**Содержание**

Введение

## 1 Понятие и криминологическая характеристика компьютерной преступности

## 2 Система компьютерных преступлений, совершаемых с использованием компьютерной информации

## 3 Квалификация преступлений в сфере компьютерной информации

## 4 Контроль над компьютерной преступностью в России

## Заключение

## Список использованных источников и литературы

**Введение**

Одним из достижений научно – технической мысли человека стало внедрение в управленческий процесс и другие сферы жизни общества электронно-вычислительной техники, без которой хранение, обработка и использование огромного количества самой разнообразной информации не было невозможным. Это достижение принесло неоценимую пользу в развитие науки, техники и других отраслей знаний. Однако выгоды, которые можно получить благодаря использованию этой техники, стали использоваться и в преступных целях. Так, появился новый вид преступной деятельности – компьютерные преступления, общественно – опасные последствия от совершения которых не шли в сравнение с ущербом от других преступлений. По оценкам экспертов правоохранительных органов стран Центральной и Восточной Европы по вопросам борьбы с компьютерной преступностью, прибыли преступников от преступлений в сфере использования электронно-вычислительных машин занимают третье место после доходов наркоторговцев и от продажи оружия, а нанесенный ущерб уже сейчас оценивается миллиардами долларов. Только в США ежегодно экономические убытки от такого рода преступлений составляют около ста миллиардов долларов. К середине восьмидесятых годов прошлого столетия в Великобритании убытки от компьютерных преступлений составляли 750 миллионов фунтов стерлингов. В настоящее время они возросли вдвое.[[1]](#footnote-1)

*Актуальность* рассматриваемой проблемы в том, что компьютерная преступность становится одним из наиболее опасных видов преступных посягательств. Проблемы информационной безопасности постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных, и, прежде всего, вычислительных систем.

Изучение проблем расследования преступлений в сфере компьютерной информации выступает одной из острейших задач современной криминалистической науки. Несмотря на то, что в последние годы в криминалистической литературе уделяется повышенное внимание методике расследования компьютерных преступлений, в этой области еще остается ряд нерешенных и дискуссионных вопросов.

*Объект исследования* составляет правовой аспект уголовной ответственности за компьютерную преступность.

*Предметом исследования* является компьютерная преступность как современная криминологическая проблема.

В связи с вышесказанным сформулируем *цели* и *задачи* контрольной работы.

*Целью работы –* является раскрытие понятия компьютерной преступности, выявление мер контроля над компьютерной преступностью, направленности действий комплекса факторов, снижающих ее эффективность. А также выработка всесторонней стратегии по профилактике и борьбе с компьютерной преступностью, и формулирование предложений повышения эффективности контроля над компьютерной преступностью в России.

Для достижения поставленной цели следует решить ряд *задач*:

1. рассмотреть понятие и дать характеристику компьютерной преступности;

2. изучить систему компьютерных преступлений;

3. рассмотреть квалификацию преступлений в сфере компьютерной информации;

4. ознакомиться с отечественным опытом в борьбе с компьютерными преступлениями.

*Структура работы* обусловлена ее целью и задачами, содержанием, взаимосвязью рассмотренных в работе проблем и соответствует логике проведенного исследования. Она состоит из введения, четырех основных глав, заключения. В конце работы приведен список литературы, использованный при ее написании, включающий 16 источников.

## 1. Понятие и криминологическая характеристика компьютерной преступности

Компьютерная сеть Интернет стремительно превратилась в общепланетарную информационную систему (для кого-то она глобальный справочник, для кого-то библиотека мировой культуры, для кого-то трибуна собственных суждений), она вобрала в себя не только достоинства глобальности, но и глобальные пороки. Возможности Сети все чаще становятся средством совершения противоправных деяний.

*Компьютерная преступность* – это совокупность компьютерных преступлений, где компьютерная информация является предметом преступных посягательств, а также преступлений, которые совершаются посредством общественно опасных деяний, предметом которых является компьютерная информация. Эти деяния посягают на безопасность сферы компьютерной информации, являются одним из наиболее опасных и вредоносных явлений современного мира.[[2]](#footnote-2)

С точки зрения уголовного законодательства Российской Федерации к компьютерным преступлениям относятся, во-первых, преступления в сфере компьютерной информации (ст. 272 – 274 УК РФ). Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, ст. 273 предусматривает ответственность и устанавливает наказание за создание, распространение и использование вредоносных программ для ЭВМ, ст. 274 устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Во-вторых, это все преступления, предусмотренные действующим УК РФ, совершающиеся в сфере компьютерной информации. Характерной особенностью многих компьютерных преступлений является то, что их предметом выступает компьютерная информация с целью приготовления к другим правонарушениям. В связи с этим недопустимо включать в компьютерные преступления только общественно опасные деяния, предметом которых является компьютерная информация.

