**О Г Л А В Л Е Н И Е**

ВВЕДЕНИЕ

ГЛАВА 1. РАЗВИТИЕ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ СВЯЗАННЫМ С КОМПЬЮТЕРНОЙ ИНФОРМАЦИЕЙ

1.1 Развитие и становление отечественного и зарубежного уголовного законодательства в сфере компьютерной информации

1.2 Предмет преступлений в сфере компьютерной информации

ГЛАВА 2. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1 Неправомерный доступ к компьютерной информации

2.2 Создание, использование и распространение вредоносных программ для ЭВМ

2.3 Нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети

ГЛАВА 3. ОСОБЕННОСТИ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ СОВЕРШАЕМЫХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

3.1 Квалификация преступлений в сфере компьютерной информации, совершенных группой лиц по предварительному сговору и организованной группой

3.2 Совершенствование мер уголовного - правовой борьбы с преступлениями в сфере компьютерной информации

ЗАКЛЮЧЕНИЕ

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Приложение 1

Приложение 2

# ВВЕДЕНИЕ

**Актуальность темы исследования.** В России 20 лет осуществляются радикальные социально-экономические реформы, идет процесс демократизации всех сторон общественной жизни. Такой процесс невозможен без становления нового социального порядка, укрепления законности, обеспечения надежной охраны конституционных прав и свобод граждан. Развитие высоких технологий позволяет каждой второй семье приобрести персональный компьютер, сотовый телефон, модем и другие средства связи, что в свою очередь приводит к появлению новых форм и видов злоупотреблений техническими средствами, в том числе преступных посягательств.

Это проявляется в том, что преступные группы и сообщества начинают активно использовать в своей противоправной деятельности новейшие информационные технологии и компьютерную технику, достижения науки и техники, в том числе основанные на кибернетике. Компьютеризация, развитие информационных технологий, привели к возникновению, закреплению и криминализации в современной России нового вида преступных посягательств, ранее не известных отечественной науке и практике и связанных с использованием средств компьютерной техники, - так называемых компьютерных преступлений. Так, потери компаний от неправомерных действий с компьютерной информацией только в 2005 г. в России составили около 450 млн. дол.[[1]](#footnote-1).

Однако, несмотря на новизну данного вида преступлений для отечественного уголовного законодательства, в государствах с высоким уровнем технологического развития проблема борьбы с компьютерной преступностью давно признана одной из первостепенных задач, важность которой неуклонно возрастает. Таким образом, возникла необходимость комплексного исследования криминализированных составов компьютерных преступлений, их состояние и тенденций развития.

**Степень научной разработанности проблемы.** Проблемами использования возможностей компьютерной техники при расследовании и судебном разбирательстве занимались такие ученые, как Ю.М Батурин, В.Д. Зеленский, А.В, Славнова, В.Н. Черкассов, В.Ф. Щепельков и др. Различным аспектам компьютерной преступности в последние годы было уделено определенное внимание в научной и специальной литературе; они нашли отражение в работах Ю.М. Батурина, В.А. Бессонова, В.Б. Вехова, П.Б. Гудкова, В.В. Крылова, В.Д. Курушина, В.Д. Ларичева, Ю. Ляпунова, В.Ю. Максимова, H.С. Полевого, Л.А. Прохорова, Т.Г. Смирновой, Е.А. Суханова, С.И. Ушакова, А.А. Харкевич, Л.И. Шершнева, Н.И. Шумилова и других ученых.

Однако, несмотря на теоретическую и практическую значимость указанных исследований, в них не рассмотрены многие проблемы эффективности уголовного закона в сфере борьбы с компьютерными преступлениями. Эффективность действия уголовного закона зависит от того, насколько быстро и полно будут раскрыты и квалифицированы эти преступления, обеспечено при этом обоснованное привлечение виновных к уголовной ответственности или освобождение от таковой с учетом требований целесообразности (в предусмотренных законом формах).

**Цель и задачи исследования.** Цель работы - комплексное изучение уголовно-правовых аспектов преступлений, в сфере компьютерной информации теоретических исследований, внесение предложений по совершенствованию законодательства, предусматривающего уголовную ответственность за преступления в сфере компьютерной информации; выявление возможных путей повышения эффективности применения практическими работниками системы уголовно-правовых.

Цель опосредует более конкретизированные задачи исследования:

* изучение исторического опыта зарубежных стран по правовому регулированию преступлений в сфере компьютерной информации;
* формулирование понятия преступлений в сфере компьютерной информации;
* анализ норм права, устанавливающих уголовную ответственность за преступления в сфере компьютерной информации, выявление особенностей квалификации преступлений в сфере компьютерной информации;

**Объект и предмет исследования.** Объектом диссертационного исследования являются общественные отношения, подвергающиеся посягательствам в результате совершения преступлений в сфере компьютерной информации.

Предмет исследования включает в себя:

* историю отечественного и зарубежного законодательства, освящающую проблемы борьбы с информационными преступлениями;
* компьютерную преступность как новый объект уголовно-правового регулирования, ее состояние, структуру и динамику;
* нормы права, предусматривающие ответственность за данные преступления в сфере уголовной юрисдикции;

**Методология и методика исследования.** Методологической основой исследования послужили общенаучные методы познания, а также частно-научные методы: историко-правовой - применительно к изучению исторического опыта реализации уголовной ответственности за совершение преступлений в сфере компьютерной информации за рубежом, сравнительно-правовой, включающий анализ позитивного опыта зарубежного уголовного законодательства в области компьютерных преступлений, формально-логический, заключающийся в детальном анализе указанных в законе уголовно-правовых и организационно-технических мер противостояния компьютерной преступности,

**Теоретическая и практическая значимость исследования** состоит в том, что оно вносит определенный вклад в развитие теории уголовного права, поскольку восполняет пробел относительно комплексного подхода к уголовно-правовым проблемам борьбы с преступностью в сфере компьютерной информации в современных условиях. Практическая значимость определяется предложениями по совершенствованию действующего законодательства по преступлениям в сфере компьютерной информации.

**Структура работы** определяется целями и задачами исследования и включает в себя введение, три главы, шесть параграфов, заключение, литературу и приложения.

# ГЛАВА 1. РАЗВИТИЕ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ СВЯЗАННЫМ С КОМПЬЮТЕРНОЙ ИНФОРМАЦИЕЙ

# 1.1 Развитие и становление отечественного и зарубежного уголовного законодательства в сфере компьютерной информации

Основоположником теории информации был американский ученый К.Э. Шеннон, который в 1948 году впервые определил само понятие "информация" и дал вероятностно-статистическое определение понятию "количество информации"[[2]](#footnote-2), связывая это явление с кибернетикой[[3]](#footnote-3).

Кибернетика занимается общими законами преобразования информации в сложных управляющих системах. Она рассматривает информацию не как общественный феномен, т.е. информацию, производимую и потребляемую обществом, а в более узком техническом аспекте, как информацию, циркулирующую по электронным каналам связи. Кибернетика доказала, что информация имеет непосредственное отношение к процессам управления и развития, обеспечивающим функционирование любых систем[[4]](#footnote-4).

Качественное измерение информации предполагает понимание смысла, необходимости информации для определенных потребителей. Для человека содержание информации важнее, чем ее объем. Значимость информации определяется через изменение вероятности достижения некоторой цели после получения информации[[5]](#footnote-5).

Информационные отношения долгое время не признавались самостоятельным объектом правового регулирования, однако в настоящее время роль информации настолько возросла, что информационные отношения признаны специфическим предметом правового регулирования.

Социальная информация это сложное многоаспектное явление, что обуславливает сложности в правовом регулировании информационных отношений. С этой целью создается новое "информационное" законодательство и система мер уголовно-правовой защиты данной группы отношений.

Наблюдается большое разнообразие мнений ученых-юристов в оцределениях таких понятий как "информационная безопасность" и "информационные преступления"[[6]](#footnote-6).

С учетом многообразия информационных угроз Л.И. Шершнев под информационной безопасностью понимает "способность государства, общества, социальной группы, личности обеспечить с определенной вероятностью достаточные и защищенные информационные ресурсы и информационные потоки для поддержания своей жизнедеятельности и жизнеспособности устойчивого функционирования и развития; противостоять информационным опасностям и угрозам, негативным информационным воздействием на индивидуальное и общественное сознание и психику людей, а также на компьютерные сети и другие технические системы информации; вырабатывать личностные и групповые навыки и умения безопасного поведения; поддерживать постоянную готовность к адекватным мерам в информационном противоборстве, кем бы оно не было навязано"[[7]](#footnote-7).

Шумилов Н.И. под информационной безопасностью понимает состояние защищенности информационной сферы государства, общества, личности, обеспечиваемое комплексом мер по снижению, предотвращению или исключению негативных последствий от воздействия на элементы информационной сферы[[8]](#footnote-8). Думается, что, понятие информационней безопасности, данное Л.И. Шершневым, более емкое, не требующее дальнейшего толкования такого понятия как информационная сфера, чем у Н. И. Шумилова.

Крылов В.В. информационными преступлениями считает общественно опасные деяния, совершенные в области информационных правоотношений и запрещенные уголовным законом под угрозой наказания[[9]](#footnote-9).

По нашему мнению, можно согласиться с Н.И. Шумиловым о наличии группы однородных преступлений, одним их признаков состава которых является информация. Преступления рассматриваемого вида есть преступления в сфере информационной безопасности, или информационные преступления[[10]](#footnote-10).

Общеюридическая терминология в сфере информационных отношений вообще, и в отношении компьютерной информации в частности, до сих пор не установлена. В настоящее время в Уголовном кодексе России криминализированы далеко не все правонарушения в информационной сфере, или как их называют, в области высоких технологий[[11]](#footnote-11), а лишь компьютерные правонарушения[[12]](#footnote-12).

Понятие "компьютерные преступления" до сих пор в литературе трактуется по-разному. Существует мнение, что "с точки зрения уголовно-пра1вовой охраны под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства". В данном случае "в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть"[[13]](#footnote-13).

Т.Г. Смирнова под преступлениями в сфере компьютерной информации подразумевает "запрещенные уголовным законом общественно-опасные виновные деяния, которые, будучи направлены на нарушение неприкосновенности охраняемой законом компьютерной информации и ее материальных носителей (в частности, компьютерной техники (ЭВМ), систем ЭВМ или их сетей), причиняют либо создают угрозу причинения вреда жизни и здоровью личности, правам и свободам человека и гражданина, государственной и общественной безопасности"[[14]](#footnote-14).

Третья точка зрения, которую придерживается И.А. Клепицкий такова, что преступлением в сфере компьютерной информации (компьютерным преступлением) является "предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности и конституционному строю)"[[15]](#footnote-15).

На наш взгляд, каждая точка зрения имеет право на существование в определенное время: в период осознания необходимости криминализировать компьютерные преступления, первые два-три года введения в Уголовный кодекс РФ составов компьютерных преступлений. В настоящее время заканчивается пятый год криминализации преступлений в сфере компьютерной информации, накоплен определенный опыт выявления составов компьютерных преступлений, привлечения к уголовной ответственности, их квалификации и расследования. Поэтому все больше встает необходимость в представлении компьютерных преступлений как подкласса преступлений, совершаемых посредством возможностей высоких технологий. По мнению А.И. Гурова, к преступлениям в области высоких технологий относятся:

нарушение тайны переписки, телефонных переговоров, телеграфных и иных сообщений с использованием специальных технических средств, предназначенных для негласного получения информации, и также незаконный сбыт или приобретение в целях сбыта таких средств;

незаконный экспорт технологий научно-технической информации и услуг, используемых при создании вооруженной техники, оружия массового уничтожения;

неправомерный доступ к компьютерной информации (ст. 272УК);

создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК);

нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК)[[16]](#footnote-16).

Изложенное дает основание определить преступления в сфере компьютерной информации (компьютерные преступления) следующим образом - это предусмотренное уголовным законом, противоправное, виновное нарушение чужих прав и интересов, связанное с использованием, модификацией, уничтожением компьютерной информации, причинившее вред либо создавшее угрозу причинения вреда подлежащим уголовно-правовой охране правам и интересам физических и юридических лиц, общества и государства (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности в области высоких технологий и конституционному строю)[[17]](#footnote-17).

История развития зарубежного законодательства показывает, что первый шаг в направлении защиты компьютерной информации был сделан зарубежным законодательством Швеции 4 апреля 1973 года, когда был принят "Закон о данных", который ввёл новое понятие в традиционное законодательство - "злоупотребление при помощи компьютера"[[18]](#footnote-18),

В США впервые правовая защита компьютерной информации получила отражение в принятом законодательными собраниями американских штатов Аризона и Флорида в 1978 году законе "Computer crime act of 1978", устанавливающем уголовную ответственность за компьютерные преступления. Согласно этому закону противоправные действия, связанные с модификацией, уничтожением, несанкционированным доступом или изъятием компьютерных данных, программ или сопутствующей документации, признавались преступлением и наказывались пятью годами лишения свободы либо штрафом в размере 5000 долларов или тем и другим одновременно в зависимости от тяжести причиненного жертве ущерба.

Те же действия, совершенные с целью хищения какой-либо собственности, наказывались 15 годами лишения свободы либо денежным штрафом в размере 10 000 долларов или и тем и другим одновременно.

В дальнейшем, во всех штатах США были приняты аналогичные специальные законы и нормативно-правовые акты, но правовые меры защиты компьютерной информации в США на этом не закончились. Суровые наказания в отношении лиц, совершивших несанкционированный доступ к компьютерным данным, содержащимся в федеральных компьютерных сетях, установлены в США федеральным "Законом о компьютерном мошенничестве" 1984 года в отношении неправомерного доступа к федеральным компьютерным сетям. Уголовная ответственность наступает для лиц, которые путем неправомерного проникновения к компьютерной информации:

1) получают определенную секретную информацию правительства США с намерением или пониманием того, что эта информация будет использована во вред Соединенным Штатам или на пользу иностранной державе,

2) получают информацию финансового учреждения или информации о клиентах,

3) сознательно используют, изменяют или уничтожают информацию в определенных компьютерах.

В § 33-02 УК штата Техас установлено, что лицо совершает преступление независимо от цели, если оно "использует компьютер без согласия владельца или уполномоченного регламентировать доступ к этому компьютеру лица; причем лицо, совершающее такие действия, знает, что существует компьютерная система защиты, которая предназначена, чтобы предотвратить использование им компьютера; или получает доступ к данным, хранящимся в компьютере или обрабатываемых компьютером без согласия владельца данных или обладателя лицензии на эти данные".[[19]](#footnote-19) Из содержания приведенной нормы следует, что необходимым и достаточным условием уголовного преследования является обязательность наличия минимальной информационной защиты. Уголовное законодательство Техаса, помимо указанной выше более общей нормы с формальным составом, содержит и специальные нормы, которые устанавливают ответственность за создание препятствий для оказания услуг отдельным пользователям, т.е. за нарушение нормальной работы компьютерных служб.

Более тяжкое наказание установлено за "доступ с причинением вреда" -преступления с материальным составом. Так, уголовному преследованию подвергается лицо, которое "без согласия владельца или уполномоченного лица" преднамеренно или осознанно "прерывает работу компьютера или влияет на нормальное функционирование компьютера" либо без согласия указанных выше лиц "изменяет, повреждает или уничтожает эти данные или компьютерные программы"[[20]](#footnote-20).

В разных штатах США и на федеральном уровне в период с 1984 по 1986 год было принято не меньше пяти законов, предусматривающих уголовную ответственность за компьютерные правонарушения. Среди них был закон, направленный на компьютерное мошенничество и злоупотребление, мошенничество с помощью кредитных карточек, доступ к закрытым данным и др. В 1983 году Организация экономического сотрудничества и развития Европы (ОЭСР) начала изучение проблемы компьютерной преступности. В 1986 году по ее инициативе был опубликован доклад "Преступления, связанные с применением компьютеров: анализ политики в области права", цель которого заключалась в создании эталонной схемы закона об уголовной ответственности за компьютерные преступления в целях установления правового единообразия по этому вопросу в различных странах. За основу было принято следующее определение компьютерного преступления: "Компьютерным преступлением считается всякое незаконное, неэтичное и несанкционированное поведение, касающееся автоматизированных процессоров и трансмиссии данных"[[21]](#footnote-21).

До 1995 года в таких зарубежных странах как Канада, ФРГ, Япония. Великобритания, Финляндия, Австралия, Норвегия, Дания, Португалия были приняты законы, устанавливающие правовую ответственность в сфере компьютерной информации. В этих законах выделяют три объекта уголовно-правовой охраны в случае компьютерных посягательств: услуги, имущество и информация[[22]](#footnote-22).

В ФРГ в 1994 году был; принят Федеральный закон "О защите информации". В §§43-44 этого закона предусмотрено наказание за " еправомерное получение данных для себя или другого лица, если они были педиально защищены от неправомерного доступа" в виде лишения свободы на срок от 1 до 2 лет или денежного штрафа до 50 тысяч марок. Этим же законом установлена ответственность для пользователей, не соблюдающих правила защиты информации[[23]](#footnote-23).

Проанализировав международный опыт в борьбе с компьютерными преступлениями, эксперты ООН разработали рекомендации о целесообразности установления различной уголовной ответственности за простой и квалифицированный виды неправомерного доступа к компьютерной информации, причем с использованием единой нормы. Рекомендации были разработаны и на другие компьютерные преступления, совершенные с корыстной целью.

Основой создания "информационного" законодательства России являются положения Конституции РФ, в которых закреплено право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29 Конституции РФ). Одновременно в Конституции РФ содержится комплекс статей, направленных на защиту права граждан, организаций и государства на тайну (ст. ст. 23, 24, 56). Поэтому законодателю в каждом конкретном случае приходится искать баланс между обеспечением тайны и обеспечением права на информацию.

Первым шагом Российского законодательства по правовой защите определенной части компьютерной информации стало издание законов от 23 сентября 1992 г. № 3523-1: "О правовой охране программ для электронно-вычислительных машин и баз данных"[[24]](#footnote-24) и от 1 января 1994 г. "О правовой охране топологий интегральных микросхем"[[25]](#footnote-25), регламентирующих порядок установления и правовую защиту авторских прав на программные средства компьютерной техники и топологии интегральных микросхем. В США аналогичный закон был принят в 1984 году, а в Нидерландах - в 1987 году.

9 июля 1993 г. был принят Закон РФ № 5351-1" Об авторском праве и смежных правах"[[26]](#footnote-26). Этот закон регулирует отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства (авторское право), фонограмм, исполнении, постановок, передач организаций эфирного или кабельного вещания (смежные права). В дальнейшем, 21 июля 1993 г. был принят Закон РФ № 5485-1 "О государственной тайне"[[27]](#footnote-27), который регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности РФ.

20 февраля 1995 года был принят закон "Об информации, информатизации и защите информации". Этот нормативный акты регулируют правовые отношения в сфере информационного обмена и обработки информации с использованием средств новых информационных технологий. Они дают юридическое определение основных компонентов информационной технологии как объектов правовой охраны, определяют категории доступа определенных субъектов к конкретным видам информации, устанавливают и определяют права и обязанности собственника на объекты правовой охраны. Также эти законы дают определение и границы правового применения термина "конфиденциальная информация" и возлагают обязанности на конкретных субъектов по ее защите от различных факторов[[28]](#footnote-28). Аналогичные законы действуют в развитых зарубежных странах уже более 20 лет.

В ст. 128 Гражданского кодекса РФ, принятого 25 октября 1994 года, информация определена как особый объект гражданских прав, наряду с вещами, иным имуществом и интеллектуальной собственностью[[29]](#footnote-29). В статье 2 Федерального Закона РФ от 20 февраля 1995 года № 24-ФЗ "Об информации, информатизации и защите информации" под информацией понимают "сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления". А в ст. ст. 4, 5 того же Закона установлено, что объектами отношений физических, юридических лиц, государства являются только информационные ресурсы. Информация может быть включена в категорию информационных ресурсов лишь при условии ее документирования. В ст. 6 Закона, об информации сказано, что информационные ресурсы являются объектами вещного права и включаются в состав имущества тех органов государственной власти, организаций, физических и юридических лиц, которыми он создается[[30]](#footnote-30). Налицо противоречие между провозглашенным правом собственности на информацию и одновременно, принципом общедоступности и открытости информации. Кроме того, отсутствие согласованности в понимании термина "имущество" в уголовном и гражданском праве создает немало дополнительных трудностей для правоприменителя, особенно в условиях появления все новых форм посягательств на собственность[[31]](#footnote-31).

