Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет»
(Национальный исследовательский университет)
Юридический институт
Кафедра «Уголовное и уголовно-исполнительное право, криминология»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ И ЕЁ ХАРАКТЕРИСТИКА

ЮУрГУ – 40.03.01.2015.554.ВКР

Руководитель выпускной
квалификационной работы
Кириенко Михаил Сергеевич,
к.ю.н., доцент кафедры
_____
_____2020г.
Автор выпускной
квалификационной работы
Кононенко Александра
Андреевна,
_____
_____ 2020г.
Нормоконтролер
Кухтина Татьяна Владимировна,
старший преподаватель кафедры
_____
_____2020г.

Челябинск 2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Информационные технологии все глубже проникают практически во все сферы общественной жизни и благодаря этому развитию начинают играть более весомую роль в общественных отношениях. В России продолжительное время осуществляются радикальные социально-экономические реформы, идет процесс демократизации всех сторон общественной жизни. Такой процесс невозможен без становления нового социального порядка, укрепления законности, обеспечения надежной охраны конституционных прав и свобод граждан. Развитие высоких технологий позволяет каждой второй семье приобрести персональный компьютер, сотовый телефон, модем и другие средства связи, что в свою очередь приводит к появлению новых форм и видов злоупотреблений техническими средствами, в том числе преступных посягательств. Это проявляется в том, что преступные сообщества начинают активно использовать в своей противоправной деятельности новейшие информационные технологии и компьютерную технику, достижения науки и техники, в том числе основанные на кибернетике. Компьютеризация, развитие информационных технологий, привели к возникновению, закреплению и криминализации в современной России нового вида преступных посягательств, ранее не известных науке, которые связанные с использованием средств компьютерной техники, - так называемых компьютерных преступлений. Однако, несмотря на новизну данного вида преступлений для отечественного уголовного законодательства, в государствах с высоким уровнем технологического развития проблема борьбы с компьютерной преступностью давно признана одной из первостепенных задач, важность которой неуклонно возрастает. Таким образом, возникла необходимость комплексного исследования криминализированных составов компьютерных преступлений, их состояние и тенденций развития.

Однако, несмотря на теоретическую и практическую значимость указанных исследований, в них не рассмотрены многие проблемы эффективности уголовного закона в сфере борьбы с компьютерными преступлениями.

Эффективность действия уголовного закона зависит от того, насколько быстро и полно будут раскрыты и квалифицированы эти преступления, обеспечено при этом обоснованное привлечение виновных к уголовной ответственности или освобождение от таковой с учетом требований целесообразности (в предусмотренных законом формах).

Все указанное выше обусловливает актуальность и причины выбора темы исследования.

Цель дипломной работы - комплексное изучение уголовно-правовых аспектов преступлений, в сфере компьютерной информации теоретических исследований, внесение предложений по совершенствованию законодательства, предусматривающего уголовную ответственность за преступления в сфере компьютерной информации; выявление возможных путей повышения эффективности применения практическими работниками системы уголовно-правовых.

Указанная цель предопределила постановку следующих взаимосвязанных задач:

• изучить российского исторического опыта и опыта зарубежных стран по правовому регулированию преступлений в сфере компьютерной информации;

• рассмотреть понятия преступлений в сфере компьютерной информации;

• проанализировать уголовно-правовые запреты, устанавливающие уголовную ответственность за преступления в сфере компьютерной информации, выявление особенностей квалификации преступлений в сфере компьютерной информации;

Объектом данной работы являются общественные отношения, регулируемые нормами уголовного законодательства, которые возникают между субъектами в процессе совершения преступлений в сфере компьютерной информации.

Предметом исследования выступают нормы Конституции РФ, Уголовно-процессуального кодекса РФ, Уголовного кодекса РФ, федеральных конституционных законов, уголовного законодательства зарубежных стран, иных нормативно-правовых актов, теоретические труды по теме исследования и

практические аспекты, касающиеся механизма определения квалификации преступлений в сфере компьютерной информации, ее основных элементов и порядка применения в деятельности правоохранительных органов и суда.

Теоретическую основу исследования составили труды следующих авторов:Ю.М. Батурина, В.А. Бессонова, В.Б. Вехова, П.Б. Гудкова, В.Д. Зеленский,В.В. Крылова, В.Д. Курушина, В.Д. Ларичева, Ю. Ляпунова, В.Ю. Максимова, Н.С. Полевого, Л.А. Прохорова, А.В, Славнова,Т.Г. Смирновой, Е.А. Суханова, С.И. Ушакова, В.Н. Черкассов,А.А. Харкевич, Л.И. Шершнева, Н.И. Шумилова,В.Ф. Щепельков и др.

Методологическую основу исследования составили положения общенаучного диалектического метода познания, а также вытекающие из него частно-научные методы: метод системного анализа теоретических работ, действующего законодательства, практики его применения и судебной статистики, формально-логического метода толкования права и другие.

Нормативной базой являются акты законодательства: Конституция Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, Уголовный кодекс Российской Федерации, ранее действующее законодательство России, федеральное законодательство, уголовное законодательство зарубежных стран, постановления пленумов Верховного Суда Российской Федерации, регулирующие процесс квалификации преступлений в сфере компьютерной информации.

Эмпирической базой послужили результаты практической деятельности судов Российской Федерации, выраженные в принятых ими судебных актах, а также статистические показатели работы этих судов.

Структура работы определяется целями и задачами исследования и включает в себя введение, две главы, шесть параграфов, заключение, библиографический список.

ГЛАВА 1 ОБЩАЯ СОЦИАЛЬНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1 Понятие преступлений в сфере компьютерной информации. Виды преступлений в компьютерной деятельности.

Понятие «компьютерные преступления» впервые появилось в зарубежной литературе вначале 60-х гг. и получило широкое распространение в связи с тем, что компьютерные технологии стали приходить в обиход всего общества, с чем связан и рост посягательств в данной сфере преступлений. Однако в России данный термин не имеет однозначного понимания, так:

- Ю.М. Батурин и А.М. Жодзишский утверждают, что «компьютерных преступлений, как преступлений специфических в юридическом смысле, не существует» , то есть они являются сторонниками позиции о том, что включенная в УК РФ гл. 28 было ошибочно.

- В.Б. Вехов, Ю.И. Ляпунов, В.Ю. Максимов, Н.А. Селиванов и др. термин «компьютерные преступления» целесообразней воспринимать в криминологическом и криминалистическом аспектах, например в случаях, когда речь идет о личности преступника; о способе совершения преступления.

- В.А. Копылов, В.В. Крылов, В.А. Пархомов и др. объединяют под «компьютерные преступления» все информационные преступления. Однако, в таком случае весь УК РФ можно будет объединить в один раздел с преступлениями в отношении информации, так как большинство преступлений касается информационной сферы и заключаются в распространении запрещенной или заведомо ложной информации, либо в непредставлении сведений. Поэтому такое обширное понятие будет достаточно ошибочным к закреплению его в законе.

Также стоит отметить, что в 1993г. координационным бюро по криминалистике при НИИ «Компьютерные преступления» были определены как «предусмотренные законом общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного

посягательства». Однако УК РФ было дополнено 28 главой как «Преступления в сфере компьютерной информации». Данные составы были введены в УК РФ по традиционному подходу, то есть по разграничению по объектам преступления. Так, в данных составах законодатель делает акцент не на компьютере как орудие совершения преступления, а как на объект об информационных отношениях, которые складываются в процессе создания, обработки, накопления, хранения, поиска, распространения и предоставления, а также создания и использования информационных технологий, средств их обеспечения и, главным образом, защиты охраняемой законом компьютерной информации.

В настоящее время также отсутствует общее понятие «Компьютерных преступлений», однако в некоторых международных актах употребляется термин «Преступления в сфере компьютерной информации». Так, в Соглашении о сотрудничестве государств-участников СНГ в борьбе с преступлениями в данной сфере закреплено понятие «Преступление в сфере компьютерной информации – уголовно наказуемое деяние, предметом которого является компьютерная информация». Однако, закрепляя данный термин, вводится некое ограничение и при квалификации преступлений, так преступления, совершенные с других устройств, уже не будут попадать под данный вид преступлений, так как уже будет отсутствовать один из элементов преступления, предмет преступления – компьютер.

В литературе уголовного права предложены различные определения данного понятия, например, Комиссаров В.С. под «преступлениями в сфере компьютерной информации» понимает «умышленные общественно опасные деяния, причиняющие вред либо создающие угрозу причинения вреда общественным отношениям, регламентирующим безопасное производство, хранение, использование или распространение информации и информационных ресурсов либо их защиту». Данное определение указывает на то, что данный вид преступлений достаточно опасен, и влечет за собой высокую латентность.

В свою очередь, М.Ю. Дворецкий и В.В. Крылов предложили иной подход к данному понятию, в связи с тем, что компьютер это лишь один из видов технического устройства, где содержится информация. Поэтому ими были предложены такие понятия как: «преступления в сфере информационных ресурсов» - М.Ю. Дворецкий, и В.В. Крылов предложил использовать термин «информационные преступления» , где не указаны конкретные технические устройства, что позволит и в дальнейшем использовать данные термины, когда устройств по хранению информации будет великое множество.

Как отмечает Дмитрий Владимирович, понятие «преступления в сфере компьютерной информации», «не дает возможности четко определить конкретный вид преступлений, что приводит к неоднозначности», в связи с тем, что компьютеры в современном мире используются уже во всех сферах жизнедеятельности общества. В связи, с чем Д.В. Добровольский, основываясь на теории Дворецкого и Крылова, предложил свое видение, обозначив его термином «преступления в сфере информационных технологий, предусмотренные уголовным законом виновные общественно опасные деяния, направленные на нарушение неприкосновенности охраняемой законом электронной информации и ее материальных носителей, совершаемые в процессе создания, использования и распространения электронной информации, а также направленные на нарушение работы ЭВМ, системы ЭВМ или их сети, причиняющие вред законным интересам собственников или владельцев, жизни здоровью, правам и свободам человека и гражданина, национальной безопасности». Однако, принимая во внимание данный термин, и применяя их к уголовному законодательству РФ, можно столкнуться с проблемой выделения нового раздела в УК РФ. Так как данное понятие охватывает новый объект преступления и уже касается не «общественной безопасности и общественного порядка», а затрагивает такие общественные отношения как «Безопасность в сфере информационных технологий», применимые к правам и интересам личности, общества и государства.

На мировом уровне часто используется термин «Киберпреступность» является широким в своем смысле куда также входят понятия «преступления в сфере компьютерной информации», «информационные преступления», «преступления, связанные с компьютерными техническими средствами», «преступления в высоких компьютерных технологиях», «преступления в информационном пространстве» и др. В РФ пробовали привить данное понятие к законодательству, соглашаясь с тем, что данное понятие точно и полно определяет преступность в информационном пространстве. Д.Н. Карпова в своей статье раскрывает понятие «киберпреступление», отражая в нем по большей мере социально-экономические проблемы, подразумевая под ним «акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба, индивиду, организации или государству посредствам любого технического средства с доступом в Интернет».

Понятие «компьютерная преступность» раскрывается как в широком, так и в узком смыслах. В широком смысле принято воспринимать «компьютерную преступность» как: «компьютерная преступность представляет собой совокупность преступлений, где основным непосредственным объектом преступного посягательства выступают общественные отношения в сфере компьютерной информации и информационных технологий, безопасного функционировании средств создания, хранения, обработки, передачи, защиты компьютерной информации, но при этом компьютерная информация, информационно-телекоммуникационные сети, средства создания, хранения, обработки, передачи компьютерной информации (компьютеры, телефоны, кассовые аппараты, банкоматы, платежные терминалы, и иные технологии) являются не только предметами преступного деяния, но и используются в качестве средства и орудия совершения преступления». А в узком смысле под «компьютерной преступностью» понимают те преступления, где объектом выступают охраняемые законом общественные отношения в сфере безопасного создания, хранения, обработки и передачи компьютерной информации, а

предметом таких преступлений является непосредственно сама компьютерная информация, средства защиты компьютерной информации, информационно-телекоммуникационные сети, средства хранения, обработки и передачи компьютерной информации» - такое определение полностью совпадает с определением данным законодателем РФ.

Для эффективной борьбы с преступлениями в сфере компьютерной информации, необходимо также четко понимать, что такое информационно-телекоммуникационная сеть, телекоммуникационные системы, компьютерная информация, носители компьютерной информации и т.п. Все основные понятия, касающиеся данной сферы, закреплены в ст. 2 ФЗ №149 «Об информации, информационных технологиях и о защите информации». В УК РФ в декабре 2011г. было добавлено примечание: «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Данным понятие законодатель опять же сузил круг преступлений попадающих под состав ст. 272 УК РФ, так как информация также может передаваться с помощью световых сигналов, либо с помощью электромагнитного излучения. Например, в случае, если хакерская атака будет совершаться с помощью переноса света внутри нитей (оптоволокна), то данное деяние нельзя будет квалифицировать по данной статье, ввиду того что, данный способ передачи информации не предусмотрен составом преступления.

Таким образом, изменения и уточнения в понятии «компьютерные преступления» необходимы для внесения их законодателем, так как позволит точно дополнять главу новыми составами, при появлении новых форм преступлений.

Стоит также учитывать данные из института судебных экспертиз и криминалистики, согласно которым в апреле 2015г. по март 2016г. со счетов российских банков было украдено порядка 348,6 млн. рублей, в сравнении с предыдущими годами показатели таких хищений возросло в 5 раз. Что

подтверждает мнение о том, что данный вид преступлений в современном обществе набирает стремительные обороты. Большому вниманию подлежат и способы защиты компьютерной информации, согласно анализам сделанными экспертами на основе того, что в 2016г. похищено с банковских карт российских граждан 650 млн. рублей, по прогнозам сделанными экспертами сумма в 2017г. возрастет до 750 млн. руб., используя при этом метод социальной инженерии. Итак, уже по итогам первого полугодия в 2017г. было похищено 550 млн. рублей.