Определение компьютерных преступлений как общественно опасных деяний, предметом либо орудием совершения которых являются средства вычислительной техники и компьютерная информация, имеет слишком широкие и нечеткие границы. Под данное определение подпадают многие преступления, в том числе и совершенно не имеющие отношения к преступлениям в сфере высоких технологий. *Например*, нанесение ноутбуком (переносным компьютером) тяжких телесных повреждений или умышленное уничтожение склада оргтехники. К компьютерным преступлениям, учитывая установленные в определении признаки, можно отнести клевету, распространенную через электронные средства информации, изготовление денежных знаков с помощью ксерокса и многое другое.

Совокупность преступлений в сфере компьютерной информации и опосредованных общественно опасных деяний образует другую часть компьютерной преступности. Симбиоз (сосуществование) этих общественно опасных деяний способен причинить значительный вред практически любым интересам личности, государства и общества.

*Компьютерные преступления против конституционных прав и свобод человека и гражданина.*

Одним из самых распространенных компьютерных преступлений является компьютерное пиратство. Действия компьютерных пиратов заключаются в незаконном копировании и распространении программ для ЭВМ и баз данных (в том числе и сетевым способом). Общественная опасность этих действий заключается в способности причинять существенный вред правоотношениям, возникающим в связи с созданием, правовой охраной (охрана авторских и других прав) и использованием программ для ЭВМ и баз данных. Кроме того, компьютерное пиратство наносит значительный экономический ущерб. Ассоциация производителей компьютерного обеспечения установила, что спрос на рынке программ для ЭВМ и баз данных удовлетворяется пиратской продукцией на 94%. Услугами компьютерных пиратов и контрафактной продукцией пользуются не только граждане, но и государственные учреждения.

Среди компьютерных преступлений против конституционных прав и свобод человека и гражданина следует выделить различные способы нарушения тайны электронных сообщений и неправомерный доступ в автоматизированные системы подсчета голосов. *Например*, при проведении выборов в различные органы государственной власти или во время работы Федерального Собрания вполне могут иметь место факты неправомерного доступа в их компьютерные системы или внедрения в них вредоносных программ для ЭВМ. Это, в частности, подтверждается зарубежным опытом использования автоматизированных систем, обеспечивающих работу государственных органов.

*Компьютерные преступления в сфере экономики.*

К данным преступлениям относятся различные формы хищения путем неправомерного доступа в автоматизированные системы обеспечения деятельности различных учреждений. Хищения подобным способом в большинстве случаев совершаются лицами, имеющими доступ к информационным ресурсам финансовых учреждений. Результаты исследований, проведенных с участием российских банкиров, показали, что две трети компьютерных преступлений совершаются с участием технического персонала банков. Эти лица могут совершать преступления самостоятельно (в одиночку) с соисполнителем либо в составе преступных формирований.

*Пример:* В г. Москве была пресечена деятельность преступной группы, занимавшейся хищениями денежных средств в международной межбанковской системе электронных платежей. В состав группы входил экономист одного из коммерческих банков столицы, который с целью хищения ввел известный ему код идентификации пользователя компьютерной сети электронных платежей банка и несанкционированно списал с корреспондентского счета 300 тыс. долл. Далее часть средств была перечислена на счет московского представительства одной из зарубежных фирм и похищена.

К этой категории компьютерных преступлений относятся также действия, направленные на изготовление кредитных либо расчетных карт.

С помощью поддельных карт преступники осуществляют неправомерный доступ к базам данных финансовых, торговых и иных компаний, а также частных лиц с целью преступного обогащения.

*Пример:* В г. Москве была обезврежена организованная группа из 25 человек, совершившая более 300 хищений с использованием кредитных карт на сумму около 600 тыс. долл. Высокое качество изготовленных кредиток буквально поразило зарубежных экспертов.

*Компьютерные преступления против общественной безопасности.*

Это непосредственно преступления в сфере компьютерной информации, которые структурно включены в разд. IX «Преступления против общественной безопасности и общественного порядка» УК РФ. В качестве примера можно назвать неправомерный доступ в компьютерное обеспечение для осуществления деятельности, создающей повышенную опасность для окружающих.

ЭВМ, системы ЭВМ, сети ЭВМ и их информационное содержание широко применяются в вооруженных силах, космонавтике, атомной энергетике, в наземных, морских, воздушных транспортировках и т.д. Неправомерный доступ в компьютерное обеспечение такой деятельности может причинить ущерб обороноспособности страны, повлечь аварийные ситуации, экологические катастрофы, гибель людей и многое другое. Кроме того, тяжкие последствия и существенный вред могут быть следствием нарушения правил эксплуатации ЭВМ, систем ЭВМ или их сети, которые применяются в деятельности, создающей повышенную опасность. Поэтому не случайно преступления в сфере компьютерной информации, которые являются ключевыми компьютерными преступлениями, введены в разд.   
IX УК РФ наряду деяниями против общественной безопасности, экологическими преступлениями, преступлениями против безопасности движения и эксплуатации транспорта и прочее.

