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

ДОПУСТИТЬ К ЗАЩИТЕ
заведующий кафедрой,
к.ю.н., доцент
_____И.М. Беляева
_____2017 г.

Преступления в сфере компьютерной информации

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
ФГАОУ ВО «ЮУрГУ» (НИУ) – 40.03.01. 2017.477 ВКР

Руководитель работы,
к.ю.н., доцент кафедры
_____ Л.В. Красуцких
_____2017 г.

Автор работы,
Студент группы Ю-477
_____ Ю.Е. Дробышевская
_____2017 г.

Нормоконтролер,
преподаватель
_____ Д.В. Бирюкова
_____ 2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В связи с развитием вычислительной техники и информационных технологий и их повсеместным применением в жизни человека возник ряд проблем в правовом регулировании непосредственно связанных с информатизацией общества. Данный факт позволил сформулировать вопрос о необходимости формирования новой отрасли права – компьютерного права сферой регулирования которого выступали бы информационные правоотношения и компьютерные посягательства. Многообразие способов совершения компьютерных преступлений также свидетельствует об актуальности поставленного вопроса.

При этом необходимо уделить особое внимание объектам таких посягательств. Ими могут быть технические средства, базы данных, программное обеспечение, да и в целом вся компьютерная информация. Сами противоправные деяния в которых так или иначе применяется цифровая техника и информационные технологии чрезвычайно разнообразны и трудноосуществимы. К ним относят несанкционированный доступ к информации, перехват сигналов различных сетей (сетей мобильной связи, сигналов, передающихся по сети Internet), подделка всевозможных ключей доступа и банковских карт, разработка вредоносного программного обеспечения, непосредственное хищение компьютерной информации и многое другое.

Наиболее часто встречающимся видом компьютерного посягательства является неправомерный доступ к компьютерной информации. Осуществляются данные противоправные действия чаще всего с корыстным умыслом и направлены на информацию, охраняемую законом. Данный вид преступления в сфере компьютерной информации с каждым годом все чаще и чаще встречается, поскольку информатизация общества приводит к тому, что информация становится наиболее дорогим и при этом массовым ресурсом общества. Разнородность и важность компьютерной информации

не позволяет недооценивать или переоценивать опасность компьютерных преступлений.

Отечественные правоведы лишь в 90-е годы стали активно исследовать компьютерную преступность. В связи с этим степень научной разработанности данной темы невелика. За прошедший период времени опубликован ряд работ, направленных на изучение данного вопроса и содержащих криминологические и криминалистические аспекты изучаемого вопроса, статистические данные, исторические ретроспективы. Публикации и исследования, посвященные уголовно-правовым вопросам компьютерных преступлений, встречаются гораздо реже. Большинство исследователей ограничивается лишь объектом, предметом или орудиями совершения компьютерных преступлений, не рассматривая их как комплексное явление. Встречаются и работы, содержащие лишь критику гл. 28 Уголовного кодекса РФ. Ряд авторов в своих трудах рассматривает компьютерные преступления исходя из достижений правовой науки, отбросив техническую сторону вопроса без которой довольно сложно уяснить и изучить суть преступлений в сфере компьютерной информации.

В связи с малым количеством теоретических исследований по теме применение ее на практике становится довольно проблематичным и как следствие – низкие показатели в борьбе с компьютерной преступностью.

В связи с изложенным ранее, можно сформулировать актуальность проблемы компьютерных преступлений которую предопределило развитие информационной инфраструктуры и развившейся на ее просторах компьютерной преступности. В связи данными процессами, протекающими в современном обществе возникла острая необходимость введения специальных составов преступлений в уголовные законы многих стран. Меры гражданско-правовой ответственности, появившиеся в качестве регуляторов информационных отношений несколько раньше уголовно-правовых, не смогли воздействовать на развитие компьютерных преступлений.

Исследованием вопросов компьютерной преступности посвятили свои труды: Агапов А.Б., Айков Д., Андреев Б.В., Батурин Ю.М., Белкин Р.С., Вейценбаум Дж., Вехов В.Б., Винеа Н., Жодзишский А.М., Жодзишский А.М., Зуев К.А., Исаченко И.И., Карась И.З., Карпинский О., Керр Д., Кочои С., Крылов В.В., Лебедев В.М., Литвинов А.В., Ляпунов Ю., Макнамара Д., Максимов В., Могилевский И.М., Мэдник С., Наумов В., Полежаев А.П., Проценко Д.Е., Россинская Е.Р., Савельев Д., Сальников В.П., Симкин Л.С., Скуратов Ю.И., Старостина Е.В Талимончик В.П., Фролов Д.Б., Черкасов В.Н., Черных А., и др

Несмотря на возрастающую популярность данной темы исследования по прежнему недостаточно внимания уделяется изучению непосредственно компьютерных преступлений. В связи с этим целью нашего исследования является изучение и анализ положений, связанных с преступлениями в сфере компьютерной информации, выявление недостатков в нормативно-правовой базе регулирующей данные вопросы и вынесении предложений по их устранению.

В соответствии с поставленной целью необходимо решить следующие задачи:

- рассмотреть понятие и дать общую характеристику преступлений в сфере компьютерной информации;
- изучить историю появления и развитие преступлений в сфере высоких информационных технологий;
- исследовать законодательство об уголовной ответственности за преступления в сфере компьютерной информации;
- дать уголовно-правовую характеристику отдельным составам преступлений в сфере компьютерной информации;
- проанализировать проблемы, возникающие в области борьбы с компьютерными преступлениями и предложить пути их решения.

Цели и задачи исследования определили его объект: правоотношения, складывающиеся в сфере охраны компьютерной информации.

Законодательство нацеленное на борьбу с компьютерными преступлениями является предметом исследования.

Для достижения поставленной цели использовались сравнительно-правовой метод, анализ, синтез, метод толкования правовых актов, статистический, логический и исторический методы.

Значимость исследования в том, что работа содержит в себе обобщение ряда исследований по данному вопросу, анализа современного законодательства, регулирующего преступления в сфере высоких технологий.

На основе результатов исследования сформулированы предложения по совершенствованию законодательства которые могут быть использованы в образовательной и правоприменительной среде.

1 КОНЦЕПТУАЛЬНЫЕ ПОДХОДЫ К ПОНЯТИЮ ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1 Понятие и общая характеристика преступлений в сфере компьютерной информации

Клод Шеннон в 1948 году впервые в истории предложил понятие такого термина как «информация» и, опираясь на положения теории вероятности и математической статистики предложил определение термина «количество информации»[1]. Оба данных термина он связывал с кибернетикой[2] – «наукой, занимающейся общими законами преобразования информации в сложных управляющих системах». Данная отрасль знаний изучает информацию исключительно в техническом аспекте, акцентируя свое внимание на информационных потоках, проходящих по цифровым каналам связи. Кибернетикой обосновано влияние информации на процессы управления, функционирования и развития любых систем.[3]

Качественный подход к измерению информации предполагает оценку количества информации исходя из ее содержимого, а именно из полезности каждого сообщения для человека его получающего. Весомость полученной информации определяется посредством изменения вероятности достижения получателем некоторой цели благодаря полученной информации[4].

На протяжении довольно длительного временного отрезка отношения, так или иначе связанные с информационными процессами, не признавались объектом правового регулирования, но начиная с конца XX века, во многом благодаря развитию вычислительной техники, ее персонализации и появлению локальных вычислительных сетей и их последующей глобализации, роль информации в жизни общества резко возросла, что, в

[1]Абдеев Р.Ф. Философия информационной цивилизации. – М. Слово, 1994. – С.33.
[2] Ожегов С.И. Словарь русского языка. – М. Наука, 1989. – С.222.
[3] Зеленский В.Д. Основы компьютеризации расследования. – Краснодар, 1998. – С.4.
[4] Харкевич А.А. О ценности информации // Проблемы кибернетики. – М., 1961. – № 4 – С.31.

