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 БАКАЛАВРА

ОСОБЕННОСТИ КВАЛИФИКАЦИИ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ЮУрГУ – 40.03.01. 2015.434. ВКР

Руководитель выпускной квалификационной работы
Горбатова Марина Анатольевна,
доцент кафедры
_____
_____2019 г.
Автор выпускной квалификационной работы
Белоусова Светлана Александровна
_____
_____ 2019г.
Нормоконтролер
Кухтина Татьяна Владимировна,
старший преподаватель кафедры
_____
_____2019 г.

Челябинск 2019

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Первоначально компьютер задумывался как устройство для математических вычислений, постепенно превратился в универсальное средство обработки любой информации, используемой человеком. На сегодняшний день практически нет ни одной сферы человеческой деятельности, в которой бы не использовались компьютеры, позволяющие создавать, обрабатывать, хранить, накапливать и передавать огромные объемы информации. Они используются в управлении банками, предприятиями, обороной страны, космическими кораблями, с помощью компьютеров создают музыку, книги, кинофильмы, диагностируют и лечат заболевания человека

Все достижения информационных технологий имеют обратную сторону. Невозможно создать абсолютно надежную технику, компьютерные программы, оборудование. Техника не может быть защищена от сбоев, ненадлежащих действий людей, совершенных умышленно или по неосторожности, что может привести к самым непредсказуемым последствиям.

Одной из характеристик киберпреступности, которая отличает их от других видов преступлений, является то, что они имеют высокую степень латентности. Подсчитано, что только 10-15% киберпреступлений общеизвестно, потому что государственные и коммерческие структуры, которые подвергаются атакам, не склонны пропагандировать последствия атаки и эффективность своих систем защиты.

Компьютерное преступление - это не просто кража денег и информации. Это и так называемые «шалости» с электронными вирусами. Распространение вредоносного программного обеспечения приводит к значительным потерям.

Во многих зарубежных странах указанные выше проблемы стали предметом правового регулирования в 70-х годах. В России актуальность этих вопросов начала рассматриваться только в начале 90-х годов. Информационные технологии пронизывают все сферы человеческой деятельности. В связи

с этим мы сталкиваемся с необходимостью понимания последствий создания и использования технологий, анализа проблем информационного общества и информационной безопасности.

Основной целью выпускной квалификационной работы является анализ неправомерного доступа к компьютерной информации по Уголовному кодексу Российской Федерации.

Реализация данной цели предполагает решение следующих задач:

– анализ развития отечественного и зарубежного законодательства в сфере неправомерного доступа к компьютерной информации;

– раскрытие элементов состава преступления.

Объектом исследования в выпускной квалификационной работе выступают общественные отношения, подвергающиеся посягательствам в результате совершения преступлений в сфере компьютерной информации.

Предмет исследования включает в себя нормативно-правовую регламентацию неправомерного доступа к компьютерной информации.

При написании настоящей работы автор руководствовался частными научными методами исследования, такими как историко-правовой, системно-структурный, социально-правовой, сравнительно-правовой, конкретно-социологический, статистический, которые в совокупности составили методологическую основу исследования.

Научно-теоретическую базу в написании работы составили такие ученые как Вехов В.Ю., Калиниченко И.А., Батурин Ю.М., Жодзишский А.М., Кудрявцева В.Н. и многие другие.

ГЛАВА 1 СРАВНИТЕЛЬНО – ПРАВОВОЙ АНАЛИЗ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

1.1 История развития российского уголовного законодательства в сфере компьютерной информации

В 1948 году, американским ученым К.Е. Шенноном, впервые было определено, что такое «информация», и понятие «объем информации» в контексте вероятностно-статистического определения, основанного на кибернетике. Кибернетика как наука имеет дело с общими законами, целью которых является преобразование информации в довольно сложные системы управления.[1]. Она рассматривает информацию не как социальное явление, а как информацию, которая циркулирует непосредственно через электронные каналы связи. Кибернетика продемонстрировала прямую связь информации с такими процессами, как управление и развитие, которая обеспечивает практически каждую систему, независимо от обстоятельств, своими функциями.

Качественное измерение информации направлено на понимание смысла, а также на обязательное понимание информации с точки зрения потребителей. Вероятная ценность информации определяется изменением степени достижения определенной цели после его получении.

В настоящее время роль информации растет, но, к сожалению, долгое время отношения, основанные на компьютерной информации не были признаны автономным нормативно-правовым объектом. Сегодня информационные отношения в рамках правового регулирования признаются как конкретные субъекты[2].

Представление специфической сложности социальной информации как более многомерного явления представляет собой некоторую проблему в рам-

[1] Шеннон К.Э. «Работы по теории информации и кибернетике»// Издательство иностранной литературы, Москва. 1963, 832 с.
[2] Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. М.: Юринформ, 2005, 182 с.

ках правового регулирования[1]. С этой целью предпринимаются шаги для создания нового «Закона об информации» и системы мер, направленных на уголовную защиту этой группы отношений. Разнообразие мнений при определении таких понятий, как «информационная безопасность», а также «компьютерная преступность» были выдвинуты отечественными учеными-правоведами.

Современные информационные угрозы довольно разнообразны. И учитывая это, Л.И. Шершнев выступает за концепцию «информационной безопасности», как «способность государства и общества в целом и, в частности, социальной группы, личности обеспечивать вероятный уровень достаточных и защищенных информационных потоков и ресурсов для их жизнедеятельности и поддержания его полного функционирования и развития». Кроме того, «информационная безопасность направлена на противодействие практически всем информационным опасностям и угрозам, а также на негативное информационное воздействие в равной степени как на индивидуальное и общественное сознание, так и на компьютерные сети и другие информационно-технические системы. А также развитие личных и групповых действий обусловлено навыками и умениями, связанными с безопасностью поведения и сохранением постоянной готовности к адекватным мерам в рамках информационного противостояния независимо от обстоятельств»[2].

С точки зрения Н.И. Шумилова «информационная безопасность – это состояние защиты всех информационных сфер государства, а также общества и личности, которое обеспечивается комплексом мер, направленных на снижение, предотвращение или устранение негативных последствий непосредственно от воздействия на элементы информационной сферы»[3].

---

[1] Батурин Ю.М. Компьютерная преступность и компьютерная безопасность./М., 1991

[2] Л. И. Шершнев. Безопасность жизнедеятельности. Современный комплекс проблем безопасности. Учебно-методическое пособие.// Фонд национальной и международной безопасности. Москва. 2009, 111 с.

[3] Криминалистические аспекты информационной безопасности. Дис. канд. юрид. наук: 12.00.09 / Шумилов Н.И. /С.-Пб., 1997, 169 с.

Понятие «информационная безопасность» представленное Л.И. Шершневым, на наш взгляд выступает более полным, нежели чем у Н.И. Шумилова.

Качество и глубина знаний – это те обстоятельства, от которых напрямую зависит эффективное противодействие преступности не только в целом или отдельных ее видов, но и от специфики конкретного вида преступления, сопровождающегося выяснением основных причинно-следственных признаков. В юридических науках анализ конкретного вида преступления применяется к уголовному праву, криминалистике, а также к криминологическим и другим характеристикам, которые повышают внимание исследователя к конкретным аспектам, относящимся к одному и тому же виду правонарушения.

Сравнительно недавно в юридической науке предметом научных исследований стали киберпреступления. В связи с выявлением преступлений, связанных с использованием компьютера, в зарубежной прессе появились термины «компьютеризированное», а также «электронное преступление», которые не имели фактического терминологического или иного обоснования. Термин «электронное преступление» возник в связи с таким явлением, как «компьютерно-телефонный фанатизм», некорректное использование компьютеров и телефонов для заказа различных товаров и услуг через бесплатное использование информационных сетей. Хотя этот термин широко используется в правоохранительных органах, он распространился как на национальном, так и на международном уровне. Пока что нет четкого толкования термина «киберпреступности» и связанных с ним преступлений.

Общая юридическая терминология в области информационных отношений и компьютерной информации еще не разработана. Согласно Уголовному кодексу Российской Федерации, не все уголовные преступления могут в настоящее время подлежать юрисдикции.

«Компьютерное преступление» не понимается таким же образом. С уголовной точки зрения, киберпреступность понимается как «преступно критичный акт», когда электронная информация представляется как уголовное

преступление»[1]. В этом случае компьютер или компьютерная система и компьютерная сеть могут быть предметом преступления.

Т.Г. Смирнова считает, что «преступление в области компьютерной информации – это деяние, запрещенное уголовным законодательством, которое определяется нарушением неприкосновенности информационных материалов, размещенных в защищенном законом компьютерном оборудовании, а также информацией, которая причиняет или угрожает физическому лицу лишению его прав и свобод»[2]. Кроме того, по ее мнению, «действия, сопровождающиеся нарушением правил работы компьютера, а также действия, связанные с распространением вредоносных программ, негативного характера, следует рассматривать как разновидность саботажа, способного нанести довольно значительный ущерб компьютерной информации из-за разрушительного воздействия в отношении материальных носителей и находящихся на них данных».

Утверждение И. А. Клепицкого, что преступление в области компьютерной информации (киберпреступность) является «преступлением по уголовному законодательству, которое нарушает права и интересы других лиц в отношении автоматизированных систем обработки данных, а также прав и интересов физических и юридических лиц, общества и общества государства затрагивает права и неприкосновенность частной жизни, имущественные права и интересы, общественную и государственную безопасность и конституционный порядок»[3].

В настоящее время, в России имеется некоторый опыт определения составов киберпреступности с последующим уголовным преследованием, а также их квалификации и расследования. В этом контексте проблема необходимости квалифицировать киберпреступность как подкласс преступления,

---

[1] Фролов Д.Б. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом // Законодательство и экономика. / 2005. /№5, С. 23.

[2] Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации. Дис. канд. юрид. наук. М., 1999, 230 с.

[3] Комментарий к Уголовному кодексу Российской Федерации / Под общ. ред. И.А. Клепицкого. М.: ИНФРА-М, 2005.