Как было отмечено М.В. Кузнецовой и И.В. Симдяновой в книге «Социальная инженерия и социальные хакеры» под «социальной инженерией понимается манипулирование человеком или группой людей с целью взлома систем безопасности и похищения важной информации». Данный метод, совершения преступления является достаточно бюджетным вариантом, а также позволяющий действовать на небольшом количестве знаний о компьютерных технологиях. Этой же точки зрения придерживаются и глава отдела информационной безопасности корпорации Gartner – Рич Могулл и управляющий директор регионального подразделения антивирусной компании Sophos Роб Форсайт, называя его «новый циничный вид мошенничества».

Киберпреступления развиваются во множествах сфер, затрагивая различные виды правоотношений. Самыми распространенными считаются:

1) Преступления в финансовой сфере к ним относятся различного рода хищения (мошенничество с кредитными картами, хищение денежных средств в ходе банковских операций и др.);

2) Фишинг используется при совершении услуги интернет-банкинга. Разновидностью данного вида считается целевой фишинг, при котором потенциальным жертвам в ходе сообщения предлагается открыть какой-либо файл или дана ссылка на какой-либо сайт, где непосредственно находится вредоносный код. Еще одним видом является «Фарминг – процедура скрытного перенаправления жертвы на ложный IP-адрес.

3) Удаленный взлом компьютера, с помощью которого злоумышленник может уничтожить, блокировать, модифицировать либо скопировать любую информацию, находящуюся на этом компьютере (информационном носителе);

4) Кибер-порнография, затрагивает права населения в отношении общественной нравственности;

5) Кибер-торговля наркотиками – отношения, касающиеся здоровья населения;

6) Кибертерроризм – затрагивает отношения о безопасности всего человечества, ярким примером стала игра «Синий кит», с которой столкнулись множества стран: Украина, Болгария, Латвия, Италия, Ближний Восток, США и в том числе Россия.

Исходя из этих видов преступлений, можно прийти к выводу, что преступления в сфере технологий, затрагивают все общественные отношения. Таким образом, можно смело говорить, что «Киберпреступление – это совокупность преступлений, которые запрещены законом, совершаемые в киберпространстве, затрагивающие такие общественные отношения как:

- конституционные права и свободы человека и гражданина;
- в сфере компьютерной информации и информационных технологий;
- в сфере экономики и экономической деятельности;
- в сфере государственной власти;
- в сфере здоровья населения и общественной нравственности.

То есть данный вид преступлений по российскому законодательству не может содержаться в одной главе, так как затрагивает большой ряд преступлений в различных общественных отношениях. Поэтому в УК РФ введены квалифицирующие составы преступлений таких как:

1) Нарушение авторских и смежных прав – ст. 146 УК РФ;

2) Мошенничество – ст. 159 УК РФ;

3) Незаконное изготовление и оборот порнографических материалов или предметов – ст. 242 УК РФ.

Однако с таким активным развитием киберпреступлений, законодателю стоит учесть все способы совершения преступления во всех сферах деятельности, в том числе дополнить некоторыми составами главу 28 УК РФ.

1.2 Развития законодательства об уголовной ответственности за преступления в сфере компьютерной информации

Общество не стоит на месте и вместе с ним развиваются общественные сферы деятельности. Так, с появлением компьютера и интернета стали появляться новые виды деятельности, стала развиваться компьютерная информация как способ развития деятельности. Также стоит отметить, что компьютерная информация, начиная с 80-х годов, получило свое развитие и не останавливается до сих пор. С развитием данной сферы появился и новый вид общественных отношений, а с ним и общественно опасные поведения, такие как преступления в сфере компьютерной информации. И вот, в 1979г. было зафиксировано первое компьютерное преступление, причинившее ущерб в 80 тыс. рублей СССР, прогремевшее на весь мир, которое было зарегистрировано Международной организацией уголовной полиции «Интерпол» в г.Вильнюсе. Преступление было совершено оператором почтовой связи путем мошенничества с использованием автоматизированного программно-технического комплекса «Онега», с помощью чего, совершалось хищение денежных средств у СССР.

Итак, началось развитие законодательства по защите прав и свобод человека в компьютерной сфере, которое можно разделить на два этапа.

Первый этап затрагивает правовое регулирование в НПА, которые закрепляли основные положения информационного обеспечения инновационной деятельности. Как и во всех сферах, основным источником послужили положения Конституции РФ, в которой в свою очередь закреплено «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» – ст. 29 Конституции РФ . В статьях 23,24,56 Конституции РФ также закреплены положения о защите прав граждан, организаций и государства на тайну, что обязывает законодателя в каждом конкретном случае

находить баланс между обеспечением тайны и обеспечением права на информацию .

Важным моментом в развитии правовых норм, регулирующих отношения в сфере компьютерной информации, было признание России в сети Интернет, в связи с тем, что в 1994 году был зарегистрирован домен RU, то есть появление Рунета.

Итак, уже с 1991г. были приняты федеральные законы регулирования правоотношений в информационной деятельности в различных сферах, например ФЗ о СМИ №2124-1, Патентный закон № 3517-1, а также затрагивающие правовую охрану в топологии интегральных микросхем, программ для ЭВМ и баз данных, хотя основные приходятся на 1995г.: ФЗ от 16.02.1995г. №15 «О связи», ФЗ от 20.02.1995г. №24 «Об информации, информатизации и защите информации», где понятие информации закрепляло – «сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления» . Эти же законы решали вопрос правового отношения в сфере обмена информации и обработки информации с помощью новых информационных технологий. А также давали правовое значение основных компонентов информационной технологии таких, как объектов правовой охраны, определяли категории доступа определенных субъектов к конкретным видам информации, устанавливали и определяли права и обязанности собственника на объекты правовой охраны.

Большую роль в правовом регулировании имел Указ Президента РФ №334 от 3 апреля 1995г. «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», который в свою очередь был направлен на усиление борьбы с организованной преступностью и повышение защищенности информационно-телекоммуникационных систем органов государственной власти, российских кредитно-финансовых структур, предприятии и организаций. Также 26 июня 1995г. было принято Постановление

Правительства РФ № 608 «О сертификации средств защиты информации», целью которого было реализация положений Указа Президента РФ. Таким образом, Постановлением Правительства появились обязательства у соответствующих министерств и ведомств о разработке и введении Положений, определяющих систему сертификации, порядок производства средств, порядок оплаты услуг по их разработке, установке и эксплуатации и т.д.

Информационная сфера также затронула и международные отношения России, в связи, с чем обеспечение информационной безопасности было рассмотрено на международном уровне. Так, был принят ФЗ №85 от 4.07.1996г. «Об участии в международном информационном обмене», в котором устанавливается ответственность за предоставление ложной информации при международном обмене (ст.14) и предусматривает ответственность как гражданско-правового характера, так и административного и уголовного за противоправный обмен на территории РФ (ст.20).

Однако, учитывая все преимущества данных правовых актов принятых до 1997г., к сожалению, они не устанавливали уголовно-правовые средства защиты, то есть об эффективности правовой системы защиты компьютерной информации говорить было рано. Поэтому второй этап развития законодательства начинается с введением в УК РФ 1996г. - главу 28 Преступления в сфере компьютерной информации, куда входило всего три нормы, предусматривающие уголовную ответственность.

Некие изменения были внесены и в саму структуру органов внутренних дел. Так, до 1999г. были созданы структурные подразделения – отделы БПСВТ. А в 1999г. благодаря Распоряжению Правительства РФ №1701-р от 22.10.99г. «Об усилении борьбы с преступлениями в сфере высоких технологий и реализации международных договоренностей и обязательств РФ» были выделены бюджетные средства для борьбы с преступностью в рамках Федеральной программы. Также были организованы и проведены международные семинары и конференции по борьбе с компьютерными преступлениями, налажено взаимодействие со

специальными службами зарубежных стран. Итогом чего было достижение нового более высокого уровня в противодействии против компьютерных преступлений в России и на мировом уровне.

А уже 9 сентября 2000г. Президент РФ утвердил «Доктрина Информационной Безопасности РФ», которая устанавливала национальные интересы РФ в информационной сфере и их обеспечение, выделял разновидности и источники угроз информационной безопасности РФ, выделялись методы, которые обеспечивали информационную безопасность РФ во многих сферах общественной жизни. В этой же доктрине были утверждены основные положения государственной политики по обеспечению информационной безопасности РФ и мероприятия, которые должны быть проведены в первую очередь для ее реализации. Положения Доктрины были направлены на защиту от несанкционированного доступа, затрагивающие информационные ресурсы как уже созданные, так и создаваемые на территории России.

С развитием информационных технологий, интернета, все сферы деятельности стали компьютеризированными, что послужило принятию таких федеральных законов, как: «Об электронной цифровой подписи», «О противодействии экстремистской деятельности», «О государственной автоматизированной системе РФ «Выборы» и др.

Был принят ФЗ №126 «О связи» от 07.07.2003г., который устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

В 2011г. были также внесены нововведения в УК РФ, так появился квалифицирующий признак в статье 272 - корыстная заинтересованность. А в ч.3 статьи 273 предусматривает неосторожное причинение тяжких последствий, при этом санкция предусматривает самое строгое наказание равное до семи лет

лишения свободы. И в 2016 году в связи с участившимся, неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации был принят Федеральный закон "О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 194-ФЗ, то есть появился новый состав преступления в сфере компьютерной информации - неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации статья 274.1 УК РФ.

Таким образом, можно прийти к выводу, что законодательство РФ начало формироваться с 1991 года в сфере компьютерной информации, однако, на первом этапе формирования не было предусмотрена ответственность уголовно-правового характера, то есть правовая система по защите информации в компьютерной сфере не была эффективной. Поэтому важным моментом в формировании законодательства по защите информационной безопасности считается принятие новых норм и введение дополнительной главы в УК РФ.

Существующая в действующем УК РФ система преступлений в сфере компьютерной информации является, с одной стороны, основополагающей для отечественного правоприменителя в силу ее прагматичности, с другой стороны — требует дальнейшего развития путем совершенствования юридических конструкций и признаков имеющихся составов преступлений, а также включения новых преступлений, отражающих современные потребности уголовно-правовой охраны компьютерной информации. Кроме того, отечественному законодателю, а также специалистам в области уголовного права и криминологии, необходимо находится в постоянной динамике, чутко реагируя на любые изменения в сфере компьютерных преступлений и преступлений в сфере высоких технологий, как в России, так и за рубежом. Только таким образом можно привести российское уголовное законодательство в соответствие с быстро развивающимися

технологиями и получить надежную правовую защиту от компьютерной преступности.

1.3 Уголовная ответственность за преступления в сфере компьютерной информации по законодательству зарубежных стран

Многие страны стали задумываться о правовой защите компьютерной информации, поэтому в 1983-85 гг. в организации экономического сотрудничества и развития был создан специальный комитет для обсуждения возможности согласования уголовного законодательства об ответственности за компьютерные преступления.

13 сентября 1989г. комитет экспертов по компьютерным преступлениям Совета Европы принял Рекомендацию №R89(9), где определял перечень компьютерных преступлений:

1) Компьютерное мошенничество;

2) Компьютерный подлог;

3) Причинение ущерба компьютерным данным, программам;

4) Компьютерный саботаж;

5) Несанкционированный доступ, перехват, воспроизведение охраняемой авторским правом компьютерной программы, а также несанкционированное воспроизведение микросхемы.

А также включался принцип ясности, однако не все государства основывают свое законодательство на данном принципе, куда, в том числе входит и Россия. Поэтому в 1995г. была издана вторая рекомендация, включающая в себя идею о разработки международной Конвенции, где были закреплены и процессуальные аспекты решения проблемы с киберпреступностью, которая вступила в силу 1 июля 2004г.

Стоит отметить, что первые преступления в сфере компьютерной информации были зафиксированы в конце 60-70-х годов, которые были совершены в США путем мошенничества, с помощью расшифровки кода были переведены деньги на собственные счета, также было зарегистрировано преступление в сфере

налоговых правоотношений с помощью доступа к ЭВМ. Столкнувшись с новым видом преступлений стали разрабатываться способы решения и урегулирования таких преступлений. Первым способом пресечения послужили прежние составы такие как: мошенничество, кража, присвоение, злоупотребление доверием, однако вскоре столкнулись с проблемой, понимание того что, что не имеет возможности данные деяния квалифицировать как данные составы преступления. Так, например, компьютерное мошенничество, попадающая под состав кражи, так как совершается путем обмана компьютера кража денег, различие этих двух составов заключается в том, что деньги в составе кражи являются материальным предметом, а в компьютерном мошенничестве выступают как информация на компьютерном носители, то есть, нет предмета преступления кражи. Также в случае разграничения с составом о мошенничестве, отсутствует объект воздействия, в случае с компьютерным мошенничеством обману подвергается компьютер, а не лицо. В связи с чем, стали предпринимать попытки урегулирования данную сферу отношений.

Первым государством, которое закрепило уголовную ответственность за компьютерные преступления, была Швеция в 1973г, закрепив такие составы как: незаконное проникновение в компьютерную систему и введение в компьютерную информацию ложных сведений, с помощью которых производится хищение денег, ценных бумаг, имущества, услуг либо ценной информации.

