Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Южно-Уральский государственный университет
(Национальный исследовательский университет)»
Институт открытого и дистанционного образования
Кафедра «Управление и право»

РАБОТА ПРОВЕРЕНА
Рецензент
Начальника ОМВД России
по Чесменскому району
подполковник полиции
_____А.В.Колесов
18 января 2018 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой
_____ А.А. Демин
23 января 2018 г.

Уголовно – правовая характеристика преступлений в сфере компьютерной информации

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
ЮУрГУ – 40.03.01.2018.39223. ВКР

Руководитель работы
доцент кафедры УиП
_____ Л.В.Красуцких
19 января 2018 г.
Автор работы
студент группы ДО–426
_____ Е.В.Полтавский
19 января 2018 г.
Нормоконтролер
ст. преподаватель кафедры УиП
_____ Е.Н. Бородина
22 января 2018 г.

Челябинск 2018

АННОТАЦИЯ

Полтавский Е.В. Уголовно – правовая характеристика преступлений в сфере компьютерной информации. – Челябинск: ЮУрГУ, 2018, ДО–426, 57 с., библиогр. список – 55 наим., плакаты – 13 наим.

Целью квалификационной работы состоит в изучении и анализе положений, характеризующих понятие «компьютерного преступления» и уголовно-правовой состав неправомерного доступа к информации, а также в выявлении недостатков в современном законодательстве по теме исследования и предложении рекомендации по их устранению

Предметом исследования является законодательство, направленное на борьбу с преступностью в сфере высоких информационных технологий.

Задачи дипломного исследования – изучить обобщение научных материалов по теме исследования и проанализировать современное законодательство, регулирующее преступления в сфере компьютерной информации. На этой основе сформулировать теоретические выводы и практические предложения, которые могут быть использованы при совершенствовании законодательства, повышении эффективности деятельности правоохранительных органов, а также в учебных целях при преподавании курса Уголовного права в средних и высших учебных заведениях.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 6
1 ЮРИДИЧЕСКИЙ АСПЕКТ НОРМАТИВНО – ПРАВОВОЙ БАЗЫ, РЕГУЛИРУЮЩИЙ ОТНОШЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ……..... 9
1.1 Понятие преступлений в сфере компьютерной информации, их появление и развитие в законодательстве России 9
1.2 Зарубежное уголовное законодательство регулирующее отношения в сфере компьютерной информации …….. 22
2 ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ. 29
2.1 Объективные и субъективные признаки преступления предусмотренного ст. 272 УК РФ .....…….. 29
2.2 Объективные и субъективные признаки преступления предусмотренного ст. 273 УК РФ ……. 35
2.3 Объективные и субъективные признаки преступления предусмотренного ст. 274 УК РФ ……... 41
2.4 Проблема квалификации преступлений предусмотренных гл.28 УК РФ.....…….. 45
ЗАКЛЮЧЕНИЕ…… 50
БИБЛИОГРАФИЧЕСКИЙ СПИСОК……. 54

ВВЕДЕНИЕ

Стремительное развитие компьютерных технологий и широкое использование электронно-вычислительных систем практически во всех сферах жизнедеятельности человека поставили многочисленные проблемы в области правового регулирования отношений, связанных с компьютеризацией общества. Это дает основание поставить вопрос о формировании отрасли компьютерного права, одним из основных аспектов которой являются так называемые компьютерные посягательства. Об актуальности проблемы свидетельствует обширный перечень возможных способов компьютерных преступлений.

Объектами посягательств могут быть сами технические средства (компьютеры и периферийные устройства) как материальные объекты, программное обеспечение, базы данных и информация, как таковая. А сами преступления, где применяются компьютерные технологии, чрезвычайно многогранны и сложны, например, это может быть: перехват конфиденциальных сигналов пейджинговых и сотовых станций, подделка кредитных карт, несанкционированный доступ к информации, ввод в программное обеспечение «логических бомб», которые частично или полностью выводят из строя компьютерную систему, разработка и распространение компьютерных вирусов, хищение компьютерной информации и многое другое.

Одним из наиболее распространенных видов компьютерных посягательств является неправомерный доступ к компьютерной информации. Такие преступления чаще посягают на охраняемую законом информацию и совершаются с умыслом на добычу и неправомерное использование ее в корыстных целях. У данного вида компьютерных преступлений большой потенциал в виду того, что информация растущими темпами приобретает характер основного ресурса человеческой деятельности и опасность неправомерного доступа к ней трудно переоценить.

В России же научная среда только в начале 90-х приступила к исследованию компьютерной преступности и на данный момент степень научной разработанности проблемы в отечественной литературе весьма невысока. За последние годы опубликован ряд работ, посвященных, в основном, криминологическим и криминалистическим аспектам компьютерных преступлений. Уголовно-правовые же аспекты компьютерных правонарушений в настоящее время выражены в научной литературе гораздо слабее. В монографиях и статьях, в основном, затрагивается вопрос об объекте, предмете, орудиях совершения компьютерного деликта и их соотношение между собой. Некоторые работы содержат конструктивную критику главы 28 Уголовного кодекса РФ, как с уголовно-правовой, так и с информационной точки зрения.

Но не только в теории, но и на практике в нашей стране нечем было отреагировать на волну компьютерных преступлений. Преступный мир всегда опережал на шаг вперед правоохранительную систему, беря на вооружение все лучшее, что могло придумать общество, когда как второй, приходилось на ходу изменять средства борьбы с первым. Но даже при имеющихся средствах и методах, борьба с компьютерной преступностью проходит на крайне низком

уровне. Причинами недостаточно высокой эффективности работы следственного аппарата и органов внутренних дел по раскрытию компьютерных преступлений являются некомпетентность сотрудников в юридической и технической стороне таких преступлений, слабая научно-техническая вооруженность, низкая эффективность тактики производства следственных действий, выбор ошибочных направлений расследования.

На основании изложенного, следует сделать вывод о том, что актуальность обозначенной проблемы определяется тем, что компьютерные преступления приобрели в странах с развитой телекоммуникационной инфраструктурой настолько широкое распространение, что для борьбы с ними в уголовное законодательство были введены специальные составы преступлений. Традиционные меры гражданско-правовой ответственности, ориентированные, прежде всего на возмещение убытков, не смогли сыграть роль сдерживающего фактора и воспрепятствовать широкому распространению этого вида правонарушений

Особую тревогу в этом плане вызывает факт появления и развития в России нового вида преступных посягательств, ранее неизвестных отечественной юридической науке и практике и связанный с использованием средств компьютерной техники и информационно-обрабатывающих технологий компьютерных преступлений. Последние потребовали от российского законодателя принятия срочных адекватных правовых мер противодействия этому новому виду преступности.

Степень научной разработанности темы исследования. В последние годы проблемы преступности в области компьютерной информации все чаще стали освящаться в научной литературе. Исследованием данных вопросов занимались: Агапов А.Б., Батурин Ю.М., Белкин Р.С., Жодзишский А.М., Зуев К.А., Исаченко И.И., Карась И.З., Литвинов А.В., Могилевский И.М., Полежаев А.П., Россинская Е.Р., Черкасов В.Н., Черных А. и другие.

Однако, несмотря на теоретическую и практическую значимость указанных исследований, в них не уделено достаточного внимания рассмотрению проблем, связанных с преступлениями в сфере высоких информационных технологий.

Цель исследования состоит в изучении и анализе положений, характеризующих понятие «компьютерного преступления» и уголовно-правовой состав неправомерного доступа к информации, а также в выявлении недостатков в современном законодательстве по теме исследования и предложении рекомендации по их устранению.

В соответствии с поставленной целью в процессе исследования нам необходимо решить следующие задачи:

1. изучить историю появления и развитие преступлений в сфере высоких информационных технологий;
2. рассмотреть понятие и дать общую характеристику преступлений в сфере компьютерной информации;
3. исследовать законодательство России об уголовной ответственности за преступления в сфере компьютерной информации;

4. дать уголовно-правовую характеристику преступлениям в сфере компьютерной информации;
5. проанализировать проблемы, возникающие в области борьбы с компьютерными преступлениями и предложить пути их решения.

Характер решаемой проблемы, цели и задачи исследования определяют, каким должен быть объект исследования. Объектом настоящего исследования являются организационно-правовые отношения, складывающиеся в сфере охраны целостности компьютерной информации.

Предметом исследования является законодательство, направленное на борьбу с преступностью в сфере высоких информационных технологий.

Изучение темы работы основано на использовании таких научных методов исследования как: общетеоретический, анализ, синтез, логический, сравнительно-правовой, исторический, статистический, а также метод анализа и толкования правовых актов.

Теоретическая основа исследования. Отдельным вопросам, касающимся преступлений в сфере компьютерной информации, а также проблемам, возникающим в области борьбы с компьютерными преступлениями, посвящены труды следующих правоведов: Андреев Б.В., Батурин Ю.М., Жодзишский А.М., Вехов В.Б., Проценко Д.Е., Сальников В.П., Карпинский О., Скуратов Ю.И., Лебедев В.М., Кочои С., Савельев Д., Крылов В.В., Ляпуно Ю., Максимов В., Наумов В., Симкин Л.С., Талимончи В.П., Фролов Д.Б., Старостина Е.В. и других исследователей, а также работы зарубежных специалистов: Д. Айкова, Дж. Вейценбаума, Н. Винера, Д. Керра, Д. Макнамара, С. Мэдника,и др.

Научная новизна исследования заключается в попытке пересмотра отдельных положений, касающихся особенностей преступлений в сфере компьютерной информации, также нами были выдвинуты предложения общетеоретического и практического характера по совершенствованию борьбы с компьютерными преступлениями.

Теоретическая и практическая значимость исследования состоит в том, что в работе содержится обобщение научных материалов по теме исследования и анализируется современное законодательство, регулирующее преступления в сфере компьютерной информации. На этой основе сформулированы теоретические выводы и практические предложения, которые могут быть использованы при совершенствовании законодательства, повышении эффективности деятельности правоохранительных органов, а также в учебных целях при преподавании курса Уголовного права в средних и высших учебных заведениях.

1 ЮРИДИЧЕСКИЙ АСПЕКТ НОРМАТИВНО – ПРАВОВОЙ БАЗЫ, РЕГУЛИРУЮЩИЙ ОТНОШЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1. Понятие преступлений в сфере компьютерной информации, их появление и развитие в законодательстве России.

Основоположником теории информации был американский ученый К.Э. Шеннон, который в 1948 году впервые определил само понятие «информация» и дал вероятностно-статистическое определение понятию «количество информации» [15, с 33], связывая это явление с кибернетикой – наукой, занимающейся общими законами преобразования информации в сложных управляющих системах [40,с. 22]. Она рассматривает информацию не как общественный феномен, т.е. информацию, производимую и потребляемую обществом, а в более узком техническом аспекте, как информацию, циркулирующую по электронным каналам связи. Кибернетика доказала, что информация имеет непосредственное отношение к процессам управления и развития, обеспечивающим функционирование любых систем [24,с. 4].

Качественное измерение информации предполагает понимание смысла, необходимости информации для определенных потребителей. Для человека содержание информации важнее, чем ее объем. Значимость информации определяется через изменение вероятности достижения некоторой цели после получения информации [49,с. 31].

Информационные отношения долгое время не признавались самостоятельным объектом правового регулирования, однако в настоящее время роль информации настолько возросла, что информационные отношения признаны специфическим предметом правового регулирования.

Социальная информация это сложное многоаспектное явление, что обуславливает сложности в правовом регулировании информационных отношений. С этой целью создается новое «информационное» законодательство и система мер уголовно-правовой защиты данной группы отношений. Наблюдается большое разнообразие мнений российских ученых-юристов в определениях таких понятий как «информационная безопасность» и «компьютерная преступность» [42, с. 34].

Н.И. Шумилов под информационной безопасностью понимает состояние защищенности информационной сферы государства, общества, личности, обеспечиваемое комплексом мер по снижению, предотвращению или исключению негативных последствий от воздействия на элементы информационной сферы. Думается, что, понятие информационной безопасности, данное Л.И. Шершневым, более емкое, не требующее дальнейшего толкования такого понятия как информационная сфера, чем у Н.И. Шумилова.

С учетом многообразия информационных угроз Л.И. Шершнев под информационной безопасностью понимает «способность государства, общества, социальной группы, личности обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности и жизнеспособности устойчивого

функционирования и развития; противостоять информационным опасностям и угрозам, негативным информационным воздействием на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические системы информации; вырабатывать личностные и групповые навыки и умения безопасного поведения; поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно не было навязано» [50, с. 35].

Результативность противодействия преступности в целом и отдельным её видами напрямую зависит, как известно, от качества и глубины знаний о ней, от специфики вида преступности, уяснение сущностных характеристик ее причин. В юридических науках при анализе конкретного вида преступности используются уголовно-правовая, криминалистическая, криминологическая и иные характеристики, концентрирующие внимание исследователя на определенных сторонах одного и того же явления. Конкретное содержание криминологической характеристики преступлений заключается в выявлении всех признаков, составляющих в своей совокупности и взаимосвязи её структуру, в которой выделяется три блока: первый блок – криминологически значимые признаки преступления; второй блок – данные, раскрывающие криминологическую ситуацию совершения преступлений таких типов; третий блок – признаки, определяющие специфику деятельности по предупреждению преступности .

По характеру проявлений и своей сущности основными элементами криминологической характеристики компьютерной преступности являются: её общественная опасность, отграничение компьютерной преступности от других смежных явлений, её типичные свойства и на этой основе выделение типологии компьютерных преступлений, сведения о социальных условиях компьютерных преступлений (социально-политических, геополитических, социально-экономических, временных и иных), проблемы латентности, личность компьютерного преступника, мотив и цель преступления, свойства личности потерпевшего, а также комплекс мер противодействия на основе установления причин и условий, воспроизводящих данный вид преступности, иных факторов, способствующих совершению компьютерных преступлений. В основе криминологической характеристики, безусловно, лежит процесс выделения данного вида преступности в качестве самостоятельного предмета научного исследования, уточнение понятийного аппарата и особенностей компьютерных преступлений в конкретных общественно-социальных условиях, определенных пространственно-временными границами.

Компьютерные преступления и компьютерная преступность стали предметом научного исследования сравнительно недавно. Термин «компьютерная» или «электронная» преступность впервые появился в зарубежной печати в связи с выявлением первых правонарушений, совершенных с использованием возможностей ЭВМ, и не имел ни терминологического, ни иного (в том числе и криминологического) обоснования. Он возник применительно к так называемому «компьютерно-телефонному фанатизму», который выражался в недобросовестном использовании компьютеров и телефонов для заказа различных

товаров и услуг через информационные сети различных торговых фирм без оплаты. Тем не менее, этот термин стал широко использоваться в правоприменительной практике и распространяться как в национальном, так и в международном масштабе. В настоящее время однозначной трактовки понятия компьютерного преступления и взаимосвязанного с ним понятия компьютерной преступности не выработано.

В.В. Крылов информационными преступлениями считает общественно опасные деяния, совершенные в области информационных правоотношений и запрещенные уголовным законом под угрозой наказания [32, с. 11].

