Содержание:

Введение.

В настоящее время, как в нашей стране, так и за рубежом идет бурный процесс компьютеризации управленческой, научно-технической и иных сложных видов деятельности человека. Компьютерная техника широко используется в вооруженных силах страны, в атомной и иных видах энергетики, в космических исследованиях и других сферах жизнедеятельности людей. Персональные компьютеры все чаще становятся жизненно важным средством, облегчающим и убыстряющим процессы умственного и физического труда, хранителем разнообразной информации, необходимой для принятия правильных управленческих и иных решений.

Актуальность этой темы состоит в том, что, как показала отечественная и зарубежная практика использования компьютеров, они могут успешно использоваться не только в общественно полезных интересах личности, общества и государства, но и в преступных целях, быть средством совершения различных преступлений в сфере экономики, обороны страны. Специалисты в области компьютерной техники могут незаконно вмешиваться в созданные компьютерные программы, системы ЭВМ и их сети, вносить в информацию на машинном носителе изменения и дополнения, разрушать либо повреждать магнитоносители и тем самым создавать помехи в получении достоверной информации по тому или иному вопросу либо проблеме. Такого рода действия могут приводить к рассекречиванию государственных, военных либо коммерческих тайн и использованию их в ущерб экономической безопасности или обороноспособности страны, в конкурентной борьбе предпринимательских структур, а равно в иных противоправных целях.

Целью данной курсовой работы является комплексное изучение вопросов, которое позволит узнать, что понимается под компьютерным преступлением, компьютерной информацией и другими терминами, связанными с ними и необходимые для лучшего понимания данной темы.

Цель работы заключается в том, чтобы узнать, что понимается под компьютерными преступлениями, провести анализ преступлений в сфере компьютерной информации.

Реализация поставленной цели осуществляется путем решения следующих задач:

- изучить, что понимается под компьютерным преступлением;

- рассмотреть виды преступлений, закрепленные в Уголовном кодексе Российской Федерации;

- привести примеры по каждому из видов преступлений из судебной практики.

Объектом настоящей курсовой работы является общественные отношения, возникающие в результате совершения преступлений в сфере компьютерной информации. Предметом исследования являются нормативно-правовая база, научная и учебная литература, материалы судебно-следственной практики, статистические данные, с помощью которых необходимо раскрыть понятие и виды компьютерных преступлений.

§1. Понятие им виды компьютерных преступлений.

§1.1 Понятие компьютерных преступлений.

Этим и объясняется то, что в УК 1996 г. предусмотрена специальная гл. 28, посвященная преступлениям в сфере компьютерной информации.

В этой главе УК пока предусматривается всего три состава преступлений: неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

В развитых в экономическом и техническом отношении зарубежных странах компьютерная преступность получила широкое распространение. По некоторым экспертным оценкам ежегодный ущерб от компьютерных преступлений достигает примерно пяти миллиардов долларов. Одним из первых преступлений, совершенных в нашей стране с использованием компьютера, было хищение денежных средств на сумму 78 584 руб (в Вильнюсе).

Впервые о проблемах борьбы с компьютерной преступностью в России было официально заявлено лишь в 1992 году, а глава «Преступления в сфере компьютерной информации», включающая три статьи появилась в Уголовном кодексе РФ только в 1997 году. Например, в Швеции несанкционированное получение компьютерных данных было объявлено преступлением еще в 1973 году. Первое подразделение «по борьбе с хищениями, совершаемыми с использованием электронных средств доступа» при Главном управлении по экономическим преступлениям МВД РФ, насчитывало четыре человека, появилось только в 1997 году. С 1 января 1997 года вводится в действие новый Уголовный Кодекс Российской Федерации, принятый Государственной думой 24 мая 1996 года. Впервые в российском уголовном законодательстве введено понятие «компьютерные преступления».

Что такое компьютерное преступление и в чем оно состоит? Четко ответить на этот вопрос весьма непросто, так как границы подобной деятельности никем еще однозначно не определены, нет полной ясности относительно параметров и критериев, по которым следует выделять и фиксировать компьютерные преступления и попытки их совершить. И все-таки законодательства многих стран сходятся в том, что компьютерное преступление, в самой его общей формулировке, есть любое противозаконное действие, объектом посягательства которого является информация, обрабатываемая в компьютерной системе, а орудием посягательства служит компьютер. Другими словами, в большинстве случаев компьютерные преступления представляют собой давно известные, традиционные виды преступлений, но совершаемые новыми орудиями и в новой среде.

Компьютерные преступления считаются очень опасными. Это вызвано следующими причинами:

- Такие преступления еще недостаточно широко известны, поскольку они появились в конце 60-х годов, а обратили на себя внимание и вовсе недавно, в начале 90-х.

- Их сложно выявить, так как современные средства их обнаружения малоэффективны. К примеру, в эксперименте по проникновению в свою же компьютерную сеть, проведенном одной из американских правительственных организаций, из всех успешных «взломов» удалось выявить лишь 4. Так, по данным одного из опросов, свыше 70% пользователей сетей в США не имеют устройств, предупреждающих о вторжении в их коммуникационные и информационные системы.

- Компьютерные преступления сложно предотвратить, поскольку средства и методы защиты постоянно отстают от средств и методов нападения.

- Компьютерные преступления совершаются в глобальном масштабе, преступники действуют на большом удалении, проследить их крайне сложно, поскольку они часто прикрываются чужим именем, и след их, если таковой остается, чрезвычайно запутан.

- Компьютерная преступность повсеместно принимает организованный характер.

- Наказать выявленного преступника не всегда представляется возможным: пользуясь несогласованностью правовых баз различных государств, преступник может совершать "взломы" из страны, где подобная деятельность не является противозаконной.

- Нейтрализовать последствия компьютерных преступлений чрезвычайно сложно.

Ввиду малочисленности составов преступлений в сфере компьютерной информации попытки классифицировать эти преступления представляются пока преждевременными, хотя некоторые рекомендации по этому вопросу уже имеются. В литературе, например, предлагается подразделять компьютерные преступления на две группы: преступления, связанные с вмешательством в работу компьютеров, и преступные деяния, при которых компьютеры используются как технические средства совершения преступления.[1]

Глава 28 Уголовного кодекса Российской Федерации содержит совершенно новые для отечественного уголовного права нормы. Перечисленные в ней деянияраньше либо вовсе не рассматривались как преступные деяния и в лучшем случае влекли гражданско-правовую ответственность, либо квалифицировались по статьям Уголовного кодекса о нарушении авторского права, шпионаже, разглашении тайны, а при наличии материального ущерба рассматривались как способы хищения, уничтожения или повреждения имущества.

В развитых странах компьютерная преступность дает доходы, уступающие разве что получаемым от оборота наркотиков и азартных игр. Термин «компьютерная преступность» впервые появился в американской, а затем другой зарубежной печати в начале 60-х годов. Позже аналитики сошлись во мнении, что под этим стоит подразумевать любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку и (или) передачу данных.

Первым зафиксированным в России компьютерным преступлением было происшествие, случившееся в августе 1983 г. на Волжском автомобильном заводе в Тольятти, где программист из мести администрации внес изменения в программу ЭВМ, обеспечивающую работу автоматической системы подачи механических узлов на главный сборочный конвейер; в итоге 200 легковых машин не сошло вовремя с конвейера и заводу был причинен ущерб в 1 млн. рублей. Программист был осужден по ч. 2 ст. 98 УК РСФСР (повреждение государственного имущества, причинившее крупный ущерб) к 3 годам лишения свободы условно с взысканием ущерба.

Выделение преступлений в сфере компьютерной информации как особого вида правонарушений связано не только со все большим распространением таких деяний, но и с тем, что в данном случае речь идет об особом предмете посягательства — компьютерной информации .[2]

Научно-техническая революция повлекла за собой серьезные социальные изменения, наиболее важным из которых является появление нового вида общественных отношений и общественных ресурсов — информационных . Информация стала первоосновой жизни современного общества, предметом и продуктом его деятельности, а процесс ее создания, накопления, хранения, передачи и обработки в свою очередь стимулировал прогресс в области орудий ее производства: электронно-вычислительной техники (ЭВТ), средств телекоммуникаций и систем связи.

Информация становится продуктом общественных отношений, начинает приобретать товарные черты и становится предметом купли-продажи. Следствием протекающих в обществе информационных процессов является возникновение и формирование новых социальных отношений, и изменение уже существующих. Например, уже сейчас можно констатировать значительный объем договорных отношений, связанных с изготовлением, передачей, накоплением и использованием информации в различных ее формах: научно-технической документации, программного обеспечения ЭВТ, баз данных, систем управления базами данных (СУБД) и др.

Появление на рынке в 1974 г оду компактных и сравнительно недорогих персональных компьютеров дали возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контролируемости доступа к информации, ее сохранности и доброкачественности. Организационные меры, а также программные и технические средства защиты

оказались недостаточно эффективными.

Особенно остро проблема несанкционированного вмешательства дала о себе знать в странах с высокоразвитыми технологиями и информационными сетями. Вынужденные прибегать к дополнительным мерам безопасности, они стали активно использовать правовые, в том числе уголовно-правовые средства защиты. Так, Уголовный кодекс Франции (1992 г.) пополнил систему преступлений против собственности специальной главой «О посягательствах на системы автоматизированной обработки данных», где предусмотрена ответственность за незаконный доступ ко всей или части системы автоматизированной обработки данных, воспрепятствование работе или нарушение правильности работы такой системы или ввод в нее обманным способом информации, уничтожение или изменение базы данных. Не остались в стороне от этой проблемы и международные организации, в частности Совет Европы, который счел необходимым изучить и разработать проект специальной конвенции, посвященной проблеме правонарушений в сфере компьютерной информации.

Российские правоведы уже давно ставили вопрос о необходимости законодательного закрепления правоотношений, вытекающих из различных сфер применения средств автоматической обработки информации. Определенным этапом на пути реализации этих пожеланий стало принятие в 1992 г. Закона РФ «О правовой охране программ для электронно-вычислительных машин и баз данных». Закон содержал положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких произведений влечет уголовную ответственность. Однако соответствующих изменений в УК РСФСР так и не было внесено.

В 1994 году был принят Гражданский кодекс, который содержит ряд норм, связанных с компьютерной информацией, в 1995 году - Федеральный закон «Об информации, информатизации и защите информации». Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стала разработка в УК РФ 1996 года группы статей, предусматривающих основания уголовной ответственности за так называемые компьютерные преступления.

Компьютерная информация - в соответствии со ст.2 закона «Об информации, информатизации и защите информации» под информацией понимаются - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, но применительно к комментируемым статьям под компьютерной информацией понимаются не сами сведения, а форма их

представления в машиночитаемом виде, т.е. совокупность символов зафиксированная в памяти компьютера, либо на машинном носителе (дискете, оптическом, магнитооптическом диске, магнитной ленте либо ином материальном носителе). При рассмотрении дел следует учитывать, что при определенных условиях и физические поля могут являться носителями информации.

Программа для ЭВМ - объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения; ЭВМ (компьютер) - устройство или система (несколько объединенных устройств) предназначенное для ввода, обработки и вывода информации.

Сеть ЭВМ - совокупность компьютеров, средств и каналов связи, позволяющая использовать информационные и вычислительные ресурсы каждого компьютера включенного в сеть независимо от его места нахождения.

База данных - это объективная форма представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Быстрый количественный рост преступности и ее качественные изменения, обусловленные обострением противоречий в различных областях общественной жизни, частой реорганизацией системы правоохранительных органов, несовершенство законодательства и частое его изменение, серьезные упущения в правоприменительной практике, способствуют ускорению процессов развития компьютерной преступности как социального явления.

Специалистами прогнозируется рост организованной преступности, связанной с использованием электронных средств, одним из которых является компьютер. По данным ФБР США российским специалистам – компьютерщикам, входящим в состав отечественных преступных групп, осуществляющих свою преступную деятельность на территории США и обладающих достаточным финансовым и кадровым потенциалом, в настоящее время не составляет особого труда «взломать» почти любые коды и получить доступ к коммерческим секретам многонациональных корпораций. В результате чего с использованием компьютерной технологии как в России, так и за рубежом совершаются банковские транзакции, при которых десятки миллионов долларов в считанные минуты незаконно снимаются со счетов

корпораций и переводятся на оффшорные счета, используемые преступниками. Согласно оценкам специалистов ежемесячно совершается около тысячи подобных «операций», проследить за которыми ни ФБР, ни другие спецслужбы пока не в состоянии.

Отсутствие четкого определения компьютерной преступности, единого понимания сущности этого явления значительно затрудняют определение задач правоприменительных органов в выработке единой стратегии борьбы с ней.

Компьютерные преступления условно можно подразделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства. Есть точка зрения, в рамках которой к « компьютерным преступлениям » относятся все противоправные деяния, так или иначе связанные с компьютерной техникой.[3] . Исходя из подобного определения, можно сделать вывод, что для квалификации не важно, в качестве чего задействована в правонарушении названная техника: объекта, предмета, орудия или средства; что именно страдает в итоге данного деяния: аппаратная часть, программное обеспечение, база данных; кто конкретно из соучастников и каким образом использовал ЭВМ. При таком понимании термина, по мнению М.В.Богомолова уравниваются юридические последствия следующих деяний:

1.незаконное копирование авторского программного продукта;

2. блокирование компьютерной системы Министерства обороны с целью подрыва обороноспособности страны;

3.кража принтера и убийство путем нанесения удара данным принтером по голове потерпевшего. Данные деяния можно квалифицировать и по другим составам преступлений, описанным в УК РФ, отпадает необходимость отнесения этих преступлений к компьютерным.

Рассмотрим определение, предложенное В.Б. Вехов ым: компьютерные преступления - предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства.[4] В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть. С вышеназванной точкой зрения согласились криминалисты, поскольку подобная трактовка понятия является весьма ясной, нет необходимости разграничивать вышеназванные понятия.

Компьютерные преступления - предусмотренные уголовным законом общественно опасные действия, совершенные с использованием средств электронно-вычислительной (компьютерной) техники.[5] Но М.В. Богомолов также критикует и это определение, поскольку оно слишком широко трактует рассматриваемое понятие. К таким преступлениям можно отнести, руководствуясь трактовкой Вехова, оплату покупки при помощи поддельной пластиковой кредитной карточки («компьютерное мошенничество») или незаконный перевод денежной суммы с одного счета в банке на другой («компьютерная кража»), несанкционированный сбор информации с целью использования ее для ослабления какой-либо организации или даже государства («компьютерный шпионаж»), которые практически не отличаются от мошенничества, кражи и шпионажа. Отличает их лишь использование в той или иной степени компьютерной техники при совершении преступления. Поэтому в этом случае также нет необходимости введения норм, которые регулируют компьютерные преступления. На квалификацию кражи, к примеру, не будет влиять, совершена она при помощи отмычки, куска провода или же персонального компьютера. С уголовно-правовой точки зрения эти орудия и средства совершенно равноценны и их фактическое своеобразие может быть только учтено судом при индивидуализации наказания во время вынесения обвинительного приговора. С этим согласен и профессор С.В. Бородин: «В тех случаях, когда компьютерная аппаратура является предметом преступления против собственности, соответственно ее хищение, уничтожение или повреждение подлежит квалификации по ст.ст. 158-168 УК РФ. Но дело в том, что информационная структура не может быть предметом преступления против собственности, поскольку машинная информация не отвечает ни одному из основных критериев предмета преступления против собственности, в частности не обладает физическим признаком. Что касается компьютера как орудия преступления, то его следует рассматривать в ряду таких средств, как оружие или транспортные средства. В этом смысле использования компьютера имеет прикладное значение при совершении преступлений, например хищения денежных средств или сокрытие налогов. Такие действия не рассматриваться в качестве самостоятельных преступлений, а подлежат квалификации по другим статьям УК в соответствии с объектом посягательства». [6]. Но в некоторых странах Европы и Америки именно это определение используется для квалификации преступления в качестве компьютерного.

Ряд авторов еще более сужают круг компьютерных преступлений , оставляя только те, которые посягают непосредственно на компьютерную информацию. Но расходятся во мнениях относительного того, чем является информация, объектом

или предметом противоправного деяния. Сторонники позиции, где информация – это объект преступления, считают, что информация, в том числе и компьютерная, является общественным благом, т.к. терпит ущерб при незаконном уничтожении или модификации. Богомолов соглашается с данным утверждением. Но, в то же время, он отмечает, что компьютерная информация может подвергнуться и незаконному копированию и блокированию, при этом сама по себе информация ни каким образом не пострадает. А объект преступления должен нести ущерб всегда, в противном случае не ясно, в чем выражается преступление. В первом случае страдают отношения законного обладателя информации по ее монопольному использованию, а во втором, страдают отношения по непосредственному законному использованию. В своей работе Богомолов приходит к следующему выводу - сама по себе компьютерная информация не всегда терпит ущерб, но во всех случаях страдают некоторые отношения по ее использованию. Следовательно, на данном этапе можно утверждать, что компьютерная информация выступает в качестве предмета компьютерных преступлений в уголовно-правовом понимании. В связи с этим в юридической литературе возникает такой вопрос: является ли компьютерная информация только лишь предметом преступлений такого вида или же она может выступать и их средством, когда электронно-вычислительная техника используется с целью совершения другого противоправного посягательства на иной объект? Как правило, авторы придерживаются точки зрения, согласно которой компьютерная информация является только предметом. Например, А.В. Сорокин считает, что «принять , что информация является также средством совершения других преступлений , означало бы слишком расширить рамки понятия « компьютерное преступление » и затруднить работу, как законодателя, так и правоприменителя». С технической точки зрения, компьютерная информация действительно является средством действия в рамках компьютерной системы, но средством в техническом и юридическом смысле информация будет только в совокупности с компьютером, а не отдельно от него. В связи с чем, вопрос можно считать исчерпанным и при квалификации преступлений, где ЭВМ является средством, воспринимать ЭВМ как комплекс аппаратного и программного обеспечения. Комиссаров приводит иное определение компьютерного преступлении -умышленные общественно опасные деяния (действие или бездействие), причиняющие вред либо создающие угрозу причинения вреда общественным отношениям, регламентирующим безопасное производство, хранение, использование или распространение информации и информационных ресурсов либо их защиту. Но Богомолов нашел изъян и в этом определении и он заключается в следующем: при анализе его видно, что В.С.

Комиссаров имеет в виду некие «общественные отношения, регламентирующие безопасное производство, хранение, использование и распространение информации и информационных ресурсов либо их защиту». Обычно под такими отношениями понимают нормативные акты или правила эксплуатации, т.е. при незаконном копировании информации страдают отношения между законным обладателем и государством (обществом), которое через нормативные акты регламентировало ему монопольное ее использование. Но, например, Абрамов считает иначе, и относит к компьютерным преступлениям, любые противоправные действия, при котором компьютер выступает либо как объект, против которого совершается преступление, либо как инструмент, используемый для совершения преступных действий.[6]

Наиболее правильным, с точки зрения данного автора, считается определение, данное В. Ю. Максимовым: компьютерные преступления - разновидность информационных преступлений, противоправные, виновно совершенные, наказуемые в уголовном порядке общественно опасные деяния, предметом которых является компьютерная информация, а объектом - отношения по ее нормальному, безопасному использованию.

В этой трактовке также существует небольшая неточность, которая состоит в том, что Максимов говорит о безопасном использовании компьютерной информации. В уголовно-правовом смысле безопасное использование, например, огня или ядерной энергии, не может быть сравнено с безопасным использованием компьютерной информации. Специфика информации ЭВМ в том, что удаление, копирование, создание или модифицирование не может быть опасным или безопасным как для законного обладателя, так и для правонарушителя. Это лишь переход информации из одного состояния в другое. Вместо слова «безопасное» следует использовать – «законное» использование информации, т.к. только законный обладатель информации должен иметь возможность удалять, копировать, создавать или модифицировать информацию.

Итак, с учетом вышесказанного М.В. Богомолов дает следующее определение: компьютерное преступление – это противоправное, виновно совершенное, наказуемое в уголовном порядке общественно опасное деяние, причиняющие вред либо создающие угрозу причинения вреда общественным отношениям по законному использованию компьютерной информации. Компьютерное преступление - общественно опасные, виновные, противоправные, уголовно-наказуемые деяния, которые причиняют вред информационным отношениям, средством обеспечения которых являются электронно-вычислительные машины,

системы или компьютерные сети.[7]

В настоящее время, как считают некоторые ученые, можно выделить два основных течения научной мысли в отношении исследуемого вопроса. Одна часть исследователей относит к компьютерным преступлениям действия, в которых компьютер является либо объектом, либо орудием посягательств. При этом кража самих компьютеров рассматривается ими один из способов совершения компьютерных преступлений. Исследователи же второй группы относят к компьютерным преступлениям только противозаконные действия в сфере автоматизированной обработки информации. Они выделяют в качестве главного классифицирующего признака, позволяющего отнести эти преступления в обособленную группу, общность способов, орудий, объектов посягательств.[8]

Специфика преступлений данной группы определяется их объектом и предметом. С одной стороны, закон относит их к преступлениям против общественной безопасности. Поэтому составы компьютерных преступлений следует толковать в том смысле, что эти преступления представляют опасность для охраняемых законом интересов неопределенного круга лиц. С другой стороны, все указанные преступления совершаются путем неправомерного воздействия на компьютерную информацию, что ограничивает объект и указывает на предмет этого преступления.Опасность компьютерных преступлений в том, что они создают опасность жизни и здоровью, имущественным правам и интересам, неприкосновенности частной жизни, иным охраняемым законом интересам личности, общества и государства. Недопустимо применение к человеку уголовной репрессии лишь за нарушение установленного порядка в сфере использования компьютерной информации, если его деяние не причинило и не могло причинить никакого реального вреда. Не будет, например, преступлением в силу ч. 2 ст. 14 УК использование одним несовершеннолетним компьютера другого несовершеннолетнего для игр без согласия последнего, даже если это привело к копированию очень большого объема информации, исчисляемого сотнямимегабайт. С другой стороны, изменение даже одной единицы информации в оборонной или транспортной системе может вызвать серьезные вредные последствия и может влечь уголовную ответственность при неправомерном доступе.Поэтому представляются обоснованными предложение Г.П. Новоселова не рассматривать уничтожение, блокирование информации и т.п. в качестве последствия преступления[9] . Целесообразно было бы определить их в качестве способа посягательства, но это не основано на действующем законе. Родовой объект преступлений в сфере компьютерной информации – общественная безопасность.

Видовым объектом данного преступления являются общественные отношения в сфере безопасности компьютерной информации и нормальной работы ЭВМ, системы ЭВМ или их сети. Видовой объект – охраняемая уголовным законом совокупность интересов в области безопасности, изготовления, использования, распространения информационных систем и технологий.

Непосредственными объектами преступлений в сфере компьютерной информации являются отдельные виды отношений, входящие в содержание данного вида общественной безопасности:

1.неприкосновенность информации, содержащейся в ЭВМ, их системе или сети;

2. правильная эксплуатации системы, исключающая причинение вреда личности, обществу и государству.

Предметом компьютерных преступлений является компьютерная информация.

Компьютерная информация — это информация в оперативной памяти ЭВМ, информация на иных машинных носителях, как подключенных к ЭВМ, так и на съемных устройствах, включая дискеты, лазерные и иные диски. Хищение дискеты (кроме грабежа и разбоя) влечет административную ответственность за мелкое хищение, что не исключает ответственности за неправомерный доступ к информации, на ней записанной, если виновный при этом умышленно приобретает доступ к информации на дискете.Компьютерная информация в системе или сети ЭВМ не может существовать иначе как на конкретных ЭВМ, в эту систему или сеть объединенных. Поэтому, например, перехват информации при ее передаче по каналам связи будет неправомерным доступомк информации в ЭВМ, с которой она передается. Компьютерная информация в ЭВМ, в свою очередь, существует только в виде записей на машинных носителях.Поскольку компьютерная информация не существует иначе как в виде записей на компьютерных машинных носителях, необ-ходимо определить, что следует понимать в этом качестве.

Специалисты прибегают к разным критериям отграничения «компьютеров» от иных вычислительных устройств. Так, например, одни используют идеальную модель «машины Тьюринга» (минимальный набор функций — по этому критерию к компьютерам можно отнести и программируемый калькулятор), другие большее внимание уделяют интерфейсу и операционной системе, третьи вовсе отрицают принципиальное отличие компьютера от иных вычислительных устройств. В уголовном праве приемлем лишь лингвистический критерий. Так, очевидно, не может рассматриваться в качестве компьютера калькулятор, и использование

чужого калькулятора без разрешения его хозяина не является преступлением. Не будет компьютером и кассовый аппарат, в том числе и оборудованный электронным запоминающим устройством. В русском языке слова «ЭВМ», «компьютер» употребляются для обозначения «карманных компьютеров», персональных компьютеров и компьютеров более высокого уровня. Компьютерами будут и электронные машины, являющиеся неотъемлемой частью какой-либо технической системы (бортовые компьютеры, компьютеры в автоматизированных производствах и т.п.). Заслуживает рассмотрения позиция некоторых авторов, которые к компьютерной информации относят не только сведения, которые человек хранит, обрабатывает или передает с помощью ЭВМ, но и компьютерные программы. Такое положение является не совсем правильным. В связи с этим заслуживает внимания позиция ученых, которые считают, что информация является свойством исключительно человеческого сознания и общения и связывают ее с наличием субъекта, который познает. Компьютерные программы представляют собой набор команд для ЭВМ. Поэтому компьютерные программы не относятся к компьютерной информации как предмету преступления, а их уничтожение или искажение можно рассматривать как уничтожение или повреждение имущества или уничтожение, повреждение или блокирование компьютерной информации, для работы с которой применяются те или иные компьютерные программы.

Таким образом, компьютерную информацию как предмет преступления можно определить следующим образом: сведения об объективном мире и происходящих в нем процессах целостность, конфиденциальность и доступность которых обеспечивается с помощью компьютерной техники, и которые имеют собственника и цену.

Охраняемая законом компьютерная информация — это любая информация, поставленная под защиту закона в связи с обеспечением вещных и обязательственных прав на ЭВМ и компьютерное оборудование, а также в связи с тайной сообщений (ст. 23 Конституции РФ).

Объективная сторона компьютерных преступлений характеризуется как действие (бездействие), связанное с использованием компьютерных систем и сетей, причинившее вред личности, обществу и государству или способное причинить такой вред. (Самовольное получение виновным возможности распоряжаться такой информацией).

Компьютерные преступления имеют материальные составы (исключением является преступление с формальным составом, предусмотренное ч. 1 ст. 273 УК: создание, использование и распространение вредоносных программ для ЭВМ).

Субъективная сторона компьютерных преступлений характеризуется как умышленной, так и неосторожной виной. Некоторые квалифицированные составы преступлений предусматривают только неосторожную форму вины.

Субъект компьютерного преступления — физическое, вменяемое, дееспособное лицо, достигшее возраста уголовной ответственности, то есть 16 лет. В ст. 274 и ч.2 ст.272 УК формулируются признаки специального субъекта : лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети.[10]

§1.2Виды компьютерных преступлений, содержащихся в Уголовном Кодексе РФ.

§1.3 Неправомерный доступ к компьютерной информации.

Непосредственный объект - отношения в сфере охраны компьютерной информации. (Общественные отношения в сфере безопасного использования компьютерной информации).[11] Объект – общественные отношения, связанные с безопасностью использования компьютерной информации.

Под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их фиксации или представления.(ФЗ п.1 ст.2). Компьютерной считается информация, обработанная на ЭВМ (компьютере). Такая информация может содержаться внутри компьютера или в устройствах, к нему подключаемых.

Предмет преступления — охраняемая законом компьютерная информация, то есть информация:

на машинном носителе;

в электронно-вычислительной машине (ЭВМ);

в системе ЭВМ;

в сети ЭВМ. Компьютерная информация может содержаться в памяти ЭВМ, которая реализуется через машинные носители, используемые как запоминающие устройства, — внешние, т. е. произвольно устанавливаемые (например, дискета), или внутренние, включенные в конструкцию ЭВМ. Запоминающее устройство, реализующее внутреннюю память ЭВМ, непосредственно связано с процессором и содержит данные, непосредственно участвующие в его операциях.

Компьютерная информация может передаваться по телекоммуникационным каналам из одной ЭВМ в другую, из ЭВМ — на устройство отображения (дисплей, например), из ЭВМ — на управляющий датчик оборудования. Телекоммуникационные каналы с соответствующим программным обеспечением связывают отдельные ЭВМ в систему или сеть.

Таким образом, данная норма уголовного законодательства оберегает компьютерную информацию, где бы она ни содержалась и ни циркулировала: в памяти ЭВМ, в каналах связи, на обособленных от ЭВМ машинных носителях.

Под ЭВМ следует понимать комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач. Система ЭВМ — это совокупность взаимосвязанных и взаимодействующих процессоров или ЭВМ, периферийного оборудования и программного обеспечения, предназначенных для автоматизации процессов приема, хранения, обработки, поиска и выдачи информации потребителям по их запросам. Сочетание компьютера и его периферийных устройств, работающих на основе ЭВМ, образует компьютерную систему (систему ЭВМ). Под сетью ЭВМ(компьютерной сетью) понимается совокупность нескольких компьютеров, соединенных друг с другом при помощи специальных кабелей в целях обмена файлами (передачи и получения информации от других подключенных к сети компьютеров), совместного использования аппаратных ресурсов (принтера, сканера, винчестера и др.), запуска общих программ, находящихся в других компьютерах. По делам о данном преступлении должно быть установлено, что компьютерная информация, к которой осуществлен доступ, охраняется законодательством о государственной тайне, о собственности, об авторском праве или др., что самим фактом несанкционированного к ней доступа нарушены прерогативы государства, права собственника, владельца, автора или другого юридического либо физического лица. Под охраной закона находятся также частная жизнь человека, коммерческая тайна, тайна сообщений. Машинный

носитель информации — это техническое средство (комплекс технических средств), предназначенное для фиксации, хранения, обработки, анализа и передачи компьютерной информации пользователем. К машинным носителям информации можно отнести, например, основной микропроцессор, гибкие магнитные диски (дискеты), жесткие магнитные диски (винчестеры), кассетные магнитные ленты (стримеры), магнитооптические диски, магнитные барабаны, магнитные карты и др.

Объективная сторона преступления выражается в доступе к информации или информационным ресурсам, содержащимся на машинном носителе, в ЭВМ, системе ЭВМ или их сети. Защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Способы неправомерного доступа к охраняемой законом компьютерной информации могут быть самыми разнообразными. Например, соединение с тем или иным компьютером, подключенным к телефонной сети, путем автоматического перебора абонентских номеров (внедрение в чужую информационную систему посредством «угадывания кода»), использование чужого имени (пароля) посредством использования ошибки в логике построения программы, путем выявления слабых мест в защите автоматизированных систем и др.

Средством совершения рассматриваемого преступления выступает компьютерная техника, т.е. различные виды ЭВМ, аппаратные средства, периферийные устройства, а также линии связи, с помощью которых вычислительная техника объединяется в информационные сети.

Объективная сторона статьи 272 УК РФ. Объективную сторону данного преступления составляет неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Неправомерный доступ к охраняемой законом компьютерной информации всегда носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем:

– использования специальных технических или программных средств позволяющих преодолеть установленные системы защиты;

– незаконного использования действующих паролей или кодов для проникновения в компьютер, либо совершение иных действий в целях проникновения в систему

или сеть под видом законного пользователя;

– хищение носителей информации, при условии, что были приняты меры их охраны если это деяние повлекло уничтожение или блокирование информации.

Обязательным признаком объективной стороны этого преступления является наступление вредных последствий для собственника или хранителя информации в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, систем ЭВМ или их сети. Это означает, что сам посебе просмотр информации, хранящейся в оперативной памяти компьютера или на машинном носителе (гибкомдиске - дискете, CD-R диске), состава преступления не образует. Необходимо, по крайней мере, внесениеизменений в соответствующие файлы или создание на базе имеющихся новых каталогов,затрудняющих законному пользователю информации доступ к ней, т. е. вызывающих уничтожение, блокирование информации или нарушение работы ЭВМ (систем ЭВМ, их сети). Под доступом к компьютерной информации подразумевается всякая форма проникновения к ней с использованием средств (вещественных и интеллектуальных) электронно-вычислительной техники, позволяющая манипулировать информацией. Завладение ЭВМ, не имеющей источников питания, а также машинным носителем информации как вещью не рассматривается как доступ к компьютерной информации и в соответствующих случаях может повлечь ответственность по статьям о преступлениях против собственности или самоуправстве. Точно так же не образует объективной стороны данного преступления уничтожение или искажение компьютерной информации путем внешнего воздействия на машинные носители теплом, магнитными волнами, механическими ударами и другими подобными методами[12] . С этой точкой зрения не соглашается другой автор, он отмечает, что такое толкование не вытекает из текста закона и что уничтожение компьютерной информации, в том числе и «путем внешнего воздействия», может быть и не связано с повреждением и уничтожением имущества (компьютерного оборудования). Вместе с тем оно может представлять значительную общественную опасность. Он приводит следующее определение доступа к компьютерной информации - это приобретение и использование лицом возможности получать, вводить, изменять или уничтожать информацию либо влиять на процесс ее обработки. Действие это может быть как простым (например, тайное проникновение в помещение, где находится компьютер, использование подкупа и угроз в отношении служащего), так и совершенным с использованием технических средств (например, использование доступа к компьютерной сети с целью неправомерного доступа к информации в ЭВМ)[13] . В.П.Ревин отмечает, что

«с точки зрения смысловойхарактеристики точнее было бы говорить о «проникновении»». Имеется ввиду неправомерное проникновение (вторжение) в охраняемую закономинформацию, находящуюся в памяти ЭВМ, в машинном носителе либоциркулирующую по коммуникационным каналам в системе или сети ЭВМ.

Доступ к компьютерной информации считается неправомерным, если лицо:

не имеет права на доступ к данной информации;

имеет право на доступ к данной информации, однако осуществляет его помимо установленного порядка, с нарушением правил ее защиты. Неправомерный доступ будет иметь место в случаях, когда лицо, не являясь собственником или иным законным владельцем компьютернойинформации, имеет право на работу с ней либо имеет доступ к работе с данным банком информации, но ограничено в объеме операций и вторгается в ту часть банка данных, которая для него закрыта.[14] (например, при использовании чужого пароля). Неправомерным проникновением к компьютерной информации будут действия лица, имеющего допуск к операциям соответствующего ранга, если доступ осуществлен с нарушением правил работы с даннымкомпьютером, системой, сетью, обеспечивающими устройствами, например, с отключением систем безопасности, с игнорированием физических условий, создавшихся в месте работы (например, высокой температуры), которые заведомо угрожают сохранности информации.[15] Несанкционированное проникновение к пульту управления ЭВМ или их системой следует рассматривать как приготовление к доступу к компьютерной информации. Неправомерный доступ к компьютерной информации часто сопровождается нейтрализацией интеллектуальных средств ее защиты. Такие действия уже сами по себе могут образовывать состав оконченного преступления, предусмотренного ст. 272 УК, либо, если при этом не наступилипоследствия в виде уничтожения, блокирования, модификации либо копирования компьютерной информации, должны рассматриваться как покушение на неправомерный доступ к компьютерной информации. Подтверждением вышесказанному служит норма, закрепленная в указе Президента: «Использование информации сопровождается строгим соблюдением требований ее защиты... Нарушение требований защиты информации расценивается как несанкционированный доступ к информации»[16] . Неправомерность доступа связана с нарушением вещных или обязательственных прав владельца или пользователя ЭВМ либо тайны сообщений (ст. 23 Конституции РФ). Нарушены могут быть права любого лица, использующего ЭВМ. Право собственности (и права титульного владельца) на ЭВМ нарушается в случае неправомерного доступа к ЭВМ

без разрешения собственника (титульного владельца) и иного законного полномочия. Обязательственные права нарушаются в случае неправомерного доступа к компьютерной информации, принадлежащей лицу, использующему ЭВМ на основе какого-либо договора. В этом случае преступление может быть совершено и собственником компьютера. (например, неправомерным будет просмотр электронной почты, доступ к информации при иных способах сетевой связи со стороны лица, предоставившего услуги связи, провайдера). Нарушение тайны сообщений правомерно только со стороны органов и должностных лиц, осуществляющих оперативно-розыскную деятельность и предварительное расследование, и только на основании судебного решения (ст. 23 Конституции РФ)[17] . В случае если тайна сообщений нарушена в результате неправомерного доступак компьютерной информации, содеянное образует совокупность преступлений, предусмотренных ст. 272 и 138 УК.

Не является неправомерным: 1) доступ к открытой информации в сети Internet и других открытых сетях. В таких сетях неправомерный доступ будет иметь место только в случае преодоления защиты информации, либо, хотя и без преодоления защиты, в связи с нарушением тайны сообщений; 2) доступ к компьютерной информации в случае, когда лицо использует принадлежащее ему компьютерное оборудование для «взлома» защиты программы или базы данных в нарушение авторских прав с целью пиратского копирования или иного неправомерного использования информации. Такие действия не посягают на общественную безопасность и целиком охватываются составом преступления, предусмотренного ст. 146 УК (нарушение авторских и смежных прав)1 . Неправомерный доступ к записям программ для ЭВМ, к первичным документам баз данных и другой подобной информации, исполненной рукой человека, отпечатанной на машинке или принтере, набранной типографским способом, не подразумевается в данной норме уголовного закона и может в соответствующих случаях повлечь ответственность лишь по другим статьям Особенной части УК РФ (ст. 137, 138, 183 и др.). Эти последствия должны находиться в причинно-следственной связи с неправомерным доступом виновного к охраняемой законом компьютерной информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети.

Под уничтожением информации понимается утрата информации, при невозможности ее восстановлена или использования в соответствии с ее целевым назначением. Имеющаяся у пользователя возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от другого пользователя не освобождает виновного

от ответственности, так как уничтожение информации на данном конкретном носителе может повлечь тяжкие последствия, даже если информация впоследствии будет восстановлена (временная дезорганизация оборонной или транспортной системы). Уничтожением информации не является переименование файла, где она содержится, а также автоматическое «вытеснение» старых версий файлов последними по времени (кроме случаев, когда последняя версия урезана лицом, получившим неправомерный доступ к компьютерной информации).

Под копированием информации имеется в виду неправомерное воспроизведение имеющейся в ЭВМ информации в любой документированной форме (в текстовом или графическом виде, на машинном носителе и т.п.), (если оно осуществляется помимо воли собственника или владельца этой информации). Одни авторы считают, что копирование информации влечет ответственность вне зависимости от того, копируется ли информация с помощью технических средств либо копирование производится вручную (например, с дисплея). Копированием информации будет и вывод ее на печатающее устройство, само отображение ее на дисплее. В литературе высказана точка зрения, что копированием информации следует считать только запись ее в файл на магнитном носителе с сохранением файла-источника. Копирование компьютерной информации от руки, путем фотографирования текста с экрана дисплея, а также считывание информации путем перехвата излучений ЭВМ, расшифровки шумов принтера не подразумевается в диспозиции ст. 272 УК. С таким толкованием закона сложно согласиться. Действительно, слово «копирование» обычно используется в языке пользовательского интерфейса программ именно в этом смысле. Хотя нажатием кнопки «Copy» нельзя заставить себя взять авторучку и переписать конфиденциальную информацию с дисплея, однако это не означают, что такое переписывание не будет копированием информации. Копирование компьютерной информации следует рассматривать как неблагоприятное последствие, предусмотренное данной статьей уголовного закона, лишь в том случае, если она охраняется законом именно от несанкционированного копирования.[18]

От копирования компьютерной информации в смысле, придаваемом этому понятию данной нормой уголовного закона, следует отличать размножение информации .В последнем случае информация повторяется не на обособленном от оригинального носителе, а на оригинальном носителе (в памяти ЭВМ заводится несколько файлов одного содержания) либо на однородном носителе, оставшемся в распоряжении пользователя (копия заводится на дискете, сознательно оставленной в компьютере).В вину лицу, проникшему к компьютерной информации для

ознакомления с ней, не может быть поставлено ее копирование, обусловленное не зависящим от его воли автоматическим действием программных средств правомерного пользователя (например, если файлы периодически копируются при всяком обращении к ним кого бы то ни было).

Нарушение работы ЭВМ, системы ЭВМ или их сетиимеет место в случае, если ЭВМ, их система или сеть не выполняет своих функций, осуществляет их не должным образом или в случае заметного уменьшения производительности системы. Нарушение работы ЭВМвключает в себя сбои в работе машины, выведение на дисплей неверной информации, отказ в выдаче информации, отключение элементов компьютерной системы (серверов, модемов и т. д.) - то есть прекращение нормального функционирования этих устройств либо возникновение каких-либо помех или перебоев в работе этих устройств.

Блокирование информации - это создание препятствий к свободному ее использованию при сохранности самой информации – это закрытие информации, характеризующееся недоступностью ее использования по прямому назначению правомочному на это пользователю; это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением.

От уничтожения и блокирования компьютерной информации следует отличать вывод из строя компьютерной программы; в последнем случае программа для ЭВМ может быть доступна как организованная в виде файла информация, но не как объект взаимодействия с пользователем. В соответствующих случаях он может рассматриваться как преступление, предусмотренное ст. 141, 267, 273, 281 и др. УК РФ. В случае, если причиной выхода из строя компьютерной программы оказались уничтожение или блокирование компьютерной информации, которой должна оперировать программа, деяние следует квалифицировать как оконченное преступление — неправомерный доступ к компьютерной информации.

Следующим вредным последствием является модификация информации. Под модификацией информации следует понимать изменение содержания информации по сравнению с первоначальной

В силу этого неправомерный доступ к охраняемой законом компьютерной информации является причиной, а наступившие вредные последствия следствием, т.е. причинная связь — необходимый признак объективной стороны рассматриваемого преступления. Если вышеперечисленные последствия не выступают в качестве следствия неправомерного доступа к компьютерной

информации, а являются результатом иной деятельности виновного, то состав преступления, выраженный в ст. 272, отсутствует. В случае пресечения преступления до момента фактического наступления указанных в норме последствий, содеянное виновным надлежит рассматривать как покушение на неправомерный доступ к компьютерной информации. Подобные последствия могут возникнуть в результате технических неисправностей или ошибок в программных средствах. В этом случае лицо совершившего неправомерный доступ к компьютерной информации не подлежит ответственности из-за отсутствия причинной связи между действиями и наступившими последствиями.

Мотивами целями этого преступления могут быть любыми: корыстные побуждения, месть, цель получить информацию, желание проверить свои профессиональные способности или самоутвердиться. Но они не являются признаками состава этого преступления и не влияют на квалификацию.

Субъектами данного преступления в основном могут являться лица, имеющие опыт работы с компьютерной техникой, и поэтому в силу профессиональных знаний они обязаны предвидеть возможные последствия уничтожения, блокирования, модификации информации либо нарушения работы ЭВМ, системы ЭВМ и их сети. По общему правилу субъектом преступления, может быть физическое, вменяемое, дееспособное лицо, достигшее 16-летнего возраста, не наделенное в силу характера выполняемой им работы возможностью доступа к ЭВМ, системе ЭВМ или их сети. Однако ч. 2 ст. 272 УК РФ предусматривает наличие специального субъекта, совершившего данное преступление: 1. лицо, использовавшее при совершении преступления свое служебное положение; 2.лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети.

Субъективная сторонапреступления характеризуется виной в форме умысла : лицо осознает, что осуществляет неправомерный (несанкционированный) доступ к охраняемой законом компьютерной

информации, предвидит, что в результате производимых им операций могут наступить или неизбежно наступят указанные в законе вредные последствия, и желает (прямой умысел) или сознательно допускает (косвенный умысел) их наступления либо безразлично относится к ним. 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.

Это преступление при отсутствии квалифицирующих признаков относится к деяниям небольшой тяжести.

Часть 2 ст. 272 УК предусматривает квалифицированный состав данного преступления, если оно совершено: а) группой лиц по предварительному сговору; б) организованной группой; в) лицом, с использованием своего служебного положения; г) лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Преступление признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении именно этого деяния.

Организованная группа — это устойчивая группа лиц, заранее объединившихся для совершения одного или нескольких преступлений. Групповой способсовершения преступления будет налицо, если предварительный сговор имел место между лицами, которые совместными усилиями непосредственно обеспечили неправомерное проникновение в память компьютера или сеть ЭВМ.

Использование должностным лицом своего служебного положения предполагает доступ к компьютерной информации благодаря занимаемому служебному положению (виновный воспользовался предоставленными ему по службе полномочиями или возможностями пользоваться компьютером, системой ЭВМ или их сетью и содержащейся в них информацией). Оно может быть произведено как со стороны служащего государственного или муниципального органов, коммерческой или некоммерческой организации, эксплуатирующей компьютерную систему, так и со стороны иных лиц, совершающих преступление с использованием служебного положения (например, со стороны работника контролирующей организации). Лицо, использующее свое служебное положение или имеющее доступ к ЭВМ, системе ЭВМ или компьютерной сети, - это законный пользователь информации, как непосредственно работающий в режиме пользования или обработки баз данных, так и по роду своей деятельности имеющий право временно эксплуатировать ЭВМ или знакомиться с хранящейся в них информацией.

Рассматриваемое преступление при наличии названных выше квалифицирующих признаков относится к категории преступлений средней тяжести.

Состав данного преступления — материальный . Преступление считается оконченным с момента наступления хотя бы одного из альтернативно перечисленных в диспозиции ч. 1 ст. 272 УК последствий: уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети.

19 января 1997 года Южно-сахалинским городским судом впервые в России был вынесен обвинительный приговор по статьям о компьютерных преступлениях. Студент Южно-сахалинского института экономики, права и информатики Гоярчук С.А. за написание программы, подбиравшей пароли к адресам пользователей электронной почты, а также копирование информации из чужих почтовых ящиков получил два года лишения свободы условно и штраф в 200 минимальных размеров оплаты труда (ч.1 ст.272 и ч.1 ст.273)

Тагилстроевский районный суд города Нижнего Тагила Свердловской области рассмотрел уголовное дело по обвинению Р. по ст. 159, 183, 272, 273 УК РФ. В октябре-ноябре 1998 года Р., пользуясь своим служебным положением, совершил изменение ведомости начисления заработной платы на предприятии так, что у работников, которым начислялось более ста рублей, списывалось по одному рублю, эти средства поступали на счет, откуда их впоследствии снял Р. Изменения в программе были квалифицированы по статье 273, сбор сведений о счетах лиц, данные о которых были внесены в базу предприятия, — по статье 183, модификация этих данных — по статье 272, а получение начисленных денежных средств — по статье 159 УК РФ. Р. был приговорен к 5 годам лишения свободы условно с лишением права заниматься профессиональной деятельностью программиста и оператора ЭВМ сроком на 2 года.

6 февраля 1999 года было возбуждено уголовное дело по признакам преступления, предусмотренного ст. 272 УК. В ходе предварительного следствия было установлено, что с целью хищения чужого имущества обвиняемые Ч. и З. вступили в сговор, по которому Ч., работающий в фирме “Самогон”, имея доступ к компьютерам фирмы, ввел в базу клиентов фирмы сфальсифицированную запись с реквизитами, назвав которые впоследствии, З. получил со склада фирмы продукцию стоимостью более 70 тысяч рублей. Действия Ч. квалифицированы на предварительном следствии по статье 272 УК РФ. Приговором Вологодского городского суда З. был осужден по статье 159 УК РФ (“Мошенничество”) к 5 годам, а Ч. по статьям 159 и 272 УК РФ к 6 годам лишения свободы условно.

30 сентября 1999 года следователем следственного отделения РУ ФСБ России по Архангельской области было возбуждено уголовное дело по факту создания и распространения вредоносных программ: распространение “троянцев” было квалифицировано по статье 273 УК РФ, доступ к чужим паролям — по статье 272. Один из обвиняемых по делу получил 2 года лишения свободы условно, второй — 3 года реально, впрочем, он был освобожден из-под стражи в зале суда по амнистии.

8 октября 1999 года было возбуждено уголовное дело по признакам преступления, предусмотренного статьей 272 УК РФ, по факту несанкционированной модификации программы публичного поискового сервера НовГУ. В результате данного изменения на поисковой странице сервера появилась ссылка на страницу, содержащую порнографические изображения. В совершении данного преступления в ходе предварительного следствия обвинялся Ф. Впоследствии он был обвинен также в незаконном распространении и рекламировании порнографических материалов по статье 242 УК РФ (“Незаконное распространение порнографических материалов или предметов”). По имеющейся информации, по делу был вынесен оправдательный приговор.

§1.4 Создание, использование и распространение вредоносных программ для ЭВМ.

Статья 273 УК РФ предусматривает ответственность за создание и распространение различного рода компьютерных «вирусов» и других программ, которые могут нарушить целостность информации, нарушить нормальную штатную работу компьютера, сети ЭВМ. Статья защищает права владельца компьютерной системы на неприкосновенность и целостность находящейся в ней информации.

Уголовный кодекс РФ 1996 года вводит в оборот новое понятие: «вредоносные программы». Под вредоносными программами для ЭВМ[19] понимаются программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, а также приводящие к нарушению работы ЭВМ, системы ЭВМ или их сети (ст. 273 УК РФ). То есть, это программы, специально созданные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций для которых эти программы предназначены, определенные в документации на программу. Вредоносные программы принято называть вирусными. Под вирусной программой (программой-вирусом) понимается результат

сознательной деятельности виновного, выразившийся в представлении в объективной форме совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью уничтожения, блокирования, модификации или копирования информации, а равно в целях нарушения работы ЭВМ, системы ЭВМ или их сети. Под вредоносными программамипонимаются те из них, которые специально созданы для нарушения нормального функционирования компьютерных систем и программ. Вредоносная программа — это специально написанная (созданная) программа, которая, получив управление, способна причинить вред собственнику или владельцу информации в виде ее уничтожения, блокирования, модификации или копирования, а также нарушения работы ЭВМ, системы ЭВМ или их сети. Наиболее опасной разновидностью вредоносной программы следует признать программу — вирус (компьютерный вирус). Программа — вирус — это специально созданная программа, способная самопроизвольно присоединяться к другим программам (т.е. «заражать» их) и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов, искажение результатов вычислений, засорение или стирание памяти, создание помех в работе ЭВМ. Такие программы, как правило, составляются на языке ассемблера, никаких сообщений на экран монитора не выдают. Переносятся при копировании с диска на диск либо по вычислительной сети. В наше время даже человек не связанный с компьютерами, имеет представление о том, что такое вирус и называет вирусом любую вредоносную программу для компьютера, что не совсем правильно, так как вирусы являются только частью вредоносного программного обеспечения. Сегодня количество известных вирусов не поддается строгому учету и постоянно увеличивается. По приблизительным оценкам специалистов, ведущих борьбу с вредоносными программами, в среднем ежедневно появляется около 30 новых вирусов.

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

Сетевой червь - вредоносный программный код, распространяющий свои копии по сети с целью проникновения на компьютер-жертву, запуска своей копии на этом компьютере и дальнейшего распространения. Большинство червей распространяются в файлах, которые содержат код червя, и, в свою очередь, распространяются через E-mail, ICQ, и.т.д. Как только пользователь сохраняет на компьютере зараженный файл червь попадает на компьютер, и начинает искать путь дальнейшего распространения, например может самостоятельно разослать

свои копии по всем адресам, обнаруженным в почтовом ящике, некоторые черви способны автоматически отвечать на полученные письма.

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

Непосредственно вирусы делятся на три типа : перезаписывающие вирусы, паразитирующие вирусы и вирусы – компаньоны. Перезаписывающие вирусы заменяют код файла своим кодом, в результате чего файл перестает работать. Восстановить зараженный таким образом файл невозможно. Паразитирующие вирусы изменяют содержимое файла, но при этом оставляют его работоспособным. Вирусы-компаньоны создают копию файла, при этом код файла-жертвы не изменяется. Обычно вирус изменяет расширение файла (например, с .exe на .com), потом создает свою копию с именем, идентичным имени файла-жертвы, и дает ему расширение, тоже идентичное. Ничего не подозревающий пользователь запускает любимую программу и не подозревает, что это вирус. Вирус, в свою очередь, заражает еще несколько файлов и запускает программу, затребованную пользователем. За создание или распространение компьютерных вирусов лицо несет уголовную ответственность по ст. 273 УК РФ. Данное преступление наиболее опасное из преступлений в сфере компьютерной информации (глава 28 УК РФ), что отражено в санкции за него

Наиболее распространенными видами вредоносных программ являются «компьютерные вирусы» и «логические бомбы».

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

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

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

Объективную сторону данного преступления составляют создание, использование и распространение вредоносных программ для ЭВМ или машинных носителей с такой программой, а равно внесение вредоносных изменений в существующие программы.

В ст. 273 УК РФ речь идет не только о программах, записанных на машинном носителе, но и о записях программ на бумаге

Состав части 1 формальный и предусматривает совершение одного из действий:

1) создание программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы аппаратной части;

2) внесение в существующие программы изменений, обладающих аналогичными свойствами;

3) использование таких программ;

4) их распространение;

5) использование машинных носителей с такими программами;

6) распространение таких носителей. Следует обратить внимание, что создание, использование и распространение вредоносных программ для ЭВМ всегда предполагает активные действия со стороны лица, совершившего это преступление. Бездействием совершить рассматриваемое преступление представляется невозможным.

Программа для ЭВМ — это объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата. Говоря проще, это совокупность данных и команд на машинном языке, предназначенных для решения определенной задачи; алгоритм решения. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

Вредоносность программ определяется как способность несанкционированного уничтожения, блокирования, модификации, копирования информации, а также нарушения работы ЭВМ, их системы или сети – т.е. не разрешенные законом, собственником информации или другим компетентным пользователем указанные действия.Это тот же «набор» последствий, который является частью объективной стороны деяния, описанного в ст. 272 УК РФ. Но там должны обязательно наступить эти последствия, а в данном преступлении достаточно реальной угрозы их, создаваемой самим фактом наличия вредоносной программы. Вредоносностьили полезность соответствующих программ для ЭВМ определяется не в зависимости от их назначения, способности уничтожать, блокировать, модифицировать, копировать информацию (это вполне типичные функции абсолютно легальных программ), а в связи с тем, предполагает ли их действие, во-первых, предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает программу для ЭВМ вредоносной. Вредоносность «компьютерных вирусов» связана с их свойством самовоспроизводиться и создавать помехи работе на ЭВМ без ведома и санкции добросовестных пользователей. Вирусные программы обычно включают команды, обеспечивающие самокопирование и маскировку.

Понятие вредоносной программы, использованное уголовным законодательством, шире, нежели бытовое употребление понятия «компьютерный вирус». Законодатель имеет в виду вредоносные программы, связанные не только с полным или частичным уничтожением информации в банке данных, на который

распространяется их действие, но и с копированием информации или созданием условий для такого копирования. При этом деяние, выразившееся в создании вредоносных программ или внесении изменений в существующие программы, образует преступление только тогда, когда такое деяние объективно создавало реальную угрозу несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. В противном случае действия лица по созданию, использованию или распространению вредоносных программ нельзя рассматривать как преступление. Например, не будут являться преступными действия лица, создавшего довольно безобидную программу — вирус, которая высвечивает на экране монитора штрих и тут же исчезает. Поэтому в тех случаях, когда вредоносная программа не представляет опасности для собственника или владельца информации и объективно не может привести к последствиям, указанным в диспозиции ч. 1 ст. 273, действия лица обоснованно расценивать как малозначительные и на основании ч. 2 ст. 14 УК освобождать его от уголовной ответственности и наказания.

Поэтому оконченным рассматриваемое преступление считается лишь с момента создания такой программы, которая может быть введена в ЭВМ. Предшествующие этапы разработки могут квалифицироваться как приготовление или покушение на преступление.

Создание вредоносной программы представляет собой комплекс операций, состоящий из подготовки исходных данных, предназначенных для управления конкретными компонентами системы, обработки данных в целях уничтожения, блокирования, модификации или копирования информации, а также нарушения работы ЭВМ, системы ЭВМ или их сети - означает любую деятельность, направленную на написание вредоносной программы. Создание включает в себяне только творческую деятельность ее автора, но и техническую помощь, оказанную ему другими лицами. Созданием вредоносной программы будет и написание вредоносной программы, лишенной свойства новизны (например, известной раннее, но утраченной или недоступной создателю). Создание программы для ЭВМ — это написание ее текста с последующим введением его в память ЭВМ или без такового.

Внесение изменений в существующую программу означает изменение ее текста путем исключения его фрагментов, замены их другими, дополнения текста программы. Внесение изменений может быть элементом объективной стороны данного преступления лишь в том случае, если виновный исправил работающую в ЭВМ программу либо распространил исправленную программу на любом носителе.

Исправление изложенной на бумаге программы само по себе не подразумевается данной нормой уголовного закона, если этот бумажный вариант не будет непременно использован для создания работающей программы и не предназначен для распространения. Внесение изменений в существующие программы — это процесс модификации программы (переработка программы или набора данных путем обновления, добавления или удаления отдельных фрагментов) до такого ее качества, когда эта программа способна вызвать вредные последствия, указанные в диспозиции ч. 1 ст. 273 УК. Ответственность по данной норме уголовного закона должна наступать и в том случае, если изменения в существующую программу вносятся лицом не непосредственно, а посредством специальной программы для ЭВМ, разработанной для внесения соответствующих изменений. Так, Советским районным судом г. Липецка был осужден Н., который в интересах и по просьбе Ш. на языке программирования Pascal создал алгоритм, т.е. исходные данные для вредоносной программы, названной Н. "sss.pas". Эта программа несанкционированно уничтожала бы дерево каталога после введения ее в любой удаленный персональный компьютер и функционировала бы без уведомления об этом его владельца при включении (загрузке) компьютера, т.е. выполняла бы не санкционированную пользователем модификацию информации, хранящуюся на жестком диске.

В ходе судебного заседания было установлено, что созданный Н. алгоритм "sss.pas" является не законченной программой, а исходными данными для такой программы, которая после ее некоторого видоизменения и дачи ей определенной команды при перезагрузке удаленного компьютера работала и выполняла бы не санкционированную пользователем модификацию информации, которая хранится на жестком диске. Поэтому по заключению экспертизы программа, написанная Н., по своей сути являлась вредоносной.

Под использованием программы понимается воспроизведение, распространение (предоставление экземпляров программы неопределенному кругу лиц) и иные действия по ее введению в оборот в изначальной или модифицированной форме, а также самостоятельное применение этой программы по назначению. Не признается использованием программы для ЭВМ или базы данных передача средствами массовой информации сообщений о выпущенной в свет программе для ЭВМ или базе данных. Использование вредоносной программы для личных нужд (например, в целях уничтожения собственной компьютерной информации) ненаказуемо.

Под использованием машинного носителя с такой программой понимается всякое его употребление для целей использования записанной на нем программы для ЭВМ.

Распространением программы признается предоставление доступа к воспроизведенной в любой материальной форме программе, в том числе сетевым и иным способами (в том числе и в виде записи на бумаге), а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей.Распространением признается любая форма их реализации - как на коммерческой, так и на иной основе, как с обозначением сущности программы, так и без этого, путем, как дублирования, так и реализации отдельных машинных носителей (флоппи-дисков, CD-R дисков) либо посредством модема или передачи по компьютерной сети. Например, распространение таких программ может быть осуществлено при работе виновного на чужом компьютере, путем использования дискеты с записью, содержащей вирус, распространение вредоносной программы через модем или передачу по компьютерной сети и т.п.

Распространение машинных носителей вредоносной программы означает передачу носителя другому лицу, включая копирование или дозволение копирования программы на носитель другого лица.

Хотя данный состав является формальным и не требует наступления каких-либо последствий, уголовная ответственность возникает уже в результате создания программы независимо от того использовалась эта программа или нет. Однако следует учитывать, что в ряде случаев использование подобных программ не будет являться уголовно наказуемым. Это, прежде всего, относится к деятельности организаций, осуществляющих разработку антивирусных программ имеющих лицензию на деятельность по защите информации, выданную Государственной технической комиссией при Президенте РФ. Обязательными признаками объективной стороны ч.1 ст. 273 УК РФ являются следующие: а) последствия должны быть, несанкционированными; б) наличие самой вредоносной программы или внесения изменений в программу.

С субъективной стороны преступление характеризуется умышленной формой вины в виде прямого умысла. Лицо сознает, что создает программу, зараженную вирусом, либо внедряет вирус в чужую программу, или распространяет и использует такие программы и желает совершить эти действия. Как и при других компьютерных преступлениях необходимо устанавливать мотив и цель. Они не обозначены в качестве признаков данного состава, но их знание необходимо не

только для индивидуализации наказания, но и для квалификации деяний по совокупности. Часть 2 ст. 273 УК РФ в качестве квалифицирующего признака предусматривает наступление тяжких последствий по неосторожности. Таким образом, уголовная ответственность не наступит, если человек пытался создать новую компьютерную игру, а нечаянно создал вирус. Уголовная ответственность не наступит и в том случае, если лицо не знало, что в отправляемом по электронной почте файле, или на передаваемом диске содержатся вирусы.

Субъект преступления – общий. То есть, субъектом данного преступления может быть любой физическое, вменяемое, дееспособное лицо, достигшее возраста 16 лет и обладающее знаниями в области программирования и пользования ЭВМ. Достаточную распространенность имеет создание, использование, распространение вредоносных программ «вундеркиндами», не достигшими указанного возраста. Эти действия нельзя оставлять безнаказанными. При доказанности умысла в отношении последствий необходимо рассматривать вопрос о квалификации содеянного по одной из статей, перечисленных в ч. 2 ст. 20 УК РФ, по которым ответственность наступает с четырнадцати лет, если характер последствий охватывается соответствующими статьями, например ч. 2 ст. 167 УК РФ – умышленное уничтожение или повреждение имущества, ч. 2 ст. 213 УК РФ – хулиганство и др. Если такая возможность отсутствует, необходимо применять меры воздействия, предусмотренные законодательством о комиссиях по делам несовершеннолетних. Закон не требует, чтобы это лицо занимало определенную должность, занималось определенной деятельностью, получило определенное образование

Предметом преступления, как и применительно к ст. 272 УК РФ, является охраняемая законом компьютерная информация, находящаяся на машинном носителе, в ЭВМ, сети ЭВМ.

Данный состав преступления формальный и не требует наступления каких-либо последствий. Уголовная ответственность наступает в результате создания программы независимо от того, использовалась эта программа или нет. Наличие исходных текстов вирусных программ является основанием для привлечения к ответственности.

Если эти последствия наступили в результате неосторожной вины по отношению к ним, вопрос о квалификации по совокупности может встать в случаях, когда специальные составы, например ст. 247, 263 УК РФ, предусматривают возможность более строгого наказания виновного, нежели рассматриваемая статья. Если же по

отношению к последствиям устанавливается хотя бы косвенный умысел, квалификация по совокупности, т.е. по ч. 1 ст. 273 и статьям УК РФ об ответственности за умышленное причинение тяжкого вреда правоохраняемым объектам, является обязательной.

Общественная опасность создания, использования и распространения вредоносных программ для ЭВМ заключается в том, что такие действия могут повлечь за собой сбои в работе ЭВМ, системы ЭВМ или их сети, прекращение их функционирования либо выдачу ими искаженной информации, на основе которой могут приниматься ошибочные государственные, политические, экономические и другие решения.

Рассматриваемое преступление относится к формальным составам и считается оконченным с момента создания или распространения вредоносной программы для ЭВМ, системы ЭВМ или их сети. Состав преступления, сконструированный в ч. 1 ст. 273, является формальным . Следовательно, для признания преступления оконченным не требуется наступления вредных последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Достаточно установить сам факт совершения хотя бы одного из альтернативно-обязательных действий, перечисленных в диспозиции ч. 1 ст. 273. Рассматриваемое преступление при отсутствии квалифицирующих признаков (ч. 1 ст. 273) относится к категории деяний средней тяжести. Создание, использование и распространение вредоносной программы для ЭВМ, повлекшее вывод из строя вычислительной техники, выступающей в качестве аппаратной структуры (например, повреждение физической целостности электронно-вычислительной машины, ее основных устройств, не подлежащие восстановлению), квалифицируются по совокупности преступлений, устанавливающих ответственность за умышленное уничтожение или повреждение имущества (ст. 167 УК) и за создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК).

Квалифицирующим признаком рассматриваемого преступления является наступление в результате создания, распространения или использования вредоносных программ для ЭВМ тяжких последствий по неосторожности. Вид состава — материальный . В силу этого обстоятельства для признания лица виновным в совершении преступления, ответственность за которое наступает по ч. 2 ст. 273, необходимо установить факт наступления или распространения вредоносных программ для ЭВМ, т.е. действий, образующих объективную сторону этого преступления.

Частью 2 ст. 273 УК РФ криминализируется более опасное преступление: те же деяния, повлекшие тяжкие последствия. При этом «тяжкие последствия» – оценочная категория, которая должна определяться правоприменителем в каждом конкретном случае, с учетом совокупности обстоятельств объективного и субъективного характера. К таким последствиям можно отнести: имущественный ущерб, сопряженный с восстановлением информации; упущенную выгоду при срыве заключения крупного контракта или соглашения; дезорганизацию работы предприятий или учреждений, деятельности государственного органа, аварию, катастрофу и т. п. Под тяжкими последствиями создания, использования или распространения вредоносных программ для ЭВМ понимаются безвозвратная утрата особо ценной информации, выход из строя важных технических средств (например, систем оборонного назначения, аэронавигационной техники), повлекший несчастные случаи с людьми, аварии, катастрофы. Форма вины по отношению к тяжким последствиям может быть только неосторожной. Санкция второй части данной статьи – относительно-определенная: лишение свободы на срок от 3 до 7 лет. Таким образом, именно это преступление из всей главы относится к категории тяжких.Специфика рассматриваемого более опасного вида данного преступления заключается в том, что оно совершается с двумя формами вины , т.е. характеризуется умыслом относительно факта создания, использования или распространения вредоносной программы для ЭВМ и неосторожностью (легкомыслием либо небрежностью) относительно наступления тяжких последствий. Это означает, что причинение тяжких последствий не охватывается умыслом виновного, однако он предвидит возможность их наступления, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение либо не предвидит, хотя и должен был и мог предвидеть возможность наступления тяжких последствий. Если такие последствия причинены умышленно, содеянное квалифицируется по ч. 1 ст. 273 УК и по совокупности по статье УК, предусматривающей ответственность за умышленное причинение тяжких последствий.

Преступная небрежность в данном случае не вменяется в вину, если между созданием, использованием и распространением вредоносной программы и соответствующими тяжкими последствиями так много последующих звеньев или неожиданных обстоятельств, что человеческой внимательности и предусмотрительности с учетом полученной данным лицом специальной подготовки явно не хватает, чтобы предвидеть столь опасный результат. В случае, если действие вредоносной программы было условием совершения лицом другого преступления, деяния должны быть квалифицированы по совокупности вне

зависимости от степени тяжести другого преступления. Данное деяние при наступлении тяжких последствий относится к категории тяжких преступлений.

Окончено преступление с момента создания программы-«вируса» либо ее использования или распространения. Оконченным данное преступление считается с момента окончания создания вредоносной программы. То есть с того момента, когда программа будет способна принести вред компьютеру. Это означает, что максимально возможный срок (3 года) лицо получит только после завершения работы над программой. Уголовная ответственность, при наличии достаточной доказательственной базы, может наступить и за попытку создания вируса, т.е. за неоконченное преступление. Однако максимально возможное наказание за неоконченное преступление составляет 3/4 от наказания за оконченное преступление.

Если создание, использование или распространение вредоносных программ для ЭВМ выступает в качестве способа совершения иного умышленного преступления, то при квалификации содеянного следует руководствоваться следующими правилами:

а) в том случае, если виновный стремился совершить преступление, состав которого сконструирован по типу материального, но по независящим от него обстоятельствам общественно опасные последствия не наступили, — деяние квалифицируется по правилам совокупности преступлений, предусматривающих ответственность за покушение на то преступление, к совершению которого лицо изначально стремилось, и за создание, использование или распространение вредоносных программ для ЭВМ (ч. 1 ст. 273 УК);

б) в случае, если виновный посредством создания, использования или распространения вредоносных программ для ЭВМ совершил иное умышленное преступление, содеянное им квалифицируется только по соответствующей статье Особенной части УК, предусматривающей ответственность за совершение этого преступления без дополнительной квалификации по ст. 273 УК РФ;

в) исключение составляют те ситуации, когда создание, использование или распространение вредоносных программ для ЭВМ выступает в качестве способа совершения менее опасного преступления, чем предусмотренного в ч. 1 ст. 273 (например, создание вредоносной программы с целью злостного уклонения от уплаты средств на содержание детей). В таких случаях, содеянное виновным, необходимо квалифицировать по правилам совокупности преступлений. Например,

по ч. 1 ст. 273 и, в том случае, если виновный для уклонения от уплаты средств на содержание несовершеннолетних детей использовал вредоносную программу, — по ч. 1 ст. 157 УК.

Достаточно, если программа рассчитана хотя бы на единичное достижениеэтого результата1 . Продавцы программного обеспечения иногда снабжают программные пакеты специальной программой-«жучком», тестирующей состояние компьютерной системы покупателя и сообщающей автоматически (при регистрации или обновлении с помощью модема) продавцу сведения об используемых покупателем компьютерном оборудовании и программном обеспечении. Данная программа может рассматриваться в качестве вредоносной программы, предназначенной для несанкционированного копирования информации в случае, если покупателю не сообщается об этом свойстве программного продукта.

Сыктывкарским городским судом вынесен приговор двум жителям столицы республики, признанным виновным в совершении неправомерного доступа к компьютерной информации и использовании вредоносных программ для ЭВМ.

Злоумышленники из корыстных побуждений неправомерно модифицировали охраняемую законом компьютерную информацию на ЭВМ, использовав при этом вредоносное программное обеспечение. В отношении "взломщиков" Следственным управлением при МВД по РК были возбуждены уголовные дела по ст. 272 и ст. 273 Уголовного кодекса России.

Судом одному из участников группы назначено наказание в виде штрафа в размере 5000 рублей и 330 часов обязательных общественно полезных работ, второму - наказание в виде 180 часов обязательных работ.

УФСБ по Кировской области впервые в истории российских спецслужб (2000 год) возбудило уголовное дело по статье 273 УК "создание, использование и распространение вредоносных программ для ЭВМ", сообщили РБК в ЦОС ФСБ РФ.

Обвиняемым по делу проходит техник отдела информации одной из частных компаний города Кирова. Он поместил на служебный компьютер программу, которая "заведомо приводит к нарушениям в работе РС и локальной сети". Обвиняемый установил эту программу на сервер своей фирмы. В результате все посетители сервера получили возможность с помощью данной программы взламывать защиту РС и пользоваться данными без ведома их владельцев.

§1.5 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Общественная опасность нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети заключается в том, что это может привести к уничтожению, блокированию или модификации охраняемой законом компьютерной информации и причинению существенного вреда собственнику, владельцу или пользователю ЭВМ, системы ЭВМ или их сети.[20]

Предметом этого преступления являются электронно-вычислительные машины (ЭВМ), системы ЭВМ или их сети.[21]

Объектом является безопасность пользования интеллектуальными и вещественными средствами вычислительной техники[22] . Объектом преступления являются общественные отношения, обеспечивающие правильную, безопасную эксплуатацию ЭВМ, их системы или сети.[23] Объектом являются общественные отношения в сфере соблюдения установленных правил, обеспечивающих нормальную эксплуатацию ЭВМ, системы ЭВМ или их сети. [24] Непосредственный объект рассматриваемого преступления - совокупность общественных отношений, обеспечивающих эксплуатацию ЭВМ, их систем или сети (включая подготовку к действию по обслуживанию после окончания действия) таким образом, что сохраняется их исправность и не создается угроз безопасности правоохраняемым объектам, в том числе компьютерной информации.[25]

Объективная сторона преступления заключается в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшем уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.[26] Объективная сторона преступления характеризуется деянием (действием или бездействием), заключающимся в нарушении правил эксплуатации компьютерной системы или сети, последствием в виде существенного вреда и причинной связью между действием и последствием.[27] Объективная сторона анализируемого преступления в качестве необходимых признаков включает общественно опасное деяние, общественно опасное последствие и причинную связь между общественно опасным деянием и последствиями, указанными в диспозиции данной нормы. [28] Общественно опасное деяние, составляющее данное преступление, заключается в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети, установленных в

соответствии с режимом информации или ее защиты Законами РФ, иными нормативными актами, включая и правила эксплуатации ЭВМ, утвержденные в конкретной организации. Фактически это может выражаться в несоблюдении или игнорировании соблюдения определенных правил, обеспечивающих нормальную эксплуатацию ЭВМ, системы ЭВМ или их сети (например, нарушение режима использования ЭВМ, системы ЭВМ или их сети, небрежность при проверке используемых физических носителей информации на наличие вредоносных программ и т.д.). Деяние может совершаться как в форме действия, так и бездействия.

Обязательным признаком объективной стороны преступления выступает общественно опасное последствие в виде уничтожения, блокирования или модификации охраняемой законом информации ЭВМ, при условии, что это деяние причинило существенный вред (ч. 1 ст. 274 УК) или тяжкие последствия (ч. 2 ст. 274 УК).[29] Объективная сторона преступления может реализовываться как действием, так и бездействием, направленным на нарушение правил эксплуатации ЭВМ, системы или сети, повлекших уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ при условии, что в результате этих действий был причинен существенный вред. Между фактом нарушения и наступившим существенным вредом должна быть установлена причинная связь и доказано, что наступившие последствия являются результатом нарушения правил эксплуатации. Объективная сторона преступления заключается в нарушении установленных правил эксплуатации ЭВМ, системы ЭВМ илиих сети, если это повлекло причинение существенного вреда (материальный состав). Фактически этовыражается в несоблюдении или прямом игнорировании определенных правил, обеспечивающих безопасностькомпьютерной системы или сети (например, требования о проверке посторонних машинных носителейинформации на наличие «вирусов», регулярном обновлении используемых «антивирусных» программ). К такому виду нарушений можно отнести: несоблюдение общих средств защиты информации, а также нарушение режима эксплуатации ЭВМ. Выделяют два основных средства защиты: копирование информации и ограничение доступа к информации. Нарушение режима эксплуатации ЭВМ образуют, например, несанкционированные изменение, уничтожение или передача информации[30] .

Существенный вред устанавливается судом в каждом конкретном случае исходя из обстоятельств дела, однако этот вред должен быть не менее значительным, чем тяжкие последствия.[31]

Правила эксплуатации ЭВМ определяются соответствующими техническими нормативными актами. Они также излагаются в паспортах качества, технических описаниях и инструкциях по эксплуатации, передаваемых пользователю при приобретении вещественных средств компьютерной техники (ЭВМ и периферийных устройств), в инструкциях по использованию программ для ЭВМ. Соответствующие инструкции могут излагаться на бумажных и машинных носителях; в последнем случае они обыкновенно встраиваются в программу, которая обеспечивает к ним доступ при желании пользователя. Под правилами эксплуатации компьютерной системы следует понимать как правила, которые могут быть установлены компетентным государственным органом, так и правила технической эксплуатации и правила работы с программами, установленные изготовителями ЭВМ и иного компьютерного оборудования, правила, установленные разработчиками программ, сетевыми администраторами, а также правила, установленные владельцем компьютерной системы или по его полномочию (например, последний может запретить служащим использование не прошедших проверку на «вирусы» дискет).

Нарушение правил эксплуатации компьютерной системы должно повлечь уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ и, кроме того, существенный вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства. Таким образом, специфической чертой этого преступления является наличие двух уровней последствий. Существенный вред — оценочное понятие, устанавливаемое судом с учетом всех значимых обстоятельств конкретного дела.

Таким образом, нарушения правил эксплуатации ЭВМ:

1) физические (неправильная установка приборов, нарушение температурного режима в помещении, неправильное подключение ЭВМ к источникам питания, нерегулярное техническое обслуживание, использование несертифицированных средств защиты и самодельных приборов и узлов)

2) интеллектуальные (неверное ведение диалога с компьютерной программой, ввод данных, обработка которых непосильна данным средствам вычислительной техники).

Под существенным вредом в диспозиции данной нормы уголовного закона понимаются утрата важной информации, перебои в производственной деятельности, необходимость сложного или длительного ремонта средств вычислительной техники, их переналадки, длительный разрыв связей между ЭВМ,

объединенными в систему или сеть. Существенность вреда определяется с учетом имущественного положения и организационных возможностей собственника или владельца ЭВМ. Формулировка закона исключает возможность привлечения лица к уголовной ответственности по ст. 274 УК, если нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети хотя и повлекло уничтожение, блокирование или модификацию информации, но объективно не могло причинить существенного вреда (тем более, не могло привести к наступлению тяжких последствий) правоохраняемым интересам личности, общества или государства. [32] Понятие «существенный вред» — оценочное. Между тем от правильного его уяснения зависит не только признание лица виновным в совершении такого преступления, как нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, но разграничение основного состава рассматриваемого преступления (ч. 1) от квалифицированного (ч. 2).[33] Существенность вреда собственнику, владельцу или пользователю компьютерной информации определяется с учетом фактических обстоятельств совершенного преступления и является вопросом факта. Например, причиненный вред следует признавать существенным, если в результате нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети утрачена важная компьютерная информация, повлекшая дезорганизацию производственной деятельности государственной или коммерческой организации, или оно вызвало сложный и дорогостоящий ремонт вычислительной техники, повлекло продолжительный перерыв в обмене информацией между ЭВМ, объединенными в систему ЭВМ или их сеть. Между нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети и наступившими последствиями, о которых говорится в законе, должна быть установлена причинная связь.[34]

Субъектом рассматриваемого преступления является только вменяемое физическое лицо, достигшее ко времени совершения преступления 16-летнего возраста. Закон не требует, чтобы это лицо занимало определенную должность, занималось определенной деятельностью, получило определенное образование. Главное, чтобы оно имело доступ к ЭВМ[35] . Субъект преступления — специальный: вменяемое лицо, достигшее возраста 16 лет, имеющее доступ к компьютерной системе или сети[36] . Субъект анализируемого преступления — специальный. Им может быть лицо 16-летнего возраста, которое в силу характера выполняемой им трудовой, профессиональной или иной деятельности имеет беспрепятственный доступ к ЭВМ, системе ЭВМ или их сети и на которое в силу закона или иного нормативного акта возложена обязанность соблюдения правил эксплуатации ЭВМ, системы ЭВМ или их сети.[37] Субъектом этого преступления может быть любое вменяемое лицо, достигшее 16-летнего возраста и имеющее

доступ к ЭВМ, системе ЭВМ или их сети. Под имеющим доступ к ЭВМ, системе ЭВМ или их сети понимается лицо, которое по характеру своей работы либо в связи с эксплуатацией ЭВМ и других устройств, либо с их техническим обслуживанием может беспрепятственно пользоваться названными выше устройствами.[38] Субъект рассматриваемого преступления специальный. Он определяется не только возрастом (шестнадцать лет), но и наличием у виновного доступа к ЭВМ, системе ЭВМ или их сети.[39]

Субъективную сторону данного преступления могут составлять и умысел, и неосторожность. Однако по отношению к общественно опасным последствиям, предусмотренным ч. 2 данной статьи, вина характеризуется только неосторожностью (легкомыслием или небрежностью). По нашему мнению, в данном случае речь идет о двойной форме вины. Это деяние при отсутствии квалифицирующих признаков (ч. 1 ст. 274) относится к категории преступлений небольшой тяжести. Субъективная сторона преступления характеризуется прямым или косвенным умыслом, направленным на нарушение правил эксплуатации ЭВМ. В случае наступления тяжких последствий ответственность по данной статье наступает только в случае неосторожных действий.[40]

Под указанными в ч. 2 ст. 274 УК тяжкими последствиями (квалифицирующий признак) нарушения правил эксплуатации ЭВМ понимаются безвозвратная утрата особо ценной информации, выход из строя важных технических средств (например, систем оборонного назначения, аэронавигационной техники), повлекшие несчастные случаи с людьми, аварии, катастрофы. Часть 2 ст. 274 УК предусматривает ответственность за те же деяния, повлекшие по неосторожности тяжкие последствия (оценочный признак). В случае умышленного причинения тяжких последствий содеянное квалифицируется по ч. 1 ст. 274 УК и по совокупности — по норме, предусматривающей ответственность за умышленное причинение тяжких последствий. Если такой нормы в УК нет (например, лицо из хулиганских побуждений причинило крупный ущерб, дезорганизовав движение транспорта), содеянное полностью охватывается ч. 1 ст. 274 УК[41] . Под существенным следует понимать такой вред, который выражается в причинении легкого вреда здоровью человека, причинении имущественного ущерба в значительных размерах законному собственнику или владельцу информации, а также иным лицам, остановке работы предприятия, организации либо учреждения, нанесении морального ущерба личности путем разглашения сведений об усыновлении детей и т.п. Квалифицирующим признаком данного преступления является наступление по неосторожности тяжких последствий в результате

нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети (ч. 2 ст. 274). Понятие тяжких последствий является оценочным. Тяжесть последствий определяется с учетом всех фактических обстоятельств содеянного. Например, тяжким последствием можно считать безвозвратную утрату особо ценной компьютерной информации, уничтожение системы ЭВМ или их сети, несчастные случаи с людьми и т.п.

Рассматриваемое преступление при наличии указанного квалифицирующего признака относится к категории преступлений средней тяжести.[42]

При обнаружении сбоев в работе ЭВМ (особенно в работе программных средств) и установлении оснований для квалификации деяний по ст. 274 УК РФ весьма важно разграничивать ответственность:

экспертов-предметников , участвовавших в подготовке алгоритмов и программного продукта, — за верность и полноту сообщенных ими знаний;

инженеров по знаниям — за применение адекватных технических и формальных программных средств (инструментальная система, язык, система управления базами данных) для создания прикладной системы, правильное отражение информации, полученной от экспертов;

программистов — за создание качественного, безошибочно работающего базового программного обеспечения;

руководителя проекта — за организацию взаимодействия разработчиков, надлежащее тестирование программного продукта на всех этапах его создания;

приемщиков программного продукта — за контроль его качества с точки зрения возможности использования, оценку и выпуск в эксплуатацию;

технических служб — за установку системы на технике пользователя, поддержание компьютеров в исправном состоянии, надлежащие условия эксплуатации техники;

пользователя — за правильный с точки зрения имеющейся задачи выбор экспертной системы, достоверность входных данных, надлежащую эксплуатацию системы, распечатку выходных материалов без заведомых искажений. В случае, когда нарушение правил эксплуатации ЭВМ повлекло также совершение лицом другого преступления, деяния должны быть квалифицированы по совокупности , если другое преступление наказывается более строго. Если другое преступление

наказывается более мягко, то следует считать, что наступившие неблагоприятные последствия уже подразумеваются данной нормой уголовного закона.[43] Состав данного преступления — материальный . Оконченным преступление признается с момента возникновения указанных в законе последствий.

Советский районный суд Нижнего Новгорода в пятницу вынес приговор студенту первого курса Нижегородской государственной медицинской академии, гражданину Марокко Адилю Абулиатиму. Как сообщает РИА "Новости", обвинение будущему врачу было предъявлено по двум статьям Уголовного кодекса: статье 165 - "Причинение имущественного ущерба путем обмана" и статье 274 - "Нарушение правил эксплуатации ЭВМ".

Сотрудники милиции задержали Адиля 4 декабря 2000 года в переговорном пункте после того, как он в очередной раз бесплатно позвонил своим родственникам за границу. При помощи манипуляций с пластиковой карточкой, предназначенной для оплаты разговора, студент добивался бесплатного соединения с абонентом. Таким способом, как следует из материалов уголовного дела, марокканец за один месяц нанес телефонной сети ущерб в 67 тысяч 560 рублей. Кроме того, связистам пришлось заниматься перепрограммированием телефонных автоматов, устраняя последствия несанкционированного доступа.

В итоге суд приговорил Адиля Абулиатима к трем годам лишения свободы условно с испытательным сроком в два года. Обвинение в нарушении правил эксплуатации ЭВМ с подсудимого было снято. По решению суда на имущество марокканца и его расчетный счет в банке наложен арест до погашения всей задолженности. Как заявил в ходе заседания суда подсудимый, заняться махинациями его заставило трудное материальное положение. По его словам, за ним числится долг за обучение и проживание в общежитии.

Заключение.

Рассмотрев научную и учебную литературу, автор пришел к следующим выводам:

1) в российской науке уголовного права существует множество трактовок понятия компьютерное преступление. Наиболее четкое определение приводят Максимов, Богомолов. Под компьютерным преступлением понимается противоправное, виновно совершенное, наказуемое в уголовном порядке общественно опасное деяние, причиняющие вред либо создающие угрозу причинения вреда

общественным отношениям по законному использованию компьютерной информации.

2) существует несколько точек зрения относительно того, что представляет собой компьютерное преступление. Одни исследователи считают, что к ним относятся те деяния, объектом или орудием совершения которых является компьютер; при этом кража самих компьютеров рассматривается ими один из способов совершения компьютерных преступлений. Другие относят к компьютерным преступлениям только противозаконные действия в сфере автоматизированной обработки информации (с использованием вычислительной техники, компьютерных информационных сетей, средств и каналов связи.)

3) в УК РФ включены только три состава компьютерных преступлений - неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

4) данный вид преступления был впервые включен в УК.

В данной работе были приведены примеры из судебной практике к каждому из составов преступлений, приведены различные точки зрения.

Список литературы.

1. Конституция Российской Федерации 12.12.1993// РГ от 25 декабря 1993 года; с последними изменениями и дополнениями, внесенными N 7-ФКЗ от 30.12.2008//РГ от 21 января 2009 г. N 7;

2. Уголовный кодекс Российской Федерации №63-ФЗ от 13.06.1996// РГ N 113, 18.06.1996, N 114, 19.06.1996, N 115, 20.06.1996, N 118, 25.06.1996.; с послед. изм. и доп., внесенными Постановлениями Конституционного Суда РФ от 27.05.2008 N 8-П, от 13.07.2010 N 15-П, Федеральным законом от 27.07.2010 N 224-ФЗ// в данном виде опубликован не был.

3. ФЗ РФ № 149 «Об информации, информационных технологиях и о защите информации» от 27.07.2006// РГ №165 от 29.07.2006; с послед изм. и доп., внесенными ФЗ №227 от 27.07.2010// РГ №, в последней редакции ФЗ № 227 от 27.07.2010// РГ №

4. Указ Президента Российской Федерации от 28 июня 1993 г. № 966 «О концепции правовой информатизации России» // САПП РФ. 1993. № 27. Ст. 2521.

5. Компьютерные преступления: определение, объект и предмет Доклад на V Международной конференции «Право и Интернет: теория и практика» Карчевский Николай Витальевич доцент Луганской академии внутренних дел МВД Украины

6. Онлайн Энциклопедия «Кругосвет» [http://www.krugosvet.ru, 2001-2009]. Абрамов, М.А., Авербах, Ю. Л. [Электронное издание

7. Компьютерные преступления: Способы совершения. Методики раскрытия [М.: Право и Закон, 1996]. Вехов В.Б.

8. Седаков, Филлипова

9. ревин

10. Козаченко

11. Кочон

3) Седаков, Филлипова

4) Компьютерные преступления: Способы совершения. Методики раскрытия [М.: Право и Закон, 1996]. Вехов В.Б.

5) Компьютерные преступления: Способы совершения. Методики раскрытия [М.: Право и Закон, 1996]. Вехов В.Б.

6) Онлайн Энциклопедия «Кругосвет» [http://www.krugosvet.ru, 2001-2009]. Абрамов, М.А., Авербах, Ю. Л. [Электронное издание

7) Компьютерные преступления: определение, объект и предмет Доклад на V Международной конференции «Право и Интернет: теория и практика» Карчевский Николай Витальевич доцент Луганской академии внутренних дел МВД Украины

8) Компьютерная преступность и компьютерная безопасность [Юридическая литература, Москва, 1991 - 159 с.]. Батурин, Ю.М.

9) Уголовное право Особенная часть Отв. ред. И Я Козаченко, ЗА Незнамова, Г П Новоселов М , 1998 С 556

10) Иногамова

11) Козаченко

[12] С.А.Пашнин

[13] Посмотреть автора

[14] В.п.РЕВИН

15) В.П.Ревин

16) Указ Президента Российской Федерации от 28 июня 1993 г. № 966 "О концепции правовой информатизации России" // САПП РФ. 1993. № 27. Ст. 2521.

17) Некоторые исключения из этого правила предусматривает ст 8 Федерального закона от 12.08 95 № 144-ФЗ «Об оперативно-розыскной деятельности» с изм на 30.06.2003 (СЗ РФ. 1995 № 33 Ст 3349, 2003. № 27 (ч I) Ст. 2700)

18) Игнатов, Красиков

19) ст. 4 Закона РФ «Об авторском праве и смежных правах» ВВС РФ. 1993. N 32. Ст. 1242.

20) Кочои

21) Кочои

22) Красиков

23) Иногамова

24)Кадникова

25) Ревин

26) Красиков

[27] Иногамова

28) Кадникова

29)Кадникова

30) Козаченко

31)Ревин

32)Кадникова

33)Кадникова

34)Кочои

35)Красиков

36)Иногамова

37) Кадникова

[38] Кочои

[39] Ревин

[40] Ревин

41)Иногамова

42) Кочои

43)Красиков, Игнатов