**Содержание**

|  |  |
| --- | --- |
| Введение | 3 |
| 1 Компьютерная информация как объект правовой защиты | 6 |
| 2 Преступления в сфере компьютерной информации | 11 |
| 2.1 Основные криминалистические особенности компьютерной информации | 11 |
| 2.2 Общая характеристика преступлений в сфере компьютерной информации | 12 |
| 2.3 Основные способы совершения компьютерных преступлений | 15 |
| 3 Уголовная ответственность за совершение преступлений в сфере компьютерной информации | 26 |
| 3.1 Анализ главы 28 УК РФ, предусматривающей ответственность за совершение компьютерных преступлений | 26 |
| 3.2 Контроль за компьютерной преступностью в России | 31 |
| Заключение | 34 |
| Список использованной литературы | 35 |
| Приложения | 37 |

**Введение**

Если ушедший XX век по праву можно назвать веком атома, то главным символом XXI века, вероятно, станет информация. И проблемы ее защиты для безопасности личности, общества и государства приобретут еще большее значение и актуальность. Современные информационные технологии интенсивно внедряются во все сферы жизни и деятельности общества, национальная безопасность начинает напрямую зависеть от обеспечения информационной защиты – главного гаранта стабильности в обществе, прав и свобод граждан и правопорядка.

Научно-технический прогресс, создав новые технологии – информационные, в короткие сроки революционно трансформировал процессы сбора, обработки, накопления, хранения, поиска и распространения информации – *информационные процессы*. Эти изменения сформировали сферу деятельности, связанную с созданием, преобразованием и потреблением информации – информационную сферу мирового сообщества, и во многом предопределяют дальнейшее развитие общественных и экономических отношений во всем мире.

Новые информационные процессы сформировали и новые общественные отношения, появилась необходимость их упорядочения. Традиционно функции социального регулятора выполняло право, однако в связи с бурным развитием информационных технологий обнаружилось его отставание – юристы оказались позади инженеров, и поэтому им в спешном порядке приходится разрабатывать новые нормы, приспосабливать действующее законодательство к складывающимся условиям.

Не явилось исключением и уголовное право. С развитием информационного общества появилась потребность в защите его главного движущего фактора – информации и, в частности, особого ее вида – компьютерной информации. Пресечь наиболее опасные проявления человеческого поведения в информационной сфере – задача уголовного законодательства. И если в США и странах ЕС составы компьютерных преступлений присутствовали в законе уже с конца 80-х гг., то в России уголовная ответственность за аналогичные деяния была введена лишь в 1997г. со вступлением в силу нового кодекса.

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

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

Эпидемии компьютерных вирусов стали реальной угрозой для всех, кто пользуется Интернетом. Если в 2002г. ежедневно в антивирусные базы компании «Лаборатории Касперского» вносилось лишь около 20 записей о новых угрозах вирусных атак, то в 2006г. их число доходит уже до 200.

Согласно статистике МВД России за 2005г. в России зарегистрировано уже более 14 тыс. преступлений в сфере телекоммуникаций и компьютерной информации. Самыми многочисленными являются нарушения, связанные с неправомерным доступом к коммерческим данным.

В последнее время стало особенно заметно, что изменилось «лицо» типичного киберпреступника: это уже не молодой человек, пробующий свои силы в программировании, а сорокалетний специалист, зачастую ворочающий миллионами. В первую очередь его интересуют банковские логины и пароли, номера кредитных карт, а также пароли доступа к виртуальному имуществу или к интернет-кошелькам. По данным «Лаборатории Касперского», количество выявленных троянских программ, ворующих банковскую информацию пользователей, за прошлый год выросло в четыре раза.

Количество преступлений в сфере информационных технологий продолжает расти не только в России, но и в мире. Активно развиваясь, компьютерное криминальное общество уже сформировало свою виртуальную среду. Согласно данным Reuters, уже в 2005г. киберпреступность заработала $105 млрд., тем самым обойдя по «официальной» доходности наркоторговлю.

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

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

В связи с вышесказанным сформулируем *цели и задачи* курсовой работы:

1. рассмотреть понятие компьютерной информации,

2. дать общую характеристику преступлений в сфере компьютерной информации и основных способов их совершения,

3. изучить законодательные акты и уголовно-правовые нормы, регулирующие информационные отношения,

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

**1 Компьютерная информация как объект правовой защиты**

Стремительное развитие информационных и коммуникационных технологий, а также компьютеризация мирового сообщества вообще, вызвали острую необходимость включения в правовую систему Российской Федерации юридических норм, которые бы регулировали правоотношения, возникающие в сфере сбора, обработки, накопления (хранения) и передачи информации, а также использование компьютерной техники, средств хранения информации (носителей информации) и каналов связи (телекоммуникаций).

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

* Закон «О средствах массовой информации» (от 27.12.91г. № 2124-1),
* Закон «О Федеральных органах правительственной связи и информации» (от 19.02.92г. № 4524-1),
* Закон «О правовой охране топологий интегральных микросхем» (от 23.09.92г. № 3526-I),
* Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.92г. № 3523-I),
* Закон «Об информации, информатизации и защите информации» (от 20.02.95г. № 24-ФЗ),
* Закон «Об участии в международном информационном обмене» (от 5.06.1996г. № 85-ФЗ),
* Закон «О правовой охране программ для электронно-вычислительных машин и баз данных» (Ведомости РФ, 1992г., № 42, ст. 2325; СЗ РФ, 1995г., № 8, ст. 609).

В данных законодательных актах были определены основные термины и понятия в области компьютерной информации, регулировались вопросы ее распространения, охраны авторских прав, имущественные и неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием программного обеспечения и новых информационных технологий. Также было осуществлено законодательное раскрытие понятий информационной безопасности и международного информационного обмена.

Значительным шагом в деле правового обеспечения деятельно­сти по защите информации яви­лось принятие Федеральным соб­ранием России закона «Об ин­формации, информатизации и за­щите информации» от 20.02.95г. № 24-ФЗ. Он уста­навливает общие правовые требо­вания к организации защиты дан­ных в процессе обработки, хране­ния и циркуляции в технических устройствах и информационно-те­лекоммуникационных линиях связи, контроля за осуществлением мероприятий по защите конфи­денциальной информации. При этом следует подчеркнуть, что за­кон не разделяет государствен­ную и частную информацию как объект защиты в том случае, если доступ к ней ограничивается[[1]](#footnote-1).

В соответствии со ст.2 Федерального закона «Об информации, информатизации и защите информации» и ч. 1 ст. 272 УК РФ, «*информация* – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления»[[2]](#footnote-2).

Иными словами, *компьютерная информация* (*computer information*) – это сведения, циркулирующие в вычислительной среде, зафиксированные на машинном носителе в форме, доступной восприятию ЭВМ, или передающиеся по каналам электросвязи посредством электромагнитных сигналов из одной ЭВМ в другую, из ЭВМ на периферийное устройство, либо на управляющий датчик оборудования. Компьютерная информация всегда опосредована через физический (машинный) носитель информации, вне которого она не может существовать.

Особенно удачным видится определениекомпьютерной информации**,** которое дается доцентом кафедры криминалистики МГУ им. М.В. Ломоносова В. Крыловым, предлагающим следующее криминалистическое определение компьютерной информации как специального объекта преступного посягательства: *компьютерная информация*есть сведения, знания или набор команд (программа), предназначенные для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях – идентифицируемый элемент информационной системы, имеющей собственника, установившего правила ее использования.