свою очередь, привело к признанию информационных отношений в качестве предмета правового регулирования.

Сложность правового регулирования информационных отношений в обществе связана, прежде всего, со сложностью роли информации в современных общественных отношениях. Для регулирования этой новой и емкой области общественных отношений создается новое «информационное» законодательство и система мер, защищающих данные отношения в рамках уголовного права. Среди российских правоведов нет единой точки зрения на содержание ряда основных понятий, связанных с «информационными» правоотношениями таких как «информационная безопасность» или, например, «компьютерная преступность». [1]

Рассмотрим данное обстоятельство на примере термина «информационная безопасность».

Н.И. Шумилов определяет информационную безопасность как «состояние защищенности информационной сферы государства, общества, личности, обеспечиваемое комплексом мер по снижению, предотвращению или исключению негативных последствий от воздействия на элементы информационной сферы».

В свою очередь, Л.И. Шершнев, опираясь на сложность и многообразие угроз которым может быть подвергнута информация, определяет информационную безопасность как «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;

[1] Погуляев В., Теренин А. Обеспечение конфиденциальности // эж-ЮРИСТ. – 2004. – №2. – С.34.

вырабатывать личностные и групповые навыки и умения безопасного поведения; поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно не было навязано»[1].

Научно обосновано, что результативность противодействия преступлениям зависит от того, насколько качественно и глубоко исследователями разъяснены характеристики отдельных видов преступлений, причины их совершения, их особенности. В юриспруденции при анализе конкретных видов преступлений используются различные характеристики: угловно-правовая, криминологическая, криминалистическая. Любая из характеристик фокусирует внимание исследователя на отдельных, специфичных сторонах исследуемого явления. Например, криминологическая характеристика преступления позволяет выявить:

– признаки преступления:
– сведения, описывающие ситуацию совершения преступления;
– специфичные действия, направленные на предупреждение преступлений данного вида.

Опираясь на данный шаблон и исследования, составим криминологическую характеристику «компьютерных преступлений» (необходимо упомянуть, что российский законодатель определяет данную группу преступлений как «преступления в сфере компьютерной информации», в работах исследователей можно также встретить такие формулировки как «IT-преступления» или «преступления в сфере высоких технологий»). Характеристика будет содержать обоснование общественной опасности данной группы деяний, их отграничение от сходных правовых явлений, типичные свойства компьютерных преступлений, классификация на основе типичных свойств, информацию об условиях совершения преступлений (геополитические, социально-экономические, временные и

[1] Шершнев Л.И. Безопасность человека. Учебно-методическое пособие, – М.: Фонд национальной и международной безопасности, 1994. – С. 33-35.

др.), проблемы латентности, особенности личности правонарушителя и потерпевшего. В результате анализа данных сведений предлагается комплекс мер противодействия данным видам преступлений.

Компьютерные преступления – один из наиболее молодых видов преступлений, возникший в связи с массовым распространением персональных компьютером, последующим их объединением в вычислительные сети различных уровней. Впервые правонарушения с использованием электронных вычислительных машин (далее ЭВМ) были описаны в зарубежных средствах массовой информации в связи с «компьютерно-телефонным фанатизмом» - деятельностью по заказу при помощи ЭВМ или телефона различных товаров и услуг без последующей их оплаты. Пресса сразу же «окрестила» данные деяния как компьютерные или электронные преступления. Данный термин длительный период не имел не только правовой характеристики, но полного и подробного описания и при этом довольно успешно использовался в правоприменительной практике зарубежных стран. В настоящее время не существует однозначного понятийного аппарата, характеризующего компьютерные преступления.

В.В. Крылов компьютерные преступления рассматривает как «общественно опасные деяния, совершенные в области информационных правоотношений и запрещенные уголовным законом под угрозой наказания».[1]

Н.И. Шумиловым, говоря о компьютерных преступлениях, акцентирует внимание на информации как одном из признаков состава преступления, определяя таким образом группу однородных преступлений. По его утверждению: «Преступления рассматриваемого вида есть преступления в сфере информационной безопасности, или информационные преступления»[2].

[1] Крылов В.В. Основы криминологической теории расследования преступлений в сфере информации. Автореф. дис.... канд. юрид. наук, – М., 1997. – С.11.
[2] Шумилов Н.И. Криминалистические аспекты информационной безопасности. Автореф. дис... канд. юрид. наук. – СПб, 1997. – С.20.

А.И. Гуров и В.П. Талимончик в своих трудах отмечают, что в настоящее время в России криминализированы далеко не все правонарушения в сфере информационной безопасности, сфере высоких технологий[1], а только компьютерные преступления[2]. Несмотря на криминализацию ряда деяний в сфере информационных технологий в мировой и отечественной юридической практике до сих пор отсутствует общий понятийный аппарат, характеризующий данную сферу общественных отношений и правонарушений связанных с ними.

Ряд ученых к компьютерным преступлениям относит противоправные деяния, в которых компьютерная информация является объектом. При этом в качестве орудия совершения преступления выступает либо сама цифровая информация, либо ЭВМ, либо некоторая локальная вычислительная сеть. [3]

Однозначности в определении понятия компьютерных преступлений среди ученых-правоведов нет. Т.Г. Смирнова под компьютерными преступлениями (преступлениями в сфере компьютерной информации) понимает «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». Также она пишет: «нарушение правил эксплуатации ЭВМ и распространение зловредных программ деструктивного характера следует рассматривать как разновидность диверсий, наносящих значительный ущерб компьютерной информации посредством

[1] Гуров А.И. Криминогенная ситуация в России на рубеже XXI века. – М., 2000. – С.36.
[2] Талимончик В.П. Компьютерные преступления и новые проблемы сотрудничества государств // Законодательство и экономика, 2005. – №5. – С.14.
[3] Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. – М. Юринформ, 2005. – С.11.

разрушительных воздействий в отношении материальных носителей и зафиксированных на них данных» [1]

И.А. Клепицкий в своих исследованиях трактует преступления в сфере компьютерной информации как «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)»[2].

С течением времени в России, как и в других странах сформировался некоторый багаж правоприменительной практики в отношении компьютерных преступлений. Что характеризует данный вид преступлений не как единичные, разрозненные факты, а как подкласс преступлений, совершаемых с использованием информационных технологий. По мнению А.И. Гурова к данным преступлениям можно отнести:

- 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;
- незаконный экспорт технологий научно-технической информации и услуг, используемых при создании вооруженной техники, оружия массового уничтожения;
- неправомерный доступ к охраняемой законом компьютерной информации (ст.272 УК);

[1] Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации. Дис… канд. юрид. наук. – М., 1999. – С.32.
[2] Уголовное право Российской Федерации. Особенная часть / Под ред. Здравомыслова Б.В. – М, БЕК, 2000. – С.353.

– создание, использование и распространение вредоносных компьютерных программ (ст.273 УК);
– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст.274 УК)[1].

Приведенные точки зрения отечественных правоведов позволяют определить компьютерные преступления как деяния, предусмотренные уголовным законом, представляющие собой нарушение прав и интересов других лиц, совершенное в результате использования, модификации или уничтожения компьютерной информации. Наиболее развернутое определение компьютерного преступления, на наш взгляд, дает В.А. Мещеряков: «…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)»[2].

