Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультетюридический
Кафедра уголовного права
Направление подготовки 40.03.01 – Юриспруденция

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ Т.Б. Чердакова
«_____»_____2017 г.

БАКАЛАВРСКАЯ РАБОТА

на тему:Преступления в сфере информационных технологий

Исполнитель
студент группы 321 сб3 _____ С.В. Синишин
(подпись, дата)

Руководитель
канд.юрид.наук, доцент _____ Т.Б. Чердакова
(подпись, дата)

Нормоконтроль _____ О.В. Громова
(подпись, дата)

Благовещенск 2017

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет юридический
Кафедра уголовного права

УТВЕРЖДАЮ
Зав. кафедрой
_____ Т.Б. Чердакова
«_____»_____2017 г.

З А Д А Н И Е

К выпускной квалификационной работе студента 321 сб 3 группы Синишина С.В.

1. Тема выпускной квалификационной работы: Преступления в сфере информационных технологий
(утверждена приказом от 10.01.2017 № 04-уч)
2. Срок сдачи студентом законченнойработы 20 января 2017
3. Исходные данные к выпускной квалификационной работе:получены от руководителя выпускной квалификационной работы Чердаковой Т. Б.
4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов):анализ преступлений в сфере высоких информационных технологий и выявление основных проблем в работе правоохранительных органов при расследовании таких преступлений.
5. Перечень материалов приложения: (наличие чертежей, таблиц, графиков, схем, программных продуктов, иллюстративного материала и т.п.) приложение отсутствует.
6. Консультанты по выпускной квалификационной работе (с указанием относящихся к ним разделов)
консультант по проблемам уголовного преследования в сфере высоких информационных технологий начальник отделения УР УМВД России по Амурской области Сорокин О.В.
7. Дата выдачи задания15 ноября 2016

Руководитель выпускной квалификационной работы:Чердакова Татьяна Борисовна,зав. кафедройуголовного права,кандидат юридических наук, доцент

Задание принял к исполнению (дата): 15 ноября 2016

РЕФЕРАТ

Бакалаврская работа содержит 63 с., 52 источника

КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ, НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ,КИБЕРШАНТАЖ, МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ,УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ

Целью данной бакалаврской работы является анализ преступлений в сфере высоких информационных технологий и выявление основных проблем в работе правоохранительных органов при расследовании преступлений в сфере высоких информационных технологий. Объектом исследования являются общественные отношения, возникающие в процессе установления и реализации уголовной ответственности за правонарушения в сфере высоких информационных технологий.

Предметом исследования выступает уголовно-правовая характеристика преступлений в сфере высоких информационных отношений.

Методологической основой исследования являются диалектический метод научного познания и системный подход. В целях получения достоверных результатов при решении поставленных выше задач использовались как общенаучный метод познания, так и частно-научные, и специальные методы: исторический, формально-юридический, логико-юридический, сравнительно-правовой, системно-структурный, статистический, а также анализ документов и материалов практики.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Информационные технологии, на современном этапе, это не только новые возможности для развития всех отраслей жизни общества, но и серьезная государственная проблема, имеющая большое социальное и политическое значение не только внутри страны, но и на международной арене.

Если 10 лет назад компьютер был еще «роскошью», то сейчас он есть практически в каждом доме, а представить себе офис, организацию, рабочее место специалиста без компьютера не возможно. Согласно официальной статистике опубликованной на сайте Федеральной службы государственной статистики[1] число персональных компьютеров в организациях в 2005 года составляло 5709,6 тыс. шт., а на конец 2015 года это уже 11992,3 тыс. шт. Из них в 2015 году доступ к глобальной информационной сети у 8362 тыс. шт., тогда как в 2005 это было лишь 2032 тыс. шт. Тоже самое можно сказать о распространении других технических средств информационных технологий: мобильные телефоны, смартфоны, планшетные устройства. По итогам мониторинга российского рынка персональных компьютеров проведенного международной исследовательской и консалтинговой компанией IDC приобретение настольных персональных компьютеров в третьем квартале 2016 года сократилось на 30,6% относительно прошлого года, из мониторинга видно, что потребители стали отдавать предпочтение мобильным форм-факторам(http://idcrussia.com/ru/).

Широкое распространение персональных компьютеров, мобильных телефонов, планшетных устройств, свободный доступ к всемирной системе объединённых компьютерных сетей «Интернет» и быстро развивающиеся компьютерные технологии породили новый видпреступлений – преступления в сфере высоких информационных технологий. Компьютерная информация и возможности ее использования в настоящее время представляют большую ценность не

[1]Информационное общество // Федеральная служба государственной статистики: офиц. сайт.[Электронный ресурс]URL:https://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/science_and_innovations/it_technology/# (дата обращения: 05.01.2017).

только для ее обладателя, но и для третьих лиц. В виду этого преступники осваивают новые знания и технологии для осуществления противоправных действий, как в хулиганских целях, так и в целях завладения чужим имуществом. Так же «компьютерные преступления» представляют серьезную угрозу государству в целом, государственной безопасности. Еще в 1999 году Председатель Правительства Российской Федерации В.Путин подписал Распоряжение главная цель которого усиление борьбы с преступлениями в сфере высоких технологий. А 15 января 2013 года Президент Российской Федерации в целях обеспечения информационной безопасности Российской Федерации подписал указ № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»[2].

Указом Президента РФ от 05.12.2016 №646«Об утверждении Доктрины информационной безопасности Российской Федерации»[3] стратегической целью обеспечения информационной безопасности в области обороны страны названа защита жизненно важных интересов личности, общества и государства.

Быстрое развитие информационных технологий, их совершенствование, появление новых устройств, способов обмена информацией затрудняет борьбу правоохранительных органов с рассматриваемыми преступлениями, успех деятельности правоохранительных органов во многом зависит от технической оснащенности и подготовленности специалистов в сфере высоких информационных технологий.

Все указанные выше факторы и обуславливают в совокупности актуальность теоретического и научно-прикладного исследования юридической природы, оснований и мер уголовной ответственности за преступления, совершаемые в сфере высоких информационных технологий.

Проблемы осуществления уголовного преследования по делам о преступ-

[2] О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [Электронный ресурс] Указ Президента РФ от 15.01.2013 № 31с. Доступ из справ.- правовой системы «Гарант».

[3] Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс] Указ Президента РФ от 05.12.2016 № 646. Доступ из справ.- правовой системы «Гарант».

лениях, совершаемых в сфере высоких информационных технологий постоянно находятся в центре внимания ученых-юристов. Понятие компьютерной информации рассматривалось различными авторами: В.Быковым, А.С.Маленкиным, А.И.Халиулиным, В.Черкасовым, А.А.Энгельгард.

Проблемы уголовного преследования были рассмотрены Ю.С. Кауфман, Н.П.Кириловой, С.П.Кушниренко, А.А.Несмеяновым, М.Третьяк, В.В.Хилюта.

Условно-цифровое вымогательство было предметом исследования Т.М.Лопатиной. Вопросы деятельности правоохранительных органов в борьбе с преступлениями в сфере высоких информационных технологии рассматривались в работах Ю.В.Белянинова, О.А.Васильева, А.П.Киселева, А.А.Топоркова, В.В.Шаповалова, Г.М.Шаповаловой, Е.С.Шевченко и др.

Целью данной выпускной квалификационной работы является анализ преступлений в сфере высоких информационных технологий и выявление основных проблем в работе правоохранительных органов при расследовании преступлений в сфере высоких информационных технологий.

Для достижения указанной цели необходимо решить следующие задачи:

– дать общую характеристику преступлений предусмотренных главой 28 Уголовного Кодекса Российской Федерации;

– проанализировать уголовно-правовую характеристику мошенничества в сфере компьютерной информации;

– рассмотретьусловно-цифровое вымогательство или кибершантаж, как преступное деяние;

– конкретизировать и проанализировать правовую основу деятельности правоохранительных органов в борьбе с преступлениями в сфере высоких информационных технологии;

– рассмотреть проблемы выявления преступлений в сфере высоких информационных технологий и особенности тактики следственных действий.

Объектом исследования являются общественные отношения, возникающие при совершении преступления в сфере высоких информационных отношений.

Предметом исследования выступает ответственность за преступления в сфере высоких информационных технологий.

Методологической основой исследования являются диалектический метод научного познания и системный подход. В целях получения достоверных результатов при решении поставленных выше задач использовались как общенаучный метод познания, так и частно-научные, и специальные методы: исторический, формально-юридический, логико-юридический, сравнительно-правовой, системно-структурный, статистический, а также анализ документов и материалов практики.

Эмпирическую базу исследования составят материалы, отражающие обусловленные темой работы результаты правоприменительной деятельности органов МВД, практика судов, данные полученные из аналитической информации УМВД России по Амурской области.

Теоретическую основу исследования составят труды отечественных ученых в области юридической ответственности преступления в сфере высоких информационных отношений, а также публикации в периодической печати, посвященные проблемам преступлений в сфере высоких информационных отношений.

1 ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙПРЕДУСМОТРЕННЫХ ГЛАВОЙ 28 УК РФ

1.1 Неправомерный доступ к компьютерной информации

С появлением современных способов хранения, накопления и обработки информациипоявились и новые способы раскрытия, уничтожения, изменения информации. В то же время, стало необходимым защищать компьютерную информацию не только посредствам предотвращения утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, но и в правовом поле. Уголовный кодекс содержит отдельную главу 28 «Преступления в сфере компьютерной безопасности», которая содержит 3 состава преступлений направленных против общественной безопасности и общественного порядка.

Рассмотрение главы 28 УК РФначнем со статьи 272, устанавливающей уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации.

Понятие доступ к компьютерной информации законодатель закрепил в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Федеральный закон № 149-ФЗ) определив «доступ к компьютерной информации»как возможность получения информации и её использования.У любой информации есть обладатель, то есть лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (статья 2 Федерального закона № 149-ФЗ)[4]. В статье 272 УК РФ законодатель говорит о несанкционированномвоздействии на информационную систему или информационно-телекоммуникационную сеть, то есть неправомерном доступе к компьютерной информации.

Так, 15 июня 2016 года промышленный районный суд г. Владикавказа

[4] Об информации, информационных технологиях и о защите информации [Электронный ресурс] Федеральный закон от 27.07.2006 № 149-ФЗ. Доступ из справ.- правовой системы «Гарант».

Республики Северная Осетия – Алания, установил, что гражданин И.с помощью мобильного телефона осуществил неправомерный доступ к охраняемой законом компьютерной информации, а именно, вопреки воли гражданина Ш. вошёл на принадлежащую ему личную страницу в социальной сети «ВКонтакте» с именем профиля «Д. ...» после чего изменил пароль для входа, поменял статус пользователя, написав «Я террорист смертник и взорву жд Техникум в понедельник!!! ИнШаАллагъ я буду в раю», поменял фотографию профиля и удалил знакомых гражданина Ш. из числа друзей.[5]

Используемый в диспозиции анализируемой статьи термин «охраняемая законом» свидетельствует о том, что уголовное законодательство берет под свою охрану совокупность общественных отношений по правомерному и безопасному использованию не любой компьютерной информации, а только той, которая находится под защитой закона. Охраняемая законом компьютерная информация – это информация ограниченного доступа, имеющая не только специальный правовой статус, но и предназначенная для ограниченного круга лиц (пользователей), имеющих право на ознакомление с ней.

Защищена ли информация, а также способы защиты информации не являются обязательным условиемдля того чтобы охранять данную информацию. Таким образом, защита информации не обязанность ее владельца и закон должен охранять данную информацию от посягательства вне зависимости от ее защищенности.[6]

«Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства» – гласит статья 9 Федерального закона № 149-ФЗ.[7]

Порядок предоставления информации или ее распространения определяет

[5] Государственная автоматизированная системаРоссийской Федерации «Правосудие»: офиц. сайт.[Электронный ресурс]URL: https://bsr.sudrf.ru/bigs/portal.html (дата обращения: 09.01.2017).

[6] Степанов-Егиянц В. Содержание термина «неправомерный доступ к компьютерной информации» в уголовном праве// Право и экономика.2014. №8. С.44.

[7] Об информации, информационных технологиях и о защите информации [Электронный ресурс] Федеральный закон от 27.07.2006 № 149-ФЗ. Доступ из справ.- правовой системы «Гарант».

4 группы информации:

– информацию, свободно распространяемую;

– информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

– информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

– информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Указом Президента РФ от 6.03.1997 № 188[8] был утвержден Перечень сведений конфиденциального характера, куда вошли:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами от 20.04.1995№45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов»[9] и от 20.08.2004№119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»[10], другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

3. Служебные сведения, доступ к которым ограничен органами государ-

[8] Об утверждении перечня сведений конфиденциального характера [Электронный ресурс] указ Президента РФ от 06.03.1997 № 188. Доступ из справ.- правовой системы «Гарант».