совершенного с использованием высокотехнологичных систем, становится все более актуальной. По мнению А.И. Гурова, «преступления, обусловленные использованием высокотехнологичных систем, представляются:

– нарушение тайны переписки, а также телефонных и телеграфных переговоров, а также других сообщений, основанных на использовании специальных технических средств, предназначенных для скрытого получения информации, и в дополнение к незаконному маркетингу, приобретению с целью сбыта;

– «экспортом технологий, на которые наложен запрет, представленных научно-технической информацией и услугами, которые используются при создании военной техники и ОМП»;

– «неправомерным доступом к охраняемой законом компьютерной информации» (ст. 272 УК);

– «создание, использование и распространение вредоносных компьютерных программ» (ст. 273 УК);

– «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» (ст. 274 УК РФ)»[1].

Данное обстоятельство приводит к определению преступления в области киберпреступности, таким образом: «преступления в области компьютерной информации являются противоправным деянием, предусмотренным уголовным законодательством, определяемым нарушением прав и интересов другой стороны. Преступления такого рода напрямую связаны с эксплуатацией, модификацией и уничтожением компьютерной информации, с сопровождающимся причинением вреда или созданием для этого соответствующих угроз. Преступления такого порядка подлежат уголовному преследованию в целях защиты прав и интересов физических и юридических лиц, а также общества».

[1] Гуров А.И. Профессиональная преступность: прошлое и современность//М., 1990

Впервые в России в 1992 году был принят закон, который предписывает правовую защиту информации, размещаемой на компьютерных устройствах (базе данных). В ст. 128 Гражданского кодекса Российской Федерации, который был принят 25 октября 1994 года, электронная информация была определена в качестве особого объекта.

20 февраля 1995 года был принят закон «Об информации, информатизации и защите информации». Целью было регулировать правоотношения в сфере обмена информацией и обработки информации. Информация в данном случае означает «сведения о лицах, событиях, фактах, объектах, явлениях и процессах независимо от формы их представления». Развитие внутреннего законодательства было обусловлено разработкой в проекте Уголовного кодекса Российской Федерации в 1996 году ряда статей, предусматривающих уголовную ответственность за преступления в области компьютерной информации. Первые попытки составить статьи об уголовной ответственности в российской научной литературе за совершения компьютерных преступлений были направлены на разработку серии рекомендаций по совершенствованию действующих положений уголовного законодательства по этим вопросам.

Правой порядок «Об информации, информатизации и защите информации» был заменен Федеральным законом (27 июля 2006 года) «Об информации, информационных технологиях и о защите информации»

Этот закон стал наиболее важным нормативным документом с целью описания концепций и определений, связанных с информационными технологиями. Он определяет принципы правового регулирования отношений в области информации, информационных технологий и защиты информации, а также регулирует отношения при осуществлении права на поиск, получение, передачу, производство и распространение информации с использованием информационных технологий.

В исследованиях Ю.М. Батурина и А.М. Жодишского посвященных компьютерной преступности, совершаемой в области компьютерной

информации, существует два основных типа, это «вторжение в электронную сеть и использование в качестве технического инструмента»[1].

Первый тип включает в себя:

1) «несанкционированный доступ к компьютерной информации»;

2) «ознакомление с программным обеспечением, так называемая «логическая бомба», которая при соответствующих условиях способна частично или в целом создать угрозу полного отключения компьютерной системы»;

3) «разработку и распространение деструктивных компьютерных программ (вирусов)»;

4) «некачественную разработку компьютерных программ вычислительного характера, приводящих к тяжелым последствиям»;

5) «замену достоверной компьютерной информации»;

6) «кражу информации, содержащейся на компьютерном носителе».

В связи с этим Ю.М. Батурин и А.М. Жодзишский указывает, что в статьях Уголовного кодекса РСФСР 1960 года встречается только определенная часть вышеупомянутых преступлений, например:

– несанкционированный вход в компьютерные системы;

– загрузка закрытой компьютерной информации;

– внедрение в компьютерную систему вирусных программ деструктивного характера». В то же время было предложено установить характерные для этих преступлений основания уголовной ответственности.

Таким образом, становится возможным выделить в некоторых статьях дополнительный квалифицирующий признак, например как, «совершение незаконного действия с использованием компьютерных технологий».

В новый проект Уголовного кодекса, опираясь на идентичные документы, касающиеся защиты, внесены предложения о включении в эту кате-

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

горию компьютерное посягательство непосредственно в один из глав раздела «Преступления против общественной безопасности».

1.2 Зарубежный опыт развития уголовного законодательства в сфере компьютерной информации

Шведское законодательство стало «первооткрывателем» в области защиты компьютерной информации. Принятый в апреле 1973 г. «Закон о данных», ввел в традиционное законодательство совершенно новую концепцию – Злоупотребление компьютером».

В 1986 году в Германии возник вопрос об обеспечении уголовной ответственности за уголовные преступления в области компьютерной информации. В УК ФРГ в 1987г. «Вторым законом о борьбе с экономической преступностью» («2 Gesetz zur Bekämpfung der Wirtschaft Kriminalität») были введены составы преступлений связанные с компьютерной информацией. Киберпреступность не является самостоятельным преступлением по Уголовному Кодексу Германии. Поэтому нормы ответственности за преступления, связанные с использованием компьютеров, рассредоточены по разделам Особенной части Кодекса:

– ст. 202a «действия, направленные на получение сведений» (Daten ausspionieren), расположенная в разделе 15 «Нарушение неприкосновенности и тайны частной жизни»;

– ст. 263a «компьютерное мошенничество» (Computerbetrug), отнесена к разделу 22 «Мошенничество и преступное злоупотребление доверием»;

– ст. 269 «фальсификация данных, имеющих доказательственное значение» (Fälschung von Beweisdaten), исходя из определения нормы, относится к разделу 23 «Фальсификация документов»;

– ст. 303a «изменение данных» (Datenänderung);

– ст. 303b «компьютерный саботаж» (Computersabotage), последние составы относятся к 27 разделу «Повреждение имущества».

Определение специального термина «данные» указано в п. 2 ст. 202a «это те данные, которые сохранены или передаются электронным, магнитным или иным, непосредственно визуально не воспринимаемым способом».

Рассмотрим уголовную ответственность за указанные выше нормы:

Так, в ст. 202a «действия, направленные на получение сведений», предусмотрена ответственность тех лиц, «кто незаконно получает данные, т.е. которые ему не предназначаются и особо охраняются от незаконного к ним доступа, или кто передает их другому лицу»[1], и санкцией является лишение свободы до трех лет, либо штраф.

Уголовный кодекс ФРГ выделил как отдельный вид мошенничества, ст. 263a «компьютерное мошенничество», в санкции, которой предусмотрено лишение свободы на срок до 5 лет, либо штраф.

Указанная статья гласит: «любое лицо, которое намеревается получить имущественную выгоду для себя или третьего лица, которая наносит ущерб чужому имуществу, путем создания программы, используя неверные или неполные данные или иное несанкционированное влияние на результат обработки данных».

Состав ст. 269 «фальсификация данных, имеющих доказательственное значение» предусматривает уголовную ответственность за «сохранение или изменение при помощи компьютера, путем обмана данных, имеющих доказательственное значение, приводящее к восприятию документов как сфальсифицированных или поддельных, либо использование такого рода сохраненных или измененных данных» в виде лишения свободы на срок до 5 лет или штраф.

Составы преступлений, отнесенные к разделу 27, устанавливают ответственность наравне со способами и видами повреждения имущества, такие

[1] Уголовный кодекс ФРГ от 15 мая 1871 (в ред. от 13.11.1998 г.)

как ст. 303a «изменение данных» и ст. 303b «компьютерный саботаж». Кратко говоря, по ст. 303a ответственность наступает за «незаконное удаление и изменение данных» в виде лишения свободы на срок до двух лет, либо в виде штрафа. По ст. 303b ответственность за «нарушение обработки данных, существенно значимых для бизнеса, организаций или учреждений третьей стороны» наказывается лишением свободы на срок до пяти лет, либо штрафом.

Исходя из вышеизложенного, законодатель сконструировал составы компьютерных преступлений, таким образом, что квалифицирующий вид простого состава преступления, имеет различный объект посягательства.

Ведущие позиции в борьбе с киберпреступностью, с момента ее появления в обществе, занимают Нидерланды. Конкретные рекомендации по внесению поправок в действующее законодательство, вынесенные созданным Консультативным комитетом, в свою очередь, не дававшим определения киберпреступности, а разрабатывал ее классификацию.

Использование определения компьютерного преступления при регистрации всех случаев киберпреступности «это поведение, которое вредно и имеет отношение к устройствам, связанным с компьютерами с точки зрения хранения, передачи и обработки данных». Полицейским разведывательным управлением проводится различие между преступлениями, в которых компьютер является объектом преступления, и тех, в котором он является предметом его совершения. Также, данное управление использует только несколько видов преступлений в сфере компьютерной информации:

1. «совершаемые обычным способом, но с использованием технической поддержки в компьютерной среди»;
2. «компьютерное мошенничество»;
3. «компьютерный террор» (совершение преступлений с целью повреждения компьютерных систем):

– использование несанкционированного доступа;

– использование вредоносных программ, типа компьютерных вирусов;

– совершение других действий, включая физическое повреждение компьютера.

4. «кража компьютерного обеспечения» (пиратство);

5. остаточная категория, включающая все другие типы преступлений, которые не подпадают под вышеперечисленные категории[1].

Опираясь на мнение голландских ученых, которые утверждают, что существует множество трудностей при формулировке определения «киберпреступности», поскольку оно является не только обширным, но и специальным. Мы можем согласиться с ними, т.к. до сих пор отсутствует общепризнанное определение «киберпреступности». В 1993 году в Нидерландах был принят «закон о киберпреступности», который внес поправки в Уголовный кодекс Нидерландов, добавив в него новые составы, такие как:

– «несанкционированный доступ в компьютерные сети» (ст. 138a (1));

– «несанкционированное копирование данных» (ст. 138a (2));

– «компьютерный саботаж» (ст. 350a (1), 350b (1));

– «распространение вирусов» (ст. 350a (3), 350b);

– «компьютерный шпионаж» (ст. 273 (2)).

При рассмотрении ответственности за совершение предусмотренных УК Нидерландов, таких как:

– «вымогательство» (ст. 317);

– «запись информационных коммуникаций, кража путем обмана служб» (ст. 36c).

Были внесены изменения в редакции других статей:

– «саботаж» (ст. 161, 351);

– «подлог банковских карт» (ст. 232).

Значительное изменение претерпели такие составы как:

– «шпионаж» (ст. 98);

[1] Волженкин Б.В.(ред.) Уголовный кодекс Голландии//СПб.: Изд-во "Юрид. центр Пресс", 2001 г., 510 с.