В законах зарубежных стран отсутствует специальная ответственность за нарушение правил эксплуатации ЭВМ и распространение компьютерных вирусов. Автор согласна с мнением Смирновой Т.Г. о том, что подобные действия рассматриваются как разновидность диверсий, наносящих значительный ущерб компьютерной информации посредством разрушительных воздействий в отношении материальных носителей и зафиксированных на них данных[[32]](#footnote-32).

Способы совершения диверсий могут быть как самыми примитивными, например, физическое разрушение частей компьютерных систем и сетей, так и более сложными, как воздействие непосредственно на программное обеспечение, а также комбинированными, использующими физическое разрушение необходимых элементов информационных систем и программ "вирусов". Например, о первом случае заражения китайских ЭВМ программными вирусами сообщалось в апреле 1989 года, когда компьютеры алюминиевого завода Синань оказались поражены вирусом неустановленного преступника, получившим название, "хлорелла" (либо "пятна"). К концу 1989 года была проведена профилактика 12 750 ЭВМ, в результате пятая часть компьютеров оказалась зараженной этим вирусом[[33]](#footnote-33). Не только за рубежом опасна вирусная эпидемия, отечественные преступники не отстают от зарубежных "собратьев". Так, ГУВД Свердловской области в отношении гражданина Флягина было возбуждено уголовное дело по факту использования им "домашнего персонального компьютера, модема и телефона, зарегистрированного Екатеринбургским ГТС, а также специализированной компьютерной программы, обеспечивающей работу компьютера с удаленными пользователями через телефонную сеть, с целью распространения вирусных программ для ЭВМ. Они заведомо приводили к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. Сами же вирусы Флягин переписывал с помощью сети Internet с одного из серверов в Бразилии"[[34]](#footnote-34).

В Канаде был принят "Закон о поправках к Уголовному кодексу" 1985 года, который установил ответственность за "причинение вреда данным" лицом, которое "а) уничтожает или изменяет данные, б) лишает данные значения, делает их бесполезными, в) препятствует их законному использованию или лишает собственника доступа к ним"[[35]](#footnote-35).

В ФРГ во "Втором законе о борьбе с экономической преступностью" 1986 года расширено понятие "повреждения и уничтожения собственности". В УК ФРГ введена статья, установившая ответственность за простое и квалифицированное уничтожение данных в ЭВМ. В части 1 ст. 303 УК предусматривается наказание за уничтожение любых данных, а часть 2 содержит квалифицированный состав относительно повреждения и уничтожения данных, имеющих серьезное значение для предприятия или административного учреждения[[36]](#footnote-36).

В США получил большое распространение новый вид компьютерного мошенничества - подделка и использование в мошеннических целях кредитных карточек. В обращении в США находятся миллионы кредитных карточек, поэтому ущерб от таких преступлений. По оценки председателя Банковской комиссии Палаты представителей конгресса, составляет ежегодно свыше 1 млрд. долларов[[37]](#footnote-37).

Между тем Российские законодательные органы, правительство практически ограничились введением в Уголовный кодекс 1996 года 28 главы, формально регулирующей преступления в сфере компьютерной информации. В статье 273 этой главы введена уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ, систем ЭВМ или их сети. Квалифицированный состав охватывает неосторожное причинение тяжких последствий, за которые предусмотрено самое тяжкое из всех компьютерных преступлений наказание, от трех до семи лет лишения свободы. Однако, остается неясным, как квалифицировать действия компьютерного злоумышленника, направленные на умышленное причинение тяжких последствий.

Такие пробелы законодательства способствуют безнаказанному созданию и распространению программ-вирусов. Отсутствие центров по отслеживанию неправомерного доступа по международным компьютерным сетям в еще большей степени способствует совершению указанных преступлений. Ведь с расширением сети Internet и других международных компьютерных сетей число пользователей растет как показательная функция, и в равной степени растет опасность компьютерных преступлений, следовательно, необходимо совершенствовать и меры безопасности[[38]](#footnote-38).

Таким образом, анализ отечественного и зарубежного законодательства в области компьютерной информации приводит к выводу о необходимости детального изучения составов преступлений в сфере компьютерной информации, для повышения эффективности уголовно-правовой борьбы с ними.

# 1.2 Предмет преступлений в сфере компьютерной информации

Рассматривая предмет компьютерных преступлений, необходимо отметить, что при его определении возникают определенные сложности.

В определении предмета компьютерных преступлений (по объему) можно выделить два направления. Одни авторы считают, что предмет компьютерных преступлений - это машинная информация, компьютер, компьютерная система или компьютерная сеть[[39]](#footnote-39), другие - только компьютерная информация[[40]](#footnote-40).

Суждение Ю.И. Ляпунова о том, что преступления, имеющие своим предметом лишь аппаратно-технические средства вычислительных машин (хищение, повреждение, уничтожение), подпадают под совершенно другой тип уголовных правонарушений, закрепленных в главе 21 являются вполне оправданным. В принципе, можно предположить случаи, когда вредоносное воздействие на ЭВМ осуществляется путем непосредственного влияния на нее информационных команд. Это возможно, если преступнику удается ввести движущиеся части машины (диски, принтер) в резонансную частоту, увеличить яркость дисплея или его части для прожигания люминофора, зациклить работу компьютера таким образом, чтобы при работе минимума его участков произошел их разогрев и вывод из строя. Однако, мы не разделяем позиции Ю.И. Ляпунова по поводу того, что в этих случаях квалификация содеянного должна проводиться по совокупности статей глав о преступлениях против собственности и компьютерной безопасности[[41]](#footnote-41).

В данных случаях компьютерная информация выступает как орудие совершения преступления и квалификация должна проводиться по статьям, находящимся в главе 21 УК РФ. И только если умысел будет направлен на уничтожение вместе с ЭВМ и информации, которая находится в ее памяти, квалифицировать следует по совокупности статей, расположенных в главах 21 и 28 УК РФ, поскольку в этом случае страдают два объекта уголовно-правовой охраны.

Основное разграничение между предметом, орудием и средством совершения преступления должно проводиться по характеру использования вещей и других материальных (и не только материальных) предметов в процессе совершения преступления. Если это использование имеет активный характер, то есть предмет используется в качестве инструмента воздействия на объект, то перед нами орудие или средство совершения преступления. Напротив, если вещь играет пассивную роль, если над ней осуществляется действие, она так или иначе "претерпевает" воздействие (уничтожается, изымается, изменяется и т.д.), то эта вещь должна быть признана предметом преступления[[42]](#footnote-42).

Если данное суждение спроецировать на компьютерные преступления то становится очевидным, что одна компьютерная информация играет пассивную роль (та информация, на которую осуществляется неправомерное воздействие) и является предметом преступления, а другая играет активную роль (информация, с помощью которой осуществляется неправомерное воз-действие на "пассивную информацию") и по праву может считаться орудием совершения преступления[[43]](#footnote-43).

По нашему мнению, основной особенностью компьютерных преступлений, способной ввести в заблуждение, является то, что на какой бы объект либо предмет не воздействовала компьютерная информация, ее воздействие в первую очередь осуществляется также на компьютерную информацию ("активная информация" воздействует на "пассивную информацию"). Если взять любое компьютерное преступление, т.е. преступление, предметом которого является компьютерная информация, то нет иных способов воздействовать на тазовую, кроме как информацией, носящей ту же природу, т.е. компьютерной информацией. Исключением здесь могут быть случаи физического или механического воздействия на компьютерную информацию (магнит, молоток и т.п.).

При воздействии на компьютерную информацию магнитом необходимо выяснить, какие данные содержала информация, и в зависимости от этого квалифицировать деяние. Если на носителе, который был подвергнут воздействию магнитом, находилась информация, имеющая стоимостное выражение (например, программное обеспечение), и лицо, имеющее доступ к ЭВМ, Умышленно воздействовало на эту информацию, то деяние следует квалифицировать по ст. 274 и 167 УК РФ. Если лицо не имело доступа к ЭВМ, системе сети, квалификация осуществляется по ст. 167 УК РФ и дополнительной квалификации по статьям гл. 28 УК не требуется. Ситуация с молотком или иным подобным предметом решается аналогичным образом. Если в качестве орудия преступления выступает не компьютерная информация, а что-либо другое, то здесь не будет компьютерного преступления. Исключение может составлять только ст. 274 УК.

Выяснение орудия совершения преступления необходимо для того, что бы отграничить компьютерные преступления от внешне схожих противоправных деяний, например, таких, как уничтожение имущества.

Таким образом, в компьютерных преступлениях машинная информация выступает не только в качестве предмета, но и в качестве орудия совершения преступления[[44]](#footnote-44).

При незаконной охоте с применением автомобиля (ст. 258 УК) автомобиль выступает как средство совершения преступления. При совершении неправомерного доступа к компьютерной информации в качестве средства совершения преступления будет выступать компьютер либо несколько компьютеров, с которых осуществлялся неправомерный доступ (см. рис. 3).

Большинство авторов, занимающихся уголовно-правовыми проблемами компьютерной преступности, склонны считать, что компьютерная информация в этих преступлениях может выступать только в качестве предмета[[45]](#footnote-45).

Чаще всего неправомерный доступ к компьютерным сетям каких-либо банков, организаций, учреждений, имеющих достаточно хорошую защиту, осуществляется с нескольких компьютеров одновременно. Это приводит к тому, что только несколько «атакующих»компьютеров отсекаются системой защиты, а остальные получают требуемый доступ[[46]](#footnote-46).

Очевидно, что говорить о компьютере, содержащем информацию, неправомерный доступ к которой осуществляется непосредственно с этого компьютера, как о средстве преступления не следует. Использование компьютера в данной ситуации является необходимым условием для осуществления неправомерного доступа к компьютерной информации.

Информацией считаются разнообразные сведения, факты, данные о явлениях и процессах, происходящих в природе и обществе, в технических кодах.

Если говорить о предмете компьютерных преступлений вообще, то таковым является компьютерная информация, под которой понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах на машинном носителе, в ЭВМ, системе ЭВМ или их сети[[47]](#footnote-47). Конкретизируя предметы преступлении, ответственность за которые предусмотрена статьями 272, 273 и 274 УК РФ, следует отметить, что предметы здесь несколько отличаются.

Так, предметом неправомерного доступа к компьютерной информации и нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети является охраняемая законом информация. Предметом преступления, предусматривающим ответственность за создания, использования и распространения вредоносных программ следует считать вредоносную программу.

В Законе "О правовой охране программ для ЭВМ и баз данных" дается определение программы для ЭВМ. Так, в законе указано, что программа для ЭВМ - это объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определенного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

Из смысла данного определения вытекает, что черновики, выполненные на каком либо носителе (например, на бумаге) и содержащие блок-схему алгоритма программы также могут быть признаны программой для ЭВМ. Это нам представляется весьма спорным. Программой можно считать лишь реализованный алгоритм в виде совокупности данных и команд, то есть текст программы, который остается лишь компилировать[[48]](#footnote-48). Нам представляется, что вредоносной программой, за создание, использование и распространение которой предусмотрена уголовная ответственность (ст. 273 УК), следует считать уже компилированный текст этой программы, т.е. программа должна находиться в электронном виде и быть способной осуществлять вредоносные, действия ее компилирования следует квалифицировать как покушение на создание вредоносной программы.

Возвращаясь к преступлениям, предусмотренным ст. 272 и 274 УК РФ, еще раз отметим, что их предметом является охраняемая законом компьютерная информация.

Уголовным законодательством России охраняются такие виды информации, как:

1) сведения, отнесенные к государственной тайне (ст. 275, 276, 283 УК РФ) Законом РФ "О государственной тайне" 1993 года.

2) информация, непосредственно затрагивающая права и свободы гражданина (тайна частной или семейной жизни (ст.137 УК РФ)), а также персональные данные (под которыми в соответствии с ч. 6 ст. 2 Федерального закона "Об информации, информатизации и защите информации" понимается информация о гражданах, то есть сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его принадлежащих распространению в средствах массовой информации в установленных федеральными законами случаях). Основными элементами информации о гражданах являются имя и фамилия, пол, дата рождения и место рождения, место проживания, образование и семейное положение. К другим элементам персональной информации относятся: сведения о социальном положении, принадлежности к политическим партиям, физическом и психическом здоровье, финансовом положении, владении собственностью, о судимости и т.д.

Согласно Федеральному закону от 15 ноября 1997 г. № 143-ФЗ сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния, являются персональными данными.

Персональные данные относятся к категории конфиденциальной информации, т.е. информации, доступ к которой ограничен в соответствии с законодательством РФ. Сбор, хранение, использование и распространение информации такого рода допускается с согласия соответствующего лица или на основании судебного решения.

К перечню сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 г. № 188) также относятся:

1.Сведения, составляющие тайну следствия и судопроизводства;

2.Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и Федеральными законами (служебная тайна);

3.Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и Федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, тайна телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее (ст. 138, 155 УК РФ));

4.Коммерческой деятельностью, доступ, к которым ограничен в соответствии с Гражданским кодексом РФ и Федеральными законами (коммерческая или банковская тайна (ст. 183 УК РФ));

5.Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них (ст.147 УК РФ), а так же информация, являющаяся объектом авторских и смежных прав (ст. 146 УКРФ)[[49]](#footnote-49).

Предметом преступлений, ответственность за которые предусмотрена статьями 272 и 274 УК РФ, является охраняемая законом компьютерная информация, а предметом преступления, предусматривающим ответственность использования и распространения вредоносных программ (ст. 273 УК РФ) выступают вредоносные программы.

Заканчивая данную главу, хотелось бы отметить, что у ученых-юристов нет единого мнения, при определении предмета преступлений в сфере компьютерной информации. Однако, основываясь на проведенном исследовании объекта и предмета преступлений в сфере компьютерной информации можно дать развернутое определение компьютерного преступления. Итак, под компьютерным преступлением (преступлением в сфере компьютерной информации) следует понимать такое общественно опасное, противоправное, виновное деяние, посягающее на общественные отношения, обеспечивающие сохранность и конфиденциальность компьютерной информации (ст. 272 УК); общественные отношения, обеспечивающие безопасность компьютерной информации и компьютеров (ст. 273 УК); общественные отношения, обеспечивающие безопасность эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК), в котором компьютерная информация выступает в качестве предмета, а в некоторых случаях - в качестве орудия совершения преступления.

# ГЛАВА 2. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

# 2.1 Неправомерный доступ к компьютерной информации

И России, по данным ГИЦ МВД РФ, в 2002 г. по ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» было возбуждено 55 уголовных дел. Это более чем в 10 раз превышает показатель 2001 г. За 2003 г. возбуждено 135 уголовных дел. В 2004 г. было воз6уждено 584 уголовных дела. По итогам 2005 г. число возбужденных по ст. 272 УК РФ уголовных дел превысило тысячу[[50]](#footnote-50).

Уголовный закон (ст. 272 УК РФ) не дает определения неправомерного доступа к охраняемой законом компьютерной информации, он рассматривает лишь его последствия: уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Непосредственным объектом анализируемого преступления являются общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ, системы ЭВМ или их сети[[51]](#footnote-51). Дополнительный объект неправомерного доступа к компьютерной Информации факультативен. Его наличие зависит от вида вреда, причиненного правам и законным интересам потерпевшего. Дополнительным объектом может выступать, например, право собственности, авторское право, Арию на неприкосновенность частной жизни, личную и семейную тайну, общественные отношения по охране окружающей среды, внешняя безопасность Российской Федерации и др.

Вопрос об отнесении конкретного электронного устройства к категории электронно-вычислительной машины является не таким простым, как кажется на первый взгляд. Законодательство не содержит определения того, что представляет собой ЭВМ, однако широко использует этот термин. Вместе с тем, отсутствие законодательного закрепления определения данного понятия на практике вызывает определенные сложности. В частности, можно ли считать ЭВМ электронный контрольно-кассовый аппарат, сотовый телефон, электронный органайзер, электронные терминалы для оформления платежа по пластиковой карте, иные микропроцессорные устройства. Рассмотрим данный вопрос более подробно.

Толковый словарь по вычислительной технике и программированию утверждает, что ЭВМ есть цифровая вычислительная машина, основные узлы которой реализованы средствами электроники. В комментарий к УК РФ под редакцией Ю.И. Скуратова и В.М. Лебедева ЭВМ определяется как вычислительная машина, преобразующая информацию в ходе своего функционирования в числовую форму[[52]](#footnote-52). В комментарии к УК РФ под ред. С.И. Никулина и содержится следующее определение: ЭВМ представляет собой совокупность аппаратно-технических средств и средств программирования, позволяющих производить операции над символьной и образной информацией[[53]](#footnote-53).

Последнее определение вызывает наибольшие возражения, поскольку в нем с правовой точки зрения не отграничиваются понятия ЭВМ и системы ЭВМ.

Для полноты освещения вопроса о понятии ЭВМ следует рассмотреть их классификации.

В кибернетике принятая за основу следующая классификация:

1. Супер-ЭВМ. Уникальные по цели создания, быстродействию, объему
памяти ЭВМ и вычислительные системы, предназначенные для решения
особо сложных задач.
2. Большие ЭВМ. Стационарные вычислительные комплексы с большим
количеством разнообразных периферийных устройств, которыми оснащались
вычислительные центры.
3. Мини - ЭВМ, микро - ЭВМ, персональные ЭВМ. В настоящее время по
этим параметрам ЭВМ разных видов существенно сблизились, и поэтому не
всегда есть возможность для данного разделения.

По размеру ЭВМ подразделяются на:

а) стационарные, т.е. установленные в конкретном помещении и имеющие возможность работать только *в* данном помещении;

б) "настольные" малогабаритные, т.е. для установки которых требуется лишь стол и которые могут быть легко перемещены из помещения в
помещение в зависимости от потребности пользователя;

в) портативные (или «ноутбуки»), т.е. малогабаритные переносные,
размером от портфеля до блокнота, обеспечивающие за счет компактных
Батарейных источников питания возможность работы с ними в любом месте;

г) малогабаритные, включенные в механические и (или) технологические системы (управляющие полетами, движением, производственным процессом и т.п.).

По местонахождению и основной решаемой в сетях задачи среди ЭВМ можно выделить:

а) машина конечного пользователя;

6) машина администратора сети или системного оператора;

в) машина, работающая как «хранилище» базы данных;

г) машина, управляющая в автономном режиме технологическим процессом;

д) машина, работающая как почтовый сервер.

Кроме того, возможны классификации ЭВМ по наличию или отсутствию у них периферийных устройств; средств связи или включения в сеть ЭВМ и другим признакам.

Исходя из вышеизложенного, можно дать следующее определение. ЭВМ *-* электронное устройство, производящее заданные управляющей программой операции по хранению и обработке информации и управлению периферийными устройствами.

Это определение дает возможность утвердительно ответить на вопрос об отнесении к ЭВМ так называемых интегрированных систем (компьютеров в нетрадиционном понимании - пейджеров, сотовых телефонных аппаратов, электронных контрольно-кассовых машин, электронных банкоматов и терминалов работы с пластиковыми расчетными картами).

Понятие «система ЭВМ», введенное законодателем, также неоднозначно трактуется в юридической литературе.

А.В. Пушкин под системой ЭВМ понимает «распределение систем обработки данных, включающих в свой контур как мощные вычислительные комплексы, так и персональные компьютеры, удаленные на определенное расстояние друг от друга для организации коммуникационных локальных, отраслевых, общегосударственных или межгосударственных сетей»[[54]](#footnote-54). Исходя из данного определения фактически не следует принципиальных различий между понятиями «система ЭВМ» и «сеть ЭВМ», поэтому с данным подходом нельзя согласиться. Авторы комментария к УК РФ под редакцией В.М. Лебедева и Ю.И. Скуратова справедливо отмечают, что система ЭВМ предназначена для совокупного решения задач[[55]](#footnote-55).

Видимо, наиболее корректным в данной ситуации будет буквально трактовать законодателя и исходить из того, что понятие «система» предполагает определенную совокупность объектов, элементы которой находятся в упорядоченной взаимосвязи и взаимозависимости.