Из анализа действующего законодательства следует, что правовой защите подлежит главным образом документированная информация (документ), зафиксированная на материальном носителе с реквизитами, т. е. информация, которая облечена в форму, позволяющую ее «идентифицировать»[[3]](#footnote-3).

 Комментаторами Закона об информации документированная информация описывается как «организационная форма, которая определяется как единая совокупность: а) содержания информации; б) реквизитов, позволяющих установить источник, полноту информации, степень ее достоверности, принадлежность и другие параметры; в) материального носителя информации, на котором ее содержание и реквизиты закреплены»[[4]](#footnote-4).

По мнению В.А. Копылова, понятие «документированная информация» основано на «двуединстве – информации (сведений) и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения. В результате документирования происходит как бы материализация и овеществление сведений...[[5]](#footnote-5)». Отсюда можно сделать вывод, что информация становится объектом Гражданского законодательства.

Между тем, отечественное уголовное законодательство обеспечивает правовую защиту наряду с документированной информацией и иным ее разновидностям и, следовательно, расширяет представление о предмете криминальной деятельности. Анализ действующего Уголовного кодекса РФ показывает, что законодатель выделил из всего объема информационных отношений как подлежащие специальной охране отношения, возникающие в области компьютерной информации. В главу о преступлениях в сфере компьютерной информации введены термины и понятия, которых ранее не было не только в уголовно-правовой терминологии, но и в законодательстве, регулировавшем информационные отношения.

Проанализировав нормы из различных отраслей права, можно сделать ряд выводов:

1. Информацией является совокупность предназначенных для передачи формализованных знаний и сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления (Федеральный закон «Об информации, информатизации и защите информации»).

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

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

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

5. Ограничения (установление режима) использования информации устанавливаются законом или собственником информации, которые объявляют степень (уровень) ее конфиденциальности.

*Конфиденциальными* в соответствии с законом являются, в частности, такие виды информации, как:

* содержащая государственную тайну (Закон РФ «О государственной тайне» ст.ст.275, 276, 283, 284 УК РФ);
* передаваемая путем переписки, телефонных переговоров, почтовых телеграфных или иных сообщений (ч.2 ст.23 Конституции РФ, ст.138 УК РФ); касающаяся тайны усыновления (ст.155 УК РФ);
* содержащая служебную тайну (ст.139 ГК РФ), коммерческую тайну (ст.139 ГК РФ и ст.183 УК РФ), банковскую тайну (ст.183 УК РФ), личную тайну (ст.137 УК РФ), семейную тайну (ст.137 УК РФ), информация, являющаяся объектом авторских и смежных прав (Закон РФ «Об авторском праве и смежных правах», ст.146 УК РФ);
* информация, непосредственно затрагивающая права и свободы гражданина или персональные данные (Федеральный закон «Об информации, информатизации и защите информации», ст.140 УК РФ) и др.

6. Любая форма завладения и пользования конфиденциальной документированной информацией без прямо выраженного согласия ее собственника (за исключением случаев, прямо указанных в законе) является нарушением его прав, т.е. неправомерной.

7. Неправомерное использование документированной информации наказуемо.

**2 Преступления в сфере компьютерной информации**

**2.1 Основные криминалистические особенности компьютерной информации**

Компьютерная информация обладает следующими *криминалистическими особенностями*:

1. Она достаточно просто и быстро преобразуется из одной объектной формы в другую, копируется (размножается) на различные виды машинных носителей и пересылается на любые расстояния, ограниченные только радиусом действия современных средств электросвязи;

2. При изъятии (копировании) компьютерной информации, в отличие от изъятия материального предмета (вещи), она сохраняется в первоисточнике, так как доступ к ней могут одновременно иметь несколько лиц (например, при работе с информацией, содержащейся на электронной странице глобальной сети Интернет, доступ к которой одновременно имеют несколько пользователей).

Информация становится продуктом общественных отношений, начинает приобретать товарные черты и становится предметом купли-продажи. Следствием информационных процессов является возникновение и формирование новых общественных отношений и изменение уже существующих. Сейчас можно зафиксировать большой объем договорных отношений, связанных с изготовлением, передачей, накоплением и использованием информации в различных ее формах. Такого рода общественные отношения закреплены в Федеральном Законе «Об информации, информатизации и защите информации», вступившем в действие с января 1995г. В связи с этим новые информационные технологии дали толчок не только в плане прогресса общества, но и стимулировали возникновение и развитие новых форм преступности. Революция в области компьютерной техники предоставила преступникам широкие возможности в плане доступа к новым техническим средствам.

**2.2 Общая характеристика преступлений в сфере компьютерной информации**

Отсутствие четкого определения компьютерной преступности, единого понимания сущности этого явления значительно затрудняют определение задач правоприменительных органов в выработке единой стратегии борьбы с ней.

В настоящее время существуют два основных течения научной мысли. Одна часть исследователей относит к компьютерным преступлениям действия, в которых компьютер является либо объектом, либо орудием посягательств. В этом случае кража компьютера тоже является компьютерным преступлением. Другая часть исследователей утверждает, что объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства. Надо сказать, что законодательство многих стран, в том числе и в России, стало развиваться именно по этому пути.

Новое российское уголовное законодательство включает в себя ряд неизвестных ранее составов преступлений, среди которых есть нормы, направленные на защиту компьютерной информации. Необходимость установления уголовной ответственности за причинение вреда в связи с использованием именно компьютерной информации вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации по сравнению, скажем, с информацией, зафиксированной на бумаге и хранящейся в сейфе [[6]](#footnote-6).

Итак, *компьютерные преступления* – это преступления, совершенные с использованием компьютерной информации. При этом компьютерная информация является предметом и (или) средством совершения преступления.

Можно выделить следующие характерные особенности компьютерных преступлений:

* неоднородность объекта посягательства,
* выступление машинной информации как в качестве объекта, так и в качестве средства преступления,
* многообразие предметов и средств преступного посягательства,
* выступление компьютера либо в качестве предмета, либо в качестве средства совершения преступления.

На основе этих особенностей можно сделать вывод, что компьютерное преступление *–* это предусмотренное уголовным законом общественно опасное действие, совершенное с использованием средств электронно-вычислительной (компьютерной) техники.

Средства компьютерной техники можно разделить на 2 группы:

1. *Аппаратные средства* – это технические средства, используемые для обработки данных. Сюда относятся:
	* персональный компьютер (комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач),
	* периферийное оборудование (комплекс внешних устройств ЭВМ, не находящихся под непосредственным управлением центрального процессора),
	* физические носители машинной информации;

*2. Программные средства* – это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения. К ним относятся: программное обеспечение (совокупность управляющих и обрабатывающих программ), куда входят:

* + - системные программы (операционные системы, программы технического обслуживания),
		- прикладные программы (программы, которые предназначены для решения задач определенного типа, например редакторы текстов, антивирусные программы, СУБД и т.п.),
		- инструментальные программы (системы программирования, состоящие из языков программирования и трансляторов – комплекса программ, обеспечивающих автоматический перевод с алгоритмических и символических языков в машинные коды),
		- машинная информация владельца, собственника, пользователя.