– «вмешательство в коммуникации» (ст.139a, 139b).

Что позволяет в настоящее время использовать данные составы для борьбы с киберпреступностью, в соответствующих случаях.

Например, голландское уголовное законодательство предлагает множество возможностей для борьбы с различными видами киберпреступности, создавая дополнительные требования в дополнение к специальным нормам.

В Уголовный кодекс Польши включена глава 22 «Преступления против защиты информации», состоящая из 6-ти статей, предметом которых выступает связь с общественность в области информации. Все отношения в сфере компьютерной информации будут являться лишь частью объекта посягательств.

На данный момент мы можем упомянуть только две статьи, находящиеся в данной главе – ст. 267 и 268 Уголовного кодекса Польши.

В ст. 267 Уголовного кодекса устанавливается уголовная ответственность за «несанкционированный доступ к информации, включая повреждение электронных, магнитных или иных средств обеспечения ее безопасности». А в ст. 268 УК Польши предусматривается уголовная ответственность «лиц, не имеющих на то полномочия уничтожения, повреждения, удаления или изменение записи на компьютерном носителе информации, имеющей особое значение обороноспособности страны, безопасности связи, функционирования правительственных или государственных органов». Уголовный кодекс определяет эту статью как разглашение информации, составляющей государственную тайну.

При рассмотрении главы 25 «Преступления против имущества», мы выделяем так же две статьи, а именно ст. 278 и ст. 287, которые можно отнести к «компьютерным» составам преступления. Данные нормы предусматривают ответственность за:

– «получение без согласия управомоченного лица чужой компьютерной программы с целью извлечения имущественный выгоды» (ст. 278);

– «Влиянием неуправомоченным на то лицом на автоматизированное преобразование, собрание или передачу информации или изменение, удаление, введение новой записи на компьютерный носитель информации с целью получения имущественный выгоды или причинения вреда другому лицу» (ст. 287)[1].

Очень интересно, что в этом случае при нанесении ущерба близкому лицу, обвинение инициируется заявлением потерпевшего.

Исходя из вышеизложенного, Уголовный кодекс Польши разделяет компьютерные преступления на две отдельные группы, в зависимости от направленности преступного умысла, к примеру, поучение самой информации или же материальной выгоды. Указанное различие довольно таки спорно, т.к. в обоих случаях преступник изымает определенный объем информации. Но при всем этом, в любом случае, виновный скорее всего будет заинтересован в получении материальной выгоды, например, вознаграждение за уничтожении информации, находящейся на компьютерной технике и имеющей отношение к обороноспособности страны.

В модели Уголовного кодекса Союза Независимых Государств компьютерные преступления помещены в XII раздел «преступления против информационной безопасности», состоящей из одной главы с таким же названием и семи статей (ст. 286 – 292 УК СНГ)[2].

В целом можно говорить о сходстве проекта Уголовного кодекса СНГ и Уголовного кодекса Российской Федерации, но есть ряд существенных отличий.

По сравнению с УК РФ количество статей объясняется выделением в модельном варианте УК СНГ самостоятельных статей в зависимости от субъективной стороны (при наличии умысла). Так, помимо, «несанкционированного доступа к компьютерной информации, повлекшее неосторожные по-

[1] Уголовный кодекс Республики Польша// СПб.: Издательство «Юридический центр Пресс», 2001, 234с.
[2] Разработка Европейского законодательства по борьбе с киберпреступностью// Уголовное право, 2005, №1, 134 с.

следствия» (ст. 286 модели УК СНГ – аналог ст. 272 УК РФ), отдельно предусмотрена уголовная ответственность. К примеру, за «модификацию компьютерной информации», «компьютерный саботаж». Проект Уголовного кодекса СНГ выгодно отличается от Уголовного кодекса Российской Федерации, который имеет общий характер в отношении киберпреступности. Модель Уголовного кодекса СНГ определяет ряд понятий, например, «модификация компьютерной информации», «компьютерный саботаж», «неправомерное завладение компьютерной информацией». Однако санкции, предусмотренные нормами Уголовного кодекса СНГ, несомненно, потребуют дальнейшей проработки, поскольку существуют разногласия между общественной опасностью действий и наказанием за них. Модель Уголовного кодекса СНГ (ст. 290) предусматривает уголовную ответственность за «производство и продажу специальных средств получения несанкционированного доступа к компьютерной системе или ее сети, что также является положительным моментом».

Положительной оценки заслуживают заложенные в ст. 287 модели УК СНГ основы для правильного разграничения компьютерных и иных смежных составов преступлений. Также заслуживает внимания системное изложение квалифицирующих признаков киберпреступности. Для Уголовного кодекса Российской Федерации в целом характерно его систематическое изложение, но в главе 28 законодательный орган ограничился простым перечислением признаков. Наказания, предусмотренные в проекте Уголовного кодекса СНГ за киберпреступность, не превышают наказания за преступления средней тяжести. Однако, «неправомерное завладение информацией, совершенное при квалифицирующих обстоятельствах (сопряженное с насилием, совершенное с целью получения особо ценной информации), наказывается как тяжкое преступление» (ч. 3 ст. 289 модели УК СНГ). За особо квалифицированный вид такого преступления, например, «совершение преступления организованной группой, сопряженное с причинением тяжкого вреда здоровью или по

неосторожности смерти, либо иных тяжких последствий» – наказание назначается как за особо тяжкое преступление (ч.4 ст. 289 модели УК СНГ)[1].

Такой подход представляется вполне обоснованным, т.к. помимо общественных отношений в сфере компьютерной информации причиняется вред другому объекту, к примеру, жизни и здоровью граждан.

При совершении преступления группой лиц по предварительному сговору или организованной группой, несомненно, повышается степень и характер общественной опасности. Введение дополнительно квалифицирующего признака – «совершение преступления с целью получения особо ценной информации», представляется спорным. Несомненно, существует более или менее ценная информация, однако данная категория является оценочной и зависит от субъективного восприятия значимости информации тем или иным лицом. При введении такого квалифицирующего признака необходимо в законодательном порядке дать некоторые ориентиры, позволяющие правоприменителю объективно определять ценность информации.

Исходя из вышеизложенного, мы можем сделать вывод, что зарубежное законодательство пошло по пути разграничения киберпреступности по отношению к сфере социальных отношений, в которую вмешивается преступник.

1 Модельный Уголовный кодекс для государств – участников СНГ/ Принят постановлением Межпарламентской Ассамблеи государств / участников СНГ от 17.02.1996 г.// https://base.garant.ru

ГЛАВА 2 ЮРИДИЧЕСКИЙ АНАЛИЗ СОСТАВА НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1 Объект и предмет

Как нам известно, установление относительно существенных идентичностей, довольно типичных фактических обстоятельств, типичных для конкретного социально опасного, а также незаконного деяния с соответствующими признаками того или иного вида преступления является процессом юридической квалификации любого преступления. Согласно «традиционной» практике, началом «квалификации преступления» является анализ объекта и субъекта преступления. Затем выделяются непосредственные признаки того или иного действия, то есть определение объема и содержания объективной стороны. После этого идентифицируются все признаки предмета, а также соответствующая предметная часть субъективной стороны. Подобная схема, по справедливому замечанию профессора Н.Г. Кадникова, становится допустимым при установлении сходства или различия в совершенном акте в контексте уголовного права. Беря ее за основу, мы можем рассмотреть все признаки, определяемые несанкционированным доступом к компьютерной информации в соответствии с отдельными элементами данного состава[1].

Итак, несанкционированный доступ к охраняемой законом информации помещен непосредственно в девятый раздел Особенной части Уголовного кодекса Российской Федерации, который определяется как «Преступления против правового порядка и общественной безопасности». В общем, объект такого доступа представлен рядом связей с общественностью, которые. в свою очередь, составляют значительную часть общественной безопасности и порядка в целом.

[1] Квалификация преступлений и вопросы судебного толкования (3-е изд., перераб. и доп.). – М.: ИД «Юриспруденция», 2013. – С. 304.

Одним из характерных критериев классификации, которые объединяют киберпреступность в общей главе, является видовой объект посягательств, совокупность которого представляет собой набор социальных отношений в системе «легального», т.е. безопасного использования компьютерной информации, а также информационных ресурсов.

Непосредственным объектом анализируемого преступления, как указывается в законе, являются общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы компьютера, компьютерной системы или их сети.

Существование дополнительного объекта зависит от ущерба, нанесенного правам и законным интересам личности, общества и государства, поэтому он не является обязательным. Им могут быть, например, собственность, авторское право, право на неприкосновенность частной жизни, личная и семейная тайна, экологическая безопасность, основы конституционного строя Российской Федерации и т. д. Конечно, наличие дополнительного предмета увеличивает общественную опасность, что необходимо учитывать при установлении справедливого наказания для виновного.

Известно, что «необходимым элементом любого общественно опасного и противоправного деяния» является объект посягательств. Если при расследовании незаконного доступа к компьютерной информации выясняется, что «действия человека не причинили вреда человеку, обществу или государству», а также «действия индивида не представляют реальной опасности, то правонарушение отсутствует, поскольку в данном случае будет отсутствовать объект преступления»[1].

Гораздо сложнее найти предмет несанкционированного доступа к компьютерной информации в виде идентифицирующего признака общественно опасных и незаконных действиях, которые кратко изложены в главе 28 Особой части Уголовного кодекса. Более того, нельзя отрицать, что предмет пре-

[1] Российское уголовное право. Особенная часть / Под ред. Кудрявцева В.Н., Наумова А.В./М.: БЕК, 2013, 670 с.

ступлений, рассматриваемых этой группой, считается ключевым фактором, отличающим компьютерное преступление от преступлений, указанных в некоторых главах Уголовного кодекса Российской Федерации.

«Компьютер как информационная система, носитель информации», по мнению ученых, должен быть признан предметом этой группы преступлений. Маловероятно, что такую позицию можно считать правильной, поскольку она значительно расширяет уголовную ответственность за незаконный доступ к компьютерной информации и, следовательно, является неприемлемой.

