### МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ

### РОССИЙСКОЙ ФЕДЕРАЦИИ

### Уфимский юридический институт

### ИСПОЛЬЗОВАНИЕ ВЫСОКИХ ТЕХНОЛОГИЙ КРИМИНАЛЬНОЙ СРЕДОЙ. БОРЬБА С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

### Учебное пособие

На правах рукописи

### В.А. Дуленко, Р.Р. Мамлеев, В.А. Пестриков

Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации: Учебное пособие. – Уфа: УЮИ МВД России, 2007. – 187 с.

### Уфа 2007

### В учебном пособии рассматриваются понятие, значение и возможности современных технологий. Приводится определение предметной области «высокие технологии». Анализируются виды и особенности высоких технологий. Содержится уголовно-правовая и криминалистическая характеристика преступлений в сфере высоких технологий. Рассматриваются актуальные задачи в области профилактики, выявления и экспертной оценки противоправных действий в области высоких технологий.

### Отдельно рассматриваются преступления в сфере компьютерной информации, а также методы и средства их фиксации и расследования.

Учебное пособие предназначено для сотрудников и руководителей правоохранительных органов, курсантов, студентов, слушателей юридических вузов и учебных центров МВД России, адъюнктов и аспирантов, преподавателей.

ОГЛАВЛЕНИЕ

Введение

РАЗДЕЛ 1. ИСПОЛЬЗОВАНИЕ ВЫСОКИХ ТЕХНОЛОГИЙ КРИМИНАЛЬНОЙ СРЕДОЙ

Глава 1. Терминология, объекты и субъекты высоких технологий

1.1 Понятие «технология»

1.2 Эволюция понятий «технология» и «техника»

1.3 Информационная технология

1.4 Сфера высоких технологий

1.4.1 Понятие и сущность компьютерной информации

1.4.2 Классификация информации

1.4.3 Свойства и признаки информации

Глава 2. Общие сведения о технических системах обработки информации

2.1 Основные понятия и определения

2.2 Особенности телекоммуникационных систем

2.3 Технические особенности информационно-технологических систем

2.4 Подсистема обеспечения информационной безопасности

Глава 3. Понятие и сущность преступлений в сфере высоких технологий

3.1 Понятие компьютерного преступления

3.2 Субъекты компьютерных преступлений

3.3 Особенности квалификации преступлений в сфере компьютерной информации

3.4 Проблемы уголовно-правовой квалификации преступлений в сфере высоких технологий

Глава 4. Теоретические основы классификации преступлений в сфере высоких технологий

4.1 Обзор отечественного и международного опыта

4.1.1 Международная классификация

4.1.2 Классификация компьютерных преступлений в соответствии с законодательством России

4.2 Преступления в сфере телекоммуникаций

4.3 Особенности криминального использования компьютерной техники в экономической сфере и материальном производстве

4.3.1 Подлог документированной информации фискальных систем

4.3.2 Преступления в сфере безналичных расчетов

4.3.3 Преступления в сети Интернет

4.3.4 Применение полиграфических компьютерных технологий

4.4 Неправомерный доступ к компьютерной информации

4.5 Создание, использование и распространение вредоносных программ для ЭВМ

4.6 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

РАЗДЕЛ 2. БОРЬБА С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Глава 5. Контроль над преступностью в сфере высоких технологий

5.1 Контроль над компьютерной преступностью в России

5.2 Уголовно-правовой контроль над компьютерной преступностью в России

5.3 Особенности оперативно-разыскнойдеятельности при расследовании преступлений в сфере высоких технологий

Глава 6. Расследование преступлений в сфере компьютерной информации

6.1 Основные следственные версии, выдвигаемые при расследовании преступлений в сфере компьютерной информации

6.2 Методика расследования преступлений в сфере компьютерной информации

6.3 Типичные следственные ситуации и действия следователя на первоначальном этапе расследования преступлений в сфере компьютерной информации

Глава 7. Особенности тактики расследования преступлений в сфере компьютерной информации

7.1 Осмотр места происшествия

7.2 Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг сети Интернет

7.3 Осмотр средств вычислительной техники

7.4 Осмотр документов и их носителей

Глава 8. Назначение компьютерно-технических экспертиз при расследовании преступлений в сфере высоких технологий

8.1 Механизм следообразования в компьютерных средствах и системах

8.2 Типовые следообразующие признаки преступной деятельности в сфере телекоммуникации

8.3 Экспертные исследования

8.3.1 Объекты компьютерно-технической экспертизы

8.3.2 Вопросы, выносимые на разрешение компьютерно-технической экспертизы

8.3.3 Перечень вопросов, разрешаемых при исследовании носителей машинной информации

8.3.4 Перечень вопросов, разрешаемых при исследовании программного обеспечения

8.3.5 Перечень вопросов, разрешаемых при исследовании баз данных

8.3.6 Перечень вопросов, разрешаемых при исследовании аппаратного обеспечения ЭВМ

Глава 9. Предупреждение преступлений в сфере высоких технологий

9.1 Организационно-технические меры предупреждения компьютерных преступлений

9.2 Правовые меры предупреждения компьютерных преступлений

Заключение

Литература

Словарь специальных терминов

# Введение

Современное состояние мирового сообщества характеризуется интенсивным развитием телекоммуникаций и компьютерных технологий, всеобъемлющим проникновением современных информационных технологий в различные области человеческой деятельности. Мир вступил в эру информатизации, и это наглядно проявляется в следующем:

- информация и информационные ресурсы стали важнейшим высокотехнологичным продуктом;

- фирмы, разрабатывающие автоматизированные информационные технологии (ИТ), занимают ведущие позиции в мировой экономике, определяют дальнейшие направления развития конкурентоспособной продукции;

- без информатизации невозможно создание высоких технологий;

- ИТ открывают новые возможности в повышении эффективности производственных процессов, сфере образования и быта, они выводят на новый уровень автоматизацию технологических процессов и управленческий труд, обеспечивают интернет-технологии и т.д.;

- развитие информатизации ведет к интернационализации производства[[1]](#footnote-1).

Приоритет в развитии общественных отношений все более зависит от степени разработанности и использования новых технологий, выраженных как результат совокупного использования «многих изобретений, усовершенствований и приспособлений, продукт творческой деятельности в прошлом и настоящем»[[2]](#footnote-2). Область применения не ограничивается техническими объектами и материальными благами, созданными человеком для удовлетворения потребностей, но в не меньшей степени включает сферу услуг, культуры, образования, науки, обороны, безопасности и политики.

Сегодня результаты научных исследований и их практического использования являются материальным воплощением экономической мощи государства. «Стратегические цели и задачи развития России могут быть достигнуты только при условии перехода на новое качество экономического роста с опорой на применение высоких технологий в промышленности… Высокие технологии, развитая высокотехнологическая промышленность, высокий уровень фундаментальных и прикладных исследований – залог развития благосостояния народа, безопасности и процветания государства. … Роль государства заключается, прежде всего, в создании единого комплекса институциональных (правовых, организационных, финансовых и т. д.) условий, благоприятных для развития и практического использования научно-технического потенциала страны»[[3]](#footnote-3).

Важность развития сферы высоких технологий подразумевает, что вопросы внедрения передовых научных открытий и связанные с ними процессы разработки, производства и реализации конечных продуктов требуют не только капиталовложений, но и их надежной правовой защиты. Это, прежде всего, относится к высшим достижениям в каждой из проблемных отраслей, особенно когда мы имеем дело с объектами телекоммуникаций, нанотехнологий и т.п., тем более, что в сфере современных технологий, как и в любой другой сфере человеческой деятельности, существует и успешно реализуется возможность совершения преступных действий с целью получения моральной, материальной или политической выгоды. Это обстоятельство привело к тому, что в правоохранительной деятельности утвердился даже термин, характеризующий подобные нарушения законности – «преступления в сфере высоких технологий». Фактически это произошло в конце 90-х годов, когда приказом министра МВД России по всей стране были созданы отделы «Р».

Наступил новый век, однако терминология, квалификационные признаки преступлений в сфере высоких технологий в законодательной практике России размыты, многие определения либо отсутствуют, либо допускают произвольные толкования, что вызывает вполне обоснованное стремление специалистов различных областей права исследовать проблему в свете последних достижений криминологии, криминалистики, уголовного и административного права и т.д. Однако единой точки зрения на проблему, систему терминов и устоявшихся уголовно-правовых норм до сих пор не выработано, хотя многие аспекты уголовно-правовых и криминалистических вопросов раскрытия и расследования преступлений, совершенных в сфере компьютерной информации, были рассмотрены в работах Ю.М. Батурина (1987), А.М. Жодзишского (1991), Н.С. Полевого (1993), В.Б. Вехова, С.П. Серебровой (1996), А.В. Касаткина (1997), Б.Х. Толеубековой, А.В. Макиенко, В.Ю. Рогозина (1998), А.В. Сорокина (1999), В.В. Крылова (1997-1999), Ю.В. Гаврилина (2000-2003), В.А. Мещерякова (2001), Е.Р. Россинской (1996-2001), Т.В. Аверьяновой (1999-2001), А.И. Усова (2002), С.А. Хвоевского (2004-2006), И.В. Лазаревой (2005-2007). Не умаляя бесспорную теоретическую значимость всех указанных выше и ряда других исследований и работ, следует констатировать, что существующие различные точки зрения и противоречивые взгляды ученых на общетеоретические и практические основы указанной проблемы до сих пор остаются неразрешенными.

Существующие тенденции криминальной ситуации в современной России, а также прогнозы ее развития характеризуются широким использованием высоких технологий при совершении преступлений и поэтому, чтобы эффективно бороться с преступностью, сотрудники органов внутренних дел должны обладать необходимым набором знаний в области использования высоких технологий криминальной средой, а также действенными методами для раскрытия и пресечения преступлений в сфере компьютерной информации.

Учебное пособие предназначено для сотрудников и руководителей правоохранительных органов, курсантов, студентов, слушателей юридических вузов и учебных центров МВД России, адъюнктов и аспирантов, преподавателей.

# РАЗДЕЛ 1. ИСПОЛЬЗОВАНИЕ ВЫСОКИХ ТЕХНОЛОГИЙ

# КРИМИНАЛЬНОЙ СРЕДОЙ

## ГЛАВА 1. ТЕРМИНОЛОГИЯ, ОБЪЕКТЫ И СУБЪЕКТЫ ВЫСОКИХ

## ТЕХНОЛОГИЙ

1.1 Понятие «технология»

Попыткой устранить предпосылки возникновения противоречий в области расследования преступлений в сфере высоких технологий может явиться выработка единого понятийного аппарата – терминологии, при этом условимся, что само определение «высокие технологии» не «вещь в себе», а продукт человеческой деятельности в научной и производственной деятельности.

Термин «технология» трактуется в большинстве энциклопедических изданиях как совокупность приемов и способов получения, обработки или переработки сырья, материалов, полуфабрикатов или изделий, осуществляемых в различных отраслях промышленности, а также научно обоснованные приемы и способы их получения (обработки, переработки и хранения), которые являются основной составной частью производственного процесса, включая инструкции и наставления по его проведению.

Более узкую и несколько иную по содержанию трактовку дают авторы политехнического словаря: «Технология … совокупность методов обработки, изготовления, изменения состояния, свойств, формы сырья, материала или полуфабриката, применяемых в процессе производства, для получения готовой продукции, … наука о способах воздействия на сырье, материалы и полупродукты соответствующими орудиями производства».

Сравнивая данные формулировки предмета обсуждения, можно говорить о различных принципах подхода к обобщающим определениям. Так, например, в «Большой советской энциклопедии» технология понимается довольно широко и делится на объективную (действующую, функционирующую в различных отраслях народного хозяйства) и субъективную (научную). При анализе практической технологии ее нельзя оторвать от техники и средств труда. Из этого следует, что понятие «современная технология» неоднозначно по своей сути и имеет несколько аспектов. Важнейшие из них – объективный и субъективный.

Таким образом, мы сталкиваемся с проблемой объективного и субъективного в технологии, то есть с практической и теоретической технологиями. Может быть, именно в этом скрыта причина различного толкования термина в энциклопедических изданиях и отсутствия каких либо единых подходов в оценке противоправных действий физических или юридических лиц, совершенных или подготавливаемых с использованием современных технологий.

Так, например, в Законе РФ «О правовой охране топологий интегральных микросхем» понятие «технология» означало[[4]](#footnote-4) сугубо научный аспект «4. Правовая охрана, предоставляемая настоящим Законом, не распространяется на идеи,… технологию или закодированную информацию, которые могут быть воплощены в топологии», а в постановлении Правительства РФ от 11 ноября 2002 г. № 817 «Об утверждении положения о лицензировании деятельности по изготовлению защищенной от подделок полиграфической продукции…» утверждается о практическом характере этого термина как законченного цикла «работ, включающего… технологию печати… с использованием высокозащищенных трудновоспроизводимых технологий производства защитных элементов».

В УК РФ в устранение разночтения термина «технология» (в вопросах предотвращения незаконного экспорта вооружений), понятия «…оборудование, технологии, научно-техническая информация, незаконное выполнение работ…» просто перечислены, как взаимодополняющие.

Обращаясь к Постановлению Правительства «О контроле за выполнением обязательств по гарантиям использования импортируемых и экспортируемых товаров и услуг двойного назначения в заявленных целях»[[5]](#footnote-5), можно говорить о технологиях как о конечных результатах труда – товарах, под которыми законодатель подразумевает «сырье, материалы, оборудование, научно-техническая информация, работы, … результаты интеллектуальной деятельности, которые могут быть использованы при создании оружия…, иных видов вооружения и военной техники».

Таким образом, очевидно, что технологии в отечественной законодательной практике отмечены одновременно и как способ, и как средство, и как результат производственной деятельности. Что же объединяет в правовом поле термин в его различных ипостасях? На наш взгляд, объединяющим является высокая степень использования научных знаний, что и вызвало появление порождаемого понятия «высокие технологии».

Период развития общества принято обозначать в терминах главенствующей технологии: «каменный» и «железный» века вполне объясняют достигнутый пик технологии производства как способа, средства и результата производственной деятельности. В начале работы мы в который раз подчеркнули, что 21 век – век информации, это «камень/железо» эпохи. Здесь и сырье, и инструмент, и товар, без которого современный рынок не намного отличается от предшествующих периодов развития человечества. Попутно отметим, что помимо криминального интереса, этот «двигатель прогресса» удостоен и военного назначения: «чем выше технологические возможности государства и чем больше число его взаимодействий с другими группами (включая внутренние группы) или государствами, тем более государство уязвимо в информационной войне»[[6]](#footnote-6).