По нашему мнению, можно согласиться с Н.И. Шумиловым о наличии группы однородных преступлений, одним их признаков состава которых является информация. Преступления рассматриваемого вида есть преступления в сфере информационной безопасности, или информационные преступления.

Общеюридическая терминология в сфере информационных отношений вообще, и в отношении компьютерной информации в частности, до сих пор не установлена. В настоящее время в Уголовном кодексе России криминализированы далеко не все правонарушения в информационной сфере, или как их называют, в области высоких технологий, а лишь компьютерные правонарушения.

Понятие «компьютерные преступления» до сих пор в литературе трактуется по-разному. Существует мнение, что «с точки зрения уголовно-правовой охраны под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства». В данном случае «в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть».

Т.Г. Смирнова под преступлениями в сфере компьютерной информации подразумевает «запрещенные уголовным законом общественно-опасные виновные деяния, которые, будучи направлены на нарушение неприкосновенности охраняемой законом компьютерной информации и ее материальных носителей (в частности, компьютерной техники (ЭВМ), систем ЭВМ или их сетей), причиняют либо создают угрозу причинения вреда жизни и здоровью личности, правам и свободам человека и гражданина, государственной и общественной безопасности» [45, с. 161]. Также, Т.Г. Смирнова полагает, что нарушение правил эксплуатации ЭВМ и распространение зловредных программ деструктивного характера следует рассматривать как разновидность диверсий, наносящих значительный ущерб компьютерной информации посредством разрушительных воздействий в отношении материальных носителей и зафиксированных на них данных.

Третья точка зрения, которой придерживается И.А. Клепицкий такова, что преступлением в сфере компьютерной информации (компьютерным преступлением) является «предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и

интересам физических и юридических лиц, общества и государства (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности и конституционному строю)» [47, с. 353].

В настоящее время в России накоплен определенный опыт выявления составов компьютерных преступлений, привлечения к уголовной ответственности, их квалификации и расследования. Поэтому все больше встает необходимость в представлении компьютерных преступлений как подкласса преступлений, совершаемых посредством возможностей высоких технологий. По мнению А.И. Гурова, к преступлениям в области высоких технологий относятся:

1. нарушение тайны переписки, телефонных переговоров, телеграфных и иных сообщений с использованием специальных технических средств, предназначенных для негласного получения информации, и также незаконный сбыт или приобретение в целях сбыта таких средств;
2. незаконный экспорт технологий научно-технической информации и услуг, используемых при создании вооруженной техники, оружия массового уничтожения;
3. неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК);
4. создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК);
5. нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК) [22, с. 36].

Изложенное дает основание определить преступления в сфере компьютерной информации (компьютерные преступления) следующим образом – это предусмотренное уголовным законом, противоправное, виновное нарушение чужих прав и интересов, связанное с использованием, модификацией, уничтожением компьютерной информации, причинившее вред либо создавшее угрозу причинения вреда подлежащим уголовно-правовой охране правам и интересам физических и юридических лиц, общества и государства (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности в области высоких технологий и конституционному строю).

Следует отметить, что понятие «компьютерных» или же «информационных» преступлений базируется исключительно на действующем уголовном законодательстве в этой области. Действительно, в России, например, глава 28 Уголовного кодекса РФ «Преступления в сфере компьютерной информации» предусматривает три состава преступлений - ст.272-274. Название соответствующей главы в Уголовном кодексе РФ некоторые российские ученые связывают с тем, что в формулировании соответствующих составов преступлений законодателем акцент был сделан на защиту именно самой компьютерной информации, хотя и признают, что название главы является в известной мере условным.

Для наиболее полного осмысления данных видов преступлений необходимо уяснить элементы их составов: объект, объективную сторону преступлений, субъект, субъективную сторону преступлений.

Родовым объектом компьютерных преступлений является общественная безопасность. В качестве дополнительных объектов в ряде случаев могут выступать права и интересы граждан в сфере обеспечения личной, семейной, врачебной и т.п. тайны, интересы собственности, защищенность государственной, банковской, коммерческой тайны и т.п.

Видовым объектом преступлений, предусмотренных в гл.28 Уголовного кодекса РФ, является совокупность общественных отношений, обеспечивающих состояние защищенности процессов создания, сбора, хранения, передачи и использования компьютерной информации, в которых правомерно участвуют собственники, владельцы и пользователи информации (информационная безопасность). В наименовании гл.28 законодатель использует термин «информация», что дало основание некоторым авторам считать именно информацию (или компьютерную информацию) объектом данных преступлений. Объектом рассматриваемых видов преступлений является информация, а действия преступника следует рассматривать как покушение на информационные отношения общества. Однако представляется, что компьютерную информацию следует рассматривать в качестве предмета данных составов, а объектом - информационную безопасность.

Информация признается одним из прав граждан. Всеобщая декларация прав человека и гражданина [1] принятая Генеральной Ассамблеей ООН 10 декабря 1948 г., в ст. 19 закрепила право каждого человека на свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ. Следуя приоритету норм международного права, Конституция Российской Федерации, принятая всенародным голосованием 12 декабря 1993 года [2] в ч.4 ст.29 подтвердила и гарантировала это право граждан, ограничив его сведениями, составляющими государственную тайну. Вместе с тем Конституция РФ содержит ряд иных ограничений, связанных с распространением информации. В частности, ст.23 закрепляет право граждан не неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а ст.24 запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

В соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» [11] от 14 июля 2006г. информация определяется как «сведения (сообщения, данные) независимо от формы их представления» (ст. 2).

В некоторых составах гл.28 УК РФ помимо информации предметом преступлений являются также компьютеры, их отдельные составляющие, компьютерные сети.

Большей частью преступления в сфере компьютерной информации могут совершаться только путем действия - неправомерный доступ к компьютерной

информации или создание либо использование вредоносных программ для ЭВМ. Однако нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети возможно и путем бездействия - в виде невыполнения обязательных предписаний таких правил.

Неправомерный доступ к компьютерной информации и нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети сформулированы как преступления с материальным составом, а создание либо использование вредоносных программ для ЭВМ - с формальным. В качестве последствий в ст.272 и 274 УК РФ указываются: уничтожение, модификация, блокирование либо копирование информации, нарушение работы ЭВМ или системы ЭВМ, причинение существенного вреда и т.п.

Временем совершения компьютерного преступления (временем совершения общественно опасного деяния независимо от времени наступления последствий - ч.2 ст.9 УК РФ) является момент нажатия клавиши клавиатуры компьютера или кнопки манипулятора («мыши»), отсылающей последнюю компьютерную команду, независимо от того, в какое время наступили опасные последствия.

Значительно сложнее обстоит дело с определением места совершения преступления. Поскольку большое количество компьютерных преступлений совершается в компьютерных сетях, объединяющих несколько регионов или стран, лидирующее место среди которых занимает всемирная компьютерная сеть Internet, постольку место совершения деяния и место наступления последствий могут отделять многие километры, таможенные и государственные границы. Один из московских межмуниципальных судов рассмотрел уголовное дело по факту хищения средств с использованием компьютерной сети Internet. Гражданин России Г., используя домашний компьютер, в одном из сайтов сети Internet обнаружил программу, производящую безналичные расчеты с кредитных карт. Г. скопировал программу на свой компьютер. После этого Г., входя в виртуальный магазин, реальный аналог которого располагался в Канаде, производил заказ и предварительную оплату товаров с чужих кредитных карточек, используя вышеупомянутую программу. После этой трансакции Г. незамедлительно отказывался от приобретения товара, однако для возврата денег указывал уже иные номера кредитных карт - собственных или своих сообщников. При этом последние были как гражданами России, так и Литвы. Деньги либо немедленно обналичивались через банкоматы, либо с помощью кредитных карт производилась покупка товаров в тех магазинах Москвы и Вильнюса, где расчеты возможны также с помощью кредитных карт. На первый взгляд, в данном деянии затронуты три страны. Однако на самом деле их значительно больше, так как пострадавшие лица, с банковских карточек которых незаконно списывались денежные средства якобы в оплату товаров, являлись гражданами различных стран.

Уголовный кодекс РФ не содержит нормы, определяющей место совершения преступления, поэтому им может быть место как совершения деяния, так и наступления последствий, либо то место, в котором деяние окончено либо пресечено.

Если применить по аналогии норму о времени совершения преступления, то местом его совершения надлежит считать место отдачи последней компьютерной команды, однако принцип законности российского законодательства (ч. 2 ст. 3 УК РФ) запрещает применение уголовного закона по аналогии. Следует также учитывать, что преступления с материальными составами считаются оконченными с момента наступления таких последствий. Общественную опасность преступления определяет не само деяние, а тот вред, который оно причинило или могло причинить. Поэтому место наступления последствий может быть определяющим. Такой подход согласуется со ст.8 УК РФ, где говорится о составе преступления как о единственном основании уголовной ответственности.

О важности определения места совершения преступления красноречиво говорит следующий пример. Российским программистом Л. и его сообщниками, являющимися гражданами других государств, с использованием компьютера, расположенного в Санкт-Петербурге, через электронную компьютерную систему телекоммуникационной связи Internet вводились ложные сведения в систему управления наличными фондами «City Bank of America», расположенного в Нью-Йорке. В результате такой деятельности было похищено более 10 млн. долларов США со счетов клиентов банка. В организованную преступную группу входили граждане США, Великобритании, Израиля, Швейцарии, ФРГ и России. Однако при привлечении Л. к уголовной ответственности в Лондоне судебная инстанция отложила принятие решения по этому делу на неопределенный срок ввиду того, что подсудимый использовал компьютер, находящийся на территории Российской Федерации, а не на территории США, как того требовало законодательство Великобритании. В результате просьба правоохранительных органов США и России о выдаче Л. была отклонена [19, с 11].

Если же говорить о мировой правоприменительной практике, то наиболее распространенными преступлениями с использованием компьютерной техники являются: компьютерное пиратство, компьютерное мошенничество, распространение вредоносных (вирусных) программ и компьютерный саботаж. К компьютерному пиратству относят, прежде всего, деятельность «хакеров» по неправомерному доступу к компьютерной информации. Когда результатом подобной деятельности являются модификация информации и утечка денежных средств - она превращается в компьютерное мошенничество. Второй вид компьютерного пиратства - незаконное копирование, тиражирование и сбыт компьютерных программ.

Затрагивая проблему компьютерного пиратства, представляет интерес тот факт, что для зарубежного законодательства очевидна следующая тенденция: составы собственно компьютерных преступлений (действия против только охраняемой компьютерной информации) либо просто отсутствуют, либо существуют наряду с традиционными составами (мошенничество, выдача государственной тайны, собирание и распространение персональных данных). Последние, либо предусматривают самостоятельный состав, который выступает как специальный по отношению к общему (тому же мошенничеству), либо находятся в той же статье в качестве квалифицированного состава.

Большинство компьютерных преступлений - это проявления профессиональной и организованной преступности, нередко носящей групповой транснациональный характер. Причем часто в состав группы входит непосредственный работник кредитной организации или иной компании, которая впоследствии оказывается пострадавшей (по некоторым оценкам, при хищениях с использованием компьютерных средств до 80% таких деяний совершались «изнутри»).

Транснациональный характер компьютерной преступности, быстрые темпы ее распространения обусловливают неизбежность объединения сил и средств многих государств по противостоянию этому явлению. В настоящее время создается острая необходимость разработки международно-правовой базы предотвращения инцидентов, связанных с обменом информацией, борьбы против «информационного терроризма», разработки комплекса мер международного характера, предотвращающих деструктивное использование средств воздействия на национальные и глобальные информационные ресурсы.

С момента зарождения человеческого общества люди испытывают потребность в общении друг с другом. Первоначально общение (обмен сведениями) осуществлялось жестами, знаками, мимикой и нечленораздельными звуками, затем появились человеческая речь, письменность, книгопечатание. В XX столетии получили развитие такие средства коммуникации, как телеграф, телефон, радио, кино, телевидение, компьютер. Параллельно проходил и иной процесс: по мере появления различных достижений науки и техники многие из них принимались на вооружение преступного мира. Однако внедрение во все сферы деятельности компьютерной техники сыграло наиболее существенную роль в деле технического вооружения преступности. «Невидимость» компьютерного преступника и одновременно «удлинение его рук» путем доступа к любым охраняемым секретам - военным, финансовым, иным - делают его весьма привлекательным для представителей преступного мира. Компьютерные махинации, как правило, остаются незамеченными на фоне уличной преступности. Даже по неполным оценкам экспертов, эти преступления обходятся минимум в 200 млрд. долларов ежегодно. Банковский грабитель рискует жизнью за 10 тыс. долларов, электронный, манипулируя компьютером и ничем не рискуя, может получить 1 млн.

Информатизация современного общества привела к формированию новых видов преступлений, при совершении которых используются вычислительные системы, новейшие средства телекоммуникации и связи, средства негласного получения информации и т.п. За последние 10-15 лет резко увеличилось количество преступлений с использованием вычислительной техники или иной электронной аппаратуры. Для совершения преступлений все чаще используются устройства, в основе которых лежат высокоточные технологии их изготовления и функционирования, иными словами, это преступления, в которых используются высокие технологии.

Так, начальник отдела по делам о преступлениях в сфере экономики и компьютерной информации Контрольно-методического управления

Следственного комитета при МВД РФ Г. Егоров отметил, что в СССР первое преступление в сфере высоких информационных технологий было совершено в 1979 году в Вильнюсе. Ущерб государству тогда составил 80 тысяч рублей - на эти деньги можно было приобрести 8 автомобилей «Волга» [26].

Первые преступления с использованием компьютерной техники в России появились в 1991 г., когда были похищены 125,5 тыс. долларов США во Внешэкономбанке СССР. Весь мир облетело уголовное дело по обвинению Левина и др., совершивших хищение денег с банковских счетов на большом расстоянии с использованием ЭВМ.

С тех пор статистика по преступлениям в сфере компьютерной информации выглядит следующим образом. по данным ГИЦ МВД России, в 1997г. было зарегистрировано всего лишь 7 преступлений в данной сфере, в 1998г. – 66, в 1999г. – 294, а в 2000г. их количество составило 800. На протяжении последующих лет эта цифра все возрастала и к 2014г. достигла 1739 зарегистрированных преступлений, в 2015г. данный показатель был равен 2383 преступления за год, в 2016г. – 1748, а за первые четыре месяца 2017г. (январь – апрель) было зарегистрировано 629 преступлений [20]. При этом необходимо отметить, что в данную статистику попали лишь преступления, о которых стало известно по различным причинам. Многие ученые, говоря о статистических данных, связанных с компьютерными преступлениями, как в России, так и в мире считают их крайне заниженными.

Как следует из представленных данных, количество регистрируемых преступлений в сфере компьютерной информации представляет собой стабильно неуклонно растущую кривую. Рост числа правонарушений в сфере компьютерной информации идет не менее быстрыми темпами, чем компьютеризация в России.

Жертвами преступников становятся учреждения, предприятия и организации, использующие автоматизированные компьютерные системы для обработки бухгалтерских документов, проведения платежей и других операций. Чаще всего мишенями преступников становятся банки. Особая актуальность вопросов защищенности технических средств приема, передачи и накопления информации от несанкционированного доступа была отмечена и отечественным законодателем.

