Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический
институт
Кафедра деликтологии и криминологии
кафедра

УТВЕРЖДАЮ
И.о. заведующего кафедрой
_____ И.А. Дамм
подпись инициалы, фамилия
«____» _____ 2018 г.

БАКАЛАВРСКАЯ РАБОТА
40.03.01 – «Юриспруденция»

Уголовно-правовая и криминологическая характеристика создания, использования и распространения вредоносных компьютерных программ

Научный руководитель _____ старший преподаватель Е.А Акунченко
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ А.О. Зубарев
подпись, дата инициалы, фамилия

Консультант _____ канд. юрид. наук, доцент И.А. Дамм
подпись, дата должность, ученая степень инициалы, фамилия

Красноярск 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Тема: «Уголовно-правовая и криминологическая характеристика создания, использования и распространения вредоносных компьютерных программ». Преступления в сфере компьютерной информации являются новыми и в наше время только приобретают актуальность. Новый вид преступлений стал популярным среди преступных сообществ, так как связан с легким получением «выгоды» и большим шансом остаться незамеченным.

Актуальность рассматриваемой темы с каждым годом возрастает, это вызвано прежде всего несовершенством и отсутствием содержания множества понятий законодательных конструкций, некачественной работой правоохранительных органов по: предупреждению, выявлению и расследованию преступлений, трудностями квалификации данного вида преступлений, снижением раскрываемости с каждым годом. К характерным особенностям компьютерных преступлений можно отнести: высокую латентность преступления и большие размеры причиняемого ущерба. Несомненно, законодатель совершенствует законы, но, как и во многих сферах продолжают существовать проблемы, которые должны постоянно совершенствоваться.

Данная тема изучалась многими отечественными учеными-юристами такими как: Кругликов Л. Л., Евдокимов К. Н., Гаврилин Ю. В., Вехов В. Б., Волеводз А. Г., Дремлюга Р. И., Ищенко Е. П., и иными авторами.

Объектом изучения выступают общественные отношения, которые возникают в сфере уголовно-правовой борьбы с созданием, использованием, распространением вредоносных компьютерных программ.

Предмет изучения: понятие преступления в сфере компьютерной информации, объективные и субъективные признаки, а также детерминанты и предупреждение создания, использования и распространения вредоносных компьютерных программ.

Цель исследования: уголовно-правовой и криминологический анализ нормы, предусматривающей ответственность за создание, использование и распространение вредоносных компьютерных программ.

Задачи исследования:

1. Детально изучить понятие преступления в сфере компьютерной информации и дать общую характеристику данным преступлениям;
2. Раскрыть субъективные и объективные признаки состава данного преступления;
3. Исследовать криминологические показатели создания, использования и распространения вредоносных компьютерных программ;
4. Исследовать субъективные и объективные детерминанты создания, использования и распространения вредоносных компьютерных программ;
5. Исследовать меры предупреждения создания, использования и распространения вредоносных компьютерных программ;

Работа состоит из введения, основной части, заключения и списка использованных источников.

1 Уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ

1.1 Объект и предмет создания, использования и распространения вредоносных компьютерных программ

Для осуществления правоохранительными органами и судами деятельности по расследованию и рассмотрению уголовных дел, необходимо правильно установить объект преступления. Это также важно для криминологической и уголовно-процессуальной наук. Мы можем выявить сущность преступления, условия и причины его возникновения, дать уголовно-правовую квалификацию деянию, установить пределы действия уголовно-правовых норм и отделить преступление от смежных составов.

Рассматриваемая статья содержит достаточно сложный объект. В современном обществе установлены ценностные отношения по поводу применения ЭВМ для обработки данных. Компьютерные системы воспринимаются как благо подлежащее правовой охране.

Разногласий касаемо определения родового объекта у исследователей не возникает, это объясняется тем, что глава о преступлениях в сфере компьютерной информации входит в раздел преступлений против общественной безопасности и общественного порядка УК РФ. Следовательно, общественная безопасность и общественный порядок в сфере компьютерной информации являются родовым объектом рассматриваемого преступления.

А вот взгляды в определении видового объекта создания, использования и распространения вредоносных компьютерных программ разделились.

Например, по мнению В. П. Ревина видовым объектом выступают общественные отношения, нарушающие формирование и использование автоматизированных информационных ресурсов и средств их обеспечения. Данный объект автор решил разделить на несколько частей включающих в себя права и законные интересы:

а) собственников и пользователей информации, компьютеров, их систем и сетей, средств обеспечения;

б) физических и юридических лиц, сведения о которых имеются в автоматизированных информационных ресурсах (банках данных);

в) общества и государства, в том числе интересы национальной безопасности. Кроме того, относительно граждан объектом посягательства может быть здоровье, имущественные права, право на личную тайну и тайну сообщений, честь и достоинства личности и другие. [32, с. 254]

Ю. И. Ляпунов, в качестве видового объекта преступления предлагает рассматривать – совокупность общественных отношений по правомерному и безопасному использованию информации.

С. В. Бородин определяет видовой объект рассматриваемого преступления как, ту часть установленного порядка общественных отношений, которая регулирует изготовление, использование, распространение и защиту компьютерной информации.

По мнению И. А. Клепицкого видовым объектом данного преступления являются – права и интересы физических и юридических лиц, общества и государства по поводу использования автоматизированных систем обработки данных.

Таким образом, на основе вышесказанного можно сделать вывод о том, что мнение ученых совпадают в том, что видовым объектом рассматриваемого преступления являются общественные отношения, в области прав и интересов какой-либо категории по безопасному использованию информационных данных.

Еще более разнообразны подходы к пониманию непосредственного объекта создания, использования и распространения вредоносных компьютерных программ.

Н. Г. Кадников говорит о непосредственном объекте, как о конкретных правах и интересах по поводу использования автоматизированных информационных систем. [26, с.621]

Согласно мнению Е.П. Ищенко, непосредственным объектом преступного посягательства являются базы и банки данных, отдельные файлы компьютерных систем и сетей, а также компьютерные технологии и программные средства, включая те, которые обеспечивают защиту компьютерной информации. [23, с.704]

По мнению В. П. Ревина непосредственным объектом создания, использования, распространения вредоносных программ являются общественные отношения, которые обеспечивают неприкосновенность защищаемой законом информации, имущественные и иные права собственника и других законных владельцев информации, безопасность личности, общества и государства. [32, с.704]

М. А. Ефремова под непосредственным объектом этого преступления понимает общественные отношения по обеспечению безопасности компьютерной информации, а также безопасности средств защиты компьютерной информации. [18, с. 50-52]

Ю. В. Гаврилин считает, что непосредственным объектом рассматриваемого преступления являются общественные отношения по безопасному использованию ЭВМ, ее программного обеспечения и информационного содержания. [13, с. 35]

Б. А. Куринов считает преступление, предусмотренное ч.1, ст. 273 УК РФ двух объектным и выделяет два непосредственных объекта:

Основной непосредственный объект – урегулированные нормами права общественные отношения, обеспечивающие законные права и интересы обладателей компьютерной информации и операторов информационных систем в сфере создания, обработки, обладания, распространения, предоставления, использования компьютерной информации, безопасного функционирования ЭВМ, системы ЭВМ, сети ЭВМ, информационно-телекоммуникационных сетей.

Факультативный непосредственный объект – урегулированные нормами права общественные отношения, обеспечивающие законные права и интересы личности, общества и государства как имущественного, так и неимущественного

характера. Например, это право собственности, экономическая деятельность, авторские и смежные права, изобретательские и патентные права, неприкосновенность частной жизни, жизнь и здоровье, личные права и свободы граждан, общественная и государственная безопасность, конституционный строй и другие.

И. Г. Чекунов придерживается совершенно иной точки зрения по данному поводу. Он отмечает, что данное преступлений, предусмотренное ст. 273 УК РФ имеет цель в виде посягательства не на отношения в сфере безопасного использования компьютерной информации, а на другие объекты, охраняемые уголовным законом, чаще всего на право собственности или основы конституционного строя и безопасности государства. В связи с этим он предлагает декриминализовать использование вредоносной компьютерной программы, так как это деяние входит в объективную сторону других преступлений. [35, с. 27]

Точка зрения о наличии двух непосредственных объектов в ст. 273 УК РФ уже высказывалась рядом авторов, например, Ю. А. Красиковым, И. А. Поповым, и является, по нашему мнению, достаточно емкой и более полно выражающей суть непосредственного объекта создания, использования, распространения вредоносных программ.

Обобщив вышеизложенные мнения, можно сделать вывод:

– родовым объектом рассматриваемого преступления является общественная безопасность и общественный порядок в сфере компьютерной информации;

– видовым объектом являются такие общественные отношения как информационные, которые содержат права и интересы различных субъектов в области функционирования информационной техники и использования компьютерной информации, необходимой для их нормальной жизнедеятельности;

– непосредственным объектом являются – общественные отношения по безопасному использованию компьютера, его программного обеспечения и

информационного содержания. Дополнительным объектом выступают интеллектуальные, имущественные и другие интересы потерпевших.

Проблемой, исследуемой учеными в сфере компьютерной информации, является то, что в результате совершения рассматриваемого преступления останавливается нормальное функционирование компьютерной системы, нарушаются авторские права и законные интересы граждан и юридических лиц, общества и государства, наносится вред собственнику, владельцу или пользователю ЭВМ.

