Специальный факультет

 ФГОУ ФВПО ВСИ МВД РФ

КОНТРОЛЬНАЯ РАБОТА

По дисциплине: «Административное производство»

Вариант№7

Выполнил: слушатель 5 «с» курса

специального факультета

заочной формы обучения

ФГОУ ФВПО ВСИ МВД России

Введение

1.Преступления в сфере компьютерной информатики

2.Неправомерный доступ к компьютерной информатики

3. Создание, использование и распространение вредоносных программ для ЭВМ

4.Неправомерный доступ к компьютерной информатики

Заключение

Список использованной литературы

**Введение**

Компьютерные преступления приобрели в странах с развитой телекоммуникационной инфраструктурой настолько широкое распространение, что для борьбы с ними в уголовное законодательство были введены специальные составы преступлений. Традиционные меры гражданско-правовой ответственности, ориентированные, прежде всего на возмещение убытков, не смогли сыграть роль сдерживающего фактора и воспрепятствовать широкому распространению этого вида правонарушений

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

Первыми шагами в этом направлении были: принятие Закона РФ “О правовой охране программ для ЭВМ и баз данных“ от 23.09.1992; Федерального закона “Об информации, информатизации и защите информации“ от 20.02.1995; включение в новый Уголовный кодекс специальной главы 28 “Преступления в сфере компьютерной информации”.

Преступления, содержащиеся в этой главе, представляют собой деяния, сущность которых заключается отнюдь не в использовании самой по себе электронно-вычислительной техники в качестве средства для совершения преступлений. Эта глава включает общественно-опасные деяния, посягающие на безопасность информации и систем обработки информации с использованием ЭВМ. Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением.

Хищение информации связано с потерей материальных и финансовых ценностей, то этот факт можно квалифицировать как преступление. Также если с данным фактом связываются нарушения интересов национальной безопасности, авторства, то уголовная ответственность прямо предусмотрена в соответствии с законами РФ.

По мере развития технологий платежей электронных, “безбумажного” документооборота и других, серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. 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. Преступлениями в сфере компьютерной информации являются:

Неправомерный доступ к компьютерной информации (ст.272 УК РФ);

Создание, использование и распространение вредоносных программ (ст.273 УК РФ);

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ);

Особенностью конструкции составов этих преступлений является то, что они сконструированы по типу материальных - предусматривают наступление общественно-опасных последствий в виде вреда для пользователей ЭВМ, который в целом состоит в нарушении нормального функционирования ЭВМ или сетей ЭВМ.

Физическое повреждение или уничтожение компьютерной техники, незаконное за владение ею, а равно машинными носителями (дискетами, CD-R дисками), как предметами, обладающими материальной ценностью, квалифицируются по статьям главы 21 УК РФ. В принципе, можно предположить случаи, когда вредоносное воздействие на ЭВМ осуществляется путем непосредственного влияния на нее информационных команд. Это возможно, когда преступнику удается ввести движущиеся части машины (диски, принтер) в резонансную частоту, увеличить яркость дисплея или его части для прожигания люминофора, зациклить работу компьютера таким образом, чтобы при использовании минимального количества его участков произошел их разогрев и выход из строя. В этих случаях квалификация содеянного должна проводиться по совокупности статей глав о преступлениях против собственности и компьютерной безопасности, поскольку страдают два объекта уголовно-правовой охраны.Преступления в области компьютерной информации впервые включены в УК РФ, вступивший в действие 1 января 1997 года. По этому необходимо определить основные понятия используемые в данном разделе.

***Компьютерная информация***- в соответствии со [ст. 2 закона "Об информации информатизации и защите информации"](http://www.relcom.ru/Archive/1997/ComputerLaw/RussiaLaws/Informat.htm#st2) под информацией понимаются - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, но в применительно к комментируемым статьям под компьютерной информацией понимаются не сами сведения, а форма их представления в машиночитаемом виде, т.е. совокупность символов зафиксированная в памяти компьютера, либо на машинном носителе (дискете, оптическом, магнитооптическом диске, магнитной ленте либо ином материальном носителе). При рассмотрении дел следует учитывать, что при определенных условиях и физические поля могут являться носителями информации.