*Родовым объектом* преступлений в сфере компьютерной информации является общественная безопасность и порядок в отношениях, связанных с информационными процессами – процессами сбора, обработки, накопления, хранения, поиска и распространения информации, с использованием ЭВМ, их систем и сетей. Существенно то, что *предметом* данных преступлений является компьютерная информация, а не информационное оборудование, обеспечивающее информационные процессы. Правонарушения, совершенные в ходе данных процессов, не связанные с использованием указанного оборудования, квалифицируются с помощью иных статей УК РФ, предусматривающих ответственность за соответствующие конкретные действия.

*Непосредственным объектом* данных преступных деяний является безопасность информационных систем, базирующихся на использовании ЭВМ, системе ЭВМ или их сети.

*Объективная сторона* компьютерных преступлений характеризуется как действием, так и бездействием. Действие (бездействие) сопряжено с нарушением прав и интересов по поводу пользования компьютерной информацией.

Компьютерные преступления имеют материальные составы. Действие (бездействие) должно причинить значительный вред правам и интересам личности, общества или государства (исключением является преступление с формальным составом, предусмотренное ч. 1 ст. 273 УК РФ: создание, использование и распространение вредоносных программ для ЭВМ). Преступные последствия конкретизируются в законе применительно к конкретным видам компьютерных преступлений. Между деянием и последствиями обязательно должна быть установлена причинная связь.

*Субъективная сторона* компьютерных преступлений характеризуется умышленной виной. Деяние, совершенное по неосторожности, признается преступлением только тогда, когда это специально предусмотрено соответствующей статьей Особенной части УК РФ. Неосторожная форма вины названа в Особенной части лишь применительно к квалифицированным видам компьютерных преступлений, предусмотренных в ч. 2 ст. 273 и ч. 2 ст. 274 УК.

*Субъект* компьютерного преступления общий – лицо, достигшее 16 лет. В ст. 274 и ч. 2 ст. 272 УК РФ формулируются признаки специального субъекта: лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети.

**2.3 Основные способы совершения компьютерных преступлений**

Важнейшим и определяющим элементом криминалистической характеристики любого, в том числе и компьютерного, преступления является совокупность данных, характеризующих способ его совершения.
Под способом совершения преступления обычно понимают объективно и субъективно обусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и соответственно определить наиболее оптимальные методы решения задач раскрытия преступления [[7]](#footnote-7).

В настоящее время можно выделить свыше 20 основных способов совершения компьютерных преступлений и около 40 их разновидностей. И их число постоянно растет.

Ю.М. Батурин классифицировал способы совершения компьютерных преступлений в пять основных групп. При этом в качестве основного классифицирующего признака выступает метод использования преступником тех или иных действий, направленных на получение доступа к средствам компьютерной техники. Руководствуясь этим признаком, Батурин выделил следующие общие группы [[8]](#footnote-8):

* + - изъятие средств компьютерной техники (СКТ);
		- перехват информации;
		- несанкционированный доступ к СКТ;
		- манипуляция данными и управляющими командами;
		- комплексные методы.

*I. Изъятие средств компьютерной техники.* К этой группе преступлений можно отнести, например, незаконное изъятие физических носителей, на которых находится ценная информация.

*II. Хищение компьютерной информации.*Если «обычные» хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. Не очень далека от истины шутка, что у нас программное обеспечение распространяется только путем краж и обмена краденым. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны.

Другой вид преступлений, связанный с хищением информации, получил название «воздушный змей». В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз («воздушный змей» поднимается все выше и выше) до тех пор, пока на счете не оказывается приличная сумма (фактически она постоянно «перескакивает» с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются, а владелец счета исчезает. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике в такую игру включают большое количество банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

Эти способы основаны на действиях преступника, направленных на получение данных путем определенного перехвата:

1. *непосредственный перехват* **–** это подключение непосредственно к оборудованию компьютера, системы или сети (например, к линии принтера или телефонной линии). Подключение осуществляется с помощью использования бытовых средств и оборудования: телефона, отрезка провода и т.д., а перехваченная информация записывается на физический носитель и переводится в человекообразную форму средствами компьютерной техники;
2. *электронный перехват* – это дистанционный перехват. Он не требует непосредственного подключения к оборудованию компьютера: основан на установлении приемника, который принимает электромагнитные волны – если настроить этот приемник на определенную частоту, то можно принимать, например, волны, которые излучает экран монитора. Благодаря этому способу можно принимать сигналы с больших расстояний;
3. *аудиоперехват* – самый опасный способ перехвата информации. Он заключается в установке специального прослушивающего устройства – «жучка». Эти устройства очень трудно обнаружить, потому что они искусно маскируются под обычные вещи. Аудиоперехват также может проводиться с помощью дорогостоящих лазерных установок, которые могут принимать звуковые вибрации, например, с оконного стекла. Этим способом пользуются, в основном, профессиональные преступники;
4. *видеоперехват –* заключается в использовании преступником видеооптической техники для перехвата информации. Способ имеет две разновидности: первая – физическая, заключается в применении преступником различных бытовых видеооптических приборов (подзорные трубы, бинокли, приборы ночного видения), полученная информация может фиксироваться на физический носитель; во втором случае преступник использует специальные электронные устройства (электронный видеоперехват), которые предполагают наличие различных каналов связи, устройства состоят из передатчика и приемника (передатчик находится в нужном помещении и передает получаемые сигналы на приемник, который находится в руках преступника), а также преступником используются цифровые видеокамеры, видеомагнитофоны и т.д.;
5. *«уборка мусора».* Этот способ совершения компьютерных преступлений заключается в неправомерном использовании преступником отходов технологического процесса. Он осуществляется в двух формах: физической и электронной. В первом случае преступник осматривает содержимое мусорных корзин, емкостей для технологических отходов; собирает оставленные или выброшенные физические носители информации. Электронный вариант требует просмотра содержимого памяти компьютера для получения необходимой информации. Последние записанные данные не всегда полностью стираются из памяти компьютера и существуют специальные программы, которые могут частично или полностью восстанавливать данные на компьютере. Преступник, используя такую программу, может получить необходимую информацию (уничтоженную с точки зрения пользователя). Подобное происходит по вине пользователя, который выполнил не все действия для полного уничтожения данных.

*III. Получение несанкционированного доступа к средствам компьютерной техники.* Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Несанкционированный доступ к файлам законного пользователя осуществляется нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз. Виды несанкционированного доступа:

1. *«за дураком».* Правонарушителем в данном случае является внутренний пользователь определенной системы. Используя этот способ, он получает несанкционированный доступ к средствам компьютерной техники путем прямого подключения к ним (например, с помощью телефонной проводки). Преступление совершается в тот момент, когда сотрудник, который отвечает за работу средства компьютерной техники, ненадолго покидает свое рабочее место, оставляя технику в активном режиме, т.е. способ становится возможным в случае низкой бдительности сотрудников организации;
2. *«компьютерный абордаж».* Если преступник получает доступ к компьютеру, он не может сразу получить нужные ему данные, т.к. на полезную информацию обычно ставят пароль доступа. Используя данный способ, преступник производит подбор кода, для чего используются специальные программы, перебирающие с помощью высокого быстродействия компьютера все возможные варианты пароля. В том случае, если преступник знает пароль, доступ получается значительно быстрее. Необходимо отметить, что существует множество программ, которые взламывают пароль доступа. Но есть также программы–«сторожи», которые отключают пользователя от системы в случае многократного некорректного доступа. В таких случаях преступниками используется другой метод – «интеллектуального подбора». В этом случае программе–«взломщику» передаются некоторые данные о личности составителя пароля (имена, фамилии, номера телефонов и пр.), добытые преступником с помощью других способов. Так как из подобного рода данных обычно составляются пароли, эффективность этого метода достаточно высока. По оценкам специалистов с помощью метода «интеллектуального подбора» вскрывается 42% от общего числа паролей;
3. *неспешный выбор*  характеризуется поиском преступником слабых мест в защите компьютерной системы. Когда такое место найдено, преступник копирует нужную информацию на физический носитель. Этот способ назван так, потому что поиск слабых мест производится долго и очень тщательно;
4. *«брешь» -* способ, при котором преступник ищет конкретно участки программы, имеющие ошибки. Такие «бреши» используются преступником многократно, пока не будут обнаружены. Дело в том, что программисты иногда допускают ошибки при разработке программных средств, и впоследствии их может обнаружить только высококвалифицированный специалист. Иногда программисты намеренно делают «бреши» с целью подготовки совершения преступления. Когда преступник находит «брешь», он может ввести туда несколько команд, которые срабатывают в определенное время или при определенных условиях, образуя тем самым «люк», который открывается по мере необходимости;
5. *«маскарад» -* способ, с помощью которого преступник входит в компьютерную систему, выдавая себя за законного пользователя. Самый простой путь к проникновению в такие системы – получить коды законных пользователей (путем подкупа, вымогательства и т.д.) либо использовать метод «компьютерный абордаж», рассмотренный выше;
6. *мистификация.* Пользователь, который подключается к чьей-нибудь системе, обычно уверен, что он общается с нужным ему абонентом. Этим пользуется преступник, который правильно отвечает на вопросы обманутого пользователя. Пока пользователь находится в заблуждении, преступник может получать необходимую информацию (коды доступа, отклик на пароль и т.д.);
7. *«аварийная ситуация» -* способ, характеризующийся тем, что преступник для получения несанкционированного доступа использует программы, которые находятся на самом компьютере. Обычно это программы, ликвидирующие сбои и другие отклонения в компьютере. Таким программам необходим непосредственный доступ к наиболее важным данным, и благодаря этим программам преступник может войти в систему;
8. *«склад без стен» –* способ, при котором преступник проникает в систему во время поломки компьютера (в это время нарушается система защиты).

*IV. Манипуляции данными и управляющими командами средств компьютерной техники. Подмена данных* – наиболее популярный способ совершения преступления, потому что достаточно простой. Действия преступника при этом направлены на изменение или введение новых данных. Это осуществляется при вводе-выводе информации. Например, в банковские счета можно добавить суммы, которые туда не зачислялись, а потом получить эти деньги.

*«Троянский конь»* – тоже весьма популярный способ совершения преступления. Он заключается во введении преступником в чужое программное обеспечение специальных программ, которые начинают выполнять новые действия, незапланированные законным владельцем средства компьютерной техники. Обычно они используется преступниками для отчисления на заранее открытый счет определенной суммы с каждой операции.

 *«Троянская матрешка»* – вид «троянского коня». Предполагает собой самоуничтожение программы из чужого программного обеспечения после выполнения своей задачи.

*«Салями»* – способ, основанный на быстродействии средств компьютерной техники: при совершении коммерческих сделок конечные суммы округляются; остаточные суммы настолько малы, что вообще не учитываются. Накопление денежных средств преступником происходит за счет отчисления таких сумм со многих операций.

*«Логическая бомба»* – представляет собой тайное внесение в чужое программное обеспечение специальных команд, которые срабатывают при определенных обстоятельствах (в наступлении которых преступник абсолютно уверен). Разновидностью этого способа является «временная бомба» –программа, которая включается по достижении какого-либо времени.

*Компьютерные вирусы.* «Троянские кони» типа «сотри все данные этой программы, перейди в следующую и сделай тоже самое» обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание. Выявляется вирус не сразу: первое время компьютер «вынашивает инфекцию», поскольку для маскировки вирус нередко используется в комбинации с «логической бомбой» или «временной бомбой». Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации.

Начиная действовать (перехватывать управление), вирус дает команду компьютеру, чтобы тот записал зараженную версию программы. После этого он возвращает программе управление. Пользователь ничего не заметит, так как его компьютер находится в состоянии «здорового носителя вируса». Обнаружить этот вирус можно, только обладая чрезвычайно развитой программистской интуицией, поскольку никакие нарушения в работе ЭВМ в данный момент не проявляют себя. А в один прекрасный день компьютер «заболевает».

Варианты вирусов зависят от целей, преследуемых их создателем. Признаки их могут быть относительно доброкачественными, например, замедление в выполнении программ или появление светящейся точки на экране дисплея. Признаки могут быть иволютивными, и «болезнь» будет обостряться по мере своего течения. Так, по непонятным причинам программы начинают переполнять магнитные диски, в результате чего существенно увеличивается объем программных файлов. Наконец, эти проявления могут быть катастрофическими и привести к стиранию файлов и уничтожению программного обеспечения.

Эти программы самопроизвольно присоединяются к другим программам и при запуске последних выполняют различные, нежелательные действия (порча файлов и каталогов, искажение и уничтожение информации и т.д.). Этот способ совершения компьютерных преступлений наиболее популярен. В настоящее время в мире существует очень много видов компьютерных вирусов, но всех их можно отнести к загрузочным либо к файловым:

* *загрузочные вирусы* – заражение происходит при загрузке компьютера с носителя информации, содержащего вирус. Заразить сам носитель достаточно просто: на него вирус может попасть, если пользователь вставил его в приемное устройство зараженного включенного компьютера. При этом вирус автоматически внедряется во внутреннюю структуру носителя;
* *файловые вирусы –* поражают исполняемые файлы: EXE, COM, SYS, BAT. Эти вирусы заражают компьютер, если была запущена программа, которая уже содержит вирус. В этом случае происходит дальнейшее заражение других программ, по сути напоминающее вирусное заболевание.

Для изучения вирусов создана специальная наука – компьютерная вирусология. С точки зрения этой науки вирусы можно разделить на:

* *резидентные* *и нерезидентные*. Резидентный вирус, оставляя свой код в оперативной памяти, возобновляется при каждом включении компьютера. Менее опасными являются нерезидентные вирусы. Они оставляют в оперативной памяти небольшие программы, которые не имеют алгоритма распространения вируса (такой вирус погибает при выключении компьютера);
* *«вульгарные» и* *«раздробленные»*. Такое деление произведено по алгоритму строения и обнаружения того или иного вируса. «Вульгарные» вирусы написаны одним блоком и легко обнаруживаются специалистами с помощью специальных антивирусных программ. Что касается Программа «раздробленного» вируса разделена на части, никак не связанные друг с другом, но они «собирающиеся» при определенных условиях во вполне здоровый вирус (после выполнении своей задачи такой вирус распадается или самоуничтожается).