*Компьютерные преступления против государственной безопасности.*

Среди компьютерных преступлений против государственной безопасности следует выделить такие общественно опасные деяния, как неправомерный доступ к государственной тайне и машинном носителе, в ЭВМ, системе ЭВМ, сети ЭВМ и диверсию в сфере компьютерной информации.

Развитие компьютерного информационного пространства и его использование государственными учреждениями открывают неограниченные возможности для осуществления незаконного сбора необходимой информации. Ярким *примером* тотального шпионажа в сфере компьютерной информации является продукция компании «Майкрософт» – мирового монополиста по производству программного обеспечения, которым оснащены девять компьютеров из десяти, используемых в мире. В одном из докладов экспертов Министерства обороны Франции говорится, что программное обеспечение компании «Майкрософт» содержит скрытые программы, предназначенные для неправомерного доступа к информации. В частности, военными делается вывод, что создание и развитие компании осуществлялось при активном участии Агенства Национальной Безопасности США, представители которого и разработали эти программы.

*Диверсия в сфере компьютерной информации* – это уничтожение, блокирование, модификация и копирование компьютерной информации, нарушение работы ЭВМ, системы ЭВМ, сети ЭВМ с целью подрыва экономической безопасности и обороноспособности Российской Федерации.[[3]](#footnote-3)

Диверсия в сфере компьютерной информации может быть связана с информационной войной, которая планируется и ведется с целью достижения информационного превосходства над противником в военное или предвоенное время.

Компьютерная преступность характеризуется высокой латентностью.

В поле зрения правоохранительных органов попадает не более 10 – 15% всех совершаемых компьютерных преступлений. Это связано с тем, что многие из них не всегда обнаруживаются потерпевшими или остаются долгое время незамеченными. Кроме того, пострадавшие от этих преступлений предпочитают не обращаться за помощью в правоохранительные органы. Опрос руководителей и сотрудников служб безопасности российских банков показал, что более 80% из них не готовы к диалогу с правоохранительными органами по вопросам взаимодействия в борьбе с электронным мошенничеством. Похожая ситуация наблюдается и в других странах.

Компьютерная преступность носит организованный и международный (транснациональный) характер, базируется на стремительном развитии и использовании телекоммуникационных средств сообщений. Около 62% компьютерных преступлений совершается в составе организованных групп, в том числе на территории нескольких стран.

*Пример*: Известное преступление В. Левина и других отнесено к категории «транснациональных сетевых компьютерных преступлений», совершаемых преступными международными организациями. В организацию входило 12 человек, из них 10 граждан России и два гражданина Нидерландов. Одни из членов преступной группы проводили неправомерный доступ к компьютерной информации, другие снимали похищенные деньги и осуществляли их транспортировку. В Санкт – Петербурге из офиса АО «Сатурн», принадлежавшего Владимиру Левину и Алексею Галахову, совершались действия по неправомерному доступу в систему управления денежными операциями «Сити – банка» (г. Нью – Йорк, США). Эта система использовалась для расчетов между финансовыми организациями, расположенными по всему миру. Финансовые операции инициировались клиентами при помощи доступа по телефонным каналам связи или с использованием сети передачи данных «Спринт / Теленет». Зная пароли и идентификаторы пользователей, используемые в системе управления денежными операциями «Сити – банка», преступники пытались осуществить 40 переводов на сумму около 10 млн. долл. Реально им удалось незаконно перевести 400 тыс. долл. Счета пострадавших находились в США, Канаде, Аргентине, Новой Зеландии, Колумбии, Гонконге, Индонезии и Уругвае. Переводились похищенные деньги в США, Россию, Финляндию, Нидерланды, Германию, Швейцарию и Израиль.

Компьютерная преступность характеризуется постоянным наращиванием и совершенствованием способов осуществления преступлений. Известно свыше шести видов компьютерных преступлений, каждое из них имеет множество способов совершения. Так, *например*, в кодификатор компьютерных преступлений Генерального Секретариата Интерпола включено семь способов компьютерного мошенничества, четыре способа незаконного копирования, пять способов изменения компьютерных данных, три способа компьютерного саботажа и т.д. Представленные виды компьютерной преступности и их характеристики формировались на протяжении 30 с лишним лет. Изучение данного процесса позволяет выделить специфику причинности и детерминации этого крайне опасного явления.