Столкнувшись на правоприменительной практике с такими составами преступлений, которые не охраняли определенный вид правоотношений, США разрабатывает в 1977г. законопроект о защите федеральных компьютерных систем, который предусматривал уголовную ответственность за:

1) Введение заведомо ложных данных в компьютерную систему (подлог компьютерной информации);

2) Незаконное использование компьютерных устройств;

3) Внесение изменений в процессы обработки информации или нарушение этих процессов;

4) Хищение денежных средств, ценных бумаг, имущества, услуг, ценной информации, совершенное с применением возможностей компьютерных технологий или компьютерной информации.

В дальнейшем на конференции адвокатов в 1979г., были сформулированы основные составы преступлений в сфере компьютерной информации. Однако, уже в 1983г. был произведен первый арест интернет-преступника, за взлом множества компьютеров, в том числе с гос. тайной, аресту было подвергнуто шесть подростков. Начиная с 80-х годов, стало заметно увеличиваться преступность в компьютерной сфере, если в 1988г. было всего шесть обращений, то уже в 1990г. число обращений выросло до 252.

Так, в 1986г. Конгресс США принимает основной НПА, который устанавливает уголовную ответственность за преступления в сфере компьютерной информации - Закон о мошенничестве и злоупотреблении с использованием компьютеров. В этом законе был закреплен запрет на несанкционированный доступ к любой компьютерной системе и получение секретной военной информации. Закон защищал и информацию принадлежащую финансовым учреждениям, правительственным и международным и межштатовыми организациям. Были нормы, регулирующие в случае повреждения данных – распространение вирусов. В общем этот закон закреплял семь составов преступления в компьютерной сфере.

В настоящее время Конгресс США принимает меры по ужесточению наказания за данный вид преступлений, так как наказание есть мера противодействия с борьбой против неправомерных действий. Так, законодатель пришел к выводу, что нужно общественную опасность таких преступлений уравнять с реальными преступлениями, и поэтому пришел к выводу, что надо повысить сроки и размеры наказания. Также были изменения и в структуре органов США, так появился новый отдел, специализирующийся на расследовании компьютерных преступлений.

Итак, к концу 80-х и начало 90-х знаменовалось тем, что в большинстве стран был высокий уровень преступлений, совершенных в сфере компьютерной информации, поэтому в эти годы были предусмотрены меры по борьбе с хакерами. И уже в 1986г. ФРГ дополняет свой УК нормами, куда входили составы преступлений в сфере компьютерной информации, построив свой уголовный закон на основании рекомендаций ЕС. Также законодатель принимает закон об изменениях к закону, об авторском праве 1991г., с поправками о защите программного обеспечения. Хотя в УК ФРГ не было выделено отдельно взятого раздела, посвященного преступлениям против компьютерной информации, нормы, которые закрепляют уголовную ответственность за такие преступления рассредоточены по всему кодексу так: в параграфе 263 предусмотрена ответственность за компьютерное мошенничество; параграфом 270 обман при помощи ЭВМ при обработке данных, параграф 303b предусматривает уголовную ответственность за компьютерный саботаж и другие. Исходя из данных составов, можно прийти к выводу о том, что эти нормы закрепляют лишь виды простых составов преступлений, и являются одним из способов совершения преступления.

Для Великобритании, решающим моментом в принятии нормы об уголовной ответственность в данной сфере преступлений, послужило дело Стивена Гоулда и Роберта Шифрина. В 1984г. был совершен несанкционированный доступ к сервису Prestel, который принадлежал компании British Telecom, тогда суд первой инстанции вынес обвинительный приговор в соответствии с Законом о подлоге и подделках 1981г., однако апелляционной инстанцией был вынесен оправдательный приговор. Поэтому уже в 1990г. был принят Закон о неуполномоченном использовании компьютерных технологий, который был направлен против ненадлежащего использования компьютерных технологий и закреплял такие составы как:

1) Умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам (ст.1);

2) Умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам для их последующего использования в противозаконных целях (ст.2);

3) Неправомерный доступ к компьютерной информации на машинном носителе, в компьютере, компьютерной системе и сети, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютера, компьютерной системы или сети (ст. 3).

Закон устанавливал ответственность лица за использования компьютера для выполнения любой функции с намерениями обеспечить доступ к любой программе или данным, содержащимися в любом компьютере, при условии, что такой доступ заведомо неправомочен. Законом предусмотрено и место совершения преступления, так в случае если, само деяние или его последствия были совершены или наступили на территории Великобритании, то такое преступление признается оконченным в Великобритании (ст. 4-7). Такое положение обоснованно тем, что такие преступления могут совершаться и на отдаленном расстоянии, так в случае, если преступление совершалось на территории страны, где не предусматривается ответственность за данное деяние, а последствия наступили в Великобритании, то за такое деяние лицо понесет ответственность в соответствии с законодательством Великобритании.

Развитие террористических атак в том числе и с помощью компьютеров - киберпространства, заставили задуматься и о регулировании правоотношений в данной области. Поэтому в Законе о терроризме 2000г. Великобритании, в котором предусматривалась ответственность за «серьезное вмешательство или серьезное нарушение работы какой-либо электронной системы».

Развитие новых правоотношений во многих государствах сказалось на структурных подразделениях органов власти, так в Нидерландах был создан Консультативный комитет по компьютерным преступлениям, который внес явные изменения в УК и УПК Нидерландов, также разработал классификацию компьютерных преступлений. Также полицейское разведывательное управление

разграничивает преступления, посягающие на объект преступления – компьютер и преступления, где орудием признается компьютер. Так, УК Нидерландов был дополнен в 1993г. такими составами как:

1) Несанкционированный доступ в компьютерные сети, несанкционированное копирование данных (ст. 138a);

2) Компьютерный саботаж, распространение вирусов (ст. 350a, 350b);

3) Компьютерный шпионаж (ст. 273).

Также были добавлены нормы в простые составы (вымогательство, кража путем обмана, подлог банковских карточек, как квалифицирующий состав. Уголовное законодательство Нидерландов позволяет привлечь к уголовной ответственности за преступления с компьютерной информацией по различным основаниям, предусмотренными множествами составами преступлений.

Уголовное законодательство Испании предусматривает ответственность за:

1) Раскрытие и распространения тайны без согласия владельца (ст. 179);

2) Мошенничество с помощью компьютера и других ЭВМ (ст.248);

3) Распространение вируса (ст.ст.264, 270);

4) За изготовление и распространение вирусных программ (ст.400).

Стоит также заметить, что предусматривается ответственность за разные объекты посягательства, хоть и единым способом – компьютерной информации.

Уже с 1991г. законодательством Ирландии предусмотрена ответственность за преступления в сфере высоких технологий. В соответствии с Актом о криминальном ущербе, где закреплено, что ответственность несет лицо вне зависимости оттого удалось ли ему получить данные, в случае если оно имело намерение получить информацию незаконным способом как на территории Ирландии, так и вне ее, а также в получении информации, находящийся на территории Ирландии. Такие преступления в Ирландии относятся к категории небольшой тяжести и не превышает заключение до 3-х месяцев.

17 февраля 1996 г. постановлением межпарламентской ассамблеей государств-участников СНГ вводится модельный УК для государств СНГ. Данный кодекс

был рекомендательным законодательным актам, для использования при разработке национального законодательства и включал в себя семь статей против информационной безопасности. Также стоит отметить, что в УК СНГ в основном все составы относятся к категории преступлений средней тяжести, однако квалифицирующие составы, которые имеют дополнительный объект, относят к категории тяжких преступлений: неправомерное завладение информацией, сопряженное с насилием, совершенное с целью получения особо ценой информации или преступление организованной группой, сопряженное с причинением тяжкого вреда здоровью или по неосторожности смерти либо иных тяжких последствий.

Так, например УК Молдавии, предусматривает ответственность за компьютерные преступления и в отдельных уголовно-правовых нормах, таких как хищение – мошенничество и рассматривается как информационное преступление, преступление в области электросвязи, где непосредственным объектом выступают общественные отношения в сфере обеспечения безопасности информационной системы и информационной сети. Также стоит разграничивать с преступлением как подлог информационных данных, повлекший в дальнейшем извлечения материальной выгоды.

Хотелось бы также отметить, что у стран СНГ различается и конструирование норм: фальсификация компьютерной информации предусмотрена законодательством р. Азербайджан (ст. 2732 УК 1999г.) Молдовы статьей 2606; компьютерный саботаж – предусмотрено УК таких стран как Белоруссия (ст. 351), Таджикистан (ст.300), Узбекистан (ст. 2785); незаконный оборот средств, изготовленных для совершения киберпреступности – ст. 2731 УК Азербайджана. УК Казахстана предусматривает ответственность за такие преступления как: предоставление услуг для размещения Интернет-ресурсов, преследующих противоправные цели (ст. 212), а также принуждение к передаче охраняемой законом информации…(ст.209). Однако, рассматриваемые преступления содержат в себе некие признаки единого состава преступления такой, как

неправомерный доступ к компьютерной информации, то есть идет разделение на более узкие преступления, с точными последствиями, не разделяя на какие-либо альтернативные варианты последствий преступления.

А УК р. Польша не предусматривает отдельную главу посвященную данным преступлениям. Законодательный орган Польши «раскидал» по всему уголовном кодексу преступления, затрагивающие отношения в сфере компьютерной информации, так в главе «Преступления против охраны информации» упоминается о двух статьях, однако компьютер там выражается как способ получения информации, а в главе «Преступления против имущества», где компьютерная информация выступает, способом совершения преступлений с целью имущественной выгоды.

Итак, можно прийти к выводу, что в УК Польши законодатель не выделяет преступления в сфере компьютерной информации по объекту преступлений, а разделяет данный вид преступлений как способ совершения преступлений (т.е., разделяет по объективной стороне) для получения информации, либо на получение материальной выгоды.

Таким образом, зарубежное законодательство пошло по пути разграничения компьютерных преступлений в зависимости от той сферы общественных отношений, на которую посягает преступник. Так, можно выделить три большие группы, подвергнутые к изъятию информации с выгодой для лица и негативными последствиями для общества:

1) Компьютерные преступления в сфере экономики, наиболее распространенный вид преступлений: компьютерное мошенничество (параграф 263а УК ФРГ);

2) Компьютерные преступления, направленные против прав и свобод: незаконное злоупотребление информацией, находящейся на компьютерных носителях, разглашение сведений, имеющих частную, коммерческую тайну (ст. 278 УК Польши);

3) Компьютерные преступления против интересов государства и общества в целом: дезорганизация работы различных систем, изменения данных при подсчете голосов на выборах и др. (параграф 1030 а УК США).

ГЛАВА 2 УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1 Неправомерный доступ к компьютерной информации

Глава 28 уголовного кодекса открывается со ст. 272 УК РФ, определяющей уголовный запрет за неправомерный доступ к компьютерной информации.

Объектом в ст. 272 УК РФ являются общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями.

В.С. Комиссаров, доцент юридических наук, профессор, определяет под неправомерным доступом к компьютерной информации получение возможности виновным лицом на ознакомление с информацией или распоряжения ею по своему усмотрению, совершаемое без согласия собственника либо иного уполномоченного лица. Самостоятельной формой неправомерного доступа являются случаи введения в компьютерную систему, сеть или в определенный массив информации без согласия собственника этого массива или иного лица заведомо ложной информации, которая искажает смысл и направленность данного блока информации.

Отличительной чертой рассматриваемого состава преступления является предмет. Легальное определение законодатель определил как: «Компьютерная информация — информация, которая зафиксирована на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ.

Если обратится к теоретическим точкам зрения, то предмет ст. 272 УК РФ в доктрине уголовного права рассматривают как В «Толковом словаре по информатике» под электронно-вычислительной машиной (ЭВМ) понимается «…комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных

задач[1]. Следует различать ЭВМ и компьютер, поскольку первая является одним из способов воплощения второго. Сегодня термин «ЭВМ» почти вытеснен из бытового употребления и в основном используется инженерами цифровой электроники. В современном мире при нарастающем технологическом прогрессе в качестве компьютеров потенциально может рассматриваться огромный круг различных устройств, предназначенных для обработки оцифрованных данных в вид, доступный восприятию потребителем. Это всевозможные персональные компьютеры, квантовые компьютеры, серверы, ноутбуки, мобильные телефоны, смартфоны, планшеты, банкоматы и пр. Неотъемлемой частью компьютерных устройств является функция компьютерной памяти - способность длительного хранения информации. Наиболее распространены в настоящее время магнитные запоминающие устройства в пластиковых картах; USB-накопители, SSD-накопители, карты памяти в телефонах и фотоаппаратах; оптические диски, например CD, DVD, Blu-Ray; жесткие диски. Не стоит забывать про возможности буферной, временной, оперативной памяти, cache-памяти устройств, а также про подключаемые к компьютерам периферийные устройства (принтеры, сканеры, факсы и др.), которые предназначены для временного хранения данных при обмене между различными устройствами или программами либо хранения промежуточных результатов обработки. Наконец, данные могут передаваться через компьютерные устройства по техническим каналам связи в информационно-телекоммуникационных сетях, подвергаясь при этом обработке (и оставляя определенные следы) в обеспечивающих процесс передачи промежуточных сетевых устройствах (сетевых серверах, маршрутизаторах, концентраторах, модемах и др..[2] Существенную роль в определении компьютерной информации играют средства компьютерной обработки данных,

[1]Першиков В.И. Толковый словарь по информатике / В.И. Першиков, В.М. Савинков; под рецензией канд. физ.-мат. наук А.С. Маркова и д-ра физ.-мат. наук И.В. Поттосина. М.: Финансы и статистика, 1991. С. 439.

[2]Грицков С.А. Получение компьютерной информации: понятие и сущность / С.А. Грицков // URL:http://saransk.ruc.su/upload/Upload_Saransk/Studium_2017/Vipusk_3/Grickov.pdf (Дата обращения: 12.09.2018).

