**Нижегородский Государственный Университет.**

**Юридический Факультет.**

**Курсовая работа**

По Уголовному праву РФ.

**Тема: Преступления в сфере информационных и компьютерных технологий.**

Выполнил:

Студент 3 курса группы \*\*\*\*

Юридического факультета

#### **Lex**

Научный руководитель:

(рецензент)

## **Нижний Новгород.**

**2002г.**

Содержание.

Введение. 3

2.Компьютерная информация, как объект правовой защиты. 5

3. Общая характеристика преступлений в компьютерной сфере по современному Российскому уголовному законодательству. 9

4. Анализ составов Компьютерных преступлений главы 28 УК РФ 13

4.1 Анализ статьи 272 УК РФ “ Неправомерный доступ к компьютерной информации” 13

4.2 Анализ статьи 273 УК РФ “Создание, использование и распространение вредоносных программ для ЭВМ” 17

4.3 Анализ статьи 274 У КРФ “Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. ” 20

5. Международный и отечественный опыт борьбы с компьютерными преступлениями. 24

6. Заключение. 28

7. Список использованной литературы. 30

*"По-настоящему безопасной можно считать лишь систему, которая выключена, замурована в бетонный корпус, заперта в помещении со свинцовыми стенами и охраняется вооруженным караулом, - но и в этом случае сомнения не оставляют меня".*

*Юджин Х. Спаффорд.*

*Эксперт по информационной безопасности*

# Введение.

"Информационная революция" застигла Россию в сложный экономический и политический период и потребовала срочного регулирования возникающих на ее пути проблем. Между тем, как известно, правовые механизмы могут быть включены и становятся эффективными лишь тогда, когда общественные отношения, подлежащие регулированию, достаточно стабилизировались. 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. Однако на этом пути неизбежны пробы и ошибки, обычные для претворения в жизнь решений, принятых с поспешностью. Важно, что терминологическая неточность изложения закона или методологической рекомендации по его исполнению может повлечь неправильное его применение, а следовательно, и негативные последствия. И если такие ошибки, допущенные в области хозяйственных отношений, могут быть тем или иным образом эффективно исправлены, ошибки в области уголовно-репрессивной отражаются на конституционных правах и свободах конкретных граждан и носят необратимый характер.

В современных условиях трудно переоценить важность точно формализованного представления о сущности и свойствах информации как феномене, над которым осуществляются разнообразные, в том числе и криминальные действия в информационной сфере. Для криминалистических задач раскрытия и расследования преступлений важно иметь стройную систему представлений о сути данного явления и проявляющихся в различных ситуациях его качествах. Развитие и все более широкое распространение информационных и телекоммуникационных технологий, обеспечивающих более эффективное пользование информационными ресурсами, определило необходимость правовой оценки ситуации и разработки организационно - правовых механизмов пресечения общественно опасного поведения (или «криминальной деятельности») в данной области.

Формирование отечественного законодательного регулирования в области информационных правоотношений прошло сложный путь. Признание обществом, а вслед за ним и законодателем факта существования информационного ресурса как реального объекта, имеющего материальное выражение, признание информации в качестве объекта гражданских прав, установление возможности признания права собственности физических и юридических лиц, государства на информацию, информационные системы, технологии и средства их обеспечения повлекло необходимость государственного реагирования в области уголовно-правовых запретов.

Анализ норм действующего УК РФ показывает, что развитие законодательного регулирования информационных правоотношений нашло в нем свое отражение, но для правильного понимания и оценки ряда предусмотренных УК РФ действий в качестве общественно опасных, необходимо привлечение норм всего законодательства, регламентирующих эти действия как незаконные, неправомерные.

Без ясного понимания норм, регулирующих информационные правоотношения, правоохранительные органы не имеют возможности правильно определить круг вопросов, подлежащих доказыванию, а затем и точно квалифицировать выявленные случаи преступлений. Без такого понимания невозможно и создание соответствующих методик расследования преступлений, совершенных в информационной сфере в целом. Между тем, подобные методики расследования криминальной деятельности являются крайне необходимыми в практике, поскольку нередко данная разновидность деятельности является составной частью иных преступлений.