Итак, под системой ЭВМ следует понимать упорядоченную совокупность взаимосвязанных и взаимодействующих как единое целое ЭВМ, обеспечивающих выполнение единой функции. Примерами систем ЭВМ могут являться системы сотовой телефонной связи. Вся система работы сотовой сети основана на компьютерной технике и обмене информацией между центральным компьютером (контроллером, коммутатором) и периферийным установками (абонентским оборудованием). Отличием самого сотового телефонного аппарата от центрального компьютера является то, что первый несет информацию о конкретном абоненте, а последний информацию обо всех абонентах сотовой телефонной сети. Абонентское оборудование несет в своей базе данных информацию о самом телефонном аппарате, в том числе о его личном и абонентском номере. При осуществлении вызова с сотового телефона другого абонента или самого этого телефона другим абонентом между центральным компьютером и абонентским оборудованием осуществляется обмен данной информацией. В связи с тем, что данная информация в любой компании сотовой телефонной связи представляет коммерческую тайну, то получение данной информации посторонним лицом с центрального или периферийного оборудования будет неправомерной.

Информация о телефонах абонентов компании сотовой телефонной связи считается базой данных, занесенной в компьютерную систему, так как центральный компьютер и периферийное оборудование (сотовые аппараты} действуют в единой компьютерной системе, являясь взаимно необходимыми друг другу.

В вопросе о понимании термина «сеть ЭВМ» также существуют различные подходы.

Так, в Комментарии к УК под редакцией С. И. Никулина, сеть ЭВМ определяется как совокупность двух или более ЭВМ, соединенных между собой каналом связи и имеющих программное обеспечение, позволяющее осуществлять эту связь[[56]](#footnote-56). Думается, что такое определение больше подходит к понятию «система ЭВМ».

Вместе с тем в основе понятия «сеть» лежит техническая задача по установлению связи между различными ЭВМ. Участники сети (абоненты, пользователи) получают техническую возможность доступа со своих рабочих мест к информации, составляющей информационные ресурсы сети и находящейся в связанных компьютерной сетью ЭВМ. Это не исключает дифференциации возможностей пользователей по доступу к различным категориям информационных ресурсов, установления иерархии возможностей доступа.

Таким образом, сеть ЭВМ можно определить как способ организации связи между несколькими самостоятельными ЭВМ с целью получения доступа к совместными информационным ресурсам или оборудованию.

Под объективной стороной состава преступления в теории уголовного права понимается совокупность существенных, достаточных и необходимых признаков, характеризующих внешний акт общественно опасного посяга-тельства, причиняющего вред (ущерб) объекту, охраняемому уголовным законом[[57]](#footnote-57). Объективная сторона преступления, предусмотренного ч.1 ст.272 УК РФ, выражается в неправомерном доступе к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Исходя из данного законодателем определения, можно выделить три обязательных признака неправомерного доступа к компьютерной информации, характеризующие это преступление с его внешней, объективной стороны. Такими признаками являются:

1. общественно опасное действие, к которому законодатель относит неправомерный доступ к охраняемой законом компьютерной информации;
2. общественно опасные последствия в виде уничтожения, блокирования, модификации или копирования компьютерной информации, нарушения работы ЭВМ, системы ЭВМ или их сети;
3. причинная связь между совершенным деянием и наступившими последствиями. Отсутствие хотя бы одного из перечисленных признаков означает и отсутствие уголовной ответственности по ст.272 УК РФ.

К объективным признакам анализируемого преступления относится общественно опасное деяние, которое всегда проявляется в активной форме поведения виновного. Совершить неправомерный доступ к компьютерной информации путем бездействия невозможно.

Одним из необходимых оснований для привлечения виновного к уголовной ответственности по ст.272 УК РФ будет являться установление неправомерности действий лица. Иными словами, оно не имело права вызывать информацию, знакомиться с ней и распоряжаться ею. Неправомерность доступа к информации *-* обязательный признак, характеризующий рассматриваемое преступление с объективной стороны.

В диспозиции статьи указывается на неправомерный доступ именно к компьютерной информации, а не к носителям, на которых информация содержится. В силу этого положения очевидно, что физическое повреждение компьютера, повлекшее уничтожение информации, хранящейся в нем, не отвечает правовому содержанию общественно опасного действия, присущего преступлению, предусмотренному ст.272 УК РФ и, следовательно, не образует основания уголовной ответственности за его совершение. Речь в этом случае может идти об умышленном либо неосторожном уничтожении или повреждении имущества, если умысел виновного не был направлен именно на уничтожение информации.

Вторым обязательным признаком объективной стороны неправомерного доступа к компьютерной информации являются общественно опасные последствия в виде уничтожения, блокирования, модификации или копирования компьютерной информации, нарушения работы Э8М, системы ЭВМ или их сети.

Под уничтожением информацииследует понимать такое изменение ее первоначального состояния (полное либо частичное удаление информации с машинных носителей), при котором она перестает существовать в силу утраты основных качественных признаков. При этом не имеет значения, имелась ли у потерпевшего копия уничтоженной виновным информации или нет.

Блокирование компьютерной информациипредставляет собой закрытие информации, характеризующееся недоступностью ее использования по прямому назначению со стороны законного пользователя, собственника или владельца.

Модификация заключается в изменении первоначального состояния информации (например, реструктурирование или реорганизация базы данных, удаление или добавление записей, содержащихся в ее файлах, перевод программы для ЭВМ или базы данных с одного языка на другой), не меняющей сущности объекта.

Под копированиемпонимают перенос информации или части информации с одного физического носителя на другой. В отношении содержания данного термина в юридической литературе мнения разделились. Можно выделить два подхода к его толкованию. В рамках первого подхода понятие копирование трактуется весьма широко: как распространение и разглашение компьютерной информации[[58]](#footnote-58). Авторы, придерживающиеся более узкого определения копирования считают, что использование понятий «воспроизведение» и «распространение», заимствованных из авторского права, для раскрытия содержания используемою в Уголовном кодексе понятия «копирование» необоснованно, так как объекты ст. 146 УК РФ «Нарушение авторских и смежных прав» и гл. 28 УК РФ «Преступления в сфере компьютерной информации» различны[[59]](#footnote-59). Вторая позиция представляется более обоснованной.

Российским законодательством предусмотрен случай, когда копирование программного обеспечения не носит противоправного характера. В соответствии с л. 1 ст. 25 Закона РФ «Об авторском праве и смежных правах», лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без получения разрешения автора или иного пйладателя исключительных прав на использование произведения и без иыплаты дополнительного вознаграждения изготовить копию программы для ЭBM или базы данных при условии, что эта копия предназначена для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал программы для ЭВМ или базы данных утерян, уничтожен или стал непригодным для использования. При этом копия программы для ЭВМ или базы данных должна быть уничтожена в случае, пели владение экземпляром этой программы для ЭВМ перестанет быть правомерным. Как указывается в п. 3 этой же статьи, применение ее положений не должно наносить неоправданного ущерба нормальному использованию программы для ЭВМ или базы данных и не должно ущемлять необоснованным образом законные интересы автора или иного обладателя исключительных прав на программу для ЭВМ или базы данных.

Сам по себе факт вызова или просмотра компьютерной информации, хранящейся на машинном носителе, состава анализируемого преступления не образует. Необходимо, по крайней мере, установить факт переноса указанной информации на другой машинный носитель. Между тем несанкционированное ознакомление с охраняемой законом компьютерной информацией может выступать в качестве приготовления или покушения на совершение иного умышленного преступления, например, вымогательства (ст. 163 УК РФ), незаконного получения и разглашения сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ), шпионажа (ст. 276 УК РФ) и др. В этом случае дополнительной квалификации по ст.272 УК РФ не требуется[[60]](#footnote-60).

Нарушение работы ЭВМ, системы ЭВМ или их сети включает в себя сбой в работе ЭВМ, системы ЭВМ или их сети, препятствующий нормальному функционированию вычислительной техники при условии сохранения ее физической целостности и требований обязательного восстановления (например, отображение неверной информации на мониторе, нарушение порядка выполнения команд, разрыв сети и др.).

В том случае, когда неправомерный доступ к компьютерной информации приводит к серьезным повреждениям компьютерной техники и тем самым причиняет значительный ущерб собственнику или владельцу, действия виновного, наряду со ст.272 УК РФ, подлежат дополнительной квалификации по ст.167 УК РФ (умышленное уничтожение или повреждение имущества).

Анализ ч.1 ст.272 УК РФ позволяет признать, что неправомерный доступ к компьютерной информации относится к материальным составам преступления и, следовательно, считается оконченным с момента наступления общественно опасных последствий, альтернативно перечисленных в диспозиции статьи закона. В случае отсутствия указанных последствий состав анализируемого преступления не считается полным. Поэтому действия лица, хотя и связанные с неправомерным доступом к компьютерной информации, но не повлекшие за собой уничтожения, блокирования, модификации либо копирования компьютерной информации, нарушение работы ЭВМ, системы ЭВМ или их сети по не зависящим от этого лица обстоятельствам, образуют предварительную преступную деятельность и квалифицируются со ссылкой на ст.30 УК РФ.

Третьим необходимым признаком объективной стороны неправомерного доступа к компьютерной информации является причинная связь между противозаконными действиями виновного и наступившими вредными последствиями. Ответственность по ст.272 УК РФ наступает только в том случае, если преступные последствия, альтернативно отраженные в ее диспозиции, явились именно необходимым следствием, закономерно вызванным неправомерным доступом лица к охраняемой законом компьютерной информации, а не наступили в силу иных причин.

Действующее уголовное законодательство не выделяет квалифицированные составы преступлений по признаку использования электронной техники. Поэтому в тех случаях, когда неправомерный доступ к компьютерной информации выступает способом совершения другого умышленного преступления, а электронно-вычислительная техника используется в качестве орудия для достижения преступной цели, содеянное виновным квалифицируется по совокупности преступлений.

Определенную сложность вызывают вопросы, связанные с установлением времени и места совершения неправомерного доступа к компьютерной информации. Дело в том, что стремительное развитие компьютерной техники уже сегодня вышло на качественно новый уровень. Созданы мировые информационные сети, объединившие пользователей практически всех развитых стран. Поэтому время и место совершения общественно опасного деяния (место происшествия) может не совпадать с местом и временем реального наступления общественно опасных последствий. В практике борьбы с компьютерной преступностью насчитывается немало случаев, когда сам факт неправомерного доступа « охраняемой информации фиксировался в одной стране, а преступные последствия наступали на территории другого государства.

Местом совершения неправомерного доступа к компьютерной информации следует признавать территорию того государства, где это преступление было окончено, что соответствует положениям ст.8 УК РФ об основании уголовной ответственности, которым является совершение деяния, содержащего все признаки состава преступления, предусмотренною Уголовным кодексом.

Действующее уголовное законодательство России временем совершения любого преступления признает время совершения общественно опасного действия (бездействия) независимо от времени наступления последствий (ч.2 ст.9 УК РФ). Очевидно, данное правило должно распространяться и на вопрос о времени совершения неправомерного доступа к компьютерной информации.

К признакам, характеризующим субъективную сторону любого преступления, относятся вина, мотив и цель общественно опасного и противоправного поведения субъекта. Все эти признаки дают представление о том внутреннем процессе, который происходит в психике лица, совершающего преступление, и отражают связь сознания и воли индивида с осуществляемым им поведенческим актом[[61]](#footnote-61).

Применительно к неправомерному доступу к компьютерной информации уголовно-правовое значение признаков субъективной стороны не равнозначно. Вина - необходимый признак субъективной стороны каждого преступления. Мотив и цель совершения неправомерного доступа к компьютерной информации законодатель отнес к числу факультативных признаков данного состава.

Раскрывая содержание вины, следует исходить из общепринятого в российской уголовно-правовой доктрине положения о том, что вина представляет собой психическое отношение лица к совершенному общественно опасному деянию и его общественно опасным последствиям. Она выражается в форме умысла или неосторожности.

Несмотря на то, что диспозиция ст.272 УК РФ не дает прямых указаний о субъективной стороне анализируемого преступления, можно с уверенностью говорить об умышленной форме вины в виде прямого или косвенного умысла. В литературе высказывалась и другая точка зрения, согласно которой неправомерный доступ к охраняемой законом компьютерной информации может быть совершен только с прямым умыслом[[62]](#footnote-62). Между тем закон вовсе не ограничивает привлечение лица к уголовной ответственности по ст.272 УК РФ в случае совершения этого преступления с косвенным умыслом. Как показывает практика, преступник не всегда желает наступления вредных последствий. Особенно это характерно при совершении данного преступления из озорства или так называемого спортивного интереса.

В силу этого положения становится очевидным, что интеллектуальный момент вины, характерный для состава анализируемого преступления, заключается в осознании виновным факта осуществления неправомерного доступа к охраняемой законом компьютерной информации. При этом виновный понимает не только фактическую сущность своего поведения, но и его социально опасный характер. Кроме того, виновный предвидит возможность или неизбежность реального наступления общественно опасных последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Следовательно, субъект представляет характер вредных последствий, осознает их социальную значимость и причинно-следственную зависимость.

Волевой момент вины отражает либо желание (стремление) или сознательное допущение наступления указанных вредных последствий, либо как минимум безразличное к ним отношение.

Неправомерный доступ к охраняемой законом компьютерной информации, совершенный по неосторожности, исключает правовое основание для привлечения лица к уголовной ответственности. Указанное положение полностью соответствует ч.2 ст.24 УКРФ: «Деяние, совершенное по неосторожности, признается преступлением только в том случае, когда это специально предусмотрено соответствующей статьей Особенной части настоящего Кодекса». О неосторожности в диспозиции ст.272 УК РФ не сказано. Следовательно, деяние может быть совершено лишь умышленно. В силу этого обстоятельства трудно согласиться с мнением авторов одного из научно-практических комментариев к Уголовному кодексу Российской Федерации, в котором утверждается, что неправомерный доступ к информации может совершаться как с умыслом, так и по неосторожности. «Неосторожная форма вины, - пишет С.А.Пашин, - может проявляться при оценке лицом правомерности своего доступа к компьютерной информации, а также I) отношении неблагоприятных последствий доступа, предусмотренных диспозицией данной нормы уголовного закона»[[63]](#footnote-63). Признание этой точки прения противоречит законодательному положению, закрепленному в ч.2 ст.24 УК РФ, что, в свою очередь, ведет к возможности необоснованного привлечения лица к уголовной ответственности за неосторожное поведение.

Таким образом, при совершении неправомерного доступа к компьютерной информации интеллектуальный и волевой моменты вины всегда наполнены определенным содержанием, выяснение которого является предпосылкой правильной юридической оценки содеянного.

Мотивы и цели неправомерного доступа к охраняемой законом компьютерной информации могут быть самыми разнообразными. Обязательными признаками состава рассматриваемого преступления они не являются и, следовательно, на квалификацию преступления не влияют. Однако точное установление мотивов и целей неправомерного доступа к охраняемой .эконом компьютерной информации позволяет выявить не только причины, побудившие лицо совершить данное преступление, но и назначить виновному справедливое наказание.

Как правило, побуждающим фактором к совершению неправомерного доступа к охраняемой законом компьютерной информации является корысть, что, естественно, повышает степень общественной опасности указанного преступления. В качестве иллюстрации корыстного доступа к компьютерной информации может служить пример, когда лицо путем подбора идентификационного кода (пароля) внедряется в компьютерную сеть, обслуживающую банковские операции, инезаконно перечисляет определенную сумму денежных средств на свой текущий счет.

Наряду с корыстью анализируемое преступление может совершаться из чувства мести, зависти, хулиганства, желания испортить деловую репутацию конкурента, «спортивного интереса» или желания скрыть другое преступление и т.д.

Согласно ст.20 УК РФ субъектом преступления[[64]](#footnote-64)*,* предусмотренного ч.1 ст.272 УК РФ, может быть любое физическое лицо, достигшее к моменту преступной деятельности шестнадцатилетнего возраста. Обязательным условием привлечения лица к уголовной ответственности за совершенное общественно опасное и противоправное деяние является вменяемость. Невменяемые лица не могут подлежать уголовной ответственности (ст. 21 УК РФ).

В ст. 272 УК РФ предусмотрены обстоятельства, отягчающие ответственность за его совершение, при наличии которых преступление признается более опасным и поэтому влечет более строгое наказание. К числу отягчающих законодатель относит следующие обстоятельства:

а) неправомерный доступ к компьютерной информации, совершенный
группой лиц по предварительному сговору;

б) неправомерный доступ к компьютерной информации, совершенный
организованной группой лиц;

в) неправомерный доступ к компьютерной информации, совершенный
лицом с использованием своего служебного положения;

г) неправомерный доступ к компьютерной информации, совершенный
лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Таким образом, признаки квалифицированного состава рассматриваемого преступления характеризуют либо объективную сторону посягательства, либо субъект преступления.

Анализ отечественного законодательства в сфере компьютерной информации позволяет отметить ряд недостатков, затрудняющих расследование неправомерного доступа к компьютерной информации:

1. Сложность конструкций правовых норм (ст. 272 УК РФ), наличие в них технических понятий и специальных терминов. Значительная сложность возникает в уяснении терминологии, назначении составных частей ЭВМ, системы ЭВМ и их сети, понимании общего режима их функционирования в различных технологических процессах. В.В. Крылов считает, что подход, согласно которому в законодательстве следует отражать конкретные технические средства себя исчерпал, поскольку ЭВМ является лишь разновидностью информационного оборудования и не охватывает всего разнообразия информационной техники[[65]](#footnote-65).
2. Обилие и порой противоречивость нормативных актов, определяющих правовой статус и специфику компьютерной информации. Это приводит к тому, что многие нормативные документы, регламентирующие правовой режим функционирования средств компьютерной техники, остаются неизвестными и соответственно не учитываются в процессе проведения проверочных мероприятий и первоначальных следственных действий. Отсутствие обобщений следственной и судебной практики, которые
могли бы быть ориентиром в правильной квалификации преступлений.
3. Мягкость санкций ст. 272 - 274 УК РФ. Максимальное наказание за эти
преступления предусмотрено ст. 273 УК РФ - лишение свободы до трех лет.
4. Сложности разграничения смежных составов преступлений[[66]](#footnote-66). При квалификации, например, неправомерного доступа к компьютерной информации могут возникнуть вопросы, касающиеся отграничения этого преступления от иных видов преступных посягательств, связанных с уничтожением, блокированием, модификацией либо копированием информации, нарушением работы ЭВМ, системы ЭВМ или их сети, а равно преступлений, предметом которых является какая-либо информация, находящаяся на машинном носителе, в электронно-вычислительной машине, системе ЭВМ или их сети. К таким преступлениям следует отнести:

а) преступления в сфере компьютерной информации: 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);

б) иные противоправные деяния, предметом посягательства которых
может являться компьютерная информация, содержащаяся на машинном носителе, в ЭВМ, системе ЭВМ или их сети: нарушение неприкосновенности частной жизни (ст.137 УК РФ), нарушение авторских и смежных прав (ст.146 УК РФ), незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну (ст.183 УК РФ), и некоторые другие.

В следственной практике нередко совершаются ошибки при квалификации незаконного подключения к сети Интернет. Следователи зачастую необоснованно отказывают в возбуждении уголовного дели или прекращают производство по делу в связи с тем, что информация в сети Интернет общедоступна, не имеет конкретного владельца, следовательно, не является охраняемой законом, т.е. не может выступать предметом преступного посягательства.

Так, З. осуществил незаконное проникновение в компьютерную сеть Интернет с использованием сервера фирмы «Эликом» под именем и паролем фирмы «Микст» и произвел копирование файлов, на основании чего следователем было обоснованно возбуждено уголовное дело по ч.1 ст.272[[67]](#footnote-67).

В процессе расследования в действиях 3. не было установлено признаков состава преступления, предусмотренного ст.272УК РФ, поскольку информация, содержащаяся в незащищенных файлах компьютерной сети Интернет, доступ к которой осуществил 3., не является охраняемой законом компьютерной информацией и не имеет конкретного владельца. В связи с этим, производство по данному делу было прекращено за отсутствием состава преступления.

Представляется, что производство по данному делу прекращено необоснованно, поскольку следователем не была до конца отработана версия о неправомерном доступе к охраняемой законом компьютерной информации, находящейся на сервере фирмы «Эликом», повлекшее ее блокирование, что также подпадает под признаки уголовно наказуемого деяния.

Неоднозначно в следственной практике разрешается вопрос и о квалификации деяний, совершаемых в отношении компьютерной информации, находящейся в ЭВМ, не являющейся компьютером в классическом понимании этого слова (таких, как пейджер, сотовый телефон, кассовый аппарат и т.п.).

