Министерство образования и науки российской федерации

Государственное образовательное учреждение

высшего профессионального образования

"Тамбовский государственный университет им. Г.Р.Державина"

Академия открытого образования и инновационного предпринимательства

Кафедра уголовного права и процесса

Преступления в сфере компьютерной информации: уголовно-правовой и криминологический анализ

Дипломная работа

Студентка 5 курса

Заочного отделения

Зайцева Екатерина Владимировна

Научный руководитель:

Копырюлин А.Н.,

Тамбов - 2010г

Содержание

Реферат

Обозначения и сокращения

Введение

1. Уголовно-правовая характеристика составов преступлений в сфере компьютерной информации и проблемы их квалификации

1.1 Компьютерная информация как объект уголовно-правовой охраны

## 1.2 Неправомерный доступ к компьютерной информации: состав преступления, проблемы квалификации

## 1.3 Создание, использование и распространение вредоносных программ для ЭВМ, состав преступления, проблемы квалификации

## 1.4 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети: состав преступления, проблемы привлечения к ответственности

2. Криминологический аспект преступлений в сфере компьютерной информации

2.1 Криминологическая характеристика личности преступника

2.2 Факторы, способствующие совершению преступлений в сфере компьютерной информации

2.3 Меры по предупреждению преступлений в сфере компьютерной информации

2.4 Международное сотрудничество в борьбе с преступлениями в сфере компьютерной информации

Заключение

Список литературы

Реферат

Зайцева Е.В. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический анализ. Дипл.работа / Зайцева Екатерина Владимировна; Тамб. Гос. Ун-т им. Г.Р. Державина; кафедра уголовного права и процесса. – Тамбов, 2010. – 77с.

Ключевые слова: компьютерная информация, неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ, нарушение правил эксплуатации ЭВМ, проблемы квалификации.

Объектом исследования выступают общественные отношения, подвергающиеся посягательствам в результате совершения неправомерного доступа к компьютерной информации. Предмет исследования включает в себя уголовно-правовые и криминологические аспекты преступлений в сфере компьютерной информации; совокупность мер по предупреждению преступлений в сфере компьютерной информации.

Цель исследования состоит в комплексном уголовно-правовом и криминологическом научном исследовании характерных черт и предупреждения преступлений в сфере компьютерной информации в Российской Федерации. Основными задачами исследования являются анализ норм права, устанавливающих уголовную ответственность; исследование проблемы квалификации преступления и проблемы привлечения к уголовной ответственности; раскрытие основных причин и условий, способствующих совершению преступлений в сфере компьютерной информации. Представлены общие рекомендации по защите компьютерной информации; определена роль организационно-правовых мер предупреждения преступности. Актуальность работы обусловлена практической значимостью вопросов, связанных со становлением и развитием в современной России действенных механизмов обеспечения информационной безопасности.

Обозначения и сокращения

ФЗ – Федеральный закон

СЗ РФ – Собрание Законодательства Российской Федерации

ФЗ РФ – Федеральное Собрание Российской Федерации

УК РФ – Уголовный кодекс Российской Федерации

УПК РФ – Уголовно-процессуальный кодекс Российской Федерации

ГК РФ – гражданский кодекс Российской Федерации

ст. – статья

ч. - Часть

п. – пункт

ред. – редакция

см. – смотри

ЭВМ – электронно-вычислительная машина

Введение

Актуальность темы исследования обусловлена теоретической и практической значимостью вопросов, связанных со становлением и развитием в современной России действенных механизмов обеспечения информационной безопасности. Открытия в различных областях науки, развитие информационно-коммуникационных технологий (ИКТ), технологическое перевооружение промышленности привели к кардинальным переменам в мире, обусловили переход к новому типу общества — обществу информационному. Основное содержание ныне происходящих преобразований связывают с процессами создания, обработки, хранения и использования информации во всех сферах общественной жизни. Информация становится одним из важнейших ресурсов.

Правовые проблемы, связанные с различными сторонами формирования и развития информационного общества, информатизации исследовались в работах таких ученых, как И.Л. Бачило, В.С. Беляева, И.Ю. Жукова, О.В.Щербакова, А.Б. Венгерова, В.А. Копылова, И.С. Мелюхина, М.М. Рассолова и других.

Компьютеризация ознаменовала современную эпоху научно-технического прогресса. Но наряду с бесспорными положительными сторонами компьютеризации, охватившей практически все сферы нашего общества, она имеет и негативные стороны, в частности появление новых видов преступлений — преступлений в сфере компьютерной информации. По своему механизму, способам совершения и сокрытия эти преступления имеют определенную специфику, характеризуются высочайшим уровнем латентности и низким уровнем раскрываемости.

Их появление застало врасплох общество. Правоохранительные органы, оказавшись не вполне готовыми к адекватному противостоянию и борьбе с этим новым социально-правовым явлением, в частности, по причине отсутствия четких научно обоснованных рекомендацией по квалификации преступлений в сфере компьютерной информации.

Преступления в сфере компьютерной информации, несмотря на их, пока незначительный удельный вес в общей структуре преступности, представляют реальную угрозу не только отдельным пользователям электронно-вычислительной техники, но и в целом национальной безопасности страны, поскольку они все больше приобретают транснациональный организованный характер. За 2007г.-7236 совершено 7236 преступлений в сфере компьютерной информации, из них раскрыто – 6614. За 2008г. совершено 9010 преступлений в данной сфере, из них раскрыто-8419 (на 24% больше). В последующий год статистика неуклонно растет, как видно из количества зарегистрированных преступлений за 2009г.-10575, из них раскрыто-9991 (на 43,6% больше). Всего лишь в первом квартале 2010г. преступлений в данной сфере было зарегистрировано 11918 (из них 1230 – в январе, 3634 – в феврале, 2541 – в марте и 4513 – в апреле), среди которых раскрыто 10488 (более 88 %).

Анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Статистические данные также свидетельствуют о том, что, несмотря на относительно небольшой удельный вес преступлений в сфере компьютерной информации в общей структуре преступности, количество их постоянно растет.

Принятие УК РФ поставило ряд проблем перед теоретиками уголовно-правовой науки: определить объект преступлений в сфере компьютерной информации, сформулировать их понятие и систему; установить критерии выделения близких по содержанию видов преступных посягательств, отграничение от других составов преступлений; решить вопрос квалификации, а также ответственности и наказания за них.

Бланкетный характер диспозиций соответствующих уголовно-правовых норм требует обращения к различным правовым актам, регулирующим возникающие правоотношения, и знания терминологии.

За время, прошедшее со времени вступления в действие Уголовного кодекса Российской Федерации, в теории и в практике применения норм о преступлениях в сфере компьютерной информации обозначился ряд проблем, которые не стали пока предметом комплексного исследования.

Отсутствие отечественной судебной практики существенно затрудняет проведение глубокого анализа данного вида преступной деятельности, проведение криминологической экспертизы норм о преступлениях гл. 28 УК РФ.

Трудности в ряде случаев вызваны сложностью, а подчас недостаточной продуманностью некоторых законодательных решений. В юридической литературе неоднократно отмечались те или иные недостатки, неточность, неконкретность, неясность, несовершенство, неопределенность положений главы 28 УК РФ.

Несмотря на теоретическую и практическую значимость этих проблем исследований, посвященных именно уголовно-правовым и криминологическим аспектам практически не проводилось.

В настоящее время в основном исследования носят фрагментарный характер. Их результаты выражены преимущественно в статьях, или небольших по объему единичных работах, как правило, посвященных либо только уголовно-правовым аспектам, либо только криминологическим.

В то же время возникает необходимость проведения исследований в данной области с учетом нового уголовного законодательства России.

Нуждаются в более детальной проработке вопросы профилактики неправомерного доступа к компьютерной информации. Их разработка приведет к повышению эффективности борьбы с преступлениям данного вида.

 Недостаточная изученность криминологической характеристики неправомерного доступа к компьютерной информации, не разработанность системы мер предупредительного характера и вопросов виктимологической профилактики, необходимость совершенствования уголовного законодательства, комплексный анализ правовых и организационно-технических мер противостояния неправомерному доступу к компьютерной информации предопределили выбор темы дипломной работы и актуальность.

Объектом исследования данной работы являются общественные отношения, подвергающиеся посягательствам в результате совершения неправомерного доступа к компьютерной информации.

Предмет исследования включает в себя: преступность в сфере компьютерной информации, как новый объект уголовно-правового регулирования, ее состояние, структуру и динамику; криминологические аспекты преступлений в сфере компьютерной информации; совокупность мер по предупреждению преступлений в сфере компьютерной информации; правовые, организационно-технические методы защиты от преступлений в сфере компьютерной информации.

Цель работы заключается в комплексном уголовно-правовом и криминологическом научном исследовании генезиса, состояния, тенденций, характерных черт и предупреждения преступлений в сфере компьютерной информации в Российской Федерации. Цель опосредует более конкретизированные задачи исследования:

- проанализировать нормы права, устанавливающие уголовную ответственность за преступления в сфере компьютерной информации;

-исследовать проблемы квалификации преступления и проблемы привлечения к уголовной ответственности;

- установить основные особенности личности компьютерных преступников, совершающих преступления в сфере компьютерной информации;

- раскрыть основные причины и условия, способствующие совершению преступления в сфере компьютерной информации;

- представить общие рекомендации по защите компьютерной информации на объектах информатизации и рекомендации по защите компьютерной информации;

- определить роль организационно-правовых мер предупреждения неправомерного доступа к компьютерной информации;

- подготовить предложения по совершенствованию системы мер предупредительного характера — уголовно-правовых и организационно-технических, направленных на улучшение их применения в противостоянии преступлениям в сфере компьютерной информации.

Данная работа не претендует на подробное изложение всех характеристик преступлений, т.к. степень разработанности данной проблемы недостаточна на сегодняшний момент. Необходимость досрочной разработки юридических основ информационных отношений привела к поспешному и не всегда корректному формированию ряда базовых правовых понятий в этой области с их уточнением в каждом следующем нормативном акте. Сейчас, когда создан и принят ряд базовых нормативных актов в области информационных отношений, наступило время для их применения на практике. Теоретической основой данной работы явились труды отечественных ученых-правоведов, специалистов в области уголовного права, криминологии, и информатики: Крылова В.В., Дворецкого М.Ю., Карелиной М.М., Батурина Ю.М., Баева О.Я., Ястребова Д.А.,Ушакова С.И., Кузнецова А.П., Козлова В.Е., Борзенкова, Г.Н., Комиссарова В.С., Ведеева Д.В., Беляева В.С. и др., а также работы зарубежных специалистов: Д. Айкова, Дж.Вейценбаума, Н.Винера, Д.Керра, Д.Макнамара, С. Мэдника,и др.

Нормативную базу составили Конституция Российской Федерации, действующее уголовное законодательство Российской Федерации, законы РФ, акты Президента РФ, Правительства РФ.В качестве эмпирической базы при подготовке работы использовались статистические данные, полученные на официальном сайте статистики ГИЦ МВД России.