Остается актуальной проблема борьбы с организованной преступностью, которая, прибегая к услугам высококвалифицированных специалистов, стала все чаще использовать различные технические средства - от обычных персональных компьютеров и традиционных средств связи до сложных вычислительных систем и глобальных информационных сетей, в том числе и Internet. Сфера применения информационных технологий в преступных целях весьма обширна.

Таким образом, с развитием общественно-экономических отношений объемы перерабатываемой информации постоянно увеличиваются, и если XX век многие ученые называли веком энергетики, то XXI - веком информатики. По мнению Сальникова В.П. ныне действует правило: «кто владеет информацией, тот владеет миром» [44,с. 101]. Научно-технический прогресс принес человечеству такие незаменимые в современной жизни новшества, как компьютеры и Internet.

Повсеместное внедрение данных технологий повлекло за собой возникновение новых видов ресурсов - информационных. Информация обрела реальную цену и с развитием информационных технологий становится все более ценным товаром. Но новые технологии стимулировали возникновение и развитие и новых форм преступности, в первую очередь компьютерных. Основную часть в этой сфере совершается с помощью компьютерных сетей. В последние годы специалистами замечена тенденция стремительного роста компьютерных преступлений посредством глобальной компьютерной сети Internet.

Широкая сфера применения компьютерных технологий затрагивает чаще уже известные виды преступлений, но только совершенные в новой форме или новым способом.

Мировая уголовно-правовая практика в зависимости от традиций законодательства той или иной страны идет в решении вышеназванной проблемы двумя путями: или путем дополнения традиционных составов преступлений новыми, в данном случае - компьютерными, аспектами, или же путем формирования новых норм и институтов права, объединенных единым специфичным объектом преступления.

Российское уголовное право и законодательство всегда шло по второму пути развития, беря за основу криминализации новых разновидностей преступлений признак их объекта и находя для него место в уголовно-правовом «дереве объектов». Хотя некоторые теоретики (Батурин Ю.М. и Жодзинский А.М.) предлагали объединить пути, внеся в Уголовный кодекс самостоятельные статьи, а ряд статей дополнить квалифицирующими признаками.

Но до изменений в Уголовный кодекс требовалось еще создать базу нормативных актов, где были бы определены основные термины и понятия в области компьютерной информации, урегулированы вопросы ее распространения, охраны авторских прав, имущественные и неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием программного обеспечения и новых информационных технологий. Также необходимо было осуществить законодательное раскрытие понятий информационной безопасности и международного информационного обмена. До 1992 года вообще не было законодательно установлена какая-либо защита отношений в сфере высоких технологий.

23 сентября 1992 года принимается Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» [7] (ныне утратил силу в связи с введением в действие части четвертой Гражданского кодекса РФ). Основной идеей этого закона, а также принятого одновременно с ним Закона Российской Федерации «О правовой охране топологий интегральных микросхем» [8] (ныне утратил силу в связи с введением в действие части четвертой Гражданского кодекса РФ) являлось урегулирование отношений в сфере защиты прав авторов и разработчиков программно-технического обеспечения.

В Законе о правовой охране программ впервые в отечественной законодательной практике были зафиксированы важнейшие понятия и правовые

конструкции, отражающие представления законодателя об элементах охраняемой сферы. Давались определения целому ряду терминов, «программа для ЭВМ», «база данных», «модификации программы» и другие, положивших основу развитию правовой терминологии в данной области [7].

Следует отметить, что Закон Российской Федерации «Об авторском праве и смежных правах» (ныне утратил силу в связи с введением в действие части четвертой Гражданского кодекса РФ) от 9 июля 1993г. регулировал отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнений, постановок, передач организаций эфирного или кабельного вещания (смежные права).

Закон Российской Федерации «О государственной тайне» [6] от 21 июня 1993г., урегулировал отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Законом «Об обязательном экземпляре документов» [12] от 29 декабря 1994г. впервые определяется понятие документа.

Принятый в 1994 году Гражданский кодекс Российской Федерации [3] (ст.128) впервые отнес к объектам гражданских прав информацию и результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность). В статье 139 законодатель конкретизировал свои представления об информационных отношениях, включив в эту сферу вопросы, связанные со служебной и коммерческой тайной (ныне норма утратила силу в связи с введением в действие части четвертой Гражданского кодекса РФ и реализована в данной части ГК РФ и в ФЗ №98-ФЗ «О коммерческой тайне» от 29.07.2004).

Федеральный закон «Об информации, информатизации и защите информации» принятый в 1995 году, регулировал отношения, возникающие при:

1. формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;
2. создании и использовании информационных технологий и средств их обеспечения;
3. защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Закон не затрагивает отношений, регулируемых законодательством об авторском праве и смежных правах.

Целью Федерального закона «Об участии в международном информационном обмене» [13] от 4 июля 1996г. является создание условий для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, защита интересов Российской Федерации, субъектов Российской Федерации и муниципальных образований при международном информационном обмене, защита интересов, прав и свобод физических и юридических лиц при международном информационном обмене. В дополнение к определениям, установленным ранее, данный Закон ввел ряд новых

определений, таких, как «массовая информация», «информационные ресурсы», «информационные продукты», «информационные услуги» и др.

Пришедший им на смену Федеральный закон «Об информации, информационных технологиях и о защите информации», принятый 2006г. [11] «регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;
2) применении информационных технологий;
3) обеспечении защиты информации».

Федеральный закон «О связи» [9] от 7 июля 2003г., установил правовую основу деятельности в области связи, определил полномочия органов государственной власти, по регулированию указанной деятельности, а также права и обязанности физических и юридических лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Следует также упомянуть Указы Президента РФ, которые касаются, прежде всего, вопросов формирования государственной политики в сфере информатизации, (включая организационные механизмы), создания системы правовой информации и информационно-правового сотрудничества с государствами СНГ, обеспечения информацией органов государственной власти, мер по защите информации (в частности, шифрования).

Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стала разработка в Уголовном кодекса РФ 1996 года группы статей, предусматривающих основания уголовной ответственности за так называемые компьютерные преступления. Но затронем с начало немного предыстории принятия УК РФ, чтобы понять насколько сложной была проделанная работа.

Однако проект не был реализован ввиду постановки новой задачи в виде формирования уже в рамках нового Уголовного кодекса преступлений в области компьютерной информации. Минюстом России и Государственно-правовым управлением Президента РФ был разработан проект нового Уголовного кодекса, два варианта которого были опубликованы в 1994 и 1995 гг., где содержалась глава «Компьютерные преступления». Заслугой авторов было верное определение родового объекта. Считая, что последствия неправомерного использования информации ЭВМ могут быть самыми разнообразными, поместили компьютерные преступления в раздел IX «Преступления против общественной безопасности и общественного порядка». Оба варианта проекта в главе «компьютерные преступления» между собой не сильно отличались. А в отношении самого первого проекта изменений и дополнений, при некоторых различиях в последовательности расположения статей и в используемой терминологии, количество и сущность остались теми же. Юристами и специалистами в области информационных технологий было указано на существенные недостатки, в частности, на отсутствие единой правовой концепции в главе, недостаточную связь с отраслевыми законами, слабую проработку терминологии и стилистику.

Отметим, что на федеральном уровне для развития законодательной базы большое значение имеет утверждаемая Президентом РФ с сентября 2000 г. Доктрина информационной безопасности Российской Федерации. В этой доктрине определены главные составляющие информационной безопасности, основные направления противодействия угрозам информационной безопасности в России, а также комплекс практических мероприятий по ее обеспечению.

Таким образом, анализ законодательства, регулирующего информационные отношения, показывает, что необходимо более детальное исследование правового содержания и сущности понятий, которые касаются одновременно и элементов информационных отношений и отношений, регулируемых уголовным законом. С помощью этих понятий в дальнейшем можно будет определить значимые элементы уголовной деятельности.

Можно сделать вывод, что понятие «компьютерного преступления» является одним из центральных в сегменте преступлений в сфере компьютерной информации, но до сих пор остается более чем не определенным. В мировой практике «… признано, что дать определение компьютерного преступления чрезвычайно сложно. Не всякое использование компьютерной системы образует состав компьютерного преступления» [41,с. 9]. По нашему мнению сложность в формулировке этого понятия существует, как по причине невозможности выделения единого объекта преступного посягательства, так и множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны. В поисках истинного юридического значения выражения «компьютерное преступление» многие ученные и практики разошлись во мнениях более чем на четыре стороны. Относительно только объекта данного преступления в науке существует уже как минимум три мнения: сторонники первого считают, что объектом является сам компьютер (ЭВМ), второго - компьютерная информация, записанная на машинных носителях компьютера, а третьего, что общественные отношения по безопасному (законному) использованию информации являются объектом данного преступления.

Ошибочность некоторых мнений исходит из того, что суть нового явления в уголовном праве пытаются понять через призму понятий уголовной науки. Но компьютерное преступление по своей сути очень специфично и своими корнями уходит вглубь профессиональной среды специалистов в области информационных технологий. Это особый мир или отдельная страна со своими законами, понятиями, лидерами, целями и даже наказаниями. Здесь нельзя навести свой порядок, установить свой «устав». Единственный путь для уголовно-правовой науки видится в том, чтобы на основе глубокого анализа пытаться смоделировать юридические понятия и в дальнейшем грамотно регулировать отношения в данной области. Ведь не секрет, что после принятия в 1996 году нового Уголовного кодекса РФ в информационной среде ничего не изменилось, там предпочли жить по собственным правилам и если, например, на какой-либо сервер в сети Internet осуществлен неправомерный доступ, то собственник сервера не идет в милицию, а нанимает хакера и «залатывает брешь» в защите.

1.2 Зарубежное уголовное законодательство регулирующее отношения в сфере компьютерной информации

Законодательство об уголовной ответственности за компьютерные преступления в различных странах мира существенно отличается. История развития зарубежного законодательства показывает, что первый шаг в направлении защиты компьютерной информации был сделан зарубежным законодательством Швеции 4 апреля 1973 года, когда был принят «Закон о данных», который ввёл новое понятие в традиционное законодательство – «злоупотребление при помощи компьютера».

Одной из первых стран мира, принявшей меры по установлению уголовной ответственности за совершение преступлений рассматриваемого вида, явились Соединенные Штаты Америки, где компьютерная преступность появилась несколько раньше, чем в других государствах. В 1977г. в США был разработан законопроект о защите федеральных компьютерных систем. Он предусматривал уголовную ответственность за:

1. введение заведомо ложных данных в компьютерную систему;
2. незаконное использование компьютерных устройств;
3. внесение изменений в процессы обработки информации или нарушение этих процессов;
4. хищение денежных средств, ценных бумаг, имущества, услуг, ценной информации, совершенные с использованием возможностей компьютерных технологий или с использованием компьютерной информации.

На основе данного законопроекта в октябре 1984г. был принят Закон о мошенничестве и злоупотреблении с использованием компьютеров – основной нормативно-правовой акт, устанавливающий уголовную ответственность за преступления в сфере компьютерной информации. В последующем он неоднократно (в 1986, 1988, 1989, 1990, 1994 и 1996гг.) дополнялся.

Нынче он включен в виде §1030 Титула 18 Свода законов США. Данный закон установил ответственность за деяния, предметом посягательств которых является «защищенный компьютер» (находящаяся в нем компьютерная информация). Под ним понимается:

1) компьютер, находящийся в исключительном пользовании правительства или финансовой организации, либо компьютер, функционирование которого было нарушено при работе в интересах правительства или финансовой организации;
2) компьютер, являющийся частью системы или сети, элементы которой расположены более чем в одном штате США.

Одновременно уголовный закон устанавливает, что уголовная ответственность наступает в случаях:

1) несанкционированного доступа – когда посторонний, по отношению к компьютеру или компьютерной системе, человек вторгается в них извне и пользуется ими;

2) превышение санкционированного доступа – когда законный пользователь компьютера или системы осуществляет доступ к компьютерным данным, на которые его полномочия не распространяются.

Данный закон устанавливает ответственность за семь основных составов преступлений, которыми признаются:

1) компьютерный шпионаж, состоящий в несанкционированном доступе или превышении санкционированного доступа к информации, а также получение информации, имеющее отношение к государственной безопасности, международным отношениям и вопросам атомной энергетики (§1030 (a) (1));

2) несанкционированный доступ или превышение санкционированного доступа к информации из правительственного ведомства США, из какого бы то ни было защищенного компьютера, имеющего отношение к межштатной или международной торговле, а также получение информации из финансовых записей финансового учреждения, эмитента карт или информации о потребителях, содержащейся в файле управления учета потребителей (§1030 (a) (2));

3) воздействие на компьютер, находящийся в исключительном пользовании правительственного ведомства США, или нарушении функционирования компьютера, используемого полностью или частично Правительством США (§1030 (a) (3));

4) мошенничество с использованием компьютера – доступ, осуществляемый с мошенническими намерениями, и использование компьютера с целью получения чего бы то ни было ценного посредством мошенничества, включая незаконное использование машинного времени стоимостью более 5 тысяч долларов в течении года, т.е. без оплаты использования компьютерных сетей и серверов (§1030 (a) (4));

5) умышленное или по неосторожности повреждение защищенных компьютеров (§1030 (a) (5));

6) мошенничество путем торговли компьютерными паролями или аналогичной информацией, позволяющей получить несанкционированный доступ к информации, если такая торговля влияет на торговые отношения между штатами и с другими государствами, или на компьютер, используемый правительством США (§1030 (a) (6));

7) угрозы, вымогательство, шантаж и другие противоправные деяния, совершаемые с использованием компьютерных технологий (§1030 (a) (7)).

Также можно выделить §1029 Титула 18 Свода законов США, которым предусмотрена ответственность за торговлю похищенными или поддельными устройствами доступа, которые могут быть использованы для получения денег, товаров или услуг.

Несмотря на столь детальную регламентацию вопросов уголовной ответственности за компьютерные преступления, правоохранительные органы США испытывают значительные затруднения в случаях, когда речь ведется о привлечении к ответственности лиц, которые совершают компьютерные преступления, осуществляя доступ к компьютерам США из-за рубежа. По мнению экспертов этого можно было бы избежать при условии включения в

статьи уголовного закона квалифицирующих признаков – совершения преступлений с использованием возможностей глобальных компьютерных сетей и осуществления несанкционированного доступа с компьютеров, находящихся за пределами США, или через них.

Была вынуждена отреагировать на компьютерные преступления и Великобритания, известная консерватизмом правовой системы. Длительное время Великобритания пыталась справляться с данным явлением, используя свой многовековый опыт судопроизводства, но под «напором» компьютерной преступности «сдалась». С августа 1990г. вступил в силу Закон о злоупотреблениях компьютерами. В соответствии с ним к уголовно наказуемым отнесены:

1. умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам (ст.1);
2. умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам для их последующего использования в противозаконных целях (ст.2);
3. неправомерный доступ к компьютерной информации на машинном носителе, в компьютере, компьютерной системе или сети, с целью, или если это повлекло уничтожение, блокирование, модификацию, либо копирование информации, нарушения работы компьютера, компьютерной системы или сети (ст.3).