Как следует из Особенной части УК РФ, информационные правоотношения в целом получили в нем широкую уголовно-правовую защиту. Из этого следует, *что информационные отношения стали новым объектом, а информация* - *новым предметом преступного посягательства.* Противоправные действия, связанные с использованием «компьютерных» и (или) «телекоммуникационных» инструментов - лишь специализированная часть преступной деятельности в сфере информации, направленной на нарушение прав и гарантий личности, юридических лиц и государства.

По мере развития технологий электронных платежей, «безбумажного» документооборота и других, серьёзный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике.

Необходимо также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надёжности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

# 2.Компьютерная информация, как объект правовой защиты.

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 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).

Непосредственно Российское информационное законодательство начало формироваться с начала 90-х годов и включало в себя ряд основополагающих законов:

1. Закон “О средствах массовой информации” (27.12.91 г. N 2124-I),
2. Закон “О Федеральных органах правительственной связи и информации” (от 19.02.92 N 4524-1)
3. Закон “О правовой охране топологий интегральных микросхем” (от 23.09.92 г. N 3526-I),
4. Закон “О правовой охране программ для электронных вычислительных машин и баз данных” (от 23.09.92 г. N 3523-I),
5. Закон “Об информации, информатизации и защите информации” (от 20.02.95 г. N 24-ФЗ),
6. Закон “Об участии в международном информационном обмене” (от 5.06.1996 г. N 85-ФЗ).
7. Закон "О правовой охране программ для электронно-вычислительных машин и баз данных" (см. Ведомости РФ, 1992, N 42, ст. 2325) и 20 февраля 1995 (см. СЗ РФ, 1995, N 8, ст. 609).

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 .[[1]](#footnote-1)

Российское законодательство определяет информацию как "сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их предоставления".[[2]](#footnote-2) 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"[[3]](#footnote-3)

В "Толковом словаре по вычислительной технике и программированию" указано, что информация - одно из первичных, не определяемых в рамках кибернетики понятий[[4]](#footnote-4).

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.[[5]](#footnote-5) Относительно природы информации существует еще ряд мнений и точек зрения специалистов как из информационной, так и из юридичесой сферы. На мой 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."[[6]](#footnote-6)

Комментаторами Закона об информации 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".[[7]](#footnote-7)

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...[[8]](#footnote-8) 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. 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 (Федеральный закон "Об информации, информатизации и защите информации").

2. Правовой защите подлежит любая документированная информация, т.е. информация, облеченная в форму, позволяющую ее идентифицировать (Федеральный закон "Об информации, информатизации и защите информации").

3. Документированная информация является объектом гражданских прав и имеет собственника.

4. Информация может быть конфиденциальной, ознакомление с которой ограничивается ее собственником или в соответствии с законодательством, и массовой, предназначенной для неограниченного круга лиц (Федеральный закон "Об информации, информатизации и защите информации").

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 (Закон РФ "Об авторском праве и смежных правах", ст.146 УК РФ);

информация, непосредственно затрагивающая права и свободы гражданина или персональные данные (Федеральный закон "Об информации, информатизации и защите информации", ст.140 УК РФ) и др.

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.

# 3. Общая характеристика преступлений в компьютерной сфере по современному Российскому уголовному законодательству.

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.[[9]](#footnote-9) Составы компьютерных 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.

На мой взгляд необходимо конкретизировать ряд понятиий и определений, используемых в данной главе УК РФ. Необходимый уровень проработки и разъяснения данных понятий дан известным специалистом в этой области Карелиной М.М.[[10]](#footnote-10)

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**.**[[11]](#footnote-11)

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[[12]](#footnote-12).

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. 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).

Рассмотрим подробнее все три статьи УК РФ, ставя целью обрисовать основные признаки совершения компьютерных преступлений.

# 4. Анализ составов Компьютерных преступлений главы 28 УК РФ.

## 4.1 Анализ статьи 272 УК РФ “ Неправомерный доступ к компьютерной информации”

Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, к которому относятся гибкие магнитные диски, магнитно – оптичиские диски, перфокарты, магнитные ленты либо непосредственно в ЭВМ, системе ЭВМ или их сети ), если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем.

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). Данная статья защищает компьютерную информацию любых предприятий, учреждений, организаций и частных лиц. Диспозиция соответствующей нормы заключается в неправомерном доступе к охраняемой законом компьютерной информации.