## 2. Система компьютерных преступлений, совершаемых с использованием компьютерной информации

С учетом распространенности отдельных видов преступлений, совершаемых с использованием компьютерной информации, система компьютерных преступлений может быть построена следующим образом:

I. Преступления против личности;

II. Преступления в сфере экономики;

III. Преступления против общественной безопасности, общественного порядка и общественной нравственности;

IV. Преступления против безопасности государства.[[4]](#footnote-4)

Не ставя целью определение санкций, которые могут быть применены к виновным за совершение ими компьютерных преступлений, диспозиции уголовно – правовых норм могут быть сформулированы в следующей редакции:

I. Преступления против личности

*Компьютерная клевета*

1. Распространение в сети ЭВМ заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию.

2. Компьютерная клевета, соединенная с обвинением лица в совершении тяжкого или особо тяжкого преступления.

*Компьютерное вторжение в частную жизнь*

1. Собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну без согласия путем неправомерного доступа к чужой компьютерной информации.

2. То же деяние, совершенное лицом с использованием своего служебного положения или повлекшее тяжкие последствия.

*Нарушение тайны электронной корреспонденции*

1. Перехват, хищение, использование или предание огласке корреспонденции, отправленной, переданной или полученной через информационно – телекоммуникационные средства, или по установке аппаратуры, для осуществления такого перехвата.

2. Те же деяния, совершенные с использованием своего служебного положения.

II. Преступления в сфере экономики

*Компьютерное хищение*

1. Компьютерное хищение, то есть противоправное безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, совершенное с корыстной целью путем изменения чужой компьютерной информации или путем неправомерного использования этой информации или иного неправомерного воздействия на процесс обработки компьютерной информации.

2. Компьютерное хищение, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба.

3. Компьютерное хищение, совершенное с использованием своего служебного положения или в крупном размере.

4. Компьютерное хищение, совершенное организованной группой или в особо крупном размере.

Значительным размером в статьях настоящей главы признается ущерб, превышающий сто тысяч рублей, крупным – превышающий пятьсот тысяч рублей, и особо крупным – превышающий один миллион пятьсот тысяч рублей.

*Компьютерный экономический шпионаж*

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну путем неправомерного копирования чужой компьютерной информации.

2. Распространение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, полученных путем неправомерного копирования чужой компьютерной информации.

3. Те же деяния, совершенные с использованием своего служебного положения, или причинившие крупный ущерб либо повлекшие иные тяжкие последствия.

*Кража компьютерных услуг*

Умышленное использование компьютера или компьютерной сети с намерением получать компьютерные услуги без разрешения.

*Торговля компьютерными паролями*

1. Торговля неправомерно полученными паролями (устройствами) для доступа к чужой компьютерной информации.

2. Торговля паролями лицом, которому пароли были доверены или стали известны в связи с выполнением им своих служебных обязанностей.

III. Преступления против общественной безопасности, общественного порядка и общественной нравственности.

*Неправомерный доступ к компьютерной информации*

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло изменение информации.

2. То же деяние, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба.

3. То же деяние, совершенное лицом с использованием своего служебного положения или с причинением крупного ущерба.

4. То же деяние, совершенное организованной группой или с причинением особо крупного ущерба либо повлекшее иные тяжкие последствия.

*Кибертерроризм*

1. Уничтожение, модификация или иные неправомерные действия с информацией, обрабатываемой ЭВМ, системой ЭВМ или их сетью, правомерное использование которой создает опасность гибели людей, причинение крупного или особо крупного ущерба либо наступления иных общественно опасных последствий, если эти действия совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на органы власти для принятия ими решения в интересах организаторов кибертерроризма.[[5]](#footnote-5)

2. Те же деяния, совершенные группой лиц по предварительному сговору.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они совершены организованной группой либо повлекли по неосторожности смерть человека или иные тяжкие последствия, а равно сопряжены с посягательством на компьютерную информацию объектов использования атомной энергии, ядерных материалов, радиоактивных веществ или источников радиоактивного излучения.

4. Деяния, предусмотренные частями первой или второй настоящей статьи, если они сопряжены с посягательствами на компьютерную информацию, связанную с национальной безопасностью или национальной обороной либо с техническими приемами или системами Вооруженных сил или военной промышленности.

*Создание, использование и распространение вредоносных программ для ЭВМ*

1. Создание с целью использования, распространения или сбыта программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы компьютерных систем и программ, а также их использование, распространение или сбыт машинных носителей с такими программами.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия.

*Компьютерное хулиганство*

1. Использование ЭВМ, системы ЭВМ или их сети для передачи информации в неприличной форме с целью запугивания, унижения чести и достоинства или угрозы совершения в отношении лица или группы лиц аморальных или незаконных действий.

*Компьютерная порнография*

1. Незаконное распространение или рекламирование компьютерной информации порнографического характера.

2. Те же действия, сопряженные с распространением или рекламированием компьютерной информации в отношении заведомо несовершеннолетних или малолетних.