Предпосылка такого положения вещей – объективно существующий факт наличия технологий, достижимых только при использовании современных наукоемких способов производства. По нашему мнению, изучение и выявление особенностей организации производства товаров и услуг, при использовании «высоких технологий», даст возможность эффективно препятствовать их противоправному применению, в том числе и на законодательном уровне.

1.2 Эволюция понятий «технология» и «техника»

Понятие «технология» впервые появилось в Европе по одним источникам – в 1772 г., по другим – в 1777 г. В отечественную научную литературу данный термин проник лишь в 1807 г. с выходом первой части учебника по химической технологии И.А. Двигубского «Начальные основания технологии, или краткое показание работ, на заводах и фабриках производимых». С публикацией первого тома книги В.И. Севергина «Начертание технологии минерального царства» (1821 г.), выпуска первого номера сборника «Технологический журнал» (1840 г.) и учебника П.А. Ильенкова «Курс химической технологии» (1851 г.) он утверждается в химии как специальный термин.

В остальных отраслях практической деятельности людей и в науке его заменяли такие термины, как «искусство», «инженерное искусство», «ремесло».

Россия в XVIII в. еще не располагала промышленностью как таковой. Процесс получения товарной продукции называли ремеслами. Лишь с зарождением в конце XVIII – начале XIX в. инженерной деятельности понятие «ремесло» заменяют сначала «делом», затем «искусством» и только в химии «технологией», причем термин «техника», по сути, заменял нынешнее понятие «технология». Под ним часто подразумевали профессиональную, целенаправленную, инженерную либо иную творческую деятельность в определенной области, и лишь в 40-е – 50-е годы 20-го столетия в отечественной литературе происходит дифференциация понятий технология и техника.

Выделение технологии в самостоятельную научную дисциплину, отграничение ее от практической, признание термина как самостоятельного понятия – явление вполне обоснованное, термин же «техника» растворился в первом.

В процессе эволюции понятий «техника» и «технология» можно установить особенности, характеризующие их сущность. Одна из них – объединение объективного и субъективного в приведенных понятиях, вторая – диалектическое единство их объективных частей в процессе развития формы и содержания.

Из этого можно сделать следующие выводы:

- при определении направлений развития общественного производства и экономики в целом отрывать технику от технологии нельзя;

- для изучения законов и закономерностей развития производства и отдельных производственных систем необходимо путем дифференциации технологии раскрыть ее противоположности и установить связь между ними;

- субъективная часть технологии не может быть однозначной, это разносторонняя и разноплановая система;

- содержанием диалектического единства технологии и техники, движущим началом остается технология.

При этом следует учесть, что на всех иерархических уровнях организации технология делится на практическую (объективную), научную и теоретическую (субъективную). С практической технологией непосредственно связана научная, а с научной – теоретическая.

Практическая технология – это отработанная опытом совокупность процессов и операций по созданию определенного вида потребительной стоимости. Данная технология может быть представлена, изображена, описана и т.д. Ее характерные признаки: динамизм, конкретность, материальная обусловленность и логичность (строгая последовательность действий, операций, движений).

Научная технология изучает и обобщает опыт создания потребительных стоимостей. Предмет ее изучения – процессы взаимодействия средств труда, предметов труда и окружающей среды при создании всего многообразия потребительных стоимостей. В области материального производства ее задачи следующие: изучение закономерностей протекания процессов преобразования предметов труда в продукцию или товары; изыскание прогрессивных способов воздействия на предметы труда, их проверка; разработка мероприятий по защите природы; выбор и проектирование наиболее эффективной и безопасной практической технологии.

Теоретическая технология изучает диалектику технологии и возможность использования законов развития природы и общества для преобразования материального и духовного мира человека. Предмет ее исследования – процессы развития познающей и преобразующей деятельности человека. Основные задачи: познание законов взаимодействия человека с природой; изучение возможностей и условий практического применения познанных законов или закономерностей; разработка, обоснование и экспериментальная проверка новых технологических процессов. С этой задачей связано много других проблем, таких как специализация и интеграция, систематизация процессов и их форм, классификация наук, естественных и технологических процессов. Теоретическая технология дала толчок возникновению синергетики, дословно – теории совместного действия, где подразумевается два смысла.

Первый – это подход, рассматривающий возникновение новых качеств у сложных систем, состоящих из взаимодействующих подсистем, которыми сами подсистемы не обладают.

Второй – это направление, развитие которого требует совместных усилий представителей различных научных дисциплин.

Синергетика технологических процессов прочно объединяет естествознание, с которым взаимодействует на низших уровнях (снизу), науку и технику (средние уровни иерархии), экономику, политику и управление (верхние). Технология как основа жизни общества дает те потребительные стоимости, образы которых формирует политика. Экономика, являясь своеобразным проводником и регулятором потоков материальных и духовных ценностей, в условиях глубокого разделения труда стала играть исключительную роль в развитии производительных сил общества. Поэтому разрыв связей между естествознанием, технологией, техникой, экономикой и политикой недопустим.

1.3 Информационная технология

Подлинная технологическая революция связана, прежде всего, с созданием электронно-вычислительных машин в конце 40-х годов, и с этого же времени исчисляется новая эра – эра развития компьютерных технологий[[7]](#footnote-7), материальное ядро которой образует микроэлектроника. Именно успехи микроэлектроники обусловили бурное развитие современных информационных технологий (ИТ) приема, передачи и обработки информации, систем управления и связи:

- ИТ является важнейшим средством реализации так называемого формального синтеза знаний, память компьютера в таких системах представляет собой как бы энциклопедию, вобравшую в себя знания из различных областей;

- фактор научно-теоретического знания приобретает решающее значение для перестройки экономики в сторону наукоемкости (все входящие в этот комплекс отрасли сами по себе наукоемки);

- ИТ является своего рода преобразователем всех других отраслей хозяйства, как производственных, так и непроизводственных, основным средством их автоматизации, качественного изменения продукции и, как следствие, перевода частично или полностью в категорию наукоемких.

Таким образом, в настоящее время именно степень развития ИТ определяет как уровень общественного производства, так и экономику в целом. Однако замечено, что информационная технология сама создает технические средства для своей эволюции. Формирование саморазвивающейся системы – важнейший итог, достигнутый в сфере информационной технологии. Это убедительно доказывает, что отрывать современную технику от технологии нельзя. Однако, на наш взгляд, именно подобное разделение привело к появлению в УК РФ главы 28 «Преступления в сфере компьютерной информации».

Отделение технического средства от технологии приводит к появлению комментариев, содержащих ссылки на федеральные законы (отмененные в настоящее время), например: «Предмет таких преступлений – компьютерная информация, т.е. сведения о лицах, предметах, фактах, событиях, явлениях и процессах, содержащихся в информационных системах» (Федеральный закон «Об информации, информатизации и защите информации»), а также непосредственно сам компьютер как носитель этой информации[[8]](#footnote-8).

Сразу после принятия УК РФ многие авторы отмечают «высокий уровень бланкетности диспозиций 28 главы, так как для конкретизации соответствующих уголовно-правовых запретов необходимо обращаться к ряду законов и других нормативных актов. В первую очередь среди них следует указать Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» 1993 г., Федеральный закон «Об информации, информатизации и защите информации» 1995 г., Закон Российской Федерации «Об авторском праве и смежных правах» 1995 г. (с последующими изменениями), Закон Российской Федерации «О государственной тайне» 1993 г. (с последующими изменениями), Федеральный закон «О связи» 1995 г., Федеральный закон «Об участии в международном информационном обмене» 1996 г., некоторые положения Гражданского кодекса РФ (например, ст. 139 о служебной и коммерческой тайне)»[[9]](#footnote-9).

Усугубляет данное обстоятельство то, что на сегодняшний день кроме закона «О связи» и «О государственной тайне» перечисленные законы утратили силу. Однако сохранившаяся бланкетность принуждает искать объяснения диспозиций в новых законах, вступивших или вступающих в силу с 1 января 2008 г., например: Федеральные законы от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации» и от 27 июля 2006 года № 152–ФЗ «О персональных данных», а так же ФЗ от 18 декабря 2006 г. № 231–ФЗ «О введении в действие части четвертой Гражданского кодекса Российской Федерации». На наш взгляд, термины и определения, изложенные в этих законах, по меньшей мере, не внесли ясности в сферу применения 28 главы УК РФ, видимо следует обратить более пристальное внимание на следующие уголовно-правовые аспекты преступных действий в области высоких технологий:

1) терминологический аппарат, позволяющий однозначно трактовать объекты, субъекты, факты и последствия преступной деятельности в сфере высоких технологий;

2) критерии правомерности и допустимости проведения отдельных следственных действий с целью выявления доказательств совершения преступления в сфере высоких технологий;

3) условия, возможности и критерии оценки компьютерной информации, полученной в качестве доказательственной;

4) методику и тактику проведения следственных действий, проводимых при расследовании дел данной категории;

5) возможный характер (уголовно-правовой аспект) противодействия расследованию, совершенного способом, аналогичным способу совершения преступления (повторность или воспрепятствование расследованию).

### 1.4 Сфера высоких технологий

Нельзя рассматривать вопросы противодействия преступлениям в сфере высоких технологий, не выяснив объект и предмет исследования. Изначально, для борьбы с преступлениями в высокотехнологичной сфере в МВД РФ был создан отдел «Р», основной функцией которого была борьба с незаконным оборотом радиоэлектронных и специальных технических средств – отсюда и буква «Р» («радио»). В то время, когда сотовая связь еще только зарождалась, но уже радиотелефоны и радиоусилители получили широкое распространение, проблема заключалась в прекращении бесконтрольного ввоза в Россию устройств, подлежащих лицензированию и сертификации.

Как оказалось, проблемы в сфере высоких технологий на этом не закончились, так как стремительное развитие получили компьютерные технологии. Всевозможные базы данных, отчеты, переписка и прочие конфиденциальные документы стали лакомым кусочком для тех, кто был сведущ в этой сфере. Это не могло не привести к появлению новых преступлений – в сфере компьютерных технологий. Кардинально изменившиеся условия привели к тому, что отдел «Р» был реорганизован и позже переименован в сложную аббревиатуру УБПСВТ (Управление по борьбе с преступлениями в сфере высоких технологий).

Бурное развитие Интернета и высокая степень анонимности были выгодны киберпреступникам и позволяли в большинстве случаев избежать наказания. В корне изменились не только используемые злоумышленниками средства, но сам контингент преступников. Сегодня зачастую взломом занимаются настоящие профессионалы, люди с высшим образованием и высоким уровнем интеллекта, которых крайне затруднительно поймать и доказать их вину. По всей России управлению приходится заниматься делами по несанкционированному доступу в Сеть, кражами интернет-аккаунтов и т.п. В число основных задач также входит борьба с разработчиками вирусов и фрикерами. На сегодняшний день Управление по борьбе с преступлениями в сфере высоких технологий преобразовано в отдел «К». Основным направлением его работы является борьба с компьютерными преступлениями и незаконным оборотом радиоэлектронных и специальных технических средств.

Конечно, прогресс в движении есть, есть и определенные результаты, но количество и разнообразие видов противоправных действий в рассматриваемой области неуклонно растет. Это привело к возникновению ряда проблем, связанных с их квалификацией, определением наказания, разработкой профилактических и контрольных мер и т.д. Для коренного изменения дел возникла необходимость в анализе и переработке практически всей законодательной и нормативно-правовой базы. В противном случае последствия от противоправных действий в сфере высоких технологий будут носить тяжелый характер.

Такие опасения небезосновательны. Когда работа с информацией/знаниями стала одной из производительных сил общества, появились страны (типа Японии), которые строят свое экономическое благополучие, в значительной степени используя информационную сферу. Иные интересы экономики извлекают другие типы инфраструктур. К примеру, Дж. Сакс в числе объяснений экономических результатов правления Б. Клинтона называет и вложения в науку, и расширение вовлеченности молодых американцев в получение высшего образования. Страна начинает «наращивать иные мускулы», создавая свое благополучие, опираясь на иные сферы. Э. Тоффлер говорит об информации как о сырье: «Для цивилизации Третьей волны одним из главных видов сырья, причем неисчерпаемым, будет информация, включая воображение»[[10]](#footnote-10).

Все это в значительной степени связано с тем, что современное общество вышло на более сложный этап своей организации, требующий для успешного функционирования более совершенных процессов координации, в более серьезной степени опирающийся на информационные процессы.

Примем за аксиому вывод, сделанный из анализа отечественной законодательной практики, что технология – это способ, средство, и результат производственной деятельности, и попробуем определить сферу высоких технологий на основе системного анализа, традиционно применяемого для анализа сложных систем. Системный подход, основанный на теории алгоритмов, позволяет в каждый момент, зная текущее состояние системы, ее правила и доступную ей информацию, предсказать множество ее возможных последующих изменений. Такой подход оправдан тем, что в этой теории «было доказано, что, используя рекурсию, можно из ограниченного количества функциональных единиц получить все многообразие вычислимых функций»[[11]](#footnote-11), иными словами, наша задача – найти ключевые термины, описывающие минимум единичных функциональных компонентов, общих для системы высоких технологий. Осуществимость реализации поставленной задачи дает существование рекурсии. Рекурсия – важнейшее фундаментальное понятие теории алгоритмов. Под рекурсией в общем смысле понимают такой способ организации системы, при котором она в отдельные моменты своего развития, определяемые ее правилами, может создавать (вызывать) собственные измененные копии, взаимодействовать с ними и включать их в свою структуру. При этом кажущиеся различия систем определяются правилами конкретной исследуемой системы.

Широко распространенное понятие «высокие технологии» (англ. high technology, high tech, hi-tech) на самом деле собирательное понятие, и отсутствие четкого и официального определения предполагает, что это наиболее новые и прогрессивные технологии современности. К высоким технологиям в настоящее время относят самые наукоемкие отрасли промышленности. Интегрирующим свойством по отношению как к научному знанию в целом, так и ко всем остальным технологиям обладают информационные технологии.

Исключительно важную роль ИТ оказывают на развитие радиоэлектронных средств (РЭС), которые обеспечивают все виды связи, вычислительные средства, продукцию оборонных промышленных комплексов и других отраслей промышленности. В настоящее время практически нет продукции, включая услуги, которая бы не содержала или не использовала ИТ. Таким образом, информационные технологии вместе с вычислительной техникой являются объединяющей основой высоких технологий.

Особо следует подчеркнуть, что в любой технический объект в настоящее время входят, как обязательная составная часть, специально разработанное математическое обеспечение, а в ряде случаев и банки данных, специально разработанные для проектирования, модификации и эксплуатации объектов, а также оценки их действия (функционирования) и использования. Причем специально разработанное математическое обеспечение, рассматривается как составная часть таких объектов: боеприпасы, транспортные средства, электронное оборудование, криогенное оборудование, лазерные системы, технологические способы металлообработки, блоки числового управления для устройств, оборудования, роботов и т.п.