логика которых построена на определенных способах кодирования и декодирования. Формой представления компьютерной информации служат электрические сигналы. В теории электрической связи «…сигналом называется физический процесс, способный распространяться в пространстве и несущий в себе информацию». Если распространяемая посредством сигналов информация принимается в системе связи, она приобретает вид совокупности знаков-символов. Дальше, при поступлении сигналов в компьютер происходит их кодирование (шифрование), т.е. отражение в виде двоичного кода. Следовательно, кодированные сигналы и есть данные, содержащиеся на машинном носителе. В свою очередь, для их отражения и восприятия человеком служит обратный процесс - декодирование (дешифрование) - преобразование двоичного визуального восприятия форму. Когда данные интерпретированы и обработаны с целью определения их истинного смысла, они становятся полезны и могут быть названы информацией. Одним из криминализирующих признаков компьютерной информации будет её охраняемость.

Под охраняемую подпадает:

· информация, составляющую государственную тайну, режим защиты которой устанавливается федеральным законом;

· конфиденциальная информация, режим защиты устанавливается в основном собственником или владельцем на основании закона, а в ряде случаев федеральным законом;

· документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Режим защиты устанавливается собственником или владельцем на основании закона.Есть мнение среди юристов-теоретиков, что «под охраняемой законом информацией понимается документированная информация, для которой установлен специальный режим правовой защиты», т.е. вся информация, и содержащая государственную тайну, и конфиденциальная информация, находящаяся в ЭВМ, чтобы стать охраняемой законом, должна быть

документирована. Но придание информации статуса охраняемой законом в зависимости от формы представления, а не от содержания, нельзя признать верным. Государственная тайна остается государственной тайной, даже если на электронном документе, содержащем ее, нет электронной цифровой подписи.

Компьютерная информация может быть представлена в форме информационных ресурсов, которые в ст.2 Закона об информации [1]рассматриваются как отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах, в частности в банках данных. Эти ресурсы согласно ст. 2 Закона содержат сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [3], где банки (или базы) данных являются объективной формой представления и организации совокупности данных, систематизированных таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ

Объективная сторона предполагает деяние в виде неправомерного доступа к компьютерной информации. Как пояснили С.В. Бородин и С.В. Полубинская: в этом составе объектом преступления выступают общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями. Объективную сторону состава преступления составляет неправомерный доступ к охраняемой законом компьютерной информации. Неправомерным признается доступ к компьютерной информации лица, не обладающего правами на получение и работу с данной информацией либо компьютерной системой, в отношении которых приняты специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ. Под охраняемой законом информацией понимается информация, для которой установлен специальный режим ее правовой защиты, например государственная, служебная и коммерческая тайна, персональные данные, объекты авторского права и смежных прав. Стоит также отметить, что предметом неправомерного доступа к

[1] Федеральный закон «Об информации, информационных технологиях, и о защите информации» от 27 июля 2006 года. №149-ФЗ.

компьютерной информации является охраняемая законом компьютерная информация, под которой понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, находящиеся на машинном носителе, в ЭВМ, системе ЭВМ или их сети.

При этом, на практике встречаются случаи, когда суд оставлял представление прокурора без удовлетворения, и возвращению уголовного дела прокурору в связи с тем, что не было указаний на положения других нормативных актов, в силу которого компьютерная информация, является охраняемой законом информацией. «Таким образом, суд апелляционной инстанции считает указание на положение закона или нормативно-правовой акт, которые бы давали основание для защиты данных от несанкционированного доступа к компьютерной информации, необходимым для правильного разрешения уголовного дела, в силу чего указанное обстоятельство является не устранимым в ходе судебного разбирательства, препятствующим рассмотрению дела по существу»[1].

Объективную сторону состава преступления, предусмотренного данной статьей, составляет неправомерный доступ к охраняемой законом компьютерной информации. Под доступом к компьютерной информации понимается получение возможности воспользоваться компьютерной информацией.

Хотя законодатель и указал, что подразумевается под «компьютерной информацией» в примечании к статье «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» , но не обозначил, что подразумевается под действиями лица – под «неправомерным доступом». Однако понятие «доступ к информации» раскрывается в ФЗ «Об информации, информационных технологиях и о защите информации» в пункте 6 статье 2. Так, под «доступом информации» следует понимать – «возможность получения информации и ее пользования». Однако, на практике, правоприменители трактуют данное понятие как:

[1]Апелляционное постановление Судебной коллегии по уголовным делам ВС Республики Тыва от 26 октября 2017г. по делу № 22-1534/2017. // СПС https://sudact.ru/.

- Преодоление технических средств защиты компьютерной информации;
- Получение информации лицом, которое неуполномочено для получения данной информации;
- Получение информации, когда имеются технические ограничения, в виде паролей, логинов и т.д.

К неправомерному доступу также относят и запреты установленные законом или каким-либо локальным документом. Итак, под неправомерным доступом к компьютерной информации, принято считать, незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации, где под доступом понимается проникновение в ее источник с использованием средств компьютерной техники, позволяющие использовать полученную информацию, со всеми вытекающими ею последствиями[1,2].

Еще одной составляющей объективной стороны является охраняемость компьютерной информации российским законом, то есть те сведения, которые относятся к ограниченному доступу, то есть для которой законом установлен специальный режим ее правовой защиты. Это, например, сведения составляющие тайну, как государственного характера, так и коммерческого, служебного или иного характера, а также информация конфиденциального характера. Перечень сведений закреплен в таких правовых актах, как Указ Президента РФ от 06.03.1997г. №188 «Об утверждении Перечня сведений конфиденциального характера», это сведения:

- связанные с коммерческой деятельностью;

- с профессиональной деятельностью (врачебная, нотариальная, адвокатская тайна);

- служебные сведения – служебная тайна и др.

---

[1]"Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации"(утв. Генпрокуратурой России) // СПС КонсультантПлюс, 2014.

[2]ФЗ от 27.07.2006 №149 «Об информации, информационных технологиях и о защите информации» // СЗ, 2006. №31 (1 ч.), ст. 2.

Также перечень, указанный в Законе РФ «О государственной тайне», куда включены сведения:

- в военной области;

- сведения в области экономики, науки и техники;

- сведения в области внешней политики и экономики;

- в области противодействия терроризму и другие.

По конструкции данный состав является материальным, то есть к уголовной ответственности, лицо будет подвергаться в случае наступления последствий. Законодатель предусмотрел несколько альтернативных наступлений последствий, по которым будет привлекаться лицо к уголовной ответственности, это:

1) Уничтожение компьютерной информации- приведение ее в существенной части или полностью в непригодное для использования по назначению состояние;

2) Блокирование компьютерной информации-создание условий ее недоступности, невозможности ее надлежащего использования;

3) Модификация компьютерной информации-любые изменения компьютерной информации, в частности, внесение изменений в программы, базы данных, текстовую информацию, находящуюся на носителе;

4) Копирование компьютерной информации-неправомерный перенос информации на другой материальный носитель.

Например: В 2013 году в отдел полиции с заявлением обратился представитель Кашлинского Регионального Управления Федеральной Почтовой Связи (РУФПС). Суть заявления состояла в подозрении на внедрении в систему Кашлинского РУФПС компьютерного вируса.

В ходе проверки было установлено, что гражданин Ф., работая в должности сотрудника IT-отдела на Кашлинском Мясокомбинате, на служебном компьютере скопировал из Интернета вредоносную программу «троянский конь». Гражданин Ф. направил эту программу в виде текстового сообщения на адрес электронной почты РУФПС и при открытии сообщения программа «троянский конь»

сработала и подозреваемый завладел охраняемой законом информацией, а именно логином и паролем для подключения к сети Интернет.

Таким образом, своими умышленными действиями гражданин Ф. совершил преступление, предусмотренное ст. 272 ч. 2 УК РФ – неправомерный доступ к компьютерной информации, а также ч. 1 ст. 165 УК РФ – причинение имущественного ущерба путем обмана или злоупотребления доверием.

По результатам следствия, учитывая все обстоятельства, дело было направлено в районный суд, приговоривший обвиняемого к одному году шести месяцам лишения свободы с отбыванием заключения в колонии общего режима, а также штрафом в размере 50 тыс.руб.

При этом стоит учитывать, что законом также установлены случае, когда модификация программ является легальной, к ним относят: модификация при исправлении явных ошибок; модификация посредством внесения изменений в программы, базы данных; модификация в виде обратной разработке программ для достижения способности к взаимодействию с другими программами. Однако отсутствие одного из этих последствий к уголовной ответственности лицо не будет привлечено.

Также стоит учесть, что последствия должны наступать в случае нахождения причинно-следственной связи с действиями лица. Так, например, часто на практике встречается, что копирование компьютерной информации и сохранение на техническом устройстве в виде: КЭШа, куки и других технических данных, правоприменитель принимает как за два тождественных последствий. Однако сохранение на ЭВМ пользователя информации в виде технических данных с помощью КЭШа и куки и др., такие действия не находятся в прямой зависимости от действий лица, так как является одной из функций программного обеспечения. Таким образом, данные действия не состоят в причинной связи, поэтому лицо не будет привлечено к уголовной ответственности за данное преступление.

Лицо, привлекается к уголовной ответственность по данному составу, только в случае, когда оно осознавало общественную опасность своих действий,

предвидело возможность или неизбежность наступления общественных последствий и желало их наступления, либо не желало, но сознательно допускало наступление этих последствий либо относилось к ним безразлично. То есть когда у лица был прямой или косвенный умысел, направленный на наступление последствий, предусмотренных 272 статьей уголовного кодекса[1], а также при наступлении этих же последствий по неосторожности лица. Уголовная ответственность наступает тогда, когда лицо предвидело возможность их наступления, но без достаточных к тому оснований самонадеянно рассчитывало на их предотвращение, или если лицо не предвидело, но должно было и могло предвидеть возможность наступления этих последствий.

Так, например приговором апелляционной инстанции челябинского областного суда, был отменен приговор Усть-Катавского городского суда Челябинской области в отношении Сидякина П.Н. по предъявленному обвинению в совершении преступлений, предусмотренных ч. 2 ст. 146 УК РФ, ч. 1 ст. 272 УК РФ, ч.1 ст. 273 УК РФ, оправдать на основании п. 2 ч. 1 ст. 24 УПК РФ за отсутствием в его деянии составов преступлений. Сидякина П.Н., осужден за незаконное использование в крупном размере объектов авторского права, правообладателями которых являются Корпорация «Microsoft» и закрытое акционерное общество «АСКОН», за использование компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, а также за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию и копирование компьютерной информации. Однако, Сидякин П.Н. программу «КОМПАС-3О VI3» и файл «КОМПАС 3D VI3 AntiHASP vL0.exe» он скачал по просьбе оперативных сотрудников путем свободного доступа в Интернете, полагая, в силу отсутствия знаний об авторском праве, что это лицензия, поскольку было указано

[1]Домкин, П. Статья 272 УК РФ: Неправомерный доступ к компьютерной информации: комментарий и правоприменительная практика / П. Домкин. // СПС https://www.advodom.ru/

«Лицензия. Скачать Бесплатно». Также П.Н. Сидякин ссылается на незнание о вредоносности файла. Также суд пришел к выводу о том, «что проведенные в отношении Сидякина П.В. 08 октября 2012 года оперативно-розыскные мероприятия "проверочная закупка" носили провокационный характер и добытые при этом доказательства являются недопустимыми, то осуждение Сидякина П.Н. по ч. 2 ст. 146 УК РФ, ч. 1 ст. 272 УК РФ, ч. 1 ст. 273 УК РФ не может быть признано законным и обоснованным». Что в следствии говорит о том, что «действия Сидякина П.Н., совершенные в результате провокации преступлений, не образуют составов преступлений»[1].

Таким образом, П.Н. Сидякин не осознавал противоправность своих действий, а также не предвидел наступление таких последствий, как уничтожение, блокирование, модификацию и копирования компьютерной информации. То есть в действиях лица, по данному делу, отсутствует признак состава преступления, а именно субъективная сторона, которая выражается в форме вины.

По данной статье привлекается лицо, достигшее 16-летнего возраста, то есть по данному составу привлекается к уголовной ответственности лицо, отвечающее всем признакам общего субъекта, а именно вменяемое физическое лицо, достигшее ко времени совершения преступления 16-летнего возраста (ст.ст. 19, 20 УК РФ)[2]. Однако, частью 3 статьи 272 предусмотрена ответственность лица, относящимся к специальным субъектам, а именно, лицо, совершившее преступление с использование своего служебного положения. Где использование служебного положения, является использование компьютерной информации в результате выполняемой работы или влияния по службе на лиц, имеющих такой доступ, например, на программиста, администратор базы данных, специалисты по эксплуатации ЭВМ и пр.

Последние изменения, внесенные в главу 28 ФЗ №420 в 2011 году, дополнили статью такими квалифицирующими признаками, как: «Причинение крупного

[1]Уголовное дело № 10-479/2014 Челябинского областного суда // СПС https://sudact.ru/.
[2]Уголовный кодекс Российской Федерации от 13. 06. 1996 № 63-ФЗ // СЗ РФ, 1996. №25. Ст. 2954.

ущерба или совершение преступления из корыстной заинтересованности» - ч. 2 ст. 272 УК РФ. В той же статье было добавлено и примечание, где говорится о крупном ущербе, превышающим один миллион рублей.