Сотовая телефонная сеть представляет собой сеть ЭВМ (микропроцессорных устройств), в качестве компонентов которой выступают: абонентское оборудование (сотовые телефонные аппараты), базовые станции, коммутатор, контроллер. Абонентское оборудование, являясь микропроцессорным устройством, т.е. устройством, способным обрабатывать информацию, имеющуюся в эфире, и отвечать на нее в случае передачи и приема информации с контроллера, который является компьютером с базой данных об абонентском оборудовании и всем оборудовании базовой станции. Данная информация хранится на жестком диске, но она также используется при обработке процесса вызова, в связи с чем возникает техническая возможность наблюдать ее часть в эфире в момент общения базовой станции с абонентским оборудованием. И в случае, когда указанная информация стала доступной для посторонних лиц, это считается доступом к компьютерной информации, хранящейся на машинном носителе, и копированием данной информации.

Вся система работы сотовой сети основана на компьютерной технике и обмене информацией между центральным компьютером (контроллером, коммутатором) и периферийными установками (абонентским оборудованием). Отличием самого сотового телефонного аппарата от центрального компьютера является то, что первый несет информацию о конкретном абоненте, а последний - информацию обо всех абонентах сотовой телефонной сети. Абонентское оборудование несет в своей базе данных информацию о самом телефонном аппарате, в том числе о его личном и абонентском номере. При осуществлении вызова с сотового телефона другого абонента или самого этого телефона другим абонентом между центральным компьютером и абонентским оборудованием осуществляется обмен данной информацией, В связи с тем что данная информация в любой компании сотовой телефонной связи представляет коммерческую тайну, то получение данной информации посторонним лицом с центрального или периферийного оборудования будет неправомерным. Информация о телефонах абонентов компании сотовой телефонной связи считается базой данных, занесенной в компьютерную систему, так как центральный компьютер и периферийное оборудование (сотовые аппараты) действуют в единой компьютерной системе, являясь взаимно необходимыми друг другу.

Таким образом, сотовую сеть можно рассматривать как компьютерную, при этом сам сотовый аппарат является удаленным рабочим местом беспроводной сети, а центральный контроллер - файловым и коммуникационным сервером. Аналогично можно рассматривать и пейджинговую сеть, с той лишь разницей, что пейджер является удаленным терминалом. В силу этого на информацию, находящуюся в сотовых и пейджинговых сетях распространяются как законы, ее охраняющие, так и диспозиции соответствующих статей 28-й главы УК Российской Федерации.

Рассмотрим положительный опыт следователей ГСУ при ГУВД Московской области, впервые применивших ст. 272 УК РФ при расследовании уголовного дела о неправомерном доступе в контрольно-кассовые аппараты одного из частных предприятий области.

В ноябре 1998 г. УРОПД ГУВД Московской области было возбуждено уголовное дело по факту совершения неправомерного доступа к охраняемой законом компьютерной информации в кассовых аппаратах частного предприятия г. Павловский Посад.

Проведенным по делу расследованием установлено, что в период с июля по ноябрь 1998 г. руководитель ЧП города Павловский Посад Московской области Т. по предварительному сговору в группе с К., действуя с ней с единым умыслом в целях сокрытия доходов от налогообложения, ежедневно с 17 до 19 часов в торговых палатках ЧП подключали в гнезда двух контрольно-кассовых аппаратов, являющихся разновидностью электронно-вычислительной машины, специально изготовленный самодельный прибор в виде микрокомпьютера, осуществляя доступ к компьютерной информации о проведенных через контрольно-кассовые аппараты финансовых операциях в течение текущей смены. После подключения прибора к контрольно-кассовым аппаратам и совершения неправомерного доступа к охраняемой законом компьютерной информации в буферной памяти контрольно-кассовых аппаратов уничтожалась вся информация о предшествующих финансовых операциях, выполненных в течение текущей смены, в том числе информация о номере покупки и общей сумме выручки за текущую смену. Уничтожив и модифицировав информацию в буферной памяти контрольно-кассовых аппаратов в течение указанного времени, обе торговые точки ЧП продолжали свою работу, накапливая информацию в буферной памяти о производимых финансовых операциях до окончания текущей смены, то есть до 21 часа, после чего в фискальную память контропьно-кассовых аппаратов заносились измененные, заниженные данные о сумме выручки за смену.

Таким образом, Т. и К. совершили неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (в соответствии с техническим паспортом контрольно-кассовый аппарат считается ЭВМ), и это деяние, совершенное группой лиц по предварительному сговору, повлекло уничтожение, модификацию информации[[68]](#footnote-68).

# 2.2 Создание, использование и распространение вредоносных программ для ЭВМ

Согласно ч. 1 ст. 273 УК РФ создание, использование и распространение вредоносных программ для ЭВМ представляет собой 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 или распространение таких программ.

По данным ГИЦ МВД России, в 2002 году было возбуждено 1 уголовное дело по ст. 273 УК РФ. В 2003 г. было зарегистрировано 12 преступлений по ст.273 УК РФ. В 2004 г. зарегистрировано 85 преступлений по ст. 273 УК РФ. В 2005 г. по ст. 273 УК РФ возбуждено 172 уголовных дела[[69]](#footnote-69).

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

С объективной стороны анализируемое преступление предусматривает совершение хотя бы одного из следующих действий:

1. создание вредоносных программ для ЭВМ;
2. внесение изменений в существующие программы для ЭВМ;
3. использование вредоносных программ для ЭВМ;
4. распространение вредоносных программ для ЭВМ.

Совершить создание, использование или распространение вредоносных программ для ЭВМ путем бездействия невозможно.

Некоторые авторы предлагают дополнить указанный перечень использованием машинных носителей с вредоносными программами, однако, на наш взгляд, указанное действие охватывается понятием «использование вредоносных программ»[[70]](#footnote-70). Рассмотрим указанные действия более подробно.

Создание вредоносных программ для ЭВМ. Для наступления уголовной ответственности данная программа должна являться вредоносной. Одно из наиболее удачных определений вредоносной программы предложено Ю.И. Ляпуновым и А.В. Пушкиным. Под вредоносной программой названные авторы понимают специально написанную (созданную) программу, которая, получив управление, способна совершать несанкционированные пользователем действия и вследствие этого причинять вред собственнику или владельцу информации, а также иным лицам в виде уничтожения, блокирования, модификации или копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети.

Под созданием вредоносной программы понимается комплекс операций, состоящих из подготовки исходных данных, предназначенных для управления конкретными компонентами системы обработки данных в целях, указанных в диспозиции ст. 273 УК РФ. Создание вредоносных программ - целенаправленная деятельность, включающая (в общем виде): 1) постановку задачи, определение среды существования и цели программы; 2) выбор средств и языков реализации программы; 3} отладку программы; 4) запуск и работу программы. Все эти действия при постановке задачи создания вредоносной программы и наличии объективных следов их выполнения могут быть признаны наказуемыми в уголовном порядке.

Вредоносность или полезность соответствующих программ для ЭВМ определяется не а зависимости от их назначения, способности уничтожать, модифицировать, копировать информацию (это вполне типичные функции вполне легальных программ), а в связи с тем, предполагает ли их действие, во-первых, предварительное уведомление собственника компьютерной информации или другого законного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из этих требований делает программу вредоносной.

Внесение изменений в существующие программы - это несанкционированная законным пользователем или собственником программы ее модификация (переработка программы путем изменения, добавления или удаления ее отдельных фрагментов) до такого состояния, когда эта программа способна выполнить новые, изначально незапланированные функции и приводить к последствиям, предусмотренным ч. 1 ст. 273 УК РФ. При этом Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» уточняет, что модификация (переработка) программы для ЭВМ - это любые ее изменения, не являющиеся адаптацией.

1. Под использованием вредоносной программы согласно ст. 1 Закона «О правовой охране программ для электронных вычислительных машин и баз данных» понимается ее непосредственный выпуск в свет, распространение и иные действия по ее введению в хозяйственный оборот (в том числе в модифицированной форме). Не признается использованием программы для ЭВМ передача средствами массовой информации сообщений о выпущенной в свет программе для ЭВМ. Однако, данная трактовка является слишком широкой, и нам представляется более верным определение, предложенное А.В. Пушкиным, указывающим, что «под использованием вредоносных программ следует понимать их введение (установку) в электронную память компьютера»[[71]](#footnote-71).

Отметим, что уголовная ответственность по этой статье возникает уже в результате создания программы независимо от того, использовалась программа или нет. По смыслу ст.273 УК наличие исходных текстов вирусных программ уже является основанием для привлечения к ответственности. Однако следует учитывать, что в ряде случаев использование подобных программ не будет являться уголовно наказуемым. Это относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих соответствующую лицензию. Также очевидно, что собственник информационного ресурса вправе внеобходимых случаях (например, исследовательские работы по созданию антивирусных средств) использовать вредоносные программы. Естественно, что для квалификации действий как использования вредоносных программ необходимо доказать, что лицо заведомо знало о свойствах используемой программы и последствиях ее применения.

Под использованием машинного носителя с вредоносной программой следует понимать всякое его употребление для целей использования записанной на нем программы для ЭВМ.

Распространение программы для ЭВМ - это предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей. Распространение вредоносных программ может осуществляться непосредственно путем их копирования на компьютер потерпевшего, например, с дискеты, а также опосредовано, путем передачи по электронной почте, по линии связи законного пользователя через компьютерную сеть.

Состав преступления, предусмотренного ч. 1 ст. 273 УК РФ, сконструирован законодателем как усеченный, или, как он еще именуется в юридической литературе, состав опасности. Особенность его в том, что в уголовном законе содержится описание признаков не только объективной стороны, но и реальной возможности наступления вреда, в данном случае в форме несанкционированного законным пользователем уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети.

Под несанкционированным уничтожением, блокированием, модификацией, копированием информации понимаются не разрешенные законом, собственником информации или другим компетентным пользователем указанные действия.

Следует обратить внимание, что большинство авторов отождествляют понятия вредоносной программы и компьютерного вируса[[72]](#footnote-72). Так, С.В. Полубинская в соавторстве с С.В. Бородулиным в учебнике «Российское уголовное право. Особенная часть» прямо указывают, что в ст. 273 УК РФ «...речь идет о разработке и распространении так называемых компьютерных вирусов как путем создания подобного рода компьютерных программ, так и путем внесения изменений в уже существующие программы»[[73]](#footnote-73). С подобным подходом вряд ли можно согласиться.

Представляется, что многообразие вредоносных программ только лишь компьютерными вирусами не ограничивается. Любая вредоносная программа, чтобы являться таковой, должна обладать как минимум следующими признаками: во-первых, она должна совершать несанкционированные пользователем действия, и, во-вторых, результатом этих действий должно быть уничтожение, блокирование, модификация или копирование компьютерной информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Вирус же, отвечая названным условиям, обладает дополнительной функцией — он способен самовоспроизводиться, то есть размножаться, присоединяться к другим программам и пр. Программу - вирус, таким образом, можно определить как специально созданную программу, способную к самовоспроизведению, выполняющую незапланированные законным пользователем функции. Эти функции могут быть различными: порча файлов, приводящая к блокированию, модификации или уничтожению находящейся в них информации; засорение памяти компьютера, влекущее замедление его работы; вывод на экран посторонних сообщений и пр.

Вредоносные программы в отдельных случаях могут производить модификацию программ законного пользователя путем тайного встраивания в них набора команд, которые должны сработать при определенных условиях через определенное время. Например, как только программа незаконно перечислит денежные средства на так называемый подставной счет, она самоуничтожится и при этом уничтожит всю информацию о проделанной операции.

Кроме того, вредоносные программы могут основываться на использовании ошибок в логике построения определенной программы законного пользователя и обнаружении так называемых «брешей». При этом программа «разрывается» и в нее вводится необходимое число определенных команд, которые помогают ей осуществлять новые, незапланированные функции при одновременном сохранении прежней ее работоспособности. Именно таким образом можно переводить деньги на подставные счета, получать информацию о недвижимости, о персональных данных личности и пр.

По своей сути вирусы весьма различны: от теоретически безопасных до настоящих боевых программ, способных привести компьютер в состояние полной негодности. Само понятие «компьютерный вирус» ввел в обиход в начале 80-х годов профессор Лехайского университета Ф. Коэн. Одним из первых официально зарегистрированных компьютерных вирусов был так называемый «Пакистанский вирус». Затем появились «Рождественская пика», «Вирус Морриса», «I love you» и др. Хорошо известен случай, когда в начале 1989 г. вирусом, написанным американским студентом Р. Моррисом, были заражены и выведены из строя тысячи компьютеров, в том числе и принадлежащих министерству обороны США[[74]](#footnote-74).

Подобные явления не обошли стороной и Россию. В 1983 г. на Волжском автомобильном заводе был изобличен программист, который из мести к руководству предприятия умышленно внес изменения в программу ЭВМ, управлявшей подачей деталей на конвейер. В результате произошедшего сбоя заводу был причинен существенный материальный ущерб: не сошло с конвейера свыше сотни автомобилей. Программист был привлечен к уголовной ответственности, обвинялся по ч. 2 ст. 98 УК РСФСР «Умышленное уничтожение или повреждение государственного или общественного имущества ... причинившее крупный ущерб». При этом обвиняемый утверждал, что ничего натурально повреждено не было - нарушенным оказался лишь порядок работы, т.е. действия, не подпадающие ни под одну статью действующего в то время законодательства. С научной точки зрения интересен приговор суда: «три года лишения свободы условно; взыскание суммы, выплаченной рабочим за время вынужденного простоя главного конвейера; перевод на должность сборщика главного конвейера»[[75]](#footnote-75).

В настоящее время квалификация действий программиста должна была бы производиться по ч.1 ст.273 УК РФ. Он умышленно создал и использовал в заводском компьютере вредоносную программу, нарушившую технологический процесс.

С распространением персональных компьютеров вирусы поистине стали их бедствием. В настоящее время количество вирусов для ЭВМ достигает нескольких тысяч и их количество постоянно растет. По подсчетам отдельных специалистов, ежедневно в мире создается от 3 до 8 новых вирусных программ[[76]](#footnote-76). И несмотря на создание и совершенствование уникальных антивирусных программ, опасность создания, использования и распространения вредоносных программ остается весьма высокой. Уже сегодня, например, существуют исследования, показывающие, что вредоносные программы (в частности, так называемый вирус «666») могут воздействовать через различные цветовые коды - заставки экрана монитора - непосредственно на психику человека, доводя его до психического заболевания или смерти[[77]](#footnote-77).

Таким образом, вредоносность компьютерных вирусов связана с их свойством само воспроизводиться и создавать помехи работе на ЭВМ без ведома и санкции добросовестных пользователей. Вирусные программы обычно включают команды, обеспечивающие самокопирование и маскировку.

Достаточно часто создание, использование и распространение вредоносных программ для ЭВМ выступает в качестве способа совершения иного умышленного преступления, например: воспрепятствование осуществлению избирательных прав граждан или работе избирательных комиссий (ст. 141 УК РФ); фальсификация избирательных документов, документов референдума или неправильный подсчет голосов (ст. 142 УК РФ); мошенничество (ст. 159 УК РФ); причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ); незаконное получение сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ); неправомерный доступ к компьютерной информации (ст. 272 УК РФ); диверсия (ст. 281 УК РФ) и др. В этом случае содеянное надлежит квалифицировать по совокупности совершенных виновным преступлений. Примером подобного преступления может являться следующее. К., являясь оператором ЭВМ в одной из организаций, на своем личном компьютере Pentium III, находящемся в его квартире, изготовил электронное почтовое сообщение с рекламой товаров народного потребления, приложив к нему в качестве подробного каталога с ценами и условиями поставки составленную им лично вредоносную программу для ЭВМ в виде файла katalog.exe, и распространил ее согласно имеющемуся у него списку электронных почтовых адресов пользователей сети Интернет 350 адресатам. В результате массового распространения этой вредоносной программы после ее запуска пользователями сети Интернет, К, несанкционированно получил по своему электронному адресу 87 учетных имен и паролей для доступа в сеть Интернет, которые скопировал на жесткий диск своего компьютера и в дальнейшем использовал для доступа в сеть Интернет[[78]](#footnote-78).

В приведенном примере налицо несколько составов преступлений.

Во-первых, несомненно, что К. совершил создание, использование и распространение вредоносных программ для ЭВМ то есть, преступление, ответственность за которое предусмотрено ч. 1 ст. 273 УК РФ.

Во-вторых, К. совершил мошенничество, то есть хищение чужого имущества, совершенное путем обмана, поскольку работал в сети Интернет за счет законных пользователей, не знавших о наличии у программы katalog.exe неких тайных, незапланированных функций, приводящих к пересылке учетных данных законных пользователей К., то есть преступление, ответственность за которое предусмотрена п. «6» ч. 2 ст. 159 УК РФ.

В - третьих, К. совершил неправомерный доступ к охраняемой законом компьютерной информации (которой являются учетные данные пользователей), повлекший ее блокирование (поскольку, в период работы К. законные пользователи не могли получить доступ к системе), то есть преступление, ответственность за которое предусмотрена ч. 1 ст. 272 УК РФ.

Субъективную сторону анализируемого состава преступления представляет вина в форме прямого или косвенного умысла. Иными словами, для квалификации деяния по ч. 1 или 2 ст. 273 УК РФ необходимо, чтобы виновное лицо сознавало общественно опасный характер своих действий (то есть что оно создает, использует или распространяет такую программу, которая способна уничтожить, блокировать, модифицировать или скицировать компьютерную информацию, нарушить работу ЭВМ, системы НИМ или их сети), желало или сознательно допускало наступление вредоносных последствий либо относилось к ним безразлично.

И юридической литературе на данный счет имеются различные точки Япония. Так, Ю.И. Ляпунов и А.В. Пушкин считают, что данное преступление может совершаться только с прямым умыслом. Однако как же тогда квалифицировать действия лица, осуществляющего распространение машинных носителей информации (дискет, CD-дисков), содержащих вредоносные программы, достоверно знающего о вредоносных последствиях записи программы (хотя бы по этикетке компакт-диска), но вместе с тем абсолютно безразлично к ним относящихся? На наш взгляд, данное лицо совершает распространение вредоносных программ для ЭВМ именно с косвенным умыслом.

Вместе с тем нельзя согласиться с мнением профессора С.В. Бородина, считающего возможным совершение анализируемого преступления по неосторожности в виде легкомыслия[[79]](#footnote-79). Как минимум, законодатель в диспозиции ст. 273 дал четкое указание на заведомый характер деятельности виновного. Уже это не позволяет признать возможным совершение данного преступления по неосторожности.

Заметим, что в процессе отладки создаваемой программы могут проявиться случайные результаты, возникшие, например, в из-за ошибок разработчика, которые могут привести к указанным в ст. 273 последствиям: уничтожению, блокированию, модификации или копированию информации, нарушению работы ЭВМ, их системы или сети. При этом подобный результат будет полной неожиданностью для самого разработчика. Например, знаменитый само размножающийся «червь» Морриса стал знаменитым только потому, что в работоспособных копиях программы отказал механизм самоуничтожения, регулирующий количество одновременно работающих копий, были ли в этом умысел юного дарования или простая ошибка проектирования программы, суд так и не разобрался. По российскому законодательству, в подобных ситуациях лицо не будет нести уголовную ответственность, поскольку указанные последствия не охватываются его умыслом.

Субъектом анализируемого состава преступления может быть любое физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста. Если создание, использование или распространение вредоносных программ для ЭВМ совершил представитель юридического лица, то уголовной ответственности подлежит непосредственный исполнитель.

Часть 2 ст. 273 УК РФ в качестве квалифицирующего признака преступления предусматривает наступление тяжких последствий. Следовательно, квалифицированный состав рассматриваемого преступления сконструирован по типу материального состава. В силу этого обстоятельства для признания лица виновным в совершении преступления, ответственность за которое наступает по ч.2 ст. 273 УК РФ, необходимо установить, что факт наступления тяжких последствий является следствием создания, использования или распространения вредоносных программ для ЭВМ или машинных носителей с такими программами, то есть действий, образующих объективную сторону преступления.