В. В. Воробьев отмечает, что под нарушением работы ЭВМ предлагается подразумевать любую нештатную ситуацию с ЭВМ, системой ЭВМ или их сетью (сбой в работе), препятствующую нормальному функционированию компьютерной техники. [10, с. 17]

По мнению Л. Л. Кругликова общественная опасность создания, использования и распространения вредоносных программ 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. [27, с. 331]

Развитие компьютерных технологий не стоит на месте и очень быстро заполняет все сферы жизни и отрасли деятельности. Поэтому традиционное представление о предмете рассматриваемого преступления нуждается в пересмотре и корректировке.

В уголовном праве предлагают понимать в качестве предмета преступления вещи материального мира, посредством воздействия на которые со стороны виновного причиняется ущерб охраняемым уголовным законом общественным отношениям либо создается реальная угроза причинения такого вреда. [21, с. 79]

Согласно соглашению о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, предметом создания, использования или

распространения вредоносных компьютерных программ для следует признавать вредоносные программы, поскольку обращение именно с этими программами причиняет существенный вред охраняемым уголовным законом общественным отношениям. [4, ст. 1460]

Л. Л. Кругликов, предметом данного преступления считает любую информацию, содержащуюся на машинном носителе, в компьютере или сети. [27, с. 332]

Ю. В. Гаврилин, считает, что предметом рассматриваемого преступления при создании, использовании и распространении вредоносных компьютерных программ является компьютерная информация.

На основе вышеизложенных точек зрения можно сделать вывод, что предметом создания, использования и распространения вредоносных компьютерных программ является компьютерная информация, данное понятие имеет ряд проблем и будет рассмотрено позднее.

1.2 Объективная сторона создания, использования и распространения вредоносных компьютерных программ

Объективная сторона основного состава преступления, предусмотренного ст. 273 УК РФ, включает комплекс действий: создание, распространение или использование вредоносной компьютерной программы (информации).

Названные действия в каждом конкретном случае могут нанести различный вред. Например, от действий проникшего в систему компьютера вируса или иной вредоносной информации может быть нанесен ущерб в виде незначительного увеличения исходящего трафика до полной потери информации, находящейся на компьютере. Могут быть еще более жесткие последствия, вследствие действия вредоносной программы или иной вредоносной информации прекращалась работа организаций, разрушались составные необходимые части для работы компьютера (разрушение процессора). [43]

Правоохранительные органы часто сталкиваются с проблемами в процессе расследования преступлений. Квалификации общественно опасного деяния в сфере компьютерной информации вызывает затруднения, и это обоснованно.

Основной проблемой данного вида преступлений в сфере компьютерной информации является уяснение судьями, прокурорами и следователями понятий, содержащихся в диспозициях ст. ст. 272 – 274 УК РФ возникшая вследствие того, что понятия: «блокирование, модификация, копирование компьютерной информации», «нейтрализация средств защиты компьютерной информации» на законодательном уровне не отражены. Приходится обращаться к комментариям соответствующих статей, где зачастую отражены авторские определения понятий, которые противоречит друг другу, что не позволяет использовать точные формулировки для уголовно-правовой квалификации. [17, с. 24-29]

Рассмотрим более подробно части объективной стороны и определим их понятие.

Под созданием компьютерной программы, заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации, или нейтрализации средств защиты компьютерной информации, а иначе говоря вредоносной компьютерной программы понимается комплекс действий:

1. подготовка исходных данных;

2. которые предназначены для управления конкретными компонентами системы обработки данных в целях, указанных выше в ст. 273 УК РФ.

Следовательно, создание вредоносной программы означает любую деятельность, которая направлена на написание вредоносной программы. Также под созданием вредоносной программы необходимо понимать не только деятельность автора по созданию, но и помощь, оказанную автору другими лицами.

В. В. Малиновский определяет под созданием программы – написание самостоятельного кода или внесение изменений в уже существующий код. В случае внесения изменений в уже существующий код, результатом должно стать

повышение ее эффективности или расширение перечня негативных функций. Разработка соответствующих данных и придание им формы электрических сигналов, является созданием вредоносной компьютерной информации [39]

По мнению С. В. Дьякова, Н. Г. Кадникова создание вредоносной программы или вредоносной компьютерной информации 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. [38]

Необходимо отметить, что в контексте момента окончания преступления исследователи по-разному оценивают действия, которые образуют создание.

Так, подготовку исходных данных во втором определении предлагается оценивать в качестве оконченного преступления, в то время как в первом определении изложена другая точка зрения, тот же комплекс действий рассматривают как покушение на совершение преступления за создание вредоносных компьютерных программ.

Определение, рассматривающее комплекс действий по созданию вредоносной компьютерной программы как оконченное преступление обоснованно тем, что результат, которого стремится достичь лицо, обладающее намерением совершить преступление порождает комплекс действий, имеющих определенное внешнее выражение:

а) постановка цели программы и определение среды ее существования;

б) выбор языка программирования;

в) написание текста;

г) проверка работоспособности программы и ее соответствия

поставленной задаче (при необходимости – отладка);

д) запуск программы. [34, с. 1316-1325]

Л. В. Инагамова-Хегай, согласна с приведенной выше точкой зрения, и рассматривает комплекс действий, направленный на создание вредоносной компьютерной программы аналогичным образом. [22, с. 517]

Более подробно описывает комплекс действий В. Б. Вехов, он делит ее на определенные операции:

1) постановка задачи, определение программно-технической среды существования и целей программы;

2) выбор средств реализации программы – языков программирования;

3) написание алгоритма работы программы в виде исходного текста, то есть описание с помощью того или иного языка программирования порядка (последовательности) обработки данных и команд, управляющих этим процессом;

4) перевод исходного текста программы на машинный язык кодов команд – объектный код, то есть из обычной читаемой человеком формы в ту или иную объективную форму существования компьютерной информации;

5) компилирование программы под определенную операционную систему;

6) отладка программы путем ее запуска с машинных носителей, в памяти компьютерного устройства, в конкретной информационной системе или информационно-телекоммуникационной сети, для работы в которых она и была создана. [8, с. 43-46]

При создании вредоносной программы, наличие вышеперечисленных действий могут являться одним из условий признания деяния уголовно-наказуемым. Полагаем, что вредоносность и полезность компьютерной программы определяется не способностью уничтожать, модифицировать, копировать информацию (легальные программы обладают аналогичными функциями), а тем, предполагает ли их действие:

– во-первых, предварительное уведомление собственника компьютерной информации или другого законного пользователя о характере действия программы;

– во-вторых, получение его согласия (санкции) на реализацию программой своего назначения.

Нарушение одного из этих требований делает программу вредоносной.

Проблема, создания вредоносной компьютерной программы в настоящее время является одной из ключевых, являясь предметом рассуждений не находит четкого понимания, что же понимать под созданием вредоносной компьютерной программы. Одни исследователи рассматривают создание вредоносной компьютерной программы как процесс, который состоит из нескольких этапов. Другие, считают созданием вредоносной компьютерной программы целенаправленный процесс, выражающийся в специальном наборе данных и команд, в последующем которые заведомо предназначены для несанкционированных действий с компьютерной информацией. В данном случае только создание как деяние будет иметь правовые последствия. Следовательно, вредоносная компьютерная программа будет созданной с того момента, когда система команд будет выполнена.

Созданием программы не считается запись ее программного кода на бумаге, так как текст, написанный на бумаге не несет никакой опасности, создать программу с определенным функционалом без ее проверки на компьютере достаточно сложно, и под силу лишь профессионально подготовленному человеку. Более подробно разберем данный вопрос, так как было сказано ранее созданием вредоносной программы признается определенный комплекс действий, направленный на преобразование информации в определенный вид, обладающей конкретно заданным функционалом для несанкционированного уничтожения, блокирования, модифицирования, копирования компьютерной информации или нейтрализовать средства защиты компьютерной информации. Согласно определению, данному в ст. 272 УК РФ, сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Написанный на бумаге программный код, по своим свойствам будет являться информацией, но отнести ее к компьютерной информации нельзя, так как она представлена не в форме электрических сигналов, а в виде записи на бумаге. А вот с момента придания информации формы электрических сигналов, непосредственной проверке ее на компьютере можно говорить о создании вредоносной программы, если она отвечает

дополнительным признакам, для того чтобы программа являлась вредоносной необходимо нарушение хотя бы одного из приведенных ниже условий:

1. предварительное уведомление собственника компьютерной информации или другого законного пользователя о характере действия программы;

2. получение его согласия (санкции) на реализацию программой своего назначения.

Считаем не маловажным тот факт, что создание вредоносной компьютерной программы без ее непосредственного использования не влечет уголовно-правой ответственности. Сама по себе программа хоть и является вредоносной, но не причинила вреда общественным отношения охраняемым уголовным законом. Уголовно-наказуемым деяние становится лишь в том случае, если лицо намеревается ее использовать в противоправных целях, то есть чтобы несанкционированно уничтожить, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации. [20, с. 12-16]

Использование вредоносной программы, В. Б. Вехов определяет, как ее непосредственный выпуск в свет, распространение и иные действия по ее форме [8, с. 43-46]. Иными словами, это 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.

Отметим, четкого единого определения «использование» не существует, мнения на данный счет разделились.

А. Г. Волеводз считает, что использование может осуществляться путем записи программы в память компьютера, на материальный носитель, распространения по сетям либо путем иной передачи другим лицам. [11, с. 70]

Полагаем, что комплекс действий, описанный А. Г. Волеводз включает в себя понятие «распространение».