Неправомерным является доступ, противоречащий действующим правовым нормам, актам управления, приказам, распоряжениям и иным актам, регулирующим отношения по доступу лиц (группы лиц) к информации.[[13]](#footnote-13) 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. [[14]](#footnote-14)

Эта статья, состоящая из 2-х частей, содержит достаточно много признаков, обязательных для объекта, объективной и субъективной сторон состава 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.[[15]](#footnote-15)

**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.

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 неизменненой 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. [[16]](#footnote-16)

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, те. все действия выполненные до формальной подачи последней команды (как например), будут образовывать состав неоконченного преступления.

**Объект** - общественные отношения, связанные с безопасностью использования компьютерной информации.[[17]](#footnote-17)

**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.

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.[[18]](#footnote-18)

Причем в отношении этой информации системы должны приниматься специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ.

Неправомерный доступ к компьютерной информации должен осуществляться умышленно. Совершая это преступление, лицо должно сознавать, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность наступления указанных в законе последствий, желает и сознательно допускает их наступление либо относится к ним безразлично.

**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).[[19]](#footnote-19) Неправомерный доступ к компьютерной информации - умышленное деяние, поскольку в диспозиции ст.272 УК не указано обратное. 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.[[20]](#footnote-20)

**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. Это совершение деяния:

- группой лиц по предварительному сговору,

- организованной группой,

- лицом с использованием своего служебного положения,

- лицом, имеющим доступ к ЭВМ, их системе или сети.

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.

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: кратный минимальному размеру оплаты труда (от 200 до 500) и кратный размеру зарплаты или иного дохода осужденного (период от 2 до 5 месяцев). Исправительные работы могут быть назначены в размере от 6 месяцев до 1 года, а лишение свободы - от 6 месяцев до 2 лет.

Санкция же согласно части 2 статьи ужесточена: в нее введен новый вид наказания (арест на срок от 3 до 6 мес.), размеры остальных увеличены: штраф от 500 до 800 минимальных размеров оплаты труда или зарплаты за период от 5 до 8 месяцев; исправительные работы от 1 года до 2 лет; лишение свободы до 5 лет. При этом надо помнить, что Федеральным законом "О введении в действие Уголовного кодекса Российской Федерации" от 13 июня 1996 г. наказание в виде ареста вводится в действие постепенно, в течение ближайших 5 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.

## 4.2 Анализ статьи 273 УК РФ “Создание, использование и распространение вредоносных программ для ЭВМ”

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. Статья защищает права владельца компьютерной системы на неприкосновенность и целостность находящейся в ней информации. Необходимо отметить, что эта статья явилась преемницей ст.269 Проекта УК РФ “Создание, использование и распространение вирусных программ”. Смена дефиниций была сделана законодателем осознано, т.к. в случае принятия только вирусов в качестве средства совершения данного преступления произошло бы неправданное смещение в понимании такого средства. Во-первых, компьютерный вирус может быть и безвредным для информации, требующей гарантированной целостности. Во-вторых, существует большое количество типов программ, приводящим к крайне нежелательным последствиям, но они не попадают под традиционное понимание “Компьютерного вируса”.

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".

"**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.

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. [[21]](#footnote-21) 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.

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.

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.[[22]](#footnote-22)

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.[[23]](#footnote-23)

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. субьектом данного преступления может быть любой гражданин, достигший 16 лет.

**Санкция** части 1 предусматривает один основной вид наказания (лишение свободы на срок до 3 лет) и один дополнительный (штраф в размере 200-500 минимальных размеров оплаты труда или зарплаты либо иного дохода лица за период 2-5 мес.).

Частью 2 ст. 273 криминализируется более опасное преступление: те же деяния, повлекшие тяжкие последствия.

При этом "тяжкие последствия" - оценочная категория, которая подлежит квалификации судом. Согласно п.8 постановления Пленума Верховного Суда Российской Федерации от 29 апреля 1996 г. N 1 суд, признавая подсудимого виновным в совершении преступления по признакам, относящимся к оценочным категориям (тяжкие или особо тяжкие последствия, крупный или значительный ущерб, существенный вред, ответственное должностное положение подсудимого и др.), 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.[[24]](#footnote-24)

**Санкция** второй части данной статьи - относительно-определенная: лишение свободы на срок от 3 до 7 лет. Таким образом, именно это преступление из всей главы относится к категории тяжких.

## 4.3 Анализ статьи 274 У КРФ “Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. ”

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.[[25]](#footnote-25)

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. [[26]](#footnote-26)

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.