Необходимо подчеркнуть, что зачастую конечный пользователь, принадлежащий к различным классификационным группам, получает один и тот же продукт с разной комплектацией математического обеспечения, и, следовательно, становится владельцем принципиально разных технологий. Следует пояснить, что зачастую понятие информационных технологий предприятия отождествляются с компьютерными системами, которые данная организация использует[[12]](#footnote-12). Однако компьютерные системы являются лишь частью информационных технологий. Термин «информационные технологии» означает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Законодательно данное утверждение закреплено в Федеральном законе от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации». Здесь хотелось бы отметить, что средства и методы технологии разделены, вследствие чего информационная система определена как «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств», при этом, из трех составляющих компонентов, два – базы данных и технические средства – никак не определены. Столь широкое, некорректное определение позволяет судить, что люди со слуховыми аппаратами являются полноправными информационными системами. По нашему мнению, и что в свое время настоятельно рекомендовали такие ученые, как В.Р.Женило и В.Ф.Макаров, в технических системах (по смыслу Закон касается технических систем) следует оперировать понятием формализованные данные, т.е. информация, преобразованная в изменения параметров материального носителя. Тогда логично использование терминов: техническое средство обработки информации и база данных.

Рассмотрим ряд основных терминов.

1.4.1 Понятие и сущность компьютерной информации

В первую очередь, следует рассмотреть понятие и сущность информации и, в частности, компьютерной информации.

Преступления в сфере компьютерной информации имеют общий предмет преступного посягательства. Им, по мнению подавляющего большинства ученых, является компьютерная информация. Последняя, как вид информации вообще, представляет собой сведения, знания или набор команд (программа), предназначенных для использования в ЭВМ или управления ею, находящихся в ЭВМ или на машинном носителе – идентифицируемом элементе информационной системы, имеющем собственника, установившего правила ее использования.

Разные научные дисциплины вводят понятие информации по-разному. Существует три подхода к определению информации:

1. Антропоцентрический.

2. Техноцентрический.

3. Недетерминированный.

Антропоцентрический подход. Информацию отождествляют со сведениями или фактами, которые могут быть получены и преобразованы в знания.

Техноцентрический подход. Информацию отождествляют с данными.

Недетерминированный подход. Отказ от определения информации на том основании, что оно является фундаментальным, как материя и энергия.

Информация сама по себе в природе не существует, а образуется в ходе взаимодействия данных и методов, а в остальное время пребывает в виде данных.

В соответствии со ст. 2 Закона РФ от 27.07.06 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации»:

- информация – это сведения (сообщения, данные) независимо от формы их представления;

- электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети, где информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

При этом защите подлежит только документированная информация – «это зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель» (ст. 2). Применительно к компьютерной информации, это определение необходимо рассматривать в ракурсе понятия электронного документа – документа, в котором информация представлена в электронно-цифровой форме (ст. 3 Закона РФ от 10.01.02 г. № 1–ФЗ «Об электронной цифровой подписи»).

В соответствии с ч. 1 ст. 272 Уголовного кодекса Российской Федерации компьютерная информация – это информация на машинном носителе, в ЭВМ, системе ЭВМ или их сети.

На основании вышеизложенного, понятие компьютерной информации можно сформулировать следующим образом: компьютерная информация (computer information) – это информация, находящаяся в памяти ЭВМ, зафиксированная на машинных или иных носителях в электронно-цифровой форме, или передающаяся по каналам связи посредством электромагнитных сигналов с реквизитами, позволяющими ее идентифицировать.

Компьютерная информация всегда опосредована через материальный – машинный носитель, вне которого она не может существовать.

1.4.2 Классификация информации

Существует несколько подходов к классификации информации. С точки зрения правоохранительной сферы информацию можно классифицировать следующим образом:

1. По степени доступа:

а) общедоступная информация;

б) информация, доступ к которой не может быть ограничен;

в) информация с ограниченным доступом;

г) информация, не подлежащая разглашению.

2. По степени систематизации:

а) систематизированная в информационной системе (каталоге, энциклопедии);

б) несистематизированная (свободная).

3. По виду носителя:

а) документированная – зафиксированная на каком-либо материальном носителе;

б) недокументированная – устная или передаваемая по различным каналам связи.

4. По сфере применения:

а) массовая информация;

б) отраслевая информация, предназначенная для определенного круга лиц, связанная с профессиональными интересами.

1.4.3 Свойства и признаки информации

Информация имеет определенные свойства и признаки.

Рассмотрим основные свойства информации.

Адекватность информации – это степень соответствия реальному объективному состоянию дела. Неадекватная информация может образовываться при создании новой информации на основе неполных или недостоверных данных. Однако и полные, и достоверные данные могут приводить к созданию неадекватной информации в случае применения к ним неадекватных методов.

Достоверность информации. В момент регистрации сигнала не все сигналы являются полезными, присутствует уровень посторонних сигналов – «информационный шум». При увеличении уровня шумов достоверность снижается. В этом случае при передаче того же количества информации требуется использовать либо больше данных, либо более сложные методы.

Актуальность информации – степень соответствия информации текущему моменту времени. Нередко с актуальностью, как и с полнотой, связывают коммерческую ценность информации. Поскольку информационные процессы растянуты во времени, то достоверная и адекватная, но устаревшая информация может приводить к ошибочным решениям. Необходимость поиска (или разработки) адекватного метода для работы с данными может приводить к такой задержке получения информации, что она становится неактуальной и ненужной. На этом, в частности, основаны многие современные системы шифрования данных с открытым ключом. Лица, не владеющие ключом (методом) для чтения данных, могут заняться поиском ключа, поскольку алгоритм его работы доступен, но продолжительность этого поиска столь велика, что за время работы информация теряет актуальность и, естественно, связанную с ней практическую ценность.

Доступность информации – мера возможности получить ту или иную информацию. Отсутствие доступа к данным или отсутствие адекватных методов обработки приводят к одинаковому результату: информация оказывается недоступной.

Избыточность – это свойство, полезность которого человек ощущает очень часто, как качество, которое позволяет ему меньше напрягать свое внимание и меньше утомляться. Обычный текст на русском языке имеет избыточность 20-25%. Попробуйте отбросить каждую пятую букву и вы увидите, что получить информацию из печатного текста все же можно , хотя читать его будет очень утомительно. Видеоинформация имеет избыточность до 98-99%, что позволяет нам рассеивать внимание и отдыхать при просмотре кинофильма.

Объективность информации. Понятие объективности информации является относительным, это понятно, если учесть, что методы являются субъективными. Более объективной принято считать ту информацию, в которую методы вносят меньший субъективный элемент. Так принято считать, что в результате наблюдения фотоснимка природного объекта или явления образуется более объективная информация, чем в результате наблюдения рисунка того же объекта выполненного человеком.

Полнота информации во многом характеризует ее качество и определяет достаточность данных для принятия решений или для создания новых данных на основе имеющихся. Чем полнее данные, тем шире диапазон методов, которые можно использовать, тем проще подобрать метод, вносящий минимум погрешностей в ход информационного процесса.

Полезность или бесполезность информации. Так как границы между этими понятиями нет, то следует говорить о степени полезности применительно к нуждам конкретных людей. Полезность информации оценивается по тем задачам, которые человек может решить с ее помощью.

Понятность информации. Информация понятна, если она выражена на языке, доступном для получателя.

Любая информация обладает рядом признаков.

Приведем основные характерные признаки информации:

1. Информация имеет нематериальный характер, т.е. она самостоятельна по отношению к носителю, ценность в ее сути.

2. Информация носит субъективный характер – информация возникает в результате деятельности человека.

3. Информации присуща количественная определенность.

4. Возможность многократного использования информации.

5. Сохранение передаваемой информации и передающего субъекта.

6. Способность к воспроизведению, копированию, сохранению, накапливанию.

Основные криминалистические особенности компьютерной информации:

1. Компьютерная информация 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 ЭВМ «Интернет», доступ к которой одновременно имеют несколько пользователей.

Определим также следующие термины.

Формализованные данные – информация, преобразованная в соответствующие изменения параметров материального носителя.

База данных – структурированная совокупность формализованных данных.

Техническое средство обработки информации – средство для приема, преобразования и обработки информации в виде формализованных данных.

Информационные технологии – технические средства сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов, включая автоматизированную обработку.

Информационная система – совокупность информации, содержащейся в базах данных и обеспечивающих ее обработку информационных технологий.

Таким образом, можно констатировать, что высокие технологии – это способы, средства и результаты производственной деятельности, основанные на использовании информационных технологий.

По определению видно, что категориям высоких технологий соответствуют средства и способы производственной деятельности, связанные с использованием информации, недоступной естественным органам чувств человека по пространственно-временным характеристикам. К отраслям высоких технологий относятся: микроэлектроника, оптоэлектроника, телекоммуникация, вычислительная техника, робототехника, нанотехнологии, энергетика, авиационно-космическая техника, биотехнологии, генная инженерия, и т.п.

Особенности информационных технологий теория передачи (приема) информации[[13]](#footnote-13) объясняет наличием двух основных свойств информации:

- любая информация может быть передана от одного объекта (источника) другому (приемнику) в виде, например, сообщения;

- любое сообщение может быть измерено в виде объема переданной информации.

С учетом теории познания, утверждающей, что человек является «приемником», способным «познавать и изменять мир», то есть является субъектом[[14]](#footnote-14), соответственно качество и полнота воспринимаемой информации имеют достаточно субъективные характеристики, в отличие от количества, которое может выражаться вполне определенно: бит, слово, символ, число импульсов и т.п.

Таким образом, основная задача информационных технологий – обеспечение оптимального взаимодействия субъекта с объектами информатизации для получения желаемых результатов. Особую актуальность эта задача имеет сегодня, когда во всем мире затраты на используемую в информационной сфере технику растут (при снижение цен на компьютеры), а эффективность использования ее возможностей остается на низком уровне.

Объясняется это отчасти низкой компетентностью субъектов производственных отношений, халатностью при выполнении технологических операций, отсутствием или деформацией систем моральной и/или материальной ответственности, изъянами в организации правовых и организационных мер защиты производства. При этом устранению перечисленных (объективных) причин совершения преступлений мешает неполное или искаженное представление или описание сути явлений и процессов, сопутствующих обработке информации с помощью технических средств.

Контрольные вопросы

1. Что такое «технология»?

2. Как соотносятся понятия «техника» и «технология»?

3. Как определяются понятия «информационные технологии» и «высокие технологии»?

4. Охарактеризуйте основные подходы к определению понятия «информация».

5. Что такое «компьютерная информация»?

6. По каким признакам классифицируется информация?

7. Каковы основные свойства и признаки информации?

8. Дайте определение понятиям: «формализованные данные», «база данных», «техническое средство обработки информации», «информационная система».

##

## ГЛАВА 2. ОБЩИЕ СВЕДЕНИЯ О ТЕХНИЧЕСКИХ СИСТЕМАХ ОБРАБОТКИ ИНФОРМАЦИИ

## 2.1. Основные понятия и определения

Система терминов является азбукой любой науки. Поэтому изучение науки об управлении целесообразно начать с рассмотрения основных понятий.

Основное назначение технических систем обработки инфрмации – «получение одних информационных объектов из других информационных объектов путем выполнения некоторых алгоритмов. Информационными объектами называются предметы, процессы, явления материального или нематериального свойства, рассматриваемые с точки зрения их информационных свойств»[[15]](#footnote-15).

Обмен информацией происходит в форме сообщений (от источника к ее приемнику) посредством установления канала связи между ними. Источник посылает передаваемое сообщение, которое кодируется в передаваемый сигнал. Этот сигнал посылается по каналу связи. В результате в приемнике появляется принимаемый сигнал, который декодируется и становится принимаемым сообщением[[16]](#footnote-16).

Сообщением называется информация, воплощенная и зафиксированная в некоторой материальной форме. Сообщения могут быть непрерывными (аналоговыми) и дискретными (цифровыми).

Аналоговое сообщение представляется некоторой физической величиной (электрическим напряжением, током и др.), изменения которой во времени отображают протекание рассматриваемого процесса, например, изменения температуры.

Дискретные сообщения состоят из фиксированного набора элементов, из которых в некоторые моменты времени формируются различные последовательности. Важным является не физическая природа элементов, а то обстоятельство, что набор элементов конечен и поэтому любое дискретное сообщение конечной длины передает конечное число значений некоторой величины.

Элементы, из которых состоит дискретное сообщение, называют буквами или символами. Набор этих букв образует алфавит. Здесь под буквами в отличие от обычного представления понимаются любые знаки (обычные буквы, цифры, знаки препинания, математические и прочие знаки), используемые для представления дискретных сообщений[[17]](#footnote-17).

Процесс совершенствования производства, характеризующийся, прежде всего, уменьшением потока информации, поступающей от человека к объекту управления получил название автоматизации производства[[18]](#footnote-18).

Под производством следует понимать создание не только материальных ценностей, но и духовных – образование и наука; денежных средств – банковская деятельность и торговля; здоровья – медицина и т.д., то есть производство включает в себя любую деятельность человека, связанную с производством продуктов и услуг.

Таким образом, в технических системах обработки информация является одновременно и исходным «сырьем», и конечным «продуктом» функционирования. Преобразования информации, происходящие в них, полностью зависят от полноты и качества исходных данных, а конечный результат определяет степень реализации и результативность применения технических средств.

Каждое из перечисленных условий в том или ином виде технических систем обработки информации (ТСОИ) накладывает ограничения на реально доступную информацию и, следовательно, изменяет информационную среду, в которой реализуются в общем случае четыре основных процесса (процедуры): прием, передача, хранение и обработка информации. Реализация всех этих процедур, как правило, сопровождается преобразованием физического носителя информации и формы ее представления.

В настоящее время высокий уровень развития электронной техники определяет в качестве основного (наиболее распространенного) вида связей между компонентами ТСОИ электрические цепи. Поэтому в большинстве из них физическую структуру разнообразных информационных процессов (ИП) преобразуют в соответствующие изменения параметров электрического тока. В частности, преобразование оптического сигнала в электрический и наоборот выполняют при помощи различных оптоэлектронных устройств.

Сигнал – это процесс изменения во времени некоторого физического параметра s(t) какого-либо объекта, служащий для отображения, регистрации и передачи сообщения.

Таким образом, информация, воплощенная и зафиксированная в некоторой материальной форме, называется сообщением, а физическое средство передачи сообщения – сигналом.