[9] О государственной защите судей, должностных лиц правоохранительных и контролирующих органов [Электронный ресурс] Федеральный закон от 20.04.1995 № 45-ФЗ. Доступ из справ.- правовой системы «Гарант».

[10] О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства [Электронный ресурс] Федеральный закон от 20.08.2004 № 119-ФЗ. Доступ из справ.- правовой системы «Гарант».

ственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2.10.2007 № 229-ФЗ «Об исполнительном производстве»[11].

В соответствии с примечанием к анализируемой статье под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Закон не раскрывает содержание таких категорий, как средства хранения, обработки и передачи компьютерной информации.

К средствам хранения, обработки и передачи компьютерной информации следует относить все машинные носители информации, то есть технические средства (комплекс технических средств), предназначенные для фиксации, хранения, обработки, анализа и передачи компьютерной информации пользователем. К машинным носителям информации можно, например, отнести магнитные диски, CD, DVD, BD, жесткие диски (винчестер), а также флэш-карты и др.

[11] Об исполнительном производстве [Электронный ресурс] Федеральный закон от 2.10.2007 № 229-ФЗ.Доступ из справ.- правовой системы «Гарант».

К устройствам хранения информации относятся и оперативная память, кэш-память, CMOS-память, BIOS.

Средством хранения, обработки и передачи компьютерной информации выступают также информационно-телекоммуникационные сети, то есть технологические системы, предназначенные для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

С объективной стороны преступление, предусмотренное ч.1 ст.272 УК РФ, выражается в неправомерном (противоречащем закону или иному нормативному акту) доступе к компьютерной информации.

Так в Постановлении Президиума Свердловского областного суда от 30.09.2009 указано, что неправомерный доступ к информации, означает несанкционированное проникновение, взлом электронной системы защиты этой информации.[12]

Способы неправомерного доступа к компьютерной информации могут бытьсамыми разнообразными и, как правило, не влияют на юридическую оценку поведения виновного лица. Например, соединение с компьютером, подключенным к телефонной сети, путем автоматического перебора абонентских номеров (внедрение в чужую информационную систему посредством «угадывания кода»), использование чужого имени (пароля), использование ошибки в логике построения программы или провоцирование ошибок соединения, выявление слабых мест в защите автоматизированных систем (взлом системы защиты), считывание информации с компьютера после окончания его работы («уборка мусора») и др.

Курганский городской суд, рассмотрев в открытом судебном заседании уголовное дело в отношении В., обвиняемого в совершении двух преступлений, предусмотренныхч. 2 ст. 272 УК РФ, а также преступлений, предусмотренных ч.3ст. 30, ч. 2 ст. 159, п. «в» ч. 2 ст. 158 УК РФ, установил, что В. находясь в

[12] Степанов-Егиянц В. Содержание термина «неправомерный доступ к компьютерной информации» в уголовном праве// Право и экономика.2014. №8. С.44.

здании ПАО «Сбербанк России» нашел на столе у компьютера двабумажныхфискальных чека, оставленных ранее незнакомой ему Ф., на которых содержалась информация о номере ее банковской карты, логин и пароль, с помощью которых можно было получить доступ к лицевому счету данной банковской карты и информацию о денежных средствах, находящихся на данном лицевом счете и остальных счетах (вкладах).Далее,воспользовавшисьинформацией, которая имелась в указанных чеках, получил доступ к лицевому счету банковской карты и вкладу и перевел со счета вклада на лицевой счет банковской карты Ф. денежные средства.После чего, поочередно ввел в диалоговое окно на официальном сайте ПАО «Сбербанк России» короткие текстовые уведомления с указанием сумм, в результате чего денежные средства, принадлежащие Ф., были зачислены на лицевой счет банковской карты И., находящейся в это время в пользовании В., вследствие чего последний получил реальную возможность распоряжаться данными денежными средствами по своему усмотрению.[13]

Состав преступления материальный.[14] Преступление считается оконченным с момента наступления хотя бы одного из альтернативно перечисленных в диспозиции ч.1 ст. 272 УК РФ последствий: уничтожения, блокирования, модификации либо копирования компьютерной информации.

Из этого вытекает, что обязательным признаком объективной стороны преступления является и причинная связь между действиями лица, заключающимися в неправомерном доступе к компьютерной информации, и наступившими вредными последствиями, прямо указаннымив диспозиции статьи. Если уничтожение, блокирование, модификация либо копирование информации не являлось следствием неправомерного доступа к компьютерной информации, а выступало результатом иной деятельности виновного, то состав преступления, предусмотренный комментируемой статьей, отсутствует.

Субъектом основного состава преступления является физическое и вме-

[13]Государственная автоматизированная системаРоссийской Федерации «Правосудие»: офиц. сайт.[Электронный ресурс]URL: https://bsr.sudrf.ru/bigs/portal.html (дата обращения: 09.01.2017).

[14] ЛысакЕ.А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ. 2013. №90. С. 20

няемое лицо, достигшее к моменту преступной деятельности шестнадцатилетнего возраста и не наделенное в силу характера выполняемой работы полномочиями доступа.

Если говорить о субъективной стороне, то нужно говорить об осознаваемых действиях, направленных непосредственно науничтожение, блокирование, модификацию, копирование компьютерной информации, то есть об умышленной форме вины. Профессор кафедры уголовного права, уголовного процесса и криминалистики МГИМО А.Г.Волеводз считает, что косвенный умысел и неосторожная форма вины могут иметь место только по отношению к наступлению вредных последствий неправомерного доступа, предусмотренных диспозицией данной нормы уголовного закона.[15]

Мотивы, подтолкнувшие лицо на неправомерный доступ к охраняемой законом информации, как и цели умышленных действий лица различные – от корыстных до хулиганства.Но, не смотря на то, что мотивы и цели совершения неправомерного доступа к информации не влияют на квалификацию установление их все же обязательно. Выяснение причин необходимо для назначения справедливого наказания, ведь законодатель предоставляет выбор наказания за преступления, предусмотренные рассматриваемой статьей от штрафа вразмере до двухсот тысяч рублейилив размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев,либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишение свободы на срок до 2-х лет.

Более суровая уголовная ответственность предусмотрена, если деяние причинило крупный ущерб или совершено из корыстной заинтересованности(ч. 2 ст. 272 УК РФ).Понятие крупного ущерба в рамках главы 28 УК РФ законодателем закреплено в примечаниях к рассматриваемой статье.

Когда уничтожение,блокирование, модификация, копирова-

[15] Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М. Изд-во «Юрлитинформ». 2001. 496 с.

ниекомпьютерной информации было осуществлено группой лиц, действующих по предварительному сговору, организованной группой или лицом, использовавшим своё служебное положение, а также если перечисленные действия повлекли тяжкие последствия или угрозу наступления таковых, то это является особо квалифицирующими признаками состава преступления.

Даже если действия, перечисленные в ч.1 ст. 272 УК РФ, были совершены другими лицами, но лицо, использовавшее своё служебное положение, предоставило этим лицам сведения, позволяющие осуществить неправомерный доступ к информации, например посредством логина и пароля, и это привело к уничтожению,блокированию, модификации, копированиюкомпьютерной информации третьих лиц, то действия лица предоставившего сведения квалифицируются по ч.3 ст. 272 УК РФ.

Если говорить о тяжких последствиях в рамках данной статьи то это может быть крупная авария, остановка производства, вызванная неправомерным вмешательством в работу автоматизированных систем или же причинение смерти по неосторожности.

В качестве общих выводов можно отметить следующее.Предметом преступления, предусмотренного ст.272 УК РФ, является охраняемая законом компьютерная информация, при этом законодатель не ставит охрану информации в зависимость от применения обладателем средств ее технической защиты.

Под доступом к компьютерной информации следует понимать получение возможности обращения к компьютерной информации, в результате которого лицо получает правомочия обладателя информации. Признаком неправомерного доступа к компьютерной информации, является отсутствие соответствующего разрешения со стороны обладателя.

1.2 Статья 273. Создание, использование и распространение вредоносных компьютерных программ

Следующая статья главы 28 УК РФ предусматривает уголовную ответственность за создание, использование и распространение вредоносных компьютерных программ.

Внешним признаком преступления предусмотренного статьей 273 УК РФ, его проявлением является создание, использование и распространение компьютерных программ.Цель данных программ – уничтожение, блокирование, модификация, копирование компьютерной информации обладателем которой лицо, совершившее перечисленные действия не является, а так же нейтрализация средств защиты компьютерной информации.

Под вредоносными программами в смысле комментируемой статьи понимаются программы, специально созданные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, что определено в документации на программу.

В наше время даже человек не связанный с компьютерами, имеет представление о том, что такое вирус и называет вирусом любую вредоносную программу для компьютера, что не совсем правильно, так как вирусы являются только частью вредоносного программного обеспечения. Сегодня количество известных вирусов не поддается строгому учету и постоянно увеличивается. По приблизительным оценкам специалистов, ведущих борьбу с вредоносными программами, в среднем ежедневно появляется около 30 новых вирусов.

Существует три больших группы вредоносных программ, а именно: троянские программы, сетевые черви и непосредственно вирусы.

Наиболее «безобидными» являются сетевые черви. Сетевой червь – вредоносный программный код, распространяющий свои копии по сети с целью проникновения на компьютер-жертву, запуска своей копии на этом компьютере и дальнейшего распространения. Большинство червей распространяются в файлах, которые содержат код червя, и, в свою очередь, распространяются через E-mail, ICQ, и т.д. Как только пользователь сохраняет на компьютере зараженный файл, полученный, к примеру, с помощью e-mail, червь попадает на компьютер, и начинает искать путь дальнейшего распространения, например, может самостоятельно разослать свои копии по всем адресам, обнару-

женным в почтовом ящике, некоторые черви способны автоматически отвечать на полученные письма.

Троянская программа – это вредоносный код, совершающий несанкционированные пользователем действия, например кража информации, уничтожение или модификация информации и.т.д. Существует несколько типов троянских программ. Лаборатория Евгения Касперского выделяет следующие: троянские утилиты удаленного администрирования (бакдоры), похитители паролей, интернет-кликеры, загрузчики, установщики, троянские прокси-серверы, шпионские программы, архивные бомбы и другие.[16]Наиболее опасными из них являются так называемые бакдоры, обладатель (хозяин) которых может без ведома пользователя осуществлять различные операции с зараженным компьютером, начиная с выключения компьютера до всевозможных операций с файлами. Достаточно интересным типом троянской программы является так называемая архивная бомба. При попытке архиватора обработать архив, программа вызывает нестандартные действия архиватора, что приводит к существенному замедлению работы компьютера, либо к его зависанию. Одновременно с этим на компьютере может быть создано огромное количество одинаковых файлов. При этом размер самой бомбы невелик, так 10 Гб повторяющихся данных умещаются в 500 Кб RAR-архиве.

Непосредственно вирусы делятся на три типа: перезаписывающие вирусы, паразитирующие вирусы и вирусы – компаньоны. Перезаписывающие вирусы заменяют код файла своим кодом, в результате чего файл перестает работать. Восстановить зараженный таким образом файл невозможно. Паразитирующие вирусы изменяют содержимое файла, но при этом оставляют его работоспособным. Вирусы-компаньоны создают копию файла, при этом код файла-жертвы не изменяется. Обычно вирус изменяет расширение файла (например, с .exe на .com), потом создает свою копию с именем, идентичным имени файла-жертвы, и дает ему расширение, тоже идентичное. Ничего не подозревающий

[16] Коцыняк М.А., Коцыняк М.М., Лаута О.С., Лаута А.С. Киберустойчивость информационно-телекоммуникационной сети. // Информационные технологии, связь и защита информации МВД РОССИИ. 2015, С. 104.

пользователь запускает любимую программу и не подозревает, что это вирус. Вирус, в свою очередь, заражает еще несколько файлов и запускает программу, затребованную пользователем.

Если говорить о форме вины, то в рассматриваемом составе преступления деяние совершается только с умыслом и только действием. То есть вредоносная программа появляется в результате осознанной деятельности, направленной на создание программывлекущейнарушенияработыинформационно-телекоммуникационных сетей или уничтожение, блокирование, модификацию, копирование информации.

Использование компьютерных программ это тоже действиенаправленное уже на применение, воспроизведение таких программ.

