Федеральное государственное образовательное бюджетное учреждение

высшего профессионального образования

ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Кафедра «Информационные технологии»

Реферат

На тему: «Компьютерные преступления»

Выполнила:

студентка группы ФК 1-3

Тимошкина Ю.М.

Научный руководитель:

доцент Магомедов Р.М.

Москва 2010

Оглавление

[Список иллюстраций 2](#_Toc278838729)

[Введение 3](#_Toc278838730)

[Понятие киберпреступление (компьютерное преступление) и основные присущие ему черты 5](#_Toc278838731)

[Преступления в сфере компьютерной информации 7](#_Toc278838732)

[Нормативно-правовые акты 7](#_Toc278838733)

[Неправомерный доступ к компьютерной информации (ст. 272 УК) 8](#_Toc278838734)

[Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК) 8](#_Toc278838735)

[Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК) 9](#_Toc278838736)

[Другие примеры 9](#_Toc278838737)

[Нелегальное получение товаров и услуг 9](#_Toc278838738)

[Незаконный доступ к информации, ее подделка или хищение 10](#_Toc278838739)

[Мошенничество в сфере электронной торговли и инвестирования 11](#_Toc278838740)

[Электронный вандализм и терроризм 11](#_Toc278838741)

[Электронное отмывание денег и уклонение от налогов 12](#_Toc278838742)

[Мошенничество с переводом электронной наличности 13](#_Toc278838743)

[Распространение нелегальных материалов 13](#_Toc278838744)

[Меры противодействия компьютерным преступлениям 15](#_Toc278838745)

[Заключение 16](#_Toc278838746)

# Список иллюстраций

[Рисунок 1 Компьютерные преступления (2004 - 2005гг) 7](#_Toc278838747)

Рисунок 2 Хакерство 10

Рисунок 3 Мошенничество с переводом электронной наличности 13

# Введение

Информационные технологии, основанные на новейших достижениях электронно-вычислительной техники, которые получили название новых информационных технологий (НИТ), находят все большее применение в различных сферах деятельности. Новые информационные технологии создают новое информационное пространство и открывают совершенно новые, ранее неизвестные и недоступные возможности, которые коренным образом меняют представления о существовавших ранее технологиях получения и обработки информации, в большей степени повышают эффективность функционирования различных организаций, способствуют их большей стабильности в конкурентном соперничестве.

Однако, вместе с положительными и, безусловно, необходимыми моментами компьютеры и НИТ привносят и новую головную боль, как бы еще раз констатируя правило, в котором утверждается, что за все надо платить. Эта боль, прежде всего, связана с проблемами обеспечения информационной безопасности. Предоставляя огромные возможности, информационные технологии, вместе с тем, несут в себе и большую опасность, создавая совершенно новую, мало изученную область для возможных угроз, реализация которых может приводить к непредсказуемым и даже катастрофическим последствиям. Ущерб от возможной реализации угроз можно свести к минимуму только приняв меры, которые способствуют обеспечению информации.

В настоящее время компьютерная преступность, приобретшая международный масштаб, уже получает адекватную оценку международным сообществом, что в частности получило отражение в специальной Конвенции по борьбе с киберпреступностью, подписанной в 2001 году в Будапеште представителя 30 государств – членов Совета Европы. О масштабах виртуальной преступности с использованием Интернета только в США можно судить по следующим цифрам: в 2001 году общий ущерб государственным и коммерческим структурам Америки от компьютерных хакеров составил около 400 млн. дол. США, их них ущерб от кражи информации оценивается в 150 млн., от мошенничества – в 100 млн. долл. США[[1]](#footnote-1).

Целью представленного реферата является исследование такого феномена как компьютерная преступность путем формулирования понятия «компьютерные преступления», выделение их особенностей в ряду других, некомпьютерных преступлений – таковы задачи работы.

# Понятие киберпреступление (компьютерное преступление) и основные присущие ему черты

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

Встал вопрос о контролируемости доступа к информации, ее сохранности и доброкачественности. Организационные меры, а также программные и технические средства защиты оказались недостаточно эффективными.