В современных ТСОИ в качестве физических носителей информации используются электрические сигналы двух видов – непрерывные (аналоговые) и дискретные (цифровые). Причем зачастую при обработке информации осуществляются множественные преобразования сигналов из одного вида в другой, в частности, при изменении носителя информации или вида обрабатываемой информации. Процедура смены вида сигнала (перекодировки) должна обязательно учитывать выполнение внутрисистемных правил, обеспечивающих однозначное соответствие между входной и выходной функцией. В случае непрерывного входного сигнала чаще всего первой процедурой изменения типа сигнала является его дискретизация[[19]](#footnote-19).

Преобразование непрерывных сообщений в цифровые получило название аналогово-цифровое преобразование (АЦП), справедливо и обратное преобразование ЦАП. Таким образом, любое сообщение может быть представлено в цифровой форме. В общем случае процесс преобразования информации в форму, отличной от исходной, называется кодированием (формализацией информации). При формализации устраняется избыточность информации, которая имела бы место при использовании естественных языков[[20]](#footnote-20). Особенно наглядно функции формализации проявляются в процессе взаимодействия человека с техническими средствами коммуникации.

Так, например, обратив внимание на особенности процессов обмена информацией между человеком и различными компонентами системы телефонной связи, реализующих информационный процесс передачи речевого сообщения, видно, что компоненты информационной системы (1-8) связаны между собой кодерами сообщения (10, 12, 14), формализующими различные формы информации (9, 11, 13, 15) в соответствии с особенностями различных каналов связи (2-3-4, 4-5-6, 6-7-8) (см. рис. 1).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| человек | ТЛФ | линия связи | АТС 1 | тракт связи | АТС 2 | линия связи | ТЛФ |
| звук | микрофон | электрические колебания | АЦП | цифровыеданные | ЦАП | электрические колебания |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |

Рис. 1. Пример организации информационной системы передачи речи

На примере телефонного канала связи просто обосновать еще несколько терминов, зачастую воспринимаемых как синонимы – линия и канал связи.

Линия (тракт) связи – совокупность технических средств, которые используются для обеспечения распространения сигналов в нужном направлении. Как правило, в линию связи, кроме среды распространения, входят сигналообразующие устройства, коммутационные элементы, усилители и переходники, а также системы защиты линий от влияния помех распространению сигнала.

Канал связи – совокупность линий связи, приемного и передающего оборудования, предназначенных для обмена информационными сообщениями.

Правила, нормы и стандарты взаимодействия различных компонентов информационной системы объединены понятием интерфейс.

Интерфейсом называется совокупность технических средств и правил взаимодействия, обеспечивающих информационное взаимодействие между компонентами информационной системы. Правила обмена, характерные для организации отдельного интерфейса связи, носят название «протокола» связи.

Процессы преобразования исходных данных по заданному алгоритму (последовательности арифметических и логических операций, которые надо произвести над исходными данными и промежуточными результатами для получения требуемого результата) можно автоматизировать, если иметь программу действий, где и какие следует произвести операции, в каком порядке и над какими словами.

Описание алгоритма, предназначенного для управления процессом обработки формализованных данных, называется программой. Для организации полного цикла программной обработки данных в состав цифровой вычислительной системы входят следующие основные устройства[[21]](#footnote-21): арифметическо-логическое устройство, память, устройство управления, устройства ввода данных в машину и вывода из нее результатов расчета. Такая организация вычислительного устройства получила название ЭВМ.

С начала 1990-х годов термин ЭВМ вытеснил термин «компьютер», который в свое время (в 1960-х годах) заменил понятие «цифровая вычислительная машина» (ЦВМ). Все эти три термина в русском языке считаются равнозначными. Слово «компьютер» является транскрипцией английского слова computer, что означает вычислитель.

Компьютер[[22]](#footnote-22) представляет собой программируемое электронное устройство, способное обрабатывать данные и производить вычисления, а также выполнять другие задачи манипулирования символами[[23]](#footnote-23).

Основным формальным отличием компьютера от классического термина ЭВМ является наличие объединенного компонента процессора, состоящего из арифметическо-логического устройства (АЛУ) и устройства управления (УУ).

Та часть процессора, которая выполняет команды, называется АЛУ, а другая его часть, выполняющая функции управления устройствами, называется УУ. Обычно эти два устройства выделяются чисто условно, конструктивно они не разделены.

В составе современных процессоров имеется ряд специализированных дополнительных ячеек памяти (встроенная кэш-память), называемых регистрами. Регистр выполняет функцию кратковременного хранения числа или команды. Над содержимым некоторых регистров специальные электронные схемы могут выполнять некоторые манипуляции. Например, «вырезать» отдельные части команды для последующего их использования или выполнять определенные арифметические операции над числами.

Основными функциями процессора являются обработка данных по заданной программе путем выполнения арифметических и логических операций и программное управление работой устройств компьютера.

Программа, фактически управляющая процессором – это последовательность двоичных чисел (единиц и нулей). Такой тип программ иногда называют машинным (объектным) кодом, что отличает его от программ, записанных программистом на языке высокого уровня (исходными кодами). Поэтому для преобразования исходных кодов в машинные требуются специальные программы – трансляторы[[24]](#footnote-24).

Транслятор (англ. translator – переводчик) – это программа-переводчик. Она преобразует программу, написанную на одном из языков высокого уровня, в программу, состоящую из машинных команд. Трансляторы реализуются в виде компиляторов или интерпретаторов. С точки зрения выполнения работы компилятор и интерпретатор существенно различаются.

Компилятор (англ. compiler – составитель, собиратель) читает всю программу целиком, делает ее перевод и создает законченный вариант программы на машинном языке, который затем и выполняется.

Интерпретатор (англ. interpreter – истолкователь, устный переводчик) каждый раз переводит и выполняет программу строка за строкой, поэтому откомпилированные программы работают быстрее, но интерпретируемые проще исправлять и изменять.

В настоящее время все программы, работающие на компьютере, можно условно разделить на три категории:

1) прикладные программы, непосредственно обеспечивающие выполнение необходимых пользователю работ;

2) системные программы, выполняющие базовые операции загрузки, преобразования и выгрузки машинных кодов в процессор, обеспечивающие такие функции как, например:

- управление ресурсами компьютера;

- передача управления прикладным задачам;

- создание копий используемой информации;

- проверка работоспособности устройств компьютера;

- выдача справочной информации о компьютере и др.;

3) инструментальные программные системы, облегчающие процесс создания новых программ для компьютера.

Самая важная системная программа – это операционная система (ОС) – программа, определяющая систему команд, распределение ресурсов и формат данных, которые обеспечивают две основные задачи: взаимодействие пользователя с компьютером и управление имеющимися ресурсами (логическими и физическими).

Операционная система, как правило, содержит следующие основные компоненты:

- процессор командного языка, который принимает, анализирует и выполняет команды, адресованные операционной системе;

- программы управления вводом/выводом (драйверы устройств);

- программы, управляющие файловой системой (способом и средствами для организации хранения файлов на материальном носителе).

Командный процессор операционной системы определяет способ выполнения анализа и исполнения команд пользователя, включая загрузку готовых программ из файлов в оперативную память и их запуск.

Для управления внешними устройствами компьютера используются специальные системные программы – драйверы. Драйверы стандартных (обязательных) устройств образуют в совокупности с минипрограммой тестирования наличия и исправности компонентов базовую систему ввода-вывода (BIOS), которая заносится в постоянное ЗУ при изготовлении сборочной кросс-платформы (материнской платы) компьютера.

Файл (англ. file – папка) – это именованная совокупность любых данных, размещенная на внешнем запоминающем устройстве и хранимая, пересылаемая и обрабатываемая как единое целое. Файл может содержать программу, числовые данные, текст, мультимедийную информацию и т.п..

Термин «мультимедиа» – собирательное понятие для различных компьютерных технологий, при которых используется несколько информационных сред, таких, как графика, текст, видео, фотография, движущиеся образы (анимация), звуковые эффекты, высококачественное звуковое сопровождение. В первом приближении его можно перевести как «многосредность»[[25]](#footnote-25).

Прикладная программа – это программа, используемая для выполнения различных специализированных задач. Например: автоматизированные системы бухгалтерского учета, системы управления базами данных, программы – редакторы мультимедийной информации.

Инструментальные программы служат для создания и адаптации прикладных программ и операционных систем. В настоящее время существуют целые системы программирования, предназначенные для разработки новых программ на языках программирования. Такие системы обычно предоставляют пользователям интегрированные наборы средств, включающих: компилятор, интерпретатор, среду разработки, библиотеки стандартных программ и функций, отладочные программы, встроенный ассемблер и т.п.

Перечисленные подходы к технической и программной реализации обработки формализованной информации в силу универсальности нашли широкое применение в различных сферах производственной деятельности, однако существуют области, где специфические требования к характеристикам, габаритам, набору фиксированных алгоритмов делают применение универсальных конфигураций компьютера неэффективным. В таких случаях используют специализированные микропроцессоры и микро-ЭВМ, с задаваемыми при изготовлении (или сборке) связями, алгоритмами и выполняемыми задачами, получившими название микроконтроллеров. Обычно микроконтроллеры выполняют специфические задачи управления техническими устройствами, алгоритмического преобразования формализованных данных, контроля и коррекции состояния информационных ресурсов и т.п.

### 2.2 Особенности телекоммуникационных систем

Развитие технических средств обработки информации не только стирает грани различия в различных технологиях, связанных со сбором, обработкой, передачей и хранением информации. Рост вычислительных возможностей одновременно с повышением доступности компьютерных средств обработки вызывает их слияние не только со средствами связи и управления производством, но и практически со всеми сферами жизнедеятельности человека. Поэтому классификация информационных технологий может проводиться по назначению, степени интегрированности в производственные процессы, области применения, степени автоматизации процессов, пространственно-временным характеристикам, форме и содержанию информационных ресурсов. Тем не менее, при всех различиях, в той или иной степени в каждой из них (при выполнении требований производственной эффективности) присутствуют три основных составляющих: телекоммуникационная, информационно-технологическая и обеспечения информационной безопасности. Важно подчеркнуть, что перечисленные компоненты не только входят в обязательный состав прочих разновидностей «высоких технологий», но и сами являются их самостоятельными видами.

Телекоммуникационная составляющая включает в себя набор сетей связи и передачи данных, реализуемых на основе современных стандартов и технологий в области связи и передачи данных.

Средства связи являются самым критичным элементом любой системы управления, не случайно в каждом руководстве по организации связи присутствует фраза «потеря связи – есть потеря управления», что на языке товарного производства равнозначно потере прибыли, причем особенности «потерь» зависят от того, какую роль играет телекоммуникационная составляющая в производственных процессах, а также ее технические особенности и характеристики. Так, материалы аналитического обзора «Europe Towards 2000»[[26]](#footnote-26) свидетельствуют, что в банковском секторе за последнее десятилетие развитие технологий, средств обработки и передачи информации помогли увеличить производительность и уменьшить стоимость банковских операций. Современные технологии позволяют практически моментально получать и использовать информацию о клиентах, продуктах и рисках, что, несомненно, оказывает влияние на конкурентоспособность банков. Однако пока очень немногие банки в полной мере используют эти возможности.

Средства телекоммуникаций, вместе с новыми информационными технологиями, становятся инструментом при разработке новых продуктов и механизмов их распространения, что расширяет сферу деятельности банков. Электронные платежи и средства расчета в точке продажи – примеры использования новых технологий, коренным образом меняющих банковскую индустрию.

Традиционный подход к классификации средств связи (СС) предполагает их деление по среде распространения и частотному диапазону сигналов связи, виду передаваемой информации, способу формирования сигналов и каналов связи и конфигурации сети. Как правило, совокупность перечисленных характеристик определяет состав, назначение, достоинства, недостатки и функциональное значение отдельных видов связи.

По среде распространения СС делятся на радио-, проводные и оптические.

В зависимости от вида передаваемых сигналов связи различают аналоговые и цифровые каналы связи.

В аналоговых каналах для формирования (кодирования) сигналов применяют амплитудную, частотную, фазовую и квадратурно-амплитудную модуляции.

В цифровых каналах для передачи данных используют импульсные сигналы, группированные в самосинхронизирующиеся коды, которыми производят модуляцию (кодо-импульсную) гармонических несущих колебаний.

По проводным линиям связи, в зависимости от назначения и типа приемопередающих устройств, организуются следующие каналы связи:

- каналы низкочастотной телефонной (аналоговой) связи;

- каналы телеграфной связи;

- каналы факсимильной связи;

- каналы передачи данных;

- комбинированные каналы (IP) телефонной связи.

При этом следует отметить, что в настоящее время такое деление представляется весьма условным, так как при коммутации (соединении) проводной линии абонента к обслуживающей ее автоматической телефонной станции (АТС) передаваемый сигнал между оконечными, узловыми и центральными АТС, как правило, поступает в общие пучки местных и междугородных соединительных линий одностороннего или двухстороннего действия[[27]](#footnote-27): по двухпроводным физическим линиям или по одному выделенному сигнальному каналу (ВСК) (в системах передачи с частотным /ЧРК/ или с временным уплотнением каналов /ВРК/) (см. рис. 2).

В результате рассмотренного или цифрового уплотнения каналов связи в соединительных трактах циркулируют только дискретные сигналы связи, а также линейные и управляющие сигналы, передаваемые в индуктивном коде.

Таким образом, вид сигнала отражает назначение и тип приемопередающих устройств только на протяжении «последней мили»[[28]](#footnote-28). Существование «последней мили», а при применении радиотелефонных удлинителей «зоны радиоканала»[[29]](#footnote-29) предоставляет возможность несанкционированного подключения к линии абонента.

Линейные и управляющие сигналы управляют сервисными функциями АТС – аппаратурой повременного учета (АПУ), предназначенной для автоматического учета продолжительности исходящей связи каждого абонента.

Кроме того, сервисными функциями цифровых АТС могут управлять сигналы тонального набора, путем формирования комбинаций двухтоновых звуковых колебаний. Этот метод получил название двухтонального многочастотного набора (dual-tone multifrecuency dialing – DTMF), который применяется в сетях связи с цифровыми автоматическими телефонными станциями (АТС) или используется в качестве сигналов управления коммутацией вторичных сетей связи.

Принцип формирования тональных посылок заключается в одновременной выработке комбинаций из двух определенных частот, закрепленных за той или иной цифрой номера вызываемого абонента (или сигналом служебной управляющей информации) (см. табл. 1).

Рис. 2. Принципы разделения (уплотнения) каналов связи: а) схема частотного разделения каналов; б) схема временного разделения каналов

Таблица 1. Таблица выработки сигналов DTMF

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 697 гц | 770 Гц | 852 Гц | 941 Гц |
| 1209 Гц | 1 | 4 | 7 | - |
| 1336 Гц | 2 | 5 | 8 | 0 |
| 1477 Гц | 3 | 6 | 9 | # |

Примером применения DTMF кода может служить домашнее (телефонное) банковское обслуживание, которое позволяет клиентам получить доступ к банковским и информационным услугам, не выходя из дома.