ПриговоромПервомайскогорайонногосудаОренбургскойобластиЕ. и О.осуждены за совершение преступлений, предусмотренных ч.2 ст. 159.6, ч.2 ст. 273 УК РФ.[17]Последнее было совершено при следующих обстоятельствах. Е. и О., обладая достаточными познаниями в области компьютерной техники и навыками работы в сети Интернет, вступили между собой в предварительный преступный сговор, с целью личного обогащения и хищения чужого имущества путём обмана неограниченного круга лиц среди пользователей сети Интернет, а также блокирования компьютерной информации и иного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации.

В осуществление своего преступного умысла, используя персональный компьютер, создали в сети Интернет сайты, в стартовый файл которых интегрировали вредоносные скрипты (программы),достоверно зная, что, с помощью указанных скриптов, осуществляется блокирование функций операционной системы и иное вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации персональных компьютеров. Посетителям таких сайтов приходят рассылки якобыот имени МВДРФ, Управле-

[17] Государственная автоматизированная системаРоссийской Федерации «Правосудие»: офиц. сайт. [Электронный ресурс]URL: https://bsr.sudrf.ru/bigs/portal.html (дата обращения: 09.01.2017).

ния МВД РФ, Интерпола, содержащие сведения о необходимости перечисления денежных средств на абонентские номера, в качестве оплаты наложенного на пользователя сети Интернет административного штрафа за просмотр, хранение и распространение материалов порнографического содержания.Таким образом, Е. и О.осуществили блокирование функций операционной системы и иное вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации персональных компьютеров.

Распространение программ – это предоставление доступа к воспроизведенной в любой материальной форме компьютерной программе, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы для любой из этих целей. Одним из самых типичных способов распространения вредоносных программ является их размещение на различных сайтах и страничках информационно-телекоммуникационной сети Интернет.

Данный состав является формальным и не требует наступления каких-либо последствий, уголовная ответственность возникает уже в результате создания, использования или распространения программы, независимо от того, наступили лив результате этого какие-либо общественно опасные последствия.

Советским районным судом г. Иваново был осужден И. за совершение преступления, предусмотренного ч.1 ст.273 УК РФ.Преступление совершено в г.Иваново при следующих обстоятельствах.[18]В 2015 годуИ. осуществил загрузку с Интернет-сайта вредоносной компьютерной программы, предназначенной для несанкционированного уничтожения, блокирования, модификации, компьютерной информации и нейтрализации средств защиты компьютерной информации. После этого И. не менее одного раза осуществил запуск вредоносной компьютерной программы, инициировал действие указанной программы по поиску в сети Интернет сайтов, которые содержат различные уязвимости. По окончании поиска сайтов, содержащих уязвимости, И. с помощью вредоносной

[18] Советский районный суд города Иванова: офиц. сайт. [Электронный ресурс]URL:https://http://sovetsky.iwn.sudrf.ru/ (дата обращения: 09.01.2017).

компьютерной программы осуществил попытки доступа к выбранным Интернет-ресурсам с использованием найденных уязвимостей. Затем, переустановил операционную систему, в результате чего вредоносная компьютерная программа была удалена.

Оконченным рассматриваемый вид преступлений считается с момента окончания создания вредоносной программы. То есть с того момента, когда программа будет способна принести вред компьютеру. Уголовная ответственность, при наличии достаточной доказательственной базы, может наступить и за попытку создания вируса, т.е. за неоконченное преступление.

Мичуринским городским судом Д. была осуждена за совершение преступлений, предусмотренных ч.2 ст.146 УК РФ, ч.1 ст.273 УК РФ.[19] Вышестоящей инстанцией данный приговор был изменен, поскольку действия Д. по распространению компьютерных программ заведомо предназначенных для несанкционированного блокирования, модификации компьютерной информации, ошибочно были квалифицированы, как оконченное преступление. Компьютерные программы были изъяты в ходе оперативно-розыскного мероприятия, в результате чего преступление не было доведено до конца по независящим от осужденной обстоятельствам, в связи с чем, действия Д. были переквалифицированы по данному эпизоду на ч.3 ст.30 ч.1 ст.273 УК РФ.

Субъектом данного преступления может быть любое вменяемое лицо, достигшее 16 лет.

Говоря о субъективной стороне преступления необходимо еще раз подчеркнуть, что вина в форме прямого умысла, то есть виновный осознавал общественную опасность своих действий, предвидел возможность либо неизбежность наступления опасных последствий.Ведь создание вредоносных программ возможно только при наличии специальных знаний и умений, а следовательно и наличия знания последствия применения этих программ.А вот если лицо, перенаправляя электронное письмо с вложенным файлом или передавая диск, где

[19] Судебная практика рассмотрения уголовных дел о преступлениях в сфере компьютерной информации // Железнодорожный районный суд города Барнаула Алтайского края.[Электронный ресурс]URL: http://zheleznodorozhny.alt.sudrf.ru. (дата обращения: 09.01.2017).

содержится вредоносная программа, не знало об этом, то в рассматриваемых случаях не будет состава преступления предусмотренного статьей 273 УК РФ.

Квалифицирующие признаки статьи 273 УК схожи со статьей 272 УК РФ и включают в себя совершение деяния группой лиц по предварительному сговору или организованной группой, лицом с использованием своего служебного положения, а так же причинение крупного ущерба или корыстную заинтересованность. И, так же как и ст. 272 УК ч.3 ст. 273 УК РФ предусматривает ужесточение наказания за деяния, если они повлекли тяжкие последствия или создали угрозу их наступления.Это может быть причинение смерти по неосторожности, например, если вредоносную программу направить на блокирование информационных систем учреждения здравоохранения, а это привело к отключению системы жизнеобеспечения пациента. Но если лицо умышленно запустило вредоносную программу для отключения системы жизнеобеспечения, то это 105 статья УК РФ – убийство.

Подводя итог, можно сделать следующие основные выводы.

Состав рассматриваемого преступления содержит только деяние – создание, распространение, использование вредоносных программ и тем самым является формальным. То есть преступление считается оконченным да же если создание, распространение и использование вредоносных программ не вызвало последствий в виде несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Но уголовная ответственность наступает лишь в том случае, когда лицо умышленно хотело создать вредоносную программу или умышлено ее распространяло и использовало.

Анализ судебной практики показывает, что наиболее часто в суде рассматриваются дела по статье 273 УК РФ, когда целью создания, использования и распространения вредоносных компьютерных программ является незаконное использование объектов авторского права, приобретение, хранение контрафактных экземпляров произведений в целях сбыта.

1.3 Статья 274. Нарушение правил эксплуатации средств хранения,

обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

«21 век – век информационных технологий» это не просто громкая фраза, не только характеристика современного этапа истории, но реальность практически каждого человека. Сложно представить современного человека без компьютера, мобильного телефона, планшета и т.д. Но информационные технологии применяются не только в развлекательных целях, а так же в строительстве, медицине, промышленности и др. И поэтомунарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетямможет привести к катастрофическим последствиям.

В статье 274 УК РФ законодатель установил уголовную ответственность за действия, названные выше, но только при условии, что эти действия привели к уничтожению, блокированию, модификации, копированию компьютерной информации, причинили крупный ущерб.

С развитием электронно-вычислительной техники постоянно в обращение вводятся все новые технические средства, на которых может находиться компьютерная информация. Машинные носители, к которым относят всякого рода магнитные диски, компьютерные схемы и др., классифицируются в зависимости от их физических и конструктивныхособенностей.[20]

Компьютерная информация может также содержаться в памяти компьютера, которая реализуется через перечисленные машинные носители, используемые как запоминающие устройства – внешние (например, флеш-память, CD или DVD диски, память телефона, смартфона, айпеда и пр.) или внутренние, включенные в конструкцию компьютера.[21]

Компьютерная информация может передаваться по телекоммуникационным каналам из одного компьютера в другой, из компьютера на устройства

[20] Быков В., Черкасов В. Новая редакция ст.274 УК // Законность. 2012. № 11. С.25.
[21] Там же. С.25.

отображения, из компьютера на управляющие датчики оборудования.

Таким образом, эта норма ч. 1 ст. 274 УК РФ оберегает компьютерную информацию, где бы она ни содержалась и как бы не циркулировала. Объективную сторону рассматриваемого преступления образуют нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям.

Особенностью данной статьи, отличающей ее от ст. 272 и 273 УК РФ, является то, что диспозиция рассматриваемой статьи бланкетная, не содержащая определенного правилаэксплуатации или правил доступа к информационно-телекоммуникационным сетям. Законодатель отсылает правоприменителяк нормативным правовым актам, а также к инструкциям, регламентам и правилам, установленным для конкретного оборудования или действующих в определенной организации. Так, например Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»[22]регулирует, в том числе, и отношенияв сфере эксплуатации всех сетей связи и сооружений связи.

Выше уже было сказано, что уголовная ответственность наступает только в случае, если нарушение правил привело к уничтожению, блокированию, модификации, копированию компьютерной информации. Но стоит отметить, что нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационныхсетей влечет за собой уголовную ответственность по ст. 274 УК РФтолько если в результате уничтожения, блокирования, модификации, копирования компьютерной информации был причинён крупный ущерб. Напомним, что в рамках главы 28 УК РФ крупный ущерб – это ущерб, сумма которого превышает один миллион рублей.

Рассматривая ст. 272 УК РФ и ст. 273 УК РФ мы говорили об умышлен-

[22] О связи [Электронный ресурс] Федеральный закон от 07.07.2003 № 126-ФЗ. Доступ из справ.- правовой системы «Гарант».

ных деяниях, а вот действия, попадающие под ст. 274 УК РФ, могут быть совершены как в форме прямого умысла, так и по неосторожности.Лицо предвидит уничтожение, блокирование, модификацию либо копирование компьютерной информации в результате нарушения им правил эксплуатации, но без достаточных к тому оснований самонадеянно рассчитывает на предотвращение последствий. Либо не предвидит указанных в законе последствий, хотя при необходимой внимательности и предусмотрительности должно было и могло предвидеть.

Так же замечается отличие и в субъекте – это вменяемое лицо, достигшее возраста 16 лет, то есть обладающее общими признаками. Но привлечь к уголовной ответственности по ст. 274 УК РФ можно лишь лицо имеющее доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию, в том числе к информационно-телекоммуникационным сетям, а также оно должно быть обязано соблюдать установленные правила эксплуатации.А в ст. 272 УК РФ лицо, осуществляет неправомерный доступ к охраняемой законом информации, то есть действует не санкционированно. Таким образом, субъект преступления ст. 274 УК РФ только специальный.

Органами предварительного следствия было установлено, что А. на основании трудового договора работал и занимал должность ведущего системного администратора отдела технической поддержки.[23] СА.было заключено соглашение о сохранении служебной и коммерческой тайны, которое обязывает сотрудника не разглашать сведения, содержащие служебную тайну, какому-либо лицу и подчиняться правилам, существующим на предприятии, и указаниям должностныхлиц, направленных на защиту служебной тайны.Согласно должностной инструкции,ведущий системный администратор поддерживает в рабочем состоянии программное обеспечение рабочих станций и серверов, обеспечивает своевременное копирование, архивирование и резервирование данных,

[23] Государственная автоматизированная системаРоссийской Федерации «Правосудие»: офиц. сайт. [Электронный ресурс]URL: https://bsr.sudrf.ru/bigs/portal.html (дата обращения 09.01.2017).

обеспечивает сетевую безопасность, сохраняет конфиденциальность служебной информации.

А., находясь на своем рабочем месте, используя средства авторизации (логин и пароль), и имея, в силу исполняемых обязанностей, доступ к информационным носителям, на которых содержится охраняемая компьютерная информация, скопировал на USB носитель информацию из базы данных, а именно: не менее 40.000 записей, содержащих не прошедших проверку имен, фамилий, никнеймов (имена, которые используются при регистрации на интернет сайтах), а так же адресов электронной почты.

Часть 1 статьи 274 УК РФ устанавливает широкий набор различных видов уголовного наказания. Лицо, осужденное по этой статье может быть наказано штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

Такой широкий набор различных видов наказания позволяет суду с учетом содеянного и личности виновного индивидуализировать наказание.

Таким образом, глава 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации» входит в состав Раздела IX «Преступления против общественной безопасности и общественного порядка» и содержит три статьи: ст.272– неправомерный доступ к компьютерной информации; ст.273– создание, использование и распространение вредоносных программ; ст.274– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Законодатель устанавливает, что в указанных статьях общим для всех трех составов объектом преступления являются общественные отношения, связанные с посягательством накомпьютерную информацию. Компьютерная информация, о которой идет речь в главе 28 УК РФ, это только разновидность информации, о которой

говорится в Федеральном законе № 149-ФЗ[24]. Эту компьютерную информацию защищает уголовный кодекс.В составах преступлений, предусмотренных в ст. 272-274 УК РФ, указаны следующие альтернативные общественно опасные последствия: уничтожение, модификация, блокирование, копирование компьютерной информации или нейтрализация средств защиты компьютерной информации. Последнее общественно опасное последствие представлено только в ст. 273 УК РФ, остальные же являются типовыми для всех указанных статей.