***Программа для ЭВМ***- объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения;

***ЭВМ (компьютер)*** - устройство или система (несколько объединенных устройств) предназначенное для ввода, обработки и вывода информации.

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

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

**Статья 272. Неправомерный доступ к компьютерной информации**

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

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.

Неправомерным признается доступ к компьютерной информации лица, не обладающего правами на получение и работу с данной информацией, либо компьютерной системой. Причем в отношении этой информации системы должны приниматься специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ.

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

Состав данного преступления носит материальный характер и предполагает обязательное наступление одного из следующих последствий:
- уничтожения информации, то есть удаление информации на материальном носителе и невозможность ее восстановления на нем;
- блокирования информации, то есть совершение действий приводящих к ограничению или закрытию доступа к компьютерной системе и предоставляемым ею информационным ресурсам;
- модификации информации, то есть внесение изменений в программы, базы данных, текстовую информацию находящуюся на материальном носителе;
- копирования информации, то есть переноса информации на другой материальный носитель, при сохранении неизменненой первоначальной информации;
- нарушения работы ЭВМ, системы ЭВМ или их сети, что может выразиться в нарушении работы как отдельных программ, баз данных, выдаче искаженной информации, так и нештатном функционировании аппаратных средств и периферийных устройств, либо нарушении нормального функционирования сети.

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

Субъективная сторона данного преступления характеризуется только прямым умыслом. В случае если в результате неправомерного доступа к системе ЭВМ управляющие процессами связанными с повышенной опасностью, например система управления атомной станцией, в результате уничтожения, блокирования, модифицирования информации была нарушена работа реактора, что привело к тяжким последствиям, даже если наступление этих последствий не охватывалось умыслом лица, уголовная ответственность за такие последствия наступает 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. 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](http://www.relcom.ru/Archive/1997/ComputerLaw/RussiaLaws/Crime2.htm#st272), может быть лицо, достигшее 16-летнего возраста, однако часть вторая предусматривает наличие специального субъекта совершившего данное преступление с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети. Под доступом в данном случае понимается фактическая возможность использовать ЭВМ, при отсутствии права на работу с защищенной информацией. Например, инженер по ремонту компьютерной техники имеет доступ к ЭВМ в силу своих служебных обязанностей, но вносить какие либо изменения в информацию находящуюся в памяти ЭВМ не имеет права.

**Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ**

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Под вредоносными программами в смысле [ст. 273](http://www.relcom.ru/Archive/1997/ComputerLaw/RussiaLaws/Crime2.htm#st273)УК РФ понимаются программы специально созданные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций для которых эти программы предназначены, определенные в документации на программу. Наиболее распространенными видами вредоносных программ являются "компьютерные вирусы" и "логические бомбы".

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

***"Логические бомбы"*** - 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.

Объективную сторону данного преступления составляет факт создания программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети (см. комментарий к [ст.272](http://www.relcom.ru/Archive/1997/ComputerLaw/RussiaLaws/Crime2.htm) п.1), а равно использование либо распространение таких программ или машинных носителей с такими программами.

Под использованием программы понимается выпуск в свет, воспроизведение, распространение и иные действия по их введению в оборот. Использование может осуществляться путем записи программы в память ЭВМ, на материальный носитель, распространение по сетям либо путем иной передачи другим лицам.

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. По смыслу [ст. 273](http://www.relcom.ru/Archive/1997/ComputerLaw/RussiaLaws/Crime2.htm#st273) наличие исходных текстов вирусных программ уже является основанием для привлечения к ответственности. Однако следует учитывать, что в ряде случаев использование подобных программ не будет являться уголовно наказуемым. Это относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих лицензию на деятельность по защите информации, выданную Государственной технической комиссией при Президенте.