При этом виде обслуживания клиент связывается с банком по телефону и дает непосредственные распоряжения по своему счету. Распоряжения могут быть отданы как голосом специальному служащему банка или электронной системе, так и в электронной форме непосредственно банковскому компьютеру. Ввод данных для платежа при голосовой связи (идентификатор, номер счета, размер платежа) производится клиентом с клавиатуры телефона. Этот вид обслуживания пользуется популярностью среди мелких предпринимателей и частных клиентов.

Как уже упоминалось, аналоговые линии проводной связи позволяют передавать импульсные сигналы связи, в параметрах которых может быть заключена (закодирована) различная информация.

В зависимости от ее вида и назначения абонентских терминалов различают следующие виды проводной связи:

- телеграфную связь (где сигналы несут информацию о передаваемых символах алфавита);

- факсимильную связь (где сигналы несут информацию о пространственной и цветовой характеристике точечного (растрового) изображения);

- модемную связь (где сигналы предназначены для межмашинного (компьютерного) обмена в различных сетях передачи данных).

Телеграфная связь обеспечивает передачу и прием оперативной информации в документальном виде. В телеграфном способе передача и прием информации осуществляются с помощью специальных устройств печати, называемых телеграфными аппаратами. В этих аппаратах применяется международный телеграфный код. Сущность его состоит в том, что каждому знаку (букве, цифре, знаку препинания) соответствует определенная комбинация электрических сигналов. Переданная электрическая комбинация через приемные устройства приводит оба аппарата в действие, от чего на рулонах бумаги аппаратов отпечатывается переданный знак.

Факсимильная связь предназначена для обмена графической информацией между специальными абонентскими терминалами – телефаксами, когда требуется передача и прием полутоновых фиксированных изображений, очертаний и глубины оригинала документа.

Современный телефакс представляет собой электромеханическое устройство, состоящее из сканера, каналообразующей аппаратуры – модема (МОдулятор-ДЕМодулятор) и принтера. Сканер считывает изображение документа, оцифровывает его и передает информацию в модем. Модем преобразует цифровые сигналы в последовательность модулированных сигналов и обеспечивает их передачу на другой факсимильный аппарат через обычную телефонную линию.

Различают две разновидности средств факсимильной связи: автономные телефаксы, выполняющие строго определенные функции, и интегрированные системы на базе персональных компьютеров. Кроме удобства использования, данная технология позволяет пользователям автоматизировать получение и отправку факсимильных сообщений по нескольким направлениям, что значительно повышает эффективность использования телефонных линий связи.

Модемная связь реализует принцип организации цифрового канала в аналоговой проводной линии. Модемные технологии, как и любые технологии передачи сигналов, накрепко связаны с характеристикой среды, по которой сигналы передаются. Процесс кодирования и декодирования аналоговых сигналов происходит следующим образом.

Вначале аналоговый сигнал поступает на вход одного их каналов системы аналогово-цифрового преобразования (АЦП), где заменяется эквивалентной ему по информационному содержанию последовательностью дискретных сигналов – отсчетов. Далее каждый отсчет заменяется некоторым двоичным кодом, учитывающим знак и амплитуду отсчета. Такой процесс носит название импульсно-кодовой модуляции – ИКМ.

При приеме последовательность принимаемых двоичных импульсов подается на вход цифроаналогового преобразователя (ЦАП), в котором производится преобразование цифрового кода в аналоговый сигнал.

Следует отметить, что скорость передачи по аналоговым линиям связи от модема клиента к цифровому модему сервера отличается от скорости приема и составляет не более 33600 Бит/сек., так как в канале присутствует АЦП (со стороны клиента), который и мешает достичь предельного (для линии связи) максимума скорости передачи данных.

Радиоканалы передачи информации образуются в результате использования в качестве материальной среды передачи сообщений электромагнитные (ЭМ) колебания различных частот, в результате чего сигнал связи представляет собой радиоволну, в параметрах которой заключена передаваемая информация. На практике в качестве модулируемых параметров используют частоту, фазу, амплитуду и длительность передаваемого ЭМ колебания.

Напомним, что амплитуда – это максимальная величина отклонения колебательного процесса от среднего значения (состояния покоя), а частота F=1/Т – это количество совершаемых колебаний в секунду.

Фаза колебания (ϕ ) – градусная мера (от 0° до 360°), которая определяет мгновенное состояние в течение периода (Т) совершения колебания.

Длиной волны λ (м) считают расстояние, пройденное радиоволной за период совершения колебания несущей частоты.

Частота ЭМ колебаний определяет их основные свойства распространения, что послужило причиной разделения радиоволн на диапазоны, дополнительно этому в немалой степени послужила зависимость емкости системы связи от частоты колебаний несущей.

Чем выше рабочая частота, тем больше емкость (число каналов) системы связи, но тем меньше предельные расстояния, на которых возможна прямая передача между двумя пунктами без ретрансляторов.

Первая из причин порождает тенденцию к созданию радиолиний более высокочастотных диапазонов, вторая – к освоению околоземного пространства, с целью создания ретрансляторов, обслуживающих большие зоны (прямой видимости) распространения радиосигналов.

Линия радиосвязи, совместно с устройствами, предназначенными для передачи и приема высокочастотных сигналов связи, образует радиоканал.

Радиочастотный диапазон относится к государственным ресурсам и строго регламентирован Государственным комитетом по радиочастотам (ГКРЧ). Для примера ниже приведены частоты, выделенные для обеспечения работы различных организаций и систем связи[[30]](#footnote-30):

25.160÷29.655 Мгц – гражданский (любительский) диапазон Си-Би;

38.750÷44.600, 254.000, 254.685, 380.000, 393.100 Министерство обороны РФ;

140÷145 Мгц – транковые сети связи;

149÷209, 450÷461 Мгц – МВД РФ;

149÷390 Мгц – радиоэлектронные средства правительственной связи, безопасности и обороны РФ;

148.050÷148.200 Мгц – пожарная охрана;

337÷343 Мгц – мобильные объекты; 368÷388 Мгц – ретрансляторы сотовой сети NMT-450;

430÷440 Мгц – транковые сети связи;

453÷457.5 МГц – мобильные объекты; 463-467.5 МГц – ретрансляторы транковой сети Алтай;

825÷845 МГц – мобильные объекты; 870÷890 МГц – ретрансляторы сотовой сети GSM;

824÷849 МГц – прием; 874÷899 МГц – передача сотовой сети CDMA;

890÷915 МГц – мобильные объекты; 935÷965 МГц – ретрансляторы сотовой сети GSM 950;

1626.5÷1646.5 МГц – восходящий луч от терминальных станций;

1530÷1545 МГц – нисходящий луч на терминальные станции спутниковая сеть Inmarsat;

1800 МГц – цифровая сеть микросотовой сети связи DECT;

1800÷1900 МГц – цифровая сеть сотовой сети GSM 1800.

Каналообразующие устройства, предназначенные для организации радиосвязи, представляют собой передающие и принимающие блоки, выполняющие функции формирования, излучения и приема электромагнитных колебаний, в параметрах которых заключено передаваемое сообщение.

Радиопередатчик – это техническое устройство, предназначенное для преобразования передаваемых сообщений в сигналы радиосвязи и излучения их в пространство.

Радиоприемник предназначен для приема радиосигналов, выделения заключенного в них информационного сообщения и выдачи его в требуемой для конкретного вида связи форме.

Для обеспечения односторонней радиосвязи в пункте, из которого ведется передача сигналов, размещают радиопередающее устройство, содержащее радиопередатчик и передающую антенну, а в пункте, в котором ведется прием сигналов – радиоприемное устройство, содержащее приемную антенну и радиоприемник.

Для двухстороннего обмена сигналами нужно иметь два комплекта оборудования. Двухсторонняя радиосвязь может быть симплексной или дуплексной. При симплексной радиосвязи передача и прием ведутся поочередно. Радиопередатчики в конечных пунктах в этом случае могут работать на одинаковой частоте, на эту же частоту настроены и радиоприемники. Радиопередатчик включается только на время передачи.

При дуплексной радиосвязи передача осуществляется одновременно с приемом. Для связи должны быть выделены две разные частоты для передачи в разных направлениях.

В ВЧ диапазонах такие виды радиосвязи обычно используются для передачи голосовых сообщений и организации региональной сети местной радиотелефонной связи, радиовещания.

В ОВЧ диапазонах радиосвязь используется для организации оперативного управления подразделениями силовых структур.

Система радиопередачи символов и отображения текстовой информации получила название пейджинговой системы (page – страница), соответственно, приемник в этой системе называется пейджер, а приемопередатчик – твейджер (two way page – двунаправленная страница).

Система многоканальной радиосвязи с коммутацией абонентов называется транковой системой (trunk – ствол). Отличием транковых радиостанций является включение в их состав блока адресации вызова, аналогичного вызывной системе проводной телефонии, а также диспетчерского пункта ретрансляции каналов связи.

Различают две основные разновидности организации коммутации абонентов:

- системы с незакрепленным каналом управления;

- системы с закрепленным каналом управления.

Транковые системы с незакрепленным каналом управления

К этому классу относятся системы, в которых на одних и тех же каналах происходит как передача служебной информации (кодов вызова, кодов радиостанций, телефонных номеров и т.д.), так и передача речевой информации. Типичным представителем данного класса транковых систем являются системы SmarTrunk II и LTR.

Основным элементом системы SmarTrunk II является многоканальная базовая станция, оснащенная ретрансляторами и транковыми контроллерами. Однако основное управление в системах SmarTrunk II осуществляют абонентские радиостанции, которые сканируют («просматривают») рабочие каналы, ищут свободный канал для связи или определяют, нет ли на одном из каналов вызывного сигнала для радиоабонента.

Системы LTR относятся к классу систем, использующих метод распределенного управления.

Преимущество распределенного метода управления состоит в том, что доступ к системе может быть выполнен по любому из свободных каналов. Каждый ретранслятор определяет, какой из каналов свободен и передает эту информацию в потоке данных одновременно с речевым сообщением. Это означает, что каждый ретранслятор поддерживает собственный поток данных и обслуживает все обращения к своим каналам. Конфликтные ситуации предотвращаются самими абонентами. Это обеспечивает полностью параллельную обработку всех вызовов.

Транковые системы с закрепленным каналом управления

К этому классу относятся транковые системы, в которых для передачи служебной информации используется отдельный канал связи.

Наиболее известным представителем систем с закрепленным каналом управления являются система MPT 1327. Она обеспечивает быстрое установление связи и целый ряд дополнительных удобств, таких как возможность передачи данных на борт мобильного объекта, построение многосотовых сетей связи, выявление и эффективное устранение нелегальных абонентов и т.д.

В исходном состоянии все абонентские радиостанции в пределах зоны действия данной базовой станции находятся на приеме на частоте управляющего канала. На этом канале система постоянно передает сообщения типа ALOHA – приглашение отвечать ей с уведомлением, сколько времени система ждет ответа абонентских станций.

Вызывающий абонент набирает на клавиатуре своей радиостанции номер нужного ему абонента и производит вызов. При этом его радиостанция посылает вызывную последовательность в ответ на очередную посылку ALOHA от базовой станции. Приняв вызов, база проверяет абонента по принципу «свой-чужой» и на том же управляющем канале вызывает второго абонента. Получив от него подтверждение о готовности к связи, база передает обеим радиостанциям команду на перестройку на один из свободных в этот момент «разговорных» каналов связи (каналов трафика).

Обе радиостанции автоматически перестраиваются на указанный канал и начинают переговоры. При нажатии любым из абонентов клавиши «отбой» происходит автоматический возврат радиостанций в ждущий режим на управляющем канале.

Сотовые системы связи. Сотовая связь (СС) отличается от традиционной радиосвязи тем, что в ней не предусматривается создание отдельных, требующих больших затрат энергии каналов связи между каждой парой абонентов. Вместо этого обслуживаемая территория делится на небольшие ячейки (соты) с соответствующим ретранслятором, таким образом, абоненты сети связываются не непосредственно с центральной, а только с ближайшим ретранслятором.

В настоящее время сотовые системы связи делятся на два вида: аналоговые и цифровые системы сотовой связи. В настоящее время наиболее востребованы системы сотовой телефонной связи цифровых стандартов, таких как GSM и CDMA.

Принцип работы сотовых систем радиосвязи основан на взаимодействии мобильных станций с фиксированной ретрансляционной сетью, объединенной с центром коммутации скоростными линиями связи. Для реализации этого принципа в состав сетей подвижной связи входят:

MSC – центр коммутации подвижной связи;

BTS – базовые станции;

MS – подвижные станции.

Центр коммутации подвижной связи (MSC) обеспечивает управление системой подвижной радиосвязи и является интерфейсом между подвижной станцией и фиксированной телефонной сетью. На рисунке 3 приведена структурная схема типовой сети сотовой связи аналогового стандарта NMT-450.

Каждый MSC обслуживает группу базовых станций. Совокупность BTS, обслуживаемых одним MSC, образует зону обслуживания (ТА).

Рис. 3. Схема работы подвижной системы радиосвязи

На каждой базовой станции один канал используется как канал вызова, он маркируется специальным сигналом опознавания. Один или несколько других каналов, когда они свободны, маркируются другим сигналом, показывающим, что канал свободен. Подвижные станции, находящиеся в зоне действия базовой станции, постоянно работают на прием на канале вызова, по нему каждый включенный сотовый телефон периодически напоминает ретранслятору о своем наличии даже тогда, когда Вы не разговариваете. Ретранслятор передает уровень принятого сигнала MS на MSC, где принимается решение – работать с ним дальше или передать на обслуживание соседней BS. Процесс передачи MS между различными BS получил название роуминг (roaming – бродяга англ.).

В цифровых системах сотовой связи процесс определения местоположения отличается. BS постоянно излучает длинный, неповторяющийся, цифровой сигнал-эталон. MS его постоянно принимает и периодически небольшой его кусочек переизлучает. BS сравнивает полученный сигнал с эталоном, вычисляет временную задержку и по ней определяет «дальность» нахождения MS, которую передает на MSC[[31]](#footnote-31).

Наиболее распространенный в России стандарт сотовой связи – GSM, помимо процедур установления местоположения, адресации вызова, и ретрансляции каналов связи, выполняет процедуры идентификации абонента и индивидуального шифрования трафика сеанса связи. Для реализации этих функций любое абонентское приемопередающее устройство (сотовый телефон) снабжено микропроцессорным комплектом, которым осуществляется выполнение трех алгоритмов (А3, А8, А5):

А3 – алгоритм аутентификации, защищающий SIM-карту абонента от клонирования;

А8 – алгоритм генерации криптоключа;

A5 – собственно алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров[[32]](#footnote-32).