Представляется, что предметами, за которые установлена ответственность в ст. 272 Уголовного кодекса, являются «компьютерная информация или информационные ресурсы, содержащиеся на компьютерных носителях, в электронном компьютере, компьютерной системе или их сети». Именно компьютерная информация или информационные ресурсы, которые действуют как нематериальные ценности и непосредственно затрагиваются нарушителем, посягающим на отношения с общественностью по обеспечению безопасности этой информации и нормальной работы компьютера, компьютерной системы или сети.

В иную группу преступлений, нарушающих охраняемые уголовным законом отношения собственности, можно отнести противоправные посягательства, которые имеют предмет преступления компьютерную технику, а не ее информацию. Это можно объяснить тем, что компьютерные технологии являются материальным объектом внешнего мира, созданным общественно необходимым трудом, имеют материальную ценность, мобильны и чужды преступнику. И, следовательно, выполняют все необходимые условия, которые характеризуют предмет преступлений против собственности (глава 21 Особенной части Уголовного кодекса).

Например, если виновный преднамеренно сжигает микропроцессор или выводит из рабочего состояния монитор (дисплей), его действия зависят от

квалификации, предусмотренной соответствующей частью статьи 167 Уголовного кодекса, в зависимости от конкретных обстоятельств дела.

Правонарушение лица, совершившего кражу непосредственно на электронном носителе, должно быть квалифицировано согласно соответствующей части ст. 158 УК РФ. Для обоснования сказанного, обратимся к примеру, «Органы предварительного следствия предъявили обвинение по ч.2 ст.272, п.«в» ч.2 ст. 158 УК РФ Ржевскому М.С являющемуся сотрудником отдела продаж сотовой связи. Из преступного умысла, направленного на хищение чужого имущества, получив дубликат сим-карты оператора сотовой связи, используя программное обеспечение, произвел вход на сайт платежного сервиса, расположенного в сети Интернет, и из корыстной заинтересованности, осуществил незаконный доступ к балансу учетной записи пользователя ФИО. После чего распорядился денежными средствами по своему усмотрению»[1].

Информационные команды, от которых зависит преступное воздействие, так же могут случаться на практике. Возможно, виновный вводит движущиеся части машины (жесткие диски, принтеры) в эксплуатацию, или увеличивает яркость дисплея, тем самым выводя технику из строя путем использования минимального количества команд. В таких случаях подвергаются два объекта посягательств, охраняемых законом, и поэтому содеянное следует квалифицировать по совокупности преступлений, за преступления предусматривающие ответственность против собственности и в сфере компьютерной информации[2].

Также, к примеру, действия лица, похитившего компьютерную технику и осуществившего несанкционированный доступ к информации, содержащейся в ней, должны быть квалифицированы по совокупности преступлений. В таком случае компьютерная техника выступает предметом преступления

[1] Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югра от 30.06.2016г. по уголовному делу № 1-991/2016 // https://bsr.sudrf.ru

2 Калиниченко И.А., Коробов А.А. и др. Теоретические основы противодействия неправомерному доступу в сфере информационных технологий. Под общ. ред.: Калиниченко И.А. - Орел, 2013. – С. 179.

против собственности, а предметом преступления по ст. 272 УК РФ будет являться компьютерная информация.

Термин, используемый в диспозиции статью «охраняемая законом», говорит нам о том, что действующее законодательство охраняет всю совокупность общественных отношений по правомерному и безопасному использованию не любой компьютерной информации, а только той, которая находится под защитой закона. Таким образом, следует признать, что «охраняемая законом компьютерная информации – это информация ограниченного доступа, которая имеет не только специальный правовой статус, установленный соответствующими законами Российской Федерации или законами субъектов Российской Федерации, но и по своему характеру предназначена для ограниченного круга лиц (пользователей), имеющих право на ознакомление с ней»[1].

Юридически защищенная информация может относиться к различным аспектам жизнедеятельности человека, общества и государства.

Так, согласно Государственному стандарту Российской Федерации, под защищаемой информацией (в том числе и компьютерной - прим. авторов) необходимо понимать «информацию, являющуюся предметом собственности и подлежащую защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (государством, юридическим лицом, группой физических лиц или отдельным физическим лицом)»[2].

В Федеральном законе «Об информации, информационных технологиях и о защите информации» определяется, что «защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

---

[1] Российское уголовное право. Особенная часть / Под ред. Кудрявцева В.Н., Наумова А.В.М.: БЕК, 2013. – С. 670.

[2] Защита информации. Основные термины и определения. ГОСТ Р 50922-2006 (утв. Приказом Ростехрегулирования от 27.12.2006 N 373-ст)// М., Стандартинформ, 2008.

– обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– соблюдение конфиденциальности информации ограниченного доступа;

– реализацию права на доступ к информации».

В этой же статье Федерального закона указывается, что «обладатель информации, информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

– предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

– своевременное обнаружение фактов несанкционированного доступа к информации;

– предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

– недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

– возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

– постоянный контроль за обеспечением уровня защищенности информации;

– нахождение на территории Российской Федерации без данных информации, с использованием которых осуществляется сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации»[1].

[1] Федеральный закон от 27.07.2006 N 149-ФЗ(ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации»// «Собрание законодательства РФ», 31.07.2006, N 31 (1 ч.), ст. 3448.

Под охраняемой законом информацией, собственником которой является государство, понимаются сведения, составляющие государственную тайну. Так, в Федеральном законе «О государственной тайне» указывается, что «государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации»[1].

К государственной тайне могут быть отнесены следующие сведения, неправомерный доступ к которым образует признаки преступления, выраженного в ст. 272 УК:

1) сведения в военной области о:

– содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию войск, о их боеспособности и мобилизационной готовности, о создании и использовании мобилизационных ресурсов;

– направлениях развития вооружения и военной техники, содержании и результатах выполнения целевых программ, научно - исследовательских и опытно - конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

– количестве, устройстве и технологии производства ядерного и специального оружия, технических средствах и методах его защиты от несанкционированного применения;

– тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, свойствах, рецептах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

1 Закон РФ от 21.07.1993 N 5485-1(ред. от 29.07.2018) «О государственной тайне»// «Собрание законодательства РФ», 13.10.1997, N 41, стр. 8220-8235.

– дислокации, назначении, степени готовности и защищенности режимных и особо важных объектов, об их проектировании и строительстве, а также об отводе земель, недр и акваторий для этих объектов;

– дислокации, действительных наименованиях, организационной структуре, вооружении и численности объединений, соединений и частей Вооруженных Сил Российской Федерации;

2) сведения в области экономики, науки и техники о:

– содержании планов подготовки Российской Федерации и ее отдельных регионов к возможным военным действиям, мобилизационных мощностях промышленности по изготовлению вооружения и военной техники, об объемах поставок и о запасах стратегических видов сырья и материалов, а также о размещении и фактических размерах государственных материальных резервов;

– использовании инфраструктуры Российской Федерации в интересах обеспечения ее обороноспособности и безопасности;

– силах и средствах гражданской обороны, дислокации, предназначении и степени защищенности объектов административного управления, обеспечения безопасности населения, о функционировании промышленности, транспорта и связи в целом по Российской Федерации;

– объемах, планах (заданиях) государственного оборонного заказа, выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, связях предприятий по кооперации, разработчиках или изготовителях указанных вооружения, военной техники и другой оборонной продукции;

– научно-исследовательских, опытно-конструкторских и проектных работах, технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность Российской Федерации;

– государственных запасах драгоценных металлов и драгоценных камней Российской Федерации, ее финансах и бюджетной политике (кроме обобщенных показателей, характеризующих общее состояние экономики и финансов);

3) сведения в области внешней политики и экономики о: внешнеполитической и внешнеэкономической (торговой, кредитной и валютной) деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб ее интересам;

4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности о:

– силах, средствах, источниках, методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

– системе правительственной и об иных видах специальной связи, о государственных шифрах, методах и средствах их анализа;

– методах и средствах защиты секретной информации;

– государственных программах и мероприятиях в области защиты государственной тайны.

Так же к охраняемой законом компьютерной информации относится информация в отношении сведений, составляющих служебную, коммерческую или банковскую тайну. Это обстоятельство, в частности, вытекает из положений, содержащихся в нормах гражданского и уголовного законодательства, выступающих надежной гарантией защиты служебной, коммерческой или банковской тайны.

Наиболее опасные посягательства на общественные отношения, возникающие в связи с осуществлением предпринимательской деятельности и

обеспечивающие сохранность коммерческой или банковской тайны, влекут уголовную ответственность по ст. 183 УК. К примеру, «Александровский А.Г. являясь сотрудником ООО «Альфа групп», совершил незаконное разглашение сведений составляющих коммерческую тайну без согласия их владельца, а именно передал персональные данные абонентов за денежное вознаграждение, путем копирования данных на неустановленный носитель информации»[1].

Компьютерная информация, являющаяся объектом авторского права, также считается объектом, подлежащим правовой защите. Кроме того, в соответствии с Конституцией Российской Федерации (ст. 44) интеллектуальная собственность (литература, искусство и т. д.) так же является охраняемой законом. Поэтому неправомерный доступ к такой информации влечет ответственность по ст. 272 УК.

В реальной жизни может возникнуть вопрос: является ли компьютерная информация, содержащая сведения о частной жизни конкретного человека, предметом преступления, ответственность за совершение которого предусмотрена ст.272 УК?

Ответ на этот вопрос следует признать положительным. Дело в том, что в соответствии с Конституцией Российской Федерации «каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» (ч. 1 ст.23 Конституции РФ). Установление права на поиск, получение, передачу, а также права на возможность осуществления деятельности по распространению персональных данных прямо предусмотрено в части 4 ст. 29 Конституции Российской Федерации. Конституция Российской Федерации основной закон нашего государства прямо предусматривает ограничение этого права, направленного на защиту личной жизни, уважения прав и репутации других лиц. Так, например, ч.1 ст.24 Конституции Российской Федерации гласит: «сбор, хранение, использование и

1 Приговор Орджоникидзевского районного суда (г. Екатеринбург) от 25.07.2017 по уголовному делу № 1-405/2017 // https://bsr.sudrf.ru

распространение информации о частной жизни лица без его согласия не допускается»[1]. Таким образом, Конституция России определяет основы правового режима информации о частной жизни, направленные, прежде всего на защиту прав личности.

Реализация этого конституционного положения находит свое прямое выражение в положениях уголовного закона и предусматривает ответственность за «нарушение неприкосновенности частной жизни» (ст.137 УК), «нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» (ст.138 УК), «разглашение тайны усыновления или удочерения» (ст.155 УК).