Формой совершения данного преступления может быть только действие выраженное в виде создания вредоносных программ для ЭВМ, внесения изменений в уже существующие программы, а равно использование либо распространение таких программ. Распространение машинных носителей с такими программами полностью покрывается понятием распространения.

3. С субъективной стороны преступление, предусмотренное частью 1 [ст.273](http://www.relcom.ru/Archive/1997/ComputerLaw/RussiaLaws/Crime2.htm#st273), может быть совершено только с прямым умыслом, так как в статье определено, что 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 только умышленно, так как в соответствии со с частью 2 [ст. 274](http://www.relcom.ru/Archive/1997/ComputerLaw/RussiaLaws/Crime2.htm#st274)УК РФ деяние, совершенное по неосторожности, признается преступлением только в том случае, когда это специально предусмотрено соответствующей статьей Особенной части настоящего Кодекса.

Часть 2 [ст. 272](http://www.relcom.ru/Archive/1997/ComputerLaw/RussiaLaws/Crime2.htm#st274)в отличие от части первой в качестве квалифицирующего признака предусматривает наступление тяжких последствий по неосторожности. Разработка вредоносных программ доступна только квалифицированным программистам, которые в силу своей профессиональной подготовки должны предвидеть возможные последствия использования этих программ.

В случае если установлен прямой умысел охватывающий и наступление тяжких последствий, квалификация данного преступления должна основываться на цели, которая стояла перед виновным, в этом случае создание программы либо внесение изменений в программу будут являться только способом совершения преступления и в этом случае должна применяться ст. 17 п.2 УК РФ. Субъектом данного преступления может быть любой гражданин, достигший 16 лет.

#### Заключение

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

Преступления в сфере компьютерной информации имеют, на мой взгляд, как бы двоякий смысл, и поэтому требуют специальных статей в Уголовном кодексе. Принятый в недавнем прошлом кодекс содержит целую главу, включающую в себя три статьи, что, на мой взгляд, несколько мало. Даже исходя из дословного толкования, позволю себе сказать, что они уже несколько устарели по смысловому значению, и требуют обновлений.

Создать абсолютно стойкую систему защиты также невозможно, как невозможно создать универсальную систему взлома. Поэтому при использовании системы защиты необходимо четко представлять диапазон ее применимости и ее способность противостоять воздействию злоумышленников разной квалификации и оснащенности. Разработка проблемы компьютерной преступности и поиск методов борьбы с нею всего лишь дело времени и опыта. И российские криминологи и криминалисты внесут в это свой вклад. Ели только российские политики не дадут им умереть с голоду.

## Список использованной литературы

1. Уголовный кодекс Российской Федерации – СПб.: Альфа, 1999;
2. Федеральный закон "Об информации, информатизации и защите информации" от 3. 20 февраля 1995 года №24-ФЗ;
3. Закон Российской Федерации "Об авторском и смежных правах" от 9 июля 1993 года №5351-1;
4. Закон Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" от 23 сентября 1992 года №3523-1;
5. Наумов А.В. Комментарий к Уголовному кодексу. – М.: Юристъ, 1997;
6. Hackzone – территория взлома, №2, 1999 (электронная версия).
7. Ю.Ляпунов, В.Максимов, “Ответственность за компьютерные преступления”, “Законность” №1, 1997г.
8. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность. - М., 1998
9. Ведеев Д.В. Защита данных в компьютерных сетях. - М., 1995;
10. Здравомыслов Б.В. Уголовное право России. Особенная часть. – М.: Юристъ, 1996;
11. Фоменков Г.В. «О безопасности в Internet» // «Защита информации. Конфидент», № 6, 1998;
12. Гайкович В.Ю “Основы безопасности информационных технологий”, Москва, “Инфо-М”;
13. Ю.Ляпунов, В.Максимов, “Ответственность за компьютерные преступления”, “Законность” №1, 1997г;
14. D.J.Icove, Как бороться со взломщиками компьютеров, Сети и Телекоммуникации, №4, 1997г.