Одним из последних подтверждений серьезности проблемы компьютерных преступлений и решительности государств в борьбе с этой проблемой может служить вступление в действие в Великобритании «Закона о терроризме 2000 года». Данный закон призван усилить борьбу в связи с использованием территории Великобритании как базы различными подрывными группировками. При этом отмечается, что в данном законе определение терроризма впервые расширяется и затрагивает область киберпространства. Английские правоохранительные органы вправе считать террористическими действия, которые «серьезно вмешиваются или серьезно нарушают работу какой-либо электронной системы» и принимать к компьютерным преступникам, изобличенным в таких действиях, столь же решительные меры как к боевикам Ирландской рабочей армии.

В Германии встал вопрос о закреплении уголовной ответственности за преступления в сфере компьютерной информации в УК уже в 1986г. (по данным статистики в 1987г. было зарегистрировано 3355 таких преступлений, а в 2002г. – уже 57488). Эти составы преступлений были введены «Вторым законом о борьбе с экономической преступностью» (2. Gesetz zur Bekämpfung der Wirtschaftskriminalität) в УК ФРГ 1 августа 1987г. В Уголовном кодексе Германии не существует специального раздела, посвященного компьютерным преступлениям (преступлениям в сфере компьютерной информации); нормы, содержащие ответственность за преступления в сфере компьютерной информации рассредоточены по разделам Особенной части кодекса:

1. §202a шпионаж данных (Ausspähen von Daten);

2. §263a компьютерное мошенничество (Computer betrug);
3. §269 фальсификация данных, имеющих доказательственное значение (Fälschung beweiser heblicher Daten);
4. §270 обман при помощи ЭВМ при обработке данных (Täuschung in Rechtsverkehr bei Datenverarbeitung);
5. §303a изменение данных (Datenveränderung);
6. §303b компьютерный саботаж (Computersabotage).

Необходимо отметить, что немецкий уголовный закон использует специальный термин – Daten, определение которого дает в абз. 2 §202a – это данные, которые сохранены или передаются электронным, магнитным или иным, непосредственно визуально не воспринимаемым способом.

В §202a – шпионаж данных, входящем в раздел 15 Уголовного кодекса ФРГ «Нарушение неприкосновенности и тайны частной жизни», предусмотрена ответственность тех лиц, «кто незаконно получает данные, то есть, которые ему не предназначаются и особо охраняются от незаконного к ним доступа, или кто передает их другому лицу». За совершение данного преступления, согласно УК ФРГ, предусмотрена уголовная ответственность в виде лишения свободы на срок до трех лет или денежного штрафа. §263a – компьютерное мошенничество, – выделено в самостоятельный вид мошенничества, за которое предусматривается ответственность до 5 лет лишения свободы или денежный штраф (т.е. как за неквалифицированный вид мошенничества). Данная норма сконструирована следующим образом: «Кто, действуя с намерением получить для себя или третьего лица имущественную выгоду, причиняет вред имуществу другого лица, воздействует на результат обработки данных путем неправильного создания программ, использования неправильных или неполных данных или иного неправомочного воздействия на результат обработки данных». В системе особенной части УК ФРГ, данный состав находится в 22 разделе – «Мошенничество и преступное злоупотребление доверием», содержащем десять параграфов, описывающих помимо простого и квалифицированного мошенничества различные его виды (в основу разделения мошенничества на виды положен способ совершения преступления).

§269 – фальсификация данных, имеющих доказательственное значение, – находится в 23 разделе – «Фальсификация документов», в котором предусмотрена ответственность за различные способы фальсификации документов. Данный вид состава предусматривает уголовную ответственность за сохранение или изменение при помощи ЭВМ, путем обмана, данных, имеющих доказательственное значение, приводящее к восприятию документов как сфальсифицированных или поддельных, либо использование такого рода сохраненных или измененных данных. В этом же разделе находится еще одна норма – обман при помощи ЭВМ при переработке данных (§ 270 УК ФРГ). Причем, под переработкой понимается получение из введенных данных посредством компьютерных программ новых данных.

В разделе 27 – «Повреждение имущества» наряду с различными способами и видами повреждения имущества находятся и два состава преступления,

относимых учеными-юристами к компьютерным преступлениям: изменение данных (§303a) и компьютерный саботаж (§303b). Ответственность за первый состав преступления в виде лишения свободы до двух лет или денежного штрафа наступает, если лицо «противоправно стирает, делает непригодным для использования или изменяет данные». За второй – в виде лишения свободы на срок до 5 лет или денежного штрафа за нарушение обработки данных, имеющих существенное значение для чужого предприятия, организации или органа, если лицо совершило преступление, предусмотренное §303a или испортило, повредило, сделало непригодным для дальнейшего использования по назначению или изменило устройство для переработки данных или носитель информации. Таким образом, составы компьютерных преступлений сконструированы как квалифицирующие виды простых составов преступлений, имеющих различные объекты посягательств.

Среди европейских государств, которые повели решительную борьбу с компьютерными преступлениями с момента их появления в жизни общества одно из ведущих мест занимают Нидерланды (Голландия). В Нидерландах был создан Консультативный комитет по компьютерным преступлениям, который предложил конкретные рекомендации по внесению изменений в Уголовный кодекс и Уголовно-процессуальный кодекс Нидерландов. Консультативный комитет не дал определения компьютерных преступлений, но разработал их классификацию.

В то же время полицейское разведывательное управление, занимающееся регистрацией всех случаев компьютерных преступлений, использует следующее определение компьютерного преступления: это поведение, которое (потенциально) вредно и имеет отношение к устройствам, связанным с компьютерами с точки зрения хранения, передачи и обработки данных. Полицейское разведывательное управление делает различие между компьютерными преступлениями, в которых компьютер является объектом преступления, и теми, в которых он – орудие преступления. Начиная с 1987г. полицейское разведывательное управление использует для анализа пять видов компьютерных преступлений:

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

1) использование несанкционированного доступа;
2) использование вредоносных программ, типа компьютерных вирусов;
3) 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.

Данный перечень видов преступлений в целом соответствует приведенной выше Рекомендации №R (89) 9 Совета Европы, но отличается более простым их

описанием. Причина отсутствия общепризнанного определения компьютерного преступления заключается в том, что, по мнению нидерландских ученых, существует множество трудностей при формулировании определения, которое, с одной стороны, было бы достаточно емким, а с другой – достаточно специальным. Применяется два понятия компьютерного преступления – в узком и широком смысле. В узком смысле – это совершение преступления, которое невозможно выполнить без использования компьютера или другого автоматического устройства как объекта или инструмента преступления. В 1993г. в Нидерландах был принят Закон о компьютерных преступлениях, дополняющий УК Голландии новыми составами:

1. несанкционированный доступ в компьютерные сети (ст.138a (1));
2. несанкционированное копирование данных (ст.138a (2));
3. компьютерный саботаж (ст.350a (1), 350b (1));
4. распространение вирусов (ст.350a (3), 350b);
5. компьютерный шпионаж (ст.273 (2)).

В ряд статей УК Голландии, предусматривающих ответственность за совершение традиционных преступлений (вымогательство (ст.317, 318), запись (прослушивание, копирование) информационных коммуникаций, кража путем обмана служб (ст.362c), были внесены дополнения, в редакции других статей (саботаж (ст.161, 351), подлог банковских карточек (ст.232) – даны специальные разъяснения. Были значительно изменены такие составы, как шпионаж (ст. ст.98, 98a), вмешательство в коммуникации (ст.139a, 139b), порнография (ст.240b), что позволяет в настоящее время использовать данные составы преступлений, в соответствующих случаях, и для борьбы с компьютерными преступлениями.

Таким образом, уголовное законодательство Нидерландов предоставляет достаточно широкие возможности для борьбы с различными видами компьютерных преступлений, устанавливая помимо специальных норм дополнительные квалифицирующие обстоятельства в уже существующие уголовно-правовые нормы.

В Уголовном кодексе Республике Польша содержится глава XXXIII «Преступления против охраны информации», состоящая из 6 статей, объектом которых являются общественные отношения в сфере информации как таковой. Общественные отношения в сфере компьютерной информации являют собой лишь часть объекта. Из этой главы можно упомянуть только о двух статьях – ст.267 и 268 УК Польши. В ст.267 УК устанавливается уголовная ответственность за неправомерный доступ к информации, в том числе путем повреждения электронного, магнитного или иного особого средства обеспечения ее безопасности. В ст.268 УК Польши предусматривается уголовная ответственность лиц, не имеющих на то уполномочия уничтожения, повреждения удаления или изменение записи на компьютерном носителе информации, имеющей особое значение обороноспособности страны, безопасности связи, функционирования правительственных или государственных органов. Данное преступление, согласно УК Польши, карается как раскрытие информации, составляющей государственную тайну.

Статьи 278, 287 УК Польши, находящиеся в главе XXXV «Преступления против имущества», также можно отнести к «компьютерным» составам преступлений. Эти нормы предусматривают ответственность за:
а) получение без согласия управомоченного лица чужой компьютерной программы с целью извлечения имущественной выгоды (ст. 278);
б) влиянием неуправомоченным на то лицом на автоматизированное преобразование, собирание или передачу информации, или изменение, удаление, введение новой записи на компьютерный носитель информации с целью получения имущественной выгоды или причинения вреда другому лицу (ст.287). Достаточно интересным представляется то, что в данном случае если вред причинен самому близкому лицу, преследование возбуждается по заявлению потерпевшего.

Таким образом, в УК Польши проведено разделение компьютерных преступлений на две самостоятельные группы (соответственно их размещению в УК Польши) в зависимости от того, на что было направленно деяние субъекта – на собственно получение информации, либо на получение материальной выгоды. Такое разграничение представляется достаточно спорным, так как и в первом и во втором случаях субъект завладевает определенным объемом информации; и в первом, и во втором случаях лицо может быть заинтересовано именно получением материальной выгоды (например, передача вознаграждения за уничтожение информации на компьютерном носителе, имеющей значение для обороноспособности страны.).

Вывод по разделу 1

Исходя из вышеизложенного, можно сделать вывод, что зарубежное законодательство пошло по пути разграничения компьютерных преступлений в зависимости от той сферы общественных отношений, на которую посягает преступник. Данные сферы соответствуют криминологическим группам компьютерных преступлений. Можно выделить следующие три группы:
1) экономические компьютерные преступления (наиболее распространенные и опасные преступления), например, компьютерное мошенничество §263а УК ФРГ;
2) компьютерные преступления против прав и свобод индивидуальных субъектов и организаций, нарушающие неприкосновенность частной сферы, например, незаконные злоупотребления информацией, находящейся на компьютерных носителях, разглашение сведений, имеющих частную, коммерческую тайну (сведения помимо конфиденциального характера, должны находиться на компьютерных носителях);
3) компьютерные преступления против интересов государства и общества в целом, например дезорганизация работы различных систем (оборонных, энергетических, газоснабжения), изменения данных при подсчете голосов на выборах и др.

2 ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1. **Объективные и субъективные признаки преступления предусмотренного ст.272 УК РФ**

Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем [5].

Данная статья защищает право лиц на неприкосновенность информации в системе. Владельцем информационной вычислительной системы (и информации в ней) может быть любое лицо, правомерно пользующееся услугами по обработке информации как собственник вычислительной системы (ЭВМ, сети ЭВМ) или как лицо, приобретшее право использования системы (информации). по ст.1280 4части ГК РФ [4]. Данная статья защищает компьютерную информацию любых предприятий, учреждений, организаций и частных лиц. Диспозиция соответствующей нормы заключается в неправомерном доступе к охраняемой законом компьютерной информации. Преступное деяние, ответственность за которое предусмотрено ст. 272 должно состоять в неправомерном доступе к охраняемой законом компьютерной информации, который всегда носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств позволяющих преодолеть установленные системы защиты; незаконного применения действующих паролей или маскировка под видом законного пользователя для проникновения в компьютер, хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

Под охраняемой законом информацией понимается информация, для которой законодательно установлен специальный режим ее правовой защиты, например - государственная, служебная и коммерческая тайна, персональные данные и т.д.

Неправомерным является доступ, противоречащий действующим правовым нормам, актам управления, приказам, распоряжениям и иным актам, регулирующим отношения по доступу лиц (группы лиц) к информации.
Кроме того, неправомерным будет доступ, если лицо незаконно использовало технические средства для проникновения в ЭВМ и (или) ее сеть, например введение чужого пароля либо снятие необходимого пароля, модификация программы и пр. Под неправомерным доступом к охраняемой законом компьютерной информации следует понимать также самовольное получение информации без разрешения ее собственника или владельца.

Эта статья, состоящая из 2-х частей, содержит достаточно много признаков, обязательных для объекта, объективной и субъективной сторон состава преступления. Исходя из диспозиции ст. 272 УК РФ, можно выделить следующие обязательные признаки объективной стороны неправомерного доступа к охраняемой законом компьютерной информации.

Общественно опасные последствия в виде уничтожения блокирования, модификации при копировании компьютерной информации, нарушения работы ЭВМ или их сети. Наличие причинной связи между совершенным деянием и наступившими последствиями. Отсутствие одного из указанных выше признаков исключает уголовную ответственность за преступление, предусмотренное ст.272 УК РФ. На практике встречаются трудности при трактовке понятия «неправомерный доступ к компьютерной информации» Вместе с тем, четкое понимание данного термина является необходимым условием для правильной квалификации рассматриваемых общественно опасных деяний. Существует мнение о том, что доступ считается неправомерным «в случае несанкционированного обращения к ресурсам ЭВМ и их сети лица, которое вообще не имеет права доступа». Более правильным, на наш взгляд, является определение данного понятия, предложенное Ю.А. Красиковым, согласно которому «неправомерным доступ считается не только при отсутствии такого права, но и при отсутствии правил защиты компьютерной информации»

Следует отметить, что в настоящее время уровень технического прогресса в области компьютерной техники, а также уровень сложности компьютерных программ достигает столь высокого уровня, что не исключается возможность сбоев в работе ЭВМ, системы ЭВМ или их сети (например, снижение быстродействия). Причиной сбоев могут также послужить и иные причины (например, неправильно подобранная конфигурация компьютера, несостыковка меду собой программ или аппаратных средств).

По утверждению В.В. Воробьева «если выполнение компьютером такой функции, как охрана информации от несанкционированного доступа, считать нарушением защиты информированных ресурсов становиться решаемой». Полагаем, что в сложившейся ситуации привлекать лицо к уголовной ответственности недопустимо, а ограничивать преступное деяние от непреступного, но наш взгляд, можно по наличию или отсутствию причинной связи меду действиями лица, осуществляющего неправомерный доступ к охраняемой законом информации, повлекший нарушение работы ЭВМ, системы ЭВМ или их сети.

На наш взгляд, несанкционированное преодоление программных средств защиты информации в этом случае можно считать оконченным преступлением, квалифицирующимся по ст.272 УК РФ. Попытка несанкционированного проникновения к охраняемой законом информации будет расцениваться как покушение на неправомерный доступ. Таким образом, действия лица, формально связанные с осуществлением неправомерного доступа к компьютерной информации, не повлекшие нарушение работы ЭВМ или их сети по независящим от лица обстоятельствам подлежат квалификации по ст.272 УК РФ со ссылкой на ч.3 ст.30 УК РФ.