На практике правоприменители сталкиваются с проблемой правильной квалификацией таких преступлений как неправомерный доступ к компьютерной информации (ст. 272 УК РФ) и составом, предусмотренным статьей 146 УК РФ – нарушение авторских и смежных прав. Проблема возникает в случае, когда лицо, посягает на компьютерную программу, которая является объектом авторского права, и используют ее в своих интересах. К основным отличия этих двух составов, является то, что объектом одного преступления является – безопасность компьютерной информации, в другом же составе, посягательство на интеллектуальную собственность. Предметы этих преступлений также не совпадает, так, ст. 272 – компьютерная информация; ст. 146 – объекты авторского права, в частности программы для ЭВМ и базы данных: Mikrosoft, Windows и др. По объективной стороне эти составы также разграничиваются, так, например: обязательным признаком в нарушении авторских и смежных прав является причинения крупного ущерба, когда в статье 272 данный признак является квалифицирующим составом, то есть, предусмотрено ч. 2 ст. 272 УК РФ. Так, на практике встречаются случае, когда лицо, копирует программу, с целью присвоения авторского права, и такие действия принято квалифицировать по совокупности преступления, в случае, если автору программы был причинен крупный ущерб. Как это было установлено по уголовному делу, рассматриваемым Златоустовским городским судом Челябинской области:

Обвиняемый Силкин М.М., имевший умысел на неправомерный доступ к охраняемой законом компьютерной информации, действовавший из корыстной заинтересованности, с целью незаконного использования объектов авторского права, копировал на 2 оптических диска один экземпляр программного продукта «Компас 3DV-11 (с библиотеками)», правообладателем которого является ЗАО. При этом правообладателем ЗАО предложено на официальном сайте

приобретение ПО за установленную цену, либо использование пробной версии, ограниченного срока пользования. После чего умысел Силкина М.М. был направлен на незаконное использование объектов авторского права, приобретение, хранение в целях сбыта контрафактного экземпляра произведения, а также незаконное использование объектов авторского права в целях сбыта, за материальное вознаграждение. Где, копирование программы является преступным деянием, предусмотренным ст. 272 УК РФ, а программа, принадлежащая ЗАО относится к объектам авторского права, а тот факт, что ущерб причиненный действиями Силкина М.М. составил 228 370 рублей, является крупным размером, то есть попадает под состав преступления, предусмотренный статьей 146 УК РФ. В связи, с чем судом был вынесен обвинительный приговор за совершенные преступления, предусмотренные ч. 2 ст. 272 и ч. 2 ст. 146 УК РФ[1].

Стоит также отметить, что нередко на практике встречаются случае, когда неправомерный доступ к компьютерной информации является лишь частью другого преступления, то есть выступает способом совершения таких преступлений как, мошенничество – статья 159 УК РФ; а также с получением конфиденциальной информации с помощью неправомерного доступа, совершается и такое преступление как вымогательство – ст. 163 УК РФ, при этом дополнительной квалификации по статье 272 УК РФ не имеет смысла.

Так, Саткинским городским судом Челябинской области вынесен обвинительный приговор в отношении Миндибаевой Ю.Р., которая совершила мошенничество с использованием своего служебного положения. Являясь директором в сети магазинов ООО «Евросеть-Ритейл» и неся в соответствии со своей должностной инструкцией ответственность за ненадлежащее исполнение или неисполнение своих служебных обязанностей, незаконное получение денег, ценных бумаг, иного имущества, а равно незаконное пользование услугами любого характера за совершение (бездействия) в связи с занимаемым служебным

[1]Приговор № 1-79/2014 от 13.02.14г. Златоустовского городского суда Челябинской области // СПС https://sudact.ru/.

положением, неправомерный доступк компьютерной информации, создание, использование и распространение вредоносных программ для ПК, нарушение правил эксплуатации ПК или их сети; разглашение коммерческой тайны. Реализуя свой преступный умысел, Миндибаева Ю.Р. в период рабочего времени с 09.00 часов до 20.00 часов, находясь на рабочем месте – в магазине ООО «Евросеть-Ритейл», используя свои служебные полномочия вопреки интересам службы, осознавая общественно-опасный и противоправный характер своих действий, действуя умышленно, из корыстных побуждений, при помощи персонального (служебного) компьютера, имеющего доступв сеть «Интернет», в сети «Интернет» приискала находящееся в свободном доступе изображение паспорта гражданина Российской Федерации.

После этого Миндибаева Ю.Р., продолжая реализовывать свой преступный умысел, используя свои служебные полномочия вопреки интересам службы, осознавая общественно-опасный и противоправный характер своих действий, действуя умышленно, из корыстных побуждений, при помощи персонального (служебного) компьютера, имеющегодоступв сеть «Интернет», через сеть «Интернет», не имея на то каких-либо законных оснований и согласия ФИО и ФИО1, направила в микрофинансовую организацию ООО «МИЛИ» собственноручно изготовленное и подделанное ей (Миндибаевой Ю.Р.) заявление от имени ФИО, где были указаны его (ФИО) анкетные данные и паспортные данные ФИО1, о предоставлении микрозайма ФИО в сумме 15000 рублей в виде электронного документа по форме, размещенной на сайте микрофинансовой организации ООО «МИЛИ». То есть в ее действиях реализуется объективная сторона, предусмотренная ст. 272 – копирование конфиденциальной компьютерной информации, однако в данном случае имея умысел на наступления последствий, предусмотренных статьей 159 УК РФ, и выполняя всю объективную

сторону состава о мошенничестве, можно сделать вывод о том, что копирование информации явилось лишь средством совершения преступления[1].

Таким образом, данный состав преступления включает в себя несколько самостоятельных преступлений. При этом на квалификацию деяния влияют последствия деяния или характеристики субъекта, то есть информация является осуществлением общественных отношений или государственного управления. С переходом России к «цифровой экономики», где под информацией понимается – основная ценность и продукт производства[2], ключевым фактором, при квалификации, будет являться информация, к которой осуществляется доступ, то есть возрастет роль информации как предмета преступления, предусмотренного ст. 272 УК РФ.

2.2 Создание, использование и распространение вредоносных компьютерных программ

В статье 273 УК РФ закреплены следующий состав преступления, предусмотренный главой 28 УК РФ, в которой предусмотрена ответственность за создание, использование или распространение компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификация копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Способом совершения данного преступления может быть только действие, выраженное в виде создания вредоносных компьютерных программ, а равно использование либо распространение таких программ либо иной компьютерной информации, что и является предметом состава преступления. Е.А. Маслакова определяет вредоносную программу как компьютерную программу, функционирование которой вызывает не санкционированное собственником

[1]Приговор № 1- 186/2018 от 23 июля 2018г. Саткинского городского суда Челябинской области // СПС https://sudact.ru/.

[2]Дремлюга Роман Игоревич Компьютерная информация как предмет посягательства при неправомерном доступе: сравнительный анализ законодательства США и России // Журнал зарубежного законодательства и сравнительного правоведения. 2018. №6 (73). С. 85.

компьютерной информации ее уничтожение, блокирование, модификацию либо копирование[1].

С.С. Шахрай под вредоносной программой понимает специально созданную, самовоспроизводящую программу, способную выполнять не санкционированные законным пользователем функции, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, а также к нарушению работы ЭВМ, системы ЭВМ или их сети[2].

Вредоносная программа отличается от других программ для ЭВМ своими свойствами. При этом, по справедливому замечанию К.Н. Евдокимова, вредоносными программами могут быть и обычные лицензионные компьютерные программы в случае их использования при совершении преступного деяния и достижения вредных последствий, указанных в ст. 273 УК РФ[3].

Таким образом, вредоносной программой следует считать представленную в объективной форме совокупность данных и команд, предназначенных для компьютера и других средств вычислительной техники в целях получения определенного результата, в виде уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Создание вредоносной программы это результат деятельности, выразившийся в представлении в объективной форме совокупности данных и команд, предназначенных для функционирования информационно-телекоммуникационных сетей, компьютерных устройств с целью уничтожения, блокирования, модификации, копирования информации, а также с целью нарушения работы информационно-телекоммуникационных сетей.

Данным составом к объекту законодатель отнес общественные отношения, которые обеспечивают безопасность в сфере компьютерной информации. Уголовно-правовые запреты направлены на обеспечение конфиденциальности, целостности и доступности компьютерных систем, в частности это касается

функционирования технических средств защиты компьютерной информации. Под использованием в свою очередь, понимается непосредственно сам запуск программы, ввод информации и манипулирование ею. А под распространением понимается – перемещения носителя программы (информации) от одного лица к другому (купля-продажа, дарение, мена и т.п.).

Вредоносные программы законодателем обозначаются как – специально созданные программы для электронно-вычислительных машин, которые способны неправомерно воздействовать на само техническое средство, и реализовывать несанкционированное уничтожение, блокирование, модификацию либо копирование информации, а также нарушению работы ЭВМ, самой системы или их сетей. При этом программой для ЭВМ является представленная в объективной форме совокупность данных и команд. Внесение изменений в существующие программы – это и есть несанкционированная модификация (переработка программы, добавление или удаление отдельных фрагментов) до состояния, когда программа становится способной выполнять новые, изначально не запланированные функции.

По смыслу закона под компьютерной программой чаще понимаются компьютерные вирусы, количество которых с каждым годом возрастает. Законодателю знакомы такие компьютерные вирусы как: черви, троянские кони, кейлоггеры, руткиты и др.

Международная компания «Лаборатория Касперского», на своем сайте четко дает понять, что такое вирусы и какую угрозу они несут обществу, так под сетевыми червями – понимается один из типов вредоносных программ, который способен распространяться по локальной сети и Интернету, создавая свои копии. При этом заражение компьютера или другого электронного устройства пользователь не заметит, в связи с тем, что «компьютерные черви» способны самовоспроизводится, то есть заражение в таком случае распространяется очень быстро. Большинство «компьютерных червей» распространяются с помощью:

1) Файла, отправленного во вложении электронного письма;

2) Ссылки на интернет;

3) Ссылки, переданной через сообщение;

4) Пиринговые сети обмена данных P2P;

5) Сетевого пакета, то есть проникновение идет через компьютерную память, где уже активируется код червя.

На современном этапе развития компьютерных программ, данные способы не являются пределом их распространения.

Троянские кони – это вредоносные программы, выполняющие несанкционированные пользователем действия. Такие действия могут включать:

1) Удаление данных;

2) Блокирование данных;

3) Изменение данных;

4) Копирование данных;

5) Замедление работы компьютеров и компьютерных сетей.

Данный вид вредоносных программ не способен самовоспроизводится. Самой известной является троянская программа бэкдор, которая позволяет, удалено управлять зараженным компьютером: отправлять, получать, открывать и удалять файлы, а также отображать данные и перезагружать компьютер.

Руткиты – является разновидностью «троянского коня». Такая программа скрывает в системе определенные объекты и действия, целью которой является предотвращения обнаружения вредоносной программы.

Кейлоггер – это вредоносное шпионское ПО, которое используется для сбора конфиденциальной информации, например, паролей или финансовых данных, которые затем отправляются третьим лицам для использования в преступных целях. «Клавиатурного шпиона» сложно обнаружить, в связи с тем, что он никак не воздействует на систему компьютера и не подает каких-либо вредоносных признаков.

Таким образом, данные программы, позволяют злоумышленникам: «считывать коды доступа к банковским счетам; рекламировать продукты или услуги на

компьютере жертвы; нелегально использовать ресурсы зараженного компьютера, чтобы разрабатывать и осуществлять сетевые атаки; шантаж»[1].

Объективная сторона этого состава преступления выражена в альтернативных действиях, а именно в создании, распространении и использовании компьютерных программ, повлекших такие последствия как несанкционированное уничтожение, блокирование, модификация и копирование. Где под созданием понимается – написание самостоятельных кодов либо разработка соответствующих данных и придание им формы электрических сигналов.

Состав преступления является формальным, то есть оконченным данный вид преступления будет считаться уже с момента создания, распространения или использования вредоносных программ или информации вне зависимости от того наступили ли последствия или нет. Однако, в квалифицирующем состава (ч.3 ст. 273 УК РФ) уголовная ответственность лица наступает за наступление тяжких последствий или создание угрозы их наступления, то есть данный состав является материальный и ответственность лица с момента наступления общественно опасных последствий, а если создана угроза их наступления, то такой состав будет усеченным.

Составом, предусмотренным статьей 272 УК РФ уголовная ответственность лица наступает только в том случае, если лицо осознает, что созданная им программа или использованная, а также распространенная программа/информация заведомо приведут к предусмотренным в диспозиции статьи общественно опасным последствиям, то есть считается, что преступление совершается с умышленной формой вины. Однако предусмотренная ч.2 ст. 273 УК РФ ответственность лица наступает за две формы вины. В таком составе умысел будет по отношению к самому деянию, а неосторожность по отношению к последствиям. При этом если лицо умышлено относилось и к деянию и к последствиям, то в зависимости от качественной и количественной оценки

[1]Официальный сайт международной компании «Лаборатория Касперского» // https://www.kaspersky.ru/.

наступивших тяжких последствий его действия будут квалифицироваться по дополнительной соответствующей статьей УК РФ.

Данной статьей также предусмотрена ответственность лица, достигшего к моменту совершения преступления 16-летнего возраста, то есть требования, предъявляемые к общему субъекту преступления.

Следует так же отметить, что ответственность по данной статье наступает за незаконные действия с компьютерными программами, которые в свою очередь могут быть зафиксированы как на электронном носителе, так и на бумаге. Это объясняется тем, что процесс создания компьютерной программы чаще всего начинается с написания ее текста с последующим введение его в компьютер или без такого. Поэтому ответственность лица наступает за наличие исходных текстов вредоносных компьютерных программ.Исключением будут являться случаи, когда лицо написало программу для личных нужд, например, для уничтожения собственной компьютерной информации, такие действия не будут попадать под состав статьи 273 УК РФ.