Методологической основой исследования послужили общенаучные методы познания, а также частно-научные методы:

- историко-правовой - применительно к изучению исторического опыта по установлению уголовной ответственности за совершение преступлений в сфере компьютерной информации;

- формально-логический, заключающийся в детальном анализе уголовно-правовых и организационно-технических мер противостояния неправомерному доступу к компьютерной информации;

- статистический, включающий сбор и анализ статистических данных о неправомерном доступе к компьютерной информации.

Структура работы включает в себя введение, 2 главы и заключение. Отдельные главы работы посвящены исследованию компьютерной информации, как предмету уголовно-правовой защиты, подробному уголовно-правовому и криминологическому анализу преступлений в сфере компьютерной информации, а также международному и отечественному опыту борьбы с компьютерными преступлениями.

1. Уголовно-правовая характеристика составов преступлений в сфере компьютерной информации и проблемы их квалификации

# 1.1 Компьютерная информация, как объект уголовно-правовой охраны

Стремительное развитие информационных и коммуникационных технологий а также компьютеризация мирового сообщества вообще, вызвало острую необходимость включения в правовую систему Российской Федерации юридических норм, которые бы регулировали общественные отношения, подвергающиеся посягательствам в результате совершения преступлений в сфере компьютерной информации. Непосредственно Российское информационное законодательство начало формироваться с начала 90-х годов и включало в себя ряд основополагающих законов: Закон "О средствах массовой информации", Закон "О Федеральных органах правительственной связи и информации", Закон "О правовой охране программ для электронных вычислительных машин и баз данных", утративший силу с 1 января 2008г., Закон "Об информации, информатизации и защите информации", Закон "Об участии в международном информационном обмене", Закон "О правовой охране программ для электронно-вычислительных машин и баз данных", утративший силу с 1 января 2008г.

Начиная с 1 января 2008г. правоотношения, возникающие в сфере сбора, обработки, накопления (хранения) и передачи информации, а также использование компьютерной техники, средств хранения информации (носителей информации) и каналов связи (телекоммуникаций) регулируются Частью четвертой Гражданского кодекса Российской Федерации, которая состоит из одного раздела VII "Права на результаты интеллектуальной деятельности и средства индивидуализации". Раздел, посвященный правовому регулированию отношений в сфере интеллектуальной собственности, представляет собой включение всех существенных норм действующих федеральных законов в один законодательных акт. При этом в сферу интеллектуальной собственности вводится ряд принципиально новых субъектов отношений и определения их прав, в частности это относится к правам изготовителя баз данных.

В данных законодательных актах были определены основные термины и понятия в области компьютерной информации, регулировались вопросы ее распространения, охраны авторских прав, имущественные и неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием программного обеспечения и новых информационных технологий.

Также было осуществлено законодательное раскрытие понятий информационной безопасности и международного информационного обмена.

Но в определенных случаях правоприменитель сталкивался с трудностями при реализации правовых предписаний. В связи с этим анализ законодательства, регулирующего информационные отношения, показал, что необходимо более детальное исследование правового содержания и сущности понятий, которые касаются одновременно и описания элементов информационных отношений и отношений, регулируемых уголовным законом [36,с.12]

Российское законодательство определяет информацию как "сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их предоставления".[12] Несмотря на кажущуюся простоту данного определения, уяснение сущности понятия "информация" - дело непростое, поскольку это понятие широко и не всегда однозначно используется и в законодательстве, и в литературе, и в обиходной речи.

Например, в специализированном курсе "Информатика" утверждается, что термины "сообщение" и "информация" - основные понятия информатики, однако "содержание указанных понятий не может быть достигнуто с помощью определения, так как последнее лишь сводило бы эти понятия к другим не определенным основным понятиям".[21,с.86]

В "Толковом словаре по вычислительной технике и программированию" указано, что информация - одно из первичных, не определяемых в рамках кибернетики понятий[36,с.68].

Отметим, что использование означенного термина обычно предполагает возникновение материально-энергетического сигнала, воспринимаемого сенсорно или на приборном уровне. В таких случаях обычно информация превращается в сообщение. Для того чтобы информация могла получаться и передаваться, необходимы приемник и передатчик сведений или устройство связи [71,с.24]. Относительно природы информации существует еще ряд мнений и точек зрения специалистов как из информационной, так и из юридической сферы. На наш же взгляд законодатель вполне приемлемо разрешает данный вопрос, а именно: устанавливает четкие правовые требования и формы для того, что подлежит охране в установленном законодательством порядке.

Таким образом, как вытекает из анализа действующего законодательства, правовой защите подлежит главным образом документированная информация (документ), зафиксированная на материальном носителе с реквизитами, т. е. информация, которая облечена в форму, позволяющую ее "идентифицировать".[39]

Документированная информация описывается как "организационная форма, которая определяется как единая совокупность: а) содержания информации; б) реквизитов, позволяющих установить источник, полноту информации, степень ее достоверности, принадлежность и другие параметры; в) материального носителя информации, на котором ее содержание и реквизиты закреплены".

По мнению В.А. Копылова, понятие "документированная информация" основано на "двуединстве - информации (сведений) и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения. В результате документирования происходит как бы материализация и овеществление сведений".[53,с.23] Отсюда можно сделать вывод, что информация становится объектом Гражданского законодательства.

Между тем отечественное уголовное законодательство обеспечивает правовую защиту наряду с документированной информацией и иным ее разновидностям и, следовательно, расширяет представление о предмете криминальной деятельности (о чем речь пойдет далее). Анализ действующего Уголовного кодекса РФ показывает, что законодатель выделил из всего объема информационных отношений как подлежащие специальной охране отношения, возникающие в области компьютерной информации. В главу о преступлениях в сфере компьютерной информации введены термины и понятия, которых ранее не было не только в уголовно-правовой терминологии, но и в законодательстве, регулировавшем информационные отношения. Поэтому эти термины и понятия требуют определенных пояснений, основанных на осмыслении технических характеристик новых средств обработки информации и сущности самой компьютерной информации как новой уголовно-правовой и криминалистической категории.[19,c.52] Вне всякого сомнения, исследование терминов, употребляемых при описании преступных деяний в сфере компьютерной информации, полезно, но не подлежит сомнению и то, что наиболее важными (базовыми) здесь являются понятия "информация" и "компьютерная информация".

Проанализировав нормы из различных отраслей права можно сделать ряд выводов:

1. Информацией является совокупность предназначенных для передачи формализованных знаний и сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

2. Правовой защите подлежит любая документированная информация, т.е. информация, облеченная в форму, позволяющую ее идентифицировать

3. Документированная информация является объектом уголовно-правовой защиты.

4. Информация может быть конфиденциальной, ознакомление с которой ограничивается ее собственником или в соответствии с законодательством, и массовой, предназначенной для неограниченного круга лиц.

5. Ограничения (установление режима) использования информации устанавливаются законом или собственником информации, которые объявляют степень (уровень) ее конфиденциальности.

Конфиденциальными в соответствии с законом являются, в частности, такие виды информации, как:

содержащая государственную тайну (Закон РФ "О государственной тайне" ст.ст.275, 276, 283, 284 УК РФ);

передаваемая путем переписки, телефонных переговоров, почтовых телеграфных или иных сообщений (ч.2 ст.23 Конституции РФ, ст.138 УК РФ); касающаяся тайны усыновления (ст.155 УК РФ);

содержащая служебную тайну (ст.139 ГК РФ), коммерческую тайну (ст.139 ГК РФ и ст.183 УК РФ), банковскую тайну (ст.183 УК РФ), личную тайну (ст.137 УК РФ), семейную тайну (ст.137 УК РФ), информация, являющаяся объектом авторских и смежных прав (ст.1255 часть 4 Гражданского кодекса РФ) [49,с.288];

6. Любая форма завладения и пользования конфиденциальной документированной информацией без прямо выраженного согласия ее собственника (за исключением случаев, прямо указанных в законе) является нарушением его прав, т.е. неправомерной.

7. Неправомерное использование документированной информации наказуемо.

Новое российское уголовное законодательство включает в себя ряд неизвестных ранее составов преступлений, среди которых есть нормы, направленные на защиту компьютерной информации. Необходимость установления уголовной ответственности за причинение вреда в связи с использованием именно компьютерной информации (т.е. информации на машинном носителе, в электронно-вычислительной машине, системе ЭВМ или их сети) вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации по сравнению, скажем, с информацией, зафиксированной на бумаге и хранящейся в сейфе. Составы преступлений приведены в 28 главе УК РФ, которая называется "Преступления в сфере компьютерной информации" и содержит три статьи: "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).

Совершенно оправданно то, что преступления данного вида помещены в раздел IX "Преступления против общественной безопасности и общественного порядка", т.к. последствия неправомерного использования информации могут быть самыми разнообразными: это не только нарушение неприкосновенности интеллектуальной собственности, но и разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений нормальной деятельности предприятия, отрасли и т.д. Ряд понятий и определений, используемых в данной главе УК РФ требует конкретизации. Необходимый уровень проработки и разъяснения данных понятий дан известным специалистом в этой области Карелиной М.М.[43]

1. ЭВМ (компьютер) - устройство или система (несколько объединенных устройств) предназначенное для ввода, обработки и вывода информации;
2. Сеть ЭВМ - совокупность компьютеров, средств и каналов связи, позволяющая использовать информационные и вычислительные ресурсы каждого компьютера включенного в сеть независимо от его места нахождения;
3. Компьютерная информация - в дополнение к определению, данном в ст. 2 закона "Об информации, информатизации и защите информации", необходимо заметить, что применительно к комментируемым статьям под компьютерной информацией понимаются не сами сведения, а форма их представления в машинном (компьютерном) 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.
4. Программа для ЭВМ (компьютера) - 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;
5. 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.

Особенно удачным видится определение Компьютерной информации, которое дается Доцентом кафедры криминалистики МГУ им. М.В. Ломоносова В.Крыловым, предлагающим следующее криминалистическое определение компьютерной информации как специального объекта преступного посягательства.

Компьютерная информация есть сведения, знания или набор команд (программа), предназначенные для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях - идентифицируемый элемент информационной системы, имеющей собственника, установившего правила ее использования.[55]

Таким образом, общим объектом компьютерных преступлений будет выступать совокупность всех общественных отношений, охраняемых уголовным законом; родовым - общественная безопасность и общественный порядок; видовым - совокупность общественных отношений по правомерному и безопасному использованию информации; непосредственный объект трактуется, исходя из названий и диспозиций конкретных статей. Необходимо различать, 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. Последняя точка зрения высказывалась ранее некоторыми авторами[74,с.37].

