальности, но ответственность за незаконное завладение информацией все-таки предусмотрена.

Рассматривая компьютерную информацию в качестве объекта посягательства, следует помнить, что последствия общественно опасного деяния могут наступить в любой точке мира[24]. Вследствие этого приобретает особое значение вопрос о пределах действия уголовного закона в пространстве.

Часть 1 ст. 272 УК РФ содержит в себе нормы о неправомерном доступе к компьютерной информации. К способам неправомерного доступа относят: использование чужого имени, изменение физического адреса технического устройства, подбор пароля, нахождение и использование

[24] Голубев В. В. Компьютеризация и уголовное право – С-Пб: Изд-во Юстицинформ, 2014. С. 27.

«пробелов» в программе, любой другой обман системы защиты информации[25].

Спорным является вопрос о последствиях, наступающих по итогам осуществления посягательства в области компьютерной информации. Данное понятие имеет оценочный характер. В действительности, содержание такого посягательства рассматривается отдельно для каждого случая с учетом всех имеющихся обстоятельств дела. К тяжким последствиям стоит относить причинение крупного материального ущерба, нанесение серьезного вреда работе предприятия, причинение здоровью людей тяжкого вреда.

В ст. 273 УК РФ говорится о создании, использовании и распространении вредоносных компьютерных программ через создание специальных программ и изменение существующих на устройстве программ. Вредоносные компьютерные программы опасны тем, что они могут полностью дезорганизовать систему компьютерной безопасности, привести к нарушению работы компьютерных систем в области обороны, космонавтики, государственной безопасности и т.д.

Статьей 274 УК РФ предусмотрено наказание за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Содержание данной статьи УК РФ состоит в несоблюдении лицом правил и режима работы ЭВМ, которые предусмотрены инструкциями.

Ответственность согласно 274 статье УК РФ наступает за уничтожение, блокирование или изменение в результате нарушения правил эксплуатации ЭВМ информации, охраняемой законом. Ответственность наступает только при условии причинения существенного вреда информации.

Настоящее уголовное законодательство Российской Федерации достаточно четко закрепляет ответственность и определяет наказание за совершенные общественно опасные деяния в информационной и компьютерной области, что позволяет сделать следующие выводы:

[25] Быков В. И. Понятие компьютерной информации как объекта преступлений – Москва: журнал Законность №12, 2015.– С. 25-29.

✓ Нормы, содержащиеся в статьях 272-273 УК РФ, не включают в себя всю совокупность общественно опасных деяний, характеризующихся как компьютерное преступление;

✓ Существует пересечение преступлений, где компьютер является лишь орудием совершения преступления и где компьютер рассматривается в качестве совокупности информационных и аппаратных структур[26].

✓ Это определяет отношение конкретного преступления к определенной статье УК РФ.

Таким образом, в компьютерных преступлениях затруднено выделение определенного объекта преступного посягательства. Для разрешения указанных проблем необходимо провести работу над совершенствованием и устранением пробелов в действующем законодательстве, затрагивающем область компьютерных преступлений.

## 1.2 Компьютерная информация как предмет преступления, объективные и субъективные признаки

Развитие компьютерных технологий в современном мире, привело к изменениям в способе охраны информации, ведь компьютеры могут предоставлять доступ к колоссальному количеству самых разнообразных данных. В связи с этим, каждый год число компьютерных преступлений увеличивается, отсюда, становится абсолютно понятно, что информация - это ресурс, который необходимо защищать.

Теория и практика пока не выработала единого определения компьютерного преступления, так как, на международном уровне прослеживаются значительные разногласия между законодательством стран о преступлениях, связанных с компьютером[27].

[26] Кузнецова Г. М. Уголовный кодекс Российской Федерации: Постатейный комментарий – Москва: Изд-во ЗЕРЦАЛО, 2016. С. 328.
[27] Сундурова Ф.Р. Практикум по уголовному праву России / Под ред. проф. Ф.Р. Сундурова, М.В. Талан, И.А. Тарханова. – М.: Статут, 2014.

Предметом этой группы преступлений является хранящаяся и обрабатываемая в компьютерных системах информация. Она может оказаться предметом посягательства; являться средством совершения преступления по отношению к информации на других компьютерах либо свидетельствовать об иной формы преступной деятельности[28].

В ст. 272 УК «Неправомерный доступ к компьютерной информации» установлено наказание за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации. Отдельные авторы не согласны с названием ст. 272 УК РФ, так как считают, что исходя из диспозиции, правильнее было против бы говорить о неправомерном воздействии на информационную систему[29]. С этим сложно согласиться, так как обозначение статьи в целом соответствует ее наполнению, и при квалификации преступления важен не заголовок статьи, а содержание диспозиции нормы.

Состав преступления в ст. 272 УК является материальным. Уголовный закон не дает определения неправомерного доступа к охраняемой законом компьютерной информации, а указывает лишь его последствия. Отсутствие законодательного определения неправомерного доступа вызывает трудности при квалификации деяния по ст. 272 УК РФ[30].

Неправомерный доступ достигается путем проникновения в компьютерную систему или незаконного использования паролей и иных данных. Неправомерным также считают доступ к информационным ресурсам сети Интернет без согласия собственника или иного законного владельца охраняемой законом информации, если это привело к уничтожению,

[28] Гаврилов М., Иванов А. Извлечение и исследование компьютерной информации // Криминалистика. 2014. № 4. С. 74.
[29] Осипенко А. Уголовная ответственность за неправомерный доступ к конфиденциальной компьютерной информации // Уголовное право. 2014. № 3. С. 43-37.
[30] Сизов А. В. Неправомерный доступ к компьютерной информации: практика правоприменения // Информационное право. 2014. № 1. С. 32-35.

блокированию, модификации или копированию информации, при обязательном условии отсутствия у лица права доступа к ней[31].

Сам факт вызова или просмотра компьютерной информации, хранящейся на машинном носителе, состава такого преступления не образует[32]. Законодатель не раскрывает понятия конкретных видов последствий, указанных в диспозиции статьи.

Необходимо отметить положительные сдвиги российского уголовного закона. Недавние изменения статей о преступлениях в сфере компьютерной информации явились серьезным шагом на пути совершенствования указанных норм. В частности, были исключены признаки, вызывающие множество трудностей при применении некоторые норм: «нарушение работы ЭВМ, компьютерной системы ЭВМ или их сети», «совершение деяния лицом, имеющим доступ к ЭВМ, системе владельца ЭВМ или их сети». В диспозиции статей были внесены несколько важных и необходимых на сегодняшний день признаков: «наступление тяжких последствий или угроза их наступления», «совершение деяния из корыстной заинтересованности», «причинение крупного ущерба». В примечании к ст. 272 УК РФ было закреплено толкование признака «крупный ущерб». Ранее используемое в ст. 274 УК понятие «существенный вред» не раскрывалось, что затрудняло применение нормы. Также, о чем уже говорилось ранее, было введено понятие «компьютерная охраняемая информация». Поэтому, можно сделать следующий вывод, что развитие информационных технологий привело к возникновению приоритета обеспечение кибербезопасности Российской Федерации. Государство активно осуществляет политику противодействия киберпреступности в рамках реализации основных принципов построения информационного общества. Это обусловлено необходимостью создания общенациональных систем безопасности информационно-коммуникационной инфраструктуры, обеспечивающих надежную ее защиту

[31] Копырюлин А. Н. Квалификация преступлений в сфере компьютерной информации // Законность. 2017. № 6. С. 40.
[32] Шурухнова Н. Г. Расследование неправомерного доступа к компьютерной информации / Под ред. Н. Г. Шурухнова. М.: Щит-М, 1999. С. 70. // СПС «КонсультантПлюс», 2018.

от возможных угроз. Ведь защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Ст. 273 УК РФ предусматривает ответственность за создание, использование и распространение вредоносных компьютерных программ. Объективная сторона данного преступления характеризуется альтернативно предусмотренными действиями в отношении особого предмета преступления: компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (в обыденном словоупотреблении обычно называемых вирусами).

Создание программы или информации предполагает любую деятельность, направленную на написание хотя бы одной копии программы или информации как единолично, так и совместно с другими лицами. При совместном создании программы лицо может принимать как творческое участие в написании, так и обеспечивать техническую поддержку написания иными лицами. Создаваемая программа не обязательно должна обладать свойствами новизны; она может являться простым повторением кода иной программы.

Распространение предполагает как возмездную, так и безвозмездную передачу программы (информации) или носителя с программой (информацией) иным лицам без признаков использования программы. Распространение возможно и в форме однократной передачи программы (информации) или носителя с программой (информацией) иным лицам. Способы распространения различны: с помощью средств связи (в том числе компьютерных сетей), сообщение кода программы в устной или письменной форме, копирование программы (информации) с одного носителя на другой, передача носителя с программой (информацией) и т.п.

Использование программы (информации) имеет место при внедрении программы в компьютер или компьютерную сеть независимо от того, повлекло ли это какие-либо последствия, поскольку преступление окончено в момент совершения соответствующих действий.

Особо квалифицированный состав (ч. 3) характеризуется наступлением или созданием реальной угрозы наступления тяжких последствий, к числу которых можно отнести нарушение работы предприятий, учреждений, организаций; сбой в работе общественного транспорта, средств массовой информации или реальная опасность катастроф на транспорте или в области связи; длительный сбой в работе компьютерных сетей; уничтожение значимых или крупных массивов данных и т.д.

Ст. 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объективная сторона характеризуется деянием в форме действия или бездействия, заключающимся в нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования либо правил доступа к информационно-телекоммуникационным сетям. Указанные правила представляют собой обязательные к соблюдению технические правила, разработанные изготовителями оборудования, разработчиками программ, службами, обслуживающими оборудование, а также уполномоченными государственными органами.

Состав преступления материальный; предполагается два последствия, наступающих друг за другом и причинно связанных. Первое описывается в законе как уничтожение, блокирование, модификация или копирование компьютерной информации, что, в свою очередь, вызывает второе последствие в виде крупного ущерба.

Субъективная сторона может характеризоваться как умышленной, так и неосторожной формой вины. Субъект преступления специальный: лицо, обязанное соблюдать соответствующие правила.

Тяжкие последствия в ч. 2 схожи по содержанию с соответствующим признаком в ч. 3 ст. 273 УК РФ.

С 1 января 2018 г. вступил в силу Федеральный закон от 26 июля 2017 г. N 194-ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" <1>, которым гл. 28 УК РФ была дополнена специальной нормой об ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274.1).

Специальная уголовно-правовая охрана информационно-коммуникационного комплекса, обеспечивающего нормальное функционирование особо важных для общества и государства объектов, не является изобретением российского законодателя и встречается во многих современных правовых режимах. Положения об уголовной ответственности за посягательства на публичные информационные ресурсы, обладающие исключительной значимостью, имеются в законодательстве Великобритании, Германии, Китая, Сингапура, США, Франции и др.

Редакция ст. 274.1 УК РФ представляет собой объединение трех традиционных для отечественного законодательства форм преступного посягательства на безопасность компьютерных данных и систем: 1) неправомерный доступ; 2) создание и распространение вредоносного контента и 3) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации.

По смыслу ст. 274.1 УК РФ все эти деяния должны быть направлены против объектов критической информационной инфраструктуры. Таким образом, анализируемая уголовно-правовая норма конкурирует сразу с тремя

статьями (ст. ст. 272, 273 и 274 УК РФ) и является специальной по отношению к ним. В некотором смысле конструирование ст. 274.1 УК РФ противоречит сложившимся отечественным традициям криминализации и использования приемов юридической техники при описании уголовно-правовых норм. Следуя им, установление более строгой уголовной ответственности за посягательства на объекты критической информационной инфраструктуры предпочтительнее было бы реализовать путем выделения соответствующих квалифицирующих и особо квалифицирующих признаков в ст. ст. 272, 273 и 274 УК РФ.

Объектом преступлений, предусмотренных ст. 274.1 УК РФ, выступает безопасность критической информационной инфраструктуры Российской Федерации, т.е. состояние ее защищенности от любого воздействия программными или программно-техническими средствами, которое способно привести к нарушению ее функционирования и (или) нарушению безопасности обрабатываемой ею информации.

Предметом преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, является компьютерная информация или компьютерные программы, заведомо предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры. Нельзя не отметить, что установление данного признака на практике может вызвать значительные затруднения. Функциональная направленность вредоносной программы, т.е. ее предназначение именно для посягательств на соответствующие объекты, может быть установлена только в случае уникальности средств и технологий программной защиты объектов критической информационной инфраструктуры, что представляется маловероятным.

Специфическим предметом преступлений, предусмотренных ч. ч. 2 и 3 ст. 274.1 УК РФ, выступают объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и

автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности и химической промышленности.

Относимость того или иного информационного ресурса к критическому определяется посредством его включения в Реестр значимых объектов критической информационной инфраструктуры (ст. 8 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации").

Объективная сторона преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, предполагает совершение любого из трех альтернативных действий: 1) создание; 2) использование или 3) распространение компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры.

Состав по конструкции (по моменту описания в законе момента окончания преступления) является формальным. Если лицо одновременно разработало, использовало и распространило вредоносную компьютерную программу, заведомо предназначенную для совершения компьютерных атак на объекты критической информационной инфраструктуры, содеянное образует единое преступление.

Объективная сторона преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, заключается в неправомерном доступе к компьютерной информации, содержащейся в критической информационной инфраструктуре. Состав по конструкции является материальным. Преступление считается оконченным только в случае причинения вреда критической информационной инфраструктуре Российской Федерации. Таким образом, следует сделать вывод, что сам по себе неправомерный доступ (так называемое "чистое хакерство", осуществляемое из профессионального интереса без намерения

причинить вред) по смыслу ч. 2 ст. 274.1 УК РФ не является преступлением. В свою очередь, если лицу, осуществившему неправомерный доступ к компьютерной информации, содержащейся в критической информационной инфраструктуре, по независящим от него обстоятельствам не удалось причинить вред критической информационной инфраструктуре Российской Федерации (например, в результате успешного срабатывания антивирусного программного обеспечения или действий сотрудников, отвечающих за информационную безопасность организации), содеянное следует квалифицировать как покушение на преступление по ч. 3 ст. 30, ч. 2 ст. 274.1 УК РФ.