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.

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 считать допустимым следующее:[[27]](#footnote-27)

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.

**Вина** выражается в форме прямого или косвенного умысла. 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 повлекших уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ при условии, что в результате этих действий был причинен существенный вред. [[28]](#footnote-28)

Как уже отмечалось, между фактом нарушения и наступившим существенным вредом должна быть установлена причинная связь и полностью доказано, что наступившие последствия являются результатом нарушения правил эксплуатации, а не программной ошибкой либо действиями, предусмотренными в ст. 272, 273 УК РФ.

**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.

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 5 лет, обязательные работы от 180 до 240 часов и ограничение свободы до 2 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.

# 5. Международный и отечественный опыт борьбы с компьютерными преступлениями.

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 сделана первая попытка реализации уголовно-правовой политики России в новой для нее области - сфере компьютерных правоотношений. Насколько она окажется успешной, как сможет снять накопившиеся здесь противоречия, защитить права заинтересованных лиц - 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, которыми оснащены более 2270 коммерческих банков.

Например, только по данным ГУЭП МВД России, в 1995-1996 гг. выявлено более 250 преступлений с использованием электронных средств доступа, ущерб от которых составил около 200 млрд. руб.[[29]](#footnote-29)

По данным Федеральной службы реагирования на ЧП в компьютерном пространстве (U.S. Federal Computer Incident Response Capability, FedCIRC), только в прошлом году было зарегистрировано более 2500 случаев, квалифицируемых как ЧП в компьютерной системе или сети, вызванное отказом механизма защиты или умышленной попыткой либо угрозой нарушения этого механизма. Согласно подсчетам отдела ФБР по борьбе с компьютерными преступлениями (Вашингтон, округ Колумбия), хотя бы просто 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. [[30]](#footnote-30) В текущем году расположенный в Сан-Франциско Институт компьютерной безопасности (Computer Security Institute, CSI) совместно с ФБР провел исследование, выявившее некоторые закономерности в области компьютерных преступлений . В основу был положен опрос, направленный на определение “размеров бедствия”, а попутно - на повышение уровня осведомленности о компьютерных преступлениях в рядах их настоящих и потенциальных жертв. Опрос CSI/FBI, охвативший 563 организации, от самых мелких до крупнейших, подтвердил известное предположение, что компьютерные преступления представляют реальную угрозу, усугубляемую тем, что она носит скрытый характер. 60% респондентов смогли оценить свои потери от этих преступлений: суммарная цифра превышает 100 млн долларов. 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. Тем не менее цифры получились любопытные. Три четверти респондентов, понесших финансовые убытки, пострадали от таких преступлений, как мошенничество (26 респондентов, 24 890 тыс. дол.), утечка секретной информации (22 респондента, 21 050 тыс. дол.) и мошенничество с использованием телекоммуникационных систем.

Остальные убытки стали результатом внедрения вирусов, диверсий против данных или сетей, несанкционированного доступа “своих” и “чужаков”, а также новой разновидности кражи - переносных компьютеров.

Долгое время считалось, что причины большинства проблем, связанных с защитой компьютеров, нужно искать внутри фирм. Однако лишь 43% опрошенных сообщили о нападениях “изнутри” (от одного до пяти случаев в каждой фирме), тогда как о таком же количестве покушений извне поведали 47% респондентов. Подобная картина требует кардинальных решений на международном уровне. И первые попытки уже сделаны.[[31]](#footnote-31)

"Мы отстаем от преступников на один шаг, а должны быть на шаг впереди" - так сформулировал главную задачу стран - членов "восьмерки" в борьбе с киберпреступностью министр внутренних дел Великобритании Джек Стро.