Принятие ее означало бы излишнее расширение рамок понятия "компьютерное преступление" и затруднить работу не только законодателя, но прежде всего правоприменителя. Разработчики УК РФ пошли по первому пути, четко сформулировав составы главы 28 таким образом, что Компьютерная Информация в каждом случае является только предметом совершения компьютерного преступления. Но представляется правильным и следующее - при использовании компьютерной информации в качестве средства совершения другого преступления отношения по ее охране страдают неизбежно, т.е. она сама становится предметом общественно опасного деяния. Невозможно противоправно воспользоваться компьютерной информацией для совершения иного преступления, не нарушив при этом ее защиты, т.е. не совершив одного из действий, перечисленных в ст. 20 Федерального закона "Об информации, информатизации и защите информации": утечки, утраты, искажения, подделки, уничтожения, модификации, копирования, блокирования и других форм незаконного вмешательства в информационные ресурсы и системы.

Даже если не пострадают сведения конкретного компьютера, правомерно употребляемые ее законным пользователем, практически неизбежно подвергнутся ущербу те, с которыми она связана сетью. Таким образом, даже при совершении такого классического преступления, как хищение денег с помощью электронных средств, ответственность за это должна наступать по правилам идеальной совокупности преступлений.

Характеризуя объективную сторону рассматриваемых составов, необходимо заметить в первую очередь, что даже большинство из них конструктивно сформулированы как материальные, поэтому предполагают не только совершение общественно опасного деяния, но и наступление общественно опасных последствий, а также обязательное установление причинной связи между этими двумя признаками.[31,с.43] Однако в силу ч. 2 ст. 9 УК РФ, временем совершения каждого из этих преступлений будет признаваться время окончания именно преступного деяния независимо от времени наступления последствий. Сами же общественно опасные деяния чаще всего выступают здесь в форме действий и лишь иногда - как бездействие. Из всех признаков субъективной стороны значение будет иметь только один - вина. При этом, исходя из ч. 2 ст. 24, для всех преступлений данного вида необходимо наличие вины в форме умысла. Представляется, что особую трудность вызовет проблема отграничения неосторожного и невиновного причинения вреда, что связано с повышенной сложностью и скрытностью процессов, происходящих в сетях и системах ЭВМ.

Диспозиции статей 28-й главы описательные, зачастую - бланкетные или отсылочные. Так, для применения ряда их необходимо обратиться к ст. 35 УК РФ, к нормативно-правовому акту об охране компьютерной информации, правилам эксплуатации ЭВМ и т.п. Санкции - альтернативные, за исключением двух квалифицированных составов, где они - в силу тяжести последствий преступления – "урезаны" до относительно-определенных. В главу 28 (Преступления в сфере компьютерной информации) группу входят нормы, которым не может быть придана обратная сила - т.е. те, которыми устанавливается преступность деяния, усиливается наказание либо иным образом ухудшается положение лица (обвиняемого, подсудимого, осужденного, отбывшего наказание).

## 1.2 Неправомерный доступ к компьютерной информации: состав преступления, проблемы квалификации

Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем. [46,с.13]

Данная статья защищает право лиц на неприкосновенность информации в системе. Владельцем информационной вычислительной системы (и информации в ней) может быть любое лицо, правомерно пользующееся услугами по обработке информации как собственник вычислительной системы (ЭВМ, сети ЭВМ) или как лицо, приобретшее право использования системы (информации). по ст.1280 4части ГК РФ[47.с.72]. Данная статья защищает компьютерную информацию любых предприятий, учреждений, организаций и частных лиц. Диспозиция соответствующей нормы заключается в неправомерном доступе к охраняемой законом компьютерной информации. Преступное деяние, ответственность за которое предусмотрено ст. 272 должно состоять в неправомерном доступе к охраняемой законом компьютерной информации, который всегда носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств позволяющих преодолеть установленные системы защиты; незаконного применения действующих паролей или маскировка под видом законного пользователя для проникновения в компьютер, хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

Под охраняемой законом информацией понимается информация, для которой законодательно установлен специальный режим ее правовой защиты, например - государственная, служебная и коммерческая тайна, персональные данные и т.д.[11] Неправомерным является доступ, противоречащий действующим правовым нормам, актам управления, приказам, распоряжениям и иным актам, регулирующим отношения по доступу лиц (группы лиц) к информации.[71] Кроме того, неправомерным будет доступ, если лицо незаконно использовало технические средства для проникновения в ЭВМ и (или) ее сеть, например введение чужого пароля либо снятие необходимого пароля, модификация программы и пр. Под неправомерным доступом к охраняемой законом компьютерной информации следует понимать также самовольное получение информации без разрешения ее собственника или владельца.

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

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

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

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

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

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

1. уничтожения информации, то есть удаление информации на материальном носителе и невозможность ее восстановления на нем;
2. блокирования информации, то есть совершение действий приводящих к ограничению или закрытию доступа к компьютерной системе и предоставляемым ею информационным ресурсам;
3. модификации информации, то есть внесение изменений в программы, базы данных, текстовую информацию находящуюся на материальном носителе;
4. копирования информации, то есть переноса информации на другой материальный носитель, при сохранении неизмененной первоначальной информации;
5. нарушения работы ЭВМ, системы ЭВМ или их сети, что может выразиться в нарушении работы как отдельных программ, баз данных, выдаче искаженной информации, так и нештатном функционировании аппаратных средств и периферийных устройств, либо нарушении нормального функционирования сети. [72]

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

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

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

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

Объект - общественные отношения, связанные с безопасностью использования компьютерной информации.[65]

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

- 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;

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

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

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

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

Однако такой подход будет противоречить нормам ст.24 УК РФ, согласно которой деяние, совершенное только по неосторожности, признается преступлением лишь в том случае, когда это специально предусмотрено соответствующей статьей Особенной части УК. Следовательно, неправомерный доступ к охраняемой законом компьютерной информации, содержащий признаки неосторожной формы вины, преступлением не является. В диспозиции ст.272 УК РФ законодателем прямо указывается на характер действия (доступа) – в отношении компьютерной информации, охраняемой законом, он должен носить неправомерным, если "лицо не имеет права на доступ к данной информации; лицо имеет право на доступ к данной информации, однако осуществляет его помимо установленного порядка, с нарушением правил ее защиты". Когда лицо сознает, что совершает доступ к компьютерной информации, не имея на это права или хоть и имеет право, но нарушает при этом режим доступа, оно поступает общественно опасно. В этом случае указанные действия виновного " легко укладывается в формулу прямого или косвенного умысла". Данное лицо предвидит также и возможность наступления указанных в законе общественно опасных последствий и желает их наступления (прямой умысел) или допускает эти последствия, либо относится к ним безразлично (косвенный умысел).

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

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

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

С субъективной стороны преступление характеризуется наличием прямого умысла (осознание неправомерного доступа, предвидение наступления вредных последствий и желание их наступления) или косвенного умысла (осознание неправомерного доступа, предвидение наступления вредных последствий и сознательное допущение их наступления либо безразличное отношение к наступлению последствий) Неправомерный доступ к компьютерной информации - умышленное деяние, поскольку в диспозиции ст.272 УК не указано обратное. [71, с.134] Человек, пытающийся получить доступ к информации, должен сознавать, что свободный доступ к информации ограничен, он не имеет прав на доступ к этой информации. Об умысле будут свидетельствовать меры защиты информации от доступа посторонних (коды, пароли и т.п.), которые приходится преодолеть, чтобы получить доступ к информации, вывод на экран дисплея компьютера предупреждающих сообщений, устные уведомления о запрете доступа к информации и т.д.[72, с.24]

Субъектами данного преступления в основном могут являться лица, имеющие опыт работы с компьютерной техникой, и поэтому в силу профессиональных знаний они обязаны предвидеть возможные последствия уничтожения, блокирования, модификации информации либо нарушения работы ЭВМ, системы ЭВМ и их сети. По общему правилу субъектами преступления, предусмотренного ст. 272, может быть лицо, достигшее 16-летнего возраста, однако часть вторая ст.272 предусматривает наличие специального субъекта, совершившего данное преступление. [78]

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

А) не имеющими права на доступ к компьютерной информации в данных условиях места и времени, но осуществляющими "неправомерный доступ к охраняемой законом компьютерной информации" (ч. 1 ст.272);

Б) совершающими неправомерный доступ группой по предварительному сговору или организованной группой (ч.2ст.272);

В) совершающими неправомерный доступ, используя для этого свое служебное положение (ч.2ст.272);

Г) имеющими право доступа к ЭВМ, системы ЭВМ или их сети, но использующими это право в целях достижения преступного результата (уничтожение, блокирование, модификации либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети).

Преступления от иных видов преступных посягательств, связанных с

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

Согласно части 1 статьи санкция основного состава альтернативно предусматривает три вида наказаний: штраф, исправительные работы и лишение свободы. Первый, в свою очередь, может быть двух видов: до двухсот тысяч рублей или кратный размеру зарплаты или иного дохода осужденного за период до восемнадцати месяцев). Исправительные работы могут быть назначены в размере от шести месяцев до одного года, а лишение свободы - до двух лет.

Санкция же согласно части 2 статьи ужесточена: в нее введен новый вид наказания (арест на срок от трех до шести месяцев), размеры остальных увеличены: штраф от ста тысяч до восьмисот тысяч или зарплаты за период от одного года до двух лет; исправительные работы на срок от одного года до двух лет; лишение свободы до пяти лет. Все виды наказаний - как ч. 1, так и ч. 2 - основные и не исключают возможность присоединения какого-либо из дополнительных видов, перечисленных в п. п. 2 и 3 ст. 45, кроме штрафа и конфискации имущества.

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

Для преступления, предусмотренного ст. 272 УК, суть общественно опасного деяния заключается в неправомерном доступе к компьютерной информации. Причем состав неправомерного доступа к компьютерной информации в отличие от создания, использования и распространения вредоносных программ для ЭВМ сконструирован как материальный. Оконченным это преступление будет только тогда, когда наступят вредные последствия, лежащие в причинной связи с поведенческим актом виновного.

##

## 1.3 Создание, использование и распространение вредоносных программ для ЭВМ, состав преступления, проблемы квалификации

Статья 273 предусматривает ответственность за создание и распространение различного рода компьютерных "вирусов" и других программ, которые могут нарушить целостность информации, нарушить нормальную штатную работу компьютера, сети ЭВМ. Под использованием либо распространением вредоносных программ или машинных носителей к ним понимается соответственно введение этих программ в ЭВМ, систему ЭВМ или их сеть, а также продажа, обмен, дарение или безвозмездная передача другим лицам.[63,с.408] Статья защищает права владельца компьютерной системы на неприкосновенность и целостность находящейся в ней информации. Во-первых, компьютерный вирус может быть и безвредным для информации, требующей гарантированной целостности. Во-вторых, существует большое количество типов программ, приводящих к крайне нежелательным последствиям, но они не попадают под традиционное понимание "компьютерного вируса". [22, с.86]

Под вредоносными программами в смысле ст. 273 УК РФ понимаются программы специально созданные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, определенные в документации на программу. Наиболее распространенными видами вредоносных программ являются "компьютерные вирусы" и "логические бомбы". [18, с.64]

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

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

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

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

Состав части 1 формальный и предусматривает совершение одного из действий:

1) создание программ (очевидно, вернее – "программы") для ЭВМ, заведомо приводящих (приводящей) к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы аппаратной части;

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

3) использование двух названных видов программ;

4) их распространение;

5) использование машинных носителей с такими программами;

6) распространение таких носителей.