IV. Преступления против государственной безопасности

*Компьютерный шпионаж*

1. Неправомерный доступ к охраняемой законом компьютерной информации для собирания сведений, составляющих государственную тайну, или иных сведений с целью их использования в ущерб интересам Российской Федерации.

В настоящее время в России нет такого размаха компьютерной преступности, которая есть в некоторых странах Американского континента, Центральной и Восточной Европы. Но успокаиваться не следует. Она к нам придет, и уголовный закон наряду с другими мерами профилактического характера должен стать реальным превентивным средством, способствующим созданию условий для нормального развития телекоммуникационных систем и охраны их от преступных посягательств. Уголовно – правовые нормы об ответственности за компьютерные преступления (ст. 272 – 274 УК РФ) не отвечают этому требованию.[[6]](#footnote-6)

## 3. Квалификация преступлений в сфере компьютерной информации

## Как показывает практика, квалификация преступлений, совершаемых в сфере компьютерной информации, представляет определенные трудности.

Особенно при оценке неправомерного доступа к компьютерной информации как самого распространенного общественно опасного деяния в рассматриваемой сфере.[[7]](#footnote-7)

Объективная сторона преступления, предусмотренного ст. 272 УК, выражается в «неправомерном доступе к охраняемой законом компьютерной информации».[[8]](#footnote-8) Неправомерным доступом следует считать также и доступ к информационным ресурсам сети Интернет без согласия собственника или иного законного владельца информации, если это привело к уничтожению, блокированию, модификации или копированию информации, при обязательном условии отсутствия у лица права доступа к ней.

Однако неправильно квалифицировать действия лица как неправомерный доступ к информации, если оно использует чужое сетевое имя и пароль доступа, поскольку основной массив информации в глобальной сети носит открытый характер, информация не запрещена к копированию. Таким образом, уголовно наказуемым данное деяние будет только при условии доступа к информации, охраняемой законом.

Например, нормы ст. 183 УК должны применяться, если виновный, имея умысел на собирание сведений, составляющих коммерческую тайну, при помощи незаконно полученных реквизитов доступа осуществляет копирование информации (баз данных, служебной документации и т.п.) с внутренней локальной сети коммерческой организации. При этом собирание сведений, составляющих коммерческую тайну, должно быть совершено с прямым умыслом, т.е. виновный знает, что его действия направлены на получение сведений, составляющих коммерческую тайну, что искомая информация заведомо обладает всеми признаками коммерческой тайны, и желает собрать именно такую информацию.

*Пример:* Органы предварительного следствия предъявили обвинение по ст. ст. 272 ч. 1, 273 ч. 1 и 183 ч. 1 УК инженеру – электронщику завода «Электроприбор» К., в служебные обязанности которого входила настройка серверов, подключение рабочих станций к локальной сети и регистрация пользователей.

Согласно материалам дела, К. совершил неправомерный доступ к компьютерной информации, не имея соответствующего разрешения для работы с ней, посредством служебной ЭВМ, получив доступ к файловым системам в локальной сети, осуществил несанкционированное копирование на ЭВМ файлов, содержащих информацию об именах пользователей и паролях локальной сети завода.

К. имел право использовать только сетевые ресурсы, предоставленные ему для выполнения служебных обязанностей. Доступ же к базам данных отдела кадров, экономического отдела был ограничен четко определенным кругом лиц, к которому К. не относился, т.е. доступа на законных основаниях к указанной информации не имел.

Приговором суда К. был призван виновным по ст. ст. 272 ч. 1 и 273 ч. 1 УК. Суд счел ст. 183 ч. 1 вмененной излишне, исключил ее из обвинения и оправдал по ней за отсутствием в действиях состава преступления, поскольку умысел К. на сбор информации, составляющей коммерческую тайну, в ходе судебного следствия подтверждения не нашел.

Неправомерный доступ к компьютерной информации должен вменяться в вину наряду с теми преступлениями, ради совершения которых такой доступ осуществляется. Поэтому, если лицо осуществляет неправомерный доступ к информации, а также собирание информации с целью ее последующего разглашения либо незаконного использования, его действия квалифицируются по совокупности ст. ст. 272 и 183 ч. 1 УК. В этой связи представляется целесообразным дополнить ст. 183, расширив перечень способов совершения данного преступления.

Квалифицировать содеянное по совокупности ст. ст. 272 и 165 УК необходимо, если лицо путем обмана, имея умысел на причинение имущественного ущерба собственнику или иному владельцу информации, совершило неправомерный доступ к охраняемой законом информации.[[9]](#footnote-9) *Например*, в целях безвозмездного использования, под чужими реквизитами осуществляет несанкционированные подключения к сети Интернет, достоверно зная, что пользование ресурсами и услугами информационной сети платное.