Британского коллегу поддержала министр юстиции США Джанет Рино, заявившая: "Мы больше не можем бороться с преступлениями XXI века с помощью инструментов XIX века. Точно так же, как компьютеры помогают преступнику, они могут помочь правоохранительным ведомствам". Стро и Рино выступили на пресс-конференции по итогам состоявшейся в Вашингтоне встречи руководителей правоохранительных органов Великобритании, Германии, Италии, Канады, России, США, Франции и Японии. На этой встрече был принят план совместных действий по борьбе с киберпреступностью, который предусматривает резкую активизацию сотрудничества правоохранительных органов стран "восьмерки". В частности, в соответствии с этим планом будет установлена круглосуточная связь для "своевременного, эффективного реагирования" на транснациональные преступления в сфере высоких технологий. Планом оговариваются также выделение "в достаточном количестве подготовленного и оснащенного специальным оборудованием персонала", "разработка средств быстрого выслеживания идущих по компьютерным сетям атак" с целью оперативного установления компьютерного взломщика. Если высылка преступника в силу его национальной принадлежности невозможна, страны "восьмерки" обязуются применить к нему те же судебные меры и выделить такие же ресурсы, какие бросила бы на это потерпевшая страна. По словам руководителей правоохранительных органов стран "восьмерки", это обязательство имеет крайне важное значение, так как слишком часто преступник покидает страну, в которой совершил преступление, и возвращается к себе на родину, надеясь укрыться от правосудия. Министры договорились также предпринять шаги, которые должны помешать киберпреступникам изменять или уничтожать "электронные улики" преступления в компьютерных сетях. Решено доработать действующие национальные законодательства таким образом, чтобы в них содержалось четкое определение компьютерного преступления. Страны "восьмерки" намерены активнее сотрудничать с компаниями -- изготовителями ЭВМ в разработке новых технических решений, облегчающих задачу предотвращения или обнаружения этого вида преступлений и наказания за них. Предполагается использование таких технологий, как видеосвязь, позволяющая получать показания у свидетелей, где бы те ни находились. По словам министра юстиции США Рино, выступившей в роли хозяйки встречи, эти шаги "знаменуют огромный прогресс в наших усилиях по борьбе со всеми видами преступлений, совершаемых с помощью компьютера".

Участники встречи приняли коммюнике, в котором подчеркивается, что "характер современных коммуникаций не позволяет ни одной стране в одиночку бороться с проблемой преступности в сфере высоких технологии" и требует выработки общего подхода.

Надо отметить, что российские правоохранительные органы (МВД, ФСБ, ФАПСИ, Прокуратура...) в достаточной степени осознали угрозу которую таит в себе информатизация ощества и государства. В меру возможностей, отпущенных скундным финансированием ведомства пытаются делать упреждающие шаги.

Один из самых крупных проектов "компьютеризации" России знаменитые компании SIEMENS NIXDORE и ORACLE осуществляют совместно с Министерством внутренних дел. Когда работа будет закончена, отечественные сыщики будут обладать одной из самых современных и самых мощных информационных сетей в мире.

Создавать компьютерную сеть МВД у нас начали еще в 1991году, понимая, что с бумажными картотеками много преступников не наловишь.

Контракт подписали с немецкой фирмой Siemens Nixdorf, известной своей основательностью и качеством. Программное обеспечение для управления базами данных, в которых МВД хранит миллионы записей, приобретено у не менее знаменитой американской фирмы Oracle. Правда, до прикладной базы, которая бы помогала разбираться в массивах милицейской информации, иностранцев допустили только на расстояние "вытянутой руки": основные программы разработаны в Новосибирске специальным Центром разработки МВД. Создание милицейской компьютерной сети, которая в конце концов должна раскинуться от Калининграда до Южно-Сахалинска, - сегодня один из немногих глобальных российских информационных проектов, который выполняется четко и в положенные сроки.

Остается пожелать, чтобы подобная сеть сама не стала объектом посягательств преступников.

В завершение хочется заметить, что страховые компании всерьез предлагают страховать риски безопасности информации[[32]](#footnote-32).

Так страховая компания "Интеррос-Согласие" приступила к страхованию банковских рисков.

"Интеррос-Согласие" будет страховать банки от хищения или потери денежных и других ценностей при перевозке, от финансовых потерь в результате мошенничества персонала банка, подделок и подлогов ценных бумаг, **электронных и компьютерных преступлений**.

Эти риски "Интеррос-Согласие" намерена перестраховывать на лондонском страховом рынке, российские компании привлекаться к перестрахованию не будут.

В основе нового страхового продукта лежат используемые в мировой практике условия страхования банковских рисков Bankers Blanket Bond (B.B.B.).

При подготовке этого продукта специалисты "Интеррос-Согласия" провели ряд консультаций с британской страховой брокерской фирмы Johnson&Higgins, которая является одним из лидеров в мировом банковском страховании.