Вирусные модификации:

* + *вирусы-«черви» -* вирусы, не изменяющие программные файлы. Они проникают в память компьютера из компьютерной сети, и вычисляют адреса других компьютеров (в обнаруженные компьютеры рассылают копии вируса);
	+ *вирусы-«невидимки» -* достаточно совершенные вирусы: их трудно обнаружить антивирусной программой и невозможно увидеть при обычном просмотре файлов, т.к. при открытии зараженного файла они немедленно удаляются из него, а при закрытии опять заражают;
	+ *вирусы-«призраки» –*  тоже трудно обнаруживаемые вирусы: заражая программы, они постоянно меняют свой код (содержание), так что во всех следующих зараженных программах нельзя заметить какого-то совпадения. Потому эти вирусы трудно обнаружить с помощью антивирусных программ, основанных на этом принципе.

*Моделирование –* способ совершения компьютерных преступлений, который представляет собой моделирование поведения устройства или системы с помощью программного обеспечения. Например: «двойная» бухгалтерия. Здесь одновременно существуют две бухгалтерские программы, одна из которых функционирует в законном режиме, а другая – незаконном. С помощью незаконной программы проводят теневые сделки.

*Копирование –* способ совершения преступления, который представляет собой незаконное копирование информации преступником программных средств компьютерной техники. Преступник незаконно копирует информацию на свой физический носитель, а затем использует ее в корыстных целях. Этот способ распространен из-за своей простоты. Например: два лица заключают договор на разработку программного средства, заказчик при этом платит определенную сумму за работу. Исполнитель просто копирует нужную программу из какого-либо источника, и, выдавая за свою, предоставляет заказчику.

*Преодоление программных средств защиты –* вспомогательный способ совершения преступления, представляющий собой умышленное преодоление системы защиты. Существует несколько разновидностей этого способа:

1. создание копии ключевой дискеты. Для запуска некоторых систем необходима ключевая дискета с необходимыми системными файлами. Преступник может незаконно создать копию такой дискеты с помощью программы DISKCOPY, что позже поможет ему попасть в нужную систему;
2. модификация кода системы защиты. Код системы защиты выполняет в компьютере проверку ключевых дискет на санкционированность запуска защищенного информационного ресурса. Модифицируя этот код, преступник просто обходит систему защиты. Данный способ может быть реализован только высококлассным опытным специалистом;
3. использование механизма установки (снятия) программных средств защиты информации. Некоторые программные средства защиты устанавливаются на физический носитель и закрепляются на нем вместе с другими данными. В связи с этим невозможно произвести копирование с такого носителя. В данном случае преступник производит некий алгоритм действий и снимает защищенные программы с носителя. Этот процесс требует немалых знаний и опыта от правонарушителя;
4. снятие системы защиты из памяти ЭВМ. Система защиты периодически загружает защищаемое программное средство в оперативную память для передачи управления этой программой коду защиты. Когда код еще не взял управление на себя, в оперативной памяти находится совершенно незащищенная программа. Преступнику остается сохранить ее в каком-нибудь файле.

**3 Уголовная ответственность за совершение преступлений в сфере компьютерной информации**

**3.1 Анализ главы 28 УК РФ, предусматривающей ответственность за совершение преступлений в сфере компьютерной информации**

В главе 28 УК РФ определяются следующие общественно опасные деяния в отношении средств компьютерной техники:

* Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (ст. 272 УК);
* Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами (ст. 273 УК);
* 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 (ст. 274 УК).

Как правило, вышеперечисленные преступления совершаются в совокупности с иными общественно опасными деяниями. Это обусловлено тем, что при использовании компьютерной информации в качестве средства совершения другого преступления, она сама становится предметом общественно опасного деяния.

Невозможно противоправно воспользоваться компьютерной информацией, не нарушив при этом ее правовой защиты, т.е. не совершив хотя бы одного из действий, перечисленных в ст. 20 Федерального закона «Об информации, информатизации и защиты информации», а именно: утечки, хищения, утраты, искажения, подделки, уничтожения, модификации, копирования, блокирования.

Чаще всего компьютерная информация используется для совершения следующих преступлений, расположенных по ранжиру:

* 1. нарушение авторских и смежных прав (ст. 146 УК);
	2. мошенничество (ст. 159 УК);
	3. подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков (ст. 327 УК);
	4. изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов (ст. 187 УК);
	5. изготовление или сбыт поддельных денег или ценных бумаг (ст. 186 УК);
	6. причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК) – при незаконном использовании чужого логина и пароля доступа в сеть Интернет;
	7. уклонение от уплаты налогов с организаций (ст. 199 УК);
	8. нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК);
	9. незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК).

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

Данная статья защищает право лиц на неприкосновенность информации в системе (см. схема 1). Владельцем информационной вычислительной системы (и информации в ней) может быть любое лицо, правомерно пользующееся услугами по обработке информации как собственник вычислительной системы (ЭВМ, сети ЭВМ) или как лицо, приобретшее право использования системы (информации). Данная статья защищает компьютерную информацию любых предприятий, учреждений, организаций и частных лиц. Диспозиция соответствующей нормы заключается в неправомерном доступе к охраняемой законом компьютерной информации.

Схема 1. Регулируемые законодательством действия, совершаемые с информацией (сообщениями)

|  |
| --- |
| Регулируемые законодательством действия, совершаемые с информацией (сообщениями) |
|  |  |  |
|  |  | Создание и обработка информации |
|  |  |
|  |  | Сбор и поиск информации (в т.ч. доступ к ней) |
|  |  |
|  |  | Накопление и хранение информации |
|  |  |
|  |  | Защита информации |
|  |  |
|  |  | Распространение и предоставление информации |
|  |  |
|  |  | Непредставление информации |
|  |  |
|  |  | Копирование информации |
|  |  |
|  |  | Уничтожение информации |
|  |  |
|  |  | Изменение (модификация) информации |
|  |  |
|  |  | Хищение, изъятие и утрата информации |
|  |  |
|  |  | Блокирование информации |
|  |  |

Неправомерным является доступ, противоречащий действующим правовым нормам, актам управления, приказам, распоряжениям и иным актам, регулирующим отношения по доступу лиц (группы лиц) к информации.[[9]](#footnote-9) Кроме того, неправомерным будет доступ, если лицо незаконно использовало технические средства для проникновения в ЭВМ и (или) ее сеть, например введение чужого пароля либо снятие необходимого пароля, модификация программы и пр. Под неправомерным доступом к охраняемой законом компьютерной информации следует понимать также самовольное получение информации без разрешения ее собственника или владельца[[10]](#footnote-10).

Под охраняемой законом информацией понимается информация, для которой законодательно установлен специальный режим ее правовой защиты, например – государственная, служебная и коммерческая тайна, персональные данные и т.д.[[11]](#footnote-11)

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

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

Ст. 273 УК предусматривает ответственность за создание, использование или распространение вредоносных программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к последствиям, описанным в ст. 272. Указанные последствия (уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети) в исследованиях по информационной безопасности рассматриваются, как угрозы системе защиты информации и «расшифровываются» при помощи трёх свойств защищаемой информации: конфиденциальности (неизвестности третьим лицам), целостности и доступности (см. табл. 1.)

Таблица 1. Классификация угроз информационной безопасности

|  |  |  |  |
| --- | --- | --- | --- |
| **Угроза** | **Нарушение конфиденциальности** | **Нарушение целостности** | **Нарушение доступности** |
| Уничтожение информации |  | + | + |
| Блокирование информации |  |  | + |
| Модификация информации | + | + |  |
| Копирование информации | + |  |  |
| Нарушение работы информационной системы | + | + | + |

Под *вредоносными программами* в смысле ст. 273 УК РФ понимаются программы, специально созданные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, определенные в документации на программу.