Как уже отмечалось, состав преступления сформулирован как материальный, причем деяние определено в форме действия и предполагается обязательное наступление одного из следующих последствий:

1. уничтожения информации, то есть удаление информации на материальном носителе и невозможность ее восстановления на нем;
2. блокирования информации, то есть совершение действий приводящих к ограничению или закрытию доступа к компьютерной системе и предоставляемым ею информационным ресурсам;
3. модификации информации, то есть внесение изменений в программы, базы данных, текстовую информацию находящуюся на материальном носителе;
4. копирования информации, то есть переноса информации на другой материальный носитель, при сохранении неизмененной первоначальной информации;
5. нарушения работы ЭВМ, системы ЭВМ или их сети, что может выразиться в нарушении работы как отдельных программ, баз данных, выдаче искаженной информации, так и нештатном функционировании аппаратных средств и периферийных устройств, либо нарушении нормального функционирования сети.

Важным является установление причинной связи между несанкционированным доступом и наступлением последствий. При функционировании сложных компьютерных систем возможны уничтожение, блокирование и нарушение работы ЭВМ в результате технических неисправностей или ошибок в программных средствах. В этом случае лицо совершившего неправомерный доступ к компьютерной информации не подлежит ответственности из-за отсутствия причинной связи между действиями и наступившими последствиями.

Данное преступление считается оконченным в момент наступления предусмотренных в данной статье последствий, т.е. все действия, выполненные до формальной подачи последней команды (как например), будут образовывать состав неоконченного преступления.

Мотивы и цели данного преступления могут быть любыми. Это и корыстный мотив, месть, зависть, цель получить какую-либо информацию, желание причинить вред, желание проверить свои профессиональные способности или самоутвердится.

Предмет преступления - компьютерная информация. Диспозиция статьи, указывая на это, требует четкого понимания рассмотренных ранее дефиниций - ЭВМ (компьютер), Сеть, Система Компьютеров, Носитель информации и т.д.

Объект - общественные отношения, связанные с безопасностью использования компьютерной информации.

Объективную сторону данного преступления составляет неправомерный доступ к охраняемой законом компьютерной информации, который всегда носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем:

1) использования специальных технических или программных средств позволяющих преодолеть установленные системы защиты;
2) незаконного использования действующих паролей или кодов для проникновения в компьютер, либо совершение иных действий в целях проникновения в систему или сеть под видом законного пользователя;

3) хищения носителей информации, при условии, что были приняты меры их охраны если это деяние повлекло уничтожение или блокирование информации.

Хотя и диспозиция ст.272 УК РФ не содержит прямых указаний на субъективную сторону неправомерного доступа к компьютерной информации, но при совершении данного общественно опасного деяния с полной уверенностью можно говорить об умышленной форме вины в виде прямого или косвенного умысла. В этой ситуации виновное лицо сознает, что осуществляет именно неправомерной доступ к компьютерной информации, охраняемой законом, предвидит, что в результате его действий может наступить или неизбежно наступит уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети и желает наступления указанных преступных последствий, либо сознательно их допускает, либо относиться к ним безразлично. А.А. Толкаченко подчеркивает, что субъективная сторона данного преступления «характеризуется только умышленной: лицо, осуществляющее доступ к информации, либо желает ее уничтожения, блокирования, либо допускает такие последствия, хотя может преследовать и другие цели (соответственно, прямой или косвенный умысел)».

Принципиально иную позицию в данном вопросе занимает С.А. Пашин. Автор считает, что «данное преступление может совершаться как с умыслом, так и по неосторожности», при этом «неосторожная форма вины может проявляться при оценке лицом правомерности своего доступа к компьютерной информации, а также в отношении неблагоприятных последствий доступа, предусмотренных диспозицией данной нормы уголовного закона». При квалификации данных преступлений установление в деяния лицом правомерности своего к компьютерной информации, а также в отношении неблагоприятных последствий доступа, предусмотренных диспозицией данного нормы уголовного закона.

При квалификации данных преступлений установление в деянии лица вины в виде умысла, а не неосторожности существенно затрудняется, так как при различных состояниях вычислительной системы (при чем, часто неизвестных преступнику) одни и те же действия могут приводить к различным последствиям. Таким образом, одни и те же действия, с одним и тем же умыслом могут приводить к неожиданным для виновного последствиям.

Однако такой подход будет противоречить нормам ст.24 УК РФ, согласно которой деяние, совершенное только по неосторожности, признается преступлением лишь в том случае, когда это специально предусмотрено соответствующей статьей Особенной части УК. Следовательно, неправомерный доступ к охраняемой законом компьютерной информации, содержащий признаки неосторожной формы вины, преступлением не является. В диспозиции ст.272 УК РФ законодателем прямо указывается на характер действия (доступа) – в отношении компьютерной информации, охраняемой законом, он должен носить неправомерным, если «лицо не имеет права на доступ к данной информации; лицо имеет право на доступ к данной информации, однако осуществляет его помимо установленного порядка, с нарушением правил ее защиты». Когда лицо сознает, что совершает доступ к компьютерной информации, не имея на это права или

хоть и имеет право, но нарушает при этом режим доступа, оно поступает общественно опасно. В этом случае указанные действия виновного « легко укладывается в формулу прямого или косвенного умысла». Данное лицо предвидит также и возможность наступления указанных в законе общественно опасных последствий и желает их наступления (прямой умысел) или допускает эти последствия, либо относится к ним безразлично (косвенный умысел).

Совсем иное происходит в случае признания возможности совершения лицом таких действий по неосторожности. В том случае, если лицо осознает факт неправомерности доступа в отношении компьютерной информации, находящейся под охраной закона, то оно уже действует умышленно, и о неосторожной форме вины речь может идти только в зависимости от его отношения к последствиям (самонадеянно рассчитывало на их предотвращение – легкомыслие; не проявило необходимой внимательности и предусмотрительности – небрежность). Подобные ситуации предусмотрены и ст.274 УК РФ, заключаются в выраженном умышленном характере рассматриваемого деяния, и в диспозиции ст.272 УК не указано обратное. Таким образом, при неправомерном доступе к компьютерной информации законодатель не связывает совершение умышленных действий с не осторожным наступлением последствий, поэтому субъективная сторона этого состава выражается только в форме умысла.

Таким образом, в рассмотренном общественно опасным деянии виновный осознает, что он осуществляет неправомерный доступ к охраняемой законом компьютерной информации, осознает общественную опасность своих действий, предвидит возможность или неизбежность наступления преступных последствий, нарушения работы ЭВМ, системы ЭВМ или их сети, желает (сознательно допускает) данные последствия либо относится к ним безразлично.

В составе преступления, предусмотрено ст.272 УК РФ, структурным элементом прямого умысла является предвидение возможности или неизбежности наступления общественно опасных последствий (например, уничтожение информации при неправомерном доступе к ней); волевым же моментом умысла будет желание, определяемое по отношению к наступлению общественно опасных последствий.

С субъективной стороны преступление характеризуется наличием прямого умысла (осознание неправомерного доступа, предвидение наступления вредных последствий и желание их наступления) или косвенного умысла (осознание неправомерного доступа, предвидение наступления вредных последствий и сознательное допущение их наступления либо безразличное отношение к наступлению последствий) Неправомерный доступ к компьютерной информации - умышленное деяние, поскольку в диспозиции ст.272 УК не указано обратное.Человек, пытающийся получить доступ к информации, должен сознавать, что свободный доступ к информации ограничен, он не имеет прав на доступ к этой информации. Об умысле будут свидетельствовать меры защиты информации от доступа посторонних (коды, пароли и т.п.), которые приходится преодолеть, чтобы получить доступ к информации, вывод на экран дисплея

компьютера предупреждающих сообщений, устные уведомления о запрете доступа к информации и т.д.

Субъектами данного преступления в основном могут являться лица, имеющие опыт работы с компьютерной техникой, и поэтому в силу профессиональных знаний они обязаны предвидеть возможные последствия уничтожения, блокирования, модификации информации либо нарушения работы ЭВМ, системы ЭВМ и их сети. По общему правилу субъектами преступления, предусмотренного ст.272, может быть лицо, достигшее 16-летнего возраста, однако часть вторая ст.272 предусматривает наличие специального субъекта, совершившего данное преступление.

В преступлении, предусмотренном ст.272 УК, неправомерный доступ к компьютерной информации осуществляется следующими лицами:

1) не имеющими права на доступ к компьютерной информации в данных условиях места и времени, но осуществляющими «неправомерный доступ к охраняемой законом компьютерной информации» (ч.1 ст.272);
2) совершающими неправомерный доступ группой по предварительному сговору или организованной группой (ч.2 ст.272);
3) совершающими неправомерный доступ, используя для этого свое служебное положение (ч.2 ст.272);
4) имеющими право доступа к ЭВМ, системы ЭВМ или их сети, но использующими это право в целях достижения преступного результата (уничтожение, блокирование, модификации либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети).

Преступления от иных видов преступных посягательств, связанных с уничтожением, блокированием, модификацией либо копированием информации, нарушением работы ЭВМ, системы ЭВМ или их сети, а равно преступлений, предметом которых вполне может являться какая-либо информация, находящаяся на машинном носителе, в электронно-вычислительной машине, системы ЭВМ или их сети.

Для выяснения признаков неправомерного доступа к компьютерной информации и ограничения его от смежных преступлений сотрудникам правоохранительных органов необходимо использовать метод юридического анализа, позволяющий исследовать конкретное преступление с различных сторон и раскрыть его конструктивные признаки. При этом важно установить, на что посягает данное действие, чему оно причиняет вред или создает угрозу причинения вреда; внешнюю, объективную сторону преступления, характеризующую само деяние (действие или бездействие), наступившие последствия и причинную связь между ними; внутреннюю, субъективную сторону преступления, определяющую представление о психическом отношении лица к содеянному и его последствиям – умысел (прямой и косвенный), неосторожность (небрежность или легкомыслие), мотив поведенческого акта субъекта и его цель; характеристику самого субъекта преступного посягательства.

Для преступления, предусмотренного ст.272 УК, суть общественно опасного деяния заключается в неправомерном доступе к компьютерной информации.

Причем состав неправомерного доступа к компьютерной информации в отличие от создания, использования и распространения вредоносных программ для ЭВМ сконструирован как материальный. Оконченным это преступление будет только тогда, когда наступят вредные последствия, лежащие в причинной связи с поведенческим актом виновного.

2.2.Объективные и субъективные признаки преступления предусмотренного ст.273 УК РФ

Статья 273 предусматривает ответственность за создание и распространение различного рода компьютерных «вирусов» и других программ, которые могут нарушить целостность информации, нарушить нормальную штатную работу компьютера, сети ЭВМ. Под использованием либо распространением вредоносных программ или машинных носителей к ним понимается соответственно введение этих программ в ЭВМ, систему ЭВМ или их сеть, а также продажа, обмен, дарение или безвозмездная передача другим лицам. Статья защищает права владельца компьютерной системы на неприкосновенность и целостность находящейся в ней информации. Во-первых, компьютерный вирус может быть и безвредным для информации, требующей гарантированной целостности. Во-вторых, существует большое количество типов программ, приводящих к крайне нежелательным последствиям, но они не попадают под традиционное понимание «компьютерного вируса».

Под вредоносными программами в смысле ст. 273 УК РФ понимаются программы специально созданные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, определенные в документации на программу. Наиболее распространенными видами вредоносных программ являются «компьютерные вирусы» и «логические бомбы».

«Компьютерные вирусы» - это программы, которые умеют воспроизводить себя в нескольких экземплярах, модифицировать (изменять) программу к которой они присоединились и тем самым нарушать ее нормальное функционирование.

«Логическая бомба» - это умышленное изменение кода программы, частично или полностью выводящее из строя программу либо систему ЭВМ при определенных заранее условиях, например наступления определенного времени. Принципиальное отличие «логических бомб» от «компьютерных вирусов» состоит в том, что они изначально являются частью программы и не переходят в другие программы, а компьютерные вирусы являются динамичными программами и могут распространяться даже по компьютерным сетям. Преступление, предусмотренное ст.273, наиболее опасное из содержащихся в главе 28, что отражено в санкции за него.

Состав преступления, предусмотренный ч.1 ст.273 УК РФ, считается усеченным именно по признаку « создания программ для ЭВМ или внесения изменений в существующие программы»

Непосредственным объектом данного преступления являются общественные отношения по безопасному использованию ЭВМ, ее программного обеспечения и информационного содержания.

Состав части 1 формальный и предусматривает совершение одного из действий:

1) создание программ (очевидно, вернее – «программы») для ЭВМ, заведомо приводящих (приводящей) к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы аппаратной части;
2) внесение в существующие программы изменений, обладающих аналогичными свойствами;
3) использование двух названных видов программ;
4) их распространение;
5) использование машинных носителей с такими программами;
6) распространение таких носителей.

Хотя данный состав является формальным и не требует наступления каких-либо последствий, уголовная ответственность возникает уже в результате создания программы, независимо от того использовалась эта программа или нет.

Создание вредоносных программ для ЭВМ в технологическом смысле идентично этапам создания любых других программ и является целенаправленной деятельностью, включающей в себя:

1) постановку задачи, определение среды существования и цели программы;
2) выбор средств и языка программирования;
3) непосредственно написание текста программы;
4) проверку соответствия работоспособности программы и ее соответствия работоспособности программ и ее соответствие поставленной задаче;
5) подготовку программы к использованию.

В.В. Крылов, приводя в своей работе этапы создания вредоносных программ для ЭВМ, вместо последнего указанного нами этапа использует этап «запуска и непосредственного действия программы (выпуск в свет), предоставление информации». Думается, что подобные действия не относятся процессу создания и распространения вредоносных программ.

По нашему мнению любое из вышеперечисленных действий охватывается признаками создания вредоносной программы и может быть признано преступлением, предусмотренным ч.1 ст.273 УК РФ, даже в том случае, когда вредоносная программа еще не создана, а находиться, так сказать еще в стадии оформления. На наш взгляд, рассматривать подобные действия как подготовительные нельзя, поскольку термин «создания» программы рассматривается законодателем как процесс, а не как результат, и такие действия в этом направлении образуют признак объективной стороны состава данного преступления. Однако следует учитывать, что в ряде случаев использование подобных программ не будет являться уголовно наказуемым. Это прежде всего относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих лицензию на деятельность по защите

информации, выданную Государственной технической комиссией при Президенте.

Обращение к анализу состава преступления, предусмотренного ст.273 УК РФ, позволяет выделить несколько подходов в определении объективной стороны. Так, например, Ю.А. Красиков полагает, что «субъективная сторона этого преступления характеризируется прямым умыслом, законодатель в ч.1 ст.273 УК указывает на заведомый характер деятельности виновного; создавая новую программу или внося изменения в существующую, виновный сознает характер своих действий, предвидит возможность уничтожения, модификации, блокирования либо копирования какой либо информации, и желает совершить эти действия». С точки зрения С. А. Пашина, «создание, использование и распространение вредоносных программ для ЭВМ – это преступление и распространение вредоносных программ для ЭВМ - это преступление, совершаемое только с прямым умыслом; лицо понимает, что программа в имеющимся виде вредоносна, заведомо знает, что она способна вызвать указанные последствия.