Диспозиции статей 28-й главы описательные, зачастую – бланкетные или отсылочные. Для их применения необходимо обратиться к Федеральному закону № 149-ФЗ, к различным правилам эксплуатации, инструкциям и т. п. Санкции – альтернативные, за исключением двух квалифицированных составов, где они – в силу тяжести последствий преступления относительно – определены. Таким образом, при применении статей 28-главы УК РФ необходимо знание не только норм уголовного права и законов в сфере информации, других нормативных правовых актов регулирующих отношения в сфере информации, а также знание документов не носящих нормативный характер. В связи с этим при применении санкций важно учитывать мнение специалистов, знающих порядок, условия, специфику работы в области информационных технологий.

[24] Об информации, информационных технологиях и о защите информации [Электронный ресурс] Федеральный закон от 27.07.2006 № 149-ФЗ. Доступ из справ.- правовой системы «Гарант».

2 УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

2.1 Мошенничество в сфере компьютерной информации

Согласно данным Федеральной службы государственной статистики население, использовавшее сеть Интернет в процентном соотношении к общей численности населения в возрасте от 15 до 72 лет в 2013 году составило 64 %, в 2015 году эта цифра выросла до 70,1 %, и лишь 22, 3 % никогда не использовали интернет, тогда как в 2013 году это было 28,6 %., число подключенных терминалов сотовой связи на 100 человек населения на конец 2015 года – 193,8 штук, в 2005 году это было всего 86,3 штук.[25] Таким образом, развитие высоких технологий, расширение сфер и способов их применения, в том числе распространение использования сети Интернет делает их доступными для населения и тем самым увеличивает аудиторию интернета, число пользователей сотовой связью и все больше лиц осваивают возможности информационных технологий.

Одним из способов применения информационных технологий оказалось мошенничество, в связи, с чем в 2012 году законодатель дополнил главу 21 УК РФ ст. 159.6 «Мошенничество в сфере компьютерной информации» (Федеральный закон от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»). До введения ст.159.6 УК РФ борьба с компьютерными преступлениями велась в рамках главы 28 УК РФ.

И так рассмотрим, что же такое мошенничество в сфере компьютерной информации и чем оно отличается от «традиционного» мошенничества.

Объект ст. 159.6 УК РФ не отличается от других статей главы 21 и им являются общественные отношения, связанные с отношениями собственности, независимо от ее формы.

[25] Информационное общество // Федеральная служба государственной статистики: офиц. сайт.[Электронный ресурс] URL:https://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/science_and_innova-tions/it_technology/# (дата обращения 05.01.2017).

Объективная сторона преступления, предусмотренного рассматриваемой статьей, представляет собой хищение либо приобретение права на чужое имущество, которое осуществляется путем различных действий как технического, так и интеллектуального характера.

Уголовно-наказуемыми являются лишь следующие способы завладения имуществом:

– ввод компьютерной информации;

– удаление компьютерной информации;

– блокирование компьютерной информации;

– модификация компьютерной информации;

– вмешательство в функционирование средств хранения, средств обработки, средств передачи компьютерной информации, информационно-телекоммуникационные сети. Под вмешательством в функционирование следует понимать осуществление неправомерных действий, нарушающих установленный процесс обработки, хранения, использования, передачи и иного обращения с компьютерной информацией.

Статья 159.6 УК РФ выделяет два действия, которыми может быть совершено мошенничество в сфере компьютерной информации: хищение чужого имущества или приобретение права на чужое имущество.

В постановлении пленума верховного суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» указанно, что в соответствии с законом под хищением следует понимать противоправное безвозмездное изъятие имущества, с причинением ущерба владельцу.

Под приобретением права на чужое имущество в судебной практике понимается возникновение у виновного лица возможности вступить во владение, пользоваться или распоряжаться чужим имуществом как своим собственным.Безверхов А.Г. в статье «Мошенничество и его виды: вопросы законодательной регламентации и квалификации»[26] считает, что в силу системности су-

[26] Безверхов А.Г. Мошенничество и его виды: вопросы законодательной регламентации и квалификации) // Уголовное право. 2015. №5. С. 10.

дебного толкования уместно использование разъяснений постановления Пленума Верховного Суда РФ от 9.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях»[27] применительно к соответствующим положениям ст. 159.6 УК РФ.А именно, понятие имущественного права разъяснено в абз. 3 п. 9 указанного постановления, согласно которому имущественные права включают в свой состав как право на имущество, в том числе право требования кредитора, так и иные права, имеющие денежное выражение, например исключительное право на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации.Незаконное предоставление виновному имущественных прав предполагает возникновение у этого лица юридически закрепленной возможности вступить во владение или распорядиться чужим имуществом как своим собственным, требовать от должника исполнения в его пользу имущественных обязательств и др.[28]Безверхов А.Г. полагает, что к имущественным правам следует относить безналичные денежные средства, так как по своей юридической (гражданско-правовой) природе безналичные деньги являются не вещами, а правами требования, их гражданско-правовой режим как объектовобязательственных, а не вещных прав исключает возможность их отождествления с вещами[29].

Такимобразом,предмет мошенничества – это чужое имущество и право на чужое имущество. А вот дополнительным предметом преступления рассматриваемого в рамках требований ст.159.6 УК РФ выступает компьютерная информация, ведь именно с ее использованием и происходит обман и завладение чужим имуществом или правом на него.

То есть исходя из требований ст. 159.6 УК РФ если виновный совершил действия, приведшие к завладению имуществом или правом на него без использования компьютерной информации (понятие компьютерной информации

[27] О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях [Электронный ресурс]Постановление Пленума Верховного Суда РФ от 9.07.2013 № 24. Доступ из справ.- правовой системы «Гарант».

[28] БезверховА.Г.Мошенничество и его виды: вопросы законодательной регламентации и квалификации)//Уголовное право. 2015. № 5. С. 10

[29] Там же. С.11

мы рассматривали в главе 1), а равно если он не преследовал цель завладеть имуществом, а лишь, к примеру, хотел ограничить, блокировать доступ владельца к имуществу, то тогда нельзя применять указанную статью.

Детальное сравнение мошенничества в сфере компьютерной информации с другими формами хищений, предусмотренных главой 21 УК РФ, показывает, что виновный не делает это тайно, не полагается на силу или угрозы, а с помощью обмана, злоупотребления доверием потерпевший сам передает свое имущество. Можно сказать практически добровольно.

Так в сентябре 2016 года в дежурную часть города Благовещенска, поступило сообщение от Б. по факту совершения в отношении него мошеннических действий.

В ходе проведения проверки установлено, следующее. Б. дал объявление на сайте «Avito.ru» о продаже надувной лодки стоимостью 7000 рублей, указав свой номер телефона. К его номеру телефона подключен «мобильный банк». 01 сентября 2016 года Б. позвонил мужчина с намерением приобрести лодку, сообщив, что оплату ему проще осуществить переводом денежных средств на банковскую карту. Б. отправил предполагаемому покупателю смс-сообщение с номером его банковской карты. Предполагаемый покупатель сообщил Б. что будет отправлять ему деньги в сумме 7000 рублей, и Б. должно прийти смс-сообщение с кодом, который необходимо назвать ему, Б. назвал ему код. После указанных действий с карты Б. были сняты деньги в сумме 14001 рубль.[30]

В настоящее время кредитные организациив общении с клиентами все чаще стали использовать мессенджеры– мобильные приложения для мгновенного обмена сообщениями. И как следствие мошенники нашли новый способ завладения денежными средствами.

В соответствии со статьей 140 ГК РФ платежи на территории Российской Федерации осуществляются путем наличных и безналичных расчетов, то есть находящиеся на счетах в банках денежные суммы могут использоваться в каче-

[30] Справка по изучению судебной практики по уголовным делам о мошенничестве (ст.159 -159-6 УК РФ) // Амурский областной суд: офиц. сайт. 10.04.2014. [Электронный ресурс] URL: http://oblsud.sudrf.ru/ modules.php?name=docum_sud=2487 (дата обращения: 05.01.2017).

стве платежного средства.

Исходя из этого с момента зачисления денег на банковский счет лица, оно получает реальную возможность распоряжаться поступившими денежными средствами по своему усмотрению, например, осуществлять расчеты от своего имени или от имени третьих лиц, не снимая денежных средств со счета, на который они были перечислены в результате мошенничества. В указанных случаях преступление следует считать оконченным с момента зачисления этих средств на счет лица, которое путем обмана или злоупотребления доверием изъяло денежные средства со счета их владельца, либо на счета других лиц, на которые похищенные средства поступили в результате преступных действий виновного.

Так, например, с помощью Viber и «аватарки» в нем с логотипом банка, а в качестве имени контакта было указано «9ОО», пользователям указанного мессенджера рассылаются поддельные сообщения от Сбербанка, который использует этот мессенджер для общения с клиентами.

Субъектом преступления является любое дееспособное лицо, достигшее 16-летнего возраста. По ч.3 ст. 159.6 УК РФ – специальным, квалифицирующим признаком выступает совершение преступления группой лиц по предварительному сговору либо организованной группой.

С субъективной стороны преступление, предусмотренное ст. 159.6 УК РФ, характеризуется прямым умыслом. При расследовании рассматриваемого преступления доказыванию подлежит умысел именно на хищение чужого имущества, либо на приобретение права на чужое имущество путем действий, указанных в диспозиции статьи, иначе состав мошенничества в действиях лица будет отсутствовать.

Спорным является вопрос, требуется ли дополнительная квалификация мошенничества в сфере компьютерной информации по ст. 272 или 273 УК РФ, когда в результате неправомерного доступа к компьютерной информации произошло уничтожение, блокирование, модификация либо копирование информации.Исходя из разъяснений Пленума Верховного Суда РФ № 51 от

27.12.2007 «О судебной практике по делам о мошенничестве, присвоении и растрате»[31]незаконные действия, в результате которых произошло уничтожение, блокирование, модификация либо копирование информации, путем несанкционированного доступа следует квалифицировать по ст. 159 УК РФ, а также по ст. 272 или ст. 273 УК РФ.

Так, Октябрьский районный суд г. Самары квалифицировал действия И. по ч. 3 ст. 272 УК РФ и по ч. 3 ст. 159.6 УК РФ.[32] И. обвинялась в том, что совершила неправомерный доступ к охраняемой законом компьютерной информации, что повлекло модификацию компьютерной информации, совершенное лицом с использованием своего служебного положения. В должности специалиста офиса продаж и обслуживания И. совершила неправомерный доступ к охраняемой законом компьютерной информации, содержащей персональные данные клиентов и их лицевых счетов, из корыстной заинтересованности с целью получения выгоды имущественного характера для себя осуществила обращение к личной карточке действующего абонента, после чего, противоправно, произвела замену сим-карты, на новую сим-карту имеющуюся в офисе продаж и обслуживания, что повлекло модификации компьютерной информации в автоматической биллинговойсистеме.В результате этого у нее появилась возможность пользоваться лицевым счетом абонента и распоряжаться денежными средствами, находящимися на нем.Она же, совершила мошенничество в сфере компьютерной информации: противоправно проверив баланс лицевого счета сим-карты с чужим абонентским номером, после чего с использованием услуги «Мобильная коммерция» незаконно осуществила перевод денежных средств на расчетный счет открытый на ее имя.

Камчатский районный суд в справке по изучению судебной практики по

[31] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]Постановление Пленума Верховного Суда РФ от 27.12.2007 № 51. Доступ из справ.- правовой системы «Гарант».

[32] Справка-обобщение изучения судебной практики рассмотрения судами Самарской области уголовных дел о преступлениях, предусмотренных ст.ст. 159.1 – 159.6 УК РФ, отграничение от смежных составов. Практика назначения наказания. // Куйбышевский районный суд города Самары: офиц. сайт. [Электронный ресурс] URL:http://kuibyshevsky.sam.sudrf.ru/ (дата обращения: 05.01.2017).

уголовным делам о мошенничестве (ст.159 -159-6 УК РФ) указывает на то, что дополнительная квалификация по ст.272 УК РФ и ст. 273 УК РФ не требуется.[33] Исключением является только если незаконные действия были осуществлены с использованием заранее изготовленных вредоносных программ, о которых говорится в ст.273 УК РФ.