Данная статья часто встречается в практике в совокупности с другими, так как часто злоумышленники используют вредоносную программу для совершения другого преступления. Так, например, Снежинским городским судом Челябинской области было рассмотрено дело в отношении Васильева А.Н., который незаконно использовал объекты авторского права, совершив это в особо крупном размере, а также использовал компьютерную программу, заведомо предназначенную для нейтрализации средств защиты компьютерной информации, совершив это из корыстной заинтересованности, данные деяния были квалифицированы по двум статьям уголовного кодекса, а именно по п. «в» ч. 3 ст. 146 и ч. 2 ст. 273 УК РФ.

Законодателем не установлено, что подразумевается под такими последствиями как: вред, повлекший тяжкие последствия или угрозу их наступления. Однако в уголовно-правовой литературе под ними понимаются:

1) Прямые имущественные потери – нанесение расходов, связанных с восстановлением уничтоженного программного обеспечения;

2) Упущенная выгода – перерыв в производственной деятельности;

3) Причинение вреда здоровью людей;

4) Дезорганизация деятельности организации;

5) Авария на производстве;

6) Уничтожение массивов данных и др[1].

При этом оценка последствий выходят за границы информационной среды, то есть оценивается наступление последствий не по отношению к предмету преступления (компьютерной информации), а по отношению дополнительно затронутых общественных отношений (жизнь и здоровье людей и др.).

Важным моментом стоит отметить трудность в разграничении ст. 273 и ст. 272 УК РФ. Проблема в разграничении касается наступления последствий, а именно несанкционированное уничтожение, блокирование, модификация либо копирование информации или нейтрализации средств защиты компьютерной информации. Однако важным разграничительным моментом будет прежде всего предмет преступления, так в ст. 272 УК РФ предметом является – информация, которая охраняется законом, когда в ст. 273 предметом является любая информация. Также разграничением этих двух составов будет является конструкция состава. А именно статья 272 УК РФ предусматривает ответственность лица, причинившего вред с наступлением общественно опасных последствий, то есть приведение компьютерной информации к уничтожению, блокированию, модификации либо копированию – материальный состав преступления. Когда ст. 273 лицо, может быть привлечено к ответственности с момента создания, использования или распространения вредоносной компьютерной программы, то есть является формальным составом преступления.

На практике выявление злоумышленников сводится к тому, что правоохранительные органы в ходе ОРМ проверяют лиц, которые выставляют

[1]Энгельгардт, А.А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) // LexRussica. 2014. №11. С. 115.

объявления в газеты, на сайтах об оказании услуг программного обеспечения: «установка антивирусных программ, лечение вирусов, сборка ПК и др». Например, Златоустовским городским судом Челябинской области, было рассмотрено дело в отношении Трясцина В.В., который с целью незаконного получения денежного вознаграждения за установку контрафактного программного обеспечения, их корыстных побуждений, разместил объявление на сайте о б оказании его услуг в сфере программного обеспечения. 1 августа 2012 года Трясицын, реализовывая свой умысел, был задержан правоохранительными органами в ходе ОРМ «Проверочная закупка», с целью проверки законности индивидуальной деятельности. Таким образом, Трясицын В.В. был признан виновным в совершении двух преступлений, предусмотренными ч. 2 ст. 146 и ч. 2 ст. 273 УК РФ[1].

Итак, данная статья предусматривает ответственность за создание, использование и распространение вредоносных компьютерных программ, заключает в себе состав формального (ч. 1 ст. 273 УК РФ) и материального (ч. 2,3 ст. 273 УК РФ) характера. Также данный состав тесно граничит с составом преступления, предусмотренного ст. 272 УК РФ. Стоит отметить и роль данного состава, так как действия, предусмотренные данной статьей, являются способом совершения преступлений, касающихся как жизни и здоровья людей, авторских и смежных прав, то есть затрагивает другие сферы деятельности.[2]

2.3 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

В связи с тем, что выход из строя компьютерного оборудования либо информационно-телекоммуникационных сетей может привести к катастрофическим последствиям законодателем была установлена уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-

[1]Приговор Златоустовского городского суда Челябинской области // https://sudact.ru/

[2] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Отв. ред. В.М. Лебедев. – 7-е изд., перераб. и доп. – М.: Юрайт-Издат, 2007. С .131.

телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям. Под правилами эксплуатации законодатель понимает те правила, которые направлены на обеспечение информационной безопасности. Такие правила содержатся в различных положениях, инструкциях, уставах, приказах, ГОСТах, проектной документации на соответствующую автоматизированную информационную систему, договорах, соглашениях и иных официальных документах.

Эта норма является бланкетной и отсылает к конкретным нормативным и нормативно-техническим актам, а также инструкциям, регламентам и правилам, устанавливающим порядок работы с информационно-телекоммуникационных сетями и оконченным оборудованием в ведомстве или организации.

Примером нормативных актов, которые устанавливают правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, могут служить:

- Федеральный закон «О связи» №126;
- Временные санитарные нормы и правила для работников вычислительных центров;
- Техническая документация на компьютерную технику;
- Конкретные принимаемые в определенном учреждении или организации оформленные нормативно и доведенные доя сведения соответствующих работников инструкции и правил внутреннего порядка.

При этом под охраняемой информацией понимается информация, для которой в специальных законах, иных нормативно-правовых актов установлен специальный режим ее правовой защиты, например, государственная, служебная, коммерческая и банковская тайны, персональные данные и т.д.

Таким образом, основным объектом преступления выступают общественные отношения, обеспечивающие безопасность в сфере компьютерной информации. Также данным составом преступления охраняются общественные отношения, затрагивающие иные социальные ценности, как жизнь человека, здоровье и т.п.,

которые выступают дополнительным объектом. При этом предметом выступают средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование.

Объективная сторона преступления включается в себя нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, повлекшие такие последствия как уничтожение, блокирование модификацию либо копирование компьютерной информации, причинившее крупный ущерб, превышающим 1 миллион рублей.

К средствам хранения компьютерной информации относятся ее материальные носители: а именно дискеты, жесткие диски, оптические диски, USB-флеш-накопители, карты памяти и др. Инструмент обработки – то есть компьютер. При этом Информационно-телекоммуникационная сеть является технологической системой, предназначенной для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

То есть за данный вид преступления наступает ответственность, в случае, когда лицо, не соблюдало правила эксплуатации предмета преступления или доступа к информационно-телекоммуникационным сетям: несвоевременное техническое обслуживание узлов и агрегатов, неправильное подключение компьютера к источникам питания, невыполнение резервного копирования, отказ от использования антивирусного программного обеспечения, обработка конфиденциальной информации вне рабочего места и т.д.

Состав, предусмотренный статьей 274 Уголовного Кодекса Российской Федерации, является материальный, и основным элементом является причинение крупного ущерба. Важным моментом квалификации по данному составу является наступление общественно-опасных последствий, имеющие причинно-следственную связь с преступным деянием. При этом наступившие последствия должны являться результатом нарушения правил эксплуатации, а не программной

ошибкой либо действиями, предусмотренными ст. 272, 273 Уголовного Кодекса Российской Федерации.

Данный состав имеет две формы вины, то есть по отношению к наступившим последствиям ответственность может наступить при наличии умысла, так и при неосторожности лица. Так, лицо будет подвергнуто уголовной ответственности за нарушение им правил эксплуатации, в случае если, оно предвидит наступление таких последствий, как уничтожение, модификацию, блокирование или копирование компьютерной информации, однако самонадеянно рассчитывает на предотвращение последствий. А также в случае, если лицо не предвидит указанных в законе последствий, хотя при необходимости внимательности и предусмотрительности должно было и могло предвидеть[1]. Например, в случае, если программист установит полученную по сетям программу без предварительной проверки на наличие компьютерных вирусов, в результате чего произошел отказ в работе систем, то такое деяние будет квалифицировано как совершенное преступление ст. 274 Уголовного Кодекса Российской Федерации по неосторожности.

Статьей 274 Уголовного Кодекса Российской Федерации предусмотрена ответственность лица, который в силу своих должностных обязанностей имеет доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию, а также к информационно-телекоммуникационным сетям и обязано соблюдать установленные для них правила эксплуатации. Таким образом, субъектом преступления за нарушение правил эксплуатации является специальный субъект. Однако согласно ч. 4 ст. 2 Федерального Закона № 149 под информационно-телекоммуникационной сетью понимается «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники»

[1]Рарог А.И. Уголовное право России части общая и особенная. Учебник 9-е издание // М.: Проспект, 2018. С. 896.

куда попадает любая компьютерная сеть, создаваемые поставщиками услуг доступа в Интернет. Отсюда следует, что провайдер также попадает под данную статью, в связи с тем, что он предоставляет доступ в Интернет, заключая договор оказания услуг, где прописываются определенные правила доступа к информационно-телекоммуникационным сетям. То есть законодатель, также предусмотрел ответственность по данной статье и для общего субъекта преступления, так как к провайдерам относят лица, оказывающие услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет»[1].

На практике правоприменители сталкиваются с проблемой разграничения таких составов преступления, которые предусмотрены статьями 272 и 274 Уголовного Кодекса Российской Федерации. Важным моментом стоит учитывать то, что статья 272 предусматривает ответственность лица за неправомерный доступ к компьютерной информации, когда в 274 статье лицо в силу своих должностных обязанностей имеет правомерный доступ к компьютерной информации, то есть лицо является законным пользователем информации.

По объективной стороне эти составы разграничиваются тем, что статьей 272 Уголовного Кодекса Российской Федерации, предусмотрена ответственность лица за активные действия, когда статьей 274 Уголовного Кодекса Российской Федерации лицо может и бездействовать, например, лицо не включает системы защиты информации, в результате чего наступают вредные последствия. По последствиям эти составы разграничиваются тем, что при нарушении правил эксплуатации, обязательным условием будет причинение крупного ущерба, когда в статье 272 Уголовного Кодекса Российской Федерации это условие относится к квалифицированному составу, а по основному составу, наступление таких последствий как уничтожение, модификация, блокирование или копирование достаточны для привлечения лица к уголовной ответственности.

[1]ФЗ от 27.07.2006 №149 «Об информации, информационных технологиях и о защите информации» // СЗ, 2006. №31 (1 ч.), ст. 2601

Стоит также отметить, что по данным ГИАЦ МВД России уголовные дела по статье 274 Уголовного Кодекса Российской Федерации в 2014 году – 3 уголовных дела; в 2015 году – 12 уголовных дел; в 2016 – 3 уголовных дела, в 2017 году – 2 уголовных дела[1]. А по данным ГИ ГУ МВД России по Челябинской области в 2018 году было возбуждено 1 уголовное дело по статье 274 Уголовного Кодекса Российской Федерации. В связи с этим в судебной практике уголовные дела по статье 274 Уголовного Кодекса Российской Федерации является редким случаем, и то дела рассмотренные судами чаще всего были прекращены. Однако состав преступления, предусмотренный статьей 274 Уголовного Кодекса Российской Федерации, чаще всего на практике встречается в совокупности с другими преступными деяниями.

Так, 11 декабря 2015 г. приговором Верх-Исетского районного суда города Екатеринбурга Свердловской области был вынесен обвинительный приговор в отношении граждан р. Молдова за совершение 11 преступлений, предусмотренных ч. 2 ст. 273 Уголовного Кодекса Российской Федерации, 9 преступлений, предусмотренных ч. 3 ст. 272 Уголовного Кодекса Российской Федерации, 9 преступлений, предусмотренных ч. 3 ст. 183 Уголовного Кодекса Российской Федерации, 6 преступлений, предусмотренных ч. 1 ст. 274 Уголовного Кодекса Российской Федерации, 6 преступлений, предусмотренных п.п. «а,б» ч. 4 ст. 158 Уголовного Кодекса Российской Федерации, и назначено наказание в виде лишения свободы сроком на 5 лет и 6 месяцев, в исправительной колонии общего режима. При этом судом было установлено, что было создано ОПГ из корыстных побуждений. В течение июня –июля 2014 года, совершили ряд преступлений против собственности в виде тайного хищения наличных денежных средств в крупных и особо крупных размерах из банкоматов марки NCR в нескольких городах страны, путем предварительного незаконного сбора сведений о коммерческой тайне банков, посредством неправомерного и скрытого доступа к компьютерной информации, используя вредоносную компьютерную программу

[1]Преступления в сфере компьютерной информации // Сводный отчет по России URL: https://мвд.рф.

«Backdoor.Win32.Tyupkin.d», влекущую нарушение правил эксплуатации банкоматов, похитили денежные средства на общую сумму 17 319 000 руб. и завершили приготовление к тайному хищению денежных средств из двух банкоматов на сумму 7 929 300 руб[1]. В данном случае, статья 274 была вменена как дополнительная квалификация преступного деяния.

В соответствии с положений Постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» при хищении денежных средств из банкоматов с помощью поддельных банковских карт действия виновных лиц должны квалифицироваться по соответствующим частям статей 159.6, 183, 187, 272, 274 Уголовного Кодекса Российской Федерации. А в случаях, когда лицо использует для хищения денежных средств из банкоматов вредоносные компьютерные программы, то деяния следует дополнительно квалифицировать по соответствующей части ст. 273 Уголовного Кодекса Российской Федерации[2].

По данным ГИАЦ МВД России в 2013 году уголовные дела по статье 274 не возбуждались вообще, в 2012 году было возбуждено 1 уголовное дело, данная статистика образовалась в связи с введением в Уголовного Кодекса Российской Федерации новый состав преступления, предусмотренный ст. 159.6 «Мошенничество в сфере компьютерной информации». Этим составом лицо, привлекается к уголовной ответственности за совершение за 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.Что позволяет теперь правоприменителю без дополнительной

[1]Уголовное дело № 1-584/2015 // Архив Верх-Исетского районного суда г. Екатеринбурга Свердловской области, 2015 г.URL: http://verhisetsky.svd.sudrf.ru/.

[2]Евдокимов К.Н. Актуальные вопросы совершенствования судебной практики по уголовным делам о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) // Российский судья. 2019. N 2. С. 12 - 16.