Необходимо отметить, что все приведенные выше определения «компьютерных» или «информационных» преступлений в своей основе содержат положения действующего уголовного закона. В российском законодательстве они расположены в главе 28 Уголовного кодекса РФ[3]

Российский законодатель, в статьях 272-274, определил лишь три состава преступлений. предусматривает три состава преступлений - ст.272-274.

---

[1] Гуров А.И. Криминогенная ситуация в России на рубеже XXI века. – М., 2000. – С.36-37.
[2] Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. – Воронеж, 2001. – С.25.
[3] Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ // «Собрание законодательства РФ» –1996. – С.2954.

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

В первую очередь необходимо определить что же является объектом исследуемых преступлений. По мнению ряда ученых родовым объектом преступлений в сфере компьютерной информации следует считать общественную безопасность (об этом косвенно говорит и законодатель, разместив компьютерные преступления в разделе IX – Преступления против общественной безопасности и общественного порядка). Родовым объектом в ряде случаев являются права и интересы граждан (врачебная тайна), юридических (коммерческая тайна) лиц или государства (государственная тайна).

В качестве родового объекта принято рассматривать те общественные отношения которые в силу своего характера формируют состояние защищенности информационных процессов (создание, сбор, обработка, хранение, передача, использование компьютерной информации), определяя круг лиц правомерно участвующих в осуществлении информационных процессов. Определяя содержание главы 28 УК РФ законодатель употребил термин «информация», что стало причиной трактовки компьютерных преступлений как деяний основным объектом которых является информация. По нашему мнению данная трактовка является некорректной.

Под предметом компьютерных преступлений законодатель понимает не только непосредственно компьютеры, но и их компоненты и компьютерные сети.

В большинстве случаев информационные преступления совершаются путем действий, что прослеживается ст. 272 и ст.273. Лишь в ст. 274 совершение преступления возможно как путем действия так и путем бездействия: нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сетей.

Среди компьютерных преступлений имеются как преступления с материальным составом (неправомерный доступ к компьютерной информации, нарушение правил эксплуатации ЭВМ), так и преступление с формальным составом – создание либо использование вредоносных программ для ЭВМ.

Временем совершения компьютерных преступлений в соответствии с ч.2 ст.9 УК РФ является момент совершения правонарушителем последней отправки команды на исполнение ЭВМ путем кнопки на клавиатуре ЭВМ или кнопки манипулятора ЭВМ («мышь», сенсорные панели ввода и др.).

Определение места совершения компьютерных преступлений является сложно разрешимой задачей в связи с тем, что большинство используемых устройств на данный момент тем или иным образом объединено в локальные вычислительные сети либо присоединено к глобальной сети Internet. Ярко демонстрирует эту точку зрения следующий пример.

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.

Преступление приведенное в примере является трансграничным, поскольку:

– затрагивает права и законные интересы лиц – держателей банковских карт проживающих в разных государствах;
– преступники являются гражданами разных государств;

Уголовный закон не дает определения места совершения преступления. Исходя из характера каждого конкретного компьютерного преступления местом его совершения может быть,

Рассмотрим еще один 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[1].

В мировой практике большая часть компьютерных преступлений приходится на такие деяния как компьютерное мошенничество, пиратство, саботаж и распространение вирусных программ. При этом, говоря о компьютерном пиратстве, подразумевают «хакерство» как его вид, т.е. деятельность, направленная на получение неправомерного доступа к компьютерной информации, в результате которой происходит модификация информации. В случаях, когда модификация информации ведет к утечке

[1] Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. – М.: Право и закон, 1996. – С.17-18.

денежных средств зарубежный законодатель вдет речь о компьютерном мошенничестве. Также зарубежный уголовный закон относит к компьютерным преступлениям копирование (тиражирование) и сбыт компьютерного программного обеспечения. В России данные действия не относятся к преступлениям в сфере компьютерной информации.

На сегодняшний день значительная часть компьютерных преступлений совершается профессиональными и организованными группами, довольно часто участниками этих групп, являются лица, осуществляющие трудовую деятельность в организациях-потерпевших.

1.2 История появления и развития преступлений в сфере информационных технологий

Как известно XX век в истории человечества ознаменовался бурным развитием техники и средств массовой коммуникации. Наиболее заметным событием стало внедрение технических средств на базе микропроцессоров в повседневную жизнь людей. Компьютеры, в силу ряда своих особенностей, стали незаменимым инструментом человека во многих сферах жизни. Эти события не обошли стороной и преступный мир во многом благодаря расширению сфер доступа и анонимности пользователей. Компьютерная преступность на сегодняшний день – один из наиболее незаметных видов преступности. На данный момент не определены ущерб и количество совершаемых компьютерных преступлений. Обнародованные сведения являются крайне расплывчатыми, а иногда и вовсе противоречивыми. Единственное в чем сходятся исследователи данной преступной направленности, так это в том, что количество компьютерных преступлений растет, но в еще большей степени растет ущерб ими причиняемый. По довольно скромным оценкам компьютерная преступность обходится мировому сообществу примерно в 200-400 млрд. долларов ежегодно.

На заре компьютерных преступлений начальник одного из отделов Контрольно-методического управления МВД отметил, что в СССР первое преступление в сфере информационных технологий было совершено в 1979 году. Тогда ущерб государству составил 80 тысяч рублей (на эти средства можно было приобрести 8 автомобилей «Волга»)[1]. Одним из первых компьютерных преступлений в 90-е годы было хищение 125,5 тысяч долларов во Внешэкономбанке. С тех пор статистика по преступлениям в сфере компьютерной информации выглядит следующим образом.

По данным ГИЦ МВД России[2], 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. 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.

Представленные данные красноречиво говорят о том, что преступления в сфере компьютерной информации представляют собой неуклонно возрастающую функцию. Кривизна данной функции соразмерна темпам информатизации российского общества и сходна с картиной развивающейся в мире.

Жертвой современного кибер-преступления может стать кто угодно: государства, предприятия, организации, физические лица. В основе всего

---

[1] Карпинский О. Защита информации, виртуальные частные сети (VPN). Технология ViPNet / По материалам компании Infotecs // Gazeta.Ru, 18.06.2001.

[2] Главный информационно-аналитический центр МВД России. Состояние преступности в России за январь – декабрь 1997-2000, 2014-2017 [Электронный ресурс]. – Режим доступа: https://мвд.рф/Deljatelnost/statistics.

этого лежит повсеместное применение вычислительной техники (компьютеров и их сетей). Компьютеры, как орудия или предметы в совершении преступлений, используются не только единичными преступниками, но и организованной преступностью

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»[1]. 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.

1.3 Нормативно-правовая база, регулирующая отношения в сфере компьютерной информации в России и за рубежом

Активное применение информационных технологий затрагивает все сферы жизни общества, в том числе и правовую. В связи с появлением и применением компьютеров не только возникли новые виды преступлений, но изменились ранее существовавшие. Они стали совершаться в новой форме или новым способом.

[1]Сальников В.П. Компьютерная преступность: уголовно-правовые и криминологические проблемы // Государство и право – 2000. – № 9. – С.101.

Основы законодательства, регулирующего информационные отношения, были заложены в 1948 году. Генеральная Ассамблея ООН во Всеобщей декларации прав человека и гражданина[1] сформулировало в качестве одно из прав право любого человека на свободу поиска получения и распространения информации любыми средствами независимо от государственных границ.

Уголовно-правовая практика в мире решает вопросы компьютерных преступлений в соответствии со своими правовыми традициями, принадлежностью к той или иной правовой семье. Наиболее часто встречается два пути разрешения данной проблемы. Один из путей состоит в дополнении уже имеющихся правовых норм, другой – в формировании новых составов преступлений и соответственно новых уголовно-правовых норм с новым объектом преступного посягательства.