Уголовное законодательство России определяет нарушение неприкосновенности частной жизни как «незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну» (ч.1 ст. 37 УК). Следовательно, под охраной закона находится любая информация, содержащая сведения о личной или семейной тайне конкретного человека. Закон не раскрывает содержание указанных дефиниций. Как показывает теория под личной тайной понимают сведения, имеющие сугубо личный характер (взаимоотношения, связи, привычки, взгляды, встречи, обстоятельства интимной жизни и т.п.), разглашение которых лицо считает нежелательным.

Исходя из этого, все сведения о семейном бюджете и денежных вкладах, личной собственности, нотариальных действиях, и даже сведения, касающиеся состояния здоровья человека мы можем отнести к сведениям о частной жизни.

Гарантия сохранения тайны имени лиц, внедренных в организованные преступные группы, штатных негласных сотрудников органов, осуществляющих оперативно-розыскную деятельность, а так же лиц, оказывающих или оказавших содействие этим органам на конфиденциальной основе, ука-

1 Конституция Российской Федерации (принята всенародным голосованием 12.12.1993)// в «Собрании законодательства РФ», 04.08.2014, N 31, ст. 4398.

зывается в Федеральном законе «Об оперативно-розыскной деятельности». Гласности эти сведения могут быть преданы только в следующих случаях:

- с согласия этих лиц в письменной форме (ч. 2 ст. 12);
- сведения предоставляются прокурору, без согласия в случае привлечения таких лиц к уголовной ответственности (ч.3 ст. 21)[1].

Таким образом, если был произведен несанкционированный доступ к информации, содержащей сведения об именах штатных сотрудников, осуществляющих оперативно-розыскную деятельность, наравне с доступом к информации, содержащей данные человека, при условии их не разглашения. предоставившего сведения средствам массовой информации, такие деяния будут квалифицированы по ст. 272 УК РФ.

К проявлениям частной жизни, что, следовательно, возможно, будет составлять личную или семейную тайну, могут быть так же отнесены увлечения и творчество. Опираясь на вышесказанные факты, следует подчеркнуть, что не все сведения о частной жизни лица могут отвечать требованиям предмета преступления, предусмотренного ст. 137 УК РФ, а равно являться охраняемой законом. Однако, в любом случае только суд решает данный вопрос, учитывая все конкретные обстоятельства, и, прежде всего, оценку степени тяжести наступивших последствий для потерпевшего[2].

Подводя итоги изложенному, к предмету преступления относятся нематериальные ценности, а так же компьютерная информация (сведения. составляющие служебную, коммерческую, банковскую или государственную тайну, информация, являющаяся объектом авторского права, а также конфиденциальные сведения о персональных данных). Если же неправомерный доступ был к информации общего пользования, т.е. к информации неохраняемой законом, и направленной неограниченному кругу лиц, не будет образовывать признаков преступления.

---

[1]Федеральный закон от 12.08.1995 N 144-ФЗ(ред. от 06.07.2016) «Об оперативно-розыскной деятельности» // «Собрание законодательства РФ», 14.08.1995, N 33, ст. 3349.

[2] Быков В.М. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ / В.М. Быков, В.Н. Черкасов // Российский судья. - №5. - 2012. - С. 14-19

Преступления, хотя и связанные с компьютерной информацией, но не предполагающие в качестве основного непосредственного объекта общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы компьютера, компьютерной системы или сети, не указывают на анализируемый состав. Эти преступления включают, среди прочего, «нарушение конфиденциальности» (ст.137 УК), «нарушение авторских и смежных прав» (ст.146 УК), «шпионаж» (ст.276 УК) и некоторые другие общественно опасные и противоправные деяния, предметом которых вполне может выступать компьютерная информация.

Именно поэтому предмет неправомерного доступа к компьютерной информации всегда следует рассматривать в тесной связи с его объектом. Отдельный анализ предмета не позволяет уяснить то отношение, которому наносится ущерб, что, в свою очередь, может привести к ошибкам в квалификации уголовных преступлений и, следовательно, к противоречию базовым принципам уголовного права: законности и справедливости.

2.2 Объективная сторона

Объективная сторона преступления, предусмотренного ч. 1 ст. 272 УК РФ, выражается в «неправомерном доступе к охраняемой законом информации, если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование компьютерной информации».

Объективно анализируемое преступление выражается в форме активных действий, заключающихся в несанкционированном доступе виновного к компьютерной информации или информационным ресурсам. Таким образом, одним из необходимых оснований для привлечения виновного к уголовной ответственности по ст. 272 УК будет являться установление того факта, что лицо действовало именно неправомерно. Следовательно, лицо не имело право вызывать информацию, знакомиться с ней и распоряжаться ею. Строго говоря, неправомерность доступа к информации – обязательный показатель,

характеризующий рассматриваемое нами преступление с объективной стороны.

Способы неправомерного доступа к компьютерной информации могут быть различными и, как правило, не влияют на юридическую оценку поведения виновного[1]. Рассмотрим несколько способов совершения преступления, прямо влияющих на квалификацию содеянного виновным.

Речь идет о неправомерном доступе к компьютерной информации с применением насилия над личностью либо угрозой такого применения.

Действительно, на практике может возникнуть ситуация, когда лицо, не обладающее определенными навыками работы с электронно-вычислительной техникой, тем не менее, желает совершить неправомерный доступ к компьютерной информации и в этих целях насильственно заставляет законного пользователя или владельца информации войти в информационную систему и, например, скопировать либо модифицировать интересующую его (виновного) информацию.

Диспозиция как простого, так и квалифицированного состава рассматриваемого преступления не охватывает своим содержанием указанный способ его совершения. Следовательно, квалификация действий виновного по одной лишь ст. 272 УК будет в этом случае явно недостаточной.

Посягая на общественные отношения по обеспечению безопасности компьютерной информации, нормальной работы ЭВМ, системы ЭВМ или их сети, виновный, одновременно с этим, посягает и на безопасность жизни и здоровья личности (в случае психического насилия) либо здоровье конкретного человека (при реальном применении физического насилия)[2].

Именно поэтому содеянное виновным, в зависимости от конкретных обстоятельств дела, надлежит квалифицировать по совокупности с преступлением против личности.

---

[1] Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. М.: Юринформ, 2005. – С. 182.

[2] Комментарий к Уголовному кодексу Российской Федерации/Под общ. ред. С.В. Дьякова. М.: ИД «Юриспруденция», 2016. С. 798.

По ст.272 и ст.112 УК РФ следует, например, квалифицировать действия лица, которое посредством причинения средней тяжести вреда здоровью законного пользователя вынуждает его вызвать ту либо иную компьютерную информацию и уничтожить ее. При этом виновный выступает в качестве опосредованного исполнителя преступления (ч.2 ст.33 УК РФ) и, в силу этого обстоятельства, несет ответственность за содеянное единолично, если, разумеется, законный пользователь находился в состоянии крайней необходимости (ст.39 УК РФ). В противном случае ответственность наступает по правилам о соучастии в преступлении, хотя, конечно, квалификация по совокупности преступлений здесь также не исключается.

Совершая неправомерный доступ к компьютерной информации в соучастии, исполнитель должен действовать свободно, в силу собственного волеизъявления и желания принять в нем участие. Насильственные способы воздействия на личность подстрекаемого образуют соучастие только тогда, когда не создают у него состояния крайней необходимости и не подавляют его волю до такой степени, что он теряет способность руководить своими действиями либо осознавать их характер. Поэтому по ст. 272 и ст.119 УК РФ необходимо квалифицировать действия лица, под страхом убийства заставившего оператора ЭВМ совершить акт неправомерного доступа к компьютерной информации. Если же виновный высказывал угрозы причинения легкого вреда здоровью или побоев, его действия квалифицируются как подстрекательство к совершению преступления, предусмотренного ст.272 УК РФ. Исполнителем преступления будет являться лицо, на сознание которого и было направлено психическое воздействие. Это объясняется тем, что причиненный вред здесь явно не соответствовал характеру и степени угрожавшей опасности и обстоятельствам, при которых опасность устранялась, когда указанным интересам был причинен вред более значительный, чем предотвращенный (ч.2 ст.39 УК РФ).

Действующее уголовное законодательство не выделяет квалифицированные составы преступлений по признаку использования электронной тех-

ники. Поэтому в тех случаях, когда неправомерный доступ к компьютерной информации выступает способом совершения другого умышленного преступления, а электронно-вычислительная техника используется в качестве орудия для достижения преступной цели, содеянное виновным квалифицируется по совокупности преступлений.

Так, если лицо с целью хищения чужого имущества расшифровало код, управляющий электронной системой банка, и ввело команду ЭВМ перевести денежные средства на свой текущий счет, то действия такого лица, с учетом всех обстоятельств дела, необходимо квалифицировать по совокупности с преступлением против собственности. Для примера, Приговором мирового суда Восточного округа г. Белгорода, подсудимый приобрел сим-карту сотового оператора, к номеру которой был привязан мобильный банк другого лица. Из корыстных побуждений, действуя умышленно, с целью хищения денежных средств, переводил с банковской карты через приложение мобильный банк и с использованием компьютера на свой личный счет денежные средства, тем самым осуществлял неправомерный доступ к охраняемой законом компьютерной информации[1].

В силу особой специфики рассматриваемого вида преступления, орудием его совершения, как правило, является компьютерная техника, то есть различные виды электронно-вычислительных машин, аппаратные средства, периферийные устройства, а также линии связи, с помощью которых вычислительная техника объединяется в информационные сети. Наиболее широко применяемое орудие совершения анализируемого преступления – персональный компьютер.

Определенную сложность у сотрудников правоохранительных органов могут вызвать вопросы, связанные с установлением времени и места совершения неправомерного доступа к компьютерной информации. Дело в том, что стремительное развитие компьютерной техники уже сегодня вышло на

[1] Приговор мирового суда Восточного округа г. Белгород от 27.12.13 по уголовному делу № 1-39/2013 // https://rospravosudie.com

качественно новый уровень. Созданы мировые информационные сети, объединившие пользователей практически из всех развитых стран мира. Поэтому время и место совершения общественно опасного деяния (место происшествия) все реже может совпадать с местом и временем наступления общественно опасных последствий.