М. М. Малыковцев под использованием вредоносной программы понимает употребление ее по назначению, приведение в действие, при котором она проявляет свои вредоносные качества. При этом оконченным использование такой программы будет с момента проявления ее вредоносных свойств. [28, с. 91]

Не признается использованием программы для компьютера или базы данных передача средствами массовой информации сообщений о выпущенной в свет компьютерной программе или базе данных. Использование вредоносной программы для личных нужд (например, в целях уничтожения собственной компьютерной информации) ненаказуемо.

На наш взгляд, под использованием вредоносной программы следует понимать запуск такой программы в компьютере с целью ее прямого назначения.

В. Б. Вехов определяет, распространение вредоносных компьютерных программ, как предоставление доступа к воспроизведенной в любой материальной форме программе для компьютера или базе данных, в том числе сетевым и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей. [8, с. 43-46]

М. А. Ефремова дает более краткое определение этого понятия, как передача вредоносной компьютерной программы с помощью специальных носителей, сети, так и иным способом другому лицу. [19, с. 12-16]

Не зависимо от того, как передается программа, на какой основе (коммерческой или иной), каким путем (копирования или передачей совместно с жестким диском), с обозначением функционала программы или нет, посредством интернет-сети или нет, любая из форм будет рассматриваться как распространение. Примером может служить использование преступником чужого компьютера для передачи с заранее подготовленного накопителя, содержащего вредоносную компьютерную программу посредством интернет-сети.

Для квалификации действий по созданию либо внесению модификаций в уже существующие программы как уголовно-наказуемого преступления,

необходимо чтобы деяние создавало реальную угрозу несанкционированного уничтожения, блокирования, модификации либо копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. В ином случае, комплекс действий, направленных на создание, использование или распространение вредоносных компьютерных программ не является уголовно-наказуемым и его нельзя квалифицировать как преступление. Деяние не будет квалифицировано как преступление, если лицо создало вредоносную, но безобидную программу. Например, вирус, который после запуска программы высвечивает на экране монитора картинку и через пару секунд исчезает. В данном случае вредоносная программа не наносит вред собственнику или владельцу информации и не может привести к последствиям, которые указаны в диспозиции ч.1 ст. 273 УК РФ. Такие действия должны быть рассмотрены в силу малозначительности деяния и на основании ч. 2 ст. 14 УК РФ, лицо необходимо освободить от уголовной ответственности. [26, с. 744]

На основе вышеизложенного, считаем необходимым добавить, что после создания вредоносной компьютерной программы, возможно, что она не будет использована, следовательно, не причинит вреда. При использовании и распространении данных программ причинение вреда обязательный признак объективной стороны. Поэтому создание вредоносной компьютерной программы характеризуется меньшей степенью общественной опасности, чем использование и распространение. По объективным причинам, авторы предлагают разделить уголовно-правовую ответственность за данные деяния, распространение и использование необходимо вынести в квалифицированный состав. [17, с. 143]

Для более детального изучения объективной стороны рассматриваемого преступления стоит рассмотреть понятия несанкционированные уничтожение, блокирование, модификация, копирование компьютерной информации и нейтрализация средств защиты компьютерной информации.

В. П. Ревин понимает под уничтожением компьютерной информации – потерю информации, ее утрату при невозможности восстановления в первоначальном виде в конкретном компьютере. [32, с. 200]

В. М. Быков, В.Н. Черкасов имеют другую точку зрения и не согласны с данным определением, так как в настоящее время современные технические средства в ряде случаев позволяют восстановить утраченную информацию полностью или какую-то ее часть. И это не должно освобождать лицо совершившее противоправное деяние от уголовной ответственности. Поскольку преступная цель этого лица оказалась недостигнутой по не зависящим от него обстоятельствам, то его действия следует рассматривать как покушение на уничтожение информации. [7, с. 36]

Под блокированием информации понимается невозможность получить доступ в течение значимого промежутка времени к компьютерной информации ее законному пользователю при сохранности самой информации в памяти компьютера. То есть различные действия и манипуляции лица, которые приводят к тому, что владелец информации временно или постоянно лишается возможности использовать эту информацию и производить с ней различные операции в своих интересах. Например, владелец компьютерной информации лишается возможности своевременно оплатить счет в банке, произвести своевременно заказ на необходимую предприятию технику и совершать другие хозяйственные операции. [7, с. 37] Разблокирование информации может быть осуществлено как в результате чьих-либо действий, так и автоматически, по истечении определенного промежутка времени. Блокирование информации должно продолжаться в течение такого отрезка времени, которого достаточно, чтобы нарушить нормальную деятельность пользователей информации или создать угрозу нарушения этой деятельности.

Под модификацией компьютерной информации следует понимать любые не санкционированные владельцем информации ее изменения, которые препятствуют нормальному и своевременному использованию компьютерной информации. [31, с. 200]

То есть, 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 программу. 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. [9, с. 92-93]

От несанкционированной модификации следует отличать внесение изменений, которые направлены исключительно на адаптацию информации, т.е. внесение таких изменений, которые направлены на приспособление этой информации к функционированию с использованием конкретных технических средств пользователя. Такого рода изменения носят технический характер и не препятствуют использованию компьютерной информации ее владельцем. [7, с. 36]

Под копированием компьютерной информации предлагается понимать несанкционированную запись информации на другой носитель информации. [31, с. 200]

Это посягательство на информацию по своему смыслу очень близко к краже документа и информации. Таким образом, исключительно важная информация может попасть без согласия ее владельца к неизвестному лицу, которое может ее использовать в своих корыстных или иных низменных целях, т.е., по существу, имеет место кража информации. Украденная (скопированная) информация остается и у ее собственника, и у лица, совершившего копирование. Но у компьютерной информации практически нет понятия «подлинник-копия», которое применительно к «бумажным» документам. [36] Поэтому, видимо, законодатель прав, когда в случаях несанкционированного копирования информации не называет это кражей информации. [7, с. 36]

Под нейтрализацией средств защиты компьютерной информации можно понимать полное или частичное уничтожение, нарушение программного

обеспечения, предназначенного для защиты от посягательств и несанкционированного проникновения в информационные системы компьютера, или его сети без возможности их восстановления, либо иное блокирование средств защиты компьютерной информации.

Выше рассмотрены действия, которые подлежат уголовной ответственности, но как уже было указано ранее они не будут являться уголовно-наказуемыми, если не будет одной из составляющих – вредоносной компьютерной программы. Интересно, что слово «вредоносные», кроме названия статьи, нигде более не указано. Видимо, законодатель предполагает под вредоносным воздействием наступление последствий в виде несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. [6, с. 219]

По нашему мнению, довольно полное определение предложено В. П. Ревиным, где под вредоносной программой он понимает специально созданную программу, которая, получив управление, способна совершать несанкционированные пользователем действия и, вследствие этого, причинять вред собственнику или владельцу информации, а также иным лицам в виде уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. [33, с. 255]

Выразим свое согласие с К. Н. Евдокимовым, он отмечает, что вредоносными программами могут быть и обычные лицензионные компьютерные программы в случае их использования при совершении преступного деяния достижения вредных последствий, указанных в ст. 273 УК РФ. [17, с. 61]

Для того, чтобы программа считалась вредоносной, она должна соответствовать следующим критериям:

1. программа способна уничтожать, блокировать, модифицировать либо копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации.

2. программа не предполагает предварительного уведомления собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети о характере своих действий.

3. программа не запрашивает согласия (санкции) у собственника, владельца или пользователя (обладателя) компьютерной информации, компьютерного устройства, информационной системы или информационно-телекоммуникационной сети на реализацию своего назначения (алгоритма).

Если у компьютерной программы хотя бы один из вышеперечисленных признаков будет отсутствовать, то ее нельзя квалифицировать как вредоносную. Заметим, что в законодательстве РФ до сих пор не содержится критериев, позволяющих определить компьютерную программу как вредоносную. Указанное замечание справедливо как для уголовного законодательства, так и для иных отраслей права. Следовательно, по аналогии их необходимо найти в других отраслях права, но ни одна отрасль права не содержит данных критериев. Для того чтобы утверждение о вредоносности программы было обоснованным и имело юридические последствия, необходима программно-техническая экспертизы с соблюдением всех установленных в уголовном судопроизводстве правил. Возникает вопрос, какими правилами должен руководствоваться эксперт, для того чтобы проведенная им экспертиза имела статус доказательства и обладала свойствами относимости и допустимости, и характеристиками достаточности и достоверности. Свойство допустимости в данном случае будет отсутствовать, потому что невозможно определить вредоносность программы без законодательно закрепленного определения, также не представляется возможным, каким именно способом это должен сделать эксперт при проведении экспертизы.

Рассмотрим вопрос о вредоносности программы на примере распространенной в сети интернет программы для активации программного продукта «keygen.exe». Данная программа содержит список ключей, которые необходимы для полного функционирования программного продукта на компьютере. Используя данную программу, пользователь получает один или несколько заранее подготовленных нелицензионных ключей для активации программного продукта, что в последующем позволяет ему пользоваться этим продуктом на равне с пользователем, который приобрел лицензионный ключ для активации программы. Возникает вопрос, является ли данная программа вредоносной. Ранее мы уже рассмотрели критерии отнесения программы к вредоносной, и так как данная программа не предполагает предварительного уведомления собственника, владельца или пользователя (обладателя) о характере своих действий, не запрашивает согласия на такое использование собственника, владельца или пользователя (обладателя) для реализации своего назначения и программа посредством ввода нелицензионного ключа нейтрализует средства защиты компьютерной информации, то она будет являться вредоносной. Так как причиняет вред собственнику данной программы открывая любому владельцу функционал, который защищен средствами защиты компьютерной информации от использования неограниченным кругом лиц.