 Под использованием либо распространением вредоносных программ или машинных носителей к ним понимается соответственно введение этих программ в ЭВМ, систему ЭВМ или их сеть, а также продажа, обмен, дарение или безвозмездная передача другим лицам [[12]](#footnote-12).

Целью действия ст. 274 должно быть предупреждение невыполнения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой информации. Данная уголовная норма, естественно, не содержит конкретных технических требований и отсылает к ведомственным инструкциям и правилам, определяющим порядок работы, которые должны устанавливаться специально управомоченным лицом и доводиться до пользователей. Применение данной статьи невозможно для систем публичного доступа, например, глобальной компьютерной сети Internet; ее действие распространяется только на компьютеры и локальные сети организаций[[13]](#footnote-13).

В этой статье также считается, что под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим ее правовой защиты, например – государственная, служебная и коммерческая, банковская тайны, персональные данные и т.д. [[14]](#footnote-14)

Данная статья требует чтобы между фактом нарушения и наступившим существенным вредом была установлена причинная связь и полностью доказано, что наступившие последствия являются результатом именно нарушения правил эксплуатации.

**3.2 Контроль над компьютерной преступностью в России**

Меры контроля над компьютерной преступностью подразделяются на правовые, организационно-тактические и программно-технические[[15]](#footnote-15).

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

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

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

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

Борьба с компьютерной преступностью в России осуществляется в условиях действия комплекса факторов, снижающих ее эффективность. К наиболее значимым факторам относятся:

* отсутствие отлаженной системы правового и организационно-технического обеспечения законных интересов граждан, государства и общества в области информационной безопасности;
* ограниченные возможности бюджетного финансирования работ по созданию правовой, организационной и технической базы информационной безопасности;
* недостаточное осознание органами государственной власти на федеральном и, особенно, региональном уровне возможных политических, экономических, моральных и юридических последствий компьютерных преступлений;
* слабость координации действий по борьбе с компьютерными преступлениями правоохранительных органов, суда и прокуратуры и неподготовленность их кадрового состава к эффективному предупреждению, выявлению и расследованию таких деяний;
* несовершенство системы единого учета правонарушений, совершаемых с использованием средств информатизации;
* серьезным отставанием отечественной индустрии средств и технологий информатизации и информационной безопасности от мирового уровня.

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

* формирование целостной системы непрерывного отслеживания обстановки в сфере обеспечения информационной безопасности различных систем в стране и упреждающего принятия решений по выявлению и пресечению компьютерных преступлений;
* организация взаимодействия и координация усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой;
* организация эффективного взаимодействия правоохранительной системы России с правоохранительными органами зарубежных стран, осуществляющими борьбу с компьютерными преступлениями;
* координация действий с общественными и частными организационными структурами (фондами, ассоциациями, фирмами, службами безопасности банковских и коммерческих структур), на своем уровне осуществляющими практические мероприятия по обеспечению информационной безопасности.

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

**Заключение**

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

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

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

Для выявления проти­воправности действий хакера и поиска следов компью­терного преступления требуется эксперт, облада­ющий опытом и знаниями в области ЭВМ никак не меньшими, чем сам преступник. Без грамотного экс­пертного заключения привлечение лица к уголовной ответственности, даже при наличии признаков состава преступления, становится проблематичным.

Именно поэтому такой высокий процент прекращенных дел по данной категории преступлений. По-видимому, только ужесточение наказания за данную категорию преступлений и его неотвратимость могут изменить сложившуюся ситуацию.

**Список использованной литературы**

1. **Законодательные акты и комментарии к ним:**
2. Уголовный кодекс Российской Федерации от 24.05.96г. – СПб.: Альфа, 1996.
3. Фе­деральный закон от 22 февраля 1995г. № 24-ФЗ «Об информации, информатизации и защите информации». // Российская газета. — 1995. — 22 февраля.
4. Федеральный закон «Об информации, информатизации и защите информации»: Комментарий. – М.: Институт государства и права РАН, 1996.
5. Постатейный Комментарий к Уголовному кодексу РФ 1996г. / Под ред. А. В. Наумова. – М.: Юристъ, 1996.
6. Скуратов Ю.И., Лебедев В.М. Комментарий к Уголовному кодексу. – М., 1996.

**2. Учебники и монографии:**

1. Батурин Ю.М., Жодзинский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 1991.
2. Батурин Ю.М. Проблемы компьютерного права. — М.: Юридическая литература, 1991.
3. Вехов Б.В. Компьютерные преступления: способы совершения, методика расследования. – М.: Право и закон, 1996.
4. Егорышев А.С. Безопасность компьютерной информации в XXI веке. / Общество, государство и право России на пороге XXI века: теория, история. Межвузовский сборник научных трудов. / Под редакцией проф. К.Б. Толкачева, проф. А.Г. Хабибулина. – Уфа: УЮИ МВД России, 2000.
5. Информатика для юристов: Учебник. / О.Э. Згадзай, С.Я. Ка­занцев, Л.А. Казанцева; под ред. С.Я. Казанцева. — М.: Мастер­ство, 2001.
6. Копылов В.А. Информационное право. – М.: Юристъ, 1997.
7. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. — М.: Новый Юрист, 1998.
8. Пущин В.С. Преступления в сфере компьютерной информации. – М., 2000.
9. Сорокин А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. – Курган, 1999.

 Уголовное право России. Особенная часть: Учебник. / Отв. ред. Б.В. Здравомыслов. – М.: Юристъ, 1996.

**3. Научные статьи в журналах:**

1. Беззубцев О.А., Ковалев А.Н. ФАПСИ: Законодательное регулирование в области защиты информации // Технологии и средства связи, 1997. – № 1. – С.94–96.
2. Голубев В.В. Компьютеризация и уголовное право. // Законодательство. – 1999г. – № 8.
3. Гульбин Ю. Преступления в сфере компьютерной информации. // Российская юстиция. – 1997г. – №10.
4. Крылов В.В. Информация как элемент криминальной деятельности. // Вестник Московского университета, серия 11. – 1998. – №4. – М.: Право.
5. Крылов В.В. Информационные преступления - новый криминалистический объект // Российская юстиция. – 1997г. – N 4.
6. Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации. // Российская юстиция. – 1999. – №1. – С.44–45.

**Материалы сайтов:**

1. Уголовный кодекс РФ от 13 июня 1996г. № 63-ФЗ (с изменениями от 27.05.98, 25.06.98г., 09.02.99г., 15.03.99г., 18.03.99г., 09.07.99 г., 20.03.01г., 19.06.01г., 07.08.01г., 17.11.01г., 29.12.01г., 14.03.02г., 07.05.02г., 25.06.02г., 25.07.02г., 31.10.02г., 11.03.03г., 08.04.03г., 07.07.03г., 08.12.03г., 2107.04г., 26.07.04г., 28.12.04г., 21.07.05г.) –<http://law.rambler.ru/library/norubs/9577/index.html>.
2. [crime-research.ru](http://www.crime-research.ru/)
3. <http://www.crime-research.ru/library/Golovin.htm>
4. Сорокин А.В. Судебная практика по делам о преступлениях в сфере компьютерной информации. – <http://www.zaural.ru/procur/my_page.htm>.