Вред как конструктивный признак состава преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, не конкретизирован. Системное толкование отечественного уголовного законодательства позволяет сделать вывод, что таковыми являются уничтожение, блокирование, модификация, копирование информации, содержащейся в критической информационной инфраструктуре, нейтрализация средств защиты указанной информации или выведение из строя аппаратных и программных средств, обеспечивающих функционирование критической информационной инфраструктуры (за исключением случаев, когда это повлекло причинение смерти или тяжкого вреда здоровью человека, причинение средней тяжести вреда здоровью двум или более лицам, массовое причинение легкого вреда здоровью людей, наступление экологических катастроф, транспортных или производственных аварий, повлекших длительную остановку транспорта или производственного процесса, дезорганизацию работы конкретного предприятия, причинение особо крупного ущерба, т.е. тяжких последствий[33], предусмотренных ч. 5 ст. 274.1 УК РФ).

Следует отдельно указать, что диспозиция ч. 2 ст. 274.1 УК РФ по сути содержит признаки составного преступления, поскольку указывает, что под

[33] Гузеева О.С. Преступления, совершаемые в российском сегменте сети Интернет: Монография. М.: Академия Генеральной прокуратуры Российской Федерации, 2015. С. 37; Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: Учебное пособие. М.: ИНФРА-М, 2017. С. 44.

неправомерным доступом следует также понимать доступ с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ. Таким образом, ч. 2 ст. 274.1 УК РФ охватывает и не требует квалифицировать по совокупности неправомерный доступ к объектам критической информационной инфраструктуры, совершенный с использованием заведомо предназначенных для этого вредоносных программ (ч. 1 ст. 274.1 УК РФ) или иных вредоносных программ (ст. 273 УК РФ). При этом если лицо, использовавшее программу, являлось и ее разработчиком, содеянное необходимо квалифицировать по совокупности преступлений. В данном случае вполне применимо известное правило квалификации, согласно которому действия по подготовке или исполнению деяния, не входящие в объективную сторону оконченного преступления (которые по сути не являются юридически значимым способом совершения этого преступления), должны получить самостоятельную уголовно-правовую оценку по другой статье закона[34].

Кроме того, совокупность преступлений, предусмотренных ст. 273 УК РФ и ч. 1 ст. 30 ч. 2 ст. 274.1 УК РФ, может иметь место и в том случае, когда лицо создает компьютерную программу либо иную компьютерную информацию, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. Однако в этом случае необходимо доказать умысел лица на их дальнейшее использование.

Практически значимым аспектом является оценка действий субъекта, который за вознаграждение изготавливает вредоносное программное обеспечение, предназначенное по своим характеристикам для осуществления атаки на объект критической информационной инфраструктуры, и сбывает

[34] Решетников А.Ю. Квалификация неоконченных преступлений при наличии признаков совокупности преступлений // Вестник Академии Генеральной прокуратуры Российской Федерации. 2016. N 4. С. 85.

его. При отсутствии осведомленности о том, что с данным информационным орудием собирается делать заказчик, действия соответствующих лиц нельзя признать согласованными и совместными. Это исключает саму постановку вопроса о возможности соучастия в данном случае. При обратной ситуации, когда лицо понимает, для каких целей изготавливается данная программа, содеянное необходимо квалифицировать как пособничество в совершении неправомерного доступа, т.е. по ч. 5 ст. 33 и ч. 2 ст. 274.1 УК РФ[35].

Объективная сторона преступления, предусмотренного ч. 3 ст. 274.1 УК РФ, заключается в нарушении:

1) правил эксплуатации: а) средств хранения, обработки или передачи охраняемой компьютерной информации; б) информационных систем; в) информационно-телекоммуникационных сетей; г) автоматизированных систем управления; д) сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации;

2) правил доступа к указанным средствам, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи.

Состав по конструкции является материальным; преступление считается оконченным только в случае причинения вреда критической информационной инфраструктуре Российской Федерации. В отличие от ст. 274 УК РФ, характеризующейся двумя уровнями взаимосвязанных общественно опасных последствий, ч. 3 ст. 274.1 УК РФ не предполагает установления признака крупного ущерба.

Учитывая специфику объектов посягательства, следует отметить, что совершение компьютерных атак на информационные ресурсы объектов транспорта, оборонной, атомной, ракетно-космической или химической промышленности может содержать признаки и других преступлений, предусмотренных ст. ст. 205, 281, 275, 276 УК РФ и др.

[35] Решетников А.Ю., Русскевич Е.А. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) // Законы России: опыт, анализ, практика. 2018. N 2. С. 51 - 55.

Субъектом преступлений, предусмотренных ч. ч. 1 и 2 ст. 274.1 УК РФ, является физическое вменяемое лицо, достигшее возраста 16 лет. Субъектом ч. 3 ст. 274.1 УК РФ может быть как общий - в части правил доступа к ресурсам, так и специальный - в части соблюдения правил эксплуатации соответствующих средств, систем и сетей.

Субъективная сторона создания, использования и распространения компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры, характеризуется прямым умыслом. Лицо, совершая те или иные действия, должно осознавать, что они направлены на публичные информационные ресурсы, обладающие исключительной важностью для общества и государства и включенные в соответствующий реестр.

При неправомерном доступе (ч. 2 ст. 274.1 УК РФ) умысел может быть как прямым, так и косвенным.

Субъективная сторона преступления, предусмотренного ч. 3 ст. 274.1 УК РФ, характеризуется двумя формами вины. Нарушение правил эксплуатации и доступа может совершаться как умышленно, так и по неосторожности. Следует поддержать точку зрения Н.Ш. Козаева, что неуказание на форму вины в составе нарушения правил эксплуатации средств хранения, обработки или передачи компьютерных данных (автор формулирует данный вывод применительно к ст. 274 УК РФ) является упущением законодателя, поскольку сама конструкция состава логически требует признания возможности совершения деяния по неосторожности, но ч. 2 ст. 24 УК РФ позволяет признавать преступление совершенным по неосторожности, только если это предусмотрено соответствующей статьей Особенной части УК РФ[36].

Квалифицированные виды неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации,

[36] Козаев Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): Монография. М.: Юрлитинформ, 2015. С. 172.

предусмотренные ч. ч. 4 и 5 ст. 274.1 УК РФ, являются традиционными для преступлений в сфере компьютерной информации и в целом хорошо освещены в современной литературе[37].

Дискуссионными, пожалуй, можно назвать два реализованных решения. Во-первых, законодатель проявил малопонятную последовательность в регламентации совершения преступления предварительно сговорившейся и организованной группами в рамках одной части. Очевидно, что уравнивание таких качественно разных по опасности форм соучастия вряд ли отвечает научно обоснованным критериям дифференциации ответственности. Во-вторых, все преступления в сфере компьютерной информации в качестве особо отягчающего обстоятельства называют наступление тяжких последствий или создание угрозы их наступления. Вместе с тем уголовно-правовая норма, предусмотренная ст. 274.1 УК РФ, такой оговорки не содержит, что, учитывая особую значимость объектов посягательства, представляется по меньшей мере ошибочным.

Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" предполагает категорирование всех объектов в зависимости от социальной, политической, экономической значимости, а также значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка. К сожалению, действующая редакция ст. 274.1 УК РФ не учитывает данное деление, что представляется существенным упущением не только с точки зрения игнорирования критериев дифференциации уголовной ответственности, но и что, пожалуй, более значимо, - анализируемая уголовно-правовая новелла не позволяет должным образом оценить различия в объеме и значимости социальных последствий криминальных посягательств на объекты критической инфраструктуры. Возможности учета опасности указанного деяния только лишь посредством дифференциации

[37] Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) / Под ред. С.В. Дьякова, Н.Г. Кадникова. 5-е изд., перераб. и доп. М.: Юриспруденция, 2017. С. 822 - 834.

уголовного наказания, как представляется, явно недостаточны. Полагаем, что в этой части уголовно-правовая норма об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации требует корректировки.

## 1.3 Классификация киберпреступлений

Активно ведутся споры относительно понятия криминализируемых деяний, которые предлагается обозначать не только как компьютерные[38], информационные[39] или киберпреступления [40], но и как преступления: «в сфере высоких технологий»[41], «в сфере обращения цифровой информации»[42], «с использованием электронной информации»[43], «с использованием компьютерных[44] или информационных, информационно-коммуникационных[45], информационно-телекоммуникационных[46] технологий», и др. Наверное, эту дискуссию нельзя считать просто спором о терминах, но наличие столь многих вариантов наименования рассматриваемых преступлений связано, главным образом, с новизной самих

[38] Степанов-Егиянц, В. Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями / В. Г. Степанов-Егиянц // Российский следователь. – 2013. – № 24. – С. 43–46; Комаров, А. А. О целесообразности использования «кибертерминологии» в исследовании проблем преступности / А. А. Комаров // Информационное право. – 2016. – № 1. – С. 4–7.

[39] Крылов, В. Информационные преступления – новый криминалистический объект / В. Крылов // Российская юстиция. – 1997. – № 4. – С. 22–23 // СПС «КонсультантПлюс», 2018.

[40] Чекунов, И. Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И. Г. Чекунов // Право и кибербезопасность. – 2013. – № 1. – С. 9–22; Халиуллин, А. И. Подходы к определению киберпреступления / А. И. Халиуллин // Российский следователь. – 2015. – № 1. – С. 34–39.

[41] Мороз, Н. О. Актуальные вопросы международного сотрудничества в борьбе с преступностью всфере высоких технологий в рамках СНГ / Н. О. Мороз // Международное уголовное право и международная юстиция. – 2016. – № 3. – С. 12–14; Третьяк, М. И. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий / М. И. Третьяк // Законность. – 2016. – № 7. – С. 41–46.

[42] Бегишев, И. Р. Преступления в сфере обращения цифровой информации / И. Р. Бегишев //Информационное право. – 2015. – № 2. – С. 18–21.

[43] Ефремова, М. А. Мошенничество с использованием электронной информации / М. А. Ефремова // Информационное право. – 2013. – № 4. – С. 19–21.

[44] Сафонов, О. М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. ... канд. юрид. наук: 12.00.08 / Сафонов Олег Михайлович. – М., 2015. С. 12.

[45] Хисамова, З. И. Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий / З. И. Хисамова // Юридический мир. – 2016. – № 2. – С. 58–62.

[46] Ефремова, М. А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения / М. А. Ефремова // Право и кибербезопасность. – 2014. – № 2. – С. 33–38.

общественных отношений, возникших и развивающихся в условиях цифровой революции. Последующая эволюция уголовного права определит жизнеспособность тех или иных терминов. Пока что – в целях простоты и удобства – представляется предпочтительным синонимичное использование терминов «компьютерные преступления» или «киберпреступления», помня об их условности. Например, по мнению И.Г. Чекунова, киберпреступность следует рассматривать шире компьютерной преступности, т.к. использование компьютера или компьютерных сетей для составляющих ее преступлений не всегда является необходимостью; кроме того, для совершения киберпреступлений используются не только компьютеры, но и мобильные (сотовые) коммуникационные технические устройства и системы связи[47]. Напротив, по оценке М. Герке, «киберпреступность» имеет более узкое значение, чем «преступления, связанные с применением компьютеров», поскольку подразумевает использование компьютерной сети. Под преступлениями, связанными с применением компьютеров, понимаются даже те правонарушения, которые затрагивают отдельно стоящие устройства и системы[48].

В УК РФ помимо главы 28, устанавливающей ответственность за преступления в сфере компьютерной информации, еще ряд норм предусматривают использование информационно-телекоммуникационных сетей (которые в некоторых случаях конкретизированы как сеть «Интернет») в качестве криминообразующего (ч. 3 ст. 137, ст. ст. $159^6$, $171^2$, $185^3$, 282) или квалифицирующего (ч. 2 ст. $205^2$, 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. $242^2$, ч. 2 ст. 280, ч. 2 ст. $280^1$) признаков. К предмету преступления, предусмотренного ст. 187 УК РФ, законодатель отнес электронные средства, электронные носители информации, технические устройства, компьютерные программы, предназначенные для

[47] Чекунов, И. Г. Понятие и отличительные особенности киберпреступности / И. Г. Чекунов // Российский следователь. – 2014. – № 18. – С. 53–56.

[48] Герке, М. Понимание киберпреступности: явление, задачи и законодательный ответ [Электронный ресурс] / М. Герке // Международный союз электросвязи: [сайт]. [2014]. URL: http://www.itu.int/en/ITU- / Cybersecurity/Documents/Cybercrime2014_R.pdf (дата обращения 03.04.2018).

неправомерного осуществления приема, выдачи, перевода денежных средств. Тем самым законодательная оценка компьютерных преступлений постепенно расширяется, с учетом чего заслуживает внимания так называемая «широкая трактовка киберпреступлений», которую В.Н. Черкасов, хотя и считает ошибочной, связывает с отнесением к преступлениям в киберпространстве любых преступных посягательств с использованием компьютерной техники и информационных технологий[49]. Тенденция развития законодательства именно в рамках данного подхода признается и другими специалистами[50], а ее экстраполяция позволяет считать правильным вывод А.И. Халлиулина, что перечень таких преступлений будет постоянно пополняться[51], причем не только в связи с отмечаемым им научно-техническим прогрессом, но и в связи с изменением социальной значимости информационных и телекоммуникационных отношений, а также криминогенными процессами в этой сфере.

Специалисты признают, что степень общественной опасности преступления повышает как способ его совершения, связанный с использованием технических средств и позволяющий конспирировать преступную деятельность[52], так и сами средства. Хотя, по мнению В.Н. Черкасова, использование современных компьютерных технологий явно повышает опасность только конкретных видов преступления, что требует введения соответствующих квалифицирующих признаков[53], следует – учитывая идею А. П. Козлова о необходимости унификации квалифицирующих и отягчающих обстоятельств – признать и допустимость внесения аналогичного признака в ст. 63 УК РФ, который в литературе,

[49] Черкасов, В. Н. Информационные технологии и организованная преступность [Электронный ресурс] /В. Н. Черкасов // Саратовский Центр по исследованию проблем организованной преступности и коррупции: [сайт]. [2014]. URL: http://sartraccc.ru/Pub/cherkasov%2824-03%29.htm (дата обращения 03.04.2018).
[50] Рассолов, И. М. Право и Интернет. Теоретические проблемы / И. М. Рассолов. – 2-е изд.,доп. – М.: Норма, 2009. – 384 с.// СПС «КонсультантПлюс», 2018.
[51] Халиуллин, А. И. Указ.соч. – С. 38.
[52] Смолин, С. Уголовно-правовая борьба с высокотехнологичными способами и средствами совершения преступлений / С. Смолин // Уголовное право. – 2014. – № 4. – С. 62–68.
[53] Черкасов, В. Н. Указ.соч. С. 32.

например, формулируется как «использование технических средств обработки электронной информации».

Кроме того, обсуждается вопрос о возможности уголовной ответственности за подделку электронного документа по ст. 327 УК РФ[54], за незаконную эмиссию или подделку электронных денег, за сбыт цифровой и документированной информации, добытой заведомо преступным путем. Внимание законодателя обращается на составы преступлений, при совершении которых использование высокотехнологичных средств и способов передачи ложной информации становится все более типичным (например, ст. ст. $128^1$, 207 УК РФ).