Следовательно, создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации или копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, либо использование таких программ признается оконченным преступлением независимо от того, наступили или нет указанные в Уголовном законе неблагоприятные последствия. Достаточно установления самого факта совершения хотя бы одного действия, альтернативно перечисленного в диспозиции ч.1.ст.273 УК РФ. Интеллектуальный момент прямого умысла в рассматриваемых составах представляет собой такое состояние сознания виновного, когда он достоверно знал (или допускал с высокой степенью вероятности), что создаваемые (используемые, распространяемые) им программы обладают определенным набором вредоносных качеств, предвидел возможность наступления общественно опасных последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети и желал создать (использовать, распространить данную программу)

Как показывает анализ ч.1. ст.273 УК РФ, законодательного определенных данного состава преступления как умышленного мы не находим. В подобных случаях для установления виновности лица необходимо обратиться к ч.2. ст.24 УК РФ, предусматривающей, что деяния, совершенное по неосторожности, признается преступлением только в том случае, когда это специально предусмотрено соответствующей статьей Особенной части УК РФ присутствует только в квалификационных состав, поэтому по смыслу ст.27 УК РФ, если в результате совершения умышленного преступления причиняются тяжкие последствия, которые по закону влекут более строгое наказание и которые не охватывались умыслом лица, уголовная ответственность за такие последствия наступает только в случае, если лицо предвидело возможность их наступления, но без достаточных к тому оснований самонадеянно рассчитывало на их

предотвращение, или в случае, если лицо не предвидело, но должно было и могло предвидеть возможность наступления этих последствий; в целом такое преступление признается совершенным умышленно.

Обязательными признаками объективной стороны ч.1 ст.273 будут два, характеризующих способ и средство совершения преступления. Это, во-первых, то, что последствия должны быть, несанкционированными, во-вторых - наличие самой вредоносной программы или внесения изменений в программу.

Последними, кроме названного компьютерного вируса, могут быть хорошо известные программистам «логическая бомба», «люк», «асинхронная атака» и другие.

С субъективной стороны состав данного преступления характеризуется виной в форме прямого умысла: когда виновный осознавал общественную опасность своих действий, предвидел возможность либо даже неизбежность наступления опасных последствий, но тем не менее желал эти действия совершить, т.е. создание вредоносных программ заведомо для создателя программы должно привести к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ. Использование или распространение вредоносных программ тоже может осуществляться умышленно.

При установлении прямого умысла в действиях виновного преступление подлежит квалификации в зависимости от цели, которую перед собой ставил последний, или когда наступили последствия - то в зависимости от наступивших последствий. В этом случае действия, предусмотренные статьей окажутся лишь способом достижения поставленной цели и совершенное деяние подлежит квалификации по классической совокупности совершенных преступлений.

Необходимо также учитывать, что преступление может быть также совершено как по неосторожности в виде легкомыслия, так и с косвенным умыслом в виде безразличного отношения к возможным последствиям.

Субъект преступления - общий, т.е. субъектом данного преступления может быть любой гражданин, достигший шестнадцати лет. Объективную сторону преступления, предусмотренного ст.273 УК РФ, составляют следующие неправомерные действия.

1) Создание программ для ЭВМ, заведомо приводящих к общественно опасным последствиям.
2) Внесение изменений в существующие программ для ЭВМ, заведомо приводящих к общественно опасным последствиям.
3) Использование таких программ или машинных носителей с такими программами.
4) Распространение таких программ или машинных носителей с такими программами.

Данные действия виновного заведомо приводят к несанкционированному уничтожении, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. Высокая степень общественной опасности создания, использования и распространения вредоносных программ для ЭВМ обусловливает формирование законодателем

данного состава преступления как формального, когда сам факт создания компьютерного вируса либо совершения иного из указанных в ч.1 ст.273 УК РФ действий, составляющих объективную сторону этого состава, является вполне достаточным для ч.1 ст.273 УК РФ действий, составляющих объективную сторону этого состава, является вполне достаточным для привлечения лица к уголовной ответственности. Наступления общественно опасных последствий в данном случае значения для квалификации не имеет.

Частью 2 ст.273 криминализируется более опасное преступление: те же деяния, повлекшие тяжкие последствия. При этом «тяжкие последствия» - оценочная категория, которая подлежит квалификации судом. Суд не должен ограничиваться ссылкой на соответствующий признак, а обязан привести в описательной части приговора обстоятельства, послужившие основанием для вывода о наличии в содеянном указанного признака.

Особого внимания заслуживает вопрос об отграничении неправомерного доступа к компьютерной информации от создания, использования и распространения вредоносных программ для ЭВМ. Сложность этого вопроса заключается в том, что и неправомерный доступ к компьютерной информации, и создание, использование и распространение вредоносных программ для ЭВМ ведут к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. Причем создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к указанным выше вредным последствиям, вполне могут сочетаться с неправомерным доступом к компьютерной информации, что еще раз свидетельствует о прикладном характере разграничения этих преступлений. Во-первых, как уже было отмечено выше, предметом преступления, предусмотренного ст.272 УК, является только та информация, которая охраняется законом. Предметом же создания, использования и распространения вредоносных программ для ЭВМ является любая информация (как охраняемая законом, так и неохраняемая), содержащаяся на машинном носителе, к ЭВМ, системе ЭВМ или их сети. Так, например, по ст.273 УК следует квалифицировать действия виновного, совершившего неправомерный доступ к программе для ЭВМ, не имеющей специального правого статуса (т.е. не охраняемой законом), если это деяние было связано с ее модификацией, заведомо приводящей к вредным последствиям, указанным в диспозиции статьи УК. Признаки состава неправомерного доступа к компьютерной информации в этом случае отсутствуют. Вторым критерием, позволяющим разграничить неправомерный доступ к компьютерной информации от создания, использования и распространения вредоносных программ для ЭВМ, является содержание общественно опасного деяния. Последнее из указанных преступлений предполагает совершение хотя бы одного из следующий действий:

1. создание вредоносной программы (вредоносных программ) для ЭВМ;
2. внесение изменений в существующие программы для ЭВМ, доводя их до качества вредоносных;
3. использование вредоносных программ для ЭВМ;

4. использование машинных носителей, содержащих вредоносные программы;
5. распространение машинных носителей, содержащих вредоносных программ;
6. распространение машинных носителей, содержащих вредоносные программы.

При этом следует обратить внимание на то, что, согласно буквы и смысла закона, состав преступления, предусмотренный ч.1. ст.273 УК, сконструирован как формальный. Следовательно, для признания преступления оконченным не требуется реального наступления вредных последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Достаточно установить сам факт совершения общественно опасного деяния, если оно создавало реальную угрозу наступления альтернативно перечисленных выше вредных последствий. В том случае, когда виновный умышленно создает вредоносную программу для ЭВМ или вносит изменения в существующую программу, доводя ее до качества вредоносной, а равно использует либо распространяет такие программы или машинные носители с такими программами и при этом не совершает неправомерного доступа к охраняемой законом компьютерной информации, то его действия подлежат квалификации по ст.273 УК.

Однако, на практике вполне допустима ситуация, когда виновный в целях создания вредоносной программы для ЭВМ, неправомерно вызывает существующую программу, являющуюся, скажем, объектом авторского права, а значит, охраняемую законом, и вносит в нее соответствующие изменения (например, добавляет или удаляет отдельные фрагменты программы, перерабатывает набор данных посредством их обновления и.т.д.), иными словами, модифицирует компьютерную информации. В этом случае налицо совокупность преступлений предусмотренных ст. ст.272 и 273 УК. Объясняется это тем, что диспозиция ст.273 УК, говоря о создании программ для ЭВМ, внесении изменений в существующие программы, использование либо распространение таких программ или машинных носителей с такими программами, не охватывает своим содержанием факт неправомерного доступа к охраняемой законом компьютерной информации. Следовательно, деяние виновного подлежит дополнительной квалификации по ст.272 УК Оконченный состав неправомерного доступа к компьютерной информации следует оценивать поведения лица, которое, неправомерно вызвав существующую программу для ЭВМ и внеся в нее ряд изменений, не сумело в силу различного рода причин, выходящих, за рамки сознания и воли виновного, довести эту программу до качества вредоносной. Если же действия виновного были пресечены на более ранней стадии, например, в момент неправомерного доступа к информации, и не были связаны с ее модификацией, налицо приготовление к созданию, использованию и распространенно вредоносных программ для ЭВМ и покушение на неправомерный доступ к компьютерной информации.

В контексте нашего изложения небезынтересно отметить, что в соответствии с ч.2 ст.30 УК уголовная ответственность наступает за приготовление только к тяжкому преступлению. Итак, отличие неправомерного доступа к компьютерной

информации от создания, использования и распространения вредоносных программ для ЭВМ следует искать в юридической характеристике предмета преступного посягательства, содержании общественно опасных действий, приводящих к вредным последствиям, в субъективной стороне, дающей представление об отношении субъекта к содеянному.

2.3 Объективные и субъективные признаки преступления предусмотренного ст.274 УК РФ

Компьютерные системы в настоящее время все больше влияют на нашу жизнь и выход из строя ЭВМ, систем ЭВМ или их сети может привести к катастрофическим последствиям, поэтому законодатель посчитал необходимым установить уголовную ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети. И именно статья 274 УК РФ устанавливает такую ответственность, акцентируя что это деяние должно причинить существенный вред. Целью действия ст.274 должно быть предупреждение невыполнения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой информации. Данная уголовная норма, естественно, не содержит конкретных технических требований и отсылает к ведомственным инструкциям и правилам, определяющим порядок работы, которые должны устанавливаться специально управомоченным лицом и доводиться до пользователей. Применение данной статьи невозможно для систем публичного доступа, например, глобальной компьютерной сети Internet; ее действие распространяется только на компьютеры и локальные сети организаций.

В этой статье также считается, что под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим ее правовой защиты, например - государственная, служебная и коммерческая, банковская тайны, персональные данные и т. д .

Данная статья требует чтобы между фактом нарушения и наступившим существенным вредом была установлена причинная связь и полностью доказано, что наступившие последствия являются результатом именно нарушения правил эксплуатации, а не программной ошибкой либо действиями, предусмотренными в ст.272, 273 УК РФ.

Непосредственный объект преступления, предусмотренного этой статьей, - отношения по соблюдению правил эксплуатации ЭВМ, системы или их сети, т. е. конкретно аппаратно-технического комплекса.

Под таковыми правилами понимаются:

1) общероссийские санитарные нормы и правила для работников вычислительных центров,

2) техническая документация на приобретаемые компьютеры,

3) конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка.

Нарушение этих правил (несоблюдение, ненадлежащее соблюдение либо прямое нарушение) может быть осуществлено путем как активного действия, так и бездействия.

Состав части 1 статьи сформулирован как материальный. При этом общественно опасные последствия заключаются в одновременном наличии двух факторов:

1. уничтожения, блокирования или модификации охраняемой законом информации ЭВМ;
2. вызванного этим существенного вреда.

Необходимо учитывать, что поскольку речь идет о правилах эксплуатации именно ЭВМ, т.е. программно-аппаратной структуры, то и нарушение их должно затрагивать только техническую сторону несоблюдения требований безопасности компьютерной информации, а не организационную или правовую.

Представляется правильным отнесение к таковым следующих: блокировку системы защиты от несанкционированного доступа, нарушение правил электро- и противопожарной безопасности, использование ЭВМ в условиях, не отвечающих тем, которые установлены документацией по ее применению (по температурному режиму, влажности, величине магнитных полей и т.п.), отключение сигнализации, длительное оставление без присмотра и многие другие. Однако все эти действия должны рассматриваться не самостоятельно, а только лишь в связи с угрозой безопасности хранимой в ЭВМ и охраняемой законом информации.

Правонарушение может быть определено как преступление только при наступлении существенного вреда.

Определение существенного вреда, предусмотренного в данной статье будет устанавливаться судебной практикой в каждом конкретном случае исходя их обстоятельств дела, однако очевидно, существенный вред должен быть менее значительным, чем тяжкие последствия.

Слабость правоприменительной практики не дает четкого понимания природы последнего, но все же целесообразно под существенным вредом следует понимать, прежде всего, вред, наносимый информации в ее значимой, существенной части. Это, например, уничтожение, блокирование, модификация ценной информации (относящейся к объектам особой важности, либо срочной, либо большого ее объема, либо трудно восстановимой или вообще не подлежащей восстановлению и т.д.); уничтожение системы защиты, повлекшее дальнейший ущерб информационным ресурсам; широкое распространение искаженных сведений и т.п.

Квалифицированный состав нарушения правил эксплуатации ЭВМ предусматривает наличие двух форм вины, поскольку конструкция рассматриваемой статьи предусматривает умысел по отношению к деянию и неосторожность по отношению к наступившим последствиям.

Первым неблагоприятным последствием является умышленное уничтожение, блокирование или модификации компьютерной информации, однако преступление будет оконченным только при наступлении второго общественно

опасного последствия опасного последствия – неосторожного причинения опасного последствия – неосторожного причинения тяжкого вреда.

Сами же правила эксплуатации ЭВМ, системы ЭВМ или их сети при совершении преступления, предусмотренными ч.2. ст.274 УК РФ, виновным нарушаются умышленно. Виновное лицо сознает общественную опасность нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, предвидит возможность или неизбежность наступления вредных последствий в виде уничтожения, блокирования, модификации компьютерной информации, нарушения работы ЭВМ, системы ЭВМ или их сети, желает или сознательно допускает наступление этих последствий либо относиться к ним безразлично. Факультативные признаки субъективной (как и объективной) стороны состава преступления могут быть учтены судом в качестве смягчающих или отягчающих ответственность обстоятельств.

Объективная сторона данного преступления состоит в нарушении правил эксплуатации ЭВМ и характеризуется:

1) Общественно опасным деянием (действием или бездействием), которое заключается в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети.
2) Настеплением общественно опасных последствий в виде уничтожения блокирования или модификации компьютерной информации, причинивших существенный вред или повлекших по неосторожности тяжкие последствия.
3) Наличием причинной связи между действием и наступившими последствиями.

При описании объективной стороны данного вида общественно опасных посягательств законодатель использует бланкетный способ: указание в диспозиции статьи на действие (бездействие) носит общий характер – «нарушение правил». Конкретное содержание этих правил раскрывается в нормативных актах других отраслей права. Правила эксплуатации ЭВМ могут быть предусмотрены как в общих требованиях по технике безопасности и эксплуатации ЭВМ и периферийных устройств, так и в специальных правилах и инструкциях, регламентирующих особые условия эксплуатации ЭВМ (например, продолжительность работы и последовательность операций).

Субъективную сторону части 1 данной статьи характеризует наличие умысла направленного на нарушение правил эксплуатации ЭВМ. В случае наступления тяжких последствий ответственность по части 2 ст.274 наступает только в случае неосторожных действий.