Сравним данную программу с похожей по своим функциям программой для улучшения программного продукта «Patch.exe». Обладая схожими признаками, программа позволяет пользователю посредством воздействия на оригинальную (лицензионную) программу получить более расширенный функционал. Так как данная программа не предполагает предварительного уведомления собственника, владельца или пользователя (обладателя) о характере своих действий, не запрашивает согласия на такое использование собственника, владельца или пользователя (обладателя) для реализации своего назначения и программа посредством воздействия на оригинальный (лицензионный) программный продукт предоставляет более расширенный функционал, но она не уничтожает, не блокирует, не модифицирует, не копирует

компьютерную информацию и не нейтрализует средства защиты компьютерной информации, то она не будет являться вредоносной.

Отвечая на вопросы квалификации преступления за создание, использование и распространение вредоносных компьютерных программ правоохранительные органы, в частности следователь должны понимать, что каждый случай индивидуален. Для правильной квалификации необходимо знать следующее. На примере личного опыта неясность понятий «компьютерная информация», «нейтрализация средств защиты компьютерной информации», «вредоносная компьютерная программа», «средства защиты компьютерной информации» порождают целый ряд проблем, начиная с неверной квалификации деяния следователем, заканчивая обвинительным приговором судьи. Рассмотрим данный вопрос более детально. По своей структуре преступление, предусмотренное ст. 273 содержит формальный состав единичного сложного преступления, которое включает в себя комплекс действий по созданию, распространению или использованию компьютерной информации, в том числе компьютерных программ заранее предназначенных для несанкционированного уничтожения, блокирования, модификации или нейтрализации средств защиты компьютерной информации.

Явным объективным признаком состава рассматриваемого преступления в ст. 273 УК РФ признается «компьютерная информация». Законодатель закрепил данное определение в законе, что прямо указано в примечании к ст. 272 УК РФ, согласно которому, под «компьютерной информацией» понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. В рассматриваемом преступлении не говорится, что «компьютерная информация должна обладать помимо общих признаков, указанных в примечании к ст. 272, дополнительными, такими как:

1) заведомо предназначена для уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

2) действия должны быть несанкционированными (т.е. без согласия владельца на определенное использование компьютерной информации);

Следующим объективным признаком состава рассматриваемого преступления является «вредоносная компьютерная программа». Что понимать под «вредоносной компьютерной программой» законодатель прямо нигде не указал. По смыслу рассматриваемой статьи предлагается рассматривать под вредоносными, программы, которые способны по своему функционалу несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации. Тем самым причинить вред своим действием компьютерной информации. Возникает вопрос, что считать «средствами защиты компьютерной информации». В законе не предусмотрено, что понимать под «средствами защиты компьютерной информации». Правоприменителю остается только гадать, что же это может быть. Следовательно, если нет четкого определения рассматриваемого понятия, то нести уголовную ответственность за данное деяние лицо не должно т.к. согласно принципу законности, невозможно определить преступность деяния из-за пробела в законодательстве. Это противоречит принципам уголовного кодекса. Законодателю необходимо устранить данный пробел для достижения целей уголовного закона и судопроизводства.

Решая вопрос о понятии «средства защиты компьютерной информации», так как законодатель официально не закрепил данное определение в уголовном законе, обратимся к стандарту «ISO/IEC 2382-1:1993» в котором дается определение понятия «информационная технология» – это практическая деятельность и прикладная наука, имеющие дело с данными и информацией. В примечании к данному определению разъясняется, что примером является сбор, изображение, обработка, обеспечение безопасности, передача, взаимообмен, представление, управление, организация, хранение и восстановление данных и информации. [40, с. 8], далее обратимся к «ГОСТ 33707-2016 (ISO/IEC 2382:2015)» в котором дается трактовка понятия «защита» – средство для

ограничения доступа или использования всей, или части вычислительной системы; юридические, организационные и технические, в том числе программные, меры предотвращения несанкционированного доступа к аппаратуре, программам и данным. [41] Таким образом, можно выделить из данного определения признаки защиты в информационной сфере, ими являются: меры предотвращения от несанкционированного доступа к аппаратуре, программам и данным. Далее обратимся к «ГОСТ Р50922-2006» где содержится определение понятия «Средство защиты информации» – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации. [42]

Объединив вышеперечисленные определения, «средствами защиты компьютерной информации» являются – технические, программные, программно-технические средства для ограничения доступа или использования всей, или части вычислительной системы; меры предотвращения несанкционированного доступа к программам и данным.

1.3 Субъект создания, использования и распространения вредоносных компьютерных программ

Субъектом создания, использования и распространения вредоносных компьютерных программ может быть любое вменяемое лицо, достигшее 16-летнего возраста и обладающее знаниями в области программирования и пользования компьютером.

Субъекты компьютерных преступлений, в том числе осуществляющие создание, использование и распространение вредоносных компьютерных программ, могут различаться по полу, возрасту, уровню их профессиональной подготовки, социальному положению.

Исходя из смысла ст. 19 УК РФ, основными признаками субъекта преступления являются:

1) физическое лицо;

2) вменяемость;

3) достижение возраста уголовной ответственности.

Из содержания ст. 273 УК РФ создание, использование и распространение вредоносных компьютерных программ осуществляется следующими лицами:

Согласно ч. 1 ст. 273 УК РФ субъектом преступления может быть физическое вменяемое лицо, достигшее возраста 16 лет. В юридической литературе по данному вопросу нет особых разногласий.

Так, по мнению проф. А. Н. Попова, «субъект преступления общий – физическое вменяемое лицо, достигшее 16 летнего возраста, которое создало либо использовало, либо распространяло вредоносную программу или машинный носитель с такими программами». [21, с. 749]

Е. А. Маслакова считает, что «субъект рассматриваемого преступления – общий. Им может быть любое вменяемое физическое лицо, достигшее 16-ти летнего возраста». [32, с. 97]

С точки зрения проф. В. М. Быкова и проф. В. Н. Черкасова, «субъектом рассматриваемого преступления, предусмотренного ч. 1 ст. 273 УК РФ, к уголовной ответственности может быть привлечено вменяемое лицо, достигшее 16 лет». [7, с. 20]

Исходя из вышеперечисленных точек зрения у авторов имеется единая точка зрения касаемо субъекта рассматриваемого преступления. Обобщая мнения, субъектом признается любое вменяемое физическое лицо, достигшее 16-ти летнего возраста, совершившее создание, распространение или использование компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

1.4 Субъективная сторона создания, использования и распространения вредоносных компьютерных программ

Состав ч.1 ст. 273 УК РФ является формальным и не требует наступления каких-либо вредных последствий, уголовная ответственность наступает уже в результате создания программы, независимо от того, использовалась эта программа или нет. Достаточно установить сам факт совершения хотя бы одного из обязательных действий, перечисленных в диспозиции указанной части статьи. То есть основанием для привлечения к уголовной ответственности будет служить наличие исходных текстов вирусных программ. Это означает, что для того, чтобы считать преступление оконченным не обязательно наступление вредных последствий, указанных в диспозиции ст. 273 УК РФ, а именно уничтожения, блокирования, модификации, копирования информации.

Считаем важным отметить необходимость учитывать, тот факт, что в некоторых ситуациях использование подобных программ не будет преследоваться по уголовному закону. 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 существующую программу.

Обращаем внимание и на то, что немаловажным фактом создания, использования и распространения вредоносных компьютерных программ обязательно являются активные действия со стороны лица, совершившего данное преступление. Деянием в форме бездействия совершить рассматриваемое преступление невозможно.

2 Криминологическая характеристика создания, использования и распространения вредоносных компьютерных программ

2.1 Криминологические показатели создания, использования и распространения вредоносных компьютерных программ

Решающее место в показателях преступности занимает анализ ее состояния, структуры и тенденций развития. Начальной точкой криминологического исследования является качественно количественная характеристика преступности в целом. Не имея данных по изучаемому виду преступлений, трудно сказать о причинах, последствиях и необходимых мерах борьбы и профилактики.

Для решения данного вопроса были взяты данные с официального сайта Судебного департамента при Верховном Суде Российской Федерации за последние 4 года. [44] и «Главного информационно-аналитического центра» с официального сайта Министерства Внутренних Дел РФ за последние 4 года. [45]

Таблица 1 – Статистика осужденных за создание, использование и распространение вредоносных компьютерных программ

Год	ч.1 ст. 273 УК РФ	ч.2 ст. 273 УК РФ	ч.3 ст. 273 УК РФ
2013	123	75	0
2014	89	63	0
2015	74	90	0
2016	46	76	1

Анализируя данные таблицы можно сделать вывод о том, что в 2013 г. было всего зарегистрировано 2563 преступления в сфере компьютерной информации это самый большой показатель за последние 4 года. В последующие годы темпы роста преступности значительно снизились, но это не является положительной тенденцией, так как рассматриваемый вид преступления является высоко латентным. Из 2563 официально зарегистрированных преступлений, 198 осуждены за создание, использование и распространение

вредоносных компьютерных программ. В 2014 г. из 1739, раскрыто 1321, и осуждено 152, что может говорить о эффективной работе правоохранительных органов за данный период. В 2015 г. темпы роста преступности немного увеличились по сравнению с предыдущим годом, а раскрываемость осталась почти на том же уровне, всего зарегистрировано 1739, раскрыто 1213, и осуждено 164. В 2016 так же прослеживается спад зарегистрированных преступлений, всего учтенных в официальной статистике 1748, раскрыто 903, и осуждено 122. Таким образом проанализировав преступность за данный период времени, коэффициент раскрываемости преступлений за создание, использование и распространение вредоносных компьютерных программ снижается ежегодно, это негативная тенденция и законодателю необходимо обратить на это особое внимание.