Началом формирования нормативно-правовой базы, регулирующей информационные отношения в России можно считать принятие новой Конституции в 1993 году[2]. В ней произошло закрепление права человека и гражданина на свободу поиска получения и распространения информации, ранее закрепленной во Всеобщей декларации прав и свобод человека и гражданина. Также Конституция РФ накладывает некоторые ограничения на это право, например, в отношении данных, составляющих государственную тайну. Дополняет ограничения ст.23 в которой закреплены право на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ст.24 усиливает данное ограничение, запрещая любые действия со сведениями о частной жизни граждан без согласия этих граждан.

Следующим шагом должно было бы быть внесение изменений в Уголовный кодекс, однако данный ход развития событий оказался бы крайне сложным, практически неисполнимым, поскольку на тот момент времени

[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.

полностью отсутствовала нормативная база, определяющая основной понятийный ряд в области компьютерной информации. Не было и законодательства регулирующего авторские и смежные с ними права, имущественные и неимущественные правоотношения связанные с созданием и распространением программного обеспечения. Аналогична складывалась ситуация с такими понятиями как «международный информационный обмен» и «информационная безопасность»

В связи с этим в 1992 году принимается закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных»[1] (ныне утратил силу в связи с введением в действие части четвертой Гражданского кодекса РФ) и Закона Российской Федерации «О правовой охране топологий интегральных микросхем»[2] (ныне утратил силу в связи с введением в действие части четвертой Гражданского кодекса РФ). Основной функцией этих законом являлось регулирование отношений в сфере авторских и смежных с ними прав, а также прав разработчиков программного и аппаратного обеспечения. Кроме того данные нормативно-правовые акты не только регулировали ряд правоотношений, но и содержали важнейшие понятия и конструкции информационных правоотношений: «программа для ЭВМ», «база данных», «модификации программы» и другие, положивших основу развитию правовой терминологии в данной области[3].

Принятый в июне 1993 года Закон Российской Федерации «О государственной тайне»[4] определил принципы регулирования информационных отношений связанных с обеспечением государственной защиты и безопасности отнеся часть сведений к государственной тайне.

---

[1] Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» (утратил силу) от 23.09.1992 №3523-1 // Российская газета – 20.10.1992 – №229.

[2] Закон РФ «О правовой охране топологий интегральных микросхем» (утратил силу) от 23.09.1992 №3526-1 // Российская газета – 21.10.1992 – №230.

[3] Крылов В.В. Информационные компьютерные преступления. – М., Инфра-М-Норма, 1997. – С.13.

[4] Закон РФ «О государственной тайне» от 21.07.1993 №5485-1 // Российская газета – 21.09.1993 – №189.

Законом «Об обязательном экземпляре документов»[1] внес свою лепту в формирование нормативно-правовой базы, регулирующей информационные отношения общества впервые определив понятие документа.

Гражданский кодекс Российской Федерации[2] (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 определено понятие информационных отношений, включены 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[3] и в ФЗ №98-ФЗ «О коммерческой тайне» от 29.07.2004).

Федеральный закон «Об информации, информатизации и защите информации»[4] принятый в 1995 году, регулировал отношения, возникающие при:

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

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

---

[1] Федеральный закон РФ «Об обязательном экземпляре документов» от 29.12.1994 №77-ФЗ // Российская газета – 17.01.1995 – №11-12.

[2] Гражданский кодекс РФ (часть первая) от 30.11.1994 №51-ФЗ // Российская газета – 08.12.1994 – №238-239.

[3] Гражданский кодекс РФ (часть четвертая) от 18.12.2006 №230-ФЗ // Российская газета – 22.12.2006 – №289.

[4] Федеральный закон РФ «Об информации, информатизации и защите информации» (утратил силу) от 20.02.1995 №24-ФЗ // Российская газета – 22.02.1995 – №39.

Федеральный закон «Об участии в международном информационном обмене»[1] разъяснил условия эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, защиты интересов Российской Федерации и ее субъектов, муниципальных образований при международном информационном обмене, защиту интересов, прав и свобод физических и юридических лиц при международном информационном обмене. Данный закон также несет в себе определения таких понятий 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.[2] «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»[3] обозначил круг полномочий органов государственной власти, юридических и физических лиц в области.

Необходимо отметить Указы Президента РФ, являющиеся одним из источников права в Российской Федерации направленные на регулирование вопросов формирования государственной политики в сфере информатизации и информационного сотрудничества с другими государствами, разработку и реализацию мер по защите информации.

Логическим завершением данной правотворческой деятельности стали изменения, внесенные в уголовный закон России. При разработке этих изменений отечественный законодатель пошел по второму пути, взяв за

[1] Федеральный закон РФ «Об участии в международном информационном обмене» (утратил силу) от 04.07.1996г №85-ФЗ // Российская газета – 11.07.1996 – №129.
[2] Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ // Российская газета – 29.07.2006 – №165.
[3] Федеральный закон РФ «О связи» от 07.07.2003 №126-ФЗ // Российская газета – 10.07.2003 – №135.

основу криминализации новых разновидностей преступлений признак их объекта и находя для него место в уголовно-правовом «дереве объектов»[1]. 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[2].

Отдельно необходимо отметить ежегодно утверждаемую Президентом РФ Доктрину информационной безопасности Российской Федерации[3], определяющую основные направления противодействия угрозам информационной безопасности в России, а также комплекс практических мероприятий по ее обеспечению.

Исходя из того что компьютерные преступления являются трансграничными, на наш взгляд, будет уместно в рамках данной работы рассмотреть уголовные законы (или акты их заменяющие) с целью ознакомления с видами преступных посягательств, наказуемых в странах Западной Европы и в США.

США стали одной из первых стран мира установившей уголовную ответственность за преступления в сфере высоких технологий. Начиная с 1984 года в этой стране был принят ряд нормативно-правовых актов, регулирующих сферу информационных отношений. По результатам такой нормотворческой деятельности уголовному наказанию в США подлежат: компьютерный шпионаж, несанкционированный доступ к информации правительственных ведомств США, воздействие на компьютер, находящийся в исключительном пользовании правительственного ведомства США, мошенничество с использованием компьютера, умышленное или по неосторожности повреждение защищенных компьютеров, мошенничество

[1] Максимов В.Ю. Компьютерные преступления (вирусный аспект). – Ставрополь: Кн. Изво, 1999. – С.27.

[2] Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М., Юрид. лит., 1991. – С.28.

[3] Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 №646 // «Собрание законодательства РФ» – 12.12.2016 – №50. – С.7074.

путем торговли компьютерными паролями, угрозы, вымогательство, шантаж и другие противоправные деяния, совершаемые с использованием ЭВМ, торговля похищенными или поддельными устройствами доступа.

В законодательстве Великобритании гораздо меньше норм уголовно-правового характера в отношении компьютерной информации, при этом оин довольно емкие: умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам; умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам для их последующего использования в противозаконных целях; 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.

В Германии нормы, содержащие ответственность за преступления в сфере компьютерной информации содержатся в различных разделах Особенной части кодекса. К ним относят: шпионаж данных, компьютерное мошенничество, фальсификация данных, имеющих доказательственное значение, обман при помощи ЭВМ при обработке данных, изменение данных, компьютерный саботаж.

Необходимо отметить, что немецкий уголовный закон использует специальный термин – Daten – это данные, которые сохранены или передаются электронным, магнитным или иным, непосредственно визуально не воспринимаемым способом.

Составы компьютерных преступлений сконструированы как квалифицирующие виды простых составов преступлений, имеющих различные объекты посягательств.