Умышленное нарушение правил эксплуатации ЭВМ, систем ЭВМ и их сети влечет уголовную ответственность в соответствии с наступившими последствиями и нарушение правил эксплуатации в данном случае становится способом совершения преступления.

Например, действия технического специалиста больницы поставившего полученную по сетям программу без предварительной проверки (что говорит о преступной неосторожности) на наличие в ней компьютерного вируса, повлекшее нарушение работы ЭВМ и отказ работы систем жизнеобеспечения

реанимационного отделения, повлекшее смерть больного должны квалифицироваться по части 2 ст.274.

Представляется, что подобные действия совершенные умышленно должны квалифицироваться как покушение на убийство.

Субъект данного преступления - специальный, это лицо в силу должностных обязанностей имеющее доступ к ЭВМ, системе ЭВМ и их сети и обязанное соблюдать установленные для них правила эксплуатации.

Часть 2 - состав с двумя формами вины, предусматривающий в качестве квалифицирующего признака наступление по неосторожности тяжких последствий. Содержание последних, очевидно, аналогично таковому для ч.2 ст.273.

По данным правоохранительных органов, имеются сведения о фактах несанкционированного доступа к ЭВМ вычислительного центра железных дорог России, а также к электронной информации систем учета жилых и нежилых помещений местных органов управления во многих городах, что в наше время подпадает под ответственность, предусмотренную ст.272 УК, либо ст.274 УК в зависимости от действий лица, осуществившего посягательство и правил эксплуатации конкретной сети. Необходимо отличать преступление, предусмотренное ст.274 УК РФ от неправомерного доступа к компьютерной информации. Указанная статья устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред (ч.1 ст.274 УК) или повлекло по неосторожности тяжкие последствия (ч.2 ст.274 УК), Основные различия между этими преступлениями состоят в том что:

А) при неправомерном доступе к компьютерной информации виновный не имеет права вызвать информацию, знакомиться с ней и распоряжаться ею, иными словами, действует несанкционированно.

Состав же нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, напротив, предполагает, что виновный, в силу занимаемого служебного положения или выполнения функциональных обязанностей, вызывает информацию правомерно, т. е. действует в этом плане на законных основаниях.

Таким образом, в отличии, субъект преступного посягательства, предусмотренногост.274 УК РФ - законный пользователь информации;

Б) неправомерный доступ к компьютерной информации – преступление, совершаемое только путем активных действий, тогда как нарушение правил эксплуатации ЭВМ или их сети может быть совершенно и бездействием (например, виновный не включает систему защиты информации от несанкционированного доступа к ней, оставляет без присмотра свое рабочее место и т. д.);

В) необходимым признаком объективной стороны анализируемых преступлений выступают общественно опасные последствия, которые, однако, по своему содержанию и объему неравнозначны. Ответственность по ст.274 УК РФ

наступает только в том случае, если уничтожение, блокирование или модификация охраняемой законом информации ЭВМ причинило существенный вред потерпевшему. Для привлечения к ответственности по ст.272 УК РФ причинение существенного вреда не требуется. Достаточно установить сам факт уничтожения, блокирования, модификации или копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Кроме того, закон не предусматривает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, если это деяние повлекло копирование информации, даже причинившее существенный вред. Указанное положение свидетельствует о неравнозначном подходе законодателя к объему преступных последствий, выступающих в качестве обязательных признаков для составов преступлений, предусмотренных ст. ст. 272 и 274 УКРФ.

Как указывалось выше, в уголовном кодексе предусмотрена также довольно большая группа преступлений, совершение которых может быть связано не только с воздействием на компьютерную информацию, но и повлечь вредные последствия на компьютерную информацию, но и повлечь вредные последствия в виде уничтожения, блокирования, модификации либо копирования информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

2.4 Проблемы квалификации преступлений предусмотренных гл. 28 УК РФ

Используемый в литературе термин «компьютерное мошенничество» применительно к УК РФ, строго говоря, является юридической фикцией, поскольку ни одна из существующих в нем норм не отражает в полной мере той специфики общественных отношений, которые подвергаются общественно опасным посягательствам, совершаемым в корыстных целях с помощью компьютеров. И это несмотря на то, что компьютеры все шире применяются во многих областях жизни российского общества. Столь же быстро растет и число преступлений, связанных с их использованием, множатся в своем разнообразии способы и формы совершения такого рода преступлений.

При компьютерном мошенничестве в юридической литературе проводится мысль о необходимости квалификации только по ст.159 УК РФ (мошенничество) либо, в зависимости от обстоятельств дела, по ст.158. Приоритет отдается преступлениям против собственности, в которых компьютер (компьютерные сети) является лишь орудием, средством. По этому же пути идет и судебная практика, которая, правда, весьма скудна.

Одним из проблемных вопросов квалификации преступлений со сложными составами является, в частности, вопрос о том, охватываются ли ими перечисленные простые составы либо требуется квалификация по совокупности. В юридической литературе отмечается, что «составляющие сложные составные деяния не могут выходить за пределы родового объекта посягательства и быть по категории и связанной с ней наказуемостью опаснее, нежели единое сложное преступление». Поэтому будет ли правомерным пиратское тиражирование

компьютерных программ квалифицировать только по ст. 146 УК РФ либо хищение денежных средств с использованием компьютерных сетей - только по ст. 159 или 158 УК РФ даже при наличии в этих статьях такого квалифицирующего признака, как использование компьютерных средств (что, кстати, предусматривалось в проекте Уголовного кодекса РФ, а сегодня существует в Кодексах Республик Узбекистан и Кыргызстан, а также в Модельном Уголовном кодексе стран-участниц СНГ)? Одни авторы считают, что в данных случаях компьютер является только средством, техническим инструментом, поэтому нельзя говорить о квалификации по совокупности; другие отстаивают иную точку зрения. На наш взгляд, именно она представляется предпочтительной. Да, при хищении безналичных денег с помощью компьютера последний является только средством, однако средством не простым - его нельзя приравнять к «фомке» или топору. При незаконном проникновении в компьютерную сеть и модификации или копировании охраняемой информации преступник не только посягает на отношения собственности или личности, но и нарушает информационную безопасность, которая является видовым объектом по отношению к родовому - общественной безопасности. Этот объект не охватывается составами преступлений против собственности, государства или личности. Ведь если лицо совершает какое-то деяние с использованием оружия, то в большинстве случаев речь пойдет о квалификации по совокупности этого преступления и незаконного ношения (хранения и т.п.) оружия, так как в данном случае страдает еще один объект - отношения общественной безопасности.

Таким образом, представляется, что при посягательстве на различные объекты (собственность, права граждан, государственная безопасность и т.п.), совершенном посредством компьютера или компьютерных сетей, при реальном выполнении виновным нескольких составов квалификация должна осуществляться по совокупности соответствующих статей, предусматривающих ответственность за преступления против собственности, прав граждан и т.п., и статей, предусмотренных гл. 28 УК РФ.

Точно так же необходимо поступать и в случаях с компьютерным пиратством. При незаконном тиражировании и распространении компьютерных программ не только страдают права автора, но и затрагиваются отношения информационной безопасности. В ряде случаев, когда дело не имеет большого общественного значения, государство не в состоянии при отсутствии заявления автора компьютерной программы привлечь преступника к уголовной ответственности.

Анализ корыстных преступлений, совершаемых с использованием компьютеров, и конструкций статей УК РФ, содержащихся в гл. 21, 28 и в отдельных статьях некоторых других глав (например, ст.201), позволяет сделать вывод о многообъектности указанных преступных посягательств и, следовательно, о сложности их квалификации.

Мы считаем, что термин «компьютерные преступления» можно рассматривать в трех аспектах:

1) преступления, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей

информации как таковых. Данные преступления не направлены на совершение противоправных операций с информацией, содержащейся в компьютерах и базах данных, и должны квалифицироваться по статьям гл. 21 УК РФ - как преступления против собственности;

2) преступления, направленные на получение несанкционированного доступа к компьютерной информации, создание компьютерных «вирусов» - вредоносных программ - и заражение ими других компьютеров, - нарушение правил эксплуатации ЭВМ. Ответственность за такие преступления предусмотрена ст. 272-274 УК РФ, помещенными в отдельную гл. 28 УК РФ;

3) преступления, в которых компьютеры и другие средства компьютерной техники используются злоумышленниками как средство совершения корыстного преступления и умысел направлен на завладение чужим имуществом путем внесения изменений в программы и базы данных различных организаций.

В настоящее время весьма распространены хищения в банковской деятельности с использованием ЭВМ или компьютерных сетей. Для этого вида хищения характерно то, что преступники, используя служебное положение, имеют доступ к компьютерной информации финансового характера, сосредоточенной в вычислительных центрах банковских учреждений, и, обнаружив пробелы в деятельности ревизионных служб, осуществляют криминальные операции с указанной информацией, находящейся в ЭВМ или на машинных носителях:

1 вносят искажения, неправильные (фальсифицированные) данные в программные выходные данные ЭВМ с последующим их использованием для хищений;

2 устанавливают код компьютерного проникновения в электронную платежную сеть расчетов по карточкам;

3 создают дубликаты платежных карточек, иногда даже моделируют бухгалтерскую систему банка или другой организации и т.д.

В ряде случаев проникновение в компьютерные сети и доступ к нужной информации осуществляется с помощью различных технических средств. В результате преступники получают возможность снимать с компьютерных счетов клиентов наличные деньги любой валюте.

Совершению этих преступлений также предшествует определенная подготовка, характер которой зависит от степени связей правонарушителей с деятельностью вычислительного центра банка. Посторонние лица продумывают пути доступа к компьютерной системе, пытаются выяснить пароли и ключи программ. Программисты, операторы и другие работники компьютерного центра либо других подразделений банка, замышляющие подобную аферу, выбирают наиболее благоприятную для ее совершения обстановку, могут создать подставную фирму с расчетным счетом для «перекачивания» похищенных денег и т.д.

Преступная акция, по сути, складывается из начала контактных действий правонарушителя с ЭВМ или машинными носителями и снятия необходимой

информации либо денег с электронных счетов банка, их непосредственного присвоения или перевода на счета «липовых» организаций.

В этих условиях возникает проблема отграничения хищений от преступлений, предусмотренных в гл. 28 УК РФ. Встает вопрос о том, что же все-таки совершают преступники: мошенничество или они обманывают потерпевшего либо совершают тайное хищение, т.е. кражу?

Представляется, что злоумышленники, совершающие действия, предусмотренные диспозициями ст. 272-274 УК РФ, и не имеющие корыстной цели, а преследующие, допустим, исследовательский интерес, должны наказываться именно по этим статьям при условии наступления указанных в них последствий. Если же лицо, преодолев системы защиты компьютерной информации, подобрав пароли и ключи, проникло в компьютерную сеть банка и внесло в нее определенные изменения, а затем внесение таких изменений позволило ему перевести на свои счета денежные средства, то в этом случае по ныне действующему законодательству его действия необходимо будет квалифицировать по совокупности ст. 272 УК РФ и статьи, предусматривающей ответственность за хищение. Некоторые авторы безапелляционно утверждают, что хищение в данном случае происходит в форме мошенничества. Этот вопрос можно считать дискуссионным.

Завидов Б.Д. не ставит вопроса о том, есть ли обман в рассматриваемых преступлениях. Он сразу раскрывает суть обмана, которая видится ему в сознательно неправильном оформлении компьютерных программ, несанкционированном воздействии на информационный процесс, неправомерном использовании банка данных, применении неполных или дефектных, искаженных программ в целях получения чужого имущества или права на него. Но происходит ли в данном случае обман?

В строгом значении этого слова злоумышленник обманывает не потерпевшего, а компьютер, компьютерную систему. И если это так, то какой вид обмана он использует? Допустим, активный, но ведь не происходит предоставления информации компьютеру. Информация в нем уже содержится и лишь определенным образом искажается. И уже только потом, осуществляя преступный замысел на заключительной стадии и обналичивая переведенные на его счета деньги, преступник контактирует с людьми, осуществляющими банковские операции, при обналичивании переведенных средств (кассирами, операционистами банка). Однако думается, что он действует все-таки тайно, так как эти лица не имеют представления о преступном характере действий их клиента, который, в свою очередь, в момент получения денег в банке никаких ложных сведений, как правило, не предоставляет, а лишь снимает со своего счета средства, якобы ему принадлежащие. Приведенные аргументы говорят в пользу того, чтобы в определенных ситуациях следует рассматривать хищения денежных средств с использованием средств компьютерной техники по совокупности статей гл.28 и ст.158 «Кража» УК РФ.

В качестве контраргумента может приводиться довод о том, что, подобно мошенническим операциям, в данном случае преступник использует определенный подлог.

В хищениях же банковских средств исключительно с помощью средств компьютерной техники без каких-либо контактов с уполномоченными сотрудниками кредитных учреждений поддельные документы не фигурируют, и поэтому присутствует тайность хищения - признак кражи. Именно как кража необходимо квалифицировать деяния, аналогичные, например, совершенному Л., который, находясь в Санкт-Петербурге, добился перевода 10 млн. долл. со счетов City Bank of America на счета своих доверенных лиц в разных странах, не удаляясь от собственного рабочего стола с компьютером.

Вывод по разделу 2

В отдельных случаях хищения денежных средств с помощью компьютера могут совершаться не только операционистами банков, но и работниками, выполняющими в банках управленческие функции. Очевидно, что в подобных ситуациях может наступать ответственность за злоупотребление полномочиями по ст.201 УК РФ. Необходимо, однако, учесть, что для применения данной уголовно-правовой нормы нужно установить факт причинения существенного вреда именно тому банку, в котором работает злоумышленник, что само по себе представляет определенную проблему ввиду отсутствия конкретного определения существенного вреда. Кроме того, согласно примечанию 2 к указанной статье уголовное преследование такого лица, причинившего ущерб банку, в котором он работает, возможно лишь по заявлению этой организации или с ее согласия. Но зачастую преступления, направленные на завладение чужим имуществом, совершенные с использованием средств компьютерной техники, необходимо квалифицировать по совокупности ст.201 и статей гл.28 «Преступления в сфере компьютерной информации» УК РФ.

ЗАКЛЮЧЕНИЕ

С момента зарождения человеческого общества люди испытывают потребность в общении друг с другом. Первоначально общение (обмен сведениями) осуществлялось жестами, знаками, мимикой и нечленораздельными звуками, затем появились человеческая речь, письменность, книгопечатание. В XX столетии получили развитие такие средства коммуникации, как телеграф, телефон, радио, кино, телевидение, компьютер. Параллельно проходил и иной процесс: по мере появления различных достижений науки и техники многие из них принимались на вооружение преступного мира. С повышением роли информации во всех сферах человеческой деятельности повышается роль и значение компьютерной информации как одной из популярных форм создания, использования, передачи информации. А с повышением роли компьютерной информации требуется повышать уровень ее защиты с помощью технических, организационных и особенно правовых мер.