**Приложение 1**

ОБВИНИТЕЛЬНОЕ ЗАКЛЮЧЕНИЕ
по уголовному делу 73129[[16]](#footnote-16)

 по обвинению Т. и К. в совершении преступления,

предусмотренного *ст. 272 ч. 2 УК РФ*.

9-го ноября 2001г. УРОПД ГУВД МО было возбуждено уголовное дело № 73129 по факту совершения неправомерного доступа к охраняемой законом компьютерной информации в кассовых аппаратах ЧП4001 г. Павловский Посад.

Проведенным по делу расследованием установлено: в период времени с июля 2001 года, точная дата следствием не установлена, по 9-е ноября 2001 года, руководитель ЧП 4001 г. Павловский Посад Московской области Т., по предварительному сговору в группе с К. и действуя с ней с единым умыслом, с целью сокрытия доходов от налогообложения, ежедневно, в период времени с 17-ти до 19-ти часов, в торговых палатках ЧП 4001 на ул. Б. Покровка г. Павловский Посад, подключали в гнезда «ЭВМ» и «Ш-К» двух контрольно-кассовых аппаратов АМС 100-Ф, 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 течении текущей смены. После подключения прибора к контрольно-кассовым аппаратам и совершения неправомерного доступа к охраняемой законом компьютерной информации, в буферной памяти контрольно-кассовых аппаратов АМС 100-Ф № 29721626 и № 29721975 уничтожалась вся информация о предшествующих финансовых операциях выполненных в течении 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 4001 продолжали свою работу, накапливая информацию в буферной памяти о производимых финансовых операциях до окончания текущей смены, то есть до 21-го часа, после чего в фискальную память контрольно-кассовых аппаратов заносились измененные заниженные данные о сумме выручки за смену.

*Таким образом, Т. и К. совершили неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ). Это деяние, совершенное группой лиц по предварительному сговору, повлекло уничтожение и модификацию информации.*

**Приложение 2**

Уфа, 2002г.

Уголовное дело № 2010053

по обвинению П. в совершении преступлений,

предусмотренных *ч.1 ст. 165, ч.1 ст. 272 УК РФ*

(неправомерный доступ к сети Интернет).

**Фабула уголовного дела:**

 Проведенным по делу предварительным расследованием установлено:

 В декабре 2001г. П. от своего знакомого С. получил логин, принадлежащий диспансеру, полученный от Информационно-коммуникационного центра по договору от 28.09.2001г.

Затем, в период с 1 декабря 2001г. по 1 марта 2002г. П., полностью осознавая всю противоправность своих незаконных действий, неоднократно, как в ночное, так и в дневное время, используя указанный выше логин, осуществлял незаконный выход в компьютерную сеть Интернет.

Для несанкционированного выхода в сеть Интернет П. использовался компьютер со следующими характеристиками: процессор – Celeron–500, материнская плата – ASUS P2-99, жесткий диск – Quantum 15Gb, устройство для чтения лазерных дисков – CD-ROM, оперативное запоминающее устройство – 256RAM, модем внутренний – Sportser 33.6 FAX Voice, видеокарта – Asus Riva TNT2 16Mb, позволяющими осуществление доступа к ресурсам сети Интернет, а так же телефонная линия, имеющая выход на городской номер, которые были расположены и установлены по месту проживания П.

Осуществляя незаконный выход в сеть Интернет, П. полностью осознавал, что его умышленные, неправомерные действия повлекли блокирование компьютерной информации, выразившееся в искусственном затруднении доступа законного пользователя к ресурсам Интернет; копирование охраняемой законом компьютерной информации, что выразилось в переносе информации с одного физического носителя на жесткий диск системного блока своего домашнего компьютера помимо воли собственника; а так же модификацию охраняемой законом статистической информации законного пользователя, что выразилось в увеличении показателей оплаты на сервере законного пользователя в лице диспансера.

 *Таким образом, П. своими умышленными действиями совершил преступление, предусмотренное ч.1 ст. 272 УК РФ – неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, повлекший блокирование, модификацию и копирование информации.*

 В процессе работы в сети Интернет, П. с целью бесплатного пользования услугами Интернет, из корыстных побуждений, умышленно, обманным путем, используя логин, принадлежащий диспансеру, полученный от Информационно-коммуникационного центра по договору от 28.09.2001 г., в период с 01.12.01г. по 01.03.02г., совершал выход и работу в сети Интернет, сознавая, что причиняет материальный ущерб собственнику указанного логина.

Всего за период с 1 декабря 2001г. по 1 марта 2002г., П. были осуществлены неправомерные выходы в Интернет на общую сумму 2 546,15 руб., согласно справке от 27.02.2002 г. диспансера. Полученные услуги П. не оплачивались, и не могли оплачиваться в связи с тем, что стоимость за пользование сетью автоматически относилась на счет законного пользователя – диспансера, при этом П. реально не изымал денежные средства и имущество у собственника. Указанные действия были произведены П. несмотря на то, что ему был известен порядок предоставления услуг Интернет, а так же порядок произведения оплаты за полученные услуги.

Своими преступными действиями П., путем обмана причинил диспансеру материальный ущерб на общую сумму 2 546,15 руб. за полученные незаконным способом услуги.

 *Таким образом, П. своими умышленными действиями совершил преступление, предусмотренное ч.1 ст. 165 УК РФ – причинение имущественного ущерба путем обмана при отсутствии признаков хищения.*

**Приложение 3**

Саратов, 2003г.

Уголовное дело [№ 82256](http://cyber-crimes.ru/practice/273/?ID=Saratov_82256)

по обвинению Т. в совершении преступлений,

предусмотренных *ч.1 ст. 146, ч.1 ст. 273 УК РФ*

(использование и распространение специальной программы

для взлома бухгалтерского программного обеспечения)

**Фабула уголовного дела:**

 Проведенным по настоящему уголовному делу расследованием установлено следующее.

 У Т., не имеющего постоянного места работы и источника доходов, в 2002г. возник преступный умысел на извлечение доходов путем реализации копий компьютерных программ, без оформления договора на право их обладания, с целью извлечения выгоды.

С целью реализации своего преступного умысла, в г. Саратове примерно 10 февраля 2003г. на территории рынка «Саратовская Горбушка», в дневное время у неустановленного в ходе следствия лица по имени А., Т. незаконно приобрел нелицензионный CD-ROM диск, являющийся машинным носителем, содержащий компьютерную программу «1С Предприятие», без заключения соглашения на право использования данной программой с официальными представителями АОЗТ «1С» в Саратовской области. Данный диск так же содержал вредоносную программу «SABLE», специально предназначенную для внесения несанкционированной модификации с целью дальнейшего использования и копирования программы «1С Предприятия», после чего хранил указанный диск при себе и у себя дома до 17 февраля 2003г.

Кроме того, одновременно с приобретением диска, содержащего программную продукцию АОЗТ «1С», Т. незаконно приобрел у указанного выше лица два CD-ROM диска, являющихся машинными носителями, содержащими компоненты компьютерной программы «Гарант-Максимум», без заключения соглашения на право использования данной программы с официальными представителями НПП «Гарант-Сервис» в Саратовской области», после чего хранил указанные диски при себе и у себя дома до 17 февраля 2003г.