Таким образом, обзор судебной практики показал, что в настоящее время существует два подхода к квалификации действий направленных на хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей: когда содеянное следует квалифицировать только по ст. 159.6 УК РФ и когда необходима также квалификация по ст.273 УК РФ, 274 УК РФ.

На наш взгляд при применении Пленума Верховного Суда РФ № 51 от 27.12.2007 «О судебной практике по делам о мошенничестве, присвоении и растрате» необходимо учитывать, что данные разъяснения вышли до появления новых составов и применять его необходимо исходя из обстоятельств конкретного дела, с учетом совершенных действий виновным лицом. 23.04.2015 в Верховном Суде РФ состоялась научно-практическая конференция на тему «Проблемы применения судами законодательства об ответственности за мошенничество, присвоение и растрату»[34], в работе которой приняли участие судьи Верховного Суда РФ, заместители председателей и судьи областных и равных им судов по уголовным делам, представители Конституционного Суда РФ, Государственной Думы РФ, Генеральной прокуратуры, Следственного комитета РФ, Минюста, МВД, ФСБ, адвокаты, а также ученые и преподаватели, в связи с чем возможно предположить, что решения проблем применения статей уголовного

[33] Справка по изучению судебной практики по уголовным делам о мошенничестве (ст.159 -159-6 УК РФ) // Камчатский краевой суд: офиц. сайт. 10.04.2014.[Электронный ресурс] URL: http://oblsud.kam.sudrf.ru/modules.php?name=docum_sud&id=2487 (дата обращения: 05.01.2017).

[34] IVНаучно-практическая конференция «Проблемы применения судами законодательства об ответственности за мошенничество, присвоение и растрату» // Верховный суд Российской Федерации: офиц. сайт.URL:http://www.vsrf.ru/catalog.php?c1=%CD%EE%E2%EE%F1%F2%E8%20%E8%20%F1%EE%E1%FB%F2%E8%FF&c2=%CD%EE%E2%EE%F1%F2%E8&c3=2015&id=9985 (дата обращения:05.01.2017).

права касающиеся преступлений в сфере компьютерной информации найдут свое отражение в разъяснениях Верховного Суда РФ.

2.2Условно-цифровое вымогательство, или кибершантаж

Все чаще в СМИ появляются предупреждения граждан о новом способе вымогательства с использованием информационных технологий: телефонные звонки, сообщения на электронную почту, блокирование работы компьютера посредствам сети Интернет.

В сентябре 2008 года житель Башкирии Ш. заблокировал сайты одного из саранских предприятий, связался с системным администратором и потребовал за прекращение вредоносной атаки 110 тыс. руб.[35] Свои требования хакер сопровождал новыми угрозами. За совершение вымогательства под угрозой повреждения чужого имущества Октябрьский районный суд г. Саранска приговорил Ш. к году лишения свободы условно.

В 2005 году молодой американец создал сайт, на котором опубликовал трогательный рассказ о своем крольчонке Тоби с его фотографией[36]. После рассказа блоггер разместил описание различных блюд из кролика и требование к любителям животных о том, что, если они в течение нескольких месяцев не переведут 50 тыс. долл., то хозяин кролика съест его. В итоге за неполные два месяца было перечислено около 20 тыс. долл.

Новый вид вымогательства с использованием современных компьютерных технологий, интернет пространства получил название кибершантаж. В уголовном кодексе такого понятия не существует, а рассматриваемые деяния квалифицируютсяпо статье 163 УК РФ.При квалификации и при рассмотрении уголовных дел о вымогательстве необходимо выявлять все обстоятельства, способствовавшие совершению преступления, нарушению прав и свобод граждан, другие нарушения закона, а также способы совершения.

Из приведенных выше примеров видно, что способы компьютерного вымогательства, способы воздействия на жертву разнообразны.Анализ позволил

[35] Лопатина Т.М. Условно-цифровое вымогательство, или кибершантаж // Журнал российского права. 2015. №1. С. 1120.

[36] Там же. С.121.

выделить наиболее встречающиеся способы, рассмотрим их.

Так называемый «вирус с сюрпризом» блокирует работу операционной системы, помещая на рабочем столе сообщение о возможности продолжить работу, только после ввода пароля, который будет сообщенпосле перевода денежных средств определенным способом. Так в апреле текущего года появилась информация от компании Apple о «заражении» компьютеров вредоносной программой «KeRanger», которая шифрует данные, а затем просит заплатить выкуп или все данные будут удалены.

Также довольно часто интернет пользователям предлагается выкупить пароли к своим же почтовым ящикам, страничкам в интернете, аккаунтам после их взлома и смены паролей, установленных их владельцем.

Еще один широко распространенный способ кибершантажа– это DDoS-атаки. В ноябре 2016 года крупнейшие финансовые организации «Сбербанк» и «Альфа-банк» подверглись DDoS-атакам.[37] Атаки были организованы с использованием десятков тысяч машин расположенных в нескольких десятках стран.DDoS-атаки (с англ. DistributedDenialofService — «отказ от обслуживания»)осуществляются с помощью многочисленных ложных запросов на сайт, что приводит к выведению его из строя.

Следующий способ шантажа не новый, но выразившийся в новой форме, с использованием высоких технологий. На компьютере может содержаться любая информация: секретные данные бизнеса, очень личные фотографии или видеофайлы, еще неопубликованная книга и злоумышленник, получив данную информацию, шантажирует ее владельца.

Для перевода денежныхсредств в распоряжение вымогателя то же существуют различные способы. Чаще всего вымогателями предлагается осуществить денежный перевод посредствам платных смс или пополнения «баланса» телефона.

Потерпевшему приходит СМС сообщение или непосредственно звонок с

[37] «Сбербанк» и «Альфа-банк» подверглись хакерской атаке // Электронное периодическое издание «Ведомости» (Vedomosti): офиц. сайт.[Электронный ресурс]URL: http://www.vedomosti.ru/finance/articles/2016/11/09/664252-sberbank (дата доступа: 09.01.2017).

незнакомого номера и якобы сын, дочь, другой близкий родственникпросит срочно перевести деньги на данный номер телефона, так как он попал в беду, у него сложная жизненная ситуация. В 2013-2015 годах довольно часто гражданам поступали звонки от «сына» якобы сбившего человека, с просьбой срочно перевести деньги на телефон для того чтобы «замять» дело. Или следующая история: «Мама я в больнице, необходимо оплатить операцию». Стрессовая ситуация, зачастую пожилой возраст потерпевших не позволяли им адекватно оценить ситуации и осознать что звонивший не их родственник.

Другой популярный способ получить деньги это потребовать перевода через электронные системы оплаты, например,Webmoney. Схема с почтовыми переводами, чеками или переводами на кредитки используется редко, ибо там проявляется человек с его персональными данными и у полиции повышаются шансы на поимку вымогателя.

В настоящее время появился еще один способ получения средств –в биткоинах. Биткоин – это интернет валюта, никто ее не централизует, ни одно учреждение не контролирует, не печатает купюры, и соответственно трудно отследить потоки виртуальных денег, однако ими вполне возможно совершать покупки, оплачивать услуги и даже играть на бирже. По сути, с технической точки зрения, сами биткоины нигде не хранятся, хранятся только секретные цифровые ключи, дающие доступ к публичным биткоин-адресам и возможность «подписывать» транзакции. Именно эта информация и хранится в биткоин кошельке.

Таким образом, интернет-вымогатели пользуются не только современными техническими средствами и современными технологиями, но и классическими способами для ст.163 УК РФ: требование передачи чужого имущества или права на имущество под угрозой уничтожения или повреждения чужого имущества, под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких.

С точки зрения закона нет разницы, совершено вымогательство в реаль-

ной жизни или в виртуальном пространстве. Постановление Пленума Верховного Суда Российской Федерации от 17.12.2015 № 56 «О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации)» (далее – ПостановлениеПленума Верховного Суда Российской Федерации № 56)[38] разъясняет,что вымогательство является оконченнымкогда требование доведено до потерпевшего. Невыполнение потерпевшим этого требования не влияет на юридическую оценку содеянного как оконченного преступления.

В 1999 году хакер с никомМаксус украл из базы данных американского виртуального магазина CD Universe информацию о номерах 300 тысяч кредитных карт и потребовал у компании 100 тысяч долларов.[39] После того, как CD Universe отказался от сделки, информация о номерах карточек 25 тысяч клиентов была выложена на сайте хакера в открытом доступе, после чего власти заблокировали ресурс.

Наиболее характерно для интернет-вымогателей применение угрозы в виде распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких, т.е. шантажа. ПостановлениеПленума Верховного Суда Российской Федерации № 56 разъясняет, что сведения, позорящие потерпевшего или его близких – это любые сведения, составляющие охраняемую законом тайну, порочащие честь, достоинство, репутацию, при этом соответствие действительности указанных сведений значения не имеет.

Однако ч.1 ст.163 УК РФ не указывает на то, что подобные действия являются шантажом.

В толковом словаре русского языка шантаж определяется как угроза разоблачения, разглашения компрометирующих сведений с целью вымогательст-

[38] О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации) [Электронный ресурс]Постановление Пленума Верховного Суда РФ от 17.12.2015 № 56. Доступ из справ.- правовой системы «Гарант».

[39] Ходорыч А. Карты военных действий // Журнал «Коммерсантъ Деньги» №19 от 19.05.2003. [Электронный ресурс]URL:http://www.kommersant.ru/doc/382608 (дата обращения: 11.01.2017).

ва, вообще угроза, запугивание чем-нибудь с целью создать выгодную для себя обстановку. Большинство ученых полагают, что в самом полном виде определение шантажа содержится именно в составе вымогательства, хотя сам термин в диспозиции и не назван. Т.М. Лопатина считает что ст.163 УК РФ необходимо дополнить примечанием следующего содержания: «Под шантажом в статьях настоящего Кодекса понимается угроза распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких».[40]В своей статье «Условно-цифровое вымогательство, или кибершантаж» Т.М. Лопатинарассматривает важный вопрос отнесения кибершантажа к определенной группе преступлений.

Анализ Уголовного кодекса позволил сделать вывод, что законодатель не отождествляет понятия хищения и вымогательства, разделяя их. Это видно из ст. 221 УК РФ, ст. 226 УК РФ, ст. 229 УК РФ где законодатель разделяет: хищение либо вымогательство.

Однако, соотнесение признаков хищения и вымогательства позволяет установить больше сходств чем различий.

Изъятие чужого имущества при хищении и при вымогательстве противоправно и имеет корыстную цель.В качестве обязательного признака любой формы хищения и вымогательства выделяется предмет посягательства в виде чужого имущества или права на него, а так же в обоих случаях предполагается реальный материальный ущерб.

Но все же отличия есть. Отличием является способ совершения: хищение может быть совершено ненасильственным способом или насильственным, вымогательство предполагает применение насилиядля завладениячужим имуществом. Так же если говорить о таком признаке как безвозмездность, то и тут есть отличия. При отдельных видах хищения возможно причинение материального ущерба собственнику имущества путем предоставления, напри-

[40] Лопатина Т.М. Условно-цифровое вымогательство, или кибершантаж// Журнал российского права. 2015. №1. С. 119.

мер,фальсифицированного товара, а вот при вымогательстве ни какие компенсационные действия не предполагаются.

Особенностью интернет-вымогательства или кибершантажа является подавление воли потерпевшего психологическим воздействием, сопровождающимся угрозой с использованием компьютерных технологий, технологий в сфере связи, а так же свойства Интернета расширяют территориальные границы нахождения вымогателя и жертвы.

Кибершантажом занимаются не только единичные злоумышленники, но и распространены преступные группы, в которые входят программисты, создающие вредоносные программы, специалистыпо способам заражения и распространения вредоносных программ в сети Интернет;владельцы ботнетов– сети компьютеров, зараженных вредоносной компьютерной программой, позволяющей управлять ими.

Так, в 2003году программисты И. Максаков, А. Петров и Д. Степанов в течение полугода организовывали DDoS-атаки на серверы британских букмекерских контор и букмекеры несли максимальные потери. За прекращение атак программисты требовали с владельцев компаний выкуп в размере 10-20 тыс. долл. По данному факту было возбуждено уголовное дело по ст.163 и ст.273 УК РФ[41].

Подводя итоги, следует сказать, что отдельной статьи уголовный кодекс не содержит, как и уголовное право не имеет сформулированного определения кибершантаж, однако данное деяние распространено в современном мире. На наш взгляд с уголовно-правовой и криминологической стороны кибершантаж– корыстное, имущественное преступление, совершаемое путем принуждения к действию.

[41] Лопатина Т.М. Условно-цифровое вымогательство, или кибершантаж // Журнал российского права. 2015. №1. С. 125.