Между тем практика борьбы с компьютерной преступностью хранит немало ярких примеров, когда сам факт неправомерного доступа к охраняемой информации фиксировался в одной стране, а преступные последствия наступали на территории другого государства. Иллюстрацией этому служит пример уничтожения, блокирования и модификации охраняемой законом компьютерной информации. Приговором Центрального районного суда г. Челябинск, подсудимый ранее являясь заместителем начальника технического обслуживания ООО, в связи со служебной необходимостью получил доступ к имени пользователя и паролю почтового сервера ООО расположенному в стране Нидерланды, после увольненья из чувства мести, используя данные почтового сервера, не имея права доступа к защищаемой законом информации, действуя умышленно удалил информацию, находящуюся на данном сервере[1].

Действующее уголовное законодательство России временем совершения любого преступления признает время совершения общественно опасного действия (бездействия) независимо от времени наступления последствий (ч.2 ст.9 УК РФ). Очевидно, данное правило не должно распространяться на вопрос о месте совершения преступления, который так и не получил законодательного разрешения. Как представляется, местом совершения неправомерного доступа к компьютерной информации следует признавать территорию того государства, где это преступление было окончено[2].

---

[1] Приговор Центрального районного суда г. Челябинск от 2010 года по уголовному делу № 1-356/2010 // https://centr.chel.sudrf.ru

[2] Аменицкая Н.А. Органы дознания и оперативно-розыскная деятельность: исторический аспект и современное состояние проблемы / Н.А. Аменицкая // Российская юстиция. - 2013. - № 7. - С. 11 - 13.

Указанная точка зрения полностью корреспондирует с законодательным положением ст.8 УК РФ об основании уголовной ответственности: «основанием уголовной ответственности является совершение деяния, содержащего все признаки состава преступления, предусмотренного настоящим Кодексом».

Анализ диспозиции ч. 1 ст.272 УК РФ позволяет сделать вывод о том, что состав рассматриваемого преступления конструктивно сформулирован как материальный. Как известно, материальные составы, помимо прочих признаков, предполагают обязательное наличие вредных последствий. В противном случае состав не считается полным. Другая же точка зрения фактически опровергает этот правовой императив, устанавливая правило, согласно которому наличие состава несанкционированного доступа к компьютерной информации презюмируется даже тогда, когда необходимые последствия еще отсутствуют: «местом совершения преступления признается место совершения общественно опасного действия (бездействия) независимо от места наступления вредных последствий».

Справедливость такого положения подтверждается и тем обстоятельством, что на практике могут возникнуть ситуации, когда лицо совершает акт неправомерного доступа к компьютерной информации на территории того государства, уголовное законодательство которого не признает такое поведение преступным. В этом случае лицо подлежит уголовной ответственности по ст.272 УК РФ, если преступные последствия наступили на территории России[1]. Следовательно, неправомерный доступ к компьютерной информации считается совершенным на территории Российской Федерации, если приготовление или покушение осуществлялось за границей, а оканчивается это преступление в нашей стране.

Аналогичным образом будет решаться данный вопрос и в том случае, если вне пределов территории Российской Федерации осуществляется орга-

1 Панов В.П., Сотрудничество государств в борьбе с международными уголовными преступлениями. М., 2006. С. 14.

низаторская деятельность, подстрекательство или пособничество совершению неправомерного доступа к компьютерной информации. Организатор, подстрекатель и пособник, где бы их деятельность ни начиналась, несут ответственность по законодательству того государства, где исполнитель завершил преступление.

Наконец, при совершении неправомерного доступа к компьютерной информации на территории двух и более государств, применяется закон того государства, где преступление было закончено или пресечено[1].

Обязательными признаками объективной стороны преступления, предусмотренного ч.1 ст.272 УК РФ, являются не только общественно опасные действия, но и наступление общественно опасных последствий, а также причинная связь между этими двумя признаками.

Общественно опасные последствия неправомерного доступа к охраняемой законом компьютерной информации выражаются в виде уничтожения, блокирования, модификации либо копирования компьютерной информации. В законе не раскрывается содержание указанных понятий. Поэтому имеются все основания остановиться на них более подробно.

Под уничтожением информации следует понимать такое изменение ее первоначального состояния (полное либо в существенной части), при котором она перестает существовать в силу утраты основных качественных признаков. При этом для квалификации преступления по ст.272 УК не имеет значения, имелась ли у потерпевшего копия уничтоженной виновным информации, или нет.

Блокирование представляет собой закрытие информации, характеризующееся недоступностью или же невозможности ее использования по прямому назначению со стороны законного пользователя.

Модификация заключается в изменении первоначального состояния информации (например, реструктурирование или реорганизация базы дан-

1 Всестороннее исследование проблемы киберпреступности – Проект//ООН Нью-Йорк. 2013 С. 360.

ных, удаление или добавление записей, содержащихся в ее файлах, перевод программы для ЭВМ или базы данных с одного языка на другой), не меняющей сущности объекта.

Под копированием понимают перенос информации или части информации с одного физического носителя на другой (например, запись информации в память компьютерного носителя).

Факт просмотра или вызова компьютерной информации, хранящейся на машинном носителе, состава анализируемого преступления не образует. Необходимо, как минимум, установить факт переноса указанной информации на другой носитель. Кроме того нельзя забывать, что несанкционированное ознакомление с охраняемой законом компьютерной информацией может выступать в качестве приготовления или покушения на совершение иного преступления: например, вымогательства, разглашения сведений, составляющих коммерческую или банковскую тайну, шпионаж и др. В этом случае дополнительной квалификации по ст.272 УК не требуется.

Итак, оконченным данное преступление признается с момента фактического наступления хотя бы одного из тех·разновидностей вредных последствий, перечень которых альтернативно указан в диспозиции статьи закона. Следовательно, действия лица, заведомо не приводящие к указанным в диспозиции последствиям, не образуют неправомерного доступа к компьютерной информации.

К примеру, нет оснований привлекать к уголовной ответственности по ст.272 УК лицо, которое с помощью подбора пароля обошло систему защиты межбанковской компьютерной сети и, получив доступ к информации о счетах клиентов, из любопытства ознакомилось с ними.

Другое дело, если действия лица, желавшего уничтожить, заблокировать, модифицировать или скопировать компьютерную информацию были пресечены до стадии оконченного преступления, иными словами, до наступления общественно опасных последствий, указанных в законе. В этом случае

содеянное виновным, квалифицируется по правилам о покушении на неправомерный доступ к компьютерной информации (ч.3 ст.30 УК РФ).

В контексте нашего изложения необходимо отметить, что преступление, ответственность за совершение которого предусмотрена ч.1 ст.272 УК РФ, относится к категории преступлений небольшой тяжести (ч.2 ст.15 УК РФ). Поэтому, в силу положений, содержащихся в ч. 2 ст.30 УК РФ, приготовление к его совершению нельзя рассматривать в качестве уголовно-наказуемой стадии развития преступной деятельности виновного.

Наконец, следующим необходимым признаком объективной стороны неправомерного доступа к компьютерной информации является причинная связь между противозаконными действиями виновного и наступившими вредными последствиями. Для признания лица виновным в совершении неправомерного доступа к компьютерной информации, органы следствия и суд обязаны с полной достоверностью установить наличие причинной связи между деянием лица и вредными последствиями в виде уничтожения, блокирования, модификации либо копирования информации, а не исходить в решении этого вопроса из каких-либо догадок или предположений.

В теории уголовного права России под причинной связью понимают такое отношение между явлениями внешнего мира, при котором одно явление (причина) закономерно с внутренней необходимостью и порождает, вызывает другое явление (следствие)[1].

Основываясь на этом определении причинной связи можно утверждать, что ответственность по ст.272 УК РФ наступает только в том случае, если преступные последствия, альтернативно отраженные в ее диспозиции, явились именно необходимым следствием, закономерно вызванным неправомерным доступом лица к охраняемой законом компьютерной информации.

В том случае, когда уничтожение, блокирование, модификация, копирование информации не являются следствием неправомерного доступа к

1 Уголовное право России. Общая часть: Учебник / Под ред. В.П. Ревина. - М.: Юстицинформ. 2016. С. 580.

компьютерной информации, а наступают в силу иных причин (например, создания вредоносной программы для ЭВМ, нарушения правил эксплуатации ЭВМ и т.д.), признаки преступления, предусмотренного ст.272 УК, отсутствуют. При этом необходимо помнить - в деянии лица могут содержаться признаки иного состава преступления, что обязаны устанавливать работники органов дознания, следствия и суда.

Если, например, допустить, что причиной уничтожения охраняемой законом компьютерной информации стало нарушение правил эксплуатации вычислительной машины, допущенное оператором ЭВМ, деяние виновного надлежит квалифицировать по соответствующей части ст.274 УК РФ.

Разумеется, обязательные признаки объективной стороны состава преступления не являются достаточным основанием и не предрешают характера уголовной ответственности. Согласно ст. 8 УК РФ единственным основанием уголовной ответственности следует признать «совершение деяния, содержащего все признаки конкретного состава преступления, предусмотренного законом», в том числе, характеризующие деяние с внутренней, субъективной стороны.

2.3 Субъект

Лица, эксплуатирующие компьютерные системы, а так же обслуживающие их, будут являться участниками отношений в области компьютерной безопасности.

Интересен тот факт, когда юридическое лицо осуществляет несанкционированный доступ к информации, то ответственности будет подлежать исполнитель этого преступления.

В ст. 272 УК РФ можно выделить несколько категорий субъектов преступления.

«Лица, осуществляющие неправомерный доступ к компьютерной информации»[1]. Признаки этой категории:

– вменяемое физическое лицо, достигшее 16 лет;

– любое лицо, как работающее в автоматизированной информационной системе или сети, либо пользующееся их услугами (законный пользователь), но не имеющее права работы с определенной информацией, так и постороннее лицо (не являющееся законным пользователем).

Таким образом, в соответствии с ч. 1 ст. 272 УК РФ человеку не обязательно иметь специальные навыки или подготовку, а так же занимать определенную должность или выполнять конкретную работу. Есть несколько случаев, когда у правонарушителя не было технических знаний вообще. В большинстве случаев данное преступление совершается лицом с достаточно высокой квалификацией, особенно когда речь идет о киберпреступности, поскольку для этого требуются сложные технологические и информационные действия. Чем сложнее и «умнее» метод несанкционированного доступа, тем более ограничен круг подозреваемых лиц.