# 6. Заключение.

Определенные факты позволяют прогнозировать большую вероятность того, что вскоре криминалистам прийдется столкнуться на практике не только с чисто компьютерными преступлениями, а и с идеальной совокупностью преступлений в случаях, когда действия по противозаконному использованию компьютерной конфиденциальной информации с использованием специального инструмента - компьютера будут направлены против собственности, экономической деятельности и иных объектов.

Эти случаях необходимо будет применять не только известные традиционные методики раскрытия и расследования, но и новые способы работы с доказательствами, разработанные в рамках расследования информационных преступлений и ее части - методики расследования преступлений в области компьютерной информации. Создание указанной методики является крайне актуальным, поскольку основная проблема следственно-судебного аппарата на современном этапе заключается в уровне специальной подготовки должностных лиц, которым и предстоит проводить в жизнь требования новых законов. Давая криминалистические рекомендации в области информационных правоотношений, следует учитывать неоднородность состава и образовательный уровень нашего следственно-судебного аппарата. Ясно, что еще многие сотрудники органов следствия и дознания не только не используют технические средства и информационные технологии в своей деятельности, но и недостаточно осведомлены о них. Другой важной побудительной причиной создания указанной методики является неявная бланкетность диспозиций уголовного закона, устанавливающего ответственность за "информационные преступления". Анализ этих норм показывает, что без знания законодательства, регулирующего информационные правоотношения, следствие и дознание не смогут правильно квалифицировать выявленные случаи преступлений, а суд не сможет адекватно применить соответствующие нормы уголовного закона.

Представляется также, что подход, согласно которому в законодательстве следует отражать конкретные технические средства, себя исчерпал. Представляется не совсем правильным принятие за основу для именования в криминалистике всей совокупности преступлений в области информационных отношений термином "компьютерные преступления".

Термин "компьютер" является разновидностью коммуникационной техники или информационного оборудования и не исчерпывает всего разнообразия этой техники и отношений, связанных с обращением конфиденциальной документированной информации. В этой связи полезен был бы опыт канадского законодательства, разделившего преступления на компьютерные и телекоммуникационные (телекоммуникационное преступление - мошенническое использование любого телефона, микроволновой, спутниковой или другой системы передачи данных).

Под "информационными преступлениями" мною понимаются общественно опасные деяния, запрещенные уголовным законом под угрозой наказания, совершенные в области информационных правоотношений. Тогда можно будет сделать вывод о том, что содержанием методики расследования информационных преступлений является система наиболее эффективных методов расследования преступлений в области документированной конфиденциальной информации (в том числе компьютерной, телекоммуникационной и иной).

Но все же я хочу подчеркнуть, что введение законодателем в Уголовный кодекс термина "компьютерная информация" является крайне своевременным. Я думаю, что разработка проблемы компьютерной преступности и поиск методов борьбы с нею всего лишь дело времени и опыта. И российские криминологи и криминалисты обязательно внесут в это свой вклад. Если только российские политики не дадут им умереть с голоду…

# 7. Список использованной литературы.

1. **Законодательные акты и комментарии к ним:**
   1. Уголовный кодекс Российской Федерации от 24.05.96. – СП б.: Альфа, 1996;
   2. Наумов А.В. Комментарий к Уголовному кодексу. – М.: Юристъ, 1997;
   3. Скуратов Ю.И., Лебедев В.М. Комментарий к Уголовному кодексу. – М., 1996;
   4. Федеральный закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года №24-ФЗ;
   5. Комментарий к Федеральному Закону «Об информации, информатизации и защите информации». М.: Институт государства и права РАН, 1996.
   6. Закон Российской Федерации "Об авторском и смежных правах" от 9 июля 1993 года №5351-1;
   7. Закон Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" от 23 сентября 1992 года №3523-1;
   8. Закон “О средствах массовой информации” от 27.12.91 г. N 2124-I
   9. Закон “О Федеральных органах правительственной связи и информации” от 19.02.92 N 4524-1

1.10.Закон “О правовой охране топологий интегральных микросхем” от 23.09.92 г. N 3526-I

1.11. Закон “Об участии в международном информационном обмене” от 5.06.1996 г. N 85-ФЗ

1.12. Закон"О связи" от 16 февраля 1995 г. N 15-ФЗ

1.13. Закон "О государственной тайне" от 21 июля 1993 г. N 5485-1

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

**2. Учебники и монографии:**

2.1Крылов В.В. Информационные компьютерные преступления. М.: ИнфраМ-Норма, 1997.