3 ПРОБЛЕМЫ УГОЛОВНОГО ПРЕСЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

3.1 Правовая основа деятельности правоохранительных органов в борьбе с преступлениями в сфере высоких информационных технологий

Прежде чем приступить к анализу правовых основ деятельности правоохранительных органов в борьбе с преступлениями в сфере высоких информационных технологий необходимо рассмотреть в общем понятие правоохранительной деятельности в Российской Федерации.

Статья 2 Конституции Российской Федерации закрепляет за государством обязанность защищать права граждан. Из этого следует, что правоохранительная деятельность – это деятельность государства направленная на признание, соблюдение и защиту прав и свобод человека. Осуществляют эту деятельность специально уполномоченные органы: органы внутренних дел Российской Федерации, органы федеральной службы безопасности, органы уголовно-исполнительной системы, таможенные органы Российской Федерации, органы Следственного комитета Российской Федерации и другие.

В борьбе с преступностью правоохранительные органы координируют свою деятельность на основании статьи 8 Федерального закона от 17.01.1992 № 2202-I «О прокуратуре Российской Федерации»[42] и в соответствии с Положением о координации деятельности правоохранительных органов по борьбе с преступностью, утвержденным Указом Президента РФ от 18.04.1996 № 567 «О координации деятельности правоохранительных органов по борьбе с преступностью»[43].

К примеру, статья 1 Федерального закона от 7.02.2011№ 3-ФЗ «О полиции»[44] (далее – Федеральный закон «О полиции») определяет, что назначение полиции, в том числе и в защите прав граждан Российской Федерации, ино-

[42] О прокуратуре Российской Федерации [Электронный ресурс] Федеральный закон от 17.01.1992 № 2202-I. Доступ из справ.- правовой системы «Гарант».

[43] О координации деятельности правоохранительных органов по борьбе с преступностью [Электронный ресурс] Указ Президента РФ от 18.04.1996 № 567. Доступ из справ.- правовой системы «Гарант».

[44] О полиции [Электронный ресурс] Федеральный закон от 7.02.2011 № 3-ФЗ. Доступ из справ.- правовой системы «Гарант».

странных граждан и лиц без гражданства.

Правовую основу деятельности полиции составляют конституция Российской Федерации, нормы международного права, федеральные конституционные законы, Федеральный закон «О полиции» и другие федеральные законы, нормативные правовые акты Президента Российской Федерации и нормативные правовые акты Правительства Российской Федерации, а также нормативные правовые акты Министерства внутренних дел Российской Федерации. Это закреплено в статье 3 Федерального закона «О полиции».

Теперь рассмотрим, что же входит в понятие «другие федеральные законы» регулирующие деятельность правоохранительных органов в борьбе с преступлениями в сфере высоких информационных технологии.

На территории Российской Федерации действует ряд федеральных законов регулирующих отношения в области информации:

1. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»[45].

2. Федеральный закон от 29.12.1994 № 77-ФЗ «Об обязательном экземпляре документов»[46].

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[47].

4. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»[48].

5. Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне»[49].

6. Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции»[50].

---

[45] Об электронной подписи [Электронный ресурс] Федеральный закон от 06.04.2011 № 63-ФЗ. Доступ из справ.- правовой системы «Гарант».

[46] Об обязательном экземпляре документов [Электронный ресурс] Федеральный закон от 29.12.1994 № 77-ФЗ. Доступ из справ.- правовой системы «Гарант».

[47] Об информации, информационных технологиях и о защите информации [Электронный ресурс] Федеральный закон от 27.07.2006 № 149-ФЗ. Доступ из справ.- правовой системы «Гарант».

[48] О связи [Электронный ресурс] Федеральный закон от 07.07.2003 № 126-ФЗ. Доступ из справ.- правовой системы «Гарант».

[49] О государственной тайне [Электронный ресурс] Федеральный закон от 21.07.1993 № 5485-I. Доступ из справ.- правовой системы «Гарант».

7. Закон РФ от 27.12.1991 № 2124-I «О средствах массовой информации»[51] и др.

Прежде всего, необходимо разобраться, чем руководствоваться правоохранительным органам, чтобы определить какая информация попадает под защиту. Прежде всего, это Федеральный закон от 27.07.2006 № 149-ФЗ«Об информации, информационных технологиях и о защите информации», где в статье 1 закреплено, что данный закон регулирует отношения, в том числе в сфере защиты информации[52]. Существует 4 основных вида информации, которые попадают под защиту законом: информация, составляющая государственную тайну; сведения, составляющие коммерческую тайну; информация, составляющая профессиональную тайну и персональные данные.

Перечень сведений попадающих под понятие государственная тайна закреплен в статье 5 Закона Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне»[53]:информация в военной и экономической области, в области науки и техники, в области внешней политики и экономики, а также в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, противодействия терроризму, обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

Условия отнесения сведений к информации составляющей коммерческую тайну закреплены в Федеральном законе от 29.07.2004 №98-ФЗ «О коммерческой тайне»[54], где определено, что это сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, ко-

[50] О защите конкуренции [Электронный ресурс] Федеральный закон от 26.07.2006 № 135-ФЗ. Доступ из справ.- правовой системы «Гарант».

[51] О средствах массовой коммуникации [Электронный ресурс] Федеральный закон от 27.12.1991 № 2124-I. Доступ из справ.- правовой системы «Гарант».

[52] Об информации, информационных технологиях и о защите информации [Электронный ресурс] Федеральный закон от 27.07.2006 № 149-ФЗ. Доступ из справ.- правовой системы «Гарант».

[53] О государственной тайне [Электронный ресурс] Закон Российской Федерации от 21.07.1993 № 5485-I.Доступ из справ.- правовой системы «Гарант».

[54] О коммерческой тайне [Электронный ресурс] Федеральный закон от 29.07.2004 № 98-ФЗ. Доступ из справ.- правовой системы «Гарант».

торые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) попадает под действие Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»[55] и подлежит защите, что отражено в статье 2 названного закона.

Если говорить об информации, составляющей профессиональную тайну, то такая информация подлежит защите, если такая обязанность закреплена в федеральных законах.То есть в данном случае единого закона, в целом регулирующего отношения в сфере «профессиональной информации» нет, а существует ряд законов регулирующих различные отношения, сферы. В качестве примера можно назвать Федеральный закон «О полиции», где в статье 27 за сотрудником полиции закрепляется обязанность сохранять информацию, ставшую известной в связи с выполнением служебных обязанностей; Федеральный закон от13.05.2008№68-ФЗ «О центрах исторического наследия президентов Российской Федерации, прекративших исполнение своих полномочий»[56] закрепляет за ревизионной комиссией Центра исторического наследия Президента Российской Федерации, прекратившего исполнение своих полномочий обязанность не разглашать информацию, которая стала известна в ходе проверки. А в Федеральном законе от 19.07.2007 № 196-ФЗ«О ломбардах»[57] не только закреплена обязанность работников ломбарда сохранять конфиденциальность информации, составляющую профессиональную тайну, но и в ч. 1 ст. 3 закреплено понятие информации, составляющую профессиональную тайну в регулируемой сфере.

[55] О персональных данных [Электронный ресурс] Федеральный закон от 27.07.2006 № 152-ФЗ. Доступ из справ.- правовой системы «Гарант».

[56] О центрах исторического наследия президентов Российской Федерации, прекративших исполнение своих полномочий [Электронный ресурс] Федеральный закон от 13.05.2008 № 68-ФЗ. Доступ из справ.- правовой системы «Гарант».

[57] О ломбардах [Электронный ресурс] Федеральный закон от 19.07.2007 № 196-ФЗ. Доступ из справ.- правовой системы «Гарант».

Понятие «информационные технологии» дано в статье 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Как отмечалось ранее, понятие компьютерной информации, то есть сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи дано в примечаниях к статье 273 УК РФ.

Таким образом, в этих преступлениях информация является объектом преступного посягательства, а также может быть предметом или орудием преступления. Основные виды компьютерных преступлений: мошенничество,DoS-атаки, вредоносные программы, были нами рассмотрены в первой и второй главах данной дипломной работы.

Как уже было сказано выше защита «информационных прав» закреплена в Конституции РФ и это является основой обеспечения информационной безопасности. Информационные технологии в современном мире развиваются стремительно и закрепить на уровне федерального законодательства все особенности данной сферы не представляется возможным, в связи с чем в своей деятельности правоохранительные органы должны не только основывается на вышеперечисленных федеральных законах, но и на различных правилах, инструкциях, стандартах в сфере информационных технологий.

3.2 Проблемы выявления преступлений в сфере высоких информационных технологий

Е.С. Шевченко[58] проведя опрос среди следователей и дознавателей, пришла к выводу, что достаточно часто им приходится расследовать преступления предусмотренные: главой 28 УК РФ, ст. 159.6 УК РФ «Мошенничество в сфере

[58] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. на соискание учёной степени кандидата юридических наук // Московский государственный юридический университет имени О.Е. Кутафина (МГЮА): офиц. сайт. [Электронный ресурс]URL: https://msal.ru/common/upload/SHevchenko_E.S.pdf (дата обращения: 25.11.2016).

компьютерной информации», ст. 242.1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», ст. 242 УК РФ «Незаконные изготовление и оборот порнографических материалов или предметов», ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации информационно-телекоммуникационных сетей», ст. 158 УК РФ «Кража», ст. 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», ст. 137 УК РФ «Нарушение неприкосновенности частной жизни», ст. 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства».

При выявлении и раскрытии преступлений в сфере высоких информационных технологий правоохранительные органы сталкиваются с рядом проблем.

При выявлении –это прежде всего высокая латентность рассматриваемых преступлений. Так как данные преступления совершаются с использованием компьютерных программ, компьютеров, средств связи, сложных технических средств, то виновные лица планируют преступления скрывая их под технические сбои аппаратуры или неполадки, то есть под естественные, обычные ситуации для сложной техники. Зачастую жертвы сами, зная о совершенном, не заявляют об этом в правоохранительные органы.

Причем латентность по причине не заявления потерпевших в правоохранительные органы в случае преступлений в сфере информационных технологий значительно выше других причин. Н.П.Кириллова и С.П.Кушниренко установили наиболее распространенные мотивы, приводящие к латентности рассматриваемых видов преступлений.[59] Если говорить о гражданах то тут две основные причины отказа от обращения с заявлением в правоохранительные органы:

[59] Кириллова Н.П., Кушниренко С.П.Преступления в сфере высоких информационных технологий // Правоведение. 2013. №3. С.79-80.

не желание тратить время, прилагать усилия, при незначительности понесенных убытков, причинного вреда, и нежелание придавать огласки личные данные, компрометирующие сведения, семейные тайны. Так же среди граждан распространено мнение, что в ряде случаев при мошенничестве в сети интернет невозможно установить виновного, а так же осознание что жертва сама не обеспечила необходимой защиты информации, информационной системы. У организаций, руководителей в дополнение к названным мотивам и другие причины. Прежде всего здесь следует отметить не желание придавать общественной огласки факт внешнего вмешательства в информационную систему организации, в результате чего был осуществлен неправомерный доступ к клиентским базам к примеру, что может повлиять на репутацию, потерю клиентов. Так же в случае обращения с заявлением в органы правопорядка для осуществления расследования может быть необходимо изъятие компьютерной техники, электронных носителей, блокирование систем, что повлечет приостановку работы организации на время следственных действий или до окончательного принятия решения судом по возбужденному уголовному делу.

Уголовное дело может быть возбужденно не только по заявлению потерпевшего, но и других лиц. Любой пользователь интернета, просматривая сайты может обнаружить нарушение авторских прав путем предложения установить определенную программу, объявление о продаже вредоносных программ или баз данных. Но здесь следует отметить восхищение молодым поколением людьми способными на совершение противоправных действий с использованием знаний, умений в сфере высоких информационных технологий и желанием не раскрыть их, а присоединиться к их «обществу». Громко с восхищением обсуждаются действия российских хакеров взламывающих системы безопасности информационных систем других государств, киберпреступники пишут статьи, издают книги, так в 2012 году издательство «Эксмо» напечатало книгу[60]К.Митник и У.Саймона «Призрак в сети: мемуары величайшего хакера». Это в свою очередь тоже влечет скрытость данных фактов и не обращения в

[60] Митник К., Саймон У. Призрак в сети: мемуары величайшего хакера. М. Эксмо, 2012.416 с.

правоохранительные органы лиц обнаруживших преступления в сфере высоких информационных технологий.