Ключи алгоритмов A3 и A8 записаны в смарт-картах абонентов, ключ алгоритмов A5 записан в самом ASIC-чипе телефона.

Базовые станции также снабжены ASIC-чипом с A5 и «центром аутентификации», использующим алгоритмы A3÷A8 для идентификации мобильного абонента и генерации сеансового ключа.

Индивидуальный модуль подлинности абонента (SIM) содержит: международный идентификационный номер (IMSI), свой индивидуальный ключ аутентификации (Ki), алгоритм аутентификации (A3).

С помощью записанной в SIM информации в результате взаимного обмена данными между микропроцессором сотового терминала (абонентского аппарата) и оборудованием базовой станции осуществляется полный цикл аутентификации и разрешается доступ абонента к сети.

Процедура проверки сетью подлинности абонента реализуется следующим образом. Сеть передает случайный номер (RAND) на абонентский терминал. На ней с помощью Ki и алгоритма аутентификации A3 определяется значение отклика (SRES), т.е.

SRES = Ki – [RAND].

Абонентский терминал посылает вычисленное значение SRES в сеть, которая сверяет значение принятого SRES со значением SRES, вычисленным сетью. Если оба значения совпадают, подвижная станция приступает к передаче сообщений. В противном случае связь прерывается, и индикатор подвижной станции показывает, что опознавание не состоялось.

Для подтверждения подлинности международного идентификационного номера оборудования сотового телефона (IМЕI) в состав базовой станции входит регистр идентификации оборудования (EIR) – (централизованная база данных). Эта база данных ведется исключительно по оборудованию подвижных станций и состоит из списков номеров IМЕI, организованных следующим образом:

БЕЛЫЙ СПИСОК – содержит номера IМЕI, о которых есть сведения, что они закреплены за санкционированными подвижными станциями.

ЧЕРНЫЙ СПИСОК – содержит номера IМЕI подвижных станций, которые украдены или которым отказано в обслуживании по другой причине.

СЕРЫЙ СПИСОК – содержит номера IМЕI подвижных станций, у которых существуют проблемы, выявленные по данным программного обеспечения, что не является основанием для внесения в «черный список».

Кроме процедур идентификации, проверки и предоставления доступа к сети контроллер базовой станции управляет распределением радиоканалов и сменой частот, контролирует соединения и их очередность, модуляцию и демодуляцию сигналов, кодирование и декодирование сообщений, кодирование речи, адаптацию скорости передачи для речи, данных и вызова, определяет очередность передачи сообщений персонального вызова[[33]](#footnote-33).

Стоит отметить, что для абонентов в стандарте GSM предусмотрено пять классов терминалов связи: от модели 1-го класса с выходной мощностью 20 Вт, устанавливаемой на транспортном средстве, до портативной модели 5-го класса, максимальной мощностью 0,8 Вт[[34]](#footnote-34).

Стремительное развитие технологий связи породило возникновение большого количества видов связи, сервисных функций и специальных терминов, для уточнения которых целесообразно привести краткие пояснения.

2,5G (2,5 Generation) – технологии переходного периода, основанные на использовании усовершенствованных средств 2-го поколения, но способные обеспечивать услуги 3-го поколения.

3G (3 Generation) – 3-е поколение. Новое поколение систем мобильной связи, разрабатываемое в рамках программы IMT-2000. Сети радиодоступа этого поколения будут обеспечивать обмен информацией со скоростью до 144 кбит/с для абонентов с высокой мобильностью (скорость движения до 120 км/ч), 384 кбит/с для абонентов с низкой мобильностью (скорость до 3 км/ч) и 2,048 Мбит/с.

AMPS (Advanced Mobile Phone System) – усовершенствованная система мобильной связи. Аналоговая система, основанная на FDMA и работающая в частоте 800 МГц. Ширина канала 30 кГц.

Bluetooth – международная инициатива компаний Ericsson, IBM, Intel, Nokia и Toshiba, направленная на установление стандарта беспроводного соединения между телефонами мобильной связи, ПК, ручными компьютерами и другими периферийными устройствами. Предусматривается использование малодистанционных (до 10 м) каналов в свободной полосе 2,45 ГГц, используемой научно-медицинскими приборами.

CDMAOne – полностью цифровой стандарт, использующий диапазон частот 824÷849 МГц для приема и 874÷899 МГц для передачи.

DAMPS (Digital Advanced Mobile Phone Service) – это цифровая версия AMPS (Advanced Mobile Phone Service). DAMPS представляет собой систему сотовой подвижной радиосвязи общего пользования первого поколения.

DECT (Didital Enhanced Cordless Telecommunications) – цифровая микросотовая система беспроводной связи. Она обеспечивает своим пользователям устойчивую высококачественную связь, защищенную от несанкционированного доступа. Стандарт DECT поддерживает речевую и факсимильную связь, а также передачу данных.

GPRS (General Packed Radio Services) – радиосистемы передачи с пакетной коммутацией. GPRS часто упоминается как GSM-IP (GSM Internet Protocol). Расчетная скорость – 64 кбит/сек, практически достижимая скорость – 48 кбит/сек, теоретически достижимая – 115 кбит/сек.

GPS (Global Positioning System) – система глобального позиционирования. Система использует навигационные спутники. При проектировании системы планировалось вывести 24 спутника на квазистационарные орбиты. Такие системы обеспечивают круглосуточную информацию о трехмерном положении, скорости и времени для пользователей, обладающих соответствующим оборудованием и находящихся на или вблизи земной поверхности (а иногда и вне ее). Первой системой GPS, широко доступной гражданским пользователям, стала NAVSTAR, обслуживаемая Министерством обороны США.

GSM (Global System for Mobile communications) – глобальная система мобильной связи, цифровой стандарт мобильной связи. Стандарт сотовой связи, использующий частоты 900, 1800 и 1900 МГц. Ответственный за стандартизацию технологии GSM Европейский институт стандартизации электросвязи (ETSI). GSM использует TDMA технологию.

GSM 1800 – цифровой стандарт GSM на частоте 1800 МГц, известен также как DCS 1800 или PCN, используется в Европе, в Тихоокеанских странах Азии, Австралии, России.

GSM 900 – цифровой стандарт GSM на частоте 900 МГц, распространен в более 100 странах Европы и Азии.

IMEI (International Mobile Equipment Identifier – международный идентификатор мобильного оборудования) – это уникальный номер мобильного телефона. Номер включает в себя 15 цифр. Он присваивается аппарату при производстве и предназначен для определения телефона в сети GSM. Когда в центр обслуживания поступает телефон, то он проверяется с помощью IMEI номера. Это позволяет проверить легальность аппарата, версию программного обеспечения, страну сборки и многое другое. Телефоны с измененными IMEI номерами фирменные сервис-центры производителей отказываются обслуживать.

I-mode – технология, обеспечивающая постоянное соединение с пропускной способностью 9,6 Кбит/с. Это позволило DoCoMo начать разработку мобильных приложений на базе IP-телефонии, опередив GPRS. Данная технология конкурирует и с WAP, так как использует компактную версию HTML, в то время как WAP работает со специальным языком маркеров WML (Wireless Markup Language).

IrDA (Infrared Direct Access) – технологии инфракрасной связи, работающей по принципу «точка-точка» в зоне прямой видимости.

LTR (LTR450 и LTR800) – стандарт транкинговой радиосвязи с постоянным каналом. Работа системы основана на организации обмена служебными сообщениями между абонентской станцией и ретранслятором. Обмен данными осуществляется постоянно на субтональной частоте 150 Гц одновременно с передачей речевых сообщений. При этом отпадает необходимость в выделенном канале управления и поэтому для обеспечения максимальной эффективности системы все каналы могут быть использованы для передачи речевых сообщений.

MMS (Multimedia Messaging Service) – сервис передачи мультимедийных сообщений посредством мобильного телефона. Этот сервис очень похож на SMS, но, в отличие от него, более универсален. Технология MMS позволяет передавать мультимедийные сообщения с телефона на телефон либо с телефона на адрес электронной почты.

МРТ (Ministry of Post and Telecommunication) – стандарт транкинговой радиосвязи с закрепленным каналом. MPT 1327 был разработан в Англии для радиосетей общего пользования в диапазоне 174÷225 МГц, в дальнейшем распространился и на другие диапазоны частот. В настоящее время транковая аппаратура MPT 1327 выпускается для диапазонов 146÷174 МГц, 300÷380 МГц, 400÷520 МГц и даже 800 МГц.

NMT (Nordic Mobile Telephone) – аналоговые мобильные системы скандинавских стран. Стандарт был разработан в скандинавских странах, работает в частотном диапазоне 450 МГц.

SIM-карта (от англ. Subscriber Identification Module) – используемый в мобильной связи идентификационный модуль абонента.

SmarTrunk II – стандарт транкинговой радиосвязи. В системе SmarTrunk II может быть от 2 до 16 каналов и, соответственно, система может обслуживать от 60 до 1100 абонентов. Основным элементом системы является многоканальная базовая станция, оснащенная ретрансляторами и транковыми контроллерами. Однако основное управление в системах SmarTrunk II осуществляют абонентские радиостанции, которые сканируют (осматривают) рабочие каналы, ищут свободный канал для связи или определяют, нет ли на одном из каналов вызывного сигнала для радиоабонента.

SMS (англ. Short Message Service) – служба коротких сообщений). Эта система позволяет посылать и принимать текстовые сообщения посредством сотового телефона. Сообщение можно отправить на выключенный/находящийся вне зоны обслуживания телефон. После появления адресата в сети, он тут же получит сообщение. Сообщение может получить и абонент, занятый разговором. Существует расширенный вариант SMS-MMS.

TETRA (Terrestrial Trunked Radio) – стандарт транкинговой радиосвязи. Этот стандарт был создан под эгидой Европейского института телекоммуникационных стандартов (ETSI) с целью заменить со временем все существующие разнородные аналоговые стандарты транкинговой связи. Сегодня он является единым стандартом цифровой транкинговой радиосвязи в странах ЕС. Уровень надежности и безопасности стандарта TETRA многократно превышает существующие аналоговые системы.

UMTS (Universal Mobile Telecommunication System) – Универсальная Мобильная Телекоммуникационная Система – скорость передачи данных до 384 кбит/сек при передвижении со скоростью до 120км/час и до 2 мбит/сек при передвижении со скоростью до 10 км/час. Данный стандарт сотовой связи третьего поколения для Европы разработан ETSI.

USSD (Unstructured Supplementary Services Data) – это услуга двунаправленной сеансовой передачи неструктурированных данных, реализованная в сетях стандарта GSM. Она является встроенной функцией инфраструктуры GSM сетей и позволяет передавать информацию между пользователями и приложениями через сеть сигнализации ОКС №7 в режиме реального времени. Причем этот обмен идет по каналу сигнализации без создания дополнительной нагрузки на голосовые каналы.

Wi-Fi – (Wireless Fidelity – беспроводная высокая точность) – технология, которая в последнее время набирает обороты. Представляет собой формат передачи цифровых данных по радиоканалам в диапазоне 2,4 ГГц. Сети Wi-Fi строятся на основе небольших базовых станций, которые получили название точки доступа или хот-споты. Скорость передачи данных в таких сетях может достигать 54 Мбит/с. Радиус действия одной точки составляет до 100 метров. При наличии усилителей сигнала передача данных может осуществляться на расстояние до 20 километров.

WAP (Wireless Application Protocol) – бесплатный нелицензированный протокол беспроводной связи, позволяющий создавать расширенные системы мобильной телефонии и получать доступ к страницам Интернета с мобильных телефонов.

### 2.3 Технические особенности информационно-технологических систем

Использование информационно-технологических систем в различных сферах производства дает возможность полнее реализовать вклад следующих составляющих:

1) автоматизация – исключение из процесса человеческого труда;

2) информатизация – сбор и переработка информации о процессе;

3) изменение последовательности (очередности) этапов процессов и обеспечение их параллельного осуществления;

4) контроль – постоянное отслеживание и регистрация состояния объектов и процессов;

5) интеграция – координирование различных заданий и процессов;

6) интеллектуализация – сбор и распределение интеллектуальных активов[[35]](#footnote-35).

Для обеспечения решения перечисленных информационных задач в состав компьютерной системы обработки информации, помимо рассмотренных ранее основных устройств обработки, может входить ряд обязательных и дополнительных устройств (см. рис 4).

Все компоненты аппаратного обеспечения компьютера вносят существенный вклад в обеспечение эффективности обработки информации, однако с точки зрения пользователя, активно влияющего на работу системы, важны только те устройства, которые отличаются от процессора и памяти, то есть внешние устройства.

Внешние устройства можно подразделить на внешние запоминающие устройства (ВЗУ) и устройства ввода/вывода (УВВ) информации. ВЗУ – это устройства, способные хранить информацию некоторое время, связанные с физическими свойствами конкретного устройства, и обеспечивать чтение и/или запись этой информации в оперативную память.

Если рассматривать ВЗУ с точки зрения использования различными компонентами программного обеспечения, то можно выделить следующие типы устройств:

- накопители на флоппи-дисках (дискетах);

- накопители на жестких дисках («винчестерах»);

- накопители на магнитной ленте (стриммеры);

- накопители на оптических дисках (CD и DVD);

- накопители на интегральной памяти (флеш-модулях).

Общее назначение перечисленных устройств – хранение цифровых двоичных данных в виде файлов, в логических и физических разделах файловой системы.

Дискета (англ. floppy disk) – носитель небольшого объема информации, представляющий собой гибкий пластиковый диск в защитной оболочке. Используется для переноса данных с одного компьютера на другой, для распространения программного обеспечения, может содержать системные файлы операционной системы и использоваться для начальной загрузки (инициирования работы) компьютера «в обход» установленной.

Рис. 4. Комплекс основных и дополнительных компонентов компьютера.

Накопитель на жестких магнитных дисках (винчестеры) (англ. HDD – Hard Disk Drive) – это запоминающее устройство большой емкости, в котором носителями информации являются круглые алюминиевые (керамические) пластины – платтеры, обе поверхности которых покрыты слоем магнитного материала. Используется для постоянного хранения данных в различных файловых системах. Физическое пространство диска при формировании таблицы размещения файлов (file allocation table – FAT) может разбиваться на логические, образуя в системе отдельные виртуальные накопители.

Современные винчестеры выпускаются с тремя типами интерфейсов: SCSI (Small Computer System Interface), IDE (Integrated Drive Electronics), RAID (redundant array of inexpensive disks). Существует 6 вариантов исполнения технологии защиты данных: RAID 1: зеркальные диски; RAID 2: матрица с поразрядным расслоением; RAID 3: аппаратное обнаружение ошибок и четность; RAID 4: внутригрупповой параллелизм; RAID 5: четность вращения для распараллеливания записей; RAID 6: двумерная четность для обеспечения большей надежности.