Стоимость работы автоматически относится на счет легального пользователя, которому блокируется доступ к компьютерной информации, содержащейся в сети, так как работу в сети в одно и то же время с одними и теми же реквизитами может осуществлять лишь один пользователь. Кроме того, искажается информация в базе учетно-статистических данных абонентов (информация о времени начала и продолжительности работы), т.е. причиняется материальный ущерб.

Если же виновный для того, чтобы осуществить неправомерный доступ, использует специальные программы, позволяющие копировать из сети Интернет файлы, содержащие пароли и логины законных пользователей, получая при этом реквизиты доступа в сеть, то содеянное следует квалифицировать также и по соответствующей части ст. 273 УК, предусматривающей уголовную ответственность за использование вредоносных программ для ЭВМ.

Однако, как показывает анализ судебной практики, существует несколько подходов к квалификации рассматриваемых деяний. Так, действия виновного, использующего вредоносную программу для «взлома» паролей доступа в сеть Интернет, а затем совершающего неправомерные выходы в сеть, судами квалифицируются по-разному. Чаще всего – по совокупности ст. ст. 272 и 165 УК (80% приговоров); в 20% случаев, кроме указанных преступлений, виновные осуждены еще по соответствующим частям ст. 273 и 183.

Действия лица, которое неправомерно работает в сети Интернет под незаконно полученными реквизитами, образуют идеальную совокупность преступлений в сфере компьютерной информации и преступлений против собственности, предусмотренных ст. ст. 272 и 165 УК. Однако квалификация действий виновного при незаконном доступе в сеть Интернет по ч. 1 ст. 165 УК, предусматривающей уголовную ответственность за причинение имущественного ущерба собственнику или иному владельцу путем обмана или злоупотребления доверием при отсутствии признаков хищения, весьма спорная. *Например*, в рамках одного уголовного дела одни и те же действия виновного квалифицированы судом как по ч. 1 ст. 272, так и по совокупности ст. ст. 272 ч. 1 и 165 ч. 1 УК.[[10]](#footnote-10)

Встречаются и уголовные дела, где суд в описательно – мотивировочной части приговора наряду с обстоятельствами неправомерного доступа устанавливает также факт причинения имущественного ущерба собственнику информации, определяет его размер, а в резолютивной части действия подсудимого квалифицирует лишь по соответствующей части ст. 272 УК, фактически исключая ст. 165 из объема предъявленного органами предварительного следствия обвинения.

Таким образом, единообразия в судебно – следственной практике при квалификации неправомерного доступа к охраняемой законом компьютерной информации не прослеживается.

## 4. Контроль над компьютерной преступностью в России

Меры контроля над компьютерной преступностью подразделяются на правовые, организационно-тактические и программно-технические.

К ***правовым мерам*** относятся разработка норм, устанавливающих ответственность за совершение компьютерных преступлений, защита авторских прав программистов, а также вопросы контроля за разработчиками компьютерных систем и применение международных договоров об их ограничениях.

К ***организационно-тактическим мерам*** относятся охрана вычислительных центров, тщательность подбора персонала, исключение случаев ведения особо важных работ только одним человеком и т.п.

К ***программно-техническим мерам*** можно отнести защиту от несанкционированного доступа к системе, профилактику от компьютерных вирусов, резервирование особо важных компьютерных подсистем, применение конструктивных мер защит от хищений, саботажа диверсий, взрывов, установку резервных систем электропитания, оснащение помещении кодовыми замками, установку сигнализации и другие меры. [[11]](#footnote-11)

Основной целью государственной политики по выявлению и пресечению компьютерных преступлений является создание эффективной национальной системы борьбы с правонарушениями в сфере компьютерной информации.

Борьба с компьютерной преступностью в России осуществляется в условиях действия *комплекса факторов*, снижающих ее эффективность. По мнению В. Минаева, к наиболее значимым относятся:

– отсутствие отлаженной системы правового и организационно-технического обеспечения законных интересов граждан, государства и общества в области информационной безопасности;

– ограниченные возможности бюджетного финансирования работ по созданию правовой, организационной и технической базы информационной безопасности;

– недостаточное осознание органами государственной власти на федеральном и, особенно, региональном уровне возможных политических, экономических, моральных и юридических последствий компьютерных преступлений;

– слабость координации действий по борьбе с компьютерными преступлениями правоохранительных органов, суда и прокуратуры и неподготовленность их кадрового состава к эффективному предупреждению, выявлению и расследованию таких деяний;

– несовершенство системы единого учета правонарушений, совершаемых с использованием средств информатизации;

– серьезным отставанием отечественной индустрии средств и технологий информатизации и информационной безопасности от мирового уровня.