Ю.И. Ляпунов и А.В. Пушкин к таким тяжким последствиям относят: причинение смерти или тяжкого вреда здоровью хотя бы одному человеку, причинение средней тяжести вреда здоровью двум и более лицам, массовое причинение легкого вреда здоровью людей, наступление экологических катастроф, транспортных и производственных аварий, повлекших длительную остановку транспорта или производственного процесса, дезорганизацию работы конкретного юридического лица, причинение крупного материального ущерба и т.п.[[80]](#footnote-80)

Специфика квалифицированного состава преступления заключается в том, что оно совершается с двумя формами вины, то есть характеризуется умыслом относительно факта создания, использования или распространения вредоносной программы для ЭВМ и неосторожностью (легкомыслием либо небрежностью) относительно наступления тяжких последствий. Это означает, что причинение тяжких последствий не охватывается умыслом виновного, однако он предвидит возможность их наступления, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение, либо не предвидит, хотя должен был и мог предвидеть возможность наступления тяжких последствий.

# 2.3 Нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети

Статья 274 УК РФ устанавливает уголовную ответственность за 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 или повлекло по неосторожности тяжкие последствия.

Среди преступлений, предусмотренных гл. 28 УК РФ, данное преступление является наименее распространенным. Так, по данным ГИЦ МВД России, в 2001 г. в Российской Федерации не было зарегистрировано ни одного факта нарушения правил эксплуатации ЭВМ, их системы или сети, в 2002 г. - одно преступление, в 2003 г. - ни одного, в 2004 г, их количество поставило 44, а по итогам 2005 г. число фактов нарушения правил эксплуатации ЭВМ впервые преодолело отметку 100[[81]](#footnote-81).

Недостаточно разработана и уголовно-правовая характеристика рассматриваемого преступления.

Уголовный закон (ст. 274 УК РФ) не дает определения нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, он раскрывает лишь его последствия: уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ. Таким образом, диспозиция ст. 274 носит бланкетный (отсылочный) характер. Представляется, что в этом состоит один из недостатков действующего уголовного законодательства в области защиты компьютерной информации.

Родовым объектом нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети является совокупность общественных отношений, составляющих содержание общественной безопасности и общественного порядка. Видовым объектом посягательства выступает совокупность общественных отношений в части правомерного и безопасного использования компьютерной информации и информационных ресурсов. Непосредственным объектом анализируемого преступления являются общественные отношения в сфере соблюдения установленных правил, обеспечивающих нормальную эксплуатацию ЭВМ, системы ЭВМ или их сети[[82]](#footnote-82). Дополнительный объект нарушения правил эксплуатации ЭВМ, их системы или сети факультативен. Его наличие зависит от вида вреда, причиненного правам и законным интересам потерпевшего. Дополнительным объектом может, например, выступать право собственности, авторское право, право на неприкосновенность частной жизни, личную и семейную тайну, общественные отношения по охране окружающей среды, внешняя безопасность Российской Федерации и др.

В диспозиции ст. 274 УК РФ содержится прямое указание на предмет преступного посягательства. Им является компьютерная информация.

Думается, что текст ст. 274 УК РФ содержит серьезный недостаток, заключающийся в отсутствии возможности привлечения лица к уголовной ответственности за нарушение правил обращения с машинными носителями информации, повлекшее предусмотренные диспозицией статьи последствия.

Объективная сторона преступного нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети состоит из общественно опасного деяния в виде действия или бездействия, наступивших последствий этого деяния, а также причинной связи между ними.

Действия или бездействия, составляющие объективную сторону состава рассматриваемого преступления выражаются в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети. Под такими правилами понимаются, во-первых, гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы[[83]](#footnote-83), во-вторых, техническая документация на приобретаемые компьютеры, в-третьих, конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка, в-четвертых, требования по сертификации компьютерных сетей и оборудования, в-пятых - должностные инструкции конкретных сотрудников, в-шестых, правила пользования компьютерными сетям.

Положение о сертификации средств защиты информации, утвержденное постановлением Правительства РФ от 26 июня 1995 г. № 608, устанавливает порядок сертификации средств защиты информации в Российской Федерации и ее учреждениях за рубежом. В соответствии с ним технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации являются средствами защиты информации. Указанные средства подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных Федеральным агентством правительственной связи и информации при Президенте Российской Федерации.

Системы сертификации (то есть совокупность участников сертификации, осуществляющих ее по установленным правилам) создаются Государственной технической комиссией при Президенте Российской Федерации, Федеральным агентством правительственной связи и информации при Президенте Российской Федерации, Федеральной службой безопасности Российской Федерации, Министерством обороны Российской Федерации, Службой внешней разведки Российской Федерации, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации.

Сертификация средств защиты информации осуществляется на основании требований государственных стандартов, нормативных документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах их компетенции. Координацию работ по организации сертификации средств защиты информации осуществляет межведомственная комиссия по защите государственной тайны (далее именуется - межведомственная комиссия). В каждой системе сертификации разрабатываются и согласовываются с межведомственной комиссией положение об этой системе сертификации, а также перечень средств защиты информации, подлежащих сертификации, и требования, которым эти средства должны удовлетворять.

Изготовители: производят (реализуют) средства защиты информации только при наличии сертификата; извещают орган по сертификации, проводивший сертификацию, об изменениях в технологии изготовления и конструкции (составе) сертифицированных средств защиты информации; маркируют сертифицированные средства защиты информации знаком соответствия в порядке, установленном для данной системы сертификации; указывают в сопроводительной технической документации сведения о сертификации и нормативных документах, которым средства защиты информации должны соответствовать, а также обеспечивают доведение этой информации до потребителя; применяют сертификат и знак соответствия, руководствуясь законодательством Российской Федерации и правилами, установленными для данной системы сертификации; обеспечивают соответствие средств защиты информации требованиям нормативных документов по защите информации; обеспечивают беспрепятственное выполнение своих полномочий должностными лицами органов, осуществляющих сертификацию, и контроль за сертифицированными средствами защиты информации; прекращают реализацию средств защиты информации при несоответствии их требованиям нормативных документов или по истечении срока действия сертификата, а также в случае приостановки действия сертификата или его отмены. Изготовители должны иметь лицензию на соответствующий вид деятельности.

Изготовитель для получения сертификата направляет в орган по сертификации средств защиты информации заявку на проведение сертификации, к которой могут быть приложены схема проведения сертификации, государственные стандарты и иные нормативные и методические документы, требованиям которых должны соответствовать сертифицируемые средства защиты информации. Орган по сертификации средств защиты информации в месячный срок после получения заявки направляет изготовителю решение о проведении сертификации с указанием схемы ее проведения, испытательной лаборатории, осуществляющей испытания средств защиты информации, и нормативных документов, требованиям которых должны соответствовать сертифицируемые средства защиты информации, а при необходимости - решение о проведении и сроках предварительной проверки производства средств защиты информации. Для признания зарубежного сертификата изготовитель направляет его копию и заявку на признание сертификата в федеральный орган по сертификации, который извещает изготовителя о признании сертификата или необходимости проведения сертификационных испытаний в срок не позднее одного месяца после получения указанных документов. В случае признания зарубежного сертификата федеральный орган по сертификации оформляет и выдает изготовителю сертификат соответствия установленного образца. Сертификация импортируемых средств защиты информации проводится по тем же правилам, что и отечественных.

Основными схемами проведения сертификации средств защиты информации являются: для единичных образцов средств защиты информации - проведение испытаний этих образцов на соответствие Фебованиям по защите информации; для серийного производства средств защиты информации - проведение типовых испытаний образцов средств защиты информации на соответствие требованиям по защите информации и последующий инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации, определяющих выполнение этих требований. Кроме того, допускается предварительная проверка производства по специально разработанной программе.

Срок действия сертификата не может превышать пяти лет.

Представляет практический интерес вопрос о том, будет ли наступать уголовная ответственность за нарушение правил пользования глобальными сетями, например сетью Интернет. Представляется, что на данный вопрос следует ответить положительно.

Сеть Интернет представляет собой глобальное объединение компью-терных сетей и информационных ресурсов, принадлежащих множеству различных людей и организаций. Это объединение является децентрализованным, и единого общеобязательного свода правил (законов) пользования сетью Интернет не установлено. Существуют, однако, общепринятые нормы работы в сети Интернет, направленные на то, чтобы деятельность каждого пользователя сети не мешала работе других пользователей. Фундаментальное положение этих норм таково: правила использования любых ресурсов сети Интернет (от почтового ящика до канала связи) определяют владельцы этих ресурсов, и только они.

Развитие Сети привело к тому, что одной из основных проблем пользователей стал избыток информации. Поэтому сетевое сообщество выработало специальные правила, направленные на ограждение пользователя от ненужной (незапрошенной) информации (спама). В частности, являются недопустимыми:

1.Массовая рассылка не согласованных предварительно электронных писем (mass mailing). Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю.

Здесь и далее под электронными письмами понимаются сообщения электронной почты, ICQ и других подобных средств личного обмена информацией.

2.Несогласованная отправка электронных писем объемом более одной границы или содержащих вложенные файлы.

3.Несогласованная рассылка электронных писем рекламного, коммерческого или агитационного характера, а также писем, содержащих грубые и оскорбительные выражения и предложения.

1. Размещение в любой конференции Usenet или другой конференции, форуме или электронном списке рассылки статей, которые не соответствуют тематике данной конференции или списка рассылки (off-topic). Здесь и далее под конференцией понимаются телеконференции (группы новостей) Usenet и другие конференции, форумы и электронные списки рассылки.
2. Размещение в любой конференции сообщений рекламного, коммерческого или агитационного характера, кроме случаев, когда такие сообщения явно разрешены правилами такой конференции либо их размещение было согласовано с владельцами или администраторами такой конференции предварительно.
3. Размещение в любой конференции статьи, содержащей приложенные файлы, кроме случаев, когда вложения явно разрешены правилами такой конференции либо такое размещение было согласовано с владельцами или администраторами такой конференции предварительно.
4. Рассылка информации получателям, высказавшим ранее явное нежелание получать эту информацию.
5. Использование собственных или предоставленных информационных ресурсов (почтовых ящиков, адресов электронной почты, страниц WWW и т.д.) в качестве контактных координат при совершении любого из вышеописанных действий вне зависимости от того, из какой точки Сети были совершены эти действия.

Не допускается осуществление попыток несанкционированного доступа к ресурсам Сети, проведение или участие в сетевых атаках и сетевом взломе за исключением случаев, когда атака на сетевой ресурс проводится с явного разрешения владельца или администратора этого ресурса. В том числе запрещены:

1. Действия, направленные на нарушение нормального функционирования элементов Сети (компьютеров, другого оборудования или программного обеспечения), не принадлежащих пользователю.
2. Действия, направленные на получение несанкционированного доступа, в том числе привилегированного, к ресурсу Сети (компьютеру, другому оборудованию или информационному ресурсу), последующее использование такого доступа, а также уничтожение или модификация программного обеспечения или данных, не принадлежащих пользователю, без согласования с владельцами этого программного обеспечения или данных либо администраторами настоящего информационного ресурса.
3. Передача компьютерам или оборудованию Сети бессмысленной или бесполезной информации, создающей паразитную нагрузку на эти компьютеры или оборудование, а также промежуточные участки сети, в объемах, превышающих минимально необходимые для проверки связности сети и доступности отдельных ее элементов.

Помимо вышеперечисленного, владелец любого информационного или технического ресурса Сети может установить для этого ресурса собственные правила его использования.

Правила использования ресурсов либо ссылка на них публикуются владельцами или администраторами этих ресурсов в точке подключения к таким ресурсам и являются обязательными к исполнению всеми пользователями этих ресурсов. Пользователь обязан соблюдать правила использования ресурса либо немедленно отказаться от его использования.

Значительная часть ресурсов Сети не требует идентификации пользователя и допускает анонимное использование. Однако в ряде случаев от пользователя требуется предоставить информацию, идентифицирующую его и используемые им средства доступа к Сети. При этом пользователю запрещается:

1. Использование идентификационных данных (имен, адресов, телефонов и т.п.) третьих лиц, кроме случаев, когда эти лица уполномочили пользователя на такое использование. В то же время пользователь должен принять меры по предотвращению использования ресурсов Сети третьими лицами от его имени (обеспечить сохранность паролей и прочих кодов авторизованного доступа).
2. Фальсификация своего IP-адреса, а также адресов, используемых в других сетевых протоколах, при передаче данных в Сеть.
3. Использование несуществующих обратных адресов при отправке электронных писем.

При работе в сети Интернет пользователь становится ее полноправным участником, что создает потенциальную возможность для использования сетевых ресурсов, принадлежащих пользователю, третьими лицами. В связи с этим пользователь должен принять надлежащие меры по такой настройке ресурсов, которая препятствовала бы недобросовестному использованию этих ресурсов третьими лицами, а также оперативно реагировать при обнаружении случаев такого использования.

Примерами потенциально проблемной настройки сетевых ресурсов понимаются:

1. открытый ретранслятор электронной почты (SMTP-relay);
2. общедоступные для неавторизованной публикации серверы новостей
(конференций, трупп);
3. средства, позволяющие третьим лицам неавторизованно скрыть источник соединения (открытые прокси-серверы и т.п.);
4. общедоступные широковещательные адреса локальных сетей;
5. электронные списки рассылки с недостаточной авторизацией подписки
или без возможности ее отмены.

Таким образом, нарушения правил эксплуатации ЭВМ могут быть подразделены на физические (неправильное подключение периферийного оборудования, отсутствие устройств бесперебойного питания, нарушение типового режима в помещении, неправильное подключение ЭВМ к источникам питания, нерегулярное техническое обслуживание, использование несертифицированных средств защиты и самодельных узлов и приборов и пр.) и интеллектуальные (невыполнение процедуры резервного копирования, несанкционированная замена программного обеспечения, параметров настройки системы ЭВМ или компьютерной сети и пр.).

При этом вряд ли можно согласиться с точкой зрения Ю.И. Ляпунова и B.C. Максимова, отмечавших что «поскольку речь идет о правилах эксплуатации именно ЭВМ, т.е. аппаратно-технической структуры, то и нарушение их должно затрагивать только техническую сторону несоблюдения требований безопасности компьютерной информации, а не организационную или правовую. К таковымможно отнести: блокировку системы защиты от несанкционированного доступа, нарушение правил электро- и противо-пожарной 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»[[84]](#footnote-84). Представляется, что пренебрежение организационными мерами защиты компьютерной информации (предоставление посторонним лицам доступа в служебное помещение, несанкционированное разглашение сетевого имени и пароля законного пользователя, уже упомянутое невыполнение процедуры резервного копирования и пр.) также составляют деяния, подпадающие под запрет, установленный диспозицией ст. 274 УК РФ.

Следующим элементом объективной стороны состава преступления, предусмотренного ст. 274 УК РФ являются вредоносные последствия. Их законодатель предусмотрел в виде уничтожения, блокирования или модификации охраняемой законом компьютерной информации, если это деяние повлекло существенный вред (ч. 1 ст. 274) или повлекло по неосторожности тяжкие последствия (ч.2 ст. 274).

Под уничтожением информации следует понимать такое изменение ее первоначального состояния (полное либо частичное удаление информации с машинных носителей), при котором она перестает существовать в силу утраты основных качественных признаков. При этом не имеет значения, имелась ли у потерпевшего копия уничтоженной виновным информации или нет.

Блокирование компьютерной информации представляет собой закрытие информации, характеризующееся недоступностью ее использования по прямому назначению со стороны законного пользователя, собственника или владельца.

Модификация заключается в изменении первоначального состояния информации (например, реструктурирование или реорганизация базы данных, удаление или добавление записей, содержащихся в ее файлах, перевод программы для ЭВМ или базы данных с одного языка на другой), не меняющей сущности объекта.

Третьим необходимым признаком объективной стороны нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети является причинная связь между противозаконными действиями виновного и наступившими вредными последствиями. Ответственность по ст.273 УК РФ наступает только в том случае, если преступные последствия, альтернативно отраженные в ее диспозиции, явились именно необходимым следствием, закономерно вызванным неправомерным доступом лица к охраняемой законом компьютерной информации, а не наступили в силу иных причин.

Под существенным вредом в ст. 274 УК РФ понимаются утрата важной и информации, перебои в производственной деятельности, необходимость сложного или длительного ремонта средств вычислительной техники, их переналадки, длительный разрыв связи между ЭВМ, объединенных в компьютерную сеть*,* причинение значительного материального ущерба законному пользователю или владельцу информации, причинение морального вреда личности путем разглашения сведений конфиден-циального характера, составляющих личную, семейную, нотариальную, адвокатскую, врачебную тайну. Данное понятие является оценочным и определение объема причиненного собственнику информационной системы вреда в результате нарушения правил эксплуатации ЭВМ должно осуществляться с учетом совокупности всех полученных данных.

Под указанными в ч. 2 ст. 274 УК РФ тяжкими последствиями (квалифицирующий признак) нарушения правил эксплуатации ЭВМ понимается безвозвратная утрата особо ценной информации, выход из строя нужных технических средств (в том числе оборонного значения, навигационной техники), повлекшие аварии, катастрофы, гибель июлей.

Субъективную сторонупреступления, предусмотренного ч. 1 ст. 274 VK РФ составляет вина в виде прямого или косвенного умысла. Мотив и цепь нарушения правил эксплуатации ЭВМ имеют факультативное течение.

Преступление, предусмотренное ч. 2 ст. 274, совершается с двойной формой вины: умышленной (в виде прямого или косвенного умысла) по отношению к нарушению правил эксплуатации ЭВМ, их системы или мчи, и неосторожной по отношению к наступившим тяжким последствиями.

Субъектанализируемого преступления - специальный. Им может быть*,* любое физическое вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста, которое в силу характера выполняемой трудовой, профессиональной или иной деятельности, имеет беспрепятственный доступ к ЭВМ, их системе или сети, на которое в силу закона, иного нормативного акта возложена обязанность соблюдения правил эксплуатации ЭВМ. Закон не требует, чтобы это лицо занимало определенную должность, занималось определенной деятельностью, получило определенное образование. Главное, чтобы оно имело доступ к ЭВМ.

# ГЛАВА 3. ОСОБЕННОСТИ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ СОВЕРШАЕМЫХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

# 3.1 Квалификация преступлений в сфере компьютерной информации, совершенных группой лиц по предварительному сговору и организованной группой

Одним из квалифицирующих признаков состава преступления, предусматривающего ответственность за неправомерный доступ к компьютерной информации является совершение этого преступления группой лиц по предварительному сговору.

Совершение преступления группой лиц по предварительному сговору -это совершение его двумя или более лицами, заранее договорившимися о совместном совершении преступления (ч. 2 ст. 35 УК РФ). Применительно к несанкционированному доступу к компьютерной информации совершение преступления группой лиц должно выражаться в совместном участии нескольких лиц в совершении деяния, запрещенного ст. 272 УК РФ. Каждый участник группы должен полностью или частично выполнять действия, образующие объективную сторону состава рассматриваемого преступления.

Для неправомерного доступа к охраняемой законом компьютерной информации уголовным законом не предусмотрено такого квалифицирующего признака, как совершение деяния простой группой (т. е. без предварительной договоренности), что скорее всего обусловлено такой степенью общественной опасности этого вида соучастия, которая не позволяет выделять его в качестве квалифицирующего обстоятельства. Несмотря на это обстоятельство, совершение неправомерного доступа группой лиц возможно и без предварительного сговора между соучастниками, хотя надо признать, что встречается это крайне редко[[85]](#footnote-85).

Особенность соучастия в преступлении без предварительного сговора заключается в том, что соглашение о совместном участии в посягательстве достигается после начала выполнения объективной стороны, т.е. на стадии покушения на преступление. Такого рода соисполнительство при совершении анализируемого деяния имеет место в том случае, когда оно начинается одним лицом, а затем уже в процессе неправомерного доступа к компьютерной информации к его действиям присоединяется другое лицо, пожелавшее участвовать в совершении начатого преступления. В этом случае имеет место не простое совпадение действий виновных во времени и пространстве, - преступление совершается сообща, путем объединения усилий для достижения единого, общего для всех соучастников преступного результата.

Действия соисполнителей неправомерного доступа к компьютерной информации, объединенных между собой без предварительного сговора, не образуют признаков, характерных для квалифицированного состава этого преступления и, следовательно, уголовная ответственность за их совершение должна наступать по ч. 1 ст. 272 УК.