Однако внедрение во все сферы деятельности компьютерной техники сыграло наиболее существенную роль в деле технического вооружения преступности. «Невидимость» компьютерного преступника и одновременно «удлинение его рук» путем доступа к любым охраняемым секретам - военным, финансовым, иным - делают его весьма привлекательным для представителей преступного мира. Компьютерные махинации, как правило, остаются незамеченными на фоне уличной преступности.

С 1992 года законодатель начал вводить правовое регулирование в сфере использования компьютерной информации, но не всегда последовательное. В частности, несоответствие терминологии различных законов, например, несоответствие сути термина «информация» употребленного в Федеральном законе «Об информации, информатизации и защите информации» и Уголовном законе. Отсутствие, законодательного закрепления некоторых терминов употребляемых в Уголовном законе, например, «ЭВМ», «система ЭВМ», «сеть ЭВМ», «копирование информации» и других. Непоследовательность обнаруживается и в самом Уголовном законе, например, при нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети упоминается о последствиях в виде уничтожения, блокирования или модификации информации, но ничего не говорится о нарушении работы ЭВМ, системы ЭВМ, их сети, хотя это, как и в двух других составах предусмотренных Уголовным кодексом, может принести собственнику ущерб. Также нужно сказать о непоследовательном подходе к формированию квалифицирующего признака о неосторожном причинении тяжких последствий. Такой признак предусмотрен в двух статьях 273 и 274 УК РФ, а это нельзя признать верным, т.к. неосторожное причинение тяжких последствий в равной степени может быть следствием всех трех незаконных деяний.

Представляется необходимым внесение значительного массива дополнений и изменений в действующее законодательство, а также издания новых законов вносящих правовое регулирование в информационные отношения,

обусловленные распространением на территории России глобальной сети Интернет.

Уникальность компьютерной сети Интернет состоит в том, что она не находится во владении какого-то физического лица, частной компании, государственного ведомства или отдельной страны. В результате практически во всех сегментах этой сети отсутствует государственное регулирование, цензура и другие формы контроля за информацией, циркулирующей в Интернет. Такое положение дел открывает почти неограниченные возможности для доступа к любой информации, которые все шире используются в преступной деятельности. Как следствие, во многих случаях сеть Интернет может с полным правом рассматриваться не только как инструмент совершения компьютерных преступлений, но и как среда для ведения разнообразной незаконной деятельности. При использовании сети Интернет в этом качестве деятельности правонарушителей, в первую очередь, привлекает возможность неограниченного обмена информацией криминального характера. Использовать коммуникационные системы, обеспечивающие такую же оперативную и надежную связь по всему миру, раньше были в состоянии только спецслужбы сверхдержав - Америки и России, которые обладали необходимыми космическими технологиями.

Другая привлекательная для преступников особенность сети Интернет связана с возможностью осуществлять в глобальных масштабах информационно-психологическое воздействие на людей. Преступное сообщество весьма заинтересовано в распространении своих антиобщественных доктрин и учений, в формировании общественного мнения, благоприятного для укрепления позиций представителей преступного мира в обществе, и в дискредитации правоохранительных органов.

Также считаем, что проработка вопросов в юридической литературе об информационных отношениях, в общем, и компьютерных преступлений в частности, находится на низком уровне. Многие суждения, как в техническом плане, так и в юридическом плане, далеки от практики. Некоторые приводимые мнения только запутывают, нежели помогают разобраться. В связи с чем, в работе приведены собственные мнения по некоторым вопросам, в частности, по формулировке понятия «ЭВМ», «системы ЭВМ», «компьютерного преступления», «неправомерного доступа» и других.

В настоящее время крайне необходимо более глубокое теоретическое осмысление нового законодательства об информационных отношениях, внесенных новелл и практики применения. Необходимо поднять многие дискуссионные вопросы для обсуждения, как в рамках специализированных конференций, так и в Интернет-конференциях и Интернет-форумах.

Анализ судебной и следственной практики показал, что следователи и судьи практически не имеют знаний в юридических и технических вопросах компьютерных преступлений и действуют по аналогии, что приводит к неправильной квалификации и необоснованным приговорам. Хотя при территориальных органах управления внутренних дел созданы подразделения по

борьбе с преступлениями в сфере высоких технологий, но работают там сотрудники по большей части недостаточно квалифицированные либо в технической стороне, либо в юридической стороне компьютерного преступления. В связи с чем, по нашему мнению, требуется осуществить следующие организационные и правовые меры:

1. по подбору в данные подразделения только специалистов в обеих областях, либо подготовке таких специалистов и дальнейшее постоянное и динамичное повышение их квалификации;
2. закрепить, в рамках подведомственности, дела о компьютерных преступления только за этими подразделениями;
3. разработать научные методики, программные средства и технические устройства для получения и закрепления доказательств совершения компьютерного преступления.

Преступления в сфере компьютерной информации, особенно это касается взлома удаленных компьютеров, практически являются идеальной возможностью для преступников совершать свои деяния без наказания. Практическая возможность доказательства этих преступлений сводится к цифре очень приближенной к нулю. Конечно, особо громкие дела известны всему миру, но в связи с компьютерной и законодательной безграмотностью нашего населения дела, связанные с хищением информации, взломов компьютеров и тому подобное, почти не когда не заводятся, а если такое случается, то редко и сложно доказуемые.

Все компьютерные преступления условно можно подразделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства. В российском уголовном законодательстве уголовно-правовая защита компьютерной информации введена впервые. Уголовный кодекс РФ содержит главу №28 «Преступления в сфере компьютерной информации».

Правонарушения, совершаемые с использованием компьютерной техники и телекоммуникационных сетей связи, характеризуются высокой степенью латентности. Основной их отличительной чертой является то, что злоумышленник может совершать противоправные действия, не покидая своей квартиры, дачи или офиса. Компьютерные преступления, в том числе хакерские «атаки» финансовых систем и крупных информационных порталов, давно приобрели уже не только организованный, но и трансграничный характер. Универсальные возможности сети Internet позволяют нарушителям из разных стран договориться и координировать свои деструктивные действия.

Рост численности преступлений, совершаемых в сфере информационного обмена, их многочисленные разновидности и изощренность, способность нарушителей оперативно устранять следы своего вмешательства в нормальное течение информационных процессов - все это обусловливает необходимость в постоянном повышении квалификации, уровня знаний и подготовки правоведов и других специалистов, которые вынуждены противостоять хакерам и другим компьютерным злоумышленникам.

Сомнений в необходимости существования уголовно-правовой защиты компьютерной информации нет. Уголовный закон достаточно строго преследует за совершение компьютерных преступлений. Это связано с высокой степенью общественной опасности.

Также хотелось бы подчеркнуть, что абсолютную надежность и безопасность в компьютерных сетях не смогут гарантировать никакие аппаратные, программные и любые другие решения. В то же время свести риск потерь возможно лишь при комплексном подходе к вопросам безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Всеобщая декларация прав человека (принята на 3-ей сессии Генеральной Ассамблеи ООН) от 10 декабря 1948 года // Российская газета. – 1995. – 5 апреля.
2. Конституция Российской Федерации (принята на всенародном голосовании 12.12.1993г.) // Российская газета. – 1993. – № 237.
3. Гражданский кодекс РФ (часть первая) от 30.11.1994 № 51–ФЗ // Российская газета. –1994. – 8 декабря.
4. Гражданский кодекс РФ (часть четвертая) от 18.12.2006 № 230–ФЗ // Российская газета. – 2006. – 22 декабря.
5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63–ФЗ. – СПС «Консультант Плюс».
6. Закон РФ «О государственной тайне» от 21.07.1993 № 5485№1 // Российская газета. – 1993. – 21 сентября.
7. Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.1992 № 3523№1 // Российская газета. – 1992. – 20 октября.
8. Закон РФ «О правовой охране топологий интегральных микросхем» от 23.09.1992 № 3526–1 // Российская газета. – 1992. – 21 октября.
9. Федеральный закон РФ «О связи» от 07.07.2003 № 126–ФЗ // Российская газета. – 2003. – 10 июля.
10. Федеральный закон РФ «Об информации, информатизации и защите информации» от 20.02.1995 № 24–ФЗ // Российская газета. – 1995. – 22 февраля.
11. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149–ФЗ // Российская газета. – 2006. – 29 июля.
12. Федеральный закон РФ «Об обязательном экземпляре документов» от 29.12.1994 № 77–ФЗ // Российская газета. – 1995. – 17 января.
13. Федеральный закон РФ «Об участии в международном информационном обмене» (утратил силу) от 04.07.1996г № 85–ФЗ // Российская газета. – 1996. – 11 июля.
14. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». – СПС «Консультант Плюс».
15. Абдеев, Р.Ф. Философия информационной цивилизации / Р.Ф. Авдеев. – М.: Слово, 1994. –336 с.
16. Барсуков, В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2000. –496 с.
17. Батурин, Ю.М. Проблемы компьютерного права / Ю.М. Батурин. – М.: Юридическая литература, 1998. – 272 с.

18. Безруков, Н.А. Введение в компьютерную вирусологию. Общие принципы функционирования, классификация и каталог наиболее распространенных вирусов в MS DOS / Н.А. Безруков. – Киев: УРЕ, 2006. – 416 с.
19. Вехов, В.Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов. – М.: Юринформ, 2005. – 182 с.
20. Главный информационно-аналитический центр МВД России. Состояние преступности в России за январь–декабрь 1997–2000, 2014–2017. – https://мвд.рф/Delj atelnost/statistics.
21. Гульбин, Ю. Преступления в сфере компьютерной информации / Ю. Гульбин // Российская юстиция. – 1997. – № 10.
22. Гуров, А.И. Криминогенная ситуация в России на рубеже XXI века / А.И. Гуров. – М.: ВНИИ МВД России , 2000. – 96 с
23. Завидов, Б.Д. О понятии мошенничества и его модификациях (видоизменениях) в уголовном праве / Б.Д. Завидов // Право и экономика. – 1998. – № 11. – С. 50–51.
24. Зеленский, В.Д. Основы компьютеризации расследования / В.Д. Зеленский. – Краснодар: Кубан. гос. ун-та, 1998. – 78 с.
25. Карелина, М.М. Преступления в сфере компьютерной информации / М.М. Карелина. – М.: Юридическая литература, 1998. – 55 с.
26. Карпинский, О. Защита информации, виртуальные частные сети (VPN). Технология ViPNet / О. Карпинский. – Gazeta.Ru.– 2001. – 18 июня.
27. Козлов, В.Е. Теория и практика борьбы с компьютерной преступностью / В.Е. Козлов. – М.: Горячая линия, Телеком. – 2012. – 336 с.
28. Комиссаров, В.С. Преступления в сфере компьютерной безопасности: понятие и ответственность / В.С. Комиссаров // Юридический мир. – 2003. – № 2. – С. 72.
29. Комментарий к уголовному кодексу РФ. Научно-практический комментарий / под ред. В.М.Лебедев. – М.: Юрайт–М, 2004. – 1359 с.
30. Кочои, С. Ответственность за неправомерный доступ к компьютерной информации / С. Кочои, Д.Савельев // Российская юстиция. – 1999. – № 1. – С. 44– 45.
31. Крылов, В.В. Информационные компьютерные преступления / В.В. Крылов. – М.: Инфра–М–Норма, 1997. – 285 с.
32. Крылов, В.В. Основы криминологической теории расследования преступлений в сфере информации: автореферат дис.... канд. юрид. наук / В.В. Крылов. – М., 1997. – 50 с.
33. Кузнецов, А.В. Некоторые вопросы расследования преступлений в сфере компьютерной информации / А.В. Кузнецов // Информационный бюллетень следственного комитета МВД РФ. – 1998. – № 2. – С. 51–54.
34. Кузнецова, Н.Ф. Квалификация сложных составов преступлений / Н.Ф. Кузнецова // Уголовное право. – 2000. – № 1. – С. 26.

35. Ляпунов, Ю. Ответственность за компьютерные преступления / Ю. Ляпунов, В. Максимов // Законность. – 1997. – № 1. – С. 19.
36. Максимов, В.Ю. Компьютерные преступления (вирусный аспект) / В.Ю. Максимов. – Ставрополь: Кн. Из-во, 1999. – 112 с.
37. Маслакова, Е.А. История правового регулирования уголовной ответственности за компьютерные преступления / Е.А. Маслакова // Информационное право. – 2006. – № 4. – С. 408.
38. Мещеряков, В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект / В.А. Мещеряков. – Воронеж: Воронеж. гос. ун-та 2001. – 120 с.
39. Научно-практический комментарий к УК РФ в двух томах. – СПС «Консультант Плюс».
40. Ожегов, С.И. Словарь русского языка / С.И. Ожегов. – М.: Наука, 1989. – 736 с.
41. Панфилова, Е.И. Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе» / Е.И. Панфилова, А.Н. Попов. – СПб.: Нолидж, 1998. – 47 с.
42. Погуляев, В. Обеспечение конфиденциальности / В. Погуляев, А. Теренин // ЮРИСТ. – 2004. - № 2. – С. 34.
43. Постатейный Комментарий к Уголовному кодексу РФ / под ред. Наумова А.В. – М.: БЕК, 2015 – 325 с.
44. Сальников, В.П. Компьютерная преступность: уголовно-правовые и криминологические проблемы / В.П. Сальников //Государство и право. – 2000. – № 9. – С.101.
45. Смирнова, Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: дис... канд. юрид. наук / Т.Г. Смирнова. – М., 1999. – 161 с.
46. Талимончик, В.П. Компьютерные преступления и новые проблемы сотрудничества государств / В.П. Талимончик //Законодательство и экономика. – 2005. – № 5. – С. 14.
47. Уголовное право Российской Федерации. Особенная часть/ под ред. Здравомыслова Б.В. – М.:, БЕК, 2000. – 559 с.
48. Хакерская атака мирового масштаба. – https://www.gazeta.ru/social/2017/05/12/10671101.shtml
49. Харкевич, А.А. О ценности информации / А.А. Харкевич // Проблемы кибернетики. – 1961. – № 4 – С. 31.
50. Шершнев, Л.И. Безопасность человека / Л.И. Шершнев. – М.: Фонд национальной и международной безопасности, 1994. – 355 с.
51. Шумилов, Н.И. Криминалистические аспекты информационной безопасности: автореф. дис... канд. юрид. наук / Н.И. Шумилов. – СПб, 1997. – 169 с.
51. Яблоков, Н.П. Криминалистическая характеристика преступлений / Н.П. Яблоков // Вестник Московского университета. Серия 11. Право. – 1999. – № 1 – С.58.

52. Уголовное дело № 1–128/2017 по обвинению Бычина А.В. по ч. 2 ст. 146, ч. 2 ст. 272, ч. 2 ст. 273 УК РФ. – https: //ro spravosudie. Com.
53. Уголовное дело № 1–21/2017 по обвинению Маликова К.О. по ч. 1 ст. 273 УК РФ. – https: //ro spravosudie. Com.
54. Уголовное дело № 1–105/2016 по обвинению Шарапова В.М., Томилова Е.В. по ч. 2 ст. 273, ч. 2 ст. 272, ч. 2 ст. 159.6, ч. 1 ст. 274, УК РФ. https://rospravosudie.com