«Лицо, осуществляющие неправомерный доступ к компьютерной информации в группе по предварительному сговору или организованной группой» (ч. 3 ст. 272).

Совершение данного преступления группой лиц по предварительному сговору означает, что два или более лица, ранее договорившиеся, прилагая совместные усилия, осуществляют или же пытаются осуществить несанкционированное проникновение в компьютер такими способами как, например, взломав систему электронной защиты, или же подобрав пароль при подключении к каналу связи. Такие действия организатора, подстрекателя или пособника будут квалифицированы по ст. 33 и ч. 3 ст. 272 УК РФ. Так, например, в апелляционном постановлении Московского городского суда, на основании ранее вынесенного приговора, в котором указывалось, что дирек-

[1] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 27.12.2018)// «Собрание законодательства РФ», 17.06.1996, N 25, ст. 2954.

тор ЗАО «Х» с целью создания условий дл разрыва деловых отношений, установленных ОАО «А» и ООО «А», и устранения конкурента своей фирмы в данной сфере, принял решение дискредитировать ООО «А».

Вступил в преступный сговор с ведущим специалистом по информационной безопасности в своей фирме, а так же двумя работниками оказывающими «хакерские услуги». Осуществляя свой умысел, каждый из них выполняя свою роль, используя вредоносную программу (бот-сеть), нанесли компьютерную Ddos-атаку (в своем роде «отказ в обслуживании») на информационные ресурсы ОАО «А». Осуществление данной атаки привело к блокированию работы системы оплаты и приобретения электронных билетов на сайте на весь период атаки[1].

При этом преступления, совершаемые такими группами, можно условно разделить на два типа: это российские организованные преступные группы и организованные группы на международном уровне.

«Лицо, осуществляющее неправомерный доступ к компьютерной информации с использованием своего служебного положения» (ч.3 ст. 272)

Таким лицом могут выступать государственный служащий, работники организаций и учреждений, которые по своей профессиональной деятельности обслуживают информационные системы.

Лицо, имеющее доступ к компьютеру, системе или их сети – это законный пользователь документированной информации, а также лицо, которое по роду деятельности вправе временно использовать компьютер и знакомиться с защищаемой законом информацией, при этом не являющееся служащим этой организации.

«Лица, осуществляющие неправомерный доступ из корыстной заинтересованности или причинившее крупный ущерб» (ч. 2 ст. 272).

Крупным ущербом признается сумма, превышающая 1 млн. руб., а корыстная заинтересованность заключается в стремлении путем совершения

[1] Апелляционное постановление Московского городского суда. г. Москва от 25.11.13 по уголовному делу « 10-11502/2013 //

действий, направленных на получение доступа к охраняемой законом информации в результате которого лицо получает имущественную выгоду для себя или других.

Субъект преступления, ответственность за совершение которого предусмотрена ч. 1 ст. 272 УК РФ, является общим – физическое вменяемое лицо, достигшее к моменту совершения преступления шестнадцатилетнего возраста.

2.4 Субъективная сторона

Как известно, субъективную сторону противоправного и общественно опасного поведения субъекта, характеризуют признаки в виде вины, мотива и цели. Представляется, что данные признаки отражают связь сознания и воли лица с совершаемым общественно опасным деянием1. Их уголовно-правовое значение не равнозначно применяемо к несанкционированному доступу к компьютерной информации.

Поскольку вина – это необходимый признак субъективной стороны, рассматриваемого преступления, то без нее не будет состава преступления, а значит, не является уголовно наказуемым деянием. Такие признаки субъективной стороны, как мотив и цель совершения этого преступления, которые законодатель счел необязательными, приобретают иное значение. На основании общепринятого положения уголовного закона, вина представляет собой психическое отношение человека к совершенному противоправному деянию, выраженное в форме умысла или неосторожности.

В то время как, диспозиция статью не раскрывает субъективную сторону преступления, предусмотренного ст. 272 УК РФ, мы можем говорить о форме вины, как о прямом или косвенном умысле.

1 Российское уголовное право. Особенная часть / Под ред. Кудрявцева В.Н., Наумова А.В.М.: БЕК, 2013. – С. 670.

Рассматривая точку зрения, которая гласит: «неправомерный доступ к компьютерной информации может быть совершен только с прямым умыслом». В то же время, привлечение лица к ответственности в случае совершения преступления с косвенным умыслом не будет ограничено законом. Исходя из практики, виновный не всегда желает наступления вредных последствий, в особенности, если преступление совершено из озорства или же «спортивного интереса»[1].

В силу этого положения ментальный фактор вины, характерный для состава анализируемого преступления, заключается в том, что правонарушитель осознает тот факт, что доступ к компьютерной информации запрещен законом. В то же время преступник понимает не только реальный характер своего поведения, но и его социально опасный характер. Кроме того, нарушитель видит возможность или неизбежность фактического возникновения общественно опасных последствий в виде уничтожения, блокирования, модификации или дублирования информации. Следовательно, субъект представляет природу вредных воздействий, осознает их социальную значимость и причинно-следственную связь.

Волевой момент вины отражает либо желание, либо сознательное предположение о возникновении определенных вредных воздействий, либо, по крайней мере, безразличное отношение к ним.

Несанкционированный доступ к компьютерной информации, совершенный по неосторожности, исключает правовое основание для привлечения лица к уголовной ответственности. Указанное положение полностью корреспондирует ч. 2 ст. 24 УК РФ «деяние, совершенное по неосторожности, признается преступлением только в том случае, когда это специально предусмотрено соответствующей статьей Особенной части настоящего Кодекса»[2].

---

1 Быков В.М. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ / В.М. Быков, В.Н. Черкасов // Российский судья. - №5. - 2012. - С. 14-19.

[2] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 27.12.2018)// «Собрание законодательства РФ», 17.06.1996, N 25, ст. 2954.

О неосторожности в диспозиции ст. 272 УК не сказано, следовательно, деяние может быть совершенно лишь умышленно. В силу этого обстоятельства трудно согласиться с мнением авторов одного из научно-практических комментариев к Уголовному кодексу РФ, в котором утверждается, что «неправомерный доступ к информации может совершаться как с умыслом, так и по неосторожности». Признание этой точки зрения противоречит законодательному положению, закрепленному в ч. 2 ст. 24 УК, что в свою очередь ведет к возможности необоснованного привлечения лица к уголовной ответственности за неосторожное поведение. Для обоснования сказанного рассмотрим пример судебного разбирательства по делу Агаркова П.И. «по просьбе сотрудника полиции Агарков П.И. нашел в информационно телекоммуникационной сети Интернет нелицензионную копию программного продукта права на которую принадлежат компании CE Европейское частное акционерное общество, и инструкцию по ее установке и модификации, сохранив их на флеш-накопитель, после чего дал согласие Е. К.В. на установку указанного программного обеспечения.

Кроме того, используя один из принадлежащих ему флеш-накопителей, на котором имелись программные файлы, с помощью которых он осуществил модификацию путем внесения изменений в системные файлы программного продукта с целью обхода средств лицензионной защиты программы, тем самым получил неправомерный доступ к компьютерной информации, права на которую принадлежит компании CE Европейское частное акционерное общество, тем самым причинил правообладателю ущерб. Осуществляя поиск программы, он узнал, что копируемый им программный продукт является не лицензионным, стоимости его он не знал. Поскольку с программой он был ранее не знаком, то для ее установки и активации он нашел пошаговую инструкцию с иллюстрациями, и сохранил данные программы на флеш-накопитель»[1].

[1] Приговор Свердловского районного суда г. Белгород от 23.07.2018 по уголовному делу № 1-143/2018 // https://sudact.ru

Так же могут быть различными цели и мотивы несанкционированного доступа к компьютерной информации. Они не будут влиять на квалификацию преступления, т.к. не обладают обязательными признаками рассматриваемого преступления. Точное определение мотивов и целей данного состава, однако, позволяет не только выявить причины, побудившие человека совершить преступление, но и определить виновному справедливое наказание.

По большей части, повышающим общественную опасность деяния является корысть, которая, как правило, выступает побуждающим фактором в совершении преступления. В качестве корыстного доступа к компьютерной информации, может служить пример действий Карпова С.В., который «действуя умышленно, незаконно, из корыстной заинтересованности, заведомо осознавая факт контрафактности программных продуктов, поскольку у него не имелось лицензионных соглашений с правообладателями данных программных продуктов, вопреки воле правообладателей, неправомерно приобрел с помощью ЭВМ через глобальную сеть Интернет контрафактные экземпляры программных продуктов, для сбыта за материальное вознаграждение»[1].

Наравне с корыстью, анализируемое преступление может совершаться из чувства мести, зависти, хулиганства, желания испортить деловую репутацию конкурента, «спортивного интереса» или желания скрыть другое преступление и т.д.

Подводя итоги рассмотрения субъективных признаков неправомерного доступа к охраняемой законом компьютерной информации, приведем наиболее важные выводы, к которым мы пришли. Так, анализируя вопросы вины по отношению к уголовно-наказуемому несанкционированному доступу к компьютерной информации, мы разделяем точку зрения большинства ученых-юристов, которые считают, что совершение преступления, ответствен-

1 Приговор Советского районного суда г. Орск от 19.11.2018 по уголовному делу № 1-315/2018 // https://bsr.sudrf.ru

ность за которое предусмотрена ст. 272 УК РФ, характеризуется виной в форме умысла.

Эта позиция обусловлена пониманием смысла ст. 272 УК РФ. Полагаем, что не являются преступлениями деяния, совершенные по неосторожности, если это специально не предусмотрено соответствующей статьей Особенной части УК РФ.

ЗАКЛЮЧЕНИЕ

Все важнейшие сферы общества в настоящее время компьютеризированы. Число возможных операций, происходящих между людьми и выполняемых с помощью ЭВМ, со временем будет только расти. Естественно увеличится число преступных посягательств на компьютерную информацию.

До введения Уголовного кодекса Российской Федерации правоохранительные органы сталкивались и начинали борьбу с компьютерными преступлениями при помощи традиционных норм о краже, мошенничестве, злоупотреблении доверием и др. Такой подход был не вполне удачным, поскольку многие преступления связанные с компьютерными технологиями не охватывались составами традиционных преступлений. Это повлекло включение новой главы 28 УК РФ «Преступления в сфере компьютерной информации».