Поскольку круг компьютерных преступлений в уголовном законе стал достаточно широким, они приобрели разнородный характер, их дальнейший анализ требует выделения подгрупп, к которым применимы – с учетом общности их признаков – как единые принципы законодательной оценки, так и единые правила квалификации. Эта исследовательская задача может быть решена при помощи метода классификации преступных деяний, которая не только является необходимым условием правильного толкования норм об этих преступлениях, но и полезна в научно-методическом отношении[55] .

Традиционно уголовно-правовая классификация выражается «в систематизации преступлений по определенным признакам, предусмотренным в УК РФ»[56]. Такие признаки (критерии классификации преступлений) последовательно различаются: на уровне единичного – дифференциации составов преступлений – ими служат отдельные признаки составов преступлений (главным образом объективной стороны), на уровне особенного (Особенной части УК) – родовой объект, на уровне всеобщего (Общей части УК) – общественная опасность в целом, ее характер и

[54] Лукьянова, А. А. Электронный официальный документ как предмет преступления, предусмотренного ст. 327 УК РФ / А. А. Лукьянова // Уголовное право. – 2016. – № 3. – С. 57–62.
[55] Клепицкий, И. А. Система хозяйственных преступлений: монография / И. А. Клепицкий. –М.: Статут, 2005. – 572 с. // СПС «КонсультантПлюс», 2018.
[56] Кудрявцев, В. Н. Борьба мотивов в преступном поведении: монография / В. Н. Кудрявцев. – М.: Норма, 2007. – 128 с. // СПС «КонсультантПлюс», 2018.

степень[57]. С учетом множества закрепленных законодателем объективных и субъективных признаков преступлений (по которым они могут быть разделены на группы) расширяются как возможности классификации преступлений, так и варианты классификаций. Это, в свою очередь, требует оценки пригодности тех или иных классификаций для уголовно-правового анализа.

В литературе сформулирован ряд требований, которым должна отвечать уголовно-правовая классификация преступлений. Так, отмечается, что при выборе классификационного критерия необходимо руководствоваться следующими положениями: во-первых, роль основания для деления преступлений на группы или классы может выполнять лишь основной существенный признак; во-вторых, этот признак должен быть объективным, вытекающим из внутренней природы преступления как социального явления; в-третьих, такой признак должен отражать не только общее, но и особенное, т.е. не только сходство, но и различие в отдельных преступлениях; в-четвертых, содержание признака должно быть четким и ясным. Считается также, что любая классификация может быть правильной, если за ее основу берется стабильный признак, выражающий качественное свойство и своеобразие классифицируемых явлений[58]. Кроме того, нельзя искусственно разбивать единую в функциональном отношении группу, основываясь на малозначительных деталях. В противном случае будет утрачено целостное видение предмета.

Весь массив преступлений обычно классифицируется по следующим критериям: по степени тяжести; по видам вины; по характеру отражения преступления в законе; по характеру вреда объекту преступления. Чаще всего специалисты считают наиболее предпочтительной для науки уголовного права классификацию преступлений по объекту посягательства.

---

[57] Кузнецова, Н. Ф. Избранные труды: монография / Н. Ф. Кузнецова; предисл. В. Н. Кудрявцева. – СПб.: Изд-во «Юридический центр Пресс», 2003. – 834 с. // СПС «КонсультантПлюс», 2018.

[58] Егиазарян, Н. А. Преступления против порядка управления в уголовном праве Армении и России (сравнительно-правовое исследование): дис. … канд. юрид. наук: 12.00.08 / Егиазарян Наира Ашотовна. – М., 2013. – 225 с. // СПС «КонсультантПлюс», 2018.

Такая классификация, по оценке В. Н. Кудрявцева, полезна, по крайней мере, в двух отношениях: во-первых, она распределяет все преступления по направленности этого посягательства – против личности, имущества, государственных, общественных интересов и т.д. и тем самым группирует их по определенным признакам, а во-вторых, она дает представление о смежных составах преступлений.

Учитывая, что в нашей стране компьютерные преступления законодатель выделил в разных главах Особенной части УК РФ, их можно классифицировать по соответствующим видовым объектам, однако такая классификация вряд ли будет отражать сущностные признаки этих деяний, поскольку их специфика определяется не объектом посягательства. Например, одна из таких классификаций включает в систему компьютерных преступлений преступления против личности; преступления в сфере экономики; преступления против общественной безопасности, общественного порядка и общественной нравственности; преступления против безопасности государства[59]. Очевидно, что эта классификация не изменится и при ее применении к традиционно выделяемым преступлениям.

При этом одним из обязательных признаков любого киберпреступления специалисты считают одновременное наличие двух объектов посягательства: как общественных отношений в сфере безопасности обращения компьютерной информации, так и связанных с ней общественных отношений, имеющих взаимосвязь с реальным миром (отношений собственности, жизни, здоровья и т.д.) В зависимости от того, являются ли отношения, возникающие в сфере компьютерной информации или обеспечивающие безопасность компьютерной информации, основным или дополнительным объектом, выделяют собственно преступления в сфере компьютерной информации (гл. 28 УК РФ) и большой круг преступных деяний, предусмотренных статьями других глав УК РФ. Вместе с тем,

[59] Широков, В. А., Беспалова, Е. В. Компьютерные преступления: основные тенденции развития / В. А. Широков, Е. В. Беспалова // Юрист. – 2006. – № 10. – С. 18–21 // СПС «КонсультантПлюс», 2018.

размещение законодателем запрещаемых форм поведения по главам носит условный характер, с учетом чего меняется и оценка объекта как основного или дополнительного. Соответственно, такая классификация носит формальный, а не сущностный характер.

Предложенная А.Г. Волеводзом классификация по своей сути также строится на признаке объекта преступлений. Так, он выделяет преступления в сфере компьютерной информации, посягающие на информационные компьютерные отношения; преступления в информационном компьютерном пространстве, посягающие на отношения, возникающие по поводу реализации прав на информационные ресурсы, информационную инфраструктуру и составляющие ее части; иные преступления, для которых характерно использование компьютерной информации или составляющих ее элементов информационного пространства, посягающие на иные охраняемые уголовным законом правоотношения[60]. Вместе с тем, проводя такую классификацию, он отмечает, что вторая группа не требует самостоятельной регламентации в уголовном законодательстве. С учетом этого, теряется уголовно-правовое значение такой классификации, поскольку она не отражает качественный признак криминализируемых деяний.

Конвенция о преступности в сфере компьютерной информации (ETS № 185) (Конвенция о киберпреступности) от 23 ноября 2001 г. предлагает государствам-участникам включить в уголовное право четыре группы преступлений: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем; правонарушения, связанные с использованием компьютерных средств; правонарушения, связанные с содержанием данных; правонарушения, связанные с нарушением авторского права и смежных прав (разделы 1-4 части 1 главы II). Конечно, в таком разделении не соблюдается ни последовательность деления, ни наличие единого критерия для этого. Аналогичные недостатки можно выделить и в

[60] Волеводз, А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества: монография / А. Г. Волеводз. – М.: Юрлитинформ, 2001. – 496 с. // СПС «КонсультантПлюс», 2018.

подготовленном группой экспертов ООН обзоре, который делит киберпреступления на три группы: преступления против конфиденциальности, целостности и доступности компьютерных данных или систем; преступления, связанные с использованием компьютеров (computer-related acts) с целью получения корыстной или личной выгоды либо причинения вреда; преступления, связанные с содержанием информации (computer content-related acts)[61]. Главной особенностью киберпреступления (компьютерного преступления, преступления в сфере высоких технологий) специалисты признают использование сетей компьютера для совершения противоправного поступка или преступления в виртуальном пространстве, что предполагает наличие прямого умысла. С умышленным характером кибепреступлений согласны и другие авторы. Хотя представляется возможным выделение состава нарушения правил кибербезопасности, повлекшего по неосторожности тяжкие последствия (который был бы смежным иным уголовно наказуемым случаем нарушения специальных правил безопасности в главе 24 УК РФ), уголовно-правовая классификация анализируемых преступлений по признакам субъективной стороны также малоперспективна. Если раньше специфика преступлений в сфере компьютерной информации была обусловлена использованием при их совершении высоких технологий и новейших достижений науки и техники, необходимостью обладания определенным уровнем специальных познаний, то в настоящее время в глобальной сети Интернет в практически свободном доступе находятся как программы, предназначенные для совершения несанкционированных действий с компьютерной информацией, так и инструкции по их применению[62]. Соответственно, значимая для уголовного права классификация этих преступлений по признакам субъекта построена

[61] Comprehensive Study on Cybercrimes [Электронный ресурс] / United Nations Office on Drugs and Crime: [сайт]. [2013]. URL: http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf (дата обращения 03.04.2018).

[62] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) [Электронный ресурс]. Документ опубликован не был. Доступ из справ. -правовой системы «Консультант Плюс».

быть не может. В литературе распространены классификации, построенные на изменении места информации (информационных технологий) в механизме совершения преступления. Например, в первой категории преступлений информационные технологии признаются в качестве объекта посягательства, т.е. преступлением является хищение информации или нанесение какого-либо урона информационной системе. Во второй категории информационные технологии используются в качестве орудий совершения традиционных преступлений и электронных атак.

Третью категорию составляют преступления, в которых информационные технологии и системы содержат запоминающие устройства, на которые совершается несанкционированный доступ[63]. Похожую классификацию приводит И.О. Морар, который считает, что она может базироваться на своеобразии способов совершения деяний: а) способы, применимые для получения доступа к информации, находящейся на машинных носителях (аппаратные устройства компьютерного типа, телефоны, пейджеры, аналоговые записывающие устройства и т.д.); б) способы, где компьютерная техника и средства коммуникации используются в качестве орудий и средств совершения преступления и/или их сокрытия; в) способы, где применяются высокотехнологичные устройства с целью незаконного доступа к компьютерной информации, ее модификации или блокирование[64]. По оценке А.И. Халиуллина, наиболее простым (но не оправдывающим себя) способом является классификация киберпреступлений по принципу определения роли компьютера (компьютерной информации) как средства либо предмета преступления. Еще больше запутывают ситуацию утверждения, что информацию следует рассматривать как предмет уголовно-правовой охраны, а не предмет состава преступления. Все подобные классификации строятся не на одном признаке состава преступления, а на

[63] Демьянец, М. В. Предпринимательская деятельность в сети Интернет: монография / М. В.Демьянец, В. М. Елин, А. К. Жарова. – М.: Юркомпани, 2014. С. 43.

[64] Морар, И. О. Могут ли в рамках науки криминологии рассматриваться способы совершения компьютерных преступлений и их последствия? / И. О. Морар // Российский следователь. – 2014. – № 12. – С. 37–41.

отнесении информации (информационных технологий) к разным элементам состава преступлений, с учетом чего они носят непоследовательный характер.

Неслучайно ряд исследователей приходят к выводу, что преступления в сфере компьютерной информации являются разнородными, вследствие чего нельзя создать классификацию способов совершения преступлений[65]. Наиболее пессимистичная оценка сводится к тому, что наличие настолько разнородных преступлений, совершаемых в информационно-телекоммуникационных сетях, не позволяет говорить о существовании киберпреступлений в уголовно-правовом смысле как отдельной группы преступлений. Действительно, в подготовленном для обсуждения на тринадцатом конгрессе ООН по предупреждению преступности и уголовному правосудию справочном документе отмечается, что в целом граница между киберпреступностью и обычной преступностью становится все более размытой[66], однако вряд ли это исключает возможность уголовно-правовой классификации киберпреступлений. Перспективным для построения естественной классификации широко понимаемых компьютерных преступлений по единому критерию представляется обращение к признакам объективной стороны и развитие идей А.А. Тер-Акопова, который считал, что деяние может иметь различную причиняющую природу: физическую, информационную и нормативно-программную. По его оценке, при информационном воздействии деяние характеризуется передачей информации, которая имеет уголовно-правовое значение, причиняющую силу. Такое воздействие А.А. Тер-Акопов делил на четыре вида: информационно-психологическое (обманы, угрозы, подделки документов, заведомо ложные сообщения и т.п.); манипулирование информацией

[65] Будаковский, Д. С. Способы совершения преступлений в сфере компьютерной информации /С. С. Будаковский // Российский следователь. — 2014. – № 4. – С. 2–4.

[66] Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия напоявляющиеся формы преступности, такие как киберпреступность и незаконные оборот культурных ценностей, в том числе извлеченные уроки и международное сотрудничество. Справочный документ семинара- практикума. Электронный ресурс] / United Nations Office on Drugs and Crime: [сайт]. [2015]. URL: A/CONF.222/12 [Электронный ресурс] // http://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_r_V1500665.pdf (дата обращения 03.04.2018).

(выдача, передача, разглашение информации; непредоставление или сокрытие информации; искажение информации); несанкционированный доступ к защищаемой информации; информационно-компьютерные способы причинения имущественного вреда[67]. Хотя сама идея информационного воздействия заслуживает поддержки, выделенные при этом виды не могут считаться последовательной классификацией, поскольку, в частности, искажение информации тесно сближается с обманом и заведомо ложными сообщениями. Кроме того, неясен критерий выделения этих видов.

Признавая информационное воздействие отличительной чертой компьютерных преступлений, можно построить уголовно-правовую классификацию по характеру (направленности) данного способа совершения преступления. Использование данного критерия позволяет выделить следующие виды анализируемых преступлений: информационно-компьютерные (для которых характерно изменение технически, компьютерной обрабатываемой информации без воздействия на психику человека или состояние технических устройств); информационно-психические (когда при помощи коммуникационных технологий информация адресуется конкретному лицу или неопределенному кругу лиц с интеллектуальным или эмоциональным воздействием); информационно-технические (когда информация передается, блокируется, изменяется с целью управляющего или разрушающего воздействия на технические устройства). Теоретически можно было бы говорить о возможности информационного воздействия не только на психику, но и на организм человека. В частности, И.Г. Чекунов утверждает, что судебной практике известны случаи, когда путем распространения информации совершались убийства или причинялся вред здоровью, способами чего служили массовый гипноз людей или зомбирование конкретного человека.

[67] Тер-Акопов, А. А. Преступление и проблемы нефизической причинности в уголовном праве: монография / А. А. Тер-Акопов. – М.: «Юркнига», 2003. – 480 с. // СПС «КонсультантПлюс», 2018.