Опрос следователей, дознавателей, сотрудников прокуратуры 13 регионов Российской Федерации проведенный Е.С. Шевченко, показал, что только 10,5 % имеют на ряду с юридическом еще и техническое образование и только 5,3 % специальное высшее образование в рассматриваемой сфере, а 78,9 % получили необходимые знания самостоятельно.[61]

Все вышесказанное: высокий уровень латентности на ряду со спецификой преступлений в сфере высоких информационных технологий, требующих определенных знаний приводит к сложности обобщения материалов следственных органов, наработки методов раскрытия рассматриваемых преступлений и ведения следственных мероприятий.

3.3 Особенности тактики следственных действий

Результаты опроса следователей и дознавателей проведенного Е.С.Шевченко показали, что при расследовании ими преступлений, рассматриваемых в данной работе, осуществлялись вербальные следственные действия – допрос и очная ставка, а также невербальные – осмотр места происшествия, обыск, выемка, следственный эксперимент, назначение судебных экспертиз.[62]

Рассмотрим некоторые невербальные следственные действия, содержащие наиболее специфические черты для данной категории преступлений.

Основными задачами осмотра места происшествия, проводящегося в порядке статьи 177 УПК РФ, при расследовании преступлений совершенных с использованием высоких информационных технологий является:

1) установление события преступления, выяснение развития событий и действий преступника, разбор обстановки места происшествия;

2) выявление и изъятие следов совершенного преступления;

3) получение информации для выдвижения следственных версий;

---

[61] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. на соискание учёной степени кандидата юридических наук // Московский государственный юридический университет имени О.Е. Кутафина (МГЮА): офиц. сайт.[Электронный ресурс] URL: https://msal.ru/common/upload/SHevchenko_E.S.pdf (дата обращения: 25.11.2016).

[62] Там же.

4) получение информации о лице (лицах) причастных к совершенному преступлению.

Еще одной задачей характерной именно для рассматриваемых преступлений является отнесение информации к защищаемой законом и определение имеющихся средств защиты информации, информационной системы, носителей информации.

Для решения всех поставленных задач осмотра места необходимо привлекать специалистов со специальными знаниями и наличием определенной аппаратуры и технических средств, например таких как, соединительные кабели, переносной компьютер со специальным программным обеспечением, внешний винчестер для запуска осматриваемого компьютера, если запуск собственной операционной системы не возможен или не желателен, так как необходимо распознать не только материальные следы, но и зачастую виртуальные. Перед началом осмотра места необходимо провести ряд мероприятий тоже требующих специальных знаний и навыков. Помимо ограничения доступа к серверу, компьютерной технике, другим средствам хранения и обработки информации необходимо выставить охрану электрических щитов и пультов с целью предотвращения несанкционированного выключения электрической энергии и препятствия в работе с названными техническими средствами. А вот следующие мероприятия уже требуют специальных знаний и навыков, а также привлечения специалистов: для того чтобы пресечь изменение или удаление информации извне необходимо отключить удаленный доступ и установить не запущенна ли программа уничтожения информации, отключить компьютер от питания, в случае установления такой программы. Далее необходимо произвести осмотр специальных средств, компьютеров, серверов, других носителей информации.

Отсутствие специальных знаний у следователя может привести к утрате важных следов. При этом привлекаемые специалисты могут выявить нештатную аппаратуру и следы противодействия аппаратной системе защиты, которая обязательно фотографируется и описывается, а специалист-криминалист устанавливает и фиксирует следы механического воздействия. Для осмотра места

преступления можно пригласить специалистов информационно-вычислительных центров региональных управлений МВД, обладающих специальными знаниями и уровнем профессиональной подготовки. Для обнаружения виртуальных следов можно применить программно-аппаратные средства сбора и анализа компьютерных данных, предназначенные для криминалистического исследования компьютерных носителей информации, на основе международных спецификаций и требований, предъявляемых к деятельности правоохранительных органов или мобильный комплекс по сбору и анализу цифровых данных «UFED», а так же мобильный подавитель работы сотовых телефонов «Соната».

Так же при осмотре места необходимо изучить следующие документы: функциональные правила работы с информационными системами, специальной техникой, носителями информации, а так же внутреннюю документацию устанавливающую распределение обязанностей, должностные полномочия, внутренние правила работы с перечисленными системами и техникой.

Далее делаются копии информации и если необходимо в порядке статьи 177 УПК РФ носители важной информации изымаются, упаковываются и опечатываются для их дальнейшего осмотра специалистами[63].

Следует отметить, что при различных преступлениях с использованием информационных технологий тактика осмотра места происшествия имеет свою специфику, но общей задачей будет установление механизма совершения преступления.

Производство обыска и выемки при расследовании рассматриваемой категории преступлений, тоже имеют свою специфику. Цель названных следственных мероприятий – получение информации или доказательств способа совершения преступления, то есть обнаружение и изъятие компьютера, техники, мобильных телефонов, других носителей информации. Для успешного проведения обыска необходимо подготовиться. Например, еще на этапе подготовки

[63] Уголовно-процессуальный кодекс российской Федерации [Электронный ресурс] Принят Государственной Думой 22.11.2001 (ред. от 19.12.2016). Доступ из справ.- правовой системы «Гарант».

необходимо запросить у оператора связи информацию о подключении к сети Интернет, о наличии беспроводной сети Wi-Fiпо адресу, где планируется обыск. Или же определить необходимость применения при обыске специальных средств из названных выше, к примеру «Соната».

Специфика рассматриваемой категории преступлений обуславливает необходимость проведения специальных судебных экспертиз: информационно-технологической и информационно-технической.

Объектом информационно-технологической экспертизы является установленный порядок обработки информации, осуществляемый по заданным алгоритмам, или информационная технология, основанная на применении современной информационно-вычислительной техники, средств связи и телекоммуникаций, составляющих основу информатизации общества.

Объектом информационно-технической экспертизы является техническое обеспечение информационной безопасности компьютерных систем и сетей.[64]

Как правило, названные виды экспертиз назначаются после осмотра места, обыска, когда собранной информации не достаточно для дальнейшего расследования.

После принятия решения о проведении экспертизы следователю необходимо определиться с перечнем вопросов перед экспертом и их формулировкой. На этом этапе тоже могут возникнуть проблемы из-за недостаточных знаний в области информационных технологий, современных возможностей технических средств, например из-за неправильной, не точной формулировки вопроса эксперту следователь не получит необходимую информацию.

Так же, результативными являются судебные психологические экспертизы, позволяющие определить личность преступника, мотивы его поступка, а также психопатологий связанных с интернет – зависимостью.

При назначении экспертизы идля постановки вопросов эксперту необходимо руководствоваться Постановлением Пленума Верховного Суда РФ от 21

[64] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации[Электронный ресурс] Утвержденные Генеральной прокуратурой. Доступ из справ.- правовой системы «Гарант».

декабря 2010№28 «О судебной экспертизе по уголовным делам»[65] и не ставить перед экспертом вопросы правового характера квалификации деяния.

Подводя итоги раздела 3 необходимо отметить, что при расследовании преступлений в сфере высоких информационных технологий не достаточно опираться на знаниях уголовного права: уголовного и уголовно-процессуального кодексов, необходимо изучить федеральное законодательство в сфере информации, а также различные подзаконные акты, инструкции, стандарты, правила эксплуатации. Но помимо знаний юридического характера, большое значение для успешного раскрытия преступления и его правильной квалификации имеют специальные знания, техническое образование которыми должны обладать работники правоохранительных органов, а так же необходимо привлекать специалистов и экспертов в области высоких информационных технологий, как для консультаций, так и для проведения конкретных следственных мероприятий.

[65] О судебной экспертизе по уголовным делам [Электронный ресурс]Постановление Пленума Верховного Суда РФ от 21.12.2010 № 28. Доступ из справ.- правовой системы «Гарант».

ЗАКЛЮЧЕНИЕ

Стремительное развитие информационных технологий, информационно-телекоммуникационных сетей, в том числе и сети Интернет, массовое применение вычислительных средств, мобильных устройств, вовлечение общества в сетевые сервисы, осуществление финансовых операций в режиме OnLine[66] все это способствует появлению и развитию преступлений с использованием современных информационных технологий. В уголовном кодексе существует ряд статей позволяющих привлекать к ответственности лиц, совершающих преступления в сфере информационных технологий. Так, Федеральным законом Российской Федерации от 07.12. 2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»[67] были внесены изменения в главу 28 УК РФ объединяющей в себе 3 статьи о преступлениях в сфере компьютерной информации.

В статье 272 УК РФ законодатель закрепил уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации, то есть доступ к информации в отсутствии соответствующего разрешения со стороны обладателя. При этом к уголовной ответственности привлекается лицо только в случае если неправомерный доступ повлек уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Состав преступления предусмотренного статьей 273 УК РФ содержит только деяние, то есть создание, распространение, использование вредоносных программ и тем самым является формальным. То есть преступление считается оконченным даже если вышеперечисленные деяния не вызвали последствий в виде несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты ком-

[66] Шаповалова Г.М., Шаповалов В.В. Криминалистика и ее роль в предупреждении преступлений на основе информационных технологий // Полицейская деятельность. 2016. № 2. С.189.

[67] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации [Электронный ресурс] Федеральный закон от 07.12. 2011 года № 420-ФЗ. Доступ из справ.- правовой системы «Гарант».

пьютерной информации.

По ст. 274 УК РФ уголовная ответственность наступает за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, но только если в результате был причинён крупный ущерб. Напомним, что в рамках главы 28 УК РФ крупный ущерб – это ущерб, сумма которого превышает один миллион рублей.

Рассматривая ст. 272 УК РФ и ст. 273 УК РФ мы говорили об умышленных деяниях, а вот действия, попадающие под ст. 274 УК РФ, могут быть совершенны как в форме прямого умысла, так и по неосторожности.

Таким образом, глава 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации» входит в состав Раздела IX «Преступления против общественной безопасности и общественного порядка» и содержит три статьи: ст. 272 – неправомерный доступ к компьютерной информации; ст. 273 – создание, использование и распространение вредоносных программ; ст. 274 – нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Еще одним способом применения информационных технологий в преступных целях стало мошенничество и законодатель Федеральным законом от 29.11.2012 № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» дополнил главу 21 УК РФ статьей 1596 «Мошенничество в сфере компьютерной информации». Хищение чужого имущества или приобретение права на чужое имущество в рамках рассматриваемой статьи совершаются следующими способами: ввод, удаление, блокирование, модификация компьютерной информации или вмешательство в функционирование средств хранения, средств обработки, средств передачи компьютерной информации, информационно-телекоммуникационные сети. Исходя из разъяснений Пленума Верховного Суда РФ № 51 от 27.12.2007 «О судебной практике по делам о мошенничестве, присвоении и

растрате»[68] незаконные действия, в результате которых произошло уничтожение, блокирование, модификация либо копирование информации, путем несанкционированного доступа следует квалифицировать по ст. 159 УК РФ, а также по ст. 272 или ст. 273 УК РФ.

На наш взгляд при применении названного выше постановления Пленума Верховного Суда РФ необходимо учитывать, что данные разъяснения вышли до появления новых составов и применять его необходимо исходя из обстоятельств конкретного дела, с учетом совершенных действий виновным лицом.

Еще одни вид преступления с использованием информационных технологий рассматриваемых в данной выпускной квалификационной работе – это интернет-вымогательство. Особенностью интернет-вымогательства или кибершантажа является подавление воли потерпевшего психологическим воздействием, сопровождающимся угрозой с использованием компьютерных технологий, технологий в сфере связи. В уголовном кодексе понятия интернет-вымогательства или кибершантажа не существует, а рассматриваемые деяния квалифицируются по статье 163 УК РФ, так как с точки зрения закона нет разницы, совершено вымогательство в реальной жизни или в виртуальном пространстве.

Правовую основу деятельности полиции в борьбе с преступлениями в сфере информационных технологий на раду с конституцией Российской Федерации, нормами международного права, федеральными конституционными законами и Федеральным законом «О полиции» так же составляют федеральные законы, регулирующие отношения в области информации.

При выявлении и раскрытии преступлений в сфере высоких информационных технологий правоохранительные органы сталкиваются с рядом проблем. Основными из них можно назвать высокую латентность преступлений в сфере информационных технологий и необходимость специальных знаний и навыков при расследовании рассматриваемых преступлений и при проведении следст-

[68] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]Постановление Пленума Верховного Суда РФ от 27.12.2007 № 51 Доступ из справ.- правовой системы «Гарант».

венных действий. Специфика рассматриваемой категории преступлений обуславливает необходимость проведения специальных судебных экспертиз: информационно-технологической и информационно-технической.