Опираясь на рассмотренный выше материал, можно отметить, что в отечественном законодательстве отсутствуют некоторые составы

компьютерных преступлений имеющих место в других государствах, недостаточно внимания уделено понятийному аппарату

Также необходимо отметить, что и в отечественной и в мировой практике до сих пор не дано точного и всеобъемлющего понятия термину «компьютерные преступления». Зарубежные ученые отмечают: «… признано, что дать определение компьютерного преступления чрезвычайно сложно. Не всякое использование компьютерной системы образует состав компьютерного преступления»[1].

Вероятно, данная проблема существует в связи с множественностью и разнообразием объекта и предмета компьютерного посягательства

Также хочется отметить, что большинство ученых-правоведов в своих изысканиях опирается исключительно на достижения уголовно-правовой науки игнорируя при этом достижения в сфере информационных технологий и компьютерной безопасности, что усложняет задачу изучения компьютерных преступлений, поскольку данный вид противоправной деятельности крайне специфичен в отношении субъекта его совершающего.

[1] Панфилова Е.И., Попов А.Н. Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе» // Науч. редактор проф. Волженкин Б.В. – СПб., 1998. – С.9.

2 УГЛОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1 Неправомерный доступ к компьютерной информации

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[1].

Эта статья гарантирует неприкосновенность информации хранящейся в какое-либо компьютерной системе. При этом необходимо отметить, что владельцем вычислительной системы и владельцем информации в ней хранящейся могут быть разные лица (пользователь системы и собственник системы) либо одно лицо одновременно выступающее в качестве пользователя и собственника системы[2].

В данной статье идет речь о защите компьютерной информации принадлежащей любому лицу на законных основаниях. Преступное деяние, за которое наступает ответственность по диспозиции статьи 272 УК РФ, заключается в совершении ряда действий, направленных на получение несанкционированного доступа к компьютерной информации, который может быть реализован в виде проникновения в компьютерную систему или сеть при помощи технических или программных средств используемых для устранения препятствий системной защиты. Кроме того осуществление данного преступления возможно при использовании действующих паролей и других ключей доступа в виде маскировки. Критичным условием квалификации данного преступления является уничтожение или блокирование защищаемой специальными средствами информации. В

[1] Козлов В.Е.Теория и практика борьбы с компьютерной преступностью – М., Горячая линия, Телеком, 2012. – С.13.

[2] Комиссаров В.С. Преступления в сфере компьютерной безопасности: понятие и ответственность // Юридический мир, 2003. – №2. – С.72.

данном контексте под охраняемой информацией понимаются данные, для которых соответствующими нормативно-правовыми актами установлен режим защиты. К таким данным относят сведения, составляющие государственную, коммерческую тайну, персональные данные.[1] Под неправомерным доступом следует понимать доступ не санкционированный действующими правовыми нормами, ограничивающими круг лиц имеющих доступ к охраняемой информации. [2]

К неправомерному доступу также отнесены действия по изменению или устранению ключей защиты или паролей, модификацию программы. Довольно часто встречается ситуация когда лицо, обладающее правом доступа к охраняемой информации использует действующий пароль доступа для проникновения в ЭВМ и завладения информацией без разрешения ее владельца. [3][4]

Статья 272 УК РФ довольно четко описывает объект, объективную сторону, субъект данного преступления. Опираясь на диспозицию данной статьи можно выделить следующие обязательные признаки объективной стороны преступления: копирование информации, приведшее к ее блокированию, модификации или уничтожению. Обязательно наличие причинно-следственной связи между неправомерными действиями в отношении защищаемой информации и наступившими последствиями.

При реализации данной нормы на практике можно столкнуться со сложностями в трактовке такого термина как «неправомерный доступ». Разнятся мнения о том, что же необходимо понимать под несанкционированным доступом. Ряд ученых под неправомерным доступом

---

[1] Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ // Российская газета – 29.07.2006 – №165.

[2] Постатейный Комментарий к Уголовному кодексу РФ / под ред. Наумова А.В. – М., 2015 – С.325.

[3] 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 // [Электронный ресурс]. – Режим доступа: https://rospravosudie.com

[4] 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 // [Электронный ресурс]. – Режим доступа: https://rospravosudie.com

понимает несанкционированные действия лица не имеющего доступа к информации хранящейся на ЭВМ или в вычислительной сети. Ю.А. Красиков определяет неправомерный доступ как доступ к информации при отсутствии соответствующего права и правил защиты информации.

Современный уровень развития компьютерной техники и компьютерных программ столь высок, что может привести к различного рода сбоям в связи с этим необходимо четко разграничивать сбои систем вызванные несанкционированным вторжением и сбои вызванные техническими неполадками разного рода. Разграничить эти два вида сбоев возможно лишь по наличию или отсутствию причинно-следственной связи между сбоем и утратой компьютерной информации или ее блокировкой. Следовательно, если сбой в ЭВМ или сети ЭВМ вызван техническими неполадками не связанными с неправомерными действиями лица привлекать такое лицо к уголовной ответственности недопустимо.

Представляется корректным считать попытку неправомерного проникновения к охраняемой законом информации считать покушением на неправомерный доступ. Соответственно преодоление всех средств программной защиты информации будет являться оконченным преступлением, предусмотренным ст.272 УК РФ.

Как уже упоминалось ранее, данный состав преступления является материальным и осуществляется исключительно в форме действия в результате, которого наступает одно из предусмотренных законодателем последствий в виде уничтожения (удаления) информации без возможности ее восстановления; блокировки информации (ограничение или закрытие доступа непосредственно к данным, либо к системе, в которой эти данные хранятся); внесение изменений в программные продукты, базы данных или отдельные файлы, находящиеся в системе (модификация информации); копирования; нарушения работы ЭВМ или систем ЭВМ[1]

[1] Научно-практический комментарий к УК РФ в двух томах. Т.2. – Новгород, 2011г. – С.134.

Преступление, предусмотренное ст.272 считается оконченным с момента наступления общественно опасных последствий. Причины совершения данного преступления могут быть любыми: корыстные мотивы, проверка собственного профессионализма, месть и др.

Объектом преступного посягательства являются общественные отношения, связанные с безопасностью использования компьютерной информации. [1]

Объективная сторона преступления может быть осуществлена с использование специальных технических или программных средств, действующих учетных данных пользователей, хищения цифровых носителей информации (при условии организации охраны этих носителей).

В качестве предмета преступного посягательства выступает компьютерная информация.

Диспозиция ст.272 УК РФ не содержит в себе указания на форму вины, однако в данном случае с уверенностью можно говорить об умысле (прямом или косвенном). В случае совершения данного состава преступления лицо осознает, что его действия носят неправомерный характер, предвидит или может предвидеть наступления общественно опасных последствий, но при этом допускает их наступление.

Подобной точки зрения в своих трудах придерживается А.А. Толкаченко, противоположную ему позицию занимает С.А. Пашин, полагая, что преступление, предусмотренное ст.272 УК РФ может быть совершено и по неосторожности. В данном случае под неосторожностью автор понимает неверную оценку правонарушителем собственных действие и тех последствий, что они за собой влекут. Данный подход противоречит ст.24 УК РФ, поскольку норма ст.272 УК РФ не предусматривает неосторожных действий. В связи с этим неправомерный доступ к компьютерной информации, содержащий признаки неосторожной формы вины

[1] Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность, 1997. – № 1. – С.8.

преступлением не является. Необходимо отметить, что совершаемые лицом действия не могут соотноситься с неосторожной формой вины поскольку «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»

Следовательно, виновный сознает неправомерность своих действий и их общественную опасность, предвидит последствия и допускает или желает их наступления или относится к возможности их наступления безразлично, что характеризует наличие умысла.