Распространение информации может явиться одним из способов доведения до самоубийства. Соответственно, путем использования информационно-коммуникационных технологий возможно не только информационное, но и физическое воздействие на человека с целью причинения вреда его здоровью или убийства. Встречаются упоминания о психонаркогенах, которые оказывают эффект, сходный с наркотическим в результате применения комбинации определенных электромагнитных излучений цвета и звука[68]. Как отмечает Л.И. Романова, в Интернете был отмечен всплеск поисковых запросов, связанных с «аудионаркотиками»[69]. В практике судов примеров доказанного воздействия такого рода найти не удалось. Конечно, возможно убийство путем информационного вмешательства в работу, например, компьютерных устройств, входящих в состав реанимационного оборудования. В данном случае способ самого киберпреступления тогда будет носить информационно-технический характер, способ же причинения смерти будет основываться на физической, а не информационной причинности. С развитием науки, если будет показана возможность зомбирования и тому подобного воздействия (меняющего не психические, а физиологические процессы в организме), оно может быть отнесено к четвертому его виду – информационно-физическому (при этом может быть более корректным будет даже термин «информационно-физиологическое»), которое должно квалифицироваться как физическое насилие.

Предложенная классификация построена по одному критерию, отражающему сущность этих преступлений и характеризующему их объективную сторону, может позволить сформировать единые подходы к уголовно-правовой оценке компьютерных преступлений, единые правила

---

[68] Основные направления противодействия транснациональному организованному криминальномунаркобизнесу: монография / Л. Драпкин, Р. Вафин, Я. Злоченко и др.; под общ. ред. И. И. Ищенко. – М.: ЛексЭст, 2003. – 424 с. // СПС «КонсультантПлюс», 2018.

[69] Романова, Л. И. Наркопреступность: криминологическая и уголовно-правовая характеристика: учеб. метод. пособие / Л. И. Романова. – 2-е изд. – Владивосток: Изд-во Дальневосточного ун-та, 2009. – 314 с. // СПС «КонсультантПлюс», 2018.

квалификации предложенных групп преступлений и, в конечном счете, единые принципы применяемой к ним уголовной политики.

# 2 ОСОБЕННОСТИ ВЫЯВЛЕНИЯ, РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РФ: ПРОБЛЕМЫ НОРМОТВОРЧЕСТВА И ПРАВОПРИМЕНИТЕЛЬНОЙ ПРАКТИКИ

## 2.1 Специфика подготовки и проведения осмотра места происшествия и обыска

Важнейшим следственным действием, направленным на обнаружение, фиксацию и изъятие следов преступления, которые впоследствии могут стать ценными вещественными доказательствами является осмотр места происшествия. Следователь, производящий осмотр места происшествия, не всегда имеет достаточный уровень знаний, позволяющий обнаружить следы преступления, совершённого с использованием компьютерной информации, надлежащим способом их изъять и упаковать. Для этого в обязательном порядке в этом следственном действии участвует специалист. Основной целью осмотра места происшествия является установление конкретного персонального компьютера и цифровой информации, выступающей в качестве предмета или орудия совершения преступления и несущей в себе следы совершения преступления[70]. Детальное описание устройств, их соединений должно сопровождаться видеофиксацией последовательности действий следователя и специалистов, а также полученного при этом результата в виде доказательств. Если при проведении осмотра используются специальные поисковые технические устройства (материалы, программы), об этом делается соответствующая отметка в протоколе следственного действия с указанием их индивидуальных признаков (тип, марка, название, заводской номер и т. д.), также необходимо указывать, что данное устройство применяет специалист. Особенно тщательно должны быть осмотрены и

[70] Галкина У. В. Проблемы возбуждения уголовного дела о незаконном использовании средств индивидуализации товаров (работ, услуг)// Мол. учёный. — 2016. — № 25-1 (129). — С. 14–15.

указаны в протоколе типичные для компьютерных преступлений вещественные доказательства: вредоносное программное обеспечение для компьютеров (всех видов) и носители с ними; программы для компьютеров, заведомо приводящие к несанкционированным пользователем действиям, а также их носители; обнаруженные специальными техническими средствами негласного получения (уничтожения, блокирования, изменения) компьютерной информации носителей; специфические следы преступления.

Особой подготовки в ходе производства предварительного следствия по данной категории дел требует такое следственное действие, как обыск. Зачастую его необходимо провести одновременно по нескольким адресам и в нескольких городах. Так, сотрудниками Управления «К» МВД России совместно с оперативниками отдела «К» УМВД России по Республике Татарстан и УФСБ России по Республике Татарстан пресечена деятельность злоумышленников, осуществлявших несанкционированный доступ к компьютерам руководителей крупных государственных и коммерческих организаций с целью получения конфиденциальной информации. Было установлено, что на территории России действует группа, которая специализируется на неправомерном доступе к компьютерной информации с использованием вредоносного программного обеспечения. Злоумышленники работали по заказам, выбирая своих жертв согласно пожеланиям клиентов. Основной целью участников группы являлось получение конфиденциальных сведений о работе государственных и коммерческих предприятий, личные документы и переписка их руководителей. В процессе осуществления кибератак использовались целевые рассылки электронных писем, содержащих архивы с троянскими программами, которые позволяли получить удалённый доступ к компьютеру. В ходе производства предварительного следствия оперативниками Управления «К» МВД России совместно с сотрудниками УФСБ России по Республики Татарстан установлено, что четверо непосредственных участников преступной группы проживают в Казани и арендуют офис в одном из бизнес-центров. В ходе

проведения скоординированной операции подозреваемых задержали. Сотрудниками полиции проведено 10 обысков, в ходе которых изъято более 100 единиц компьютерной техники, сетевое и серверное оборудование, носители информации, содержащие сведения, которые доказывают причастность данных лиц к совершению противоправных действий[71].

На данный момент правоохранительные органы испытывают затруднения при расследовании данных преступлений. Эти затруднения носят как технический, так и методический характер. Из всей массы имеющейся информации в методиках расследования отсутствуют максимально современные подходы к интернет-технике, интернет-информации и работе с ней, это связано с быстрым техническим прогрессом.

## 2.2 Взаимодействие служб и подразделений ОВД с общественными объединениями и коммерческими организациями при выявлении, раскрытии и расследовании преступлений в сфере использования компьютерной информации.

Взаимодействие следователя с должностными лицами различных правоохранительных органов и государственных органов при расследовании преступлений в сфере компьютерной информации представляет собой согласованную и совместную их деятельность, направленную на установление истины по уголовному делу. Главной целью взаимодействия является раскрытие и расследование преступления.

Следователь выполняет главную и руководящую роль, несет личную ответственность за принимаемые решения и результаты расследования. Деятельность всех остальных участников взаимодействия направлена на решение задач, которые поставлены перед ними следователем.

[71] Официальный сайт МВД РФ. // [Электронный ресурс]. — Режим доступа: https://мвд.рф (дата обращения: 03.04 2018).

Координационная деятельность участников реализуется в различных формах взаимодействия: координационные совещания руководителей правоохранительных органов; информационный обмен по вопросам борьбы с киберпреступностью; проведение при совместных выездах в регионы согласованных действий, проверок и оказание помощи правоохранительным органам регионов в борьбе с преступлениями в сфере компьютерной информации, изучении и распространении положительного опыта; создание СОГ для расследования конкретных преступлений в сфере компьютерной информации; совместные конференции и семинары; издание совместных приказов, указаний, подготовка различного рода организационно-распорядительных документов; разработка и утверждение согласованных планов координационной деятельности.

Быстрое раскрытие преступлений и качественное их расследование видятся только при успешном взаимодействии следователя и оперативного сотрудника, осуществляемом в рамках совместно выработанного, конкретного, согласованного и аргументированного плана.

Справедливо заметил С.А. Янин, что организация взаимодействия – это одна из важнейших задач следователя, так как его деятельность по надлежащей организации первоначального этапа расследования является залогом эффективности деятельности ОВД в противодействии преступности[72].

Общественные организации располагают большим объемом информации, которая может использоваться при раскрытии и расследования преступлений в сфере компьютерной информации. Взаимодействие с общественными организациями реализуется путем: содействия при производстве розыскных мероприятий; выявления источников

[72] Янин С.А. Организация первоначального этапа расследования незаконного сбыта наркотических средств и психотропных веществ // Организация деятельности органов предварительного следствия и дознания в системе МВД России: управленческие и криминалистические проблемы: Сб. материалов Всероссийской научно-практической конференции: В 2 ч. М.: Академия управления МВД России, 2012. Ч. 1. С. 271 //СПС «КонсультантПлюс2, 2018.

доказательственной и ориентирующей информации; получение независимых характеристик тех или иных лиц и т.п.

В качестве повода для возникновения, изменения и прекращения взаимодействия следователя с общественными организациями при расследовании компьютерных преступлений, как правило, выступает информация, которой располагает следователь в данный момент расследования.

Следователь, привлекая представителей общественных организаций к выявлению и расследованию преступлений, всегда может быстрее пресечь преступную деятельность, носящую продолжающийся характер.

При расследовании преступлений в сфере использования компьютерной информации наибольший эффект проявляется при взаимодействии следователя с представителями коммерческих организаций специальной направленности, ориентированных на противодействие киберпреступлениям и обеспечение информационной безопасности. Примером такой совместной работы является опыт взаимодействия следователей с компанией «Лаборатория Касперского», в составе которой существует специализированный отдел, занятый заказными расследованиями инцидентов в области компьютерной информации.

В силу своего правового статуса отдел по расследованию компьютерных инцидентов «Лаборатории Касперского» не осуществляет собственно оперативно-розыскную деятельность, однако он проводит первичный анализ компьютерного инцидента, его предварительное «расследование» до обращения клиента в правоохранительные органы и ведет экспертное сопровождение уголовного дела.

Лаборатория компании Group-IB – единственная в России, в которой специалисты имеют сертификаты GIAC по Digital Forensics и Malware Analysis. Результаты её экспертиз гарантированно принимаются в качестве доказательств не только в российских, но и в иностранных судах.

Таким образом, можно сделать вывод о том, что эффективное использование помощи общественности в расследовании преступлений способствует оптимизации затрат времени, средств и сил органов предварительного следствия на расследование преступлений.

Взаимодействие с общественными организациями реализуется путем: содействия при производстве розыскных мероприятий, выявления источников доказательственной и ориентирующей информации, получение независимых характеристик тех или иных лиц и т.п.

## 2.3 Использование специальных познаний при расследовании преступлений в сфере использования компьютерной информации

Круг экспертиз, назначаемых по делам о преступлениях в сфере компьютерной информации, достаточно широкий. В их перечне присутствуют как традиционные криминалистические экспертизы, так и нетрадиционные. По каждому уголовному делу перечень экспертиз индивидуален, зависит от вида компьютерного преступления и, как правило, определяется необходимостью исследования конкретных следов совершения преступления (объектов)[73].

При расследовании преступлений в сфере компьютерной информации наиболее характерны судебные компьютерные экспертизы (СКЭ). Прежде всего, это связано с тем, что достаточно часто злоумышленники при совершении преступлений используют компьютеры, ноутбуки, смартфоны, телефоны, различные гаджеты для хранения файлов, которые могут иметь отношение к расследуемому делу; для обмена этими данными и для общения с другими соучастниками компьютерного преступления с использованием различных почтовых клиентов (различные версии Outlook, TheBat!,

[73] Вехов В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки : автореф. дис. …д-ра юрид. наук / В.Б. Вехов. – Волгоград, 2008. // СПС «КонсультантПлюс», 2018.

MozillaThunderbird, KMail и т.д.), приложений для обмена быстрыми сообщениями (ICQ, WhatsApp, Viber, Mail.Ru Агент и т.д.[74]].

Также в борьбе с компьютерными преступлениями используют устройство криминалистического исследования сотовых телефонов «UFED», которое позволяет правоохранительным органам и службам безопасности извлекать важнейшие криминалистические данные из мобильных телефонов, смартфонов и КПК. Особенностями данного устройства являются:

1. Полное извлечение таких данных мобильного телефона, как телефонная книга, текстовые сообщения, фотографии, видеоизображения, журналы звонков (исходящих, входящих, пропущенных), звуковые файлы, ESN, IMEI, ICCID и IMSI и многое другое

2. Клонирование идентификатора SIM-карты Анализ содержимого телефона без каких-либо сетевых операций и необходимости «взламывать» SIM-карту, заблокированную PIN-кодом

3. Возможность извлечения данных из более чем 1700 мобильных телефонов. Поддержка более 1700 моделей мобильных телефонов, включая интеллектуальные устройства Apple iPhone, Symbian, Microsoft Mobile, Blackberry и Palm.

4. Мобильная судебная лаборатория в полевых условиях Портативное, быстрое и удобное в использовании устройство UFED повышенной защищенности работает от мощного аккумуляторного источника; в его комплект входят все принадлежности, необходимые для работы в самых суровых полевых условиях.

Кроме того, для исследования мобильных устройств, извлечения данных из облачных хранилищ и анализа биллингов операторов сотовой связи существует программный комплекс «Мобильный криминалист».

«Мобильный криминалист» позволяет:

[74] Репин М.Е. Преступления в сфере компьютерной информации: проблемы выявления и раскрытия / М.Е. Репин, А.Ю. Афанасьев // Молодой ученый. – 2015. – №15. – С. 461.

1. Извлекать данные из всех популярных моделей мобильных устройств на iOS, Android, BlackBerry, Windows Phone и аппаратов на китайских чипсетах.

2. Импортировать резервные копии устройств, а также их физические образы (JTAG, Chip-off).

3. Получать данные из облачных хранилищ по логину/паролю или токену: iCloud, Google, Microsoft, Email сервер и из других популярных облачных сервисов.

4. Загружать и анализировать биллинги операторов сотовой связи.

5. Извлекать весь набор данных из устройств: контакты, сообщения, звонки, файловую систему, местоположения и удаленную информацию.

6. Находить общие места пребывания нескольких лиц и строить маршруты их передвижения на встроенной оффлайн карте.

7. Выявлять общие связи между несколькими устройствами и устанавливать близкий круг общения пользователя.

8. Просматривать все события в хронологическом порядке и выявлять периоды активности пользователя.

9. Использовать ключевые слова, регулярные выражения и прочие фильтры для быстрого поиска информации.

10. Создавать отчеты в различных форматах (PDF, RTF, XLS, XML).

Судебная компьютерная экспертиза (СКЭ) направлена на получение виртуальной информации, исходя из специфики объекта и предмета ее исследования, поскольку основной формой использования специальных знаний по компьютерным преступлениям является судебная экспертиза[75].

Задачами СКЭ является поиск, обнаружение, анализ и оценка информации, хранящейся на различных устройствах.