Хотя данный состав является формальным и не требует наступления каких-либо последствий, уголовная ответственность возникает уже в результате создания программы, независимо от того использовалась эта программа или нет. [50] Создание вредоносных программ для ЭВМ в технологическом смысле идентично этапам создания любых других программ и является целенаправленной деятельностью, включающей в себя:

1) постановку задачи, определение среды существования и цели программы;

2) выбор средств и языка программирования;

3) непосредственно написание текста программы;

4) проверку соответствия работоспособности программы и ее соответствия работоспособности программ и ее соответствие поставленной задаче;

5) подготовку программы к использованию.

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

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

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

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

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

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

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

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

При установлении прямого умысла в действиях виновного преступление подлежит квалификации в зависимости от цели, которую перед собой ставил последний, или когда наступили последствия - то в зависимости от наступивших последствий. В этом случае действия, предусмотренные статьей окажутся лишь способом достижения поставленной цели и совершенное деяние подлежит квалификации по классической совокупности совершенных преступлений.[20, с.14] Необходимо также учитывать, что преступление может быть также совершено как по неосторожности в виде легкомыслия, так и с косвенным умыслом в виде безразличного отношения к возможным последствиям.

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

1.Создание программ для ЭВМ, заведомо приводящих к общественно опасным последствиям.

2.Внесение изменений в существующие программ для ЭВМ, заведомо приводящих к общественно опасным последствиям.

3.Использование таких программ или машинных носителей с такими программами.

4.Распространение таких программ или машинных носителей с такими программами.

Данные действия виновного заведомо приводят к несанкционированному уничтожении, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. Высокая степень общественной опасности создания, использования и распространения вредоносных программ для ЭВМ обусловливает формирование законодателем данного состава преступления как формального, когда сам факт создания компьютерного вируса либо совершения иного из указанных в ч.1 ст.273 УК РФ действий, составляющих объективную сторону этого состава, является вполне достаточным для ч.1 ст 273 УК РФ действий, составляющих объективную сторону этого состава, является вполне достаточным для привлечения лица к уголовной ответственности. Наступления общественно опасных последствий в данном случае значения для квалификации не имеет.

Санкция части 1 предусматривает один основной вид наказания (лишение свободы на срок до трех лет) и один дополнительный (штраф в размере до двухсот тысяч рублей или зарплаты либо иного дохода лица за период до восемнадцати месяцев).

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

Санкция второй части данной статьи - относительно-определенная: лишение свободы на срок от трех до семи лет. Таким образом, именно это преступление из всей главы относится к категории тяжких.

Особого внимания заслуживает вопрос об отграничении неправомерного доступа к компьютерной информации от создания, использования и распространения вредоносных программ для ЭВМ. Сложность этого вопроса заключается в том, что и неправомерный доступ к компьютерной информации, и создание, использование и распространение вредоносных программ для ЭВМ ведут к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. Причем создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к указанным выше вредным последствиям, вполне могут сочетаться с неправомерным доступом к компьютерной информации, что еще раз свидетельствует о прикладном характере разграничения этих преступлений. Во-первых, как уже было отмечено выше, предметом преступления, предусмотренного ст. 272 УК, является только та информация, которая охраняется законом. Предметом же создания, использования и распространения вредоносных программ для ЭВМ является любая информация (как охраняемая законом, так и неохраняемая), содержащаяся на машинном носителе, к ЭВМ, системе ЭВМ или их сети.

Так, например, по ст. 273 УК следует квалифицировать действия виновного, совершившего неправомерный доступ к программе для ЭВМ, не имеющей специального правого статуса (т.е. не охраняемой законом), если это деяние было связано с ее модификацией, заведомо приводящей к вредным последствиям, указанным в диспозиции статьи УК. Признаки состава неправомерного доступа к компьютерной информации в этом случае отсутствуют. Вторым критерием, позволяющим разграничить неправомерный доступ к компьютерной информации от создания, использования и распространения вредоносных программ для ЭВМ, является содержание общественно опасного деяния.[44,с.12] Последнее из указанных преступлений предполагает совершение хотя бы одного из следующий действий:

А) создание вредоносной программы (вредоносных программ) для ЭВМ;

Б) внесение изменений в существующие программы для ЭВМ, доводя их до качества вредоносных;

В) использование вредоносных программ для ЭВМ;

Г) использование машинных носителей, содержащих вредоносные программы;

Д) распространение машинных носителей, содержащих вредоносных программ;

Е) распространение машинных носителей, содержащих вредоносные программы.

При этом следует обратить внимание на то, что, согласно буквы и смысла закона, состав преступления, предусмотренный ч.1. ст. 273 УК, сконструирован как формальный. Следовательно, для признания преступления оконченным не требуется реального наступления вредных последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Достаточно установить сам факт совершения общественно опасного деяния, если оно создавало реальную угрозу наступления альтернативно перечисленных выше вредных последствий. В том случае, когда виновный умышленно создает вредоносную программу для ЭВМ или вносит изменения в существующую программу, доводя ее до качества вредоносной, а равно использует либо распространяет такие программы или машинные носители с такими программами и при этом не совершает неправомерного доступа к охраняемой законом компьютерной информации, то его действия подлежат квалификации по ст. 273 УК.[50, с.560]. Однако, на практике вполне допустима ситуация, когда виновный в целях создания вредоносной программы для ЭВМ, неправомерно вызывает существующую программу, являющуюся, скажем, объектом авторского права, а значит, охраняемую законом, и вносит в нее соответствующие изменения (например, добавляет или удаляет отдельные фрагменты программы, перерабатывает набор данных посредством их обновления и.т.д.), иными словами, модифицирует компьютерную информации. В этом случае налицо совокупность преступлений предусмотренных ст. ст. 272 и 273 УК. Объясняется это тем, что диспозиция ст. 273 УК, говоря о создании программ для ЭВМ, внесении изменений в существующие программы, использование либо распространение таких программ или машинных носителей с такими программами, не охватывает своим содержанием факт неправомерного доступа к охраняемой законом компьютерной информации.

Следовательно, деяние виновного подлежит дополнительной квалификации пост.272 УК Оконченный состав неправомерного доступа к компьютерной информации следует оценивать поведения лица, которое, неправомерно вызвав существующую программу для ЭВМ и внеся в нее ряд изменений, не сумело в силу различного рода причин, выходящих, за рамки сознания и воли виновного, довести эту программу до качества вредоносной. Если же действия виновного были пресечены на более ранней стадии, например, в момент неправомерного доступа к информации, и не были связаны с ее модификацией, налицо приготовление к созданию, использованию и распространенно вредоносных программ для ЭВМ и покушение на неправомерный доступ к компьютерной информации.

В контексте нашего изложения небезынтересно отметить, что в соответствии с ч.2 ст. 30 УК уголовная ответственность наступает за приготовление только к тяжкому преступлению. Итак, отличие неправомерного доступа к компьютерной информации от создания, использования и распространения вредоносных программ для ЭВМ следует искать в юридической характеристике предмета преступного посягательства, содержании общественно опасных действий, приводящих к вредным последствиям, в субъективной стороне, дающей представление об отношении субъекта к содеянному.

1.4 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети: состав преступления, проблемы привлечения к ответственности

## Компьютерные системы в настоящее время все больше влияют на нашу жизнь и выход из строя ЭВМ, систем ЭВМ или их сети может привести к катастрофическим последствиям, поэтому законодатель посчитал необходимым установить уголовную ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети. И именно статья 274 УК РФ устанавливает такую ответственность, акцентируя что это деяние должно причинить существенный вред. Целью действия ст. 274 должно быть предупреждение невыполнения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой информации. Данная уголовная норма, естественно, не содержит конкретных технических требований и отсылает к ведомственным инструкциям и правилам, определяющим порядок работы, которые должны устанавливаться специально управомоченным лицом и доводиться до пользователей. Применение данной статьи невозможно для систем публичного доступа, например, глобальной компьютерной сети Internet; ее действие распространяется только на компьютеры и локальные сети организаций.[50]

В этой статье также считается, что под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим ее правовой защиты, например - государственная, служебная и коммерческая, банковская тайны, персональные данные и т.д.[11].

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

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

Под таковыми правилами понимаются,

1. во-первых, Общероссийские санитарные нормы и правила для работников вычислительных центров,
2. во-вторых, техническая документация на приобретаемые компьютеры,
3. в-третьих, конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка.

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

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

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

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

Представляется правильным отнесение к таковым следующих: блокировку системы защиты от несанкционированного доступа, нарушение правил электро- и противопожарной безопасности, использование ЭВМ в условиях, не отвечающих тем, которые установлены документацией по ее применению (по температурному режиму, влажности, величине магнитных полей и т.п.), отключение сигнализации, длительное оставление без присмотра и многие другие. Однако все эти действия должны рассматриваться не самостоятельно, а только лишь в связи с угрозой безопасности хранимой в ЭВМ и охраняемой законом информации. [56,c.58]

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

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

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

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

Первым неблагоприятным последствием является умышленное уничтожение, блокирование или модификации компьютерной информации, однако преступление будет оконченным только при наступлении второго общественно опасного последствия опасного последствия – неосторожного причинения опасного последствия – неосторожного причинения тяжкого вреда.

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

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

1. Общественно опасным деянием (действием или бездействием), которое заключается в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети.

2. Настеплением общественно опасных последствий в виде уничтожения блокирования или модификации компьютерной информации, причинивших существенный вред или повлекших по неосторожности тяжкие последствия.

3. Наличием причинной связи между действием и наступившими последствиями.

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

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

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

Например, действия технического специалиста больницы поставившего полученную по сетям программу без предварительной проверки (что говорит о преступной неосторожности) на наличие в ней компьютерного вируса, повлекшее нарушение работы ЭВМ (сети ЭВМ) и отказ работы систем жизнеобеспечения реанимационного отделения, повлекшее смерть больного должны квалифицироваться по части 2 ст. 274. [62]

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

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

Санкция части 1 ст. 274 состоит из трех альтернативных видов наказания: лишение права занимать определенную должность или заниматься определенной деятельностью на срок до пяти лет, обязательные работы от ста восьмидесяти до двух сорока часов и ограничение свободы до двух лет.

Часть 2 - состав с двумя формами вины, предусматривающий в качестве квалифицирующего признака наступление по неосторожности тяжких последствий. Содержание последних, очевидно, аналогично таковому для ч. 2 ст. 273. Санкция нормы существенно отличается от предыдущей: только лишение свободы до 4 лет.