Неправомерный доступ к компьютерной информации - умышленное деяние, поскольку в диспозиции ст.272 УК не указано обратное[1]. 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.[2]

Чаще всего субъектами данных преступлений являются лица, обладающие специфическими знаниями и умениями в сфере компьютерных технологий, подобная профессиональная подготовленность позволяет предвидеть возможные последствия. По общему правилу, ответственность за совершение преступлений, предусмотренных статьей 272 УКРФ наступает с 16 лет, однако часть вторая ст.272 предусматривает наличие специального субъекта, совершившего данное преступление.[3]

---

[1] Постатейный Комментарий к Уголовному кодексу РФ / под ред. Наумова А.В. – М., 2015 – С.330.

[2] Научно-практический комментарий к УК РФ в двух томах. Т.2. – Новгород: – 2011. – С.24.

[3] Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция, 1997. – №10.

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).

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 с момента наступления общественно опасных последствий.

2.2 Создание, использование и распространение вредоносных программ для ЭВМ

Ответственность за создание различного вредоносного программного обеспечения предусмотрена статьей 273 УК РФ. Использование и распространение в данном контексте следует понимать как размещение этих программных продуктов в памяти вычислительной машины, а также как

продажу, обмен, дарение или безвозмездную передачу другим лицам. [1] Норма, содержащаяся в данной статье, направлена на защиту прав и законных интересов владельцев аппаратного обеспечения, а также на целостность информации, находящейся в «атакуемой» ЭВМ, системе или сети. Комплексность данного подхода необходима в связи с разнообразием вредоносного программного обеспечения (одни виды «вирусов» направлены на организацию сбоев аппаратного обеспечения, другие – на уничтожение или блокирование информации)[2].

Законодатель под вредоносным программным обеспечением понимает программы, созданные специально для нарушения режима нормального функционирования как аппаратного, так и программного обеспечения. При этом под нормальным функционированием следует понимать процессы включенные разработчиком программного обеспечения в его непосредственный функционал.

По мнению ряда исследователей наиболее распространенными видами вредоносных программ являются «компьютерные вирусы» и «логические бомбы»[3].

Под компьютерными вирусами чаще всего понимается программный продукт, обладающий функциями к самокопированию (клонированию), собственному видоизменению (мутации) направленному на сокрытие вируса от систем безопасности устройства, модификации программы-компаньона («зараженный» программный продукт совместно с которым вирус проникает в «заражаемую» систему).

«Логическая бомба» - это программный код, действие которого направлено прежде всего на вывод «заражаемой» системы из строя при

---

[1] Маслакова Е. А. История правового регулирования уголовной ответственности за компьютерные преступления // Информационное право. – 2006. – № 4. – С.408.

[2] Безруков Н.А. Введение в компьютерную вирусологию. Общие принципы функционирования, классификация и каталог наиболее распространенных вирусов в MS DOS – Киев, 2006. – С.86.

[3] Барсуков В.С., Водолазский В.В. Современные технологии безопасности – М., Нолидж, 2000. – С.64.

наступлении каких-либо условий (или наоборот – отсутствии некоторого условия). «Логическая бомба» статична по своей структуре, в ней отсутствует код, отвечающий за самокопирование и видоизменение.

Последствия деятельности вредоносного программного обеспечения разнообразны по своей сути и по объему причиняемого ущерба. Самые примитивные вирусы занимают все свободное пространство на носители информации, при этом вред имеющейся информации или аппаратному обеспечению не причиняется. О возможностях других же остается только размышлять. Яркий тому пример компьютерная атака 12.05.2017 года в результате которой была нарушена деятельность различных систем и сетей в 74 странах мира. Среди «пострадавших» есть госпитали, компании предоставляющие услуги мобильной связи, министерства.[1] В вязи с этим будет корректно согласиться с мнением законодателя, посчитавшего данный состав самым опасным из компьютерных преступлений, что нашло свое отражение в санкции ст.273 УК РФ.

Состав данного преступления (по части 1) является усеченным по признаку «создания программ для ЭВМ или внесения изменений в существующие программы»

Безопасные общественные отношения, связанные с использованием ЭВМ, программного обеспечения являются непосредственным объектом данного преступления.

Часть 1 ст.273 представляет собой формальный состав, характеризующийся закрытым перечнем совершаемых действий. К этим действиям законодатель относит создание программ, внесение изменений обладающих схожими функциями в готовые программные продукты, распространением вредоносных программ, использование носителей, содержащих такие программы, распространение этих носителей.

[1] Хакерская атака мирового масштаба // Газета.Ру [Электронный ресурс]. – Режим – https://www.gazeta.ru/social/2017/05/12/10671101.shtml

В связи с тем что состав данной статьи формальный для возникновения уголовной ответственности не требуется наступления общественно-опасных последствий[1].

Разработка вредоносного программного продукта проходит те же этапы технологического процесса, что и любая другая программа. Это осознанная, волевая деятельность, включающая в себя:

1) постановку и разъяснение задачи,
2) выбор средств программирования (языка или среды программирования),
3) разработку и написание программного кода,
4) тестирование и отладку программного продукта в лабораторных условиях, в условиях приближенных к реальным.

В.В. Крылов, включает в этот перечень еще и «запуск и непосредственное действие программы (выпуск в свет), предоставление информации». На наш взгляд, данная точка зрения далека от действительности и противоречит мнению ученых сформировавшемуся в 70-х годах XX века. Ряд исследователей склонен считать, что выполнение любого из технологических этапов написания вредоносного программного продукта можно считать преступлением, предусмотренным частью 1 ст.273, что представляется корректным, поскольку термин «создание» представляет собой целостный процесс, включающий все этапы разработки программы.

Из деятельности, подпадающей под состав преступления, содержащийся в ст.273 есть правомерное исключение – деятельность лицензированных организаций, направленная на создание средств защиты от вредоносных программ. Спорной как в отечественной, так и в мировой практике остается деятельность частных лиц, нанятых пострадавшими от вирусной атаки компаниями, направленная на поиск и устранение «брешей» в системе безопасности.

[1]Комментарий к Уголовному кодексу Российской Федерации. Научно-практический комментарий / Отв.ред. Лебедев В.М. – М., Юрайт-М, 2004. – С.560.

В юридической науке можно наблюдать несколько подходов в определении субъективной стороны данных преступлений.

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. А. Пашин трактует это следующим образом: «создание, использование 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».

Все они говорят о том, что преступление предусмотренное ст.273 может быть совершено только с прямым умыслом, причем данные преступления считаются оконченными с момента совершения действий, направленных на создание или использование вредоносных программ не зависимо от того наступили ли общественно опасные последствия.

В рассматриваемых составах прямой умысле представляет собой такое состояние субъекта преступления при котором ему достоверно известно, что программный продукт им созданных, распространенный или используемый является вредоносным, предвидел возможность наступления негативных последствий, и не смотря на это продолжал действия по созданию, либо использованию, либо распространению вредоносного программного продукта.

При анализе данного состава преступления необходимо обратиться к ч.2 ст.72 УК РФ, говорящей о том, что деяние признается совершенным по неосторожности, лишь в том случае, когда это оговорено соответствующей нормой УК РФ. Это подтверждает нашу точку зрения касательно того, что

преступления предусмотренные ст.273 УК РФ совершаются исключительно с формой вины в виде прямого умысла.

Для объективной стороны ч.1 ст.273 необходимо наличие двух признаков: наличие вредоносной программы или изменений в программе, несанкционированность последствий.

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[1]. 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.

[1]Батурин Ю.М. Проблемы компьютерного права – М., Юридическая литература, 1998. – С.14.