Объектами производства СКЭ компьютера или иного устройства, в зависимости от конкретного вида экспертизы, являются:

[75] Нарижный А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий : автореф. дис. ... канд. юрид. наук / А.В. Нарижный. – Краснодар, 2009. – 21 с. // СПС «КонсультантПлюс», 2018.

1. Аппаратные объекты: компьютеры; периферические устройства (сканеры, принтеры, модемы и т.д.); комплектующие для компьютеров; сетевые аппаратные средства (сетевые кабели, серверы и т.д.); интегрированные системы (органайзеры, мобильные телефоны и др.).

2. Программные объекты: системное и прикладное программное обеспечение.

3. Информационные объекты (данные): данные в мультимедийные форматах (аудио - видеофайлы, изображения и т.д.); документы, изготовленные при помощи компьютерных средств; компьютерная информация, содержащаяся в базах данных[76].

Кроме того, что большое количество различной информации о совершенном преступлении в сфере компьютерной информации может содержать мобильный телефон. К ней относятся: звонки, SMS (MMS) – сообщения, различные заметки и напоминания, которые делает для себя владелец данного устройства, информация, хранящаяся в браузере (история, закладки), фото (видео) изображения и др.

На сегодняшний день выделяют следующие виды СКЭ: информационно-технологическую, программно-компьютерную, аппаратно-компьютерную, компьютерно-сетевую.

По делам рассматриваемой категории назначают также некоторые традиционные виды экспертиз: дактилоскопическую, трасологическую, почерковедческую, автороведческую экспертизу документов и др.

Сущность СКЭ состоит в изучении свойств и состояний объектов экспертизы, исследовании механизмов, процессов и действий по результатам использования компьютерного средства в мошенничестве (в том числе компьютерном). При помощи СКЭ можно получить большое количество информации, хранящейся на компьютерных устройствах. Эксперты извлекают не только свободно хранящуюся информацию, но и информацию,

[76] таманов Р.С. Основы методики расследования мошенничества в сети интернет : автореф. дис. … канд. юрид. наук / Р.С Атаманов. – М., 2015. – С. 25.

хранящуюся в зашифрованном виде, а также ту информацию, которая была удалена.

Развитие нанотехнологий и сращивание нейротехнологий с микроэлектроникой, становление психотехнических экспертиз, технологий географических информационных систем (ГИС) в жизнь общества и государства, активное внедрение принципиально отличных от современных технологий, основанных на телекоммуникационных и информационных составляющих, свидетельствуют о важности дальнейшего развития уже существующих и формирования новых направлений судебной компьютерно-технической экспертизы.

В заключение отметим, что для успешной борьбы с компьютерной преступностью наряду с разработкой методического обеспечения производства экспертных исследований необходимо проведение регулярных международных встреч представителей правоохранительных органов. Целью этих встреч, должна быть конкретизация основных направлений данного вида деятельности и обмен опытом, а также взаимодействия по борьбе с международными преступными группами, специализирующихся на преступлениях в области информационных технологий.

# 3 ТЕНДЕНЦИИ РАЗВИТИЯ МЕТОДОВ И СПОСОБОВ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

## 3.1 Мировой опыт борьбы с кибепреступностью

В последнее время, актуализировались проблемы, связанные с преступлениями в сфере информационных технологий. Проблема достигает такого размаха, что выходит за пределы одного государства, и затрагивает интересы не только частных лиц, но и интересы национальной безопасности. Например, можно вспомнить массовую хакерскую атаку 12 мая 2017 года сети российских телекоммуникационных компаний, и баз силовых ведомств[77]. В данном параграфе рассматриваются подходы зарубежных законодателей к ответственности за преступления в информационной сфере. Информационным преступлением считаются преднамеренные умышленные действия, направленные на хищение или разрушение информации в информационных системах и сетях, исходящие из корыстных или хулиганских побуждений. Отметим, так же особенность таких преступлений. В первую очередь такое преступление может совершаться удаленно (даже из другой страны). Во-вторых, чаще всего, объект посягательства представлен в цифровом виде, и в случае кражи или взлома, происходит не хищение объекта в прямом смысле слова а «копирование», т.е. у собственника сохраняется доступ к объекту. Можно выделить несколько подходов по закреплению норм, предусматривающих ответственность за информационные преступления. Первый подход, предусматривает включение таких норм в уголовное законодательство в виде самостоятельных норм, и появления соответствующего раздела, регулирующего данный субинститут. Такой подход нашел свое отражение в законодательстве

[77] Что известно об атаке хакеров на Россию. Н. Кондрашова, А. Вовнякова, И. Рождественский // сайт РБК [Электронный ресурс] URL: http://www.rbc.ru/society/12/05/2017/5915ebf29a794763a8bff785 (дата обращения 03.04.2018).

Испании, Ирландии, Италии, России. Свои особенности имеет законодательство Германии, где нормы касающиеся преступлений в сфере информации, включены в уже существующие нормы, и разделы (в основном в разделе о преступлениях против собственности)[78]. Другой подход, подразумевает принятие отдельных правовых актов (или даже несколько) закрепляющих ответственность за данные правонарушения. Данный подход реализован в США[79], Великобритании[80], Филиппинах[81], Японии[82], т. е как в странах прецедентного, так и в странах континентального права. Кроме того, законодательство США, имеет двухуровневую структуру уголовного законодательства, при этом федеральное законодательство обладает приоритетом над законодательством штатов, поэтому в данной работе рассматривается только федеральное законодательство. Основным федеральным нормативным актом является Свод законов США, но изменения, связанные с определенной тематикой, и новые главы, вводятся актами, имеющими собственные названия. Основным актом, регламентирующим ответственность за злоупотребления с использованием компьютеров в США является так называемый «Computer Fraud and Abuse Act»

(Закон о компьютерном мошенничестве и злоупотреблениях) Свода законов США. Кроме того, в США отдельно подошли к проблеме нарушения авторских прав, с учетом современных технических достижений, приняв «Digital Millennium Copyright Act» (Закон об авторском праве в цифровую

[78] Strafgesetzbuch // Bundesministerium der Justiz und für Verbraucerscutz [Электронный ресурс] URL: https://www.gesetze-im-internet.de/stgb/ (дата обращения 03.04.2018).
[79] Computer Fraud and Abuse Act // U.S. Department of Energy [Электронный ресурс] URL: https://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf (дата обращения 03.04.2018).
[80] Computer Misuse Act 1990 // Legislation.gov.uk [Электронный ресурс] URL: http://www.legislation.gov.uk/ukpga/1990/18 (дата обращения 03.04.2018).
[81] Cybercrime Prevention Act of 2012 // University of the Philippines Los Banos [Электронный ресурс] URL: https://itc.uplb.edu.ph/resources/ictpolicies/republic-act-no-10175-cybercrime-prevention-act-of-2012/ (дата обращения 03.04.2018).
[82] Law Concerning the Prevention of Unauthorized Computer Access // The John Marshall Institutional Repository [Электронный ресурс] URL: http://repository.jmls.edu/cgi/viewcontent.cgi?article=1695&context=jitpl (дата обращения 03.04.2018).

эпоху)[83]. Главной особенностью данного закона, является запрет на разработку технических средств, предназначенных для обхода мер защиты от копирования произведения, охраняемого авторским правом. В Великобритании преступления в сфере информации находятся сразу в нескольких актах, таких как Закон о телекоммуникациях 1997 г. (Telecommunication Act 1997)[84], Закон о защите данных 1998 г. (Data Protection Act 1998)[85] и Закон об электронных коммуникациях 2000 г. (Electronic Communications Act 2000)[86]. Особого рассмотрения требует закон «О злоупотреблении компьютером 1990 г». (Computer Misuse Act 1990), который и закрепляет основные преступления в информационной сфере, меры воздействия, а так же условия привлечения к ответственности по этим преступлениям. В частности, закон отмечает, что если хотя бы одна из частей системы, с помощью которой было совершено компьютерное преступление, находится на территории Великобритании, то преступление признается совершенным на территории Великобритании, и попадает под действие этого закона. Подобная норма встречается нечасто (например, в законодательстве Филиппин), и отчасти расширяет пределы действия законодательства этих стран. В Японии и Нидерландах, информационные преступления нашли свое отражение в уголовном законодательстве, но при этом существуют и отдельные законы. В Нидерландах, это Закон о борьбе с компьютерными преступлениями (Wet computercriminaliteit) от 1995 года[87] и закон «О компьютерной преступности II» (Wet computercriminaliteit II) 2006 года[88], которые дополняют уголовный кодекс новыми составами, вносят коррективы

---

[83] Digital Millennium Copyright Act 1998 // Government Publishing Office [Электронный ресурс] URL: https://www.gpo.gov/fdsys/pkg/PLAW105publ304/pdf/PLAW-105publ304.pdf (дата обращения 03.04.2018).

[84] Telecommunication Act 1997 // Legislation.gov.uk [Электронный ресурс] URL: https://www.legislation.gov.au/Details/C2016C00845 (дата обращения 03.04.2018).

[85] Data Protection Act 1998 // Legislation.gov.uk [Электронный ресурс] URL: http://www.legislation.gov.uk/ukpga/1998/29/contents (дата обращения 03.04.2018).

[86] Electronic Communications Act 2000 // Legislation.gov.uk [Электронный ресурс] URL: http://www.legislation.gov.uk/ukpga/2000/7/contents (дата обращения 03.04.2018).

[87] Wet computercriminaliteit (1995) // Ius mentis [Электронный ресурс] URL:http://www.iusmentis.com/beveiliging/hacken/computercriminaliteit/comp utervredebreuk/ (дата обращения 03.04.2018).

[88] Wet computercriminaliteit II (2006) // Ius mentis [Электронный ресурс] URL: http://www.iusmentis.com/beveiliging/hacken/computercriminaliteit/cybercrime / (дата обращения 03.04.2018).

в уже действующие «традиционные» правовые составы (вымогательство, педофилия, мошенничество), и закрепляют такие понятия как «данные» и «автоматизированная работа». В Японии, уголовный кодекс дополнен законом «О несанкционированном проникновении в компьютерные сети», что обусловлено высокой долей электронного документооборота в Японии (некоторые виды официальных документов существуют только в электронном виде).

Что касается видов преступлений, и тяжести наказаний, то в рассмотренных нами странах есть своя специфика в понимании того, что относится к информационным преступлениям. Нидерланды, четко разделяют преступления на две группы, собственно информационные преступления (взлом) и традиционные составы, преступлений, которые могут быть совершены с использованием информационных технологий (мошенничество, подстрекательство). Это обусловлено рядом причин, например, законодательно предусмотрена максимальная мера пресечения, но не устанавливается минимальная. Кроме того, существует право так называемого «прокурорского усмотрения», когда прокурор решает вопрос о целесообразности преследования за преступления, урон от которых крайне мал. Максимальное наказание за некоторые виды информационных преступлений составляет 1 год, в связи, с чем некоторые исследователи требуют ужесточения наказания. При этом, за традиционные преступления с использование информационных технологий наказание суровее. В США же, наоборот, информационные преступления рассматриваются в самом широком смысле, и включают в себя такие составы как создание вредоносных программ направленных на нарушение авторских прав, шпионаж, мошенничество. В связи с таким подходом, велико и наказание, которое может составлять до 20 лет лишения свободы и штраф. Мошенничество к информационным преступлениям относит и Япония, которая приравнивает к нему в первую очередь внесение в компьютер или сеть используемых для деловых операций записей, о приобретении,

изменении или потере имущественных прав. До 2003 года, в японском законодательстве не предусматривалась уголовная ответственность за информационные преступления, однако рост случаев совершения данного вида преступлений потребовал внесения изменений в действующий УК, и принятия нового закона.

В Великобритании все информационные преступления собраны в два состава: 1) умышленный противозаконный доступ к компьютерным материалам; 2) умышленный противозаконный доступ к компьютерным материалам для их последующего использования в противозаконных целях (с целью совершить какое-либо другое преступление). В рамках этих составов предусмотрены отягощающие и смягчающие обстоятельства, а также объекты на которые может быть направлено деяние. Максимальный срок за подобные правонарушения, составляет 14 лет. В странах, где информационные преступления включены в уголовное законодательство, составы преступлений в целом схожи с уголовным законодательством Российской Федерации. Учитывая все сказанное, можно прийти к следующим выводам:

1) Несмотря на рекомендацию конвенции по киберпреступлениям, на которую ссылается некоторые акты, законодательство большинства стран (в том числе и Россия не подписавшая данную конвенцию) не предусматривает уголовную ответственность за нарушение авторских и смежных прав. При этом, в ряде стран (США, Россия) уголовная ответственность предусмотрена за создание программ, которые могут нанести вред авторским правам.

2) В законодательстве США, Японии, Нидерландов, и ряда других государств прослеживается тенденция к ужесточению наказания за информационные преступления, что вызвано не только ростом числа подобных преступлений, но и увеличением вреда, который они наносят.

3) Нет единого подхода к пониманию того, насколько широко понятие информационного преступления, и входят ли в это понятие

преступления, совершенные с использованием информационных технологий. Наиболее логичным представляется подход Нидерландов, где законодатели четко разграничили информационные преступления и преступления с использованием информационных технологий.

4) Пример Японии показывает, что при развитии электронного документооборота, возможно, потребуется введение дополнительных норм в российское законодательство, предусматривающих наказание за несанкционированный доступ к официальным документам в корыстных или хулиганских целях, а также внесения изменений в такие документы.

## 3.2 Проблемы правоприменительной практики расследования преступлений в сфере использования компьютерной информации и способы их решения на примере

Изучение следственно судебной практики позволил выявить некоторые проблемы, возникающие при расследовании преступлений в сфере информационных технологий, а именно:

1) Длительность (до нескольких месяцев) получения информации, имеющей доказательственное значение по уголовным делам от компаний операторов сотовой связи и финансово-кредитных учреждений (сведений о владельцах сим-карт и банковских карт, движении денежных средств потерпевшего и подозреваемого и др.)[89].

Для решения данной проблемы правоохранительным органам и организациям обладателям информации целесообразно организовывать электронный обмен документами и соответствующими сведениями на основе действующего законодательства и заключённых договоров о сотрудничестве.

[89] Мешков МВ. Гончар В В. Досудебное соглашение о сотрудничестве. проблемы и перспективы // Закон и право. 2014. № 1. С. 93.

2) Использование для совершения преступлений сим-карт и банковских карт, оформленных на других лиц, а также смена преступниками мобильных телефонов и абонентских номеров сим-карт.