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

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

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

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

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

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

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

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

2. Криминологический аспект преступлений в сфере компьютерной информации

2.1 Криминологическая характеристика личности преступника

Собранные в процессе исследования сведения о личности преступления, о его криминальном поведении и виновности создают фактическую базу для принятия обоснованных решений по его уголовному преследованию.[47,c.161]

Заслуживает внимания классификация лиц, склонных к совершению преступления в сфере компьютерной информации, предложенная А.В.Кузнецовым.[62] К первой группе относятся лица, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами фанатизма и изобретательности. Вторая включает лиц, страдающих новым видом психических заболеваний – информационными и компьютерными фобиями, и третью группу составляют профессиональные компьютерные преступники с ярко выраженными корыстными целями. Именно эта группа представляет собой основную угрозу для общества, являясь кадровым ядром компьютерной преступности. Особую категорию преступников составляют хакеры.[65, c.129] Их определяют как особую категорию специалистов в сфере вычислительной техники, осуществляющих негативные действия в области систем компьютерной связи и информационных технологий с целью получения доступа к защищенной компьютерной информации. На основе имеющихся публикаций и результатов анализа следственной практики можно предложить следующую классификацию лиц, совершающих преступления в сфере компьютерной информации, в зависимости от их специализации:

1. Кракеры – лица, деятельность которых направлена на "взлом" различного программного обеспечения. Их целями обычно являются: устранение защиты от несанкционированного копирования, бесплатная регистрация программных продуктов, устранение каких-либо ограничений или расширение возможностей программ.

2. Фрикеры – специализируются на неправомерном использовании коммуникационных услуг и средств связи. Их деятельность направлена на безвозмездное использование услуг междугородной телефонной связи ( включая телефонные переговоры через сеть Интернет), услуг мобильной связи.

3. Кардеры (от англ.card- карта). Направленность их деятельности предполагает наличие глубоких знаний в области программирования микросхем и микропроцессов. Их целью становится неправомерная модификация информации на электронных банковских, телевизионных и других картах.

4. Хакеры (сетевые хакеры). Предметом посягательств являются различные сетевые ресурсы: серверы электронной почты, серверы, предоставляющие услуги по размещению веб-страниц, информационные ресурсы крупных компаний и т.п.

Важную роль в формировании антисоциальной направленности в сознании играют условия внутреннего (субъективного) характера. В отличие от внешних условий. Они охватывают явления. Связанные с особенностями личности правонарушителя[16,c.28].К ним на наш взгляд относятся: недостаточный уровень правовой культуры; ослабленность волевых качеств личности; импульсивность, которая проявляется в сниженном контроле своего поведения; отсутствие правильных целей в жизни и умения их добиваться; неуверенность в себе, выражающаяся в предпочтительном выборе виртуального общения и т.п.

Особенности характера и темперамента лица, совершившего преступление в сфере компьютерной информации, необходимо принимать во внимание для выявления таких качеств личности, которые могут способствовать совершению данного преступления, это также может конкретизировать меры предупредительно-воспитательного воздействия на данное лицо с учетом его личностных особенностей.

Способы совершения преступлений.

Под способом совершения преступления понимается система объединенных единым замыслом действий преступника (и связанных с ним лиц) по подготовке, совершению и сокрытию преступления, детерминированных объективными и субъективными факторами и сопряженных и использование соответствующих орудий и средств.

На сегодняшний день существует несколько классификаций способов совершения преступлений в сфере компьютерной информации. Одна из классификации предложена А. Н, Родионовым и А. В. Кузнецовым. Согласно ей, способы совершения компьютерных преступлений можно подразделить на:

1) изъятие средств компьютерной техники;

2) неправомерный доступ к компьютерной информации преступления, совершенные в отношении компьютерной информации, находящееся в глобальных компьютерных сетях; преступления, совершенные в отношении компьютерной информации, находящееся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (пейджер, сотовый телефон, кассовый аппарат, и.т.п.);

3) изготовление или распространение вредоносных программ (вирусы, программы – взломщики и.т.п.);

4) перехват информации.

На наш взгляд, способы совершения неправомерного доступа компьютерной информации можно объединить в три основные группы.

Первая группа- это способы непосредственного доступа. При их реализации информация уничтожается, блокируется, модифицируется, копируется, а также может нарушаться работа ЭВМ, системы ЭВМ или их сети путем отдачи соответствующих команд с компьютера, на котором информация находится. Непосредственный доступ может осуществляться как лицами, работающими с информацией (имеющими отношение к этой работе), так и лицами, специально проникающими в закрытые зоны и помещения, где производится обработка информации.

Другой способ непосредственного доступа к компьютерной информации заключается в неправомерном использовании преступником технических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой. Он осуществляется в двух формах: физической и электронной.

Физический поиск отходов сводится к обследованию рабочих мест программистов, содержимого мусорных баков, емкостей для технологических отходов для сбора оставленных или выброшенных физических носителей информации, а также обследованию различной документации, оставленной на рабочем месте ежедневников.

Вторая группа способов совершения рассматриваемого преступления включает способы опосредованного (удаленного доступа к компьютерной информации. При этом неправомерный доступ к определенному компьютеру и находящееся на нем информации осуществляется с другого компьютера, находящегося на определенном расстояние через компьютерные сети. Способы опосредованного доступа к компьютерной информации, в свою очередь, можно разделить на две подгруппы: способы преодоления парольной а также иной программой или технической защиты и последующего подключения к чужой системе; способы перехвата информации.

К способам первой подгруппы относятся:

1) Подключение к линии связи законного пользователя (например, к телефонной линии) и получение тем самым доступа к его системы. Подключившись, преступник дожидается сигнала, означающего окончание работы, перехватывает его на "себя", а потом, когда законный пользователь закончил сеанс работы, осуществляет доступ к его системе. Данный способ сравним с работой двух параллельных телефонных аппаратов, подключенных к одному абонентскому номеру: если один телефон находиться в активном режиме (ведется разговор по первому закончен и трубка положена, он может быть продолжен по второму.

2) Проникновение в чужие информационные сети путем автоматического перебора абонентских номеров с последующими соединением с тем или иным компьютером (перебор осуществляется до тех пор, пока на другом конце линии не "отзовется чужой" компьютер). Поскольку в подобном случае один несанкционированный пользователь может быть легко обнаружен, подобный "электронный взлом" осуществляется в одновременно с несколькими рабочих мест: в заданное время несколько (более десяти)персональных компьютеров одновременно предпринимают попытку несанкционированного доступа.

3) Проникновение в компьютерную систему и использованием чужих паролей, выдавая себя за законного пользователя. При подобном способе незаконный пользователь осуществляет подбор пароля для доступа к чужому компьютеру. Подбор паролей может осуществляться двумя методами. Первый: подбор паролей путем простого перебора всех возможных сочетаний символов до тех пор, пока не будет установлена нужный код, что позволило преступнику получить исчерпывающий список личных кодов пользователь.

Ко второй подгруппе способов опосредованного (удаленного) доступа к компьютерной информации относятся способы ее непосредственного, электромагнитного и других видов перехвата.

Непосредственный перехват осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного "подслушивания" являются кабельные и проводные системы, наземные микроволновые системы, системы правительственной связи.

Электромагнитный перехват. Современные технические средства позволяют получить информацию без непосредственного подключения к компьютерной системе: за счет перехвата излучений центрального процессора, дисплея, коммуникационных каналов, принтера и.т.д. Все это можно осуществить, находясь на достаточном удалении от объекта перехвата. Например, используя специальную аппаратуру, можно "снимать" информацию с компьютера, расположенного в соседнем помещении, здании. Таким образом, при несанкционированном доступе в Интернет происходит обращение к "списку" имен и паролей на компьютере провайдера, который является коммерческой тайной. Что касается наступления общественно опасных последствий, их может быть несколько. В самом общем случае – это нарушение работы сети ЭВМ, под которым надо понимать следующие:

1. Выдачу искаженных информации, поскольку во всех протоколах фигурирует имя зарегистрированного пользователя.

2. Сбои в работе оборудования, поскольку оборудование провайдерской фирмы рассчитано на определенное количество пользователей и, разумеется, не учитывает нелегально подключившихся. Повышенная загрузка оборудования приводит к ошибкам при передачи данных и, как следствие, необоснованным задержкам при работе.

При этом обязательным условием является сохранение физической целостности ЭВМ, системы ЭВМ или их сети. Если наряду с названными нарушениями работы оборудования нарушается и физическая целостность компьютерной ЭВМ, системы ЭВМ или их сети. Если наряду с названными нарушениями работы оборудования нарушается и физическая целостность компьютерной системы как физической вещи, содеянное требует дополнительной квалификации по статьям о преступлениях против собственности. Помимо нарушения работы, в случае монопольного режима доступа(либо статического IP адреса), происходит блокирование информации, т.е.другой пользователь под этим же именем ( адресом) лишается возможности входа. При этом нарушение работы по п.2 не будет, так как количество пользователь не меняется. Причинение материального ущерба наносимого в результате списания денежных средств со счетов зарегистрированных пользователей должно быть квалифицирована как причинение имущественного ущерба путем обмана или злоупотребления доверием при отсутствии признаков хищения т.е. по ч.1 ст. 165; либо в случае неоднократности по ч.1, либо в случае крупного ущерба по ч.3. Однако неоднократность в данном случае следует разграничивать с длящимися преступлением. Так, неоднократным целесообразно считать вход различными сетевыми реквизитами, а длящимся – разделенный по времени вход под одним и тем же именем и паролем.

2.2 Факторы, способствующие совершению преступлений в сфере компьютерной информации

За последнее годы предлагаются различные пути решения вопросов связанных с выявлением факторов совершения преступлений в сфере компьютерной информации и условий, способствующих его совершению. Однако указанные решения на наш взгляд, не являются исчерпывающими и нуждаются в дальнейшей разработке. К числу нерешенных относятся, в частности вопросы о составе совокупности явлений подлежащих установлению в качестве причин и условий по каждому уголовному делу, а также о роли и значении для наступления события преступления отдельных обстоятельств входящих в эту совокупность.

По мнению Г.Г. Зуйкова, совокупность причин и условий, вызывающих совершение какого либо преступления, можно определить следующим образом.[38, c.15]

- непосредственная причина совершения преступления.

- условия, способствующие действию непосредственной причины и конкретному преступному посягательству.

- обстоятельства, сформировавшие непосредственную причину и являющиеся таким образом причинами непосредственной причины, условия способствующие действию факторов формирующих непосредственную причину и.т.д.

Необходимо отметить, что в связи с многообразием факторов, объективно и субъективно влияющих на совершение преступлений в сфере компьютерной информации не всегда удается открыть их фактическое взаимодействие и установить какие из них привели непосредственно к совершению преступления, а какие служили более или менее отдаленными причинами этого явления.[46, c.161]

Непосредственной причиной совершения рассматриваемых деяний, как правило, выступает антисоциальная направленность, выразившаяся в формировании и сознательной реализации преступного умысла, так как с субъективной стороны преступления в сфере компьютерной информации могут быть совершены только умышленно.