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.[1] Причем создание программ для

[1] 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 // [Электронный ресурс]. – Режим доступа: https://rospravosudie.com

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[1]. Последнее из указанных преступлений предполагает совершение хотя бы одного из следующий действий:

- создание вредоносной программы (вредоносных программ) для ЭВМ;
- внесение изменений в существующие программы для ЭВМ, доводя их до качества вредоносных;
- использование вредоносных программ для ЭВМ;
- использование машинных носителей, содержащих вредоносные программы;

[1] Карелина М.М. Преступления в сфере компьютерной информации – М., 1998. – С.12.

– распространение машинных носителей, содержащих вредоносных программ;
– 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[1].

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

[1] Комментарий к уголовному кодексу РФ. Научно-практический комментарий / Отв.ред. Лебедев В.М. – М., Юрайт-М, 2004. – С.560.

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 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Компьютерные системы и сети прочно и повсеместно вошли в жизнь каждого современного человека. Выход из строя одной из таких систем может, в конечном счете, привести к трагедии в связи с этим законодатель

уделил особое внимание безопасности ЭВМ, систем ЭВМ или их сетей, установив уголовную ответственность за нарушение правил их эксплуатации. Данный состав преступления размещен в ст. 274 УК РФ. Данная статья оберегает системы и сети ЭВМ не только от стороннего посягательства, но и от невыполнения пользователями этих систем своих должностных обязанностей. Необходимо уточнить, что уголовная ответственность за данное преступление наступает лишь в том случае, когда ЭВМ, системе ЭВМ или их сети причинен существенный вред. Уголовно-правовая норма, содержащаяся в данной статье не устанавливает конкретных технических требований, а лишь отсылает к соответствующим нормативным актам, содержащим правила и порядок эксплуатации. Требования по эксплуатации ЭВМ, их систем и сетей доводятся до сведения конечного пользователя лицом, управомоченным на это. Действие данной статьи распространяется на системы и сети различных организаций[1] и не распространяется на системы и сети общего доступа, такие как Internet, поскольку не существует нормативных актов регламентирующих порядок работы в сети и конечный круг пользователей в данном случае совершенно не определен.

В данном случае под охраняемой законом информацией необходимо понимать лишь те данные для которых специальными законами установлен специальный режим их правовой защиты (это различные виды тайн, персональные данные). [2]

В соответствии со строением данного состава преступления требуется чтобы между фактом нарушения правил эксплуатации и наступившими последствиями в виде существенного вреда была обязательно установлена причинно-следственная связь и было доказано, что причиненный вред полностью является результатом именно нарушения правил эксплуатации, а не последствием какого-либо сбоя или несанкционированного доступа.

---

[1] Комментарий к уголовному кодексу РФ. Научно-практический комментарий / Отв.ред. Лебедев В.М. – М., Юрайт-М, 2004. – С.560.

[2] Федеральный закон РФ «Об информации, информатизации и защите информации» от 20.02.1995 №24-ФЗ // Российская газета – 22.02.1995 – №39.

Соблюдение правил эксплуатации конкретного аппаратно-технического комплекса является непосредственным объектом преступлений данного вида.

К правилам эксплуатации можно отнести общие санитарно-гигиенические нормы, правила внутреннего трудового распорядка работников вычислительных центров, техническая документация, поставляемая в комплекте с приобретаемым оборудованием. Не надлежащее соблюдение или несоблюдение правил эксплуатации технических средств может быть осуществлено как путем бездействия, так и путем совершения активных действий.

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

- уничтожения, блокирования или модификации охраняемой законом информации ЭВМ;
- 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[1].

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.

---

[1] Яблоков Н.П. Криминалистическая характеристика преступлений // Вестник Московского университета. Серия 11, Право. – 1999 – № 1 – С.58.

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) Наступлением 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[1].

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

[1] Кузнецов А.В.Некоторые вопросы расследования преступлений в сфере компьютерной информации // Информационный бюллетень следственного комитета МВД РФ

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 компьютерных преступлений.

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»[1]. 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

[1] Кузнецова Н.Ф. Квалификация сложных составов преступлений // Уголовное право. – 2000. – № 1. – С. 26.

говорить о квалификации по совокупности; другие отстаивают иную точку зрения[1]. 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

[1] Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. – 1997. – № 1. – С.19.

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:

- вносят искажения, неправильные (фальсифицированные) данные в программные выходные данные ЭВМ с последующим их использованием для хищений;
- устанавливают код компьютерного проникновения в электронную платежную сеть расчетов по карточкам;
- 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[1]. 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[2]. 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

---

[1] Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. – 1999. – № 1. – С. 44-45.

[2] Завидов Б.Д. О понятии мошенничества и его модификациях (видоизменениях) в уголовном праве // Право и экономика. – 1998. – № 11. – С. 50-51.

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.

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

Информатизация современного общества – один из наиболее значимых процессов современности требующий особого внимания со стороны законодателя и правоприменителя в силу своей многогранности и сложности. Отечественный законодатель заложил основы правового регулирования данной сферы общественных отношений в 1992 году. В регулировании информационных правоотношений, как и в любом другом новом, развивающемся направлении деятельности, есть много неразрешенных противоречий, неточностей и проблем о чем красноречиво говорит разночтение одного из основных терминов – «информация» а также отсутствие официального трактования таких понятий как «ЭВМ», «система ЭВМ», «сеть ЭВМ» и др. В Уголовном законе обнаруживается также непоследовательность в составах компьютерных преступлениях, например, если речь идет о нарушении правил эксплуатации ЭВМ, систем ЭВМ и их сетей, в то необходимо отметить, что результатом такого преступления может быть не только уничтожение, блокировка, модификация информации, но и причинение ущерба в связи нарушением функционирования ЭВМ, системы или сети.

На наш взгляд необходимо более детальное и всестороннее регулирование правоотношений, связанных со взаимодействием в сети Internet. Это вызвано, прежде всего, особенностями данной сети: анонимностью пользователей, фактическим отсутствием владельца, трансграничностью, отсутствием ограничений. Данные особенности сети делают ее конечного пользователя (гражданина любого государства) беззащитным перед массой правонарушителей, переместивших свою противоправную деятельность из реальной жизни в виртуальный мир.

Кроме осуществления в виртуальном мире различных видов преступной деятельности, сеть является бескрайней площадкой для формирования общественного мнения, воздействия на моральные установки пользователей

и других видов психологических манипуляций. Фактически оба эти аспекта не регламентированы и не подвергаются регулированию со стороны государства.

Также необходимо уделить внимание доработке существующей нормативно-правовой базы, поскольку информационные технологии развиваются крайне быстро и правовые нормы в связи с этим «морально устаревают», т.е. становятся далекими от фактических обстоятельств, от практики. Особое внимание при этом необходимо уделить установлению, пусть даже минимального, но соответствия юридических формулировок и технической терминологии. Разрешение данного затруднения позволит повысить уровень правовой грамотности тех граждан, которые в силу своих профессиональных навыков могут стать субъектами компьютерных преступлений.

Анализ правоприменительной практики красноречиво говорит о проблемах в данной сфере, возникших вследствие низкой компетентности в сфере информационных технологий. Результатом этого является применение закона по аналогии, что недопустимо, неверная квалификация правонарушений и как следствие – снижение авторитета государства в лице правоохранительных органов и судебной системы.

В связи с чем, по нашему мнению, требуется осуществить следующие организационные и правовые меры:

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

Преступления в сфере компьютерной информации, на наш взгляд, наиболее труднодоказуемые из всех, особенно это обстоятельство характеризует взлом удаленных компьютеров, являющихся частью вычислительных систем. На сегодняшний день фактическая возможность доказательства такого преступления рядовым следователем равна нулю. Особенно это касается тех случаев, когда потерпевшими являются обычные люди, а не крупные компании или люди публичные.