Таким образом, при расследовании преступлений в сфере высоких информационных технологий необходимо изучить законодательство в сфере информации, различные подзаконные акты, инструкции, стандарты, правила эксплуатации. Так же помимо знаний юридического характера, большое значение для успешного раскрытия преступления и его правильной квалификации имеют специальные знания, техническое образование которыми должны обладать работники правоохранительных органов, а так же необходимо привлекать специалистов и экспертов в области информационных технологий, как для консультаций, так и для проведения конкретных следственных мероприятий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

I Правовые акты

1 Конституция Российской Федерации от 12.12.1993 (с поправками от 21.07.2014) // Соб.законодательства Российской Федерации. – 2014. – № 31. ст. 11747.

2 Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в ред. Федерального закона от (19.12.2016 № 436-ФЗ) // Соб. законодательства Российской Федерации. –1996. № 25. ст. 2954; 2016. № 52 (5 ч.).ст.7485.

3 Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 года № 174-ФЗ(в ред. Федерального закона от 19.12.2016 № 457-ФЗ) // Соб. законодательства Российской Федерации. –2001. № 52 (1 ч.).ст. 4921; 2016. № 52 (5 ч.). ст.7506.

4 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. Федерального закона от 23.06. 2016 № 208-ФЗ) // Соб. законодательства Российской Федерации. – 2006. № 31(1 ч.).ст. 3448; 2016. № 52 (5 ч.). ст.7491.

5 Федеральный закон от 02.10.2007 № 229-ФЗ «Об исполнительном производстве» (в ред. Федерального закона 28.12.2016 № 492-ФЗ) // Соб. законодательства Российской Федерации. –2007. № 41. ст. 4849; 2017. № 1 (1 ч.).ст.33.

6 Федеральный закон от 20.08.2004 № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» (в ред. Федерального закона от 03.07. 2016 № 305-ФЗ) // Соб. законодательства Российской Федерации. –2004. № 34. ст. 3534; 2016. № 27 (2 ч.).ст.4238.

7 Федеральный закон от 20.04.1995 № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» (в ред. Федерального закона от 03.07.2016 № 305-ФЗ) // Соб. законодательства Российской Федерации. –1995. № 17. ст. 1455; 2016. № 27 (2 ч.).ст.4238.

8 Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» (в ред. Федерального закона от 12.03.2014 № 35-ФЗ) // Соб. законодательства Российской Федерации. –2004. № 32. ст. 3283; 2014. № 11. ст.1100.

9 Федеральный закон от 19.07.2007 № 196-ФЗ «О ломбардах»(в ред. Федерального закона от 13.07.2015 № 231-ФЗ) // Соб. законодательства Российской Федерации. –2007. № 31. ст. 3992; 2015. № 29 (1 ч.).ст.4357.

10 Федеральный закон от 7.02.2011 № 3-ФЗ «О полиции» (в ред. Федерального закона от 06.04.2015 № 68-ФЗ) // Соб. законодательства Российской Федерации. –2011. № 7. ст. 900; 2015. № 14. ст.2008.

11 Федеральный закон от 17.01.1992 № 2202-I «О прокуратуре Российской Федерации» (в ред. Федерального закона от 19.12.2016 № 434-ФЗ) // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1992. № 8. ст. 366; Соб. законодательства Российской Федерации. –2016. № 52 (5 ч.).ст.7483.

12 Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (в ред. Федерального закона от 06.07.2016 № 374-ФЗ) // Соб. законодательства Российской Федерации. –2013. № 28. ст. 2895; 2016. № 28. ст.4558.

13 Федеральный закон от 13.05.2008 № 68-ФЗ «О центрах исторического наследия президентов Российской Федерации, прекративших исполнение своих полномочий» (в ред. Федерального закона от 23.06.2014 № 171-ФЗ) // Соб. законодательства Российской Федерации. –2008. № 20. ст. 2253; 2014. № 26 (1 ч.).ст. 3377.

14 Закон Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне» (в ред. Федерального закона от 08.03.2015 № 23-ФЗ) // Соб. законодательства Российской Федерации. – 1997. № 41. ст. 4673; 2015. № 10. ст. 1393.

15 Постановление Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда Российской Федерации. – 2008. № 2, стр. 3.

16 Постановление Пленума Верховного Суда РФ от 9.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных пре-

ступлениях» (в ред. Постановления Пленума Верховного Суда от 03.12.2013 № 33) // Бюллетень Верховного Суда Российской Федерации. – 2013. № 9. стр. 2; 2014. № 2. стр. 3-4.

17 Постановление Пленума Верховного Суда РФ от 17.12.2015 № 56 «О судебной практике по делам о вымогательстве (статья 163 Уголовного кодекса Российской Федерации)»// Бюллетень Верховного Суда Российской Федерации. – 2016. – № 2. –С. 15.

18 Постановление Правительства РФ от 29.06.1995 № 653 «О заключении соглашений о сотрудничестве между Министерством внутренних дел Российской Федерации и компетентными ведомствами иностранных государств» (в ред. Постановления Правительства РФ от 12.04.2010 № 227) // Соб. законодательства Российской Федерации. –1995. № 28. ст. 2705; 2010. № 16. ст.1914.

19 Указ Президента РФ от 18.04.1996 № 567 «О координации деятельности правоохранительных органов по борьбе с преступностью» (ред. Указа Президента РФ от 07.12.2016) // Соб. законодательства Российской Федерации. – 1996. № 17. ст. 1958; 2016. № 50. ст.7077.

20 Указ Президента РФ от 06.03 1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (ред. Указа Президента РФ от 13 июля 2015 года) // Соб. законодательства Российской Федерации. –1997. № 10. ст. 1127; 2015. № 29 (2 ч.).ст.4973.

21 Указ Президента РФ от 05.12. 2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»// Соб. законодательства Российской Федерации. – 2016. – №50. – ст. 7074.

22 Приказ МВД РФ, Минюста РФ, ФСБ РФ, Федеральной службы охраны РФ, Федеральной службы РФ по контролю за оборотом наркотиков и Федеральной таможенной службы от 06.10.2006 № 786/310/470/454/333/971 «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» (ред. Приказа МВД РФ, Минюста РФ, ФСБ РФ, Федеральной службы охраны РФ, Федеральной службы РФ по контролю за оборотом наркотиков и Федеральной таможенной службыот 22.09.2009 №

727/302/480/570/425/1739) //Бюллетень нормативных актов федеральных органов исполнительной власти. – 2006.№ 47. ст.3; 2009. № 44.

23 Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации[Электронный ресурс]: Утвержденные Генеральной прокуратурой РФ. Доступ из справ.- правовой системы «Гарант».

II Специальная литература

24 Безверхов, А.Г. Мошенничество и его виды: вопросы законодательной регламентации и квалификации / А.Г. Безверхов//Уголовное право. – 2015. – № 5. – С. 9-15.

25 Быков, В.Новая редакция ст.274 УК / В. Быков, В. Черкасов // Законность. – 2012. – № 11. –С.25-28.

26 Быков, В. Понятие компьютерной информации как объекта преступлений / В. Быков, В. Черкасов // Законность. – 2013. – № 12. –С.37-40.

27 Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волевозд.– М.: Изд-во Юрлитинформ, 2001. –496с.

28 Воробьев, А.В. Создание системы защиты информации в составе информационно-технологической инфраструктуры МВД России с учетом ее «облачной архитектуры» / А.В. Воробьев, В.В. Поваров// Информационные технологии, связь и защита информации МВД РОССИИ. – 2015, – С.50-52.

29 Гребельский, А.В. Электронные доказательства в международном коммерческом арбитраже / А.В. Гребельский//Закон. – 2015. – №10. – С. 59-70.

30 Жарова, А.К. Право и информационные конфликты в информационно-телекоммуникационной сфере [Электронный ресурс]: монография / А.К. Жарова. – М.: Янус-К, 2016. – 248 с. Доступ из справ.- правовой системы «Гарант».

31 Кириллова, Н.П. Проблемы осуществления уголовного преследования по делам о преступлениях, совершаемых в сфере высоких информационных технологий / Н.П. Кирилова, С.П.Кушниренко // Правоведение. – 2013. – № 3. – С. 79-80.

32 Киселев, А.П. Комментарий к Федеральному закону от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» [Электронный ресурс]: О.А.Васильев, Ю.В.Белянинова. Доступ из справ.- правовой системы «Гарант».

33 Криминалистическая методика для дознавателей[Электронный ресурс]: учебник для вузов / под ред. А.Г. Филиппова. – М.:Юрайт, 2015. – 326 с. Доступ из справ.- правовой системы «Гарант»

34 Коцыняк, М.А.Киберустойчивость информационно-телекоммуникационной сети / М.А.Коцыняк, М.М. Коцыняк, О.С. Лаута, А.С. Лаута// Информационные технологии, связь и защита информации МВД РОССИИ. – 2015, –С.104 – 105.

35 Кудрявцев, В.Л. Преступления в сфере компьютерной информации: общая характеристика / В.Л. Кудрявцев // Уголовное законодательство в XXI веке: современное состояние, проблемы трактовки и применения его положений с учетом задач дальнейшего укрепления экономического правопорядка. Материалы международной научно-практической конференции (Нижний Новгород, 1 марта 2012 года).– Нижний Новгород: НИУ ВШЭ - Нижний Новгород, 2012. – С. 69-76.

36 Лебедев, В.Н.Некоторые теоретические аспекты защиты персональных данных в органах внутренних дел / В.Н. Лебедев // Информационные технологии, связь и защита информации МВД РОССИИ. – 2015, – С.92 – 96.

37 Лопатина, Т.М. Условно-цифровое вымогательство, или кибершантаж/ Т.М. Лопатина // Журнал российского права. – 2015. – № 1. – С. 118-126.

38 Лысак, Е.А. Проблемы квалификации преступлений в сфере компьютерной информации / Е.А. Лысак // Научный журнал КубГАУ, – 2013. – № 90. – С 36-41.

39 Степанов-Егиянц, В. Содержание термина «неправомерный доступ к компьютерной информации» в уголовном праве / В. Степанов-Егиянц// Право и экономика. – 2014. – № 8. – С. 22-45.

40 Суслопаров, А.В.Эволюция института ответственности за компьютерные преступления / А.В. Суслопаров; [Электронный ресурс]. Доступ из справ.-правовой системы «Гарант».

41 Третьяк, М.И. Правила квалификации компьютерного мошенничества и преступлений, предусмотренных гл.28 УК РФ / М.И. Третьяк // Уголовное право. – 2014. – № 4. – С. 69-74.

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

43 Третьяк, М.И. Проблемы квалификации новых способов мошенничества / М.И. Третьяк // Уголовное право. – 2015. – № 2. – С. 94-98.

44 Уголовное право Армении и России. Общая и Особенная части[Электронный ресурс]: учеб.пособие / под ред. С.С. Аветисян, А.И. Чучаев; М.: Контракт, 2014. – 421 с. Доступ из справ.- правовой системы «Гарант».

45 Уголовное право России. Общая часть [Электронный ресурс]:учебник / подред. В.П.Ревина; М.:Юстицинформ, 2009. – 312 с. Доступ из справ.- правовой системы «Гарант».

46 Уголовный процесс: учебник / под ред. В.П. Божьева. – М.: Высшее образование, 2009. – 291 с.

47 Хилюта, В.В. Уголовная ответственность за хищения с использованием компьютерной техники / В.В. Хилюта // Журнал российского права. – 2014. – № 3. – С.111-118.

48 Ходорыч, А. Карты военных действий [Электронный ресурс] // Журнал «Коммерсантъ Деньги» №19 от 19.05.2003. – Режим доступа: http://www.kommersant.ru/doc/382608. – 05.01.2017

49 Шаповалова, Г.М., Шаповалов В.В. Криминалистика и ее роль в предупреждении преступлений на основе информационных технологий/ Г.М. Шаповалова, В.В. Шаповалов // Полицейская деятельность. – 2016. – № 2. – С. 187-197.

50 Шевченко, Е.С. Актуальные проблемы компьютерных преступлений / Е.С. Шевченко // Журнал «Актуальные проблемы российского права»: [Электронный ресурс]. Доступ из справ.- правовой системы «Гарант».

51 Шевченко, Е.С. Тактика производства следственных действий при расследовании киберпреступлений [Электронный ресурс]: автореф.дис. на соискание учёной степени кандидата юридических наук / Е.С.Шевченко;Моск.гос.юр. ун-т имени О.Е. Кутафина. –М., 2016. Режим доступа: https://msal.ru/common/upload/SHevchenko_E.S.pdf. – 25.11.2016.

52 Шевченко, Е.С. Социально-технологические детерминанты следственных действий при расследовании киберпреступлений [Электронный ресурс]: Журнал «Актуальные проблемы российского права» /Е.С. Шевченко. Доступ из справ.- правовой системы «Гарант».