Обстоятельства, формирующие антисоциальную направленность, то есть непосредственную причину, по мнению Ушакова С.И. можно разделить на объективные и субъективные.[88, c.169]

К числу объективных условий относятся такие как:

1. непродуманная кадровая политика в вопросах приема на работу сотрудников и их увольнения. Мировой опыт развития компьютерной техники свидетельствует, что специалисты высокой квалификации, неудовлетворенные условиями или оплатой труда, нередко уходят из компании для того, чтобы начать собственный бизнес. При этом, они "прихватывают" с собой различную информацию, являющуюся собственностью владельцев фирмы, включая технологию, список потребителей и т.д. Иными словами, всё, что имело какую-либо интеллектуальную ценность, покидало ворота предприятия в дипломатах, нанося при этом многомиллионные убытки;[82, c.21]

2. нарушение должностными лицами организаторских хозяйственных и социальных функций, выразившихся в возникновении у сотрудников материальной незаинтересованности осуществления своих обязанностей, необоснованном ограничении трудовых прав и возможностей использования льгот и социальных гарантий, препятствовании учебе, повышению квалификации, осуществлении права на отдых и т.п.;

3. недостаточно серьезное отношение руководителей к вопросам обеспечения информационной безопасности и защиты информации. Нередко в крупных организациях, обрабатывающих значительный объем компьютерной информации, отсутствует не только служба или отдел информационной компьютерной безопасности. Но и отдельное лицо, в обязанности которого входило бы ее обеспечение.[68, c.27] Это может спровоцировать совершение рассматриваемого преступления.

К внешним условиям можно отнести следующие:

1. недостаточная защита используемого программного обеспечения от несанкционированного доступа. Например, операционные системы MicroSoft отличается несовершенным алгоритмом шифрования сохраняемых паролей (в сети Интернет распространены программы расшифровки " PWL" файлов, содержащих пороли). Подобные программы были использованы в ходе совершения неправомерного доступа к компьютерной информации в 14, 7% изученных уголовных дел. В 8,8 % случаев при осуществлении такого доступа использовались программы, предназначенные для тестирования надежности сетевых программных и аппаратных средств защиты информации;

2. уязвимость защиты электронной почты (на пути к адресату сообщение проходит через многочисленные компьютеры. Причем часто новым маршрутом, к тому же при пересылке почты остается большое число копий, сильно снижающих уровень защиты). Электронное сообщение само по себе может нести существенную опасность, из-за возможности прикрепления к электронным письмам активных компонентов, среди которых может оказаться и вредоносная программа так, при совершении 5,9 % изученных преступлений использовались вредоносных программы, типа "троянский конь", которые посылались будущей " жертве" прикрепленными к обычному электронному письму;

3. недостаточная надежность технических средств защиты компьютерной техники. Существующие сегодня методы эмуляции и перехвата позволяют обойти большинство аппаратных средств защиты, например, электронных "HASP" ключей, подключаемых к портам компьютера, через которые происходит соединение с периферийным оборудованием;

4. отсутствие контрольных проверок программным оборудованием соответствия и правильности вводимой информации.

К внутриорганизационным условиям можно отнести:

1. отсутствие должного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации и ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа. Зарубежный опыт свидетельствует о том, что создание соответствующих подразделений или должностей в значительной степени снижает риск несанкционированного доступа к охраняемой компьютерной информации.;

2. неконтролируемый доступ сотрудников к элементам управления средств компьютерной технике (устройствам ввода информации), используемых как автономно, так и в качестве элементов автоматизированной сети;

3. несовершенство парольной системе защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

4. неприменение категорийности допуска сотрудников к документации строгой финансовой отчетности, в том числе находящейся в электронном виде;

5. отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной компьютерной информации;

6. легкомыслие и небрежность собственников и пользователь компьютерной информации;

7.нарушение установленных сроков хранения копий программ и компьютерной информации, а иногда и полное их отсутствие.

Определяющее значение имеет деятельность государства в лице уполномоченных органов по разработке и регламентации общегосударственных вопросов защиты Российского информационного пространства, выявлению и устранению обстоятельств, способствующих посягательствам на компьютерную информацию. При этом необходимо учитывать влияние как внешних, так и внутренних факторов, способствующих количественному росту рассматриваемых преступлений.

Внешние общегосударственные факторы, на наш взгляд, следующие:

1. ускоренная интеграция Российской Федерации в международное информационное пространство. Объединение с локальными и глобальными сетями граничащих с Россией информационно развитых стран. Непрерывное увеличение количества и пропускной способности каналов связи с глобальной сетью Интернет;

2. рост числа ЭВМ, используемых в России, увеличение числа пользователей, объемов информации, хранимой и передаваемой ЭВМ;

3. возможность выхода российского пользователя в мировые информационные сети для обмена информацией[39, c.110]. Заключения контрактов, осуществления платежей и покупок.

Подобный обмен в настоящее время производится абонентами самостоятельно, без контроля со стороны государственных органов, минуя государственные границы.

К внутренним общегосударственным факторам относятся:

1. недостаточный уровень специальной подготовки должностных лиц правоохранительных органов, в обязанности которых входит предупреждение, раскрытие и расследование компьютерных преступлений;

2. отсутствие скоординированности в работе государственных и общественных структур в сфере обеспечения информационной безопасности. Помимо правоохранительных органов (МВД, ФСБ и прокуратуры), вопросами информационной безопасности занимаются Комитет по политике информатизации при Президенте РФ, Палата по информационным спорам при Президенте РФ, Государственная техническая комиссия при Президенте РФ, Министерство связи РФ, Международная Академия информатизации;

3. ограничения на импорт в Россию защищенных от электронного шпионажа компьютеров и сетевого оборудования;

4. использование в преступной деятельности современных технических средств, в том числе ЭВМ. Во-первых, организованная преступность включена в крупномасштабный бизнес, выходящий за рамки отдельных государств, где без компьютеров невозможно руководить и организовать сферу незаконной деятельности. Во- вторых, из организаций, использующих ЭВМ, удобнее "вытягивать" деньги с помощью такой же техники, дающей возможность повысить прибыль и сократить риск.

Деятельность по выявлению и устранению обстоятельств, способствующих совершению неправомерного доступа к компьютерной информации, в конечном счете, направлена на создание таких условий, при которых совершение данного преступления будет максимально затруднено или невозможно, но если оно совершено, первостепенное значение приобретает выявление всех эпизодов преступления.

2.3 Меры по предупреждению преступлений в сфере компьютерной информации

К организационным мерам предупреждения преступлений в сфере компьютерной информации можно отнести следующую совокупность мероприятий.

- совершенствование научно-технических средств, тактических приемов и методов расследования неправомерного доступа к компьютерной информации;

- своевременное явление и пресечение как начавшихся преступлений, так и неправомерного доступа к компьютерной информации на стадии покушения или подготовки к нему;

- установление обстоятельств, способствовавших совершению каждого преступления, разработка и совершенствование методов и приемов выявления таких образов;

- создание подразделений в МВД, ФСБ и прокуратуре, специализирующихся на расследовании высокотехнологичных преступлений, в частности неправомерного доступа к компьютерной информации, а также экспертно – криминалистических подразделений, способных отвечать на все вопросы компьютерно-технических и компьютерно-информационных эксперзиз;

- своевременная регистрация и надлежащий учет этих преступлений;

- переподготовка и повышение квалификации работников правоохранительных органов, расследующих неправомерный доступ к компьютерной информации;

- информационное обеспечение деятельности органов внутренних дел[54,c.33];

- разработка и внедрение политики безопасности компьютерной информации, включающий подбор, проверку и инструктаж персонала, участвующего во всех стадиях информационного процесса.

В настоящее время основными задачами отделов по борьбе с преступлениями в сфере высоких технологий (ОБПСВТ) являются:

1. Выявление преступлений в сфере компьютерной информации когда объектом преступного посягательства является ЭВМ, их системы м сети права собственника информации, в сфере телекоммуникаций ЭВМ их системы и сети являются орудием совершения преступления, а также посягательств на конституционные права граждан - неприкосновенность личной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, совершенных путем неправомерного прослушивания сообщений и снятия информации с технических каналов связи.

2. Возбуждение уголовных дел и производство неотложных следственных действий, при необходимости пресечение указанных преступлений.

3. Выявление лиц, групп и сообществ, занимающихся противоправной деятельностью в данной области, документирование их преступной деятельности, проведение мероприятий по предупреждению таких преступлений.

4. Выполнение поручений следователей по расследованию указанных преступлений, производство оперативно - розыскных мероприятий, а также участие в расследовании в составе следственно - оперативных групп.

Аналогичные подразделения созданы и в других российских правоохранительных органах - Генеральной прокуратуре и Федеральной службе безопасности.

1. Аналитическую разведку совершенствование информационного - аналитического обеспечения деятельности подразделении криминальной милиции, изучение перспективных средств и методов поиска и сопоставительного анализа самой разнообразной, имеющей значение для борьбы с данным компьютерным преступлением информации от материалов средств массовой информации в электронных библиотеках сети Интернет до конкретных оперативных данных. Целью такого анализа является формирование новых знаний о способах совершения неправомерного доступа к компьютерной информации, способах его сокрытия, выявления фактов несанкционированного доступа о которых не поступило заявлений в правоохранительные органы и.т.п.

2. Компьютерную разведку - применение средств и методов организации гласного и негласного получения информации, хранимой и обрабатываемой компьютерными системами для получения сведений о готовящихся преступлениях. Деятельность по скрытому получению компьютерной информации может предусматривать как непосредственный доступ к интересующим информационным ресурсам, так и перехват электронных сообщений, передаваемых по компьютерным проводам и радиосетям.

3. Обеспечение информационной безопасности органов внутренних дел которое распространяется от защиты субъектов и интересов органов внутренних дел от недоброкачественной информации до защиты ведомственной информации ограниченного доступа, информационных технологий и средств их обеспечения. Информационная безопасность ОВД определяется надежностью систем ее обеспечения включая надежность аппаратных средств и программного обеспечения [35, c.75].

Международное сотрудничество при расследовании рассматриваемого преступления осуществляется в формах[26, c.495]:

а) обмена информацией, в том числе:

- о готовящемся или совершенном неправомерном доступе к компьютерной информации и причастных к нему физических и юридических лицах.

- о формах и методах предупреждения, выявления, пресечения, раскрытия и расследования данного преступления.

- о способах его совершения

- о национальном законодательстве и международных договорах, регулирующих вопросы предупреждения выявления пресечения, раскрытия и расследования как рассматриваемого преступления, так и других преступлений в сфере компьютерной информации.

б) исполнения запросов о провидении оперативно - розыскных мероприятий, а также процессуальных действий, в соответствии с международными договорами о правовой помощи.

в) планирования и проведения скоординированных мероприятий и операций по предупреждению, выявлению, пресечению, раскрытию и расследованию неправомерного доступа к компьютерной информации.