* 1. Здравомыслов Б.В. Уголовное право России. Особенная часть. – М.: Юристъ, 1996;
  2. . Уголовное право. Особенная часть. П/р Казаченко И.Я., Незнамовой З.А., Новоселова Г.П. – М.: Норма – Инфра, 1998;
  3. В.С. Горбатов, О.Ю. Полянская, “Доказывание в судебных делах по компьютерным преступлениям”, Москва, МИФИ, 1997

Карелина М.М. Преступления в сфере компьютерной информации, Москва,1998

* 1. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность. - М., 1991;
  2. Борзенков Г.Н., Комиссаров В.С. Уголовное право Российской Федерации. – М.: Олимп, 1997;
  3. . Ведеев Д.В. Защита данных в компьютерных сетях. - М., 1995;

2.10. Беляев В.С. Безопасность в распределительных системах. – М., 1995;

* 1. Копылов В.А. Информационное право. – М.: Юристъ, 1997;

2.12. Гайкович В.Ю “Основы безопасности информационных технологий”, Москва, “Инфо-М”, 1998

1. **Научные статьи в журналах:**

3.1. “Информационные преступления - новый криминалистический объект “(Крылов В.,"Российская юстиция", 1997 г., N 4)

3.2."Криминалистическая характеристика финансовых преступлений" (Яблоков Н.П., "Вестник Московского университета", Серия 11, Право, 1999, N 1)

3.3. "Как остановить компьютерное пиратство?" (Симкин Л., "Российская юстиция", 1996, N 10)

3.4. "Информация как элемент криминальной деятельности" (Крылов В.В., "Вестник Московского университета", Серия 11, Право, 1998, N 4)

3.5. "Преступления в сфере компьютерной информации" (Гульбин Ю., "Российская юстиция", 1997, N 10)

3.6.Расследование хищений, совершаемых в кредитно-финансовой сфере с использованием электронных средств (В.Г.Баяхчев, В.В. Улейчик, "Законодательство", N 6, июнь 2000 г.)

3.7."Ответственность за неправомерный доступ к компьютерной информации" (Кочои С., Савельев Д., "Российская юстиция", 1999, N 1)

3.8."Компьютеризация и уголовное право" (В.В. Голубев, "Законодательство", 1999 г., N 8)

3.9.”Криминогенные аспекты глобальной сети Интернет” (И.Н. Соловьев, "Налоговый вестник", N 4, апрель 2001 г.)

3.10. Ю.Ляпунов, В.Максимов, “Ответственность за компьютерные преступления”, “Законность” №1, 1997г.

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

* 1. Никифоров И. ''Компьютерные преступления'', ''Защита информации. Конфидент'', № 5, 1995.
  2. Рачук Т.В. ''Уголовные наказания за информационные преступления'', ''Защита информации. Конфидент'' № 4, 1997.
  3. Фоменков Г.В. ''О безопасности в Internet'' ,''Защита информации. Конфидент'', № 6, 1998.

## **В работе использованы также**

**электронные информационные ресурсы:**

www.relcom.ru

http://ftp.infoart.ru

http://old.pcweek.ru

http:/www.rbcnet.ru

www.leningrad.spb.ru

http://www.zaural.ru/procur/my\_page.htm#practica

http://law.bugtraq.ru/

P.S. За основу взята работа неизвестного автора. Отзывы, вопросы, пожелания прошу присылать на