Решение этой проблемы видится в усилении контроля за деятельностью операторов связи по распространению сим-карт. Эффективность подобного контроля возрастет с 1 июня 2018 г., когда вступит в силу Федеральный закон от 29 июля 2017 г. № 245-ФЗ «О внесении изменений в Федеральный закон «О связи» в соответствии с которым «... лицо, действующее от имени оператора связи, при заключении договора об оказании услуг подвижной радиотелефонной связи обязано внести в него достоверные сведения об абоненте.. .». Так же оператор связи обязан осуществлять проверку достоверности сведений об абоненте и сведений о пользователях услугами связи абонента - юридического лица либо индивидуального предпринимателя, в том числе представленных лицом, действующим от имени оператора связи, в соответствии с настоящим Федеральным законом и правилами оказания услуг связи.

3) Трудности в определении места совершения преступления, поскольку зачастую похищенные денежные средства зачисляются на несколько лицевых счетов в разных регионах России или иных странах.

При решении данной проблемы целесообразно учитывать позицию Генеральной прокуратуры Российской Федерации, зафиксированную в информационном письме от 3 ноября 2015 г. .№ 36-11-2015 «Об определении места производства предварительного расследования мошенничеств, совершаемых с использованием телефонной (сотовой) связи», в котором указано: «Поскольку преступления рассматриваемого вида нередко имеют трансграничный и высокотехнологичный характер, не позволяющий своевременно установить место их совершения и обеспечить объективное расследование в установленные законом процессуальные сроки, правомерным является признание территориальной подследственности в субъекте Российской Федерации, где непосредственно выполнялись

действия, входящие в объективную сторону преступления, вне зависимости от того, что последствия наступили на другой территории, а также по месту наступления общественно-опасных последствий или обращения потерпевшего в правоохранительные органы»[90].

4) Использование правонарушителями возможностей зарубежных телекоммуникационных компаний и программ, обеспечивающих анонимность в сети «Интернет» (например, ТОК VPN P2P, 1P телефония и т.п.).

Данную проблему, считаем наиболее сложной с технической точки зрения, так как ,по имеющимся сведениям, до настоящего времени исследования по деанонимизации пользователей программ - анонимизаторов не носят «прорывного» характера.

Отдельные правовые основы по ограничению использования анонимайзеров заложены в Федеральном законе от 29 июля 2017 г. № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» (вступит в действие с 1 ноября 2017 г.), согласно которому Роскомнадзор создаст и будет вести Федеральную государственную информационную систему (ФМС), содержащую перечень информационных ресурсов информационно-телекоммуникационных сетей доступ к которым ограничен на территории Российской Федерации.

Кроме того, на основании обращения сотрудников правоохранительных органов Роскомнадзор будет определять провайдера, который допускает размещение в интернете программно-аппаратных средств доступа к запрещенным информационным ресурсам. Такому провайдеру будет направляться электронное уведомление на русском и английском

[90] Новикова Е.А., Волченко А.В. и др. О некоторых вопросах определения территориальной подследственности по преступлениям, связанным с хищением денежных средств путем использования информационно-коммуникационных систем [Электронный РеСУРС] // https://cyberleninka.ru/article/n/o-nekotoryh-voprosah-opredeleniya-territorialnoypodsledst vennosti- po-prestupleniyam- svyazannym-s-hischeniem-denezhnyh-sredstv-putem (дата обращения: 03.04.2018).

языках о необходимости предоставления данных, позволяющих идентифицировать владельца анонимайзера.

5) Недостаточное количество экспертов, имеющих допуск к производству компьютерно-технических судебных экспертиз, значительная длительность их производства, существенная стоимость при проведении в иных учреждениях (до нескольких сотен тысяч рублей за одну экспертизу)[91].

Решить вопрос с подготовкой экспертов необходимого профиля поможет только ориентация ВУЗов на данную деятельность. Конечно, данный подход предусматривает необходимость существенных изменений, как в структуре, так и в организации учебного процесса. Считаю, что достаточно быстрый и положительный результат может дать только взаимодействие ВУЗов с организациями, имеющими определённые достижения в области обеспечения информационной безопасности (например, АО «Лаборатория Касперского», Group-lB)[92].

В контексте рассматриваемого вопроса следует отметить, что исполнение требований закона (ч. 9.1 ст. 182 и ч. 3.1 ст. 183 УПК РФ) об обязательном участии специалиста при изъятии электронных носителей информации отвлекает экспертов от выполнения экспертиз, что влечет увеличение срока расследования.

Одним из способов решения подобной проблемы, может быть привлечение к участию в процессуальных действиях сотрудников не государственных организаций, специализирующихся на информационной безопасности.

В качестве положительного примера можно привести успешное расследование преступления, возбужденного 25 декабря 2015 г. СУ УМВД России по г. С. по признакам преступления, предусмотренного ч. 1 ст. 272 УК РФ в отношении И. и направление материалов в суд, чему способствовало привлечение специалистов местного Интернет-провайдера,

[91] Аналитические материалы СД МВД России за 2017 год.
[92] Мешков М В. Гончар В В. Следователь в уголовном процессе России: понятийно-правовые проблемы // Российский следователь. 2014. .№ 23. С. 19.

которые оказали помощь в установлении IP-адреса и места, с которого обвиняемый, путем подбора пароля, осуществил несанкционированный доступ и временно заблокировал электронный почтовый ящик С.[93].

6) Недостаточные сроки хранения электронной информации в финансово-кредитных учреждениях, у операторов платежных систем и операторов сотовой связи.

Решение данной проблемы видится в реализации положений ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ (в действующей редакции) «О связи», в соответствии с которыми операторы связи обязаны хранить на территории Российской Федерации информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи - в течение трех лет (выделено авт.) с момента окончания осуществления таких действий а текстовые сообщения пользователей услугами связи ,голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи - до шести месяцев (выделено авт.) с момента окончания их приема ,передачи, доставки и (или) обработки.

В этом же законе зафиксировано, что операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, указанную информацию, информацию о пользователях услугами связи и об оказанных им услугах связи и иную информацию, необходимую для выполнения возложенных на эти органы задач.

7) Отсутствие единого подхода в различных субъектах Российской Федерации к квалификации однотипных преступлений данной категории.

Решение данной проблемы видится в принятии Постановления Пленума Верховного Суда Российской Федерации по делам о преступлениях в сфере информационных технологий, подготовке и распространению

[93] Материалы уголовного дела № 214-2016 // Архив УМВД России по Республике Татарстан за 2016 г.

разъяснений Генеральной Прокуратурой Российской Федерации совместно с правоохранительными органами, обеспечивающими расследование подобных преступлений.

В заключении следует отметить, что решение основных проблем возникающих при расследовании преступлений в сфере информационных технологий возможно только при комплексном взаимодействии государственных органов и представителей бизнеса, специализирующихся на вопросах информационной безопасности. Необходимость привлечения таких специалистов для противодействия киберпреступности и в целях обеспечении безопасности киберпространства обусловлена децентрализованной структурой современных информационно-телекоммуникационных сетей и их трансграничным характером. Только обеспечив подобное взаимодействие появится возможность успешно расследовать преступления в сфере информационных технологий, обеспечить информационную безопасность и технологическую независимость России на должном уровне.

# ЗАКЛЮЧЕНИЕ

На основании проведенного исследования основных проблем правоприменительной практики при квалификации преступлений в сфере компьютерной информации в конце работы можно сделать следующие выводы:

1. Настоящее уголовное законодательство Российской Федерации достаточно четко закрепляет ответственность и определяет наказание за совершенные общественно опасные деяния в информационной и компьютерной области, что позволяет сделать следующие выводы:

– Нормы, содержащиеся в статьях 272-273 УК РФ, не включают в себя всю совокупность общественно опасных деяний, характеризующихся как компьютерное преступление;

– Существует пересечение преступлений, где компьютер является лишь орудием совершения преступления и где компьютер рассматривается в качестве совокупности информационных и аппаратных структур[94].

– Это определяет отношение конкретного преступления к определенной статье УК РФ.

2. В компьютерных преступлениях затруднено выделение определенного объекта преступного посягательства. Для разрешения указанных проблем необходимо провести работу над совершенствованием и устранением пробелов в действующем законодательстве, затрагивающем область компьютерных преступлений.

3. Выявление, раскрытие и расследование преступлений в сфере использования компьютерной информации и высоких технологий, по-прежнему остается одной из труднейших задач для уголовного розыска и органов предварительного расследования. Это, безусловно связано с целым рядом проблем, среди которых выделяются такие из них как отсутствие

[94] Кузнецова Г. М. Уголовный кодекс Российской Федерации: Постатейный комментарий – Москва: Изд-во ЗЕРЦАЛО, 2016. С. 328.

должного мониторинга следственной и судебной практики в области киберпреступлений, в целом не значительным опытом работы, подготовкой следователей и сотрудников уголовного розыска, которые ранее не сталкивались с подобными преступлениями, наконец, общая нехватка научно обоснованных и апробированных на практике методических рекомендаций по тактике и методике расследования преступлений в сфере компьютерной информации и высоких технологий.

4. Способы незаконного доступа к компьютерной информации могут быть разнообразными, начиная от представления поддельных документов на право доступа к информации, изменения кода или адреса технического устройства, нарушения средств или системы защиты информации и заканчивая кражей носителя информации.

В целях совершенствования данного института предлагаем следующее:

1. Считаем целесообразным дополнить главу 28 УК РФ статьей 272.1: «Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации». Это обусловлено тем, что преступник, тайно или обманным путем завладев, например, флеш-картой или DVD-диском с компьютерной информацией для последующего ее использования, избегает уголовной ответственности в силу малозначительности совершенного деяния, т.к. стоимость вышеуказанных носителей не превышает тысячи рублей, что влечет в лучшем случае административную ответственность. При этом виновное лицо получает доступ к информации, представляющей большую ценность для ее владельца, чем сам носитель информации».

2. Включить в ст. 273 УК РФ такие преступные действия, как «внесение изменений в существующие программы» и «приобретение компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации». Данный вопрос приобретает

актуальность также в связи с тем, что в последние годы создаются, используются и распространяются уже не отдельные вредоносные программы, а целые семейства компьютерных вирусов, имеющих однотипный компьютерный код. Подавляющие количество киберпреступников для своих противозаконных целей используют программы, купленные у представителей хакерский сообществ. При этом данные вредоносные компьютерные программы наносят не малый вред сообществу.

3. Серьезным пробелом отечественного уголовного законодательства следует также, на наш взгляд, считать отсутствие нормы об уголовной ответственности юридических лиц, в т.ч. за компьютерные преступления.

Дискуссия о необходимости введения в российское законодательство института уголовной ответственности юридических лиц ведется уже несколько десятилетий, и автор солидарен с позицией тех ученых, которые считают, что закрепление уголовно-правовой нормы об ответственности юридических лиц расширило бы правовой инструментарий противодействия российской преступности. Регламентация уголовной ответственности юридических лиц за компьютерные преступления в законодательстве многих зарубежных государств (Австралия, Албания, Бельгия, Великобритания, Венгрия, Дания, Израиль, Индия, Ирландия, Исландия, Канада, КНР, США, Франция и др.) доказывает практическую целесообразность данного шага.

# СПИСОК ЛИТЕРАТУРЫ

## Нормативные правовые акты

1 Дохинская декларация о включении вопросов предупреждения преступности и уголовного правосудия в более широкую повестку для Организации Объединенных Наций в целях решения социальных и экономических проблем и содействия обеспечению верховенства права на национальном и международном уровнях, а также участию общественности // Библиотека криминалиста. – 2015. – № 6. – С. 366–379.

2 Конституция Российской Федерации: (в редакции Закона Российской Федерации о поправке к Конституции Российской Федерации от 21 июля 2014 г. № 11-ФКЗ) // Российская газета. – 1993. – № 237.; Собрание законодательства Российской Федерации. – 2014. – № 31. – Ст. 4398.

3 Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 19 февраля 2018г.) // Собрание законодательства Российской Федерации. – 1996. – № 25 – Ст. 2954.

4 Уголовный процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (в ред. от 19 февраля 2018г.) // Собрание законодательства Российской Федерации. – 2001. – № 52 (ч. I). – Ст. 4921.

5 Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно – розыскной деятельности» (в ред. от 19 февраля 2018г.) // Собрание законодательства Российской Федерации. – 1995. – № 33. – Ст. 3349.

6 Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (в редакции Федерального закона от 6 июля 2016 г. № 374-ФЗ) // Собрание законодательства Российской Федерации. – 2003. – № 28 – Ст. 2895.

7 Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» (в ред. от 19 февраля 2018г.) // Собрание законодательства Российской Федерации – 2006. – № 11. – Ст. 1146.

8 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в редакции

Федерального закона от 6 июля 2016 г. № 374-ФЗ) // Собрание законодательства Российской Федерации. – 2006. – № 31 (ч. I). – Ст. 3448.

9 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (в редакции Федерального закона от 3 июля 2016 г. № 231-ФЗ) // Собрание законодательства Российской Федерации. – 2006. – № 31 (ч. I). – Ст. 3451.

10 Федеральный закон от 22 декабря 2008 г. № 272-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием государственного контроля в сфере частной охранной и детективной деятельности» (в редакции Федерального закона от 3 июля 2016 г. № 227-ФЗ) // Собрание законодательства Российской Федерации. – 2008. – № 52 (ч. I). – Ст. 6227.

11 Федеральный закон от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» (в редакции Федерального закона от 3 июля 2016 г. № 329-ФЗ) // Собрание законодательства Российской Федерации. – 2011. – № 50. – Ст. 7362.

12 Федеральный закон от 29 ноября 2012 г. № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» (в редакции Федерального закона от 3 июля 2016 г. № 325-ФЗ) // Собрание законодательства Российской Федерации. – 2012. – № 49. – Ст. 6752.

13 Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. – 2017. – № 31 (Часть I). – Ст. 4743.

14 Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской

Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (в редакции Указа Президента Российской Федерации от 22 мая 2015 г. № 260) // Собрание законодательства Российской Федерации. – 2008. – № 12. – Ст. 1110.

15 Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Собрание законодательства Российской Федерации. – 2013. – № 3. – Ст. 178.

16 Указ Президента Российской Федерации от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. – 2015. – № 21. – Ст. 3092.

17 Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. – 2016. – № 1 (ч. II). – Ст. 212.

18 Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074.

Специальная литература

19 Айсанов Р. М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: автореф. дис. … канд. юрид. наук. М., 2006. С. 8. // СПС «КонсультантПлюс», 2018.

20 Атаманов Р.С. Основы методики расследования мошенничества в сети интернет : автореф. дис. … канд. юрид. наук / Р.С Атаманов. – М., 2015. – С. 25.

21 Бегишев И. Р. Преступления в сфере обращения цифровой информации / И. Р. Бегишев //Информационное право. – 2015. – № 2. – С. 18–21.