Конкуренция между этими стандартами привела к существенному увеличению скорости обмена данными. Так, например, скорость передачи по стандарту SCSI-2 достигает 10 Мбайт/с в 8-битном Fast-режиме и 20 Мбайт/с в 16-битном FaslWide-режиме, что позволяет применять этот интерфейс для широкого класса компьютеров, включая супер-ЭВМ.

Интерфейс IDE (или иначе АТА) – гораздо более дешевый вариант, до последнего времени он существенно уступал по возможностям интерфейсу SCSI. Положение изменилось с внедрением нового стандарта АТА-2 (или Enhanced IDE). Его особенности: поддержка до четырех устройств, в том числе накопителей на CD-ROM и на магнитной ленте (ATAPI–ATA Packet Interface).

Накопитель на магнитной ленте (англ. tape streamer) – устройство для резервного копирования больших объемов информации. В качестве носителя здесь применяются кассеты с магнитной лентой емкостью 1-2 Гб и больше. Встроенные в стример средства аппаратного сжатия позволяют автоматически уплотнять информацию перед ее записью и восстанавливать после считывания, что фактически увеличивает объем сохраняемой информации.

Накопители на оптических дисках (CD, DVD) представляют собой прозрачные полимерные диски диаметром 8 и 12 см, на одну сторону которого напылен светоотражающий металлизированный слой.

Штампованный CD-ROM – поликарбонат, покрытый с одной стороны отражающим слоем и защитным лаком. Смена отражающей способности осуществляется за счет штамповки углублений в металлическом слое. Время хранения оценивается в 10 лет.

CD-R (CD-WORM) – вместо штамповки отражающего слоя используется разрушение участков покрывающей его термочувствительной краски. Голубые и зеленые цианиновые (cyanine) болванки имеют предполагаемое время хранения 75 лет, фталоцианиновые (phtalocyanine) – 200 лет. Фталоцианин устойчивее к нагреванию и свету, но требует тщательной настройки мощности лазера. На верхнем слое поликарбоната нанесена спиральная дорожка разметки (pregroove), содержащая коды ATIP – требуемая мощность лазера, возможная скорость записи и временные коды каждого кадра, а также информация о носителе (информация определяется изготовителем матрицы, изготовитель диска может использовать матрицу не по назначению: залить другую краску и т.п.):

CD-RW (CD-E) – CD диск с возможностью перезаписи информации способом преобразования кристаллического состояния записывающего слоя в аморфное (низкая отражательная способность) и обратно под воздействием точечного нагревания лазером. Срок хранения – 10 лет. Циклов записи – 1000. Также имеет предварительно выдавленную дорожку разметки с ATIP.

DDCD (Sony) – CD диск с уменьшенным расстоянием между витками и размерами информационных пит. Емкость – 1.3 Гб.

ML-ROM, ML-R, ML-RW (TDK) – CD диск с модифицированным (3 бита на пит) алгоритмом кодирования. Диски 120 мм – 2 Гб, 80 мм – 650 Мб, 60 мм – 200 Мб.

DVD-ROM – носитель аналогичен CD-ROM (120 мм и 80 мм), но длина волны лазера снижена с 780 нм до 635/650 нм, что позволило уменьшить расстояние между витками до 0.74 мкм, а размер пита до 0.14 мкм. Более узкая фокусировка луча позволила уменьшить толщину диска до 0.6 мм и склеивать их по два, делая таким образом двухсторонние диски, увеличивая емкость с 4.7 Гб (Type A, DVD-5, SS/SL, 120 мм) до 9.4 Гб (Type B, DVD-10, DS/SL). При этом данные (на каждой стороне) могут храниться в одном или двух слоях (используется фокусировка луча на различную глубину), таким образом, увеличивая емкость до 8.5 Гб (Type C, DVD-9, SS/DL) или 17 Гб (Type D, DVD-18, DS/DL).

DVD-R – односторонние (4.7 Гб – 1S) и двухсторонние (9.4 Гб – 2S). Термокраска как в CD-R, но другого типа. Читаются на любых DVD-ROM. DVD-R(A) – могут записываться только на профессиональном оборудовании. DVD-R(G) – могут записываться только на бытовом оборудовании, защищены от копирования на них. Для записи на диски A и G используются лазеры с различной длиной волны (635 и 650 нм). Максимальная скорость записи до 16x.

DVD-RAM – одно- и двухсторонние диски. Первая версия – 2.6 Гб, вторая – 4.7 Гб. Используется изменение фазы как в CD-RW в комбинации с магнитооптикой. Отражающая способность ниже, чем у DVD-ROM. Версия для записи видео называется DVD-VR. Помещаются в открываемые (type 2) или цельные кассеты (type 1) или без них (только для чтения). Предусматривается специальная кассета (type 3) для помещения в нее дисков. При извлечении диска из кассеты типа 2 необходимо пробить отверстие, которое позволяет устройству однозначно определить, что диск вынимался или заменялся. Некоторые устройства отказываются записывать на такие диски. Стандарт предусматривает до 100 тысяч циклов перезаписи. Продолжительность хранения – 30 лет.

DVD-RW – разработан на базе DVD-R, но используется изменение фазы как в CD-RW.

DVD+RW – используется изменение фазы как в CD-RW. Первая версия – 3 Гб, вторая – 4.7 Гб. Односторонние (тип S) и двухсторонние (тип D). Позволяет перезаписывать часть данных, не затрагивая окружающие (например, перезапись плохо записанного сектора). До 1000 циклов перезаписи. Максимальная скорость, определенная в стандарте – 4x÷8x.

DVD+R – гибрид форматов – структура данных от DVD+RW, химия от CD-R. Односторонние (тип S) и двухсторонние (тип D). Максимальная скорость, определенная в стандарте – 8x (бывают устройства 16x).

DVD+R9 – двухслойный DVD+R. 8.5 Гб. Максимальная скорость, определенная в стандарте – 2x÷4x.

В скором будущем альянс производителей (DVD Forum) обещает появление нового носителя – DVD-RDL.

Внешние накопители на перепрограммируемой постоянной памяти (Flash-память – Flash Memory) – устройства, содержащие энергонезависимую память, допускающие многократную перезапись своего содержимого. Они подразделяются на (см. рис. 5):

- PC Card (или PCMCIА ATA);

- Mini Card;

- CompactFlash;

- SmartMedia;

- IBM Microdrive;

- MultiMedia Card;

- Sony Memory Stick;

- SD Card;

- DataPlay.

PC Card ATA – карта памяти хранения данных большой емкости для портативных компьютеров, – размер 85,6х 54х 3,3 мм, имеет 68 pin-овое соединение на торцевом разъеме. Существует несколько типов PC Card: Type I, Type II, Type III, различие которых в толщине. Это 3.3, 5.0, 10.5 мм соответственно. Стандарт PC Card ATA Type I – используется как память SRAM, Flash и т.п. типы памяти; стандарт PC Card ATA Type II – помимо памяти – как устройства ввода-вывода (например: модемы, сетевые карты); стандарт PC Card ATA Type III – как жесткие диски.

Mini Card (или Miniature Card) – это сменный цифровой носитель информации. Его размеры 38 мм длина, 33 высота, 3,5 мм ширина. На торцевом разъеме находятся штырьки, которые легко можно повредить при использовании.

СompactFlash – это маленькое сменное устройство хранения данных большой емкости без движущихся частей, размером 42,8 x 36,4 x 3.3 мм. Карта имеет 50 pin-овое соединение на торцевом разъеме, и соответствует всем ATA спецификациям, вплоть до всех электрических и механических процессов. Во-первых, этот формат не имеет движущихся частей, во-вторых – малое энергопотребление 3,3 и 5 вольт, в-третьих – высокая совместимость с PC (из-за встроенного контроллера).

|  |  |  |
| --- | --- | --- |
|  |  |  |
| PCMCIА ATA | Mini Card | CompactFlash |
|  |  |  |
| SmartMedia | IBM Microdrive | MultiMedia Card |
|  |  |  |
| Sony Memory Stick | SD Card | DataPlay |

Рис. 5. Внешние накопители – карты памяти хранения данных

SmartMedia Card. Ранее они носили еще название – Solid State Floppy Disk Card (гибкий диск с твердым телом), размером 45.1×37×0,76 мм, вес 2 грамма. Энергопотребление – 3,3 и 5 вольт. 22 pin-овое подсоединение. Скорость записи/чтения примерно 512 килобайт в секунду. В карте отсутствует контроллер, и как следствие, структура имеет только носитель информации и контактную позолоченную панель.

IBM Microdrive – это миниатюрный жесткий диск объемом 170, 340, 512 Мб и 1 Гб. Может использоваться в камерах, оборудованных слотом для CompactFlash Type II, потому что сам он имеет точно такой же размер, что и CompactFlash Type II.

MultiMedia Card – это одно из самых маленьких сменных устройств хранения данных небольшой емкости. Эта карта имеет размер приблизительно с почтовую марку. Длина 32 мм, ширина 24 мм, высота 1.4 мм, вес – меньше 2х грамм.

Memory Stick от Sony. Размер 50 мм длиной, 21.5 мм шириной, 2.8 мм высотой, вес 4 грамма. Это, как и все карты памяти, применяемые в цифровых фотокамерах, энергонезависимый носитель информации. Основана на технологии Flash RAM. Имеет 10-контактный разъем и защиту от случайного стирания.

SD Card (Secure Digital) (SD – сокращенно от Secure Digital) – карты безопасного хранения. Это карта размером 24 х 32 х 2.1 мм, 9 штырьковый разъем на торце. Вес 2 грамма. Скорость считывания данных – около 6Мб в секунду. Карта имеет криптозащиту от несанкционированного копирования, повышенную защиту информации на карте от случайного стирания или разрушения. Слот для приема SD карт совместим со слотом MultiMedia Card.

DataPlay – это миниатюрные диски большого объема. Привод похож на привод обычных винчестеров, однако, фактически диски DataPlay – это миниатюрные DVD-R диски. Данное устройство имеет размер – 33,53 мм высотой, 39,5 мм шириной, объем до 4Гб.

Следует отметить, что в настоящее время особо широкую популярность приобретает реализация Flash-памяти в виде Flash-«брелоков» различных исполнений и емкостей. Максимальная емкость современных Flash-«брелоков» составляет 16 Гб.

На физическом уровне, любые данные, хранящиеся на материальных носителях, состоят из информационных полей (адресов) и собственно формализованных данных (представляемых в виде двоичных символов). Соответственно, обращение к памяти большого объема требует и большой длины адреса. Основной обобщающей характеристикой устройств ввода/вывода может служить скорость передачи данных (максимальная скорость, с которой данные могут передаваться между устройством ввода/вывода и основной памятью или процессором). В таблице 2 представлены основные устройства ввода/вывода, применяемые в компьютерах, а также указаны примерные скорости обмена данными, обеспечиваемые этими устройствами.

Таблица 2. Скорости обмена данными устройств ввода/вывода

|  |  |  |
| --- | --- | --- |
| Тип устройства | Направление передачи данных | Скорость передачи данных (Кбайт/с) |
| Клавиатура | Ввод | 0,01 |
| Мышь | Ввод | 0,02 |
| Голосовой ввод | Ввод | 0,02 |
| Сканер | Ввод | 200,0 |
| Голосовой вывод | Вывод | 0,06 |
| Лазерный принтер | Вывод | 100,00 |
| Графический дисплей | Вывод | 30000,00 |

Соединение и взаимодействие с перечисленными устройствами обеспечивают специальные интерфейсы связи: последовательный – СОМ, параллельный – LPT и универсальная последовательная шина USB (Universal Serial Bus). Следует отметить, что USB обеспечивает более высокую скорость обмена данными. Максимальная пропускная способность USB версии 1.1 – 12 Мбит/с, более современной версии 2.0 – 480 Мбит/с. Впрочем, для низкоскоростных устройств предусмотрена скорость 1,5 Мбит/с.

Для связи между компьютерами существует три основных способа организации межкомпьютерной связи:

- объединение двух рядом расположенных компьютеров через их коммуникационные порты посредством специального кабеля;

- передача данных от одного компьютера к другому посредством модема с помощью проводных или спутниковых линий связи;

- объединение компьютеров в компьютерную сеть.

Часто при организации связи между двумя компьютерами за одним компьютером закрепляется роль поставщика ресурсов (программ, данных и т.д.), а за другим – роль пользователя этих ресурсов. В этом случае первый компьютер называется сервером, а второй – клиентом или рабочей станцией. Работать можно только на компьютере-клиенте под управлением специального программного обеспечения. Клиентом также называют прикладную программу, которая от имени пользователя получает услуги сервера. Соответственно, программное обеспечение, которое позволяет компьютеру предоставлять услуги другому компьютеру, называют сервером – так же, как и сам компьютер.

Для организации связи между компьютерами в настоящее время широко используются семейство протоколов TCP/IP, IPX/SPX, AppleTalk и NetBEUI:

TCP/IP – протокол, используемый для адресного объединения компьютеров в сеть Internet;

IPX/SPX – протокол, применяемый в сетях на базе Novell NetWare;

AppleTalk – протокол поддержки клиентов сетей Apple Macintosh;

NetBEUI – протокол, предназначенный для применения в локальных сетях.

В настоящее время TCP/IP (IP-сети) является доминирующим протоколом межмашинного обмена данными с использованием уникальных адресов клиентов сети. Вторым, не менее важным параметром, характеризующим машину, является маска подсети – величина, определяющая максимальное число машин, которые могут находиться в одном локальном сегменте сети. Администратор сети присваивает IP-адреса машинам в соответствии с тем, к каким IP-сетям они подключены. Старшие биты четырехбайтного IP-адреса определяют номер IP-сети. Оставшаяся часть IP-адреса – номер узла (хост-номер). Существует 5 классов IP-адресов, отличающихся количеством бит в сетевом номере и хост-номере (см. таб. 3).

При разработке структуры IP-адресов предполагалось, что они будут использоваться в сетях разного масштаба:

- адреса класса A предназначены для использования в больших сетях общего пользования;

- адреса класса B предназначены для использования в сетях среднего размера (сети больших компаний, научно-исследовательских институтов, университетов);

- адреса класса C предназначены для использования в сетях с небольшим числом компьютеров (сети небольших компаний и фирм);

- адреса класса D используют для обращения к группам компьютеров.

Таблица 3. Классификация IP-адресов

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 |  | 8 |  | 16 |  | 24 |  | 31 |
| Класс A | 0 | № СЕТИ | № ХОСТА |
| Класс B | 10 | № СЕТИ | № ХОСТА |
| Класс C | 110 | № СЕТИ | № ХОСТА |
| Класс D | 1110 | ГРУППОВОЙ АДРЕС |
| Класс E | 11110 | ЗАРЕЗЕРВИРОВАНО |

Особое внимание имеет адрес 127.0.0.1, который предназначен для тестирования программ и взаимодействия процессов в рамках одного компьютера. В большинстве случаев в файлах настройки этот адрес обязательно должен быть указан.