квалификации по статье 274 Уголовного Кодекса Российской Федерациикваливицировать преступное деяние с целью хищение денежных средств из банкоматов, согласно абз. 2 п. 20 Постановления Пленума Верховного Суда Российской Федерации № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

Таким образом, можно сделать вывод о том, что статья 274 Уголовного Кодекса Российской Федерации утратило свое значение. Исходя из данных ГИЦ МВД России, где заметен спад возбуждаемых уголовных дел по данной статье.

2.4 Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

Состав преступления, предусмотренный статьей 274.1, является достаточно новым составом, который был принят в 2017 году. Законодатель выделил данный состав в отдельную статью, в связи с тем, что объект посягательства критическая информационная инфраструктура РФ, стала часто подвергаться кибератакам, что в итоге может привести к проблемам на государственном уровне. А также данная норма была принята для восполнения пробела в уголовном законе по защите отношений в сфере компьютерной информации[1].

Понятие критическая информационная инфраструктура (КИИ) РФ закреплено в ст. 2 федерального закона №187 «О безопасности критической инфраструктуры РФ», где указано, что КИИ это объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. В той же статье законодатель определил, что под объектами КИИ понимаются: «информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры». Также законодатель ввел новые для правовой практики понятия: «компьютерная атака» и «компьютерный инцидент».

[1]Криминализация и декриминализация как формы преобразования уголовного законодательства: монография / И.С. Власов, Н.А. Голованова, А.А. Гравина и др.; отв. ред. В.П. Кашепов. М.: ИЗиСП, КОНТРАКТ, 2018. С. 132.

Объективная сторона данного состава включает в себя действия предусмотренные статьями главы 28 УК РФ, в частности ст. 272, то есть неправомерный доступ к охраняемой компьютерной информации, содержащийся в критической информационной инфраструктуре РФ (ч.2 ст. 274.1 УК РФ). Данный состав считается материальным, то есть преступление считается оконченным только в случае причинения вреда критической информационной инфраструктуре РФ. При этом стоит учитывать, что преступлением будет признаваться только действия лица с умыслом направленным на причинение вреда КИИ РФ. Действия лица будут квалифицированы по ч. 3 ст. 30, ч. 2 ст. 274.1 УК РФ, то есть как покушение на преступление, в случае когда, по независящим от лица обстоятельствам не удалось причинить вред критической информационной инфраструктуре Российской Федерации (например, сработала антивирусная программа). Стоит также учитывать, что если лицо, которое использовало вредоносную программу, также являлось и ее разработчиком, то такое преступление стоит квалифицировать по совокупности преступлений, предусмотренных ст. 273 и ст. 274.1 УК РФ. В таком случае применяется правило квалификации, в соответствии с которым, «действия по подготовке или исполнению деяния, не входящие в объективную сторону оконченного преступления, должны получить самостоятельную уголовно-правовую оценку по другой статье закона»[1].

Признаки состава, предусмотренного ст. 273 УК РФ – создание, распространение и (или) использование компьютерных программ, для неправомерного воздействия на КИИ РФ (ч. 1 ст. 274.1 УК РФ) и по своей конструкции состав является формальным. Если лицо одновременно разработало, использовало и распространило вредоносную компьютерную программу, заведомо предназначенную для совершения компьютерных атак на объекты

[1]Решетников А.Ю. Квалификация неоконченных преступлений при наличии признаков совокупности преступлений // Вестник Академии Генеральной прокуратуры Российской Федерации. 2016. № 4. С. 85.

критической информационной инфраструктуры, содеянное образует единое преступление.

И положения статьи 274 УК РФ – нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащийся в критической информационной инфраструктуре РФ (ч. 3 ст. 274.1 УК РФ). Данный состав также является материальным, так как предусматривает наступление таких последствий, как причинение вреда КИИ РФ[1]. Отсюда видно, что законодатель объединил в данном составе три нормы главы 28 УК РФ, выделив при этом особый объект посягательств.

При этом предметом преступления является компьютерная информация, которая содержится в критической информационной инфраструктуре, так и объекты инфраструктуры в виде информационных систем, информационно-телекоммуникационных сетей, а также автоматизированных систем управления.Так как компьютерные атаки на информационные ресурсы, могут совершаться на такие объекты как: транспорт, оборона, атомная промышленность, ракетно-космической промышленность, химическая промышленность, то в таком случае, могут содержаться признаки других преступлений (ст.ст 205, 275, 276, 281 УК РФ).

Объектом преступления является, как было отмечено ранее, общественные отношения, которые обеспечивают нормальную работу, функционирование ЭВМ, сети ЭВМ, системы ЭВМ, которые имеют отношение к критической информационной инфраструктуре РФ.

Объективная сторона преступления может быть выражена как действием, так и бездействием. Так, например, в декабре 2017 года был задержан системный администратор аэропорта, который построил в Московском центре управления воздушным движением ферму для майнингакриптовалюты, в связи, с чем

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

образовывались постоянные скачки напряжения, так и в форме бездействия, например, администратор не обновляет антивирусные базы.

Важным моментом в составах, предусмотренных статьей 274.1 УК РФ, является наступление общественно-опасных последствий в виде причинения вреда критической информационной инфраструктуре Российской Федерации. Стоит отметить, что место совершения преступления по статье 274.1 УК РФ тоже играет не маловажную роль, так как последствия наступают в причинение вреда КИИ РФ, то и место наступления таких последствий, может быть только место нахождения КИИ РФ. А значит квалифицировать деяния лица по данному составу можно только в том случае, если местом совершения преступления является КИИ РФ[1].

Субъективная сторона этого преступления выражается как в форме умысла, так и неосторожностью в зависимости от совершаемого деяния. С умышленной формой вины совершается преступление, предусмотренное ч. 1 ст. 274.1 УК РФ, при этом обязательным признаком будет цель, которая направлена на нарушение и (или) прекращение их функционирование и (или) создание угрозы безопасности обрабатываемой такими объектами информации, с помощью компьютерной атаки. В части 2 статьи 274.1 УК РФ предусмотрена ответственность лица по отношению к последствиям в форме умысла, так и может быть выражено неосторожной формой вины.Субъективная сторона ч. 3 ст. 274.1 также может выражаться двумя формами вины, то есть лицо, предвидит причинение вреда КИИ РФ в результате нарушение 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»[2]. Стоит также отметить, что умышленные действия с целью хищения,

[1]Попов А.Н. Преступление в сфере компьютерной информации: учебное пособие / А.Н. Попов // СПбЮИ(ф)УП РФ, 2018. С. 69.
[2]Рарог А.И. Уголовное право России. Части общая и особенная: учебник для бакалавров / А.И. Рарог. М., Проспект, 2019. С.1203.

квалифицируются по соответствующим статьям УК РФ, в частности по главе 21 – преступления против собственности.

Субъект преступления, предусмотренный ч. 1, 2 ст. 274.1 является вменяемое физическое лицо, которому на момент совершения преступления исполнилось 16 лет. В части 3 статьи субъектом преступления может выступать как вменяемое физическое лицо, достигшее к моменту совершения преступления 16-летнего возраста в отношении правил доступа к ресурсам, так и специальный субъект, в случае, когда на лице лежала обязанность по соблюдению специальных правил.

Квалифицируемыми составами данной статьи является совершения деяния группой лиц по предварительному сговору или организованной группой, а также лицом с использованием своего служебного положения. «Под лицами, использующими свое служебное положение, законодатель относит должностных лиц, государственных или муниципальных служащих, не являющихся должностными лицами, а также иных лиц»[1].

Следующим квалифицированным признаком наступление тяжких последствий, однако, законодатель не установил, что подразумевается под тяжкими последствиями, поэтому суд при рассмотрении дела должен установить размер, вред и тяжесть последствий. При этом в рамках данной статьи к таким последствиям можно отнести: причинение вреда здоровья людей, разрушение инфраструктуры, нанесение вреда безопасности государства и т.п.

Стоит отметить, что данный состав преступления законодатель относит к тяжким преступлениям, поскольку данный состав преступления подразумевает угрозу безопасности государства и населения[2].Это связано также с встречающимися преступлениями на практике, так например, в мае 2012 г. житель Красноярска совершил хакерскую атаку на сайт Президента РФ. При этом суд приговорил его к одному году лишения свободы, что говорит о

[1]Постановление Пленума Верховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате»от 30 ноября 2017г. №48 // СПС https://rg.ru
[2]Куприянова, В.Н. Преступления в сфере компьютерной информации // В.Н. Куприянова, 2019. СПС http://juresovet.ru/.

несоразмерности наказания данному деянию. В 2013 году был осужден томский хакер, который взломал сайт Президента РФ, вызвав тем самым блокировку указанного сайта. Судом также было назначено мягкое наказание в виде полутора лет ограничения свободы[1]. Законодатель также отнес данный вид преступления к подследственности сотрудников федеральной службы безопасности. Также санкция ч. 5 ст. 274.1 предусматривает уголовное наказание в виде 10 лет лишения свободы, в связи с высокой общественной опасности данного деяния.

Таким образом, статья 274.1 УК РФ защищает критическую информационную инфраструктуру РФ от неправомерного преступного воздействия. При этом законодатель объединил в данном составе основные объективные и субъективные признаки трех составов преступлений, которые предусмотрены статьями 272-274 УК РФ, но установил разграничивающий признак, содержащийся в объекте преступления, а именно критическую информационную инфраструктуру РФ[2]. Еще одним разграничивающим признаком составов, предусмотренных ч. 1 ст. 274.1 и 273 УК РФ будет являться признак субъективной стороны – цель. Разграничением между ч. 2 ст. 274.1 и 272 УК РФ будет заключаться в признаках, как объективной стороны, так и субъективной, в частности: последствия, выраженные в причинение вреда критической информационной инфраструктуре Российской Федерации, когда в 272 статье последствиями будут уничтожение, блокирование, модификация либо копирование компьютерной информации. Итак, можно сделать вывод, что статьи предусмотренные главой 28: 272, 273, 274 УК РФ закрепляют в себе общие положения, когда в статье 274.1 законодатель вкладывает особую значимость данного состава, то есть он по отношению к общим, будет признан специальным. Поэтому в случаи конкуренции норм, действия лица будут квалифицированы по статье 274.1 УК РФ.

На сегодняшний день судебная практика не сталкивалась с данным составом преступления, однако, до вступления в законную силу 2017 года ФЗ № 194 «О

[1]Осужден томский хакер, взломавший сайт Президента РФ // РИА Новости, 2013. 23 декабря.
[2]Барышева, К.А. Комментарий к Уголовному кодексу Российской Федерации (постатейный; восьмое издание, перераб. и доп.). М., Проспект, 2019. С. 344.

безопасности критической информационной инфраструктуры Российской Федерации» правоохранительными органами пресекались деяния попадающие под состав статьи 274.1 уголовного законодательства.

ЗАКЛЮЧЕНИЕ

С повышением роли информации во всех сферах деятельности повышается роль и значение компьютерной информации как одной из самых популярных форм создания, использования, передачи информации. А с повышением роли компьютерной информации требуется повышать уровень ее защиты с помощью технических, организационных и особенно правовых мер. Одной из причин возникновения компьютерной преступности явилось информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных.

Можно прийти к выводу, что законодательство РФ начало формироваться с 1991 года в сфере компьютерной информации, однако, на первом этапе формирования не было предусмотрена ответственность уголовно-правового характера, то есть правовая система по защите информации в компьютерной сфере не была эффективной. Поэтому важным моментом в формировании законодательства по защите информационной безопасности считается принятие новых норм и введение дополнительной главы в УК РФ.

Существующая в действующем УК РФ система преступлений в сфере компьютерной информации является, с одной стороны, основополагающей для отечественного правоприменителя в силу ее прагматичности, с другой стороны — требует дальнейшего развития путем совершенствования юридических конструкций и признаков имеющихся составов преступлений, а также включения новых преступлений, отражающих современные потребности уголовно-правовой охраны компьютерной информации. Кроме того, отечественному законодателю, а также специалистам в области уголовного права и криминологии, необходимо находится в постоянной динамике, чутко реагируя на любые изменения в сфере компьютерных преступлений и преступлений в сфере высоких технологий, как в России, так и за рубежом. Только таким образом можно привести российское уголовное законодательство в соответствие с быстро развивающимися

технологиями и получить надежную правовую защиту от компьютерной преступности.

Исходя из этих видов преступлений, можно прийти к выводу, что преступления в сфере технологий, затрагивают все общественные отношения. Таким образом, можно смело говорить, что «Киберпреступление – это совокупность преступлений, которые запрещены законом, совершаемые в киберпространстве, затрагивающие такие общественные отношения как:

- конституционные права и свободы человека и гражданина;
- в сфере компьютерной информации и информационных технологий;
- в сфере экономики и экономической деятельности;
- в сфере государственной власти;
- в сфере здоровья населения и общественной нравственности.

То есть данный вид преступлений по российскому законодательству не может содержаться в одной главе, так как затрагивает большой ряд преступлений в различных общественных отношениях. Поэтому в УК РФ введены квалифицирующие составы преступлений таких как:

1) Нарушение авторских и смежных прав – ст. 146 УК РФ;

2) Мошенничество – ст. 159 УК РФ;

3) Незаконное изготовление и оборот порнографических материалов или предметов – ст. 242 УК РФ.

Однако с таким активным развитием киберпреступлений, законодателю стоит учесть все способы совершения преступления во всех сферах деятельности, в том числе дополнить некоторыми составами главу 28 УК РФ.