Особенно остро проблема несанкционированного вмешательства дала о себе знать в странах с высокоразвитыми технологиями и информационными сетями.

Компьютерные преступления чрезвычайно многогранные и сложные явления. Объектами таких преступных посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты или программное обеспечение и базы данных, для которых технические средства являются окружением; компьютер может выступать как предмет посягательств или как инструмент.

Специалисты считают, что все компьютерные преступления имеют ряд отличительных особенностей. Во-первых, это высокая скрытность, сложность сбора улик по установленным фактам. Отсюда сложность доказательств при рассмотрении в суде подобных дел. Во-вторых, даже единичным преступлением наносится весьма высокий материальный ущерб. В-третьих, совершаются эти преступления высоко квалифицированными системными программистами, специалистами в области телекоммуникаций.

Виды компьютерных преступлений чрезвычайно многообразны. Это и несанкционированный доступ к информации, хранящейся в компьютере, и ввод в программное обеспечение "логических бомб", которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему, и разработка и распространение компьютерных вирусов, и хищение компьютерной информации. Компьютерное преступление может произойти также из-за небрежности в разработке, изготовлении и эксплуатации программно-вычислительных комплексов или из-за подделки компьютерной информации.

# Преступления в сфере компьютерной информации

До недавнего времени, а именно до 1 января 1997 года, даты вступления в действие нового Уголовного Кодекса Российской Федерации (УК РФ), в России отсутствовала возможность эффективно бороться с компьютерными преступлениями. Несмотря на явную общественную опасность, данные посягательства не были противозаконными, т.е. они не упоминались нашим уголовным законодательством. Хотя, еще до принятия нового УК в России была осознана необходимость правовой борьбы с компьютерной преступностью. Был принят ряд законов, которые внесли правовую определенность в явление компьютеризации нашего общества вообще и проблему компьютерной преступности в частности и вместе с другими правовыми актами сформировали пласт, именуемый "законодательством в сфере информатизации", охватывающий в настоящее время несколько сотен нормативно-правовых актов.

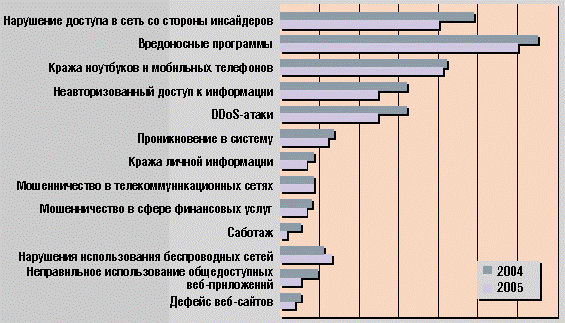


Рисунок Компьютерные преступления (2004 - 2005гг)

## Нормативно-правовые акты

Преступлениями в сфере компьютерной информации являются:

* Неправомерный доступ к компьютерной информации (ст.272 УК РФ);
* Создание, использование и распространение вредоносных программ для ЭВМ (ст.273 УК РФ);
* Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ);

### Неправомерный доступ к компьютерной информации (ст. 272 УК)

Уголовная ответственность за неправомерный доступ к компьютерной информации установлена ст. 272 УК РФ. Непосредственным объектом данного преступного деяния являются общественные отношения, обеспечивающие безопасность информационных систем от внешних воздействий сточки зрения конфиденциальности содержащейся в них компьютерной информации. Конфиденциальность понимается как предотвращение возможности использования информации лицами, которые не имеют к ней отношения. Предметом преступления является компьютерная информация, охраняемая законом, находящаяся либо на машинном носителе, либо в ЭВМ, либо в системе ЭВМ или в сети ЭВМ.

Особо следует отметить компьютерную информацию, собственником которой является государство или его субъекты и образования.

### Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК)

Под распространением программ в соответствии с законом понимается предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей. Распространением вредоносных программ является не только передача самих программ в виде набора объектных кодов, но и опубликование или индивидуальная рассылка исходных текстов подобных программных продуктов. Указанные действия должны находиться в причинной связи с наступившими последствиями - уничтожением, блокированием, модификацией либо копированием информации, нарушением работы ЭВМ, системы ЭВМ или их сети.