Для оценки деяния, ответственность за которое предусмотрена ст. 272 УК, как совершенного группой лиц по предварительному сговору, в каждом конкретном случае необходимо установить, что договоренность о совместном совершении преступления будущими соисполнителями была достигнута до непосредственного осуществления действий, образующих объективную сторону состава этого преступления. При этом промежуток времени между сговором и началом совершения конкретных общественно опасных действий не имеет решающего значения. Сговор может иметь место задолго до совершения таких действий, либо непосредственно перед началом по смыслу закона, достижение соглашения на совершение подобных действий следует отождествлять со стадией приготовления к неправомерному доступу к компьютерной информации.

Дискуссионным является вопрос о том, должны ли все участники неправомерного доступа, совершаемого по предварительному сговору группой лиц, быть исполнителями (соисполнителями) этого преступления[[86]](#footnote-86). Полагаем, что ответ на него должен быть только утвердительным, несмотря на то, что ч. 2 ст. 35 УК РФ непосредственно не характеризует участников данного вида группового преступления как исполнителей (соисполнителей). В связи с этим следует согласиться с аргументом B.C. Комиссарова, который, отстаивая аналогичную заявленной нами точку зрения, утверждает, что в случаях, когда группа лиц по предварительному сговору предусматривается в Особенной части УК как квалифицирующий признак, она должна состоять только из соисполнителей[[87]](#footnote-87). Подобное понимание соисполнительства при совершении преступления вытекает и из систематического толкования норм Общей части уголовного закона, которыми установлены признаки соучастия. Если признать пособника или подстрекателя участником преступной группы, образованной по предварительному сговору, законодательное обособление сложного соучастия с распределением ролей теряло бы смысл[[88]](#footnote-88). Такую точку зрения занимают и авторы, подготовившие монографию о расследовании неправомерного доступа к компьютерной информации[[89]](#footnote-89).

Это не означает, что между соучастниками квалифицированного неправомерного доступа вообще не может быть распределения ролевых функций. Соисполнительство не исключает распределения исполнительских функций между участниками, не влияющего на квалификацию содеянного[[90]](#footnote-90). Действия соисполнителей квалифицируются без ссылки на ст. 33 УК РФ.

При совершении неправомерного доступа к компьютерной информации группой лиц по предварительному сговору распределение ролевых функций между различными соучастниками также сводится к совершению действий, которые состоят в частичном выполнении объективной стороны состава этого преступления и не содержат признаков материального пособничества или иной формы сложного соучастия. Например, один из соучастников "взламывает" закрытую компьютерную сеть и передает управление тому лицу, которое произведет поиск и уничтожение (либо блокирование, копирование, модификацию) интересующей виновных информации. Подобные ситуации могут возникать при неправомерном доступе в компьютерные сети банков, с последующим несанкционированным перечислением денежных средств. Одни лица занимаются взломом защиты компьютерной сети банка, а другие - внесением изменений в бухгалтерскую информацию.

Лица, непосредственно не участвовавшие в совершении неправомерного доступа, а исполнявшие роль организатора, подстрекателя или пособника, должны нести ответственность по соответствующей части ст. 33 УК РФ и ст. 272 УК РФ.

Деятельность двух или более лиц по совершению данного преступления не может быть признана групповой, в смысле квалифицирующего признака неправомерного доступа к компьютерной информации, если одно лицо выступает в качестве подстрекателя, а другое - непосредственного исполнителя, т.к. участники этой группы не являются соисполнителями. Действия исполнителя в данном случае должны квалифицироваться по ч. 1 ст. 272 УК так как исполнитель, подстрекатель же должен отвечать по ч. 1 ст. 272 УК РФ со ссылкой на ч. 4 ст. 33 УК РФ (подстрекатель).

Если лицо сообщает виновному пароль доступа к информации, то его действия должны быть квалифицированны по ч. 1 ст. 272 со ссылкой на ч. 5 ст. 33 УК (пособник).

На практике имели место случаи, когда при осуществлении неправомерного доступа осуществлялось чисто техническое распределение ролей, т.е. действия некоторых участников по своим внешним чертам соответствовали признакам пособничества. Эти действия выполнялись одновременно с осуществлением неправомерного доступа к компьютерной информации. Так, сотрудник коммерческого банка, вступив в преступный сговор с другим лицом, в заранее обусловленное время блокирует систему защиты с тем, что бы его соучастник проник в компьютерную сеть банка. При рассмотрении этой ситуации необходимо иметь в виду, что при совершении конкретного преступления в пределах объективной стороны внутри группы лиц по предварительному сговору вполне возможно "техническое" распределение ролей, не влияющее на квалификацию[[91]](#footnote-91). То же самое можно сказать и о неправомерном доступе к компьютерной информации. Распределение ролей при совершении этого преступления может быть связано с технологией выполнения действий, образующих его объективную сторону, что не влияет на квалификацию деяния (так же, как не влияет на квалификацию действий соисполнителей при совершении групповой кражи распределение между ними различных ролевых функций, ни одна из которых не содержит признаков материального пособничества или какой-либо другой формы сложного соучастия (взлом помещения, изъятие имущества, обеспечение тайности изъятия имущества и т. п.)[[92]](#footnote-92).

При совершении рассматриваемого преступления группой лиц по предварительному сговору распределение ролевых функций между различными соучастниками также сводится к совершению действий, которые состоят в частичном выполнении объективной стороны состава этого преступления и не содержат признаков материального пособничества или иной формы сложного соучастия. В данном случае имеет место соисполнительство с распределением ролей, если виновные объединены предварительной договоренностью на совершение неправомерного доступа к защищаемой законом компьютерной информации.

Для признания неправомерного доступа к компьютерной информации совершенным по предварительному сговору группой лиц, не требуется, чтобы все соисполнители в полном объеме принимали участие в совершении этого преступления. Для признания участника такой группы соисполнителем преступления, ответственность за которое предусмотрена ч. 2 ст. 272 УК РФ, достаточно совершения им действия, которое непосредственно направлено на достижение общего преступного результата. Например, одно лицо "взламывает" защиту информации, а другое выполняет какие либо манипуляции с ней (уничтожает, блокирует, модифицирует или копирует), либо первый соучастник начинает уничтожение информации, а второй его заканчивает. Важным в данном случае является лишь наличие предварительного сговора о совершении этого деяния до момента выполнения объективной стороны преступления.

Особого внимания заслуживает вопрос об участии в групповом совершении неправомерного доступа к компьютерной информации двух лиц, если одно из них во время совершения преступного деяния не отвечает признакам субъекта преступления (вменяемость, возраст уголовной ответственности).

Одни авторы полагают, что действия лица, соответствующего признакам субъекта, участвовавшего вместе с подростком в совершении преступления, предусмотренного ст. 272 УК, образуют групповой способ посягательства только в том случае, если подросток обладал общими признаками субъекта лицо, достигшее шестнадцатилетнего возраста выступает в качестве единственного исполнителя этого деяния и квалификации по ч. 2 ст. 272 УК РФ не требуется[[93]](#footnote-93). Другие авторы вкладывают в понятие "группа" не только юридический, но и социальный смысл[[94]](#footnote-94). С данной позицией трудно согласиться, так как в Постановление Пленума Верховного Суда РФ от 27 декабря 2002 года № 29 «О судебной практике по делам о краже, грабеже и разбое» прямо указано об отсутствии группы в случае если один из соучастников не является субъектом преступления, без учета его группового способа.[[95]](#footnote-95).

Нам представляется, что более объективным было бы решение данного вопроса с учетом значимости участия лица, не подпадающего под признаки субъекта, в достижении совместного преступного результата. Так, если участие лица в выполнении объективной стороны преступления оказывало существенное влияние на достижение результатов преступления, то вполне логичным было бы квалифицировать деяние виновного, соответствующего признакам субъекта, как совершенное в составе группы лиц. Если же участие лица, не достигшего возраста уголовной ответственности являлось не существенным (при совершении неправомерного доступа это лицо занималось лишь разархивацией данных), то полагаем, что нет необходимости в квалификации деяния, совершенного взрослым участником группы по ч. 2 ст. 272 УК. Здесь достаточно будет квалифицировать содеянное по ч. 1 ст. 272 УК и ст. 150 УК (вовлечение несовершеннолетнего в совершение преступления).

Степень значимости участия в совершении преступления должна определяться в зависимости от всех обстоятельств дела, в том числе от обстановки, места совершения преступления, технической оснащенности, профессиональной подготовленности лица, особенностей неправомерного доступа к компьютерной информации в каждом конкретном случае[[96]](#footnote-96).

Вызывает сложность представляет определение системы признаков организованной группы применительно к неправомерному доступу к компьютерной информации (ч. 2 ст. 272 УК РФ). В ст. 35 УК РФ установлено, что преступление признается совершенным организованной группой, если оно совершено устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений. Таким образом, уголовный закон определяет только два признака организованной группы: устойчивость и особую цель ее образования (совершение одного или нескольких преступлений), что не дает достаточно четкого представления о ее отличии от группы лиц, действующих по предварительному сговору.

В практике высших судебных органов неоднократно предпринимались попытки дать разъяснение признаков организованной группы, которое позволило бы более четко отграничить таковую от других объединений. Так, пленум Верховного Суда РФ в Постановлении от 10 февраля 2000 г. № 6 "О судебной практике по делам о взяточничестве и коммерческом подкупе"[[97]](#footnote-97) определил, что организованная группа отличается высокой степенью организованности, распределением ролей, а также наличием организатора. В руководящих постановлениях Верховный Суд РФ также разъяснял признаки организованной группы, указывая на то, что ее отличительной чертой является тщательная подготовка и планирование преступления, распределение ролей между соучастниками и т. п.[[98]](#footnote-98), а также стабильность состава, тесная связь между ее членами, согласованность их действий, постоянство форм и методов преступной деятельности, длительность ее осуществления и количество совершенных преступлений[[99]](#footnote-99).

Однако следует согласиться с мнением тех ученых, которые утверждают, что содержание такого признака организованной группы, как устойчивость, не может интерпретироваться однозначно, а поэтому он не вносит ясности в понятие этого вида преступного объединения[[100]](#footnote-100). Хотя некоторыми авторы делают попытку разобраться в этом понятии и предлагают под признаком устойчивости подразумевать умысел соучастников на совершение нескольких преступлений или даже одного, но требующего тщательного планирования совместных действий, распределения ролей между участниками, оснащения их орудиями, средствами, техникой, а равно наличия организатора или руководителя группы[[101]](#footnote-101). Полагаем, что данное разъяснение также не дает четкого представления об устойчивости организованной группы.

Содержание системы признаков организованной группы, достаточного представления о данном виде криминального сотрудничества ни в теории уголовного права, ни на практике применения уголовного закона не сложилось.

Исходя из современных научных представлений о данной форме преступных объединений и руководящих разъяснений высших судебных органов РФ, нам представляется возможным выделить отдельные признаки совершения неправомерного доступа к охраняемой законом информации организованной группой. Такая группа должна отличаться наличием организатора или руководителя. Именно организатор, как справедливо отмечают Л.Д. Гаухман и С.В. Максимов, создает группу, осуществляет подбор соучастников, распределяет роли между ними, устанавливает дисциплину и т.п., а руководитель обеспечивает целенаправленную, спланированную и слаженную деятельность как группы в целом, так и каждого ее участника[[102]](#footnote-102).

В организованную группу могут входить лица, выполняющие управленческие функции в коммерческих или иных организациях, а также должностные лица, равно как и иные служащие. Участие таковых в организованной группе может заметно облегчить подготовку и совершение неправомерного доступа к компьютерной информации, а также сокрытие этого преступления. При этом использование ими своего служебного положения в целях непосредственного совершения этого преступления либо в целях содействия другим участникам организованной группы в совершении неправомерного доступа должно учитываться при назначении им наказания.

В отличие от участников преступной группы лиц, действующей по предварительному сговору, отдельные участники организованной группы могут быть не только соисполнителями преступления, но и выполнять функции организатора либо пособника. Согласно разъяснениям Пленума Верховного Суда РФ, их действия должны квалифицироваться как соисполнительство при совершении преступления организованной группой (по ч. 2 ст. 272 УК РФ) без ссылки на ст. 33 У К РФ. Однако при совершении неправомерного доступа к компьютерной информации организованной группой, как и при совершении других преступлений в соучастии указанного вида, все же возможно и сложное соучастие. Например, когда лицо, не являющееся участником организованной группы, выступает пособником совершения такого деяния, в частности, оказывая помощь участникам организованной группы путем предоставления необходимой для совершения преступления информации.

# 3.2 Совершенствование мер уголовного - правовой борьбы с преступлениями в сфере компьютерной информации

Человечество вступило в новую эпоху - эпоху информационного общества. Информационные технологии - принципиально новый инструмент, одновременно и созидательный, и разрушительный. Вместе со стремительным ростом числа персональных компьютеров и пользователей глобальной сети Интернет (только за период 1998-2005 гг. число пользователей сети возросло со 143 миллионов человек до 2 милиардов) растет и количество преступлений, совершаемых с использованием вычислительной техники (компьютерных технологий)[[103]](#footnote-103).

Информационные отношения в целом достаточно успешно регулируются российским законодательством. Серьезной проблемой остается, на наш взгляд, именно криминализация деяний, сопряженных с компьютерными технологиями. Введение в УК РФ гл. 28 - Преступления в сфере компьютерной информации, по нашему мнению, проблемы не снимает, появляется лишь видимость ее решения. Данная глава, на наш взгляд, крайне несовершенная, а главное - в ней идет речь о преступлениях, совершаемых в отношении средств компьютерной техники и информации, но не преступлений, совершаемых с их использованием[[104]](#footnote-104).

Следует отметить, что именно такой подход складывался во время обсуждения проекта Закона РСФСР "Об ответственности за правонарушения при работе с информацией"[[105]](#footnote-105), где речь с самого начала шла о правонарушениях, объектом которых являлись информационные системы и информация как таковая.

Из-за своей специфической природы и повышенной социальной опасности компьютерные преступления практически с момента своего появления анализировались криминологами, криминалистами и специалистами в области компьютеров с различных точек зрения, однако до сих пор не выработано единого взгляда на данный вид преступлений.

Условно точки зрения специалистов в данной области можно разделить на две группы:

1. Компьютерные преступления представляют собой самостоятельный вид преступной деятельности.

2. Компьютерных преступлений как самостоятельного вида нн существует, их следует рассматривать лишь как квалифицирующий признак обычных, "традиционных" преступлений.

Предлагается также к этой группе неосновательно широкое понятие компьютерных преступлений, относящие любые посягательства на связи и отношения людей, опосредующие применение и использование компьютерной техники[[106]](#footnote-106).

Первый же - совершенно очевиден, общедоступен и, именно из-за этого, широко применяется в мировой практике. Наиболее яркими примерами последних законодательных актов такого рода можно назвать британский "Закон о терроризме" от 2000 г. и новый антитеррористический закон США, известный как "Акт 2001 г.". Этим законом Конгресс ввел в оборот новые понятия, расширяющие трактовку термина "терроризм", создав новое законодательное понятие "кибертерроризм" (ст. 814)[[107]](#footnote-107).

Нам представляется более целесообразным второе направление, точнее, два взаимосвязанных и взаимодополняющих подхода, позволяющих произвести определенную корректировку УК без его коренного пересмотра.

Во-первых, следует трактовать содержащиеся в уголовном законе термины и понятия в соответствии с определениями, закрепленными в ряде федеральных законов РФ

Во-вторых, расширить в ряде случаев квалифицирующие признаки преступлений, путем включения в них определения "с использованием современных компьютерных технологий" (в тех случаях, когда их применение явно повышает опасность конкретного вида преступления).

По нашему мнению необходимо внести в Уголовный кодекс дополнения и комментарии.

Начнем с гл. 17 - Преступление против свободы чести и достоинства личности.

Статья 129-Клевета. Разве неочевидно, что клевета, "выпущенная" в Интернет, несравненно более опасна, чем опубликованная в "самых массовых" СМИ и соответственно должна наказываться более жестко. То же можно отнести и к ст. 130-Оскорбление. Следовательно, можно предложить добавить в ч. 2 ст.ст. 129-130 следующую формулировку: "а также распространение в сети Интернет и других глобальных сетях".

Глава 13 - Преступления против конституционных прав и свобод человека и гражданина. Ст. 137 - нарушение неприкосновенности частной жизни - безусловно требует дополнительной квалификации: "с использованием современных компьютерных технологий". Положение ст. 140 - отказ в предоставлении гражданину информации - должно распространяться и на информацию, хранящуюся в автоматизированных базах и банках данных.

Особого внимания заслуживает ст. 144 - воспрепятствование осуществлению избирательных прав или работе избирательных комиссий. С учетом существования и функционирования Государственной автоматизированной системы (ГАС) "Выборы"[[108]](#footnote-108) в ч. 2 целесообразно включить п. "г": "совершенные с вмешательством в функционирование автоматизированной системы "Выборы", в т. ч. путем ввода недостоверных данных или фальсификации результатов". Вмешательство в программы системы (модификация) регулируется ст. 272 УК РФ. Все сказанное относится и к ст. 142 - фальсификация избирательных документов. Что касается ст. 146 - Нарушение авторских и смежных прав, то ее положения должны, по нашему мнению, распространяться на произведения, хранящиеся в цифровой (компьютерной) форме, что следует указать в соответствующем комментарии. То же относится кет. 147 - Нарушение изобретательских и патентных прав[[109]](#footnote-109).

В гл. 20 - Преступление против семьи и несовершеннолетних - ст. 155 - Разглашение тайны усыновления (удочерения) - следует дополнительно квалифицировать по аналогии с клеветой, оскорблением и т.п.

Особого внимания требует рассмотрение гл. 21 - Преступления против собственности. В данном случае возможны два подхода, во-первых, дополнение данной главы новой статьей, предусматривающей ответственность за хищение, где применение компьютерных технологий выступает в качестве способа совершения. Вторым путем, на наш взгляд, более предпочтительным является оценка ряда преступлений данной главы по совокупности преступлений. Так, с учетом того факта, что Закон "Об информации..." определяет понятие собственника информации, а объективной стороной хищения является посягательство на отношение собственности, можно полагать незаконное копирование информации одним из видов кражи и квалифицировать это преступление по совокупности ст.ст. 158 и 272.

В частности, такая квалификация может оказаться полезной в тех случаях, когда информация не подпадает под категорию охраняемой законом и, следовательно, не может быть квалифицирована по ст. 272, но является собственностью юридического или физического лица, на создание и накопление которого затрачены определенные финансовые и прочие ресурсы. Хищение (кража, незаконное копирование) такой информации наносит реальный материальный ущерб ее собственнику или владельцу.

Статью 159 - Мошенничество - следует расширить, указав "в том числе с использованием компьютерных технологий". Аналогично можно трактовать ст. 160 - присвоение или растрата.

Точно так же может совершаться преступление, предусмотренное ст. 163, - вымогательство, которое может совершаться с использованием компьютерных технологий. Например, с угрозой уничтожения, повреждения или блокирования информации (ст. 272), или угрозой разглашения информации, добытой из автоматизированных банков данных (ст. 272 - копирование).

Статья 165- Причинение имущественного ущерба путем обмана или злоупотребление доверием, также требует в ч. 3 дополнения "совершенное с использованием компьютерных технологий".

Также по совокупности обстоятельств могут квалифицироваться умышленное (ст. 167) или неосторожное (ст. 168) уничтожение или повреждение имущества в тех случаях, когда объектом преступления была компьютерная информация. То есть ст. 272 - Уничтожение информации и, соответственно, ст.ст. 167-168.

Особый интерес представляет для нас гл. 22 - Преступления в сфере экономической деятельности, в частности, ст. 171 (незаконное предпринимательство). 172 (незаконная банковская деятельность), 173 (лжепредпринимательство), 174 (легализация денежных средств, приобретенных незаконным путем) Общеизвестно, что в настоящее время подобные преступления, как правило, совершаются путем фальсификации компьютерной информации.

Отсюда следуют два вывода.

Во-первых, преступления, совершенные по указанным статьям, в случае применения при этом компьютерных технологий должны квалифицироваться по совокупности соответствующих статей и ст. 272 (модификация).

Во-вторых, "использование компьютерных технологий" может быть в таком случае квалифицирующим признаком, так как в этом случае увеличивается опасность преступного деяния.

"Применение компьютерных технологий" может, на наш взгляд, являться отягчающим обстоятельством при совершении преступления, предусмотренного ст. ст. 183 разглашении сведений, составляющих коммерческую или банковскую тайну.