г) оказания содействия ив подготовке и повышении квалификации кадров, в том числе путем стажировки специалистов, организации конференций, семинаров, и учебных курсов.

д) создания информационных систем, обеспечивающих выполнение задач по предупреждению, выявлению, пресечению, раскрытию и расследованию данного преступления.

е) проведения совместных научных исследований по представляющим взаимный интерес проблемам борьбы с рассматриваемым преступлениями, а с другой стороны- увеличить объем информации, проходящей через государственные СМИ, направленной на повышение уровня правовой, информационной и компьютерной культуры общества.

Организационные мероприятия по предупреждению неправомерного доступа к компьютерной информации рассматриваются многими специалистами, занимающимися вопросами безопасности компьютерных систем как наиболее важные и эффективные. Это связано с тем что они являются фундаментом на котором строится вся система защиты компьютерной информации от неправомерного доступа.

Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно- технических средств защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти. Правительство Российской Федерации определяет порядок осуществления такого контроля. В организациях обрабатывающих государственную информацию с ограниченным доступом создается специальные службы обеспечивающие защиту такой информации[79, c.30].

Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации, в случае невыполнения этих требований. Он также вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство Российской Федерации. Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки. Субъектами, осуществляющими профилактику неправомерного доступа к компьютерной информации являются правоохранительные органы, поскольку профилактическая деятельность составляет обязательную составную часть правоохранительной деятельности: органы межведомственного контроля, отраслевые органы управления, международные органы и общественные организации, а так же непосредственные руководители предприятий и организаций в которых обращается конфиденциальная компьютерная информация ответственные сотрудники по информационной безопасности. Практика борьбы с преступлениями в сфере компьютерной информации показывает, что положительный результат можно получить только при использовании комплекса правовых, организационных и технических мер предупреждения неправомерного доступа к компьютерной информации, причем все они одинаково важны и лишь дополняя друг друга образуют целенаправленную систему предупреждения и профилактики исследуемого преступления.

2.4 Международное сотрудничество в борьбе с преступлениями в сфере компьютерной информации

Исходя из изложенного, можно сделать выводы о том, что сложность компьютерной техники, неоднозначность квалификации, а также трудность сбора доказательственной информации не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по статьям 272-274 УК. Кроме этого, нас ждет появление таких специфических форм компьютерных правонарушений, к которым не применимы составы преступлений, предусмотренные вышеуказанными статьями. Но все же попытка реализации уголовно-правовой политики России в новой для нее области - сфере компьютерных правоотношений, поможет снять накопившиеся здесь противоречия, защитить права заинтересованных лиц. Ее успех будет зависеть от многих факторов политического, экономического, научно-технического, организационного характера. Немаловажное значение будет играть понимание правоведами транснационального характера компьютерной преступности и, как следствие, установление международных контактов с правоохранительными структурами. Такими же значимыми факторами будут и контакты с частными охранными структурами и структурами информационной безопасности в кредитно-денежной сфере. Сегодняшние реалии заставляют двигаться в этих направлениях. По данным правоохранительных органов криминальное поле кредитно-банковской системы активно заполняется преступлениями, связанными с использованием электронных средств доступа к информации (компьютерные, телекоммуникационные системы, кредитные карточки и др.). Для правоохранительных органов эта проблема наиболее остро встает в связи с переходом абсолютного числа банковских и финансовых структур на расчеты с использованием компьютерных сетей.

Например, только по данным ГИЦ МВД России, в 2007-2009 гг. выявлено 26821 преступление преступлений с использованием электронных средств доступа. По данным Федеральной службы реагирования на ЧП в компьютерном пространстве, только в 2008г. было зарегистрировано 9010 преступлений, из них раскрыто-8419, на 24% больше, чем в предыдущем году. За 2009г. раскрыто-9991 из 10575 (на 43,6% больше, чем в 2008г.) В первом квартале 2010г. преступлений в данной сфере было зарегистрировано 11918 (из них 1230 – в январе, 3634 – в феврале, 2541 – в марте и 4513 – в апреле), среди которых раскрыто 10488 (более 88 %). Обнаружить удается менее 15% всех преступлений этого рода и лишь 10% из них предаются огласке. Понятно, что без тщательно отработанных методик расследования, помогающих людям обрести чувство защищенности, под сомнением оказывается - ни больше ни меньше - стабильность сегодняшних военных и коммерческих предприятий, не говоря уже об электронной торговле на базе Internet. Результаты статистического анализа убытков и типов преступлений не могут считаться достаточно корректными, поскольку, во-первых, не все группы жертв смогли предоставить достоверные сведения о своих финансовых потерях, а во-вторых, чисто денежными потерями ущерб в данном случае далеко не ограничивается.

Подобная картина требует кардинальных решений на международном уровне. И первые попытки уже сделаны. Надо отметить, что российские правоохранительные органы в достаточной степени осознали угрозу которую таит в себе информатизация общества и государства. В меру возможностей, отпущенных финансированием ведомства пытаются делать упреждающие шаги. Создавать компьютерную сеть МВД у нас начали еще в 1991году, понимая, что с бумажными картотеками много преступников не наловишь. Программное обеспечение для управления базами данных, в которых МВД хранит миллионы записей, приобретено у не менее знаменитой американской фирмы Oracle. Создание милицейской компьютерной сети, которая в конце концов должна раскинуться от Калининграда до Южно-Сахалинска, - сегодня один из глобальных российских информационных проектов, который выполняется четко и в положенные сроки. Остается пожелать, чтобы подобная сеть сама не стала объектом посягательств преступников.

#

# Заключение

В ходе проведенного исследования:

- выявлены недостатки законодательной техники при конструировании ст. 272 УК РФ, сформулированы и обоснованы рекомендации по решению ряда задач прикладного характера;

- дана общая характеристика составов преступлений в сфере компьютерной информации и проблемы их квалификации;

-рассмотрен состав преступления по ст. 272 "Неправомерный доступ к компьютерной информации" и проблемы квалификации данного преступления;

-исследованы проблемы квалификации преступления по ст.273 "Создание, использование и распространение вредоносных программ для ЭВМ";

- проанализированы проблемы привлечения к уголовной ответственности по ст.274 УК РФ "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

-дана криминологическая характеристика особенностям преступлений в сфере компьютерной информации;

-установлены основные особенности личности компьютерных преступников, совершающих неправомерный доступ к компьютерной информации;

-указаны основные факторы, способствующие совершению преступлений;

-рассмотрены меры по предупреждению преступлений в сфере компьютерной информации и обобщен опыт международного сотрудничества в борьбе против преступлений данного вида.

Новизна работы определяется также теми результатами исследования:

1. Компьютерная сфера является основой для возникновения нового вида общественных отношений - компьютерных, которые, в свою очередь, стали одним из объектов уголовно-правовой охраны.

2. Применение компьютерных технологий для обработки информации повлекло появление новых преступлений — преступлений в сфере компьютерной информации.

3. Проанализировав терминологический аппарат, использованный законодателем при конструировании состава ст. 272 УК РФ, установлено следующее:

- в существующем понятийном аппарате гл. 28 УК РФ отсутствует качественная определенность, что несовместимо с требованиями законодательной техники;

- основным из недостатков в использовании названных признаков является то, что все они не имеют количественного выражения и не могут характеризоваться различной интенсивностью проявления;

при конструировании уголовно-правовых норм законодателю необходимо отказаться от введения в уголовное законодательство узкопрофессиональных технических терминов без их легального толкования, а те из них, без которых невозможно обойтись в настоящее время, должны получить легальное толкование в базовом российском информационном законодательстве.

4. В рамках общей профилактики государство должно создавать и финансировать специальные научно-исследовательские центры в целях изучения и предупреждения неправомерного доступа к компьютерной информации и других преступлений в сфере компьютерной информации.

5. Содержащиеся в исследовании теоретические положения и выводы, направленные на развитие и совершенствование общей теории правового регулирования отношений в сфере компьютерной информации, могут использоваться для дальнейших исследований, связанных с проблемой уголовной ответственности за преступления в сфере компьютерной информации. В соответствии с поставленными целями и задачами все выводы и положения, составляющие теоретическую часть работы, подчинены идее использования их в практической деятельности. На основе расчетов реальных данных, выполненных в ряде организаций и внедренных в их практику, показано, что проведение профилактических мероприятий существенно снижает риск неправомерного доступа к компьютерной информации.

Итак попытка реализации уголовно-правовой политики в новой для нее области - сфере компьютерных правоотношений, сможет окажется успешной, если поможет снять накопившиеся здесь противоречия, защитить права заинтересованных лиц - будет зависеть от многих факторов политического, экономического, научно-технического, организационного характера.

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

Список использованной литературы

Нормативные правовые акты

1.Конституция Российской Федерации (принята на всенародном голосовании 12.12.1993 г.)// Российская газета от 1993.25 декабря.№237.

2.Уголовный кодекс Российской Федерации от 13 июня 1996г.№63-ФЗ. // СЗ РФ.1996.№25.Ст.2954

3.Федеральный Закон "Об информации, информационных технологиях и защите информации" от 27 июля 2006г. №149-ФЗ// СЗ РФ. 2004.№31 (Ч.1).Ст.3283

4.Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации"

5.Федеральный Закон "О коммерческой тайне" от 29 июля 2004г.298-ФЗ.2004.№32.Ст.3283

6.Часть четвертая Гражданского кодекса РФ, принятая Государственной Думой ФС РФ (24.11.2006г.)

7.Федеральный закон "О связи" от 07 июля 2003 г. №126-ФЗ.2003."28.Ст.2895

8.Доктрина информационной безопасности Российской Федерации 9 утв. Указом Президентом РФ от 17 декабря 1997г. №1300//СЗ РФ.2000.28 сентября"187

9. Закон "О государственной тайне" от 21 июля 1993 г. № 5485-1

10. Закон "Об обязательном экземпляре документов" от 29 декабря 1994 г. 77-ФЗ

11. Федеральный закон "Об информации, информатизации и защите информации" (от 20.02.95 г. N 24-ФЗ),

12. Модельный Уголовный Кодекс. Рекомендательный законодательный акт для Содружества Независимых Государств. Принят на 7-м пленарном заседании Межпарламентской ассамблеи государств-участником СНГ 17 февраля 1996г.//Приложение к информационному бюллетеню".1996.№10

13. Указ Президента РФ от 12 мая 2004 г.№611 "О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена"// СЗ РФ.2000.№2.Ст.170

14. Соглашение о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств – участников Содружества Независимых Государств в сфере информатизации (Москва, 24 декабря 1999 г.) // Бюллетень международных договоров,2002..№11.

15. Соглашение с сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации 9Минск,1 июня 2001 г.) Текст Соглашения официально опубликован не был// СПС "Гарант".

Научная и учебная литература

16. Антонян Ю.М., Еникеев М.И.Психология преступника и расследования преступлений / Ю.М. Антонян, М.И. Еникеев. – М.: Юрист,1996.- С.28

17. Баев О.Я., Мещеряков В.А. Проблемы уголовно-правового регулирования в сфере компьютерной информации /О.Я. Баев, В.А. Мещеряков // Защита информации. - Конфидент. -1998.- № 5.