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

Непосредственным объектом данного преступного деяния являются общественные отношения, обеспечивающие внутреннюю безопасность информационных систем, базирующихся на использовании ЭВМ, системы ЭВМ или их сети с точки зрения целостности и конфиденциальности содержащейся в них компьютерной информации. Объективная сторона данного деяния заключается в действиях или бездействии лица, которое в соответствии с правилами, установленными собственником информационной системы, обязано было осуществлять операции с компьютерной информацией в определенном порядке, но не соблюдало эти правила, и это послужило причиной уничтожения, блокирования или модификации информации.

## Другие примеры

### Нелегальное получение товаров и услуг

Этот очень распространенный вид преступления заключается в получении товара или услуги либо бесплатно, либо за счет другого лица. Наиболее часто встречающейся его разновидностью является бесплатное пользование услугами связи, предоставляемыми за плату различными телефонными компаниями. Такие преступления начали отмечаться с 1961 года. Пользуясь тем, что многие телекоммуникационные системы, по сути дела, представляют собой компьютерные сети, мошенники поначалу путем нехитрых манипуляций эксплуатировали служебные каналы этих систем. Зная, что оба конца каждого служебного канала имеют отдельные, закрепленные за ними номера, преступники входили в этот канал, вызывали один из его концов и получали возможность использовать канал связи бесплатно и сколь угодно долго. Со временем преступные методы стали совершенствоваться и распространились на остальные каналы систем связи. В 60-х годах был создан "синий ящик" - устройство для генерации тональных сигналов готовности, - который позволял преступнику бесплатно использовать телекоммуникационную систему, выдавая себя за ее технического работника. Делалось это примерно так: пользуясь тем, что в традиционной телефонной линии тональные сигналы управления передаются по тем же линиям, что и информация, мошенники, скажем в Германии, набирали бесплатный телефонный номер в США и соединялись с оператором коммутатора, затем связь прерывалась посылкой сигнала отбоя, но сама линия удерживалась открытой за счет посылки сигнала удержания. После этого набирался необходимый номер в США, и разговор велся бесплатно. Благодаря мерам противодействия, предпринятым телефонными компаниями, этот способ сейчас работает только между ограниченным количеством стран.

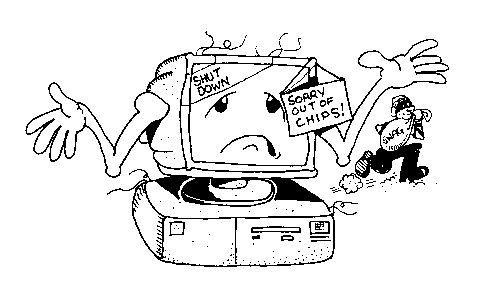
### Незаконный доступ к информации, ее подделка или хищение

Объектом этого весьма распространенного преступления является интеллектуальная собственность, рыночная информация (например, о новых продуктах, клиентуре и т.д.). Как правило, такие преступления совершаются с целью нанести ущерб конкурентам по бизнесу или разорить их.

Несанкционированный доступ к информации, хранящейся в компьютере, осуществляется обычно путем использования чужого имени, изменения физических адресов технических устройств, использования информации, оставшейся после решения тех или иных задач, модификации программного и информационного обеспечения, хищения носителя информации, установки аппаратуры перехвата в каналах передачи данных.

Мы здесь не будем говорить о "хакерах", которые взламывают чужие информационные сети ради забавы, любопытства или из желания доказать себе и другим, что это им под силу. Давайте сосредоточимся на тех, кто совершает такие действия со злым умыслом.