Статьи 186 (Изготовление или сбыт поддельных денег или ценных бумаг) и 187 (Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов), на наш взгляд, не требуют особой квалификации, так как способ изготовления не является для них квалифицирующим признаком. Следует все же отметить, что судебная практика отмечает все возрастающую роль компьютерных технологий в указанных деяниях.

Глава 24 - Преступление против общественной безопасности.

Статья 205 - Терроризм - Вполне достаточно дополнить ст. 205 ч. 2 пунктом "г": "с применением современных компьютерных технологий". Для ст. 207 - Заведомо ложное сообщение об акте терроризма - возможно, было бы целесообразным внесение дополнения о применении для этих целей информационных технологий (компьютерных сетей).

Трудно впрямую отнести к ст. 223 (Незаконное изготовление оружия) советы, чертежи, рекомендации по его изготовлению, размещаемые на некоторых сайтах Сети, но какой-то правовой оценки такие действия явно требуют. Это же относится к ст. 228 (Незаконное изготовление, приобретение, хранение, перевозка, пересылка либо сбыт наркотических средств или психотропных веществ) гл. 25. Следует отметить, что российским уголовным законодательством в сфере преступления против здоровья никаким образом не предусмотрена ответственность за такие деяния, связанные с использованием компьютерных технологий, которые могут повлечь человеческие жертвы. Между тем, зарубежные законодатели такие ситуации в настоящее время предусматривают. Безусловно, следует включить квалифицирующий признак "в том числе с использованием компьютерных технологий" в ст. 242 - Незаконное распространение порнографических материалов и предметов.

Глава 29 - Преступление против основ конституционного строя и безопасности государства.

Рассмотрим "информационный" подход к статьям данной главы на примере ст. 284 - Утрата документов, содержащих государственную тайну. Было бы целесообразным включить квалифицирующий признак "совершенное с использованием компьютерных технологий" в ст. 292 (Служебный подлог) гл. 30 (Преступление против государственной власти), в ст. 298 (Клевета в отношении судьи, присяжного заседателя, прокурора ...) гл. 31 (Преступления против правосудия).

Особого внимания требует ст. 303 (Фальсификация доказательств), так как цифровые технологии в принципе позволяют фальсифицировать не только письменные документы, но и звук, изображение и т.д.

Многократно указанный выше квалифицирующий признак можно, по нашему мнению, также отнести к ст. 327 гл. 32; ст. 354 гл. 34 и пр.

В заключение следует еще раз подчеркнуть, что существуют весьма специфические компьютерные преступления, которые вообще не нашли своего отражения в Уголовном кодексе. В частности, и это отражено в Концепции российского законодательства, в сфере обеспечения безопасности информации[[110]](#footnote-110), в качестве объектов должны рассматриваться не только право личности на доступ к информации, и право неприкосновенности частной жизни, но и защита человека и общества от "вредной" информации.

Резюмируя изложенное, можно сделать следующие выводы:

уголовно-правовое регулирование в сфере преступлений, сопряженных с компьютерными технологиями, не в полной мере соответствует реальной ситуации;

целый ряд реально существующих (или - возможных в ближайшей перспективе) преступных деяний невозможно квалифицировать по имеющемуся УК;

оптимальным путем устранения отмеченных пробелов является введение в ряд статей существующего УК дополнений, квалифицирующих отдельные деяния, и соответствующая интерпретация (применительно к компьютерным технологиям) ряда терминов и понятий, употребляющихся в "традиционном" смысле;

в отдельных случаях - при отсутствии в действующем УК принципиально новых составов, присущих только компьютерным технологиям, - разработка и введение новых норм, предусматривающих уголовную ответственность за деяния такого рода.

# ЗАКЛЮЧЕНИЕ

Современный этап характеризуется устойчивой тенденцией роста компьютерных преступлений, как в России, так и во всем мировом информационном пространстве.

Главным этапом в криминализации компьютерных преступлений стало принятие нового Уголовного кодекса РФ, в котором 28 глава содержит три статьи (272-274 УК РФ), предусматривающие уголовную ответственность за преступления в сфере компьютерной информации.

1. Сравнивая позиции различных ученых-правоведов, было сформулировано свое понятие **преступления в сфере компьютерной информации** - предусмотренное уголовным законом, противоправное, виновное нарушение чужих прав и интересов, связанное с использованием, модификацией, уничтожением компьютерной информации, причинившее вред либо создавшее угрозу причинения вреда охраняемым законом правам и интересам физических и юридических лиц, общества и государства.

2. В определении предмета преступлений в сфере компьютерной информации мы придерживаемся той точки зрения, что предметом компьютерных преступлений может быть только компьютерная информация.

3. Критерием разграничения между предметом, орудием и средством совершения преступлений в сфере компьютерной информации является характер использования предметов в процессе совершения преступления.

Следует различать компьютерную информацию, на которую осуществляется неправомерное воздействие ("пассивная информация") и компьютерную информацию, с помощью которой осуществляется неправомерное воздействие на "пассивную информацию" ("активная информация"). "Пассивная информация" выступает в качестве предмета преступления, а "активная информация" - в качестве орудия совершения преступления.

В качестве "пассивной информации" (предмета преступления в сфере компьютерной информации) могут выступать различные банки данных, госy дарственная или банковская тайна, персональные данные, тайна частной жизни, компьютерные программы и т.д. В роли "активной информации" (орудия совершения преступления в сфере компьютерной информации) выступают команды, вводимые с клавиатуры и т.п. или с помощью звуковых сигналов, различного рода "вирусные" и "троянские" программы, а также иная информация, способная осуществить неправомерное воздействие на "пассивную информацию".

4. Уголовно-правовое регулирование в сфере преступлений, сопряженных с компьютерными технологиями, не в полной мере соответствует реальной ситуации. Оптимальным путем устранения отмеченных пробелов является введение в ряд статей существующего УК дополнений, квалифицирующих отдельные деяния, и соответствующая интерпретация (применительно к компьютерным технологиям) ряда терминов и понятий, употребляющихся в "традиционном" смысле.

Так предлагается включить в статьи Особенной части Уголовного кодекса Российской Федерации квалифицирующий признак использования современных компьютерных технологий. Прежде всего это ст.ст. 129 –Клевета, 130-Оскорбление, 137 - Нарушение неприкосновенности частной жизни, 140 - Отказ в предоставлении гражданину информации - должно распространяться и на информацию, хранящуюся в автоматизированных базах и банках данных, 144 - Воспрепятствование осуществлению избирательных прав или работе избирательных комиссий, 146 - Нарушение авторских и смежных прав, 147 - Нарушение изобретательских и патентных прав, 155 - Разглашение тайны усыновления (удочерения),159 – Мошенничество, 163, - вымогательство, которое может совершаться с использованием компьютерных технологий, 165- причинение имущественного ущерба путем обмана или злоупотребление доверием, также требует в ч. 3 дополнения "совершенное с использованием компьютерных технологий".

Особый интерес представляет для нас гл. 22 - Преступления в сфере экономической деятельности, в частности, ст. 171 (незаконное предпринимательство). 172 (незаконная банковская деятельность), 173 (лжепредпринимательство), 174 (легализация денежных средств, приобретенных незаконным путем) Общеизвестно, что в настоящее время подобные преступления, как правило, совершаются путем фальсификации компьютерной информации, ст. 183 незаконном получении и разглашении сведений, составляющих коммерческую или банковскую тайну, ст.186 -Изготовление или сбыт поддельных денег или ценных бумаг и 187 -Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов, ст. 205 - Терроризм - Вполне достаточно дополнить ст. 205 ч. 2 пунктом "г": "с применением современных компьютерных технологий". Для ст. 207 - Заведомо ложное сообщение об акте терроризма - возможно, было бы целесообразным внесение дополнения о применении для этих целей информационных технологий (компьютерных сетей).

Безусловно, следует включить квалифицирующий признак "в том числе с использованием компьютерных технологий" в ст. 242 - Незаконное распространение порнографических материалов и предметов.

В ст. 284 - Утрата документов, содержащих государственную тайну, было бы целесообразным включить квалифицирующий признак "совершенное с использованием компьютерных технологий" в ст. 292 (Служебный подлог) гл. 30 (Преступление против государственной власти), в ст. 298 (Клевета в отношении судьи, присяжного заседателя, прокурора ...) гл. 31 (Преступления против правосудия).

Особого внимания требует ст. 303 (Фальсификация доказательств), так как цифровые технологии в принципе позволяют фальсифицировать не только письменные документы, но и звук, изображение и т.д.

Несомненно данный перечень является не исчерпывающим и данный проблемы потребуют дополнительного внимания и детального рассмотрения в праве.

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК

**Нормативно-правовые акты**

1. Конституция Российской Федерации. М., Закон. 1994.- 96 с.
2. Уголовный кодекс Российской Федерации. М., Росич. 2006.- 144 с.
3. Гражданский кодекс Российской Федерации ч.1-3 М.ТК Велби. 2005.-442 с.
4. Федеральный закон РФ от 20 февраля 1995 года № 24-ФЗ "Об информации, информатизации и защите информации"//Собрание законодательства РФ. – 1995.- № 8.- ст. 609.
5. Федеральный закон РФ от 7 июля 2003 года № 126 – ФЗ «О связи»//Собрание законодательства РФ. – 2003.- № 28.- Ст. 2895.
6. Закон РФ от 23 сентября 1992 г. № 3523-1: "О правовой охране программ для электронно-вычислительных машин и баз данных"// Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации.-, 1992.- № 42. -Ст. 2325.
7. Закон РФ от 1 января 1994 г. "О правовой охране топологий интегральных микросхем"// Ведомости Верховного Совета РФ. - №42. - 1992. - Ст. 2328.
8. Закон РФ от 9 июля 1993 г. № 5351-1" Об авторском праве и смежных правах"// Ведомости Съезда народных депутатов РФ и Верховного Совета. - 1993. - №32. - Ст. 1242.
9. Закон РФ от 21 июля 1993 г. № 5485-1 "О государственной тайне"// Собрание законодательства РФ. - 1993. - №41. - Ст. 4673.
10. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»//Собрание законодательства РФ.-1997.- № 10.- ст. 1127.
11. Постановление Госкомсанэпиднадзора России от 14 июля 1996. № 14 « Об утверждении гигиенических требований к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы //Социальная защита. 1998. №5.- С.11.
12. Постановление Правительства РФ от 18.12.1995 г. № 1242 «Об утверждении Федеральной целевой программы развития ГАС РФ "Выборы" на - 2000 годы» // СЗ РФ.-1995. -№ 52. - Ст. 5166.
13. Решение Центральной избирательной комиссии Российской Федерации при Президенте Российской Федерации от 11 06. 1996 г № Юб-р/580 "О приемки в опытную эксплуатацию Государственной автоматизированной системы РФ "Выборы" // Вестник Центральной избирательной комиссии РФ.- 1996. -№ 15.- С.12.
14. Указ Президента РФ от 17 декабря 1997 года № 1300 « Об утверждении концепции национальной безопасности»//Российская газета.-1997.- 26 дек.
15. Распоряжение Правительства РФ "О мерах по усилению борьбы в сфере высоких технологий" от 22 октября 1999 г. № 1701-р//Собрание законодательства РФ. -1999. - № 44. - Ст. 5335.

**Научная и учебная литература**

1. Абдеев Р.Ф. Философия информационной цивилизации. М. Слово. 1994. – 342 с.
2. Алексеев И.А. Различные аспекты компьютерной преступности // Проблемы преступности в капиталистических странах. - 1987. - №3.- С.16-19.
3. Александров А. Внимание вирус//Аргументы и факты. 2005. 21 дек.
4. Баев О.Я., Мещеряков В.А. Проблемы уголовно-правового регулирования в свете компьютерной информации // Правовая наука и реформа юридического образования: Сборник научных трудов. Вып. 9. Воронеж: ВГУ, 1998. - С. 84.
5. Быков В., Нехорошев А., Черкасов В. Совершенствование уголовной ответственности за преступления сопряженные с компьютерными технологиями// Уголовное право.- 2003.-№ 3.- С.34.
6. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. М. Юринформ. 2005. – 182 с.
7. Воройский Ф.С. Систематизированный толковый словарь по информатике. – М., Либерия, 1998. – 456 с.
8. Гаухман Л.Д., Максимов С.В. Уголовная ответственность за организацию преступного сообщества (преступной организации). - М., 1997. – 144 с.
9. Гражданский кодекс Российской Федерации. Часть первая. Научно-практический комментарий/ Под ред. Абовой Т.Е., Кабалкина А.Ю., Мозолина В.П. М.,Норма. 2005. – 674 с.
10. Гульбин Ю. Преступления в сфере компьютерной информации// Российская юстиция. – 1997.- №10.- С.34.
11. Гуров А.И. Криминогенная ситуация в России на рубеже XXI века. М., 2000. – 96 с.
12. Дидатов Ю.А. Соисполнителъство в преступлении по российскому уголовному праву: Автореф. дис... к-та. юрид. наук. - М., 1998. – 34 с.
13. Завидов Б.Д., Ибрагимова З.А. Мошенничество в СВТ // Современное право. - 2001. - № 4. - С. 43.
14. Защита прав в сфере интеллектуальной собственности / Под ред. Белова В. В. М., Академия экономических наук и предпринимательской деятельности России; Международная академия информатизации 1995.- 244 с.
15. Зеленский В.Д. Основы компьютеризации расследования. Краснодар. 1998. – 112 с.
16. Зибер У. Справочник по компьютерным преступлениям. М., Норма. 2003.- 134 с.
17. Иванов В.В. Законодательные меры по борьбе с компьютерной преступностью. // Проблемы преступности в капиталистических странах. - 1988. - №10. -С.40.
18. Комментарий к Уголовному кодексу Российской Федерации. Особенная часть. /Под ред. Скуратова Ю.И. и Лебедева В.М. М., БЕК. 1999. – 564 с.
19. Комментарий к Уголовному кодексу Российской Федерации / Под общей ред. руководителя Департамента законодательства о государственной безопасности и правоохранительной деятельности Министерства юстиции Российской Федерации, государственного советника юстиции 2-го класса С.И. Никулина. М., 2001. – 724 с.
20. Комментарий к Уголовному кодексу Российской Федерации/ Под общ. ред. Рарога А.И. М, Юристъ. 1998. – 728 с.
21. Комментарий к Уголовному кодексу Российской Федерации / Под ред. Наумова А.В. М., Юристъ. 2004. – 678 с.
22. Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации //Российская юстиция. -1999. -№ 1. - С. 44.
23. Кригер ГА. Квалификация хищений социалистического имущества. - М, 1974. – 234 с.
24. Крыжановская А.А. Использование программ для ЭВМ- деятельность создающая повышенную опасность для окружающих//Журнал российского права.- 2004. - № 6.- С.13 - 15.
25. Крылов В.В. Основы криминологической теории расследования преступлений в сфере информации. Автореф. дис.... канд. юрид. наук, М., 1997. – 44 с.
26. Крылов В.В. Расследование преступлений в сфере информации. М., 2005. – 180 с.
27. Кузнецов А. Пираты в Интернете // Милиция. - 2000. - №2. - С. 26.
28. Куринов Б.А. Научные основы квалификации преступления. - М., Норма. 2003. – 134 с.
29. Курс уголовного права. Общая часть: Учебник для вузов / Под ред. Н.Ф. Кузнецовой. - М, 1999. - Том 1: Учение о преступлении. – 456 с.
30. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. М., Новый Юрист,1998.- 56 с.
31. Лавров В.В. Уголовная ответственность за легализацию (отмывание) денежных средств или иного имущества, приобретенных незаконным путем. Дис... канд. юр. наук. – Н. Новгород, 2000.- 234 с.
32. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления//Законность. -1997. -№ 1.-С.23.
33. Максимов В.Ю. Незаконное обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания. Автореф. дис... к-нт юрид. наук. - Краснодар: Ставропольский государственный университет, 1998. - С. 13.
34. Милкус А., Мызалин В, Если денег дома нет - потрясите Интернет // Комсомольская правда. 2005. 18 дек.
35. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. Воронеж, 2001. – 180 с.
36. Научно-практический комментарий к Уголовному кодексу Российской Федерации/ Под ред. Панченко П.Н. Н. Новгород, 1999. Т. 2. – 780 с.
37. Никифоров И.В. Уголовно-правовые меры борьбы с компьютерной преступностью и обеспечение компьютерной безопасности. // Вести. С.-Петерб.ун-та. Сер.6. 1995. Вып.4.- С.92.
38. Новое уголовное право России. Особенная часть: Учебное пособие/Под ред. Кузнецовой Н.Ф. - М., Зерцало, ТЕИС. 1996. – 452 с.
39. Ожегов С.И. Словарь русского языка. М. Наука. 1989. – 1200 с.
40. Пикуров Н.И. Уголовное право в системе межотраслевых связей. Волгоград. 1998. – 238 с.
41. Погуляев В., Теренин А. Обеспечение конфиденциальности //эж-ЮРИСТ.- 2004. -№ 2.- С.34.
42. Практикум по уголовному праву: Учебн. пособие / Под ред. Кругликова Л.Л. -М., 1997.- 132 с.
43. Разработка Европейского законодательства по борьбе с киберпреступностью// Уголовное право.- 2005. - № 1.- С. 134.
44. Рарог А.И. Проблемы субъективной стороны преступления. М., 2003. – 182 с.
45. Расследование неправомерного доступа к компьютерной информации: Научно-практическое пособие / Под ред. Шурухнова Н.Г. М., Юринформ. 1999. – 98 с.
46. Расследование преступлений в области высоких технологий // Вестник МВД России. - 2005. - № 6. – C. 2-14.
47. Ревяко Т.Н. Компьютерные террористы на службе преступного мира. Минск. 1997. – 98 с.
48. Решетов Л. Опасный Интернет//Труд. 2005. 10 нояб.
49. Российское уголовное право. Особенная часть / Под ред. Кудрявцева В.Н., Наумова А.В. М., БЕК. 2003. – 670 с.
50. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. - М., Бек. 2001.- 124 с.
51. Сергеев В.В. Компьютерные преступления в банковской сфере // Банковское дело. -2005.- №2.-С. 27-28.
52. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации. Дис… канд. юрид. наук. М., 1999. – 230 с.
53. Степанов-Егинянц В. Ответственность за компьютерные преступления// Законность.- 2005.- №12. - С.49.
54. Талимончик В.П. Компьютерные преступления и новые проблемы сотрудничества государств //Законодательство и экономика.- 2005.- №5.- С.14.
55. Уголовное право Российской Федерации. Особенная часть/ Под ред. Здравомыслова Б.В. М, БЕК. 2000. – 568 с.
56. Уголовное право России. Особенная часть: Учебник / Под ред. Рарога А.И. - М.: Инст. межд. права и экон., 1999. – 766 с.
57. Уголовное право РФ. Особенная часть: Учебник / Под ред. Здравомыслова Б.В. - М., Юрист. 1996. – 732 с.
58. Уголовное право. Особенная часть /Под ред. Ветрова Н.И., Ляпунова Ю И.- М., Норма. 1998. – 824 с.
59. Уголовное право. Особенная часть / Под ред. Козаченко И.Я., Незнамова З.А., Новоселова Г.П. М, 2000. – 620 с.
60. Харкевич А.А. О ценности информации. // Проблемы кибернетики.- 1961. -Вып. 4. - С.31.
61. Фролов Е.А. Спорные вопросы общего учения об объекте преступления. Вып.10. - Свердловск: Свердловский юрид. ин-т., 1969. - С. 225.
62. Фролов Д.Б. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом// Законодательство и экономика. - 2005.- № 5.- С.23.
63. Шершнев Л.И. Безопасность человека. Учебно-методическое пособие, М.: Фонд национальной и международной безопасности. 1994. – 68 с.
64. Шлыков В.В. Экономическая преступность: историко-правовые аспекты. Рязань. 2000. – 126 с.
65. Шумилов Н.И. Криминалистические аспекты информационной безопасности. Автореф. дис... канд. юрид. наук, CПб, 1997. – 24 с.

**Материалы юридической практики**

1. Постановление Пленума Верховного Суда РФ от 27 декабря 2002 года № 29 «О судебной практике по делам о краже, грабеже и разбое»// Бюллетень Верховного Суда РФ.-2003 -№ 2. -С. 6.
2. Постановление Пленума Верховного Суда РФ от 10 февраля 2000 г. № 6 «О судебной практике по делам о взяточничестве и коммерческом подкупе»// Российская газета. - 2000. -23 февраля.
3. Постановление пленума Верховного Суда от 4 мая 1990 года № 5 «О судебной практике по делам о вымогательстве» // Сборник Постановлений Пленумов Верховных Судов СССР и РСФСР (РФ) по уголовным делам. - М, 1995. - С. 515.
4. Постановление Пленума Верховного Суда РФ от 17 января 1997 года № 1 «О практике применения судами законодательства об ответственности за бандитизм» // Российская газета. - 1997. - 30 января.