18. Барсуков В.С., Водолазский В.В. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский .- М.:Нолидж,2000. - С.64

19.Батурин Ю.М., Жодзинский А.М. / Компьютерная преступность и компьютерная безопасность// Ю. М. Батурин, А.М. Жодзинский. - М.: Юридическая литература, 1998. - С.52-54.

20.Батурин Ю.М.Проблемы компьютерного права / Ю.М. Батурин.- М.: Юридическая литература, 1998. - С.14.

21.Бауэр Ф.Л., Гооз Г. Информатика: Вводный курс./ Ф.Л.Бауэр, Г.С. Гооз. - М.: 1990. - С. 18.

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

23. Беляев В.С. Безопасность в распределительных системах / В.С. Беляев – М., 1995.

24. Борзенков Г.Н., Комиссаров В.С. Уголовное право Российской Федерации / Г.Н. Борзенков, В.С. Комисаров. – М.: Олимп, 1997.

25. Ведеев Д.В. Защита данных в компьютерных сетях / Д.В. Ведеев - М.: 1995.

26.Волеводз А.Г.Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. - М.: Изд-во Юрлитиформ, 2000.-С.495.

27. Вехов В.Б., Рогозин В.Ю. Методика расследования преступлений в сфере компьютерной информации // Криминалистическая методика расследования отдельных видов преступлений: Учеб. пособие в 2-х частях.

28. Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: Учеб. - метод. пособие. Изд. 2-е, доп. и испр. - М.: МЦ при ГУК и КП МВД России, 2000. - 64 с.

29. Гайкович В.Ю. Основы безопасности информационных технологий / В.Ю. Гайкович. - М.: Инфо-М, 1998.

30. Горбатов В.С., Полянская О.Ю., Доказывание в судебных делах по компьютерным преступлениям В.С. Горбатов, О.Ю. Полянская. –М.: МИФИ, 1997.

31.Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания / М.Ю. Дворецкий. - Тамбов, 2003.

32.Дворецкий М.Ю. Преступления в сфере информации: Научно-практический комментарий к гл.28.Уголовного кодекса РФ/ М.Ю.Дворецкий. - М.,2005.

33.Дворецкий М., Копырюлин А. Проблемы квалификации преступлений, сопряженных с созданием, использованием и распространением вредоносных программ / М. Дворецкий, А. Копырюлин // Уголовное право. — 2007. — №4.

34. Дворецкий М.Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование) / М.Ю. Дворецкий. Волгоград, 2001 (Диссертация и автореферат)

35. Жуков Ю.И., Приманкин А.И., Щербаков О.В.Информационная безопасность и аппаратно-программная надежность компьютерных средств органов внутренних дел//Вестник МВД России,2000, - №3.-С.75-81

36. Заморин А.П., Марков А.С. Толковый словарь по вычислительной технике и программированию. Основные термин.// А.П. Заморин, А.С. Марков. - М., 1988. С. 68.

37. Информация как элемент криминальной деятельности /Крылов В.В., "Вестник Московского университета", Серия 11, Право, 1998, № 4. – С.28.

38. Зуйков Г.Г. К вопросу о понятии причин преступления и условий, способствующих его совершению//Вопросы предупреждения преступности,вып.2 "Юрид.лит-ра",1995г.-С.15

39. Иванов В.П. Защита от электронного шпионажа / В.П. Иванов //Сети и системы связи. - 1996. - №3 –С.110

40. Информация как элемент криминальной деятельности /Крылов В.В./Вестник Московского университета, Серия 11, Право, 1998, № 4

41. Информационные вызовы национальной и международной безопасности/ под. общ. ред. А.В.Федорова, В.Н.Цыгиченко.М.,2001.

42. Информационные преступления - новый криминалистический объект / Крылов В.// Российская юстиция. 1997 г., № 4

43. Как остановить компьютерное пиратство? / Симкин Л.// Российская юстиция, 1996, №10)

44. Карелина М.М. Преступления в сфере компьютерной информации / М.М. Карелина. - М., 1998.

45. Кириченко А.Н. Вирусы научились размножаться по своим законам / А.Н. Кириченко // МН Коллекция. -2003. -№2. - С.12

46. Козлов В.Е.Теория и практика борьбы с компьютерной преступностью /В.Е. Козлов. - М.: Горячая линия, Телеком. - 2002. – С.161

47. Комиссаров В.С. Преступления в сфере компьютерной безопасности: понятие и ответственность/ В.С. Комисаров // Юридический мир. 2003. -№2. -С.13

48. Комментарий к Гражданскому кодексу РФ части четвертой. Правовое регулирование отношений в сфере интеллектуальной собственности. Автор комментариев и составитель – А.Б.Борисов –М.: Книжный мир,2008.-288с.

49. Комментарий к Гражданскому кодексу РФ части 4.Правовое регулирование отношений в сфере интеллектуальной деятельности. С постатейными материалами и практическими разъяснениями. Автор комментариев и составитель- А.Б.Борисов –М.:Книжный мир,2008- С.51

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

51.Компьютеризация и уголовное право /В.В. Голубев,

//Законодательство, 1999 г., № 8

52. Компьютерные технологии в юридической деятельности: Учебное и практическое пособие / Отв. ред. пpоф. H. Полевой, канд. юpид. наук В. Крылов. М., 1994. - С.7-10.

53. Копылов В.А. Информационное право / В.А. Копылов. - М.:Юрист, 1997. - С. 23.

54. Котухов М.М., Марков А.С. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем / М.М. Котухов, А.С.Марков – СПб.: ВУС, 2004. – 190 с.

55. Криминогенные аспекты глобальной сети Интернет /И.Н. Соловьев //Налоговый вестник, № 4, апрель 2001 г.

56. Криминалистическая характеристика преступлений/ Яблоков Н.П.// Вестник Московского университета .Серия 11, Право, 1999, № 1

57. Крылов В.В. Информационные компьютерные преступления / В.В. Крылов. - М.: Инфра М-Норма, 1997.

58. Курушин В.Д., Минаев В.А. Компьютерные преступления информационная безопасность / В.Д. Курушин, В.А. Минаев - М.: Новый юрист,1998. - С.58

59. Копылов В.А. Информационное право / В.А. Копылов – М.: Юрист, 1997;

60. Копырюлин А. Н. Преступления в сфере компьютерной информации: Уголовно-правовой и криминологический аспекты: Автореф. дис. ... канд. юрид. наук. / А. Н. Копырюлин. — Тамбов, 2007.

61. Копырюлин А.Н. Квалификация преступлений в сфере компьютерной информации / А. Копырюлин // Законность. — 2007. — № 6.

# 62. Кузнецов А.В.Некоторые вопросы расследования преступлений в сфере компьютерной информации//Информационный бюллетень следственного комитета МВД РФ;

# 63. Кузнецов А. П. Ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (ст. 274 УК РФ) / А. П. Кузнецов // Правовые вопросы связи. — 2007. — № 2.

# 64. Кузнецов А. П. Ответственность за преступления в сфере компьютерной информации по зарубежному законодательству / А. П. Кузнецов // Международное публичное и частное право. — 2007. — N 3.

65. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления / Ю. Ляпунов, В. Максимов // Законность. — 1997. — № 1.

66. Никифоров И. Компьютерные преступления //Защита информации. Конфидент, № 5, 1995.

67. Маляров А. И. Объект преступления в сфере электронно-цифровой (компьютерной) информации и вопросы квалификации (российский и зарубежный опыт) / А. И. Маляров // Общество и право. — 2008. — N 2.

68. Маслакова Е. А. История правового регулирования уголовной ответственности за компьютерные преступления / Е. А. Маслакова // Информационное право. — 2006. — N 4.

69. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: ВГУ, 2002. - 408 с.

70. Наумов А. В. Практика применения Уголовного кодекса Российской Федерации: Комментарий судебной практики и доктринальное толкование / А. В. Наумов. — М.: Волтерс Клувер, 2005.

71. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А.В.)

72. Научно-практический комментарий к УК РФ в двух томах. Т.2.Новгород: - НОМОС,1996г.С.134

73. Осипенко А. Уголовная ответственность за неправомерный доступ к конфиденциальной компьютерной информации / А. Осипенко // Уголовное право. — 2007. — № 3.

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

75. Попов В.Офицеры безопасности//Компьютера,1996.№43.-С.27-30

76. Преступления в сфере компьютерной информации /Гульбин Ю.//Российская юстиция, 1997, №10

77. Правовая информатика и кибернетика: Учебник / Под ред. Н.С. Полевого. М., 1993. С. 24 - 29;

78. Преступления в сфере компьютерной информации // Гульбин Ю., Российская юстиция, 1997, N 10

79. Расследование хищений, совершаемых в кредитно-финансовой сфере с использованием электронных средств /В.Г.Баяхчев, В.В. Улейчик, //Законодательство, № 6, июнь 2000 г.

80. Рачук Т.В. Уголовные наказания за информационные преступления //Защита информации. Конфидент, № 4, 1997.

81. Резвана А.П., Субботиной М.В. - М.: ИМЦ ГУК МВД России, 2002. - С. 84-108.

82. Селиванов Н И. Проблемы борьбы с компьютерной преступностью. - Законность, 1993, №. 8, с. 37.

83. Скуратов Ю.И., Лебедев В.М. Комментарий к Уголовному кодексу. – М., 1996;

84. Состояние преступности в Российской Федерации: Статистика // Официальный сайт МВД РФ www.mvd.ru

85. Ткаченко А. Уголовник в компьютере//Юридическая газета, №23,2002г –С.64.

86. Уголовное право РФ. Особенная часть: Учебник / Под ред. проф. Б. В. Здравомыслова. — 2-е изд., перераб. и доп. — М.: Юристъ, 2001.

87. Уголовное право Российской Федерации. Особенная часть: Учебник/ Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. — 2-е изд.,

88. Ушаков С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика) – Ростов-на-Дону,2001г.- С.169

89. Федоров В.И.Борьба с транснациональной организованной преступностью в сфере "высоких технологий"//Прокурорская и следственная практика,1999.№3.-С.30

90. Фоменков Г.В. О безопасности в Internet. Защита информации. // Конфидент. № 6, 1998.

91. Черных Э.А. "Компьютерные хищения. Как их предотвратить?"/

Советская Юстиция,1993. - №3-С.21-22

92. Ястребов Д. А. Вопрос о латентности неправомерного доступа к компьютерной информации в Российской Федерации / Д. А. Ястребов // Юридический мир. — 2008. — № 10.

93. Ястребов Д. А. Вопросы отграничения неправомерного доступа к компьютерной информации от смежных составов преступлений / Д. А. Ястребов // Российский следователь. — 2008. — № 17.

94. Ястребов Д. А. Законодательный опыт стран — участниц Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации / Д. А. Ястребов // Российский следователь. — 2008. — № 6.