ss\_lex@mail.nnov.ru

1. "Информация как элемент криминальной деятельности" (Крылов В.В., "Вестник Московского университета", Серия 11, Право, 1998, N 4) [↑](#footnote-ref-1)
2. ст.2 Федерального закона “Об информации, информатизации и защите информации” (от 20.02.95 г. N 24-ФЗ), [↑](#footnote-ref-2)
3. Бауэр Ф.Л., Гооз Г. Информатика: Вводный курс. М., 1990. Ч.1. С. 18. [↑](#footnote-ref-3)
4. См.: Заморин А.П., Марков А.С. Толковый словарь по вычислительной технике и программированию. Основные термины: около 3000 терминов. М., 1988. С. 68. [↑](#footnote-ref-4)
5. О понятии информации см.: Правовая информатика и кибернетика: Учебник / Под ред. Н.С. Полевого. М., 1993. С. 24 - 29; Компьютерные технологии в юридической деятельности: Учебное и практическое пособие / Отв. ред. пpоф. H. Полевой, канд. юpид. наук В. Крылов. М., 1994. С.7-10. [↑](#footnote-ref-5)
6. "Информация как элемент криминальной деятельности" (Крылов В.В., "Вестник Московского университета", Серия 11, Право, 1998, N 4) [↑](#footnote-ref-6)
7. Федеральный закон "Об информации, информатизации и защите информации": Комментарий. М., 1996. С. 15. [↑](#footnote-ref-7)
8. Копылов В.А. Информационное право М., 1997. С. 23. [↑](#footnote-ref-8)
9. "Ответственность за неправомерный доступ к компьютерной информации" (Кочои С., Савельев Д., "Российская юстиция", 1999, N 1) [↑](#footnote-ref-9)
10. Карелина М.М. Преступления в сфере компьютерной информации, М. 1998

    http://www.relcom.ru/ComputerLaw/New\_code.htm [↑](#footnote-ref-10)
11. В.Крылов, “Российская юстиция” №4, 1997г. [↑](#footnote-ref-11)
12. Н. Селиванов. Проблемы борьбы с компьютерной преступностью. - Законность, 1993, No. 8, с. 37. [↑](#footnote-ref-12)
13. "Преступления в сфере компьютерной информации" (Гульбин Ю., "Российская юстиция", 1997, N 10) [↑](#footnote-ref-13)
14. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А.В.) [↑](#footnote-ref-14)
15. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А.В.) [↑](#footnote-ref-15)
16. "Ответственность за неправомерный доступ к компьютерной информации" (Кочои С., Савельев Д., "Российская юстиция", 1999, N 1) [↑](#footnote-ref-16)
17. "Преступления в сфере компьютерной информации" (Гульбин Ю., "Российская юстиция", 1997, N 10) [↑](#footnote-ref-17)
18. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации"

    Закон Московской области от 12 марта 1998 г. N 9/98-ОЗ "Об информации и информатизации в Московской области", принят решением Московской областной Думы

    oт 25 февраля 1998 г. N 4/8 [↑](#footnote-ref-18)
19. "Преступления в сфере компьютерной информации" (Гульбин Ю., "Российская юстиция", 1997, N 10) [↑](#footnote-ref-19)
20. "Ответственность за неправомерный доступ к компьютерной информации" (Кочои С., Савельев Д., "Российская юстиция", 1999, N 1) [↑](#footnote-ref-20)
21. "Компьютеризация и уголовное право" (В.В. Голубев, "Законодательство", 1999 г., N 8) [↑](#footnote-ref-21)
22. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А.В.) [↑](#footnote-ref-22)
23. Там же. [↑](#footnote-ref-23)
24. "Преступления в сфере компьютерной информации" (Гульбин Ю., "Российская юстиция", 1997, N 10) [↑](#footnote-ref-24)
25. "Компьютеризация и уголовное право" (В.В. Голубев, "Законодательство", 1999 г., N 8) [↑](#footnote-ref-25)
26. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" [↑](#footnote-ref-26)
27. Карелина М.М. Преступления в сфере компьютерной информации,М 1998 [↑](#footnote-ref-27)
28. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А.В.) [↑](#footnote-ref-28)
29. И.Викторов, М.Миронов. "ЗАКОННОСТЬ В КРЕДИТНО-БАНКОВСКОЙ СФЕРЕ", Законность №11, 1997г. [↑](#footnote-ref-29)
30. D.J.Iocoveю. Как бороться со взломщиками компьютеров, Сети и Телекоммуникации №5, 1998г.

    http://ftp.infoart.ru/it/press/cwm/30\_97/colla.htm [↑](#footnote-ref-30)
31. Министры "восьмерки" приняли план борьбы с киберпреступностью, ИТАР-ТАСС

    Компьютерная неделя N5 (129) от 10.2.1998 Москва

    http://old.pcweek.ru/98\_05/iso/ns20.htm [↑](#footnote-ref-31)
32. RBCNET, компания “Интеррос-Согласие”, 04.09.97

    http:/www.rbcnet.ru/ecopress/040997/1009/insure\_68\_2 [↑](#footnote-ref-32)