К *базовым направлениям повышения эффективности контроля над компьютерной преступностью в Росси следует отнести:*

– формирование целостной системы непрерывного отслеживания обстановки в сфере обеспечения информационной безопасности различных систем в стране и упреждающего принятия решений по выявлению и пресечению компьютерных преступлений;

– организация взаимодействия и координация усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой;

– организация эффективного взаимодействия правоохранительной системы России с правоохранительными органами зарубежных стран, осуществляющими борьбу с компьютерными преступлениями;

– координация действий с общественными и частными организационными структурами (фондами, ассоциациями, фирмами, службами безопасности банковских и коммерческих структур), на своем уровне осуществляющими практические мероприятия по обеспечению информационной безопасности.

Создаваемая система должна быть обеспечена высококвалифицированными кадрами. Создание целостной системы обучения, подготовки и переподготовки специалистов по борьбе с компьютерными правонарушениями является одной из основных задач.

## *Уголовно-правовой контроль над компьютерной преступностью в России.*

В целях борьбы с компьютерной преступностью российским законодательством (глава 28 УК РФ) предусмотрена уголовная ответственность за 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).

В соответствии со ст. 272 УК РФ преступлением является 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.

В соответствии со ст. 273 УК РФ, преступлением является 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.

В соответствии со ст. 274 УК РФ, преступлением признается нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.

***Международное сотрудничество***.

В рамках ООН регулярно проводятся симпозиумы по профилактике и пресечению компьютерной преступности, целью которых является поиск адекватных путей противодействия на международном уровне. Кроме того. вырабатываются контрмеры против этого нового вида преступлений и универсально применимые стандарты и нормы, гарантирующие надежное использование компьютерных систем и средств телекоммуникаций.

Признано, что для *выработки всесторонней стратегии по профилактике и борьбе с компьютерной преступностью необходим единый* *coгласованный план действий*, включающий:

– неправительственные мероприятия, под которыми подразумевается программа инициатив по внедрению принципов ответственности в экономике и промышленности, стандартов профессиональной квалификации, технических и процедурных норм, а также этических установок и кодексов поведения;

– правительственные меры, то есть действия правительства на национальном уровне, направленные на совершенствование национального уголовного законодательства, а там, где это необходимо, и промышленного производства средств противодействия компьютерным преступлениям;

– межправительственные меры и международное сотрудничество, направленные на унификацию законодательных актов, развитие международных стандартов и координацию действий органов уголовной юстиции.

*Вывод:* Компьютерные преступления – это своеобразная плата за прогресс в технической сфере. С ростом совершенства компьютерной техники возрастает изощренный характер компьютерной преступности. Соответственно должны совершенствоваться способы борьбы с этим видом преступлений. Этим методы должны носить системный характер и учитывать наряду с другими и социальные аспекты.

**Заключение**

Преступления в сфере компьютерной информации, особенно это касается взлома удаленных компьютеров, являются практически идеальной возможностью для преступников совершать свои деяния без наказания. Практическая возможность доказательства этих преступлений является весьма проблематичной.

Кроме того, парадоксальность компьютерных преступлений состоит в том, что трудно найти другой вид преступлений, после совершения которого его жертва не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность на поприще компьютерного взлома, мало что утаивая от представителей правоохранительных органов.

Этому можно найти объяснения. Во-первых, потерпевшая сторона не всегда стремится афишировать факт несанкционированного проникновения к ее базе данных, поскольку это может вызвать отток клиентуры, обеспокоенной отсутствием действенной системы защиты получаемой и обрабатываемой информации. Во-вторых, преступник, даже получив максимальный срок лишения свободы, чаще всего условный, приобретает широкую известность в деловых и криминальных кругах, что позволяет ему с выгодой использовать приобретенные знания и умения. Вместе с тем одной из основных проблем является отсутствие разработанных методик по проведению компьютерных экспертиз, а также нехватка высококвалифицированных специалистов.

Без грамотного экспертного заключения привлечение лица к уголовной ответственности, даже при наличии признаков состава преступления, становится проблематичным.

Именно поэтому такой высокий процент прекращенных дел по данной категории преступлений. Только ужесточение наказания за данную категорию преступлений могут изменить сложившуюся ситуацию.

**Список использованных источников и литературы**

**Нормативно-правовые акты**

1. Уголовный Кодекс Российской Федерации. – М.: ТК Велби, Изд – во Проспект, 2007. – 192 с.
2. Федеральный закон от 27.07.06 №149-ФЗ «Об информации, информационных технологиях и о защите информации» // Справочная информационно-правовая система Консультант-Плюс
3. Федеральный закон от 9 июля 1993 года №5351–1 «Об авторском и смежных правах» (в ред. Федеральных законов от 19.07.1995 №110-ФЗ, от 20.07.2004 №72-ФЗ) // Справочная информационно-правовая система Консультант-Плюс