Условно все компьютерные преступления можно поделить на две группы: преступления, в которых ЭВМ участвует в качестве средства совершения преступления, и преступления составом которых предусмотрено преступное посягательство на работу ЭВМ. В главе 28 УК РФ нашли свое место лишь преступления, относящиеся ко 2 группе. Это обусловлено исключительно объектом преступления, а именно информацией, хранящейся в памяти компьютера. Обе эти категории преступлений отличаются высокой латентностью как результатом анонимности пользователей сети и практически ничем не ограниченным простором для разнородной деятельности. На данном этапе своего развития «компьютерная преступность» характеризуется не единичными действиями, а организованностью, слаженностью действий направленных преимущественно на деятельность крупных компаний или учреждений.

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

Раздел 1 Нормативно-правовые акты и иные официальные акты

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 – 08.12.1994 – №238-239.
4. Гражданский кодекс РФ (часть четвертая) от 18.12.2006 №230-ФЗ // Российская газета – 22.12.2006 – №289.
5. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ // Собрание законодательства РФ – 17.06.1996.
6. Закон РФ «О государственной тайне» от 21.07.1993 №5485-1 // Российская газета – 21.09.1993 – №189.
7. Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.1992 №3523-1 // Российская газета – 20.10.1992 – №229.
8. Закон РФ «О правовой охране топологий интегральных микросхем» от 23.09.1992 №3526-1 // Российская газета – 21.10.1992 – №230.
9. Федеральный закон РФ «О связи» от 07.07.2003 №126-ФЗ // Российская газета – 10.07.2003 – №135.
10. Федеральный закон РФ «Об информации, информатизации и защите информации» от 20.02.1995 №24-ФЗ // Российская газета – 22.02.1995 – №39.
11. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ // Российская газета – 29.07.2006 – №165.

12. Федеральный закон РФ «Об обязательном экземпляре документов» от 29.12.1994 №77-ФЗ // Российская газета – 17.01.1995 – №11-12.
13. Федеральный закон РФ «Об участии в международном информационном обмене» (утратил силу) от 04.07.1996г №85-ФЗ // Российская газета – 11.07.1996 – №129.
14. Указ Президента РФ от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // «Собрание законодательства РФ» – 12.12.2016 – №50. – С.7074.

Раздел 2 Литература

15. Абдеев Р.Ф. Философия информационной цивилизации. – М. Слово, 1994. – С. 33.
16. Барсуков В.С., Водолазский В.В. Современные технологии безопасности – М., Нолидж, 2000. – С.64.
17. Батурин Ю.М. Проблемы компьютерного права – М., Юридическая литература, 1998. – С.14.
18. Безруков Н.А. Введение в компьютерную вирусологию. Общие принципы функционирования, классификация и каталог наиболее распространенных вирусов в MS DOS – Киев, 2006. – С.86.
19. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. – М. Юринформ, 2005. – С.11.
20. Главный информационно-аналитический центр МВД России. Состояние преступности в России за январь – декабрь 1997-2000, 2014-2017 [Электронный ресурс]. – Режим доступа: https://мвд.рф/Deljatelnost/statistics.
21. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция, 1997, – №10.
22. Гуров А.И. Криминогенная ситуация в России на рубеже XXI века. – М., 2000. – С.36-37.

23. Завидов Б.Д. О понятии мошенничества и его модификациях (видоизменениях) в уголовном праве // Право и экономика, 1998. – №11. – С.50-51.
24. Зеленский В.Д. Основы компьютеризации расследования. – Краснодар, 1998. – С.4.
25. Карелина М.М. Преступления в сфере компьютерной информации – М., 1998. – С.12.
26. Карпинский О. Защита информации, виртуальные частные сети (VPN). Технология ViPNet / По материалам компании Infotecs // Gazeta.Ru. – 18.06.2001.
27. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью – М., Горячая линия, Телеком, 2012. – С.13.
28. Комиссаров В.С. Преступления в сфере компьютерной безопасности: понятие и ответственность // Юридический мир, 2003. – №2. – С.72.
29. Комментарий к уголовному кодексу РФ. Научно-практический комментарий / Отв.ред. В.М.Лебедев. – М., Юрайт-М, 2004. – С.560.
30. Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция, 1999. – № 1. – С.44-45.
31. Крылов В.В. Информационные компьютерные преступления. – М., Инфра-М-Норма, 1997. – С.13.
32. Крылов В.В. Основы криминологической теории расследования преступлений в сфере информации. Автореф. дис.... канд. юрид. наук, – М., 1997. – С.11.
33. Кузнецов А.В. Некоторые вопросы расследования преступлений в сфере компьютерной информации // Информационный бюллетень следственного комитета МВД РФ.
34. Кузнецова Н.Ф. Квалификация сложных составов преступлений // Уголовное право. – М., 2000. – № 1. – С.26.

35. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность, 1997. – № 1. – С.19.
36. Максимов В.Ю. Компьютерные преступления (вирусный аспект). – Ставрополь: Кн. Из-во, 1999. – С.27.
37. Маслакова Е.А. История правового регулирования уголовной ответственности за компьютерные преступления // Информационное право, 2006. – №4. – С.408.
38. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. – Воронеж, 2001. – С.25.
39. Научно-практический комментарий к УК РФ в двух томах. – Т.2.Новгород, 2011г. – С.134.
40. Ожегов С.И. Словарь русского языка. – М. Наука, 1989. – С.222.
41. Панфилова Е.И., Попов А.Н. Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе» // Науч. редактор проф. Волженкин Б.В. – СПб., 1998. – С.9.
42. Погуляев В., Теренин А. Обеспечение конфиденциальности // эж-ЮРИСТ, 2004 – №2. – С.34.
43. Постатейный Комментарий к Уголовному кодексу РФ / под ред. Наумова А.В. – М., 2015 – С.325.
44. Сальников В.П. Компьютерная преступность: уголовно-правовые и криминологические проблемы //Государство и право, 2000. – № 9. – С.101.
45. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации. Дис… канд. юрид. наук. – М., 1999. – С.32.
46. Талимончик В.П. Компьютерные преступления и новые проблемы сотрудничества государств //Законодательство и экономика, 2005. – №5. – С.14.
47. Уголовное право Российской Федерации. Особенная часть/ Под ред. Здравомыслова Б.В. – М, БЕК, 2000. – С.353.

48. Хакерская атака мирового масштаба // Газета.Ру [Электронный ресурс]. – Режим доступа – https://www.gazeta.ru/social/2017/05/12/10671101.shtml
49. Харкевич А.А. О ценности информации // Проблемы кибернетики, 1961. – № 4 – С.31.
50. Шершнев Л.И. Безопасность человека. Учебно-методическое пособие, – М., Фонд национальной и международной безопасности, 1994. – С.33-35.
51. Шумилов Н.И. Криминалистические аспекты информационной безопасности. Автореф. дис... канд. юрид. наук, – СПб, 1997. – С.20.
52. Яблоков Н.П. Криминалистическая характеристика преступлений // Вестник Московского университета. Серия 11, Право, 1999 – №1 – С.58.

Раздел 3 Постановления высших судебных инстанций и материалы судебной практики

53. 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 //[Электронный ресурс]. – Режим доступа: https://rospravosudie.com
54. Уголовное дело №1-21/2017 по обвинению Маликова К.О. по ч.1 ст.273 УК РФ // [Электронный ресурс]. – Режим доступа: https://rospravosudie.com
55. 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 // [Электронный ресурс]. – Режим доступа: https://rospravosudie.com