Проанализировав уголовно-правовые запреты, я пришла к выводу, что

Неправомерный доступ к компьютерной информации включает в себя несколько самостоятельных преступлений. При этом на квалификацию деяния влияют последствия деяния или характеристики субъекта, то есть информация является осуществлением общественных отношений или государственного управления. С переходом России к «цифровой экономики», где под информацией

понимается – основная ценность и продукт производства , ключевым фактором, при квалификации, будет являться информация, к которой осуществляется доступ, то есть возрастет роль информации как предмета преступления, предусмотренного ст. 272 УК РФ.

Использование и распространения вредоносных компьютерных программ тесно граничит с составом преступления, предусмотренного ст. 272 УК РФ. Стоит отметить и роль данного состава, так как действия, предусмотренные данной статьей, являются способом совершения преступлений, касающихся как жизни и здоровья людей, авторских и смежных прав, то есть затрагивает другие сферы деятельности.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей предусмотрена ответственность лица, который в силу своих должностных обязанностей имеет доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию, а также к информационно-телекоммуникационным сетям и обязано соблюдать установленные для них правила эксплуатации. Таким образом, субъектом преступления за нарушение правил эксплуатации является специальный субъект. Стоит также отметить, что по данным ГИАЦ МВД России уголовные дела по статье 274 Уголовного Кодекса Российской Федерации в 2014 году – 3 уголовных дела; в 2015 году – 12 уголовных дел; в 2016 – 3 уголовных дела, в 2017 году – 2 уголовных дела . А по данным ГИ ГУ МВД России по Челябинской области в 2018 году было возбуждено 1 уголовное дело по статье 274 Уголовного Кодекса Российской Федерации. В связи с этим в судебной практике уголовные дела по статье 274 Уголовного Кодекса Российской Федерации является редким случаем, и то дела рассмотренные судами чаще всего были прекращены. Таким образом, можно сделать вывод о том, что статья 274 Уголовного Кодекса Российской

Федерации утратило свое значение. Исходя из данных ГИЦ МВД России, где заметен спад возбуждаемых уголовных дел по данной статье.

Статья 274.1 УК РФ защищает критическую информационную инфраструктуру РФ от неправомерного преступного воздействия. При этом законодатель объединил в данном составе основные объективные и субъективные признаки трех составов преступлений, которые предусмотрены статьями 272-274 УК РФ, но установил разграничивающий признак, содержащийся в объекте преступления, а именно критическую информационную инфраструктуру РФ . Еще одним разграничивающим признаком составов, предусмотренных ч. 1 ст. 274.1 и 273 УК РФ будет являться признак субъективной стороны – цель. Разграничением между ч. 2 ст. 274.1 и 272 УК РФ будет заключаться в признаках, как объективной стороны, так и субъективной, в частности: последствия, выраженные в причинение вреда критической информационной инфраструктуре Российской Федерации, когда в 272 статье последствиями будут уничтожение, блокирование, модификация либо копирование компьютерной информации. Итак, можно сделать вывод, что статьи предусмотренные главой 28: 272, 273, 274 УК РФ закрепляют в себе общие положения, когда в статье 274.1 законодатель вкладывает особую значимость данного состава, то есть он по отношению к общим, будет признан специальным. Поэтому в случаи конкуренции норм, действия лица будут квалифицированы по статье 274.1 УК РФ.

На сегодняшний день судебная практика не сталкивалась с данным составом преступления, однако, до вступления в законную силу 2017 года ФЗ № 194 «О безопасности критической информационной инфраструктуры Российской Федерации» правоохранительными органами пресекались деяния попадающие под состав статьи 274.1 уголовного законодательства.

Анализируя материал данной дипломной работы можно сделать вывод о необходимости внесения значительного массива дополнений и изменений в действующее законодательство Российской Федерации. Кроме того, требуется

издание новых законов вносящих правовое регулирование в информационные отношения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ I НОРМАТИВНЫЕ ПРАВОВЫЕ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

1. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. // Российская газета. 1993. №237.
2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 29.03.2019) // Российская газета. 22.12.2001. № 249.
4. Федеральный закон «Об информации, информационных технологиях, и о защите информации» от 27 июля 2006 года. №149-ФЗ// Собрание законодательства РФ. 2006. № 8. Ст. 609.
5. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ // СЗ РФ, 17.06.1996, N 25, ст. 2954.
6. Конституция Российской Федерации - (принята всенародным голосованием 12.12.1993) // в "Собрании законодательства РФ", 04.08.2014, N 31, ст. 4398.
7. Федеральный закон "Об информации, информационных технологиях и защите информации" от 27 июля 2006 года. №149-ФЗ// "Собрание законодательства РФ". 2006. N 8. Ст. 609.
8. Федеральный закон "Об информации, информационных технологиях и защите информации" от 27 июля 2006 года. №149-ФЗ//"Собрание законодательства РФ". 2006. N 8. Ст. 2895.
9. Уголовный кодекс Российской Федерации от 13. 06. 1996 № 63-ФЗ // Собрание Законодательства РФ, 1996. №25. Ст. 2954.

РАЗДЕЛ II ЛИТЕРАТУРА

1. Батурин, Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. М., Юрид. Лит, 1991. 160 с.

2. Бытко, С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: дис. …канд.юрид. наук / С.Ю. Бытко, Саратов, 2002. 204 с.
3. Вехов, В.Б. Компьютерные преступления: Способы совершения. Методики расследования / В.Б. Вехов. М., Право и Закон, 1996. 182 с.
4. Крылов, В.А. Указ. соч. С. 612-614
5. Селиванова, Н.А. Расследование преступлений повышенной общественной опасности: пособие для следователя / Н.А. Селиванов, А.И. Дворкин, В.П. Касьяненко и др.; М., Лига Разум, 1998. 444 с.
6. Бюллетень международных договоров. 2009. №6 С.12-17.
7. Комиссаров, В.С. Преступления в сфере компьютерной безопасности: понятие и ответственность /В.С. Комиссаров. М., Юридический мир, 1998.102 с.
8. Дворецкий, М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: монография/ М.Ю. Дворецкий. М., ТГУ, 2003. 197 с.
9. Крылов, В.В. Расследование преступлений в сфере информации / В.В. Крылов, М., Городец, 1998. 264 с.
10. Добровольский, Д.В. Актуальные проблемы борьбы с преступностью (уголовно-правовые и криминологические проблемы): дис. …канд. юрид. наук / Д.В. Добровольский, М., Проспект, 2005. 218 с.
11. Номоконов В.А. Киберпреступность, как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. 2012. №1(24). С. 102-103.
12. Богданова Т.Н., К вопросу об определении понятия «преступления в сфере компьютерной информации» / Т.Н. Богданова// Вестник ЧелГУ. 2012. №37. Право. Вып. 34. С. 64-67.
13. Кибермошенники за год украли со счетов россиян почти 350 млн. рублей [Электронный ресурс] // Общая газета: офиц. сайт. URL: https://og.ru/society/2016/10/13/84213.

14. Кибермошенники в 2016г. похитили с банк. карт россиян 650 млн. рублей [Электронный ресурс] // Общая газета: офиц. сайт. URL: https://og.ru/society/2017/08/14/90702.
15. Кузнецов М.В. Социальная инженерия и социальные хакеры / М.В. Кузнецов, И.В. Симдянов , М., СПб., 2007. 315 с.
16. Кочкина Э.Л. определение понятия «киберпреступление». Отдельные виды киберпреступлений. / Э.Л. Кочкина// сибирские уголовно-процессуальные и криминалистические чтения. 2017. С. 76-77.
17. Жиделев В.Г. Эволюция законодательства об уголовной ответственности за совершение преступлений в сфере высоких технологий / В.Г. Жиделев // М., Экономика и право. 2011. 420 с.
18. Киберпреступность и закон: обзор положений законодательства Великобритании, касающегося компьютерных преступлений. URL: http://www.viruslist.com/ru/analysis?pubid=204007656
19. Першиков В.И. Толковый словарь по информатике / В.И. Першиков, В.М. Савинков, А.С. Маркова, И.В. Поттосина. М.: Финансы и статистика, 1991. 439 с.
20. Грицков С.А. Получение компьютерной информации: понятие и сущность / С.А. Грицков/ URL:http://saransk.ruc.su/upload/Upload_Saransk/Studium_2017/Vipusk_3/Grickov.pdf (Дата обращения: 12.09.2018).
21. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации"(утв. Генпрокуратурой России) // СПС КонсультантПлюс, 2014. 130 с.
22. Домкин, П. Статья 272 УК РФ: Неправомерный доступ к компьютерной информации: комментарий и правоприменительная практика / П. Домкин. СПС https://www.advodom.ru/

23. Дремлюга, Р.И. Компьютерная информация как предмет посягательства при неправомерном доступе: сравнительный анализ законодательства США и России/ Р.И. Дремлюга // Журнал зарубежного законодательства и сравнительного правоведения. 2018. №6. С. 73-74.
24. Энгельгардт, А.А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) / М.; LexRussica, 2014. №11. 250 с.
25. Рарог А.И. Уголовное право России части общая и особенная: учебник / А.И. Рарог, М., Проспект, 2018. 896 с.
26. Преступления в сфере компьютерной информации // Сводный отчет по России URL: https://мвд.рф
27. Евдокимов, К.Н. Актуальные вопросы совершенствования судебной практики по уголовным делам о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ)/ К.Н. Евдокимов // Российский судья. 2019. N 2. С. 12 - 16.
28. Криминализация и декриминализация как формы преобразования уголовного законодательства: монография / И.С. Власов, Н.А. Голованова, А.А. Гравина и др.; отв. ред. В.П. Кашепов. М.: ИЗиСП, КОНТРАКТ, 2018. 280 с.
29. Решетников А.Ю. Квалификация неоконченных преступлений при наличии признаков совокупности преступлений / А.Ю. Решетников // Вестник Академии Генеральной прокуратуры Российской Федерации. 2016. № 4. С. 66-67.
30. Решетников, А.Ю. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) / А.Ю. Решетников // Законы России: опыт, анализ, практика. 2018. N 2. С. 51 - 55.
31. Преступление в сфере компьютерной информации: учебное пособие / А.Н. Попов,М., СПбЮИ(ф)УП РФ, 2018. 63 с.

32.Рарог, А.И.Уголовное право России. Части общая и особенная: учебник для бакалавров / А.И. Рарог. М., Проспект, 2019г. 443 с.

33.Куприянова, В.Н. Преступления в сфере компьютерной информации // В.Н. Куприянова, 2019. СПС http://juresovet.ru/

34.Барышева,К.А. Комментарий к Уголовному кодексу Российской Федерации (постатейный; восьмое издание, перераб. и доп.) / К.А. Барышева, Ю.В. Грачёва, Г.А. Есаков. М.,Проспект, 2019 г. 799 с.

35.Воробьев В.В. Преступления в сфере компьютерной информации: Автореф. дис. ... канд. юрид. наук / В.В. Воробьев. М., 2000. С. 28.

36.Григоренко, С.В. Преступления в сфере компьютерной информации / С.В. Григоренко, С.Н. Ткаченко, А.А. Каспаров. М., Полтекс, 2013. С.36-40.

37.Гринберг М.С. Преступления против общественной безопасности / М.С. Гринберг. М., Средне-Уральское, 1974. 65 с.

38.Дворецкий, М. Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ / М. Дворецкий, А. Копырюлин // М., 2007. N 4. 234 с.

39.Доронин, А.М. Уголовная ответственность за неправомерный доступ к компьютерной информации: Автореф. дис. … канд. юрид. наук. / А.М. Доронин. М., 2003. С. 54-58.

40.Зинина, У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: Автореф. дис. … канд. юрид. наук. / У.В. Зинина. М., 2007. С.32-33.

41.Зубкова, М.А. Компьютерная информация как объект уголовно - правовой охраны: Автореф. дис. … канд. юрид. наук. / М.А. Зубкова. М., 2008. С. 78-79.

42.Каспаров А.А. Создание, использование и распространение вредоносных программ для ЭВМ: уголовно-правовые аспекты: Лекция / А.А. Каспаров. М., ТИССО, 2003. 40 с.

43.Козаченко, И.Я. Уголовное право. Общая часть: Учебник / Козаченко И.Я., Галиакбаров Р.Р., Красиков Ю.А., и др.М., Волтерс Клувер, 2013. 568 с.

44. Лебедев, В.М. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / В.М. Лебедев. М., Юрайт-Издат, 2007. http://www.consultant.ru/cons/
45. Радченко, В.И. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / В.И. Радченко, А.С. Михлин, В.А. Казакова. М., Проспект, 2008. http://www.consultant.ru/cons/
46. Копырюлин А. Квалификация преступлений в сфере компьютерной информации / А. Копырюлин // Законность. – 2007. - N 6. С.62-63.

РАЗДЕЛ III ПОСТАНОВЛЕНИЯ ВЫСШИХ СУДЕБНЫХ ИНСТАНЦИЙ И МАТЕРИАЛЫ ЮРИДИЧЕСКОЙ ПРАКТИКИ

1. Постановление ПленумаВерховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» от 30 ноября 2017 г. № 48 // СПС https://rg.ru
2. Уголовное дело № 1-584/2015 // Архив Верх-Исетского районного суда г. Екатеринбурга Свердловской области, 2015 г.URL: http://verhisetsky.svd.sudrf.ru/
3. Приговор № 1-79/2014 Златоустовского городского суда Челябинской области // СПС «Правосудие» - https://sudact.ru/
4. Приговор № 1- 186/2018 Саткинского городского суда Челябинской области // СПС «Правосудие» - https://sudact.ru/
5. Уголовное дело № 10-479/2014 Челябинского областного суда // СПС https://sudact.ru/
6. Апелляционное постановление Судебной коллегии по уголовным делам ВС Республики Тыва от 26 октября 2017г. по делу № 22-1534/2017. // СПС https://sudact.ru/