Таблица 2 – Статистика зарегистрированных преступлений в сфере компьютерной информации

Год	**ЗАРЕГИСТРИРОВАНО (в отчетном периоде)**		**в том числе**			**Из числа преступлений, дела и материалы о которых находились в производстве:**	
			выявлено сотрудниками ОВД			**РАСКРЫТО**	
	Всего	+, %	Всего	+, %	Уд. вес	Всего	+, %
2013	2563	-9,1	2424	-11,7	94,6	2301	-5,1
2014	1739	-32,3	1643	-32,2	94,6	1321	-42,6
2015	2382	36,9	2217	34,9	93,3	1213	-8,6
2016	1748	-26,6	1539	-30,6	88,0	903	-25,6

Исходя из данных статистики прослеживается снижение преступности по данной статье. Что касается использования и распространения, то это связано со снижением заинтересованности в нелицензионном программном продукте у покупателя, и в повышении уровня правосознания у общества. Что касается

создания, если нет спроса на нелицензионный программный продукт, то и предложение на него будет ничтожно мало.

Уменьшение количества зарегистрированных преступлений еще не хороший признак данного вида преступлений, реальная доля данного вида деяний в ближайшем будущем еще возрастет, так как государство не предпринимает каких-либо мер направленных на сокращение преступных действий по распространению вредоносных компьютерных программ по данной статье. В то же время продолжается рост компьютерной техники и распространение сети интернет. В настоящее время компьютер и интернет есть практически в каждой семье. А это средства совершения рассматриваемого преступления.

Снижение числа осужденных может быть связано с высокой латентностью преступления. Говоря о латентности, необходимо более детально рассмотреть данный вопрос.

Так, например, Н. В. Сазонова предлагает определять латентную преступность как «часть преступности, внешне выраженную в совокупности преступлений, не вошедших в систему государственного статистического учета, характеризующуюся определенными особенностями возникновения и развития, социальным и уголовно-правовым характером, общественной опасностью, имеющую свои качественные и количественные характеристики, временные и пространственные границы» [33, с. 164]

Для исследования латентной преступности необходимо брать во внимание, что основная цель уголовной политики – снижение показателей преступности в обществе. Фактическая преступность будет являться объективным показателем эффективности уголовной политики в совокупности зарегистрированной и латентной преступности в целом, исходя из данных НИИ Академии Генеральной прокуратуры РФ скрытая часть преступности у нас в стране составляет 5/6,[23] что может говорить о актуальности изучаемой проблемы. В научной литературе криминологи по-разному разделяют детерминанты латентности преступлений, разделяя их на группы, виды, совокупности. Это связано с установлением и

изучением определенных закономерностей, характерных латентным преступлениям.

В 1970 году А. М. Алексеев и А. Н. Роша говорили о том, что латентность преступлений можно разбить на виды:

1) естественно-латентная, она возникает, когда правоохранительные органы не знают о факте совершения преступления (иными словами это преступность, которую не раскрыли уполномоченные органы в силу особенностей самих преступлений, не достаточных действий контролирующих органов и бездействий со стороны населения в силу их правовой неосведомленности);

2) искусственно-латентная (иными словами скрываемая преступность), она возникает, когда правоохранительные органы знают о факте совершения преступления, но осознанно не ставят его на учет;

3) латентность пограничных ситуаций – она имеет место, когда о факте совершения преступления известно правоохранительным органам, но не ставится на учет из-за неправильной фактической оценки самого преступления.

Считаем вышеприведенное деление наиболее удачным, данным делением согласно большинство исследователей

В свою очередь Р. М. Акутаев считает, что всю латентную преступность, если брать во внимание выявленные и учтенные преступления и лиц, их совершивших, необходимо подразделять на две группы преступлений:

1) естественно-латентные;

2) искусственно-латентные.

Данный автор считает, что, к естественно-латентным преступлениям относится группа преступлений, которая не стала известна органам и учреждениям, регистрирующим их и осуществляющим преследование виновных, и, вследствие чего не отраженных в уголовной статистике, в последующем в отношении которых не предприняты необходимые меры, которые предусмотрены законом. Автор подразделяет естественно-латентные

преступления, от особенных факторов, которые способствуют естественной латентности преступлений, он делит их на четыре группы:

1) преступления, о совершении которых никто не знает, включая и самого правонарушителя: такие преступления совершаются по небрежности, либо, когда в силу юридической необразованности субъекты правоотношений подменяют одну норму (содержащуюся в уголовном кодексе) другой нормой (нравственной, или содержащейся в КоАП);

2) преступления, в которых потерпевшие специально не сообщают о противоправном деянии из-за того, что незаинтересованны в их раскрытии. Примером может служить изнасилование;

3) преступления, в которых сложно определить потерпевшую сторону, следовательно, и некому заявить о противоправном деянии в уполномоченные органы. Например, экологические преступления;

4) преступления, в которых факт совершения преступления известен малому кругу лиц, либо только преступнику. Примером могут служить взяточничество, убийство с последующим сокрытием трупа, хранение наркотических средств.

Искусственно-латентные преступления создают как известные правоохранительным органам преступления, но не включенные ими в официальную статистику, так и включенные, но не раскрытые, либо не до конца раскрытые.

Которые Р. М. Акутаев делит на две разновидности:

1) неучтенные правоохранительными органами преступления, по которым уголовные дела не возбуждены, хотя информацией о них располагают те или иные учреждения, предприятия, организации, когда информация стала достоянием и правоохранительных органов, но последние не принимают необходимых мер, направленных на законную реализацию этой информации;

2) субъектно-латентные преступления, то есть не раскрытые (неполно раскрытые) преступления, когда сам факт известен и учтен, но неизвестны и не

привлечены к уголовной ответственности лица, совершившее преступление, либо отдельные из них (если преступление совершено в соучастии).

Отличаются они от прочих форм латентности, тем, что разграничение делается по латентности совершившего противоправное деяние субъекта, а не по латентности самого преступления. В аналогичных ситуациях лицо совершившее преступление не несет ответственности в соответствии с уголовным законодательством, в силу того, что это лицо невозможно установить. [5, с. 62-67]

В. В. Лунеев выделяет три группы латентных преступлений:

1) незаявленные преступления, «когда потерпевшие, свидетели, должностные лица и другие граждане, осведомленные о совершенном преступлении, не сообщают этого в правоохранительные органы»;

2)неучтенные преступления, «когда правоохранительные органы, получив сообщение о совершенном преступлении, не регистрируют и не расследуют его»;

3)неустановленные преступления, «когда правоохранительные органы зарегистрировали и расследовали преступление, но в силу недостаточного желания, слабой профессиональной подготовки или ошибочной уголовно-правовой квалификации не установили события или состава преступления».

По мнению В. И. Кириллова и А. А. Старченко указанное деление латентных преступлений представляется не совсем точным, поскольку все названные деяния являются неучтенными. Они считают, что в этом случае происходит «нарушение правила соразмерности деления понятий». Кроме того, третий член деления – «неустановленные преступления» – является видовым по отношению ко второму – «укрытые преступления», что также свидетельствует о наличии деления с лишними членами. Помимо этого, из латентной преступности необоснованно исключены деяния, не зарегистрированные в силу несовершенства нормативного регулирования регистрации преступлений. [25, с. 49]

Достаточно подробная классификация латентных преступлений произведена Б. Дзиовым, который выделяет пять групп латентных преступлений:

1) преступления, о совершении которых не знает никто, либо кто-то может о них лишь догадываться (некоторые неосторожные преступления; незнание лицом, совершающим преступление и потерпевшим, уголовно-правовых норм);

2) преступления, о совершении которых известно только преступнику;

3) преступления, о которых знают только преступник и потерпевший;

4) преступления, о которых известно преступнику, потерпевшему и очевидцам, но никто из указанных лиц не обращается органы противодействия преступности;

5) уголовно наказуемые деяния, информация о которых поступила в правоохранительные органы, либо была выявлена сотрудниками данных органов в результате проведенных мероприятий, но не была должным образом проверена и не нашла отражения в официальных учетах. [15, с. 108]

Именно высокая латентность рассматриваемого преступления, способствует совершению новых преступлений. Совершающий преступление понимает, что найти и наказать его будет очень сложно. Вследствие чего, идет на совершение преступления. Таким образом, полагаем, что необходима четкая процедура по выявлению преступников и общественная огласка после их задержания, чтобы у общества сформировалось мнение, что не так-то просто уйти от наказания за данный вид преступления.