**Специальная литература**

1. Комментарий к Уголовному кодексу Российской Федерации (под ред. Лебедева В.М.) – М.: Юрайт – М, 2002
2. Абызов К.Р., Гриб В.Г., Ильин И.С. Криминология: курс лекций / под ред. В.Г. Гриба. – М.: Маркет ДС, 2008. – 352 с.
3. Криминология: учеб. для студентов вузов, обучающихся по специальности «Юриспруденция» (Гуров А.И. и др.); научные редакторы – Н.Ф. Кузнецова, В.В. Лунеев. – М.: Вольтере Клувер, 2005. – 640 с.
4. Криминология: учеб. пособие / Г.И. Бауш и др.; под ред Н.Ф. Кузнецовой. – М.: ТК Велби, Изд – во Проспект, 2007. – 328 с.
5. Криминология: Учебник / Под ред. В.Н. Кудрявцева и В.Е. Эминова – 3 – е изд., перераб. и доп. – М.: Юристъ, 2006 – 734 с.
6. Криминология: Учебник для вузов / под ред. д. ю. н. В.Н. Бурлакова, д. ю. н. Н.М. Кропачева – СПб.: Санкт – Петербургский государственный университет, Питер, 2004. – 427 с. – (Серия «Учебники для вузов»).
7. Криминология: Учебник для вузов / Под общ. ред. д. ю. н., проф. А.И. Долговой. – 3 – е изд., перераб. и доп. – М.: Норма, 2007. – 912 с.
8. Криминология: Учебник для вузов / под ред. проф. В.Д. Малкова – 2 – е изд., перераб. и доп. – М.: ЗАО «Юстицинформ», 2006. – 528 с.
9. Криминология: учеб. пособие / И.А. Моисеева, Г.Г. Шиханцов. – Минск: Амалфея, 2008. – 204 с.

**Материалы периодической печати**

1. Копырюлин А. Квалификация преступлений в сфере компьютерной информации / А. Копырюлин // Законность. – 2007. – №6. – С. 40 – 42.
2. Степанов В. – Егиянц. Ответственность за компьютерные преступления / В. Степанов – Егиянц // Законность. – 2005. – №7. – С. 49 – 51.
3. Талимончик В.П. Информационная безопасность в контексте всеобъемлющей системы международной безопасности / В.П. Талимончик // Правоведение. – 2008. – №2. – С. 103 – 110.
4. Широков В.А., Беспалова Е.В. Компьютерные преступления: основные тенденции развития / В.А. Широков, Е.В. Беспалова // Юрист. – 2006. №10. – С. 18 – 21.

1. Широков В. А., Беспалова Е. В. Компьютерные преступления: основные тенденции развития / В. А. Широков, Е. В. Беспалова // Юрист. – 2006. № 10. С. 18 [↑](#footnote-ref-1)
2. Криминология: Учебник для вузов / Под общ. ред. д. ю. н., проф. А. И. Долговой. – 3 – е изд., перераб. и доп. – М.: Норма, 2007. - С. 735 [↑](#footnote-ref-2)
3. Криминология: Учебник для вузов / Под общ. ред. д. ю. н., проф. А. И. Долговой. – 3 – е изд., перераб. и доп. – М.: Норма, 2007. - С. 743 [↑](#footnote-ref-3)
4. Широков В. А., Беспалова Е. В. Компьютерные преступления: основные тенденции развития / В. А. Широков, Е. В. Беспалова // Юрист. – 2006. № 10. С. 19 [↑](#footnote-ref-4)
5. Талимончик В. П. Информационная безопасность в контексте всеобъемлющей системы международной безопасности / В. П. Талимончик // Правоведение. – 2008. - № 2. С. 106. [↑](#footnote-ref-5)
6. Криминология: учеб. для студентов вузов, обучающихся по специальности «Юриспруденция» (Гуров А. И. и др.); научные редакторы – Н. Ф. Кузнецова, В. В. Лунеев. – М.: Вольтере Клувер, 2005. – С. 345 [↑](#footnote-ref-6)
7. Копырюлин А. Квалификация преступлений в сфере компьютерной информации / А. Копырюлин // Законность. – 2007. - № 6. С. 40 [↑](#footnote-ref-7)
8. Уголовный Кодекс Российской Федерации. – М.: ТК Велби, Изд – во Проспект, 2007. – С. 141 [↑](#footnote-ref-8)
9. Копырюлин А. Квалификация преступлений в сфере компьютерной информации / А. Копырюлин // Законность. – 2007. - № 6. С. 41 [↑](#footnote-ref-9)
10. Уголовный Кодекс Российской Федерации. – М.: ТК Велби, Изд – во Проспект, 2007. – С. 79; 141. [↑](#footnote-ref-10)
11. Криминология: учеб. для студентов вузов, обучающихся по специальности «Юриспруденция» (Гуров А. И. и др.); научные редакторы – Н. Ф. Кузнецова, В. В. Лунеев. – М.: Вольтере Клувер, 2005. - С. 437. [↑](#footnote-ref-11)