Действуя с целью реализации своего преступного умысла, Т. предпринял меры к поиску клиентов, согласных на приобретение нелицензионных программ АОЗТ «1С» и НПП «Гарант-Сервис», за незаконное денежное вознаграждения и, в результате, ему удалось договориться о сбыте программ.

После этого Т., осознавая, что незаконно приобретенная им программа «1С: Предприятие, комплексная поставка версия 7.7», стоимостью 88340 руб., является собственностью АОЗТ «1С», и что копирование этой программы и распространение ее копий запрещено правообладателем и нарушает его авторские права, причиняя правообладателю крупный ущерб, тем не менее, имея доступ к указанной компьютерной информации, из корыстных побуждений, с целью извлечения выгоды, 17 февраля 2003г., в период времени с 12 часов до 12 часов 20 минут, находясь на торговой точке ЧП «К.», расположенной на рынке «Саратовская Горбушка», продал Н. имевшийся у него при себе диск, являющийся машинным носителем, содержащий программу «1С: Предприятие комплексная поставка версия 7.7», осуществив тем самым несанкционированное распространение с целью извлечение выгоды информации, неразрешенное ее собственником. При этом Т. был осведомлен о том, что на диске так же содержится программа, предназначенная для нейтрализации ключа «HASP», являющегося интеллектуальным средством защиты программы от копирования, поставляемого правообладателем вместе с программой «1С: Предприятие, комплексная поставка версия 7.7», а именно программа «SABLE». Данная программа специально предназначена для внесения несанкционированной модификации программного продукта АОЗТ «1С», эмулирующую указанный ключ.

Таким образом, Т. совершил незаконное использование объектов авторского права с целью извлечения выгоды, причинив крупный ущерб правообладателю АОЗТ «1С», официальным представителем которой на территории Саратовской области является ООО «А.», на сумму 88340 рублей, а так же в виде подрыва деловой репутации указанных фирм, являющийся для АОЗТ «1С» крупным ущербом, поскольку включает в себя не только ущемление имущественных прав и причинение реального материального ущерба законным интересам правообладателей, но и нарушение конституционных прав и охраняемых законами РФ и международными договорами прав, а так же подрыв их деловой репутации.

Кроме того, 17 февраля 2003г., одновременно с незаконным сбытом программного продукта АОЗТ «1С», в период времени с 12 часов до 12 часов 20 минут, Т., осознавая, что незаконно приобретенная им программа «Гарант-Максимум», стоимостью 58752 руб. является собственностью НПП «Гарант-Сервис», и что копирование этой программы и распространение ее копий запрещено правообладателем и нарушает его авторские права, причиняя правообладателю крупный ущерб, тем не менее, имея доступ к указанной компьютерной информации, из корыстных побуждений, с целью извлечения выгоды, находясь на торговой точке ЧП «К.», расположенной на рынке «Саратовская Горбушка», продал Н. имевшиеся у него при себе два диска, являющиеся машинными носителями, содержащими программу «Гарант-Максимум», осуществив тем самым несанкционированное распространение с целью извлечение выгоды информации, неразрешенное ее собственником.

Таким образом, Т. совершил незаконное использование объектов авторского права с целью извлечения выгоды, причинив крупный ущерб правообладателю НПП «Гарант-Сервис», официальным представителем которой на территории Саратовской области является ООО «Компания «Гарант-Саратов»», на сумму 58752 руб., а так же в виде подрыва деловой репутации указанных фирм, являющийся для НПП «Гарант-Сервис» крупным ущербом, поскольку включает в себя не только ущемление имущественных прав и причинение реального материального ущерба законным интересам правообладателей, но и нарушение конституционных прав и охраняемых законами РФ и международными договорами прав, а так же подрыв их деловой репутации.

После этого Т., в качестве вознаграждения, получил от Н. за копии указанных программ наличные деньги в сумме 2100 руб., после чего был задержан сотрудниками правоохранительных органов.

 *Таким образом, своими действиями Т. совершил преступление, предусмотренное ч.1 ст. 146 УК РФ – незаконное использование объектов авторского права, если это деяние причинило крупный ущерб.*

 Кроме того, Т. осознавал, что защитная система лицензионной программы «1С: Предприятие, комплексная поставка версия 7.7» не позволит использовать продукт авторского права, принадлежащий АОЗТ «1С» без системного ключа «HASP». С целью нейтрализации ключа «HASP», являющегося интеллектуальным средством защиты программы от копирования, поставляемого правообладателем вместе с программой «1С: Предприятие, комплексная поставка версия 7.7», Т. передал Н. программу «SABLE», специально предназначенную для внесения несанкционированной модификации программного продукта АОЗТ «1С», эмулирующую указанный ключ, находившуюся на диске, проданном им. Тем самым он осуществил распространение вредоносной программы «SABLE».

 *Таким образом, своими действиями Т. совершил преступление, предусмотренное ч.1 ст. 273 УК РФ – создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному модификации и копированию информации, а равно использование и распространение таких программ.*

1. Беззубцев О.А., Ковалев А.Н. ФАПСИ: Законодательное регулирование в области защиты информации // Технологии и средства связи, 1997. – № 1. – С. 96. [↑](#footnote-ref-1)
2. Ст.2 Федерального закона «Об информации, информатизации и защите информации» от 20.02.95г. № 24-ФЗ. [↑](#footnote-ref-2)
3. Крылов В.В. Информация как элемент криминальной деятельности. // Вестник Московского университета, серия 11. – 1998. – №4. – М.: «Право». [↑](#footnote-ref-3)
4. Федеральный закон «Об информации, информатизации и защите информации»: Комментарий. – М.: Институт государства и права РАН, 1996. – С. 15. [↑](#footnote-ref-4)
5. Копылов В.А. Информационное право. – М.: Юристъ, 1997. – С. 23. [↑](#footnote-ref-5)
6. Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации. // Российская юстиция. – 1999. - №1. – С.44-45. [↑](#footnote-ref-6)
7. Сорокин А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. – Курган, 1999. [↑](#footnote-ref-7)
8. Батурин Ю.М*.* Проблемы компьютерного права. — М.: Юрид. лит., 1991. [↑](#footnote-ref-8)
9. Гульбин Ю. Преступления в сфере компьютерной информации. // Российская юстиция. - 1997г. - №10. [↑](#footnote-ref-9)
10. Постатейный Комментарий к Уголовному кодексу РФ 1996г. / Под ред. А. В. Наумова. – М.: Юристъ, 1996. [↑](#footnote-ref-10)
11. Федеральный закон от 20 февраля 1995г. № 24-ФЗ «Об информации, информатизации и защите информации». [↑](#footnote-ref-11)
12. Постатейный Комментарий к Уголовному кодексу РФ 1996г. / Под ред. Наумова А.В. – М.: Юристъ, 1996. [↑](#footnote-ref-12)
13. Голубев В.В. Компьютеризация и уголовное право. // Законодательство. - 1999г. - № 8. [↑](#footnote-ref-13)
14. Федеральный закон от 20 февраля 1995г. № 24-ФЗ «Об информации, информатизации и защите информации». [↑](#footnote-ref-14)
15. Уголовное право России. Особенная часть: Учебник. / Отв. ред. Б.В. Здравомыслов. - М.: Юристъ, 1996. - С. 352. [↑](#footnote-ref-15)
16. <http://narod.zaural.ru/procur/delo7.htm> [↑](#footnote-ref-16)