Рисунок Хакерство



Несанкционированное изменение и подделка данных является, пожалуй, наиболее молодой разновидностью компьютерных преступлений, которая, если верить статистике, практикуется прежде всего в отношении медицинских (37%) и финансовых (21%) учреждений и совершается, как правило, либо конкурентами, либо по их заказу. Причем этот вид правонарушения требует от его исполнителя весьма высокой квалификации. Идея преступления состоит в изменении выходной информации компьютеров с корыстной целью. Объектом подделки может выступать практически что угодно: данные о результатах выборов, голосований, референдумов, детали уголовных дел, базы данных, конфиденциальная информация фирм, которая используется их руководством для принятия важных решений и т.д. К примеру, в большинстве западных банков операции по оценке степени доверия к потенциальному получателю банковского кредита автоматизированы. Зная алгоритмы этой оценки, хороший специалист может изменить исходные данные или сам алгоритм оценки с целью мошеннического получения крупной денежной суммы.

### Мошенничество в сфере электронной торговли и инвестирования

Данный вид преступлений основан на уникальных возможностях в плане дезинформации потенциальных жертв, которые предоставляет мошенникам система Интернет, где любая информация может распространяться абсолютно анонимно, с минимальными затратами, практически мгновенно и на огромную аудиторию. Такая оперативность и безопасность делают упомянутый "бизнес" весьма привлекательным. Ну а сферы деятельности здесь практически не ограничены: продажа несуществующих товаров, предложение мифических услуг, привлечение средств на ложную благотворительность, азартные игры (лотереи, казино, тотализаторы), традиционные финансовые пирамиды, инвестиционные проекты, которые сулят якобы огромные доходы, фиктивные брачные конторы: Всего не перечесть. Ставка здесь делается на тех, у кого жадность или доверчивость преобладают над здравым смыслом. И, как ни странно, таких людей в мире оказывается еще достаточно много. Ну а мошенники, набрав с миру по нитке себе на приличный гардероб, бесследно исчезают, чтобы через некоторое время появиться под новой вывеской и с новым проектом.

### Электронный вандализм и терроризм

Данный вид преступности представляет очень серьезную проблему, поскольку сегодня от нормального функционирования компьютерных сетей и систем связи зависят и экономика, и управление, и даже отдельные граждане большинства стран мира. Мотивами такого рода преступлений могут быть либо желание проявить себя, либо желание отомстить, либо желание расправиться с конкурентом. Но каким бы мотивом ни руководствовался преступник, повреждение компьютерных систем или вмешательство в их работу могут приводить к очень серьезным, а иногда и катастрофическим последствиям. А случаев такого вмешательства не перечесть. Причем они имеют место на всех уровнях, вплоть до самых высоких. Так, в 1992 году в результате "заражения" компьютера Игналинской атомной электростанции в Литве мог повториться Чернобыль; в 1998 году были зарегистрированы попытки нарушить работу компьютерной системы правительства Шри-Ланки; в 1999 году во время бомбардировок Белграда была предпринята попытка нарушить работу компьютерной системы НАТО.

Электронный вандализм и терроризм осуществляются путем внедрения в компьютерные системы и сети таких программ, которые способны повредить или уничтожить внутреннюю информацию в ПК. Особенно широко программы-вредители распространяются через нелегальные копии программных продуктов. Ниже приводится классификация известных диверсионных программ.

### Электронное отмывание денег и уклонение от налогов

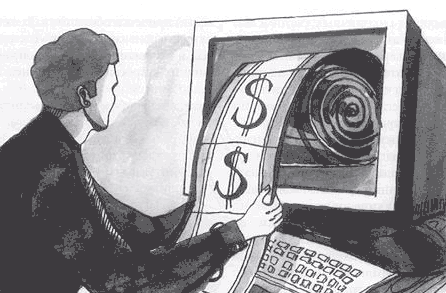
Стремительное развитие компьютерных и телекоммуникационных систем привело к появлению электронной наличности и возникновению глобальной системы электронных денежных расчетов, вокруг которой не замедлила сформироваться параллельная банковская система с целой сетью полулегальных финансовых учреждений. Быстро сложившаяся новая инфраструктура тут же привлекла внимание преступных сообществ своими уникальными возможностями. Она позволила переводить денежные средства в любую страну земного шара быстро, анонимно, по чрезвычайно запутанным маршрутам и в обход государственных систем финансового контроля. С тех пор электронные переводы стали использоваться преступниками как эффективный инструмент, позволяющий без особого труда скрывать источники поступления денежных средств, отмывать преступно нажитые деньги и укрывать свои доходы от налогообложения.