# Приложение 1


# Приложение 2

**Предмет, орудие и средства неправомерного доступа к компьютерной информации через компьютерную сеть с помощью нескольких ЭВМ**

1. Милкус А., Мызалин В, Если денег дома нет - потрясите Интернет // Комсомольская правда. 2005. 18 дек. [↑](#footnote-ref-1)
2. Абдеев Р.Ф. Философия информационной цивилизации. М. Слово. 1994. - С. 33. [↑](#footnote-ref-2)
3. Ожегов С.И. Словарь русского языка. М. Наука. 1989. - С.222. [↑](#footnote-ref-3)
4. Зеленский В.Д. Основы компьютеризации расследования. Краснодар. 1998. - С.4. [↑](#footnote-ref-4)
5. Харкевич А.А. О ценности информации // Проблемы кибернетики.- 1961. -Вып. 4. - С.31. [↑](#footnote-ref-5)
6. Погуляев В., Теренин А. Обеспечение конфиденциальности //эж-ЮРИСТ.- 2004. -№ 2.- С.34. [↑](#footnote-ref-6)
7. Шершнев Л.И. Безопасность человека. Учебно-методическое пособие, М.: Фонд национальной и международной безопасности. 1994. - С. 33-35. [↑](#footnote-ref-7)
8. Там же. - С.20. [↑](#footnote-ref-8)
9. Крылов В.В. Основы криминологической теории расследования преступлений в сфере информации. Автореф. дис.... канд. юрид. наук, М., 1997. - С. 11. [↑](#footnote-ref-9)
10. Шумилов Н.И. Криминалистические аспекты информационной безопасности. Автореф. дис... канд. юрид. наук, CПб, 1997. - С. 20. [↑](#footnote-ref-10)
11. Гуров А.И. Криминогенная ситуация в России на рубеже XXI века. М., 2000. - С. 36. [↑](#footnote-ref-11)
12. Талимончик В.П. Компьютерные преступления и новые проблемы сотрудничества государств //Законодательство и экономика.- 2005.- №5.- С.14. [↑](#footnote-ref-12)
13. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. М. Юринформ. 2005. - С.11. [↑](#footnote-ref-13)
14. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации. Дис… канд. юрид. наук. М., 1999. - С. 32. [↑](#footnote-ref-14)
15. Уголовное право Российской Федерации. Особенная часть/ Под ред. Здравомыслова Б.В. М, БЕК. 2000. - С. 353. [↑](#footnote-ref-15)
16. Гуров А.И. Криминогенная ситуация в России на рубеже XXI века. М., 2000. - С. 36-37. [↑](#footnote-ref-16)
17. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. Воронеж, 2001. - С. 25. [↑](#footnote-ref-17)
18. Иванов В.В. Законодательные меры по борьбе с компьютерной преступностью. // Проблемы преступности в капиталистических странах. - 1988. - №10. -С.40. [↑](#footnote-ref-18)
19. Никифоров И.В. Уголовно-правовые меры борьбы с компьютерной преступностью и обеспечение компьютерной безопасности. // Вести. С.-Петерб.ун-та. Сер.6. 1995. Вып.4.- С.92. [↑](#footnote-ref-19)
20. Там же. - С.93. [↑](#footnote-ref-20)
21. Зибер У. Справочник по компьютерным преступлениям. М., Норма.2003. - С.65. [↑](#footnote-ref-21)
22. Алексеев И.А. Различные аспекты компьютерной преступности // Проблемы преступности в капиталистических странах. - 1987. - №3.- С.16-19. [↑](#footnote-ref-22)
23. Баев О.Я., Мещеряков В.А. Проблемы уголовно-правового регулирования в свете компьютерной информации // Правовая наука и реформа юридического образования: Сборник научных трудов. Вып. 9. Воронеж: ВГУ, 1998. - С. 84. [↑](#footnote-ref-23)
24. Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации.-, 1992.- № 42. -Ст. 2325. [↑](#footnote-ref-24)
25. Ведомости Верховного Совета РФ. - №42. - 1992. - Ст. 2328. [↑](#footnote-ref-25)
26. Ведомости Съезда народных депутатов РФ и Верховного Совета. - 1993. - №32. - Ст. 1242. [↑](#footnote-ref-26)
27. Собрание законодательства РФ. - 1993. - №41. - Ст. 4673. [↑](#footnote-ref-27)
28. Собрание законодательства РФ. - 1995. - №8. - Ст. 609. [↑](#footnote-ref-28)
29. Гражданский кодекс Российской Федерации. Часть первая. Научно-практический комментарий/ Под ред. Абовой Т.Е., Кабалкина А.Ю., Мозолина В.П. М.,Норма. 2005. - С.222. [↑](#footnote-ref-29)
30. Распоряжение Правительства РФ "О мерах по усилению борьбы в сфере высоких технологий" от 22 октября 1999 г. № 1701-р//Собрание законодательства РФ. -1999. - № 44. - Ст. 5335. [↑](#footnote-ref-30)
31. Пикуров Н.И. Уголовное право в системе межотраслевых связей. Волгоград. 1998. - С.199. [↑](#footnote-ref-31)
32. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации // Дис.. канд. юрид. наук. М, 1999. - С. 51. [↑](#footnote-ref-32)
33. Ревяко Т.Н. Компьютерные террористы на службе преступного мира. Минск. 1997. - С.275-276. [↑](#footnote-ref-33)
34. Кузнецов А. Пираты в Интернете // Милиция. - 2000. - №2. - С. 26. [↑](#footnote-ref-34)
35. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации // Дис. ... канд. юрид. наук. М., 1999. - С. 52. [↑](#footnote-ref-35)
36. Завидов Б.Д., Ибрагимова З.А. Мошенничество в СВТ // Современное право. - 2001. - № 4. - С. 43. [↑](#footnote-ref-36)
37. Шлыков В.В. Экономическая преступность: историко-правовые аспекты. Рязань. 2000. - С.48-49. [↑](#footnote-ref-37)
38. Быков В., Нехорошев А., Черкасов В. Совершенствование уголовной ответственности за преступления сопряженные с компьютерными технологиями// Уголовное право.- 2003.-№ 3.- С.34. [↑](#footnote-ref-38)
39. Новое уголовное право России. Особенная часть: Учебное пособие/Под ред. Кузнецовой Н.Ф. - М., Зерцало, ТЕИС. 1996. - С. 273-274; Уголовное право РФ. Особенная часть: Учебник / Под ред. Здравомыслова Б.В. - М., Юрист. 1996. - С. 356. [↑](#footnote-ref-39)
40. Уголовное право России. Особенная часть: Учебник / Под ред. Рарога А.И. - М.: Инст. межд. права и экон., 1999. - С. 322. [↑](#footnote-ref-40)
41. Ляпунов Ю.И. Указ. работа. - С. 9. [↑](#footnote-ref-41)
42. Фролов Е.А. Спорные вопросы общего учения об объекте преступления. Вып.10. - Свердловск: Свердловский юрид. ин-т., 1969. - С. 225. [↑](#footnote-ref-42)
43. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. - М., Бек. 2001.- С.15. [↑](#footnote-ref-43)
44. Степанов-Егинянц В. Ответственность за компьютерные преступления// Законность.- 2005.- №12. - С.49. [↑](#footnote-ref-44)
45. Максимов В.Ю. Незаконное обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания. Автореф. дис... к-нт юрид. наук. - Краснодар: Ставропольский государственный университет, 1998. - С. 13. [↑](#footnote-ref-45)
46. Сергеев В.В. Компьютерные преступления в банковской сфере // Банковское дело. -2005.- №2.-С. 27-28. [↑](#footnote-ref-46)
47. Собрание законодательства РФ. - 1995. - № 8. - Ст. 609. [↑](#footnote-ref-47)
48. Воройский Ф.С. Систематизированный толковый словарь по ин­форматике. – М., Либерия, 1998. - С.220. [↑](#footnote-ref-48)
49. Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»//Собрание законодательства РФ.-1997.- № 10.- ст. 1127. [↑](#footnote-ref-49)
50. Расследование преступлений в области высоких технологий // Вестник МВД России. - 2005. - № 6. - С.2. [↑](#footnote-ref-50)
51. Уголовное право. Особенная часть /Под ред. Ветрова Н.И., Ляпунова Ю И.- М., Норма. 1998. - С. 549. [↑](#footnote-ref-51)
52. Комментарий к Уголовному кодексу Российской Федерации. Особенная часть. /Под ред. Скуратова Ю.И. и Лебедева В.М. М., БЕК. 1999. - С. 416. [↑](#footnote-ref-52)
53. Комментарий к Уголовному кодексу Российской Федерации / Под общей ред. руководителя Департамента законодательства о государственной безопасности и правоохранительной деятельности Министерства юстиции Российской Федерации, государственного советника юстиции 2-го класса С.И. Никулина. М., 2001. - С. 883. [↑](#footnote-ref-53)
54. Комментарий к Уголовному кодексу Российской Федерации/ Под общ. Ред. Рарога А.И. М, Юристъ. 1998. - С. 596. [↑](#footnote-ref-54)
55. Комментарий к Уголовному кодексу Российской Федерации. Особенная часть. /Под ред. Скуратова Ю.И. и Лебедева В.М. М., БЕК. 1999. - С. 416. [↑](#footnote-ref-55)
56. Комментарий к Уголовному кодексу Российской Федерации / Под общей редакцией руководителя Департамента законодательства о государственной безопасности и правоохранительной деятельности Министерства юстиции Российской Федерации, государственного советника юстиции 2-го класса Никулина С.И. М., 2001. - С. 883 [↑](#footnote-ref-56)
57. Уголовное право. Общая часть./ Под. ред. Ветрова Н.И., Ляпунова Ю.И. М., Норма. 1998. - С. 194. [↑](#footnote-ref-57)
58. Научно-практический комментарий к Уголовному кодексу Российской Федерации/ Под ред. Панченко П.Н. Н. Новгород, 1999. Т. 2. - С. 235-236. [↑](#footnote-ref-58)
59. Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации //Российская юстиция. -1999. -№ 1. -С. 44. [↑](#footnote-ref-59)
60. Расследование неправомерного доступа к компьютерной информации: Научно-практическое пособие /Под ред. Шурухнова Н.Г. М., 1999. - С. 70. [↑](#footnote-ref-60)
61. Уголовное право. Общая часть / Под ред. Ветрова Н.И., Ляпунова Ю.И. М., 1998. С. 239; Рарог А.И. Проблемы субъективной стороны преступления. М., 2003. - С.45. [↑](#footnote-ref-61)
62. Комментарий к Уголовному кодексу Российской Федерации / Под ред. Наумова А.В. М., Юристъ. 2004. - С.665. [↑](#footnote-ref-62)
63. Пашин А.С.. Комментарий к ст. 274-274 УК РФ. Комментарий к Уголовному индексу Российской Федерации / Под ред. Скуратова Ю.И.и Лебедева В.М.. М.,БЕК. 1999. - С.640. [↑](#footnote-ref-63)
64. Уголовное право / Общая часть. Под ред. Ветрова Н.И., Ляпунова Ю.И. М., Норма. 1998. - С. 270. [↑](#footnote-ref-64)
65. Крылов В.В. Расследование преступлений в сфере информации. М., 2005. - С. 163-164. [↑](#footnote-ref-65)
66. Расследование неправомерного доступа к компьютерной информации: Научно-практическое пособие / Под ред. Шурухнова Н.Г. М., Юринформ. 1999. - С. 93-102. [↑](#footnote-ref-66)
67. Расследование преступлений в области высоких технологий // Вестник МВД России. - 2005. - № 6. - С.11. [↑](#footnote-ref-67)
68. Расследование преступлений в области высоких технологий // Вестник МВД России. - 2005. - № 6. - С.14. [↑](#footnote-ref-68)
69. Расследование преступлений в области высоких технологий // Вестник МВД России. - 2005. - № 6. - С.2. [↑](#footnote-ref-69)
70. Уголовное право. Особенная часть / Под ред. Ветрова Н.И., Ляпунова Ю.И. М., 1998. - С. 554. [↑](#footnote-ref-70)
71. Пушкин А.В. Комментарий к ст. 273 УК РФ. Комментарий к Уголовному кодексу Российской Федерации. / Под ред. Наумова А.В. М., Юристъ. 2004. - С. 600. [↑](#footnote-ref-71)
72. Ваулина Т.Н. Преступления в сфере компьютерной информации. Уголовное право. Особенная часть / Под ред. Козаченко И.Я., Незнамова З.А., Новоселова Г.П. М, 2000. - С. 560. [↑](#footnote-ref-72)
73. Бородулин С.В., Полубинская С.В. Преступления в сфере компьютерной информации. Российское уголовное право. Особенная часть / Под ред. Кудрявцева В.Н., Наумова А.В. М., БЕК. 2003. - С. 350. [↑](#footnote-ref-73)
74. Крыжановская А.А. Использование программ для ЭВМ- деятельность создающая повышенную опасность для окружающих//Журнал российского права.- 2004. - № 6.- С.15. [↑](#footnote-ref-74)
75. Расследование преступлений в области высоких технологий // Вестник МВД России. - 2005. - № 6. - С.6. [↑](#footnote-ref-75)
76. Александров А. Внимание вирус// Аргументы и факты. 2005. 21 дек. [↑](#footnote-ref-76)
77. Решетов Л. Опасный Интернет//Труд. 2005. 10 нояб. [↑](#footnote-ref-77)
78. Расследование преступлений в области высоких технологий // Вестник МВД России. - 2005. - № 6. - С.11. [↑](#footnote-ref-78)
79. Комментарий к Уголовному кодексу Российское Федерации / Под ред. Наумова А.В. М., Юристъ. 2004.- С. 666. [↑](#footnote-ref-79)
80. Ляпунов Ю.И., Пушкин А,В. Преступления в сфере компьютерной информации. Уголовное право. Особенная часть / Под. ред. Ветрова Н.И., Ляпунова Ю.И. М, 1998. - С. 559. [↑](#footnote-ref-80)
81. Расследование преступлений в области высоких технологий // Вестник МВД России. - 2005. - № 6. - С.2. [↑](#footnote-ref-81)
82. Ляпунов Ю.И., Пушкин А,В. Преступления в сфере компьютерной информации. Уголовное право. Особенная часть / Под. ред. Ветрова Н.И., Ляпунова Ю.И. М, 1998. - С. 560. [↑](#footnote-ref-82)
83. Постановление Госкомсанэпиднадзора России от 14 июля 1996. № 14 « Об утверждении гигиенических требований к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы //Социальная защита. 1998. №5.- С.11. [↑](#footnote-ref-83)
84. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления//Законность. -1997. -№ 1.-С.23. [↑](#footnote-ref-84)
85. Расследование неправомерного доступа к компьютерной информации / Под ред. Шурухнова Н.Т. - М., 1999. - С. 86. [↑](#footnote-ref-85)
86. Кригер ГА. Квалификация хищений социалистического имущества. - М, 1974. - С. 217. [↑](#footnote-ref-86)
87. Курс уголовного права. Общая часть: Учебник для вузов / Под ред. Кузнецовой Н.Ф. - М, 1999. - Том 1: Учение о преступлении. - С. 417. [↑](#footnote-ref-87)
88. Лавров В.В. Уголовная ответственность за легализацию (отмывание) денежных средств или иного имущества, приобретенных незаконным путем. Дис... канд. юр. наук. – Н. Новгород, 2000.-С. 215. [↑](#footnote-ref-88)
89. Расследование неправомерного доступа к компьютерной информации / Под ред. Шурухнова К. Г. - М, 1999. - С. 83. [↑](#footnote-ref-89)
90. Курс уголовного права. Общая часть: Учебник для вузов. В 2 т. / Под ред. Кузнецовой Н.Ф. - М., 1999. - Том 1: Учение о преступлении. - С. 417. [↑](#footnote-ref-90)
91. Курс уголовного права. Общая часть: Учебник для вузов. В 2 т. / Под ред. Кузнецовой Н.Ф. - М, 1999. - Том 1: Учение о преступлении. - С. 417. [↑](#footnote-ref-91)
92. Лавров В.В. Указ. работа. - С. 216. [↑](#footnote-ref-92)
93. Расследование неправомерного доступа к компьютерной информации / Под ред. Шурухнова Н.Т. - М, 1999. - С. 90. [↑](#footnote-ref-93)
94. Куринов Б.А. Научные основы квалификации преступления. - М., Норма. 2003. - С. 141-142; Практикум по уголовному праву: Учебн. пособие / Под ред. Кругликова Л.Л. -М., 1997.-С. 111. [↑](#footnote-ref-94)
95. Бюллетень Верховного Суда РФ.-2003 -№ 2. -С. 6. [↑](#footnote-ref-95)
96. Крыжановская А.А. Использование программ для ЭВМ- деятельность создающая повышенную опасность для окружающих//Журнал российского права.- 2004. - № 6.- С.13. [↑](#footnote-ref-96)
97. Постановление Пленума Верховного Суда РФ от 10.02.2000 года № 6 «О судебной практике по делам о взяточничестве и коммерческом подкупе: //Российская газета. - 2000. -23 февраля. [↑](#footnote-ref-97)
98. Постановление пленума Верховного Суда от 4.05.1990 года № 5«О судебной практике по делам о вымогательстве» // Сборник Постановлений Пленумов Верховных Судов СССР и РСФСР (РФ) по уголовным делам. - М, 1995. - С. 515. [↑](#footnote-ref-98)
99. Постановление Пленума Верховного Суда РФ от 17.01.97 года № 1 «О практике применения судами законодательства об ответственности за бандитизм» // Российская газета. - 1997. - 30 января. [↑](#footnote-ref-99)
100. Дидатов Ю.А. Соисполнителъство в преступлении по российскому уголовному праву: Автореф. дис... к-та. юрид. наук. - М., 1998. - С. 22. [↑](#footnote-ref-100)
101. Расследование неправомерного доступа к компьютерной информации / Под ред.. Шурухнова Л.Г. - М., 1999. - С. 91. [↑](#footnote-ref-101)
102. Гаухман Л.Д., Максимов С.В. Уголовная ответственность за организацию преступного сообщества (преступной организации). - М., 1997. - С. 9. [↑](#footnote-ref-102)
103. Разработка Европейского законодательства по борьбе с киберпреступностью// Уголовное право.- 2005. - № 1.- С. 134. [↑](#footnote-ref-103)
104. Гульбин Ю. Преступления в сфере компьютерной информации// Российская юстиция. – 1997.- №10.- С.34. [↑](#footnote-ref-104)
105. Курушин В.Д., Минаев В.А. Компьютерные преступления и ин­формационная безопасность. М., Новый Юрист,1998.- С. 18. [↑](#footnote-ref-105)
106. Фролов Д.Б. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом// Законодательство и экономика. - 2005.- № 5.- С.23. [↑](#footnote-ref-106)
107. Курушин В.Д., Минаев В.А. Компьютерные преступления и ин­формационная безопасность. М., Новый Юрист,1998.- С. 18. [↑](#footnote-ref-107)
108. Решение Центральной избирательной комиссии Российской Федерации при Президенте Российской Федерации от 11 06. 1996 г № Юб-р/580 "О приемки в опытную эксплуатацию Государственной автоматизированной системы РФ "Выборы" // Вестник Центральной избирательной комиссии РФ.- 1996. -№ 15; Постановление Правительства РФ от 18.12.1995 г. № 1242 «Об утверждении Федеральной целевой программы развития ГАС РФ "Выборы" на - 2000 годы» // СЗ РФ.-1995. -№ 52. - Ст. 5166. [↑](#footnote-ref-108)
109. Защита прав в сфере интеллектуальной собственности / Под ред. Белова В. В. М., Академия экономических наук и предпринимательской деятельности России; Международная академия информатизации 1995.- С.34. [↑](#footnote-ref-109)
110. Указ Президента РФ от 17 декабря 1997 года № 1300 « об утверждении концепции национальной безопасности»//Российская газета.-1997.- 26 дек. [↑](#footnote-ref-110)