Преступления, содержащиеся в данной главе, представляют собой деяния, сущность которых заключается не в использовании самой по себе электронно-вычислительной техники в качестве средства совершения преступления. Она включает общественно-опасные деяния, посягающие на безопасность информации и систем обработки информации с использованием ЭВМ. Объектами могут быть как технические средства, программные обеспечения, так и информация.

Даже после введения данной главы в УК РФ на практике часто возникают вопросы при квалификации того или иного состава преступления по той или иной статье УК РФ, связанного с информационными технологиями, т.к. общественная опасность посягательств на интересы, охраняемые главой 28 УК РФ, в сочетании с недостатками диспозиции норм были недооценены. А так же имеет место быть недостаточный уровень подготовки првоприменительных органов, призванных вести борьбу с компьютерными преступлениями.

Данное положение можно объяснить рядом причин, среди которых необходимо выделить:

а) недостаточная разработанность теоретической модели компьютерных преступлений;

б) недостаточная изученность криминологической характеристики компьютерных преступлений и в этой связи неразработанность более совершенных методик по раскрытию и расследованию преступлений, комплекса мер предупредительного характера и рекомендаций по виктимологической профилактике.

Анализируя материал работы можно сделать вывод о необходимости внесения значительного массива дополнений и изменений в действующее законодательство Российской Федерации.

1. Дополнить диспозицию ч.3 ст.272 УК РФ новым квалифицирующим признаком: «Те же деяния, совершенные с целью устрашения населения или воздействия на принятие решения органами государственной власти и(или) местного самоуправления, а также воспрепятствование нормальной деятельности средств массовой информации, органов государственной власти и местного самоуправления, государственных и муниципальных учреждений, предприятий», установив санкцию до 5-ти лет лишения свободы;
2. Внести изменения в ст. 151 УПК РФ и отнести преступления, предусмотренные частями 2.3,4 ст. 272 УК РФ к подследственности органов ФСБ РФ;
3. Введение в Российское законодательство института уголовной ответственности юридических лиц, в т. ч. за компьютерные преступления. В частности, 23 ноября 2001 г. в Будапеште была принята Конвенция о киберпреступности, ратифицированная 47-ю государствами. К сожалению, Россия не является страной-участницей данной Конвенции как раз по причине отсутствия в УК РФ нормы, предусматривающей уголовную ответственность юридических лиц. Это, безусловно, создает препятствия эффективному международному сотрудничеству в борьбе с компьютерной преступностью;

4. Включить квалифицирующий признак «в том числе с использованием компьютерных технологий» в ст. 242 (Незаконное распространение порнографических материалов и предметов);

5. Включить квалифицирующий признак: «совершенное с использованием компьютерных технологий» в ст. 284 (Утрата документов, содержащих государственную тайну), ст. 292 (Служебный подлог), гл. 30 (Преступление против государственной власти), ст. 298 (Клевета в отношении судьи, присяжного заседателя, прокурора), гл. 31 (Преступления против правосудия).

Дальнейшее усовершенствование законодательства в области преступлений в сфере компьютерной информации поможет не только избежать проблем в настоящее время, но и будет способствовать предотвращению появления еще более глобальных проблем в будущем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ I НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

1. Волженкин Б.В.(ред.) Уголовный кодекс Голландии//СПб.: Изд-во «Юрид. центр Пресс», 2001 г., С. 510.
2. Всестороннее исследование проблемы киберпреступности – Проект//ООН Нью-Йорк. 2013 С. 360.
3. Комментарий к Уголовному кодексу Российской Федерации / Под ред. Лебедева В.М. М.: Юрайт, 2013. – С. 564.
4. Комментарий к Уголовному кодексу Российской Федерации / Под общей ред. руководителя Департамента законодательства о государственной безопасности и правоохранительной деятельности Министерства юстиции Российской Федерации, государственного советника юстиции 2-го класса С.И. Никулина. М., 2001. – С.724.
5. Комментарий к Уголовному кодексу Российской Федерации / Под ред. Наумова А.В.М.: Юристъ, 2004. – С. 678.
6. Комментарий к Уголовному кодексу Российской Федерации / Под общ. ред. И.А. Клепицкого. М.: ИНФРА-М, 2005.
7. Комментарий к Уголовному кодексу Российской Федерации/Под общ. ред. С.В. Дьякова. М.: ИД «Юриспруденция», 2016. С. 798.
8. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993)// в «Собрании законодательства РФ», 04.08.2014, N 31, ст. 4398.
9. Модельный Уголовный кодекс для государств – участников СНГ/ Принят постановлением Межпарламентской Ассамблеи государств / участников СНГ от 17.02.1996 г.// https://base.garant.ru

10. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 27.12.2018)// «Собрание законодательства РФ», 17.06.1996, N 25, ст. 2954.
11. Уголовный кодекс Республики Польша// СПб.: Издательство «Юридический центр Пресс», 2001. — С. 234.
12. Уголовный кодекс ФРГ от 15 мая 1871 (в ред. от 13.11.1998 г.).
13. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 01.04.2019, с изм. от 17.04.2019)// «Собрание законодательства РФ», 24.12.2001, N 52 (ч. I), ст. 4921.
14. Указ Президента Российской Федерации от 28 июня 1993 г. № 966 (ред. от 22.03.2005г.) «О концепции правовой информатизации России» // https://base.garant.ru
15. Федеральный закон от 27.07.2006 N 149-ФЗ(ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации»// «Собрание законодательства РФ», 31.07.2006, N 31 (1 ч.), ст. 3448.
16. Закон РФ от 21.07.1993 N 5485-1(ред. от 29.07.2018) «О государственной тайне»// «Собрание законодательства РФ», 13.10.1997, N 41, стр. 8220-8235.
17. Защита информации. Основные термины и определения. ГОСТ Р 50922-2006 (утв. Приказом Ростехрегулирования от 27.12.2006 N 373-ст)// М., Стандартинформ, 2008.
18. Федеральный закон от 12.08.1995 N 144-ФЗ(ред. от 06.07.2016) «Об оперативно-розыскной деятельности» // «Собрание законодательства РФ», 14.08.1995, N 33, ст. 3349.

РАЗДЕЛ II ЛИТЕРАТУРА

1. Александров А. Внимание вирус // Аргументы и факты. 2005. 21 дек.
2. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. М.: Юринформ, 2005. – С. 182.

3Гуров А.И. Профессиональная преступность: прошлое и современность//М., 1990

3. Завидов Б.Д., Ибрагимова З.А. Мошенничество в СВТ // Современное право. - 2011. - №4. - С. 43.
4. Калиниченко И.А., Коробов А.А. и др. Теоретические основы противодействия неправомерному доступу в сфере информационных технологий. Под общ. ред.: Калиниченко И.А. - Орел, 2013. – С. 179.
5. Квалификация преступлений и вопросы судебного толкования (3-е изд., перераб. и доп.). – М.: ИД «Юриспруденция», 2013. – С. 304.
6. Компьютерная преступность и компьютерная безопасность / Батурин Ю.М., Жодзишский А.М. - М.: Юрид. лит., 1991. – С. 160.
7. Крыжановская А.А. Использование программ для ЭВМ - деятельность, создающая повышенную опасность для окружающих // Журнал российского права. - 2004. - №6. - С. 13 - 15.
8. Л. И. Шершнев. Безопасность жизнедеятельности. Современный комплекс проблем безопасности. Учебно-методическое пособие.// Фонд национальной и международной безопасности. Москва. 2009 – 111с.
9. Разработка Европейского законодательства по борьбе с киберпреступностью // Уголовное право. - 2005. - №1. - С. 134.
10. Российское уголовное право. Особенная часть / Под ред. Кудрявцева В.Н., Наумова А.В.М.: БЕК, 2013. – С. 670.
11. Талимончик В.П. Компьютерные преступления и новые проблемы сотрудничества государств // Законодательство и экономика. - 2005. - №5. - С. 14.
12. Уголовное право России. Общая часть: Учебник / Под ред. В.П. Ревина. - М.: Юстицинформ. 2016. С. 580.
13. Фролов Д.Б. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом // Законодательство и экономика. - 2005. - №5. - С. 23.

14. Шеннон К.Э. «Работы по теории информации и кибернетике»// Издательство иностранной литературы, Москва. 1963 – С. 832.

РАЗДЕЛ III ПОСТАНОВЛЕНИЯ ВЫСШИХ СУДЕБНЫХ ИНСТАНЦИЙ И МАТЕРИАЛЫ ЮРИДИЧЕСКОЙ ПРАКТИКИ

1. Приговор Советского районного суда г. Орск от 19.11.2018 по уголовному делу № 1-315/2018 // https://bsr.sudrf.ru
2. Приговор Орджоникидзевского районного суда (г. Екатеринбург) от 25.07.2017 по уголовному делу № 1-405/2017 // https://bsr.sudrf.ru
3. Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югра от 30.06.2016г. по уголовному делу № 1-991/2016 // https://bsr.sudrf.ru
4. Приговор Свердловского районного суда г. Белгород от 23.07.2018 по уголовному делу № 1-143/2018 // https://sudact.ru
5. Приговор мирового суда Восточного округа г. Белгород от 27.12.13 по уголовному делу № 1-39/2013 // https://rospravosudie.com
6. Апелляционное постановление Московского городского суда г. Москва от 25.11.13 по уголовному делу № 10-11502/2013 // https://rospravosudie.com

РАЗДЕЛ IV ДИССЕРТАЦИИ И АВТОРЕФЕРАТЫ ДИССЕРТАЦИЙ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ

1. Аменицкая Н.А. Органы дознания и оперативно-розыскная деятельность: исторический аспект и современное состояние проблемы / Н.А. Аменицкая // Российская юстиция. - 2013. - № 7. - С. 11 - 13.
2. Быков В.М. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ / В.М. Быков, В.Н. Черкасов // Российский судья. - №5. - 2012. - С. 14-19.

3. Быков В.М. Новое: об уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ / В.М. Быков, В.Н. Черкасов // Российский судья. - №7. - 2012. - С. 16-21.
4. Криминалистические аспекты информационной безопасности. Дис. канд. юрид. наук: 12.00.09 / Шумилов Н.И. - С.-Пб., 1997. – С.169.
5. Панов В.П., Сотрудничество государств в борьбе с международными уголовными преступлениями. М., 2006. С. 14.
6. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации. Дис. канд. юрид. наук. М., 1999. – С.230.