### Мошенничество с переводом электронной наличности

Этот вид преступлений заключается в изменении информации, отображающей электронную наличность на счетах в системе электронных банковских расчетов.

Известно несколько способов такого мошенничества. В одном из них информация о наличности, имеющейся на счетах клиентов, переписывается на счета, которыми распоряжаются преступники. В другом - модифицируется алгоритм, по которому функционирует система обработки информации об электронных банковских расчетах. Например, занижается коэффициент исчисления курса валют при их обмене, а итоговая разница от каждой операции обмена зачисляется на счета преступников. Существует способ, когда десятичные доли, образующиеся в результате финансовых расчетов, автоматически переводятся на счет преступника, что при большом количестве денежных операций дает весьма внушительные суммы.

Рисунок Мошенничество с переводом электронной наличности



### Распространение нелегальных материалов

Этот вид преступления, процветающий в системе Интернет, задевает интересы как отдельной личности, так и общества в целом. Используя возможности информационных сетей, преступники распространяют порнографию (в том числе и детскую), материалы, рекламирующие насилие и расизм или порочащие отдельных лиц. Нередко распространение незаконных материалов преследует политические цели. Достаточно вспомнить недавние случаи использования интернетовских сайтов чеченскими боевиками в попытке дискредитировать правительство РФ.

# Меры противодействия компьютерным преступлениям

В настоящее время все меры противодействия компьютерным преступлениям можно подразделить на технические, организационные и правовые.

К техническим мерам можно отнести защиту от несанкционированного доступа к компьютерной системе, резервирование важных компьютерных систем, принятие конструкционных мер защиты от хищений и диверсий, обеспечение резервным электропитанием, разработку и реализацию специальных программных и аппаратных комплексов безопасности и многое другое.

К организационным мерам относятся охрана компьютерных систем, подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство) , возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п. В мире и нашей стране техническим и организационным вопросам посвящено большое количество научных исследований и технических изысканий.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие соответствующих международных. Только в последние годы появились работы по проблемам правовой борьбы с компьютерной преступностью, (в частности, это работы Ю. Батурина, М. Карелиной, В. Вехова) и совсем недавно отечественное законодательство встало на путь борьбы с компьютерной преступностью. И поэтому, представляется весьма важным расширить правовую и законодательную информированность специалистов и должностных лиц, заинтересованных в борьбе с компьютерными преступлениями.

# Заключение

Компьютер стал любимым детищем человека. Уровень развития страны во многом определяется по уровню компьютеризации. С вычислительной техникой человечество связывало надежды на резкий скачок в интеллектуальной и духовной областях, информатике, сервисе, обороноспособности и многое другое, что может сделать нашу жизнь беззаботнее.

Но к сожалению, далеко не всем надеждам удалось осуществиться. Наряду с несомненными благами компьютеризация еще более нарушила нашу безопасность. Количество ошибок, связанных с неправильным использованием вычислительной техники, с переоценкой ее надежности и защищенности, постоянно растет. В ПК и в вычислительных сетях сосредотачивается информация, исключительное пользование которой принадлежит определенным лицам или группам лиц, действующем в порядке личной инициативы или в соответствии с должностными обязанностями. Такая информация должна быть защищена от всех видов постороннего вмешательства. К тому же в вычислительных сетях должны принимать меры по защите вычислительных ресурсов сети от их несанкционированного использования, т.е. доступа к сети лиц, не имеющих на это права. Физическая защита более надежна в отношении компьютеров и узлов связи, но оказывается уязвимой для каналов передачи данных большой протяженности. Защита сетей приобретает все более важное значение, однако, не все считают, что это наилучшее решение проблемы защиты. Эту проблему следует рассматривать глобально. Необходимо защищать информацию на всем пути ее движения от отправителя до получателя.

1. И.М. Рассолов. Право и Интернет, С. 251 [↑](#footnote-ref-1)