Для обмена данными чаще всего используется стек протоколов TCP/IP, и хотя он был разработан до появления модели взаимодействия открытых систем (ISO/OSI) (имеет собственную многоуровневую структуру), он обладает определенным соответствием уровням модели OSI[[36]](#footnote-36).

Для универсальной схемотехнической реализации канала связи вычислительных систем, модель OSI предусматривает реализацию программно-аппаратного решения классического канала связи источника с приемником (см. рис. 6).

Прикладные процессы ЭВМ, включенной в сеанс связи, реализуют протокол связи TCP (Transmission Control Protocol) через порты связи. Для отдельных приложений выделяются общеизвестные номера портов. Когда прикладной процесс использует TCP, например, для передачи файлов FTP (File Transfer Protocol), кодер и декодер взаимодействующих ЭВМ последовательно реализуют стек протоколов FTP/TCP/IP/ENET. При любом другом соединении ЭВМ, например, при реализации UDP (User Datagram Protocol – протокола пользовательских датаграмм), информацию о состоянии соединения (виртуального канала), поддерживают оконечные модули TCP. Этот виртуальный канал потребляет ресурсы обоих оконечных модулей TCP. Канал является дуплексным: данные могут одновременно передаваться в обоих направлениях. Один прикладной процесс пишет данные в TCP-порт, они проходят по сети, и другой прикладной процесс читает их из своего TCP-порта.

Протокол TCP разбивает поток байт на пакеты; он не сохраняет границ между записями. Например, если один прикладной процесс делает 5 записей в TCP-порт, то прикладной процесс на другом конце виртуального канала может выполнить 10 чтений для того, чтобы получить все данные. Но этот же процесс может получить все данные сразу, сделав только одну операцию чтения. Не существует зависимости между числом и размером записываемых сообщений с одной стороны и числом и размером считываемых сообщений с другой стороны.

Рис. 6. Семиуровневая реализация протокола открытых систем

Таким образом, можно заключить, что обработка информации в компьютерной системе есть циклический процесс хранения и передачи данных во времени и пространстве, что накладывает особенные требования к физической целостности данных. Что касается защиты от несанкционированного получения конфиденциальной информации при ее автоматизированной обработке, то считалось, что автономность работы ЭВМ первых поколений, индивидуальность алгоритмической реализации процедур обработки информации, представление информации в запоминающих устройствах ЭВМ и на машинных носителях в закодированном виде и относительная простота организационного контроля всего процесса обработки обеспечивают надежную защиту информации от несанкционированного доступа к ней.

Однако, по мере развития электронной вычислительной техники, форм, способов и масштабов ее использования использовавшиеся защитные механизмы стали терять свою эффективность, повысилась уязвимость информации. Это подтверждается конкретными фактами несанкционированного получения информации в злоумышленных целях.

2.4 Подсистема обеспечения информационной безопасности

Составляющая по обеспечению информационной безопасности (ИБ) должна быть реализована в виде комплексной системы информационной безопасности технических систем обработки информации (ТСОИ), обеспечивающей современные методы и средства защиты информации в процессах ее электронной обработки, передачи и хранения, защиту информационных и сервисных ресурсов системы.

Вышеперечисленные особенности информационных технологий по мере своего проявления обусловливают уязвимость информации, в том числе:

- подверженность физическому или логическому искажению или уничтожению;

- возможность несанкционированной (случайной или злоумышленной) модификации;

- опасность несанкционированного (случайного и преднамеренного) получения информации лицами, для которых она не предназначалась.

Кроме этого, информационным технологиям присуща подверженность различным видам воздействий, снижающих информационную безопасность (см. рис.7). Эти воздействия принято называть угрозами безопасности информации и информационной безопасности. Вполне очевидно, что понятия таких угроз формируются с учетом соответствующих понятий безопасности. Наиболее общие понятия безопасности и угроз сформулированы в Законе Российской Федерации «О безопасности».

|  |  |  |
| --- | --- | --- |
|  | УГРОЗЫ БЕЗОПАСНОСТИ |  |
| По природе возникновения | По ориентации на ресурсы |
| Стихийные бедствия природного, техногенного и социального характера |  |  | Угрозы персоналу |
|  |  |
| Несчастные случаи |  |  | Угрозы материальным ресурсам |
|  |  |
| Ошибки обслуживающего персонала, пользователей |  |  | Угрозы финансовым ресурсам |
|  |  |
| Злоупотребления персонала, пользователей |  |  | Угрозы информации |
|  |  |
| Противоправные действия со стороны злоумышленников |  |  | Угрозы информационным ресурсам |
|  |  |
| Сбои и отказы в программном обеспечении и оборудовании |  |  | Угрозы информационным системам |
|  |  |
| Другие |  |  | Другие |
|  |

Рис. 7. Виды угроз безопасности

Безопасность – состояние защищенности жизненно важных интересов личности, общества, государства от внешних и внутренних угроз.

Угроза безопасности – совокупность условий, факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Таким образом, независимо от вида объекта безопасности, угроза безопасности представляет совокупность факторов, явлений, условий и действий, создающих опасность для нормального функционирования объектов, реализующих определенные цели и задачи. С учетом этих понятий, для ТСОИ можно представить следующее определение угрозы.

Угроза информационной безопасности – реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению, уничтожению информации, обрабатываемой в ТСОИ, и сведений о самой системе, а также к прямым материальным убыткам.

Подсистемы защиты информации должны преследовать достижение следующих целей[[37]](#footnote-37).

1) обеспечение физической целостности защищаемой информации, т.е. заданной синтаксической ее структуры;

2) обеспечение логической целостности, т.е. семантических характеристик информации и установленных взаимосвязей между ее элементами;

3) обеспечение доверия к информации в прагматическом плане, т.е. предупреждения несанкционированной ее модификации с изменением или без изменения синтаксических или семантических характеристик;

4) предупреждение несанкционированного получения защищаемой информации лицами или программами (процессами), не имеющими на это специальных полномочий, т.е. обеспечения установленного статуса ее секретности (конфиденциальности);

5) предупреждение несанкционированного копирования (размножения) информации, объявленной чьей-либо собственностью;

6) защита от демаскирования, т.е. скрытия назначения, архитектуры, технологии и самого факта функционирования системы обработки информации;

7) защита личности, общества, государства, в т.ч. их информационных ресурсов, информации, информационных систем от воздействия информации, наносящей ущерб, внешних и внутренних угроз.

Для достижения рассмотренных целей комплексной защиты информации необходимо предусмотреть адекватные по содержанию и достаточные по количеству способы и средства защиты, как отдельных образцов ТСОИ и в целом любой системы обработки информации.

Проблему защиты информации усугубляет бурное развитие мобильных технологий. Исследования аналитиков в области информационной безопасности говорят о безответственности людей в обращении со своими мобильными устройствами. Именно этот тип утечек приводит к серьезным убыткам пользователей гаджетов[[38]](#footnote-38).

Благодаря высоким коммуникационным возможностям современные мобильные устройства получают все большее распространение.

Функции почты, управление контактами, Интернет, создание документации делает современные портативные устройства незаменимыми помощниками. Наличие bluetooth, IrDA, Wi-Fi – все это идеально подходит для массового использования. Вследствие резкого роста «мобильного потенциала» общества существенно повышается риск утечки информации. Подавляющее большинство (более 70%) пользователей хранят на мобильном устройстве конфиденциальные данные, причем как свои, так и своего работодателя. И при этом 17% пользователей хотя бы раз теряли мобильный телефон, карманный персональный компьютер (КПК), смартфон, а то и ноутбук. Организации, служащие которых применяют мобильные устройства, входят в группу повышенного риска.

Около 90% компаний сегодня не в состоянии предотвратить неавторизованное подключение мобильных накопителей к корпоративной сети, при этом только половина компаний осознает существующий риск утечек. Инциденты по утечке корпоративной информации случаются все чаще и чаще, носят глобальный характер. От потери данных страдают банки, сотовые операторы, хостинг-провайдеры, малый бизнес и большие корпорации, коммерческие фирмы и государственные учреждения - все эти организации зафиксировали массу утечек в 2006 году. Многие из этих компаний теперь могут стать жертвой мошенников, лишиться всех сбережений и навсегда испортить кредитную историю.

Из года в год убытки от утечек конфиденциальной информации растут на 20-25%, по оценкам специалистов по ИБ в 2006 году только в США потеряли более 60-65 млрд. долларов вследствие утечек приватных сведений. По прогнозам, совокупные потери мировой экономики из-за кражи коммерческих секретов достигнут в 2008 году 1 трлн. долларов.

Нельзя не отметить и то, что в последнее время недобросовестные конкуренты стали прибегать к услугам должностных лиц правоохранительных и контролирующих органов, которые, используя имеющиеся у них властные полномочия и оперативно-технические возможности, получают информацию о деятельности коммерческих структур. Так, в Калининграде было возбуждено уголовное дело в отношении сотрудника уголовного розыска и работника таможни, которые пытались передать коммерческой организации электронную базу конфиденциальных данных Калининградской таможни[[39]](#footnote-39).Фактам тайного хищения информации, совершенных при разных обстоятельствах, сопутствует лишь одно общее обстоятельство – «отсутствие свободного доступа на законном основании», которое собственник должен обеспечивать самостоятельно, организуя защиту информации «от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации». При этом выбор способов осуществляется с учетом обеспечения рассмотренных выше целей комплексной защиты информации или защиты системы от воздействий разрушающей информации. К таким способам можно отнести:

- препятствие – создание на пути возникновения или распространения дестабилизирующего фактора определенного барьера, не позволяющего соответствующему фактору принять опасные размеры;

- управление, определение и выработка на каждом шагу функционирования системы обработки информации управляющих воздействий на элементы системы, в результате которых будет обеспечено решение одной или нескольких задач защиты информации;

- маскировка преобразования информации, исключающая или существенно затрудняющая доступ к ней злоумышленников;

- регламентация – способ защиты информации, состоящий в разработке и реализации в процессе функционирования системы обработки информации комплекса мероприятий, создающих условия обработки информации, существенно затрудняющих проявление и воздействие дестабилизирующих факторов;

- принуждение – способ защиты, обеспечивающий соблюдение пользователями и обслуживающим персоналом правил и условий обработки информации под угрозой материальной, административной или уголовной ответственности;

- побуждение – способ защиты информации, при котором пользователи и обслуживающий персонал систем обработки информации побуждаются (материально, морально, этически, психологически) к соблюдению всех правил ее обработки.

Как правило, перечисленные способы предотвращения угроз реализуются следующими видами защит:

- организационно-правовой защитой, основывающейся на реализации системы общегосударственных законодательных актов, нормативно-правовых актов отдельных министерств и ведомств, органов управления, а также на системе разработанных на их базе организационных, организационно-технических и иных мероприятий, используемых для защиты информации;

- технической (инженерно-технической) защитой, основывающейся на использовании технических устройств, узлов, блоков, элементов, систем, как в виде отдельных средств, так и встроенных в процессе единого технологического цикла создания средств обработки информации, сооружений и т.д.;

- программно-аппаратной защитой, предполагающей использование программного обеспечения ЭВТ, комплексов и систем, а также аппаратных устройств, встроенных в состав технических средств и систем обработки информации.

Контрольные вопросы

1. Что называется сообщением?

2. Что называется сигналом?

3. Какие сообщения называются аналоговыми, а какие – дискретными?

4. Что называется линией связи, каналом связи, интерфейсом?

5. Что такое «компьютер»?

6. Что такое «файл»?

7. На какие классы подразделяется программное обеспечение компьютеров?

8. Какие основные составляющие можно выделить в информационных технологиях?

9. Перечислите и охарактеризуйте основные виды связи.

10. Перечислите и охарактеризуйте основные виды каналов связи.

11. Какие виды запоминающих устройств используются в компьютерах?

12. Какие существуют способы организации межкомпьютерной связи?

13. Каковы основные аспекты уязвимости информации?

14. Назовите основные виды угроз информационной безопасности.

15. Какие цели должны преследовать подсистемы защиты информации?

16. Перечислите способы предотвращения угроз информационной безопасности.

## ГЛАВА 3. ПОНЯТИЕ И СУЩНОСТЬ ПРЕСТУПЛЕНИЙ В СФЕРЕ

## ВЫСОКИХ ТЕХНОЛОГИЙ

3.1 Понятие компьютерного преступления

В рамках общепризнанного понимания в российской и зарубежной науке международного уголовного права установлено деление международных преступных деяний на международные преступления и преступления международного характера. «В то время как международные преступления затрагивают интересы всего мирового сообщества и подлежат юрисдикции Международного уголовного суда, преступления международного характера касаются ряда отдельных государств и в рамках принципа двойной подсудности подпадают под регулятивное действие института выдачи (экстрадиции). Здесь вопрос решается на основе принципа или выдай или накажи и принципа или выдай или суди»[[40]](#footnote-40).

Характер новации в системе международного уголовного права приобрели так называемые «компьютерные преступления», которые подпадают по всем меркам под понятие «преступление международного характера».

Компьютеризация – явление социально значимое. Однако значимость компьютеризации можно рассматривать с разных сторон. Признание компьютеризации как социально-значимого явления ставит перед нами задачу выявления тех последствий, которые сопутствуют данному феномену. И как не раз случалось в истории, когда научные достижения пользовались не только во благо, но и во вред, новая сфера деятельности человечества не стала исключением.

Существует несколько точек зрения о возникновении «компьютерной преступности». Так, по данным американского ученого Д.Б. Паркера, преступность, «связанная с системой электронной обработки данных, возникла одновременно с появлением компьютерной техники около 1940 г. Эта преступность получила название «компьютерной преступности, или злоупотребления компьютерами».

Ряд источников утверждают, что терминологическое понятие «компьютерная преступность» появилось в 50-е годы, когда были выявлены первые преступления с использованием ЭВМ. А если быть точнее, в 1958 году, когда произошло первое в мире зарегистрированное компьютерное преступление.

В 1983 году в Париже группой экспертов ОЭСР было дано криминологическое определение компьютерного преступления, под которым понималось любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку и/или передачу данных.

В результате интенсивных исследований, проведенных в разных странах, обоснованным представляется заключение о выделении самостоятельного вида преступлений, обобщенно называемого компьютерными преступлениями.

Компьютерное преступление как уголовно-правовое понятие – это 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.

Первое преступление подобного рода в СССР было зарегистрировано в 1979 году в Вильнюсе. Ущерб государству от хищения составил 78584 