2.2. Субъективные и объективные детерминанты создания, использования и распространения вредоносных компьютерных программ

Детерминация – понятие, производное от слов «детерминант», «детерминировать». Латинское слово determinare означает «определять». Детерминант соответственно означает «определитель», детерминировать – «определять, обусловливать», а детерминация – «процесс обуславливания,

определения». Когда говорят о детерминизме, то имеют в виду признание всеобщей взаимосвязи, взаимодействия всех вещей, объектов, явлений и процессов. Именно в таком значении слово «детерминизм» вошло в русский язык. Причем здесь пока не выделяются разные виды взаимосвязей, хотя их насчитывается более трех десятков. Просто говорят о детерминантах, или «обстоятельствах». [14, с. 234]

Понятие детерминации отражает одну из существенных особенностей бытия – всеобщую связь, взаимозависимость и взаимообусловленность предметов, явлений и процессов. Причинность, как ядро детерминации, в общенаучном плане означает такую связь, в которой одно явление (процесс) при определенных условиях порождает, воспроизводит, продуцирует другое. Наряду с причинностью в систему детерминации входят другие связи, например, функциональные, корреляционные. Из всех видов взаимосвязи детерминации для криминологии наибольшее значение имеют причины и условия.

В литературе криминологические признаки подразделяются на несколько групп:

1. Субъективные, которые включают:

– свойства личности преступника;

– мотив и цель преступления;

– свойства личности потерпевшего;

2. Объективные, включающие:

– статистика преступлений;

– сведения о социальных условиях (обстановке) преступления (социально-политическая; геополитическая; социально-экономическая; время; география и т. п.).

3. Комплексные:

– причины преступлений;

– последствия преступлений;

– механизм преступления;

– обстоятельства, способствующие преступлениям.

Преступность связана со множеством явлений, состояний, процессов. Из них причинами являются лишь те, которые действуют генетически, то есть порождают, воспроизводят преступность как свое следствие. Статистическими наблюдениями зафиксированы зависимость преступности, ее состояния и других характеристик, например, от времени года, половозрастной структуры населения.

Если причины порождают следствие (преступность, преступление), то условия как разновидность детерминации лишь способствуют этому, обеспечивая возможность действия причин. Плохая охрана имущества не порождает корыстные посягательства на него, не вызывает их как следствие, а значит, и не является их причиной, но она создает благоприятную почву – одно из важных условий для совершения краж, грабежей, разбойных нападений. Именно взаимодействие причин и условий приводит к результату (преступлению).

По нашему мнению, говоря о детерминантах компьютерных преступлений, совершаемых на территории России, можно выделить наиболее значимые из них:

1. Продажа нелицензионной продукции и ее высокий спрос у потребителя. Вследствие чего нарушаются авторские и патентные права производителя программного продукта. У потребителя нет возможности обнаружить контрафактный продукт в силу его не компетенции в данном в вопросе, либо при обнаружении потребитель сознательно приобретает такой продукт из-за большой разницы по сравнению с лицензионным в стоимости, так как правило лицензионный продукт стоит в десятки раз дороже нежели контрафактный.

2. С широким распространением интернета и компьютеров, появилась новая категория преступников, использующих вредоносные компьютерные программы с целью получения материальной выгоды. С помощью таких программ преступники проникают в компьютер жертвы и похищают жизненно

важные для владельца компьютерные данные, впоследствии требуя денежное или иное материальное вознаграждение за возврат этих данных.

3. В настоящее время остается не решенной проблема определения ущерба, причиненного вредоносными компьютерными программами. Вопрос, чем должен руководствоваться суд при определении такого ущерба не урегулирован до сих пор. Несовершенство уголовного законодательства в вопросах привлечения за совершение преступления, уголовно-правовая квалификация деяния. Все эти не разрешенные проблемы позволяют преступнику и в дальнейшем совершать преступления.

4. Большая часть уголовных дел за создание, использование и распространение вредоносных компьютерных программ прекращаются на стадии предварительного следствия, ввиду недостатков соответствующих органов дознания и предварительного следствия.

5. Низкая подготовка и уровень знаний у оперативных сотрудников, которые осуществляют розыскную деятельность. Отделы «К», специально созданные для борьбы с преступлениями в сфере компьютерной информации не обладают специальным образованием, позволяющим более эффективно выявлять преступления.

6. Судебная практика по данному вопросу также отсутствует. До сих пор пленум Верховного суда РФ не разъяснил вопросы квалификации и наказания за данный вид преступлений. Что порождает следующую проблему, суды зачастую назначают наказание, которое не соответствует общественной опасности деяния. Судами назначается не связанное с лишением свободы наказание. Например, штраф, условное осуждение ограничение свободы и т.п.

7. Пострадавшие от действий злоумышленников не хотят сообщать о данном факте в полицию. Причиной может быть боязнь потерять репутацию, вследствие разглашения судом информации о данном факте. Преступник, видя такое поведение жертвы, может повторно совершить преступление зная, что ответственности за это не наступит. Из-за такого поведения преступление становится высоко-латентным.

8. Преступления совершаются организованными группами с профессиональной подготовкой.

9. Лицензионные программы стоят в разы дороже, чем их нелицензионные копии. Многие корпорации недовольны этим фактом. Часто копируемой корпорацией является «Microsoft», из-за действий преступников, создающих нелицензионные копии данного программного продукта, она терпит убытки, исчисляемые в миллионах долларов. Это обусловлено тем, что нелицензионные, модифицированные копии программ по своим функциям могут быть лучше оригинальных.

11. Средства массовой информации не контролируются государством в полной мере. Некоторые публикуют информацию, побуждающую лиц на совершение преступления, и иногда даже описывают полный алгоритм действий по преодолению защиты программ от несанкционированного использования. Примером могут служить книги и журналы, содержащие информацию с так называемых обучающих взлому и модификации сайтов.

По нашему мнению, важно повышать уровень правосознания общества, так как компьютерная информация нуждается в защите, также, как и любой другой объект собственности. Нужно прививать обществу мысль о том, что не вся компьютерная информация является общедоступной. Анализ наиболее значимых причин и условий из них позволяет сделать вывод о том, что в данное время продолжает снижаться рост компьютерной преступности. Это положительная тенденция.

3 Предупреждение создания, использования и распространения вредоносных компьютерных программ

3.1 Предупреждение преступлений: понятие и содержание

Для того чтобы разобраться с вопросом предупреждения создания, использования и распространения вредоносных компьютерных программ надо понимать, что из себя представляет предупреждение преступности в общем.

Таким образом, криминологическая теория предупреждения преступности – это учение о совокупности всех законных видов, форм, способов, средств и методов контроля над преступностью независимо от того какой отраслью права они предусмотрены. [37, с. 6]

Предупреждение преступности – это целенаправленное воздействие государства, общества, физических и юридических лиц на процессы детерминации и причинности преступности в целях недопущения вовлечения в преступность новых лиц, совершения новых криминальных деяний, расширения криминализации общественных отношений. [14, с. 435]

Не стоит путать предупреждение с профилактикой, пресечением и предотвращением преступлений. Потому что, предупреждение как более широкое понятие включает в себя профилактику (стадия формирования намерения), предотвращение (стадия приготовления), пресечение (стадия покушения).

Роль значения предупреждения преступления обсуждали древние мыслители Платон и Аристотель, Монтескье и Беккариа, Вольтер и К. Маркс отмечали «Лучше предупреждать преступления, чем карать за них.» С этим мнением нельзя не согласиться, потому что любое современное государство будет стараться остановить преступность на этапе зарождения мыслей о его совершении, нежели карать и наказывать виновных после совершения негативных действий.

Герасимов С. И. отмечает, что под предупреждением преступления следует понимать деятельность государства и общества, направленную против возможного (но еще не задуманного), задуманного (готовящегося), а также происходящего и совершенного преступления. [12, с. 3]

По нашему мнению, данное определение более четко отражает сущность предупреждения преступления. Это обязательно деятельность государства и общества, целью которой является не дать совершить преступление на различных его стадиях.

Говоря о предупреждении преступлений необходимо подразделять ее на виды: общее предупреждение преступлений, специальное и индивидуальное.

Общее предупреждение преступности – это система мер по устранению процессов детерминации и причинности преступности, воздействующих на все население или его группы, выделяемые по общим экономическим, социальным, иным критериям, и создающих вероятность преступного поведения практически всех представителей этих социальных групп.

Специальное предупреждение преступности – система воздействия на процессы детерминации и причинности преступности, касающиеся отдельных социальных групп, сфер деятельности и объектов, характеризующихся повышенной вероятностью совершения преступлений. Особое внимание уделяется тем, которые могут быть особо привлекательными для преступников, либо тем, в которых сосредоточиваются, формируются и действуют преступники.

Индивидуальное предупреждение преступлений – это, прежде всего, воздействие на тех лиц, от которых можно ожидать совершения преступлений, а также на окружающую их социальную среду. Данный вид деятельности представляет собой целенаправленную работу с конкретным человеком и его ближайшим окружением.

Одним из элементов индивидуального предупреждения преступления, является недопустимость замышляемого или готовящегося лицом уголовно-

наказуемого деяния, склонение к добровольному отказу от его совершения является предотвращением.

Для предупреждения преступления необходимо определить вид предупредительных мер, соответствующий виду криминогенной деформации и выбрать меру воздействия.

Меры предупреждения преступности могут классифицироваться по различным признакам. Рассматривая меры предупредительного воздействия можно выделить четыре основные группы:

1. меры стимулирования (поощрения),
2. меры наказания (ответственности),
3. меры восстановления (компенсации),
4. меры безопасности (защиты).

Различие их состоит в методе, непосредственных целях, основаниях, содержанию, субъектах и сроках применения.

Меры стимулирования – это предоставление различных благ за определенные общественно полезные действия (заслуги). В уголовном праве поощрение реализуется устранением обременений в ответ на общественно полезное поведение. Поощрительным последствием позитивного поведения является и юридическое признание.