22 Будаковский Д. С. Способы совершения преступлений в сфере компьютерной информации /С. С. Будаковский // Российский следователь. -– 2014. – № 4. – С. 2–4.

23 Быков В. И. Понятие компьютерной информации как объекта преступлений – М.: Законность №12, 2015.– С. 25-29.

24 Вехов В. Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // Уголовное право. 2004. № 4. С. 17. // СПС «КонсультантПлюс», 2018.

25 Вехов В.Б. Криминалистическое учение о компьютерной информации и средствах ее обработки : автореф. дис. …д-ра юрид. наук / В.Б. Вехов. – Волгоград, 2008. // СПС «КонсультантПлюс», 2018.

26 Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международногосотрудничества: монография / А. Г. Волеводз. – М.: Юрлитинформ, 2001. – 496 с. // СПС «КонсультантПлюс», 2018.

27 Гаврилов М., Иванов А. Извлечение и исследование компьютерной информации // Криминалистика. 2014. № 4. С. 74.

28 Галкина У. В. Проблемы возбуждения уголовного дела о незаконном использовании средств индивидуализации товаров (работ, услуг)// Мол. учёный. — 2016. — № 25-1 (129). — С. 14–15.

29 Геллер А. В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета: автореф. дис. … канд. юрид. наук. М., 2006. С. 7. // СПС «КонсультантПлюс», 2018.

30 Герасимова О. С. Особенности преступлений в сфере компьютерной информации // Вестник ТГУ. 2007. № 12. С. 329. // СПС «КонсультантПлюс», 2018.

31 Герке М. Понимание киберпреступности: явление, задачи и законодательный ответ [Электронныйресурс] / М. Герке // Международный

союз электросвязи: [сайт]. [2014]. URL: http://www.itu.int/en/ITU- / Cybersecurity/Documents/Cybercrime2014_R.pdf (дата обращения 03.04.2018).

32 Голубев В. В. Компьютеризация и уголовное право – СанктПетербург: Изд-во Юстицинформ, 2014. С. 27.

33 Гребеньков А. А. Общие подходы к определению понятия «компьютерная информация» в уголовно-правовой теории // Известия Юго-Западного государственного университета. Серия: История и право. 2013. № 1-2. С. 138.

34 Григорьев О. В. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: автореф. дис. … канд. юрид. наук. Омск, 2007. С. 8. // СПС «КонсультантПлюс», 2018.

35 Гузеева О.С. Преступления, совершаемые в российском сегменте сети Интернет: Монография. М.: Академия Генеральной прокуратуры Российской Федерации, 2015. С. 37.

36 Демьянец М. В. Предпринимательская деятельность в сети Интернет: монография / М. В.Демьянец, В. М. Елин, А. К. Жарова. – М.: Юркомпани, 2014. С. 43.

37 Евдокимов К.Н. Проблемы уголовно – правовой квалификации преступлений в сфере компьютерной информации // Вектор науки ТГУ. Серия: Юридические науки. № 4 (19). 2014. С. 33 – 36.

38 Егиазарян Н. А. Преступления против порядка управления в уголовном праве Армении и России(сравнительно-правовое исследование): дис. … канд. юрид. наук: 12.00.08 / Егиазарян Наира Ашотовна. – М., 2013. – 225 с. // СПС «КонсультантПлюс», 2018.

39 Ефремова М. А. Мошенничество с использованием электронной информации / М. А. Ефремова // Информационное право. – 2013. – № 4. – С. 19–21.

40 Ефремова М. А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения / М. А. Ефремова // Право и кибербезопасность. – 2014. – № 2. – С. 33–38.

41 Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис. … канд. юрид. наук. Челябинск, 2010. С. 9. // СПС «КонсультантПлюс», 2018.

42 Иванов Н. А. О понятии «цифровые доказательства» и их месте в общей системе доказательств // Проблемы профилактики и противодействия компьютерным преступлениям: материалы Международной научно-практической конференции (г. Челябинск, 30 мая 2007 г.) и «круглого стола» (г. Челябинск, 18 мая 2007 г.) / отв. ред. А. В. Минбалеев; Челябинский центр по исследованию проблем противодействия организованной преступности и коррупции. Челябинск, 2008. С. 96. // СПС «КонсультантПлюс», 2018.

43 Клепицкий И. А. Система хозяйственных преступлений: монография / И. А. Клепицкий. –М.: Статут, 2005. – 572 с. // СПС «КонсультантПлюс», 2018.

44 Козаев Н.Ш. Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства): Монография. М.: Юрлитинформ, 2015. С. 172.

45 Комаров А. А. О целесообразности использования «кибертерминологии» в исследовании проблемпреступности / А. А. Комаров // Информационное право. – 2016. – № 1. – С. 4–7.

46 Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) / Под ред. С.В. Дьякова, Н.Г. Кадникова. 5-е изд., перераб. и доп. М.: Юриспруденция, 2017. С. 822 - 834.

47 Копырюлин А. Н. Квалификация преступлений в сфере компьютерной информации // Законность. 2017. № 6. С. 40.

48 Крылов В. Информационные преступления – новый криминалистический объект / В. Крылов // Российская юстиция. – 1997. – № 4. – С. 22–23 // СПС «КонсультантПлюс», 2018.

49 Кудрявцев В. Н. Борьба мотивов в преступном поведении: монография / В. Н. Кудрявцев. – М.: Норма, 2007. – 128 с. // СПС «КонсультантПлюс», 2018.

50 Кузнецова Г. М. Уголовный кодекс Российской Федерации: Постатейный комментарий – Москва: Изд-во ЗЕРЦАЛО, 2016. С. 328.

51 Кузнецова Н. Ф. Избранные труды: монография / Н. Ф. Кузнецова; предисл. В. Н. Кудрявцева. – СПб.: Изд-во «Юридический центр Пресс», 2003. – 834 с. // СПС «КонсультантПлюс», 2018.

52 Кургузкина Е. Б., Ратникова Н. Д. Место совершения компьютерных преступлений // Вестник Воронежского института ФСИН России. 2016. № 1. С. 81.

53 Лукьянова А. А. Электронный официальный документ как предмет преступления, предусмотренногост. 327 УК РФ / А. А. Лукьянова // Уголовное право. – 2016. – № 3. – С. 57–62.

54 Маляров А. И. Уголовно-правовые и криминологические аспекты международного сотрудничества в сфере защиты электронно-цифровой информации: автореф. дис. … канд. юрид. наук. Краснодар, 2008. С. 9. // СПС «КонсультантПлюс», 2018.

55 Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) [Электронный ресурс]. Документ опубликован не был. Доступ из справ. -правовой системы «Консультант Плюс».

56 Мешков М В. Гончар В В. Следователь в уголовном процессе России: понятийно-правовые проблемы // Российский следователь. 2014. .№ 23. С. 19.

57 Мешков МВ. Гончар В В. Досудебное соглашение о сотрудничестве. проблемы и перспективы // Закон и право. 2014. № 1. С. 93.

58 Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж : Изд-во Воронеж. гос. ун-та, 2002. С. 46. // СПС «КонсультантПлюс», 2018.

59 Морар И. О. Могут ли в рамках науки криминологии рассматриваться способы совершениякомпьютерных преступлений и их последствия? / И. О. Морар // Российский следователь. – 2014. – № 12. – С. 37–41.

60 Мороз Н. О. Актуальные вопросы международного сотрудничества в борьбе с преступностью всфере высоких технологий в рамках СНГ / Н. О. Мороз // Международное уголовное право и международная юстиция. – 2016. – № 3. – С. 12–14

61 Нагорный А. А. Содержания понятия компьютерной информации как предмета компьютерных преступлений // Актуальные проблемы российского права. 2014. № 8. С. 1697.

62 Нарижный А.В. Использование специальных познаний при выявлении и расследовании преступлений в сфере компьютерной информации и высоких технологий : автореф. дис. ... канд. юрид. наук / А.В. Нарижный. – Краснодар, 2009. – 21 с. // СПС «КонсультантПлюс», 2018.

63 Новикова Е.А., Волченко А.В. и др. О некоторых вопросах определения территориальной подследственности по преступлениям, связанным с хищением денежных средств путем использования информационно-коммуникационных систем [Электронный РеСУРС] // https://cyberleninka.ru/article/n/o-nekotoryh-voprosah-opredeleniya-territorialnoypodsledst vennosti- po-prestupleniyam- svyazannym-s-hischeniem-denezhnyh-sredstv-putem (дата обращения: 03.04.2018).

64 Онлайн-газета Ведомости. Официальный сайт. // [Электронный ресурс]. — Режим доступа:// https://www.vedomosti.ru/technology/articles/ 2016/10/13/660728-hakeri-ukrali-android (дата обращения: 03.04 2018).

65 Осипенко А. Уголовная ответственность за неправомерный доступ к конфиденциальной компьютерной информации // Уголовное право. 2014. № 3. С. 43-37.

66 Основные направления противодействия транснациональному организованному криминальному наркобизнесу: монография / Л. Драпкин, Р.

Вафин, Я. Злоченко и др.; под общ. ред. И. И. Ищенко. – М.: ЛексЭст, 2003. – 424 с. // СПС «КонсультантПлюс», 2018.

67 Практикум по уголовному праву России / Под ред. проф. Ф.Р. Сундурова, М.В. Талан, И.А. Тарханова. – М.: Статут, 2014.

68 Расследование неправомерного доступа к компьютерной информации / Под ред. Н. Г. Шурухнова. М.: Щит-М, 1999. С. 70. // СПС «КонсультантПлюс», 2018.

69 Рассолов И. М. Право и Интернет. Теоретические проблемы / И. М. Рассолов. – 2-е изд.,доп. – М.: Норма, 2009. – 384 с.// СПС «КонсультантПлюс», 2018.

70 Репин М.Е. Преступления в сфере компьютерной информации: проблемы выявления и раскрытия / М.Е. Репин, А.Ю. Афанасьев // Молодой ученый. – 2015. – №15. – С. 461.

71 Решетников А.Ю. Квалификация неоконченных преступлений при наличии признаков совокупности преступлений // Вестник Академии Генеральной прокуратуры Российской Федерации. 2016. N 4. С. 85.

72 Решетников А.Ю., Русскевич Е.А. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) // Законы России: опыт, анализ, практика. 2018. N 2. С. 51 - 55.

73 Романова Л. И. Наркопреступность: криминологическая и уголовно-правовая характеристика: учеб. метод. пособие / Л. И. Романова. – 2-е изд. – Владивосток: Изд-во Дальневосточного ун-та, 2009. – 314 с. // СПС «КонсультантПлюс», 2018.

74 Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: Учебное пособие. М.: ИНФРА-М, 2017. С. 44.

75 Сафонов О. М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы

совершенствования: дис. ... канд. юрид. наук: 12.00.08 / Сафонов Олег Михайлович. – М., 2015. С. 12.

76 Сивицкая Н. А. К вопросу об определении понятия «компьютерная информация» // Проблемы правовой информатизации. 2005. № 2. С. 35. // СПС «КонсультантПлюс», 2018.

77 Сизов А. В. Неправомерный доступ к компьютерной информации: практика правоприменения // Информационное право. 2014. № 1. С. 32-35.

78 Смагин П. Г. О понятии «компьютерной информации» и особенностях ее использования при расследовании преступлений в ОВД // Вестник Воронежского института МВД России. 2008. № 1. С. 80. // СПС «КонсультантПлюс», 2018.

79 Смолин С. Уголовно-правовая борьба с высокотехнологичными способами и средствами совершения преступлений / С. Смолин // Уголовное право. – 2014. – № 4. – С. 62–68.

80 Старичков М. В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. 2014. № 1. С. 20.

81 Статистика «Страны с самым большим процентом компьютерных преступлений в сфере «пиратства»» [Электронный ресурс]. – Режим доступа: http://statistic.su/blog/countries_with_pirate_soft/2011-09-12-394

82 Степанов-Егиянц В. Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями / В. Г. Степанов-Егиянц // Российский следователь. – 2013. – № 24. – С. 43–46.

83 Тер-Акопов А. А. Преступление и проблемы нефизической причинности в уголовном праве: монография / А. А. Тер-Акопов. – М.: «Юркнига», 2003. – 480 с. // СПС «КонсультантПлюс», 2018.

84 Титарева Е. Г. Мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий // Научный альманах. 2015. № 7. С. 1160.

85 Третьяк М. И. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий / М. И. Третьяк // Законность. – 2016. – № 7. – С. 41–46.

86 Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия на появляющиеся формы преступности, такие как киберпреступность и незаконные оборот культурных ценностей, в том числе извлеченные уроки и международное сотрудничество. Справочный документ семинара- практикума. Электронный ресурс] / United Nations Office on Drugs and Crime: [сайт]. [2015]. URL: A/CONF.222/12 [Электронный ресурс] // http://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_r_V1500665.pdf (дата обращения 03.04.2018).

87 Халиуллин А. И. Подходы к определению киберпреступления / А. И. Халиуллин // Российский следователь. – 2015. – № 1. – С. 34–39.

88 Хилюта В. В. Правовая информатизация и уголовный закон // Проблемы правовой информатизации. 2007. № 1. С. 76. // СПС «КонсультантПлюс», 2018.

89 Хисамова З. И. Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий / З. И. Хисамова // Юридический мир. – 2016. – № 2. – С. 58–62.

90 Центр исследования компьютерной преступности. Официальный сайт. //[Электронный ресурс] Режим доступа:// http://www.crime-research.ru (дата обращения: 03.04 2018).

91 Чекунов И. Г. Понятие и отличительные особенности киберпреступности / И. Г. Чекунов // Российский следователь. – 2014. – № 18. – С. 53–56.

92 Чекунов И. Г. Современные киберугрозы. Уголовно-правовая и криминологическая классификация и квалификация киберпреступлений / И. Г. Чекунов // Право и кибербезопасность. – 2013. – № 1. – С. 9–22.

93 Черкасов В. Н. Информационные технологии и организованная преступность [Электронный ресурс] /В. Н. Черкасов // Саратовский Центр по

исследованию проблем организованной преступности и коррупции: [сайт]. [2014]. URL: http://sartraccc.ru/Pub/cherkasov%2824-03%29.htm (дата обращения 03.04.2018).

94 Что известно об атаке хакеров на Россию. Н. Кондрашова, А. Вовнякова, И. Рождественский // сайт РБК [Электронный ресурс] URL: http://www.rbc.ru/society/12/05/2017/5915ebf29a794763a8bff785 (дата обращения 03.04.2018).

95 Широков В. А., Беспалова Е. В. Компьютерные преступления: основные тенденции развития / В. А. Широков, Е. В. Беспалова // Юрист. – 2006. – № 10. – С. 18–21 // СПС «КонсультантПлюс», 2018.

96 Щепетильников В. Н. Уголовно-правовая охрана электронной информации: автореф. дис. … канд. юрид. наук. Елец, 2006. С. 7. // СПС «КонсультантПлюс», 2018.

97 Юрченко И. А. Информация конфиденциального характера как предмет уголовно-правовой охраны: автореф. дис. … канд. юрид. наук. М., 2000. С. 12. // СПС «КонсультантПлюс», 2018.

98 Янин С.А. Организация первоначального этапа расследования незаконного сбыта наркотических средств и психотропных веществ // Организация деятельности органов предварительного следствия и дознания в системе МВД России: управленческие и криминалистические проблемы: Сб. материалов Всероссийской научно-практической конференции: В 2 ч. М.: Академия управления МВД России, 2012. Ч. 1. С. 271 //СПС «КонсультантПлюс», 2018.

99 Comprehensive Study on Cybercrimes [Электронный ресурс] / United Nations Office on Drugs and Crime: [сайт]. [2013]. URL: http://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf (дата обращения 03.04.2018).

100 Computer Fraud and Abuse Act // U.S. Department of Energy [Электронный ресурс] URL:

https://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf (дата обращения 03.04.2018).

101 Computer Misuse Act 1990 // Legislation.gov.uk [Электронный ресурс] URL: http://www.legislation.gov.uk/ukpga/1990/18 (дата обращения 03.04.2018).

102 Cybercrime Prevention Act of 2012 // University of the Philippines Los Banos [Электронный ресурс] URL: https://itc.uplb.edu.ph/resources/ictpolicies/republic-act-no-10175-cybercrime-prevention-act-of-2012/ (дата обращения 03.04.2018).

103 Data Protection Act 1998 // Legislation.gov.uk [Электронный ресурс] URL: http://www.legislation.gov.uk/ukpga/1998/29/contents (дата обращения 03.04.2018).

104 Digital Millennium Copyright Act 1998 // Government Publishing Office [Электронный ресурс] URL: https://www.gpo.gov/fdsys/pkg/PLAW105publ304/pdf/PLAW-105publ304.pdf (дата обращения 03.04.2018).

105 Electronic Communications Act 2000 // Legislation.gov.uk [Электронный ресурс] URL: http://www.legislation.gov.uk/ukpga/2000/7/contents (дата обращения 03.04.2018).

106 Law Concerning the Prevention of Unauthorized Computer Access // The John Marshall Institutional Repository [Электронный ресурс] URL: http://repository.jmls.edu/cgi/viewcontent.cgi?article=1695&context=jitpl (дата обращения 03.04.2018).

107 Strafgesetzbuch // Bundesministerium der Justiz und für Verbraucerscutz [Электронный ресурс] URL: https://www.gesetze-im-internet.de/stgb/ (дата обращения 03.04.2018).

108 Telecommunication Act 1997 // Legislation.gov.uk [Электронный ресурс] URL: https://www.legislation.gov.au/Details/C2016C00845 (дата обращения 03.04.2018).

109 Wet computercriminaliteit (1995) // Ius mentis [Электронный ресурс] URL:http://www.iusmentis.com/beveiliging/hacken/computercriminaliteit/computervredebreuk/ (дата обращения 03.04.2018).

110 Wet computercriminaliteit II (2006) // Ius mentis [Электронный ресурс] URL: http://www.iusmentis.com/beveiliging/hacken/computercriminaliteit/cybercrime / (дата обращения 03.04.2018).

Материалы судебной и иной практики

111 Приговор Чистопольского городского суда Республики Татарстан от 4 мая 2012 г. по уголовному делу № 1-80/12. [Электронный ресурс]. – URL: https://rospravosudie.com/court-chistopolskij-gorodskoj-sud-respublika-tatarstan-s/act-104673919/ (дата обращения: 16.01.2017).

112 Приговор Авиастроительного районного суда г. Казани Республики Татарстан от 17 апреля 2012 г. по уголовному делу № 90/12. [Электронный ресурс]. – URL: https://rospravosudie.com/court-aviastroitelnyj-rajonnyj-sud-g-kazanirespublika-tatarstan-s/act-105043335/ (дата обращения: 16.01.2017).

113 Приговор Набережночелнинского городского суда Республики Татарстан от 13 октября 2010 г. по уголовному делу № 1-1487/10. [Электронный ресурс]. – URL: https://rospravosudie.com/court-naberezhnochelninskij-gorodskoj-sudrespublika-tatarstan-s/act-106458840/ (дата обращения: 16.01.2017).

114 Материалы уголовного дела № 214-2016 // Архив УМВД России по Республике Татарстан за 2016 г.

115 Официальный сайт МВД РФ. // [Электронный ресурс]. — Режим доступа: https://мвд.рф (дата обращения: 03.04 2018).

116 Аналитические материалы СД МВД России за 2017 год.

117 Преступления в сфере компьютерной информации. Сводный отчет по России за январь - декабрь 2017 г. URL: https://mvd.ru (дата обращения: 03.04.2018).

# ПРИЛОЖЕНИЯ

Приложение 1

Сведения о зарегистрированных в Российской Федерации преступлениях в сфере компьютерной информации

| Годы | 2011 | 2012 | 2013 | 2014 | 2014 | 2016 | 2017 |
|---|---|---|---|---|---|---|---|
| Количество зарегистрированных преступлений | 7398 | 2698 | 2820 | 2563 | 1739 | 2382 | 1748 |

Приложение 2

Сведения о зарегистрированных в Российской Федерации преступлениях в сфере компьютерной информации по статьям УК РФ

| **Статья УК РФ** | **2012** | **2013** | **2014** | **2015** | **2016** |
|---|---|---|---|---|---|
| 159.6 УК РФ | 43 | 693 | 995 | 5443 | 4329 |
| 272 УК РФ | 6309 | 2005 | 1930 | 1799 | 1151 |
| 273 УК РФ | 1089 | 693 | 889 | 764 | 585 |
| 274 УК РФ | 0 | 0 | 1 | 0 | 3 |

АНТИПЛАГИАТ
ТВОРИТЕ СОБСТВЕННЫМ УМОМ

**УВАЖАЕМЫЙ ПОЛЬЗОВАТЕЛЬ!**

Обращаем ваше внимание, что система «Антиплагиат» отвечает на вопрос, является ли тот или иной фрагмент текста заимствованным или нет. Ответ на вопрос, является ли заимствованный фрагмент именно плагиатом, а не законной цитатой, система оставляет на ваше усмотрение. Данный отчет не подлежит использованию в коммерческих целях.

# Отчет о проверке на заимствования №1

**Автор:** Каримов Адель Миннурович karimov485@mail.ru / ID: 59
**Проверяющий:** Каримов Адель Миннурович (karimov485@mail.ru / ID: 59)
**Организация:** Казанский юридический институт МВД России

Отчет предоставлен сервисом «Антиплагиат»- http://кюи.ап.мвд.рф

## ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 4
Начало загрузки: 18.04.2018 09:32:10
Длительность загрузки: 00:01:22
Имя исходного файла: Диплом. Преступления в сфере использования компьютерной информации
Размер текста: 422 кБ
Символов в тексте: 113422
Слов в тексте: 12946
Число предложений: 1140

## ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 18.04.2018 09:33:33
Длительность проверки: 00:00:23
Комментарии: не указано
Модули поиска: Модуль поиска ЭБС "БиблиоРоссика", Модуль поиска ЭБС "BOOK.ru", Коллекция РГБ, Цитирование, Модуль поиска ЭБС "Университетская библиотека онлайн", Коллекция eLIBRARY.RU, Коллекция ГАРАНТ, Модуль поиска ЭБС "Айбукс", Модуль поиска Интернет, Модуль поиска "КЮИ МВД РФ", Модуль поиска ЭБС "Лань", Кольцо вузов

| ЗАИМСТВОВАНИЯ | ЦИТИРОВАНИЯ | ОРИГИНАЛЬНОСТЬ |
|---|---|---|
| 31,14% | 6,42% | 62,44% |

| № | Доля в отчете | Доля в тексте | Источник | Ссылка | Актуален на | Модуль поиска | Блоков в отчете | Блоков в тексте |
|---|---|---|---|---|---|---|---|---|
| [01] | 7,27% | 7,94% | СОВЕРШЕНСТВОВАНИЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕН... | http://elibrary.ru | 15 Фев 2018 | Коллекция eLIBRARY.RU | 11 | 24 |
| [02] | 0,91% | 5,83% | ВКР В.doc | не указано | 18 Авг 2016 | Кольцо вузов | 11 | 46 |
| [03] | 2,99% | 5,73% | 08_04_16_МХГильмутдинов_ДЗЮЧ-111.Р.doc.docx | не указано | 08 Апр 2016 | Кольцо вузов | 22 | 56 |
| [04] | 3,62% | 5,55% | 224920 | http://biblioclub.ru | раньше 2011 | Модуль поиска ЭБС "Университетская библиотека онлайн" | 76 | 109 |
| [05] | 0,3% | 5,32% | Глухов Н.А. 08-306 | не указано | 29 Мая 2017 | Кольцо вузов | 6 | 55 |
| [06] | 0,46% | 4,91% | ДИПЛОМ.docx | не указано | 25 Авг 2016 | Кольцо вузов | 9 | 65 |

**Отзыв**
о ходе выполнения выпускной квалификационной работы слушателя 032 учебной группы

Романовой Екатерины Владимировны

на тему: «Преступления в сфере использования компьютерной информации: основные проблемы правоприменительной практики»

Тема выпускной квалификационной работы является весьма актуальной. Рост информационных технологий в России, как и во всем мире, обусловил расширение сфер применения высоких технологий, платной дистрибуции контента, мобильных платежей, интернет банкинга в предпринимательской деятельности и в повседневной жизни. При этом быстрое развитие таких технологий создает предпосылки для их использования в преступных целях. Одновременно с количеством пользователей увеличивается как число потенциальных жертв, так и возможность использовать сеть Интернет для совершения противоправных деяний. При этом анонимность глобальных информационных сетей и быстрота передачи информации позволяют использовать все эти преимущества для совершения преступлений, которые нередко именуются киберпреступлениями. Эти проблемы носят сложный, многоаспектный характер, что обусловило выбор структуры выпускной квалификационной работы, которая состоит из введения, 3 – х взаимосвязанных разделов (глав), поделенных на 7 параграфов, заключения и списка использованных источников

К положительным сторонам выпускной квалификационной работы следует отнести комплексный анализ решения обозначенных в исследовании проблем, требующих совершенствования законодательство, методики выявления, раскрытия и расследования преступлений, совершаемых в сфере использования компьютерной информации, повышения эффективности взаимодействия министерств, ведомств, других государственных органов, организаций по совместной борьбе с кибепреступностью.

За время исследовательской работы Романова Е.В. проявила себя как ответственный слушатель. Она постоянно стремилась повысить свой профессиональный уровень, активно использовала различные философские общенаучные и частнонаучные методы исследования.

Данная работа содержит некоторые недостатки, например небольшой объем провоприминительной практики по РТ, которая является одним из «передовых» регионов, способных активно противодействовать

преступлениям совершаемым в информационной сфере. Данные недостатки являются несущественными и не влияют на общую оценку выпускной квалификационной работы.

Романова Е.В. показала умение анализировать и систематизировать полученную информацию, а также делать самостоятельные выводы, умозаключения, предложения и обобщения.

Выпускная квалификационная работа слушателя выполнена в соответствии с рекомендациями и требованиями по оформлению выпускных квалификационных работ вузов. В работе есть комплексность, логичность изложения материала, актуальность и новизна. Изложенный в исследовании текст полностью соответствует поставленным задачам.

При выполнении выпускной квалификационной работы слушатель обоснованно и аргументировано использовал информационные ресурсы, справочно-правовые системы, прикладное программное обеспечение ,технологии, необходимые для решения поставленных в работе задач с учетом современных требований и подходов к борьбе с спреступлениями в сфере использования компьютерной информации.

В достаточной степени использованы теоретические и нормативные источники по теме выпускной квалификационной работы.

Выпускная квалификационная работа в полной мере может быть допущена к защите с высокой положительной оценкой.

преподаватель кафедры экономики, финансового права
и информационных технологий в ОВД
майор полиции А.М. Каримов

**РЕЦЕНЗИЯ**
на выпускную квалификационную работы
слушателя 032 учебной группы
Романовой Екатерины Владимировны

на тему: Преступления в сфере использования компьютерной информации: основные проблемы правоприменительной практики.

Тема представленной выпускной квалификационной работы, несомненно, одна из актуальных, так как в современном мире информация является самым ценным глобальным ресурсом. Информация постоянно усложняется, меняется качественно, растет количество ее источников и потребителей. В то же время растет уязвимость современного информационного общества от недостоверной (а иногда и вредной) информации, ее несвоевременного поступления, промышленного шпионажа, преступлений в сфере использования компьютерных сетей. Количество преступлений, совершаемых в сфере компьютерной информации и высоких технологий, увеличивается соразмерно росту пользователей компьютерных сетей. Об этом, в частности, свидетельствуют отдельные электронные ресурсы, разработанные правительствами некоторых стран мира для приема заявлений граждан на преступления, совершенные в телекоммуникационной сети «интернет».

Изучив содержание рецензируемой работы, можно сделать вывод о том, что заявленная тема в целом раскрыта. Вопросы темы рассмотрены автором достаточно полно. Достигнута обозначенная во введении цель работы, которая заключается в исследовании особенностей совершения преступлений в сфере использования компьютерной информации, их предупреждения, выявлению, раскрытия и расследования.

В работе анализируются международное и российское законодательство, правоприменительная практика, приводятся авторские предложения по разрешению обозначенных в исследовании проблем.

Выполненное исследование может иметь как теоретическое, так и практическое значение. Результаты исследования могут быть использованы в законотворческой и правоприменительной деятельности правоохранительных

Выполненное исследование может иметь как теоретическое, так и практическое значение. Результаты исследования могут быть использованы в законотворческой и правоприменительной деятельности правоохранительных органов, а так же в дальнейших научных исследованиях по рассмотренной проблематике.

В целом работа Романовой Е.В. производит благоприятное впечатление и заслуживает положительной оценки.

В качестве замечания автору следовало использовать больше статистических данных однако данные замечания являются не существенным и не повлияло на качество работы в целом.

В соответствии с вышеизложенным, выпускная квалификационная работа Романовой Е.В. соответствует предъявленным требованиям и может быть допущена к защите.

Рецензент

Начальник ОП № 10 в УМВД России по г. Кемерово — Коганов В.Н.

(место работы, занимаемая должность, ученая степень, ученое звание) — подпись — (инициалы,фамилия)

«10» января 2017 г.