Создание системы стимулов, побуждающих людей подчиняться закону и делающих выгодным именно законопослушное поведение, на наш взгляд, в плане предупреждения преступлений, более значимо, чем принуждение. Любой гражданин должен иметь законные возможности для обеспечения нормальной жизни, для удовлетворения своих минимальных потребностей. В противном случае он вынужден прибегнуть к криминальным способам.

Одним из эффективных средств социального управления является предоставление режима наибольшего благоприятствования для законопослушных граждан и организаций, которые соблюдают закон. К сожалению, в России чаще используют не пряник, а кнут.

Основой социальной профилактики являются всеобразные виды стимулирования, методы с помощью которых у личности формируется правильное правовое восприятие, более эффективны по сравнению с мерами наказания.

По существу, социальная профилактика преступлений – это один из видов социальной работы. Это – социальная, медицинская, психологическая и материальная помощь, повышение культурного, общеобразовательного и профессионального уровня, трудовое и бытовое устройство. Исчерпывающий перечень всех разновидностей социальной профилактики займет очень много места.

Можно сказать, что в нее входят все виды воздействия, кроме принудительных, к которым относятся меры наказания, восстановления и безопасности. Меры восстановления (компенсации) направлены на «устранение вреда, причиненного противоправным деянием общественным отношениям, на исполнение невыполненных обязанностей». Они включают: принудительное исполнение обязанности, отмену незаконных актов и обязанность возместить ущерб. Тем самым воссоздается система правоотношений, нарушенная невыполнением предписаний закона обязанными субъектами. В большей степени эта группа мер присуща гражданско-правовой отрасли. Но она используется и в уголовном праве, где восстановление осуществляется возложением обязанности загладить причиненный вред.

Принуждая правонарушителя к заглаживанию вреда, возмещению ущерба, компенсационные меры одновременно служат удовлетворению справедливых требований жертвы, восстановлению социальной справедливости. Большой предупредительный потенциал восстановительных мер российской криминологией пока недооценивается. Между тем во многих странах профилактические проекты «компенсация вместо наказания» «примирение вместо наказания» пользуются значительной популярностью и имеют применительно к некоторым видам преступлений хороший предупредительный эффект.

Традиционно сложилась точка зрения под наказанием понимать принудительное лишение определенных благ, соответствующее совершенному деянию. Нарушитель, понимая, что за совершение общественно опасного деяния он будет лишен определенных благ, в большинстве случаев он не станет совершать противоправные действия. Таким образом достигаются цели общего и специального предупреждения. Самым важным средством предупреждения преступности рассматривают наказание. Общество наблюдая за наказанием, будет сдерживаться от преступных действий. Но наказание это всего лишь один из видов предупреждения преступности, остальные виды воздействия по большей степени не берутся во внимание и их эффективность до сих пор не изучена.

Меры безопасности, понимают, как применяемые в целях предотвращения вредоносного воздействия источника опасности, принудительные меры, ограничивающие поведение и определенную деятельность, которые применяются в отношении физических и юридических лиц. Меры безопасности также не изучены полностью.

Также необходимо определить объект предупреждения преступления.

В криминологической литературе в качестве объекта предупреждения преступления рассматривают:

1. личность профилактируемого,
2. отклоняющееся поведение,
3. личность в своих связях с микросредой,
4. преступные группы,
5. места концентрации лиц с преступным поведением,
6. территории городов или даже государственные образования,
7. социально-криминогенное пространство,
8. негативные социальные процессы, в общем, любые криминогенные явления. [37, с. 24]

3.2 Основные направления предупреждения создания, использования и распространения вредоносных компьютерных программ

На настоящий момент выделяются две основные группы мер предупреждения компьютерных преступлений: правовые и организационно-технические.

В группу правовых мер относят нормы законодательства, устанавливающие уголовную ответственность за противоправные деяния в компьютерной сфере.

Нормативно-правовым актом, устанавливающим уголовную ответственность за совершение преступлений в сфере компьютерной информации на территории Российской Федерации, является Уголовный кодекс РФ. Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ установлена ч. 1 ст. 273 УК РФ.

Кроме того, другие федеральные законы также имеют значение при определении правовых мер по предупреждению рассматриваемого преступления, поскольку они дают юридическое определение основных компонентов информационной технологии как объектов правовой охраны; устанавливают и закрепляют права и обязанности собственника на эти объекты; определяют правовой режим функционирования средств информационных технологий; определяют категории доступа определенных субъектов к конкретным видам информации и другое.

Таким законами, в частности, являются Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ и Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

Отметим, поскольку на настоящий момент уголовно-правовое законодательство России в области преступлений в сфере компьютерной информации характеризуется наличием пробелов и несовершенством юридической терминологии, то законодателю необходимо непрерывно и быстро отслеживать и реагировать на изменения в техническом прогрессе. Необходимо

устранять неопределенность норм, регулирующих ответственность в области преступлений в сфере компьютерной информации.

Организационно-технические меры предупреждения рассматриваемого преступления предполагают:

1) предотвращение утечки, хищения, утраты, искажения и подделки информации;

2) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и системы;

3) обеспечение правового режима функционирования документированной информации как объекта собственности;

4) сохранение конфиденциальности документированной информации.

5) обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

В. В. Овчинский предлагает предупреждать преступность в сфере компьютерной информации со стороны поставщиков услуг Интернета и хостинга. По мнению автора, поставщики услуг имеют важную роль в предупреждении преступлений в сфере компьютерной информации. Автор предлагает классифицировать их следующим образом:

1. хранение данных пользователей, к которым впоследствии могут получить доступ правоохранительные органы, чтобы использовать эти данные в расследовании киберпреступлений;

2. активная «фильтрация» информационного обмена в Интернете или содержания данных, прежде всего в целях предупреждения киберпреступлений. [30, с. 228]

Далее анализируются технические и нормативные аспекты этих направлений.

Также В. В. Овчинский предлагает осуществлять фильтрацию содержания данных в целях предупреждения совершения преступлений в сфере компьютерной информации. Необходимо чтобы, провайдеры Интернета блокировали доступ к незаконному контенту, такому как детская порнография. Существуют различные способы, с помощью которых провайдеры Интернета могут это делать, причем разные методы предполагают разные варианты выбора с точки зрения сочетания скорости, стоимости, действенности и точности. Применение фильтров DNS позволяет поставщикам услуг Интернета контролировать ответы, которые DNS серверы направляют их абонентам, и ограничивать доступ к домену, такому как Google.com, но не к конкретной странице или набору результатов поиска. Такие ограничения легко обойти, поскольку пользователи могут просто использовать альтернативные серверы DNS, которые дадут подлинные результаты. Для определенного компьютера можно использовать фильтрацию по IP адресу, чтобы частично блокировать определенные сервисы. На одном интернет сервере может размещаться большое количество веб сайтов, что может повлиять на не связанные с проблемой веб сайты, причем иногда их число может быть очень велико. Также автор предлагает применять углубленную проверку пакетов, которая может применяться для анализа основного массива компьютерной информации содержания интернет трафика. Такой подход как заверяет В. С. Овчинский очень эффективен, но в тоже время он требует дорогостоящего оборудования, которое приходится устанавливать на высокоскоростных каналах ISP и которое может замедлять прием компьютерной информации и в целом соединения всех абонентов. Для сокращения стоимости оборудования и увеличения эффективности данных мер автор предлагает объединить два режима фильтрации. Более простые фильтры, например, на основе DNS, часто используются для выявления трафика, который следует направить для проверки более сложными фильтрами. Такой объединенный подход обеспечивает сложную фильтрацию, которая будет эффективнее при значительном сокращении необходимых ресурсов. [30, с. 232]

Фильтрация интернет контента. Помимо содействия предупреждению преступности за счет возможностей, связанных с хранением данных, поставщики услуг Интернета также могут принимать участие в деле предупреждения киберпреступности за счет активного анализа информационного обмена в Интернете и передаваемых при этом данных. В связи с этим одной из основополагающих концепций является фильтрация интернет контента поставщиками услуг Интернета. Фильтрация интернет соединений имеет место на определенном уровне практически в любой сети. Самый простой уровень фильтрации, используемый для повышения эффективности работы и безопасности сети, состоит в блокировании неверных или иным образом поврежденных данных. Провайдеры Интернета также могут иметь технические возможности для фильтрации данных на предмет определенного вредоносного или незаконного контента. Например, многие провайдеры Интернета могут применять базовые спам фильтры для фильтрации сообщений в электронной почте их абонентов и обеспечивать защиту от хорошо известного вредоносного трафика, связанного с вирусами или преступными атаками на основной сервер, отказываясь передавать далее трафик, отнесенный к этой категории. [30, с. 233]

ЗАКЛЮЧЕНИЕ

Данная норма имеет ряд проблем, начиная с пробелов в законодательстве, заканчивая высокой латентностью данного вида преступлений, которые негативно влияют на уголовное правосудие.

В результате быстрого развития высоких технологий сформировался новый вид общественных отношений - информационные. Указанные отношения стали новым объектом, а информация - новым предметом преступного посягательства. Результатом появления новых общественных отношений стали компьютерные преступления, которые являются реальной угрозой для общества. Отличие указанных преступлений от «традиционных» создало ряд проблем при определении общих понятий, а также при их расследовании.

Проведенные исследования в рамках данной темы выявили ряд специфических черт данной категории преступлений.

Таким образом, я выяснил, что понятие «компьютерные преступления» гораздо шире, чем «преступления в сфере компьютерной информации». Последнее можно определить, как умышленные общественно опасные деяния, создающие вред либо возможную угрозу причинения вреда общественным отношениям по безопасному использованию компьютера, его программного обеспечения и информационного содержания. Уголовный Кодекс Российской Федерации впервые установил норму, объявляющую общественно опасным деянием создание, использование и распространение вредоносных компьютерных программ. Множество вопросов вызвала объективная сторона рассматриваемого вида преступления, так как при квалификации деяния невозможно воспользоваться единым источником. Для решения этой проблемы было проанализировано законодательство и сформулированы некоторые термины, не отражённые законодателем.

В результате исследования, проведенного в рамках данной работы был выявлен ряд проблем: высокая латентность данного вида преступлений, отсутствие четких понятий и разъяснения законодателя по многим проблемным

вопросам, таких как термин «компьютерная информация», «нейтрализация средств защиты компьютерной информации», «средства защиты компьютерной информации», «вредоносная компьютерная программа» и других понятий, отсутствие единого подхода к определению непосредственного объекта рассматриваемого преступления, а так же относительно содержания объективной стороны и другие. Было выяснено что, объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит лишь орудием посягательства.

Широкое развитие высоких технологий в сфере компьютерной информации привело к кардинальному изменению мира, сделало его цифровым и информационным. Но в это же время это негативно коснулось всех сфер нашей жизни и породило разные виды интернет преступности. Двадцать первый век - век высоких технологий. И, конечно, все более стремительно будут появляться новые проблемы в сфере компьютерной информации, и разрабатываться способы их решения.

В рамках исследования выявлены и изучены следующие проблемы:

1. Несовершенство норм уголовного закона, отсутствие определения понятий: «нейтрализация средств защиты компьютерной информации», «средства защиты компьютерной информации», «вредоносная компьютерная программа (информация)».
2. Снижение раскрываемости данного преступления с каждым годом.
3. Высокая латентность вследствие неэффективной деятельности правоохранительных органов и государства.

По нашему мнению, наиболее актуальные проблемы на сегодняшний день освещены в данной работе. Таким образом, можно сделать вывод, что существует необходимость совершенствования уголовно-правовой защиты компьютерной информации в связи с постоянно возрастающим значением и широким применением компьютера во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации. Со стороны государства не предпринимается мер по устранению пробелов в

законодательстве, это может негативно сказаться на эффективности уголовного судопроизводства.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // СЗ РФ. 2014. № 31. Ст. 4398.

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 17.04.2017) // СЗ РФ. 1996. № 25. Ст. 2954.

3. Федеральный Закон от 27 июля 2006 года № – 149 «Об информации, информационных технологиях и защите информации» [Электронный ресурс] // СПС «Консультант Плюс». – Режим доступа: www.consultant.ru.

4. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Собрание законодательства РФ. №13. 2009. Ст. 1460.

Специальная литература

5. Акутаев Р. М. Криминологический анализ латентной преступности: дис. … д-ра юрид. наук. СПб, 1999. 358 с.

6. Бегишев И. Р. Создание, использование и распространение вредоносных компьютерных программ // Проблемы права. 2012. № 3. С. 218 – 222.

7. Быков В. М., Черкасов В. Н. Новое об уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ. // Российский судья. 2012. № 7. С. 35 – 39.

8. Вехов В. Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. 2015. № 2. С. 43 – 46.

9. Вехов В. Б., Голубев В. А. Расследование компьютерных преступлений в странах СНГ / под ред. проф. Б. П. Смагоринского. Волгоград, 2004. 304 с.

10. Воробьев В. В Преступления в сфере компьютерной информации: юридическая характеристика составов и квалификация: автореферат дисс. … кан. юрид. наук. Нижегородская академия Министерства внутренних дел РФ. Нижний Новгород, 2000. 28 с.

11. Волеводз А. Г. Противодействие компьютерным преступлениям. М.: Юрлитинформ, 2002. 315 с.

12. Герасимов С. И. Предупреждение преступности: теория, опыт, проблемы // Законность. № 2. 2002. С. 2 – 7.

13. Гаврилин Ю. В., Головин А. Ю., Кузнецов А. В., Толстухина Т. В. / Под ред. Ю. В. Гаврилина. Преступления в сфере компьютерной информации: квалификация и доказывание. Москва. Издательство «Книжный мир», 2003. 245 с.

14. Долгова А. И. Криминология. Учебник для вузов. 3-е изд., перераб. и доп. М.: Норма, 2005. 912 с.

15. Дзиов Б. Латентная преступность в контексте практики предупреждения и раскрытия преступлений // Латентная преступность: познание, политика, стратегия. Сборник материалов международного семинара. М.: Изд-во ВНИИ МВД России, 1993. С. 103 – 117

16. Евдокимов К. Н. Актуальные вопросы уголовно-правовой квалификации преступлений в сфере компьютерной информации // Российский следователь. 2015. № 10. С. 24 – 29.

17. Евдокимов К. Н. Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты. Иркутск: Иркутский юридический институт (филиал) Академии Генеральной прокуратуры РФ, 2013. 267 с.

18. Ефремова М. А. К вопросу о понятии компьютерной информации // Российская юстиция. 2012. № 7. С. 50 – 52.

19. Ефремова М. А. К вопросу об уголовной ответственности за создание, распространение и использование вредоносных компьютерных программ // Информационное право. 2015. № 3. С. 12 – 16.

20. Звечаровский И. Э. Уголовное право России: особенная часть: учебник. М.: Норма-Инфра, 2010. 976 с.

21. Иногамова-Хегай Л. В. Уголовное право Российской Федерации: общая часть. Москва, 2006. 559 с.

22. Иногамова-Хегай Л. В., Рарог А. И., Чучаев А. И. Уголовное право Российской Федерации. Особенная часть: учебник для вузов. Изд. испр., доп. М.: Инфра-М, 2008. 795 с.

23. Ищенко Е. П. Криминалистика. М.: Инфра-М Контакт, 2010. 781 с.

24. Иншаков С. М. Латентная преступность как показатель эффективности уголовной политики // Российский следователь. 2008. № 14. С. 73 – 78.

25. Кириллов В. И., Старченко А. А. Логика. М.: Юристъ, 1995. 623 с.

26. Кадников Н. Г. Уголовное право. Общая и Особенная части. М.: Городец, 2006. 911 с.

27. Кругликов Л. Л. Уголовное право России. Особенная Часть. М.: Издательство «Волтерс Клувер», 2005. 464 с.

28. Малыковцев М. М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ. Москва, 2006. 186 с.

29. Маслакова Е. А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты. Орел, 2008. 198 с.

30. Овчинский В. С. Криминология цифрового мира: учебник для магистратуры. Москва. Издательство: Норма, 2018. 347 с.

31. Питулько К. В., Коряковцев В. В. Уголовное право. Особенная часть. СПб., 2010. 256 с.

32. Ревин В. П. Уголовное право России. Особенная часть. М.: «Юстицинформ», 2010. 496 с.

33. Сазонова Н. В. Латентная преступность: понятие, причины, измерение: дис. … канд. юрид. наук. Красноярск, 2004. 210 с.

34. Энгельгард А. А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) // LexRussica. 2014. № 11. С. 1316 – 1325.

35. Чекунов И. Г. Некоторые особенности квалификации преступлений в сфере компьютерной информации // Российский следователь. 2012. № 3. С. 26 – 28.

36. Черкасов В. Н. Дискретность интеллектуальной собственности, или с чего начинается копия? // Защита информации. Инсайт. 2011. № 2(38). С. 35 – 37.

37. Щедрин Н. В. Основы общей теории предупреждения преступности / Учебное пособие. Красноярск: КГУ. 1999. 56 с.

38. Комментарий к Уголовному кодексу РФ (научно-практический, постатейный) / Под ред. Дьякова С. В, Кадникова Н. Г., 2013 [Электронный ресурс] // СПС «Гарант». – Режим доступа: http://www.garant.ru.

39. Комментарий к Уголовному кодексу РФ для работников прокуратуры (постатейный) / Отв. ред. В. В. Малиновский, науч. ред. А. И. Чучаев. Москва, 2012 [Электронный ресурс] // СПС «Гарант». – Режим доступа: http://www.garant.ru.

Стандарты и другие нормативные акты

40. Стандарт ISO/IEC2382-1:1993. Термины и определения. Стокгольм. 1993. 42 с.

41. ГОСТ 33707-2016 (ISO/IEC 2382:2015). Информационные технологии (ИТ). Словарь. Москва. Стандартинформ. 2016. 206 с.

42. ГОСТ Р50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения. Москва. Стандартинформ. 2006. 12 с.

Интернет-ресурсы

43. URL: http://www.securelist.com/ru/a№alysis.
44. URL: http://www.cdep.ru/
45. URL: https://мвд.рф

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический
институт
Кафедра деликтологии и криминологии
кафедра

УТВЕРЖДАЮ
И.о. заведующего кафедрой
_____ И.А. Дамм
подпись инициалы, фамилия
«13» 06 2018 г.

БАКАЛАВРСКАЯ РАБОТА
40.03.01 – «Юриспруденция»

Уголовно-правовая и криминологическая характеристика создания, использования и распространения вредоносных компьютерных программ

Научный руководитель _____ старший преподаватель Е.А Акунченко
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ А.О. Зубарев
подпись, дата инициалы, фамилия

Консультант _____ канд. юрид. наук, доцент И.А. Дамм
подпись, дата должность, ученая степень инициалы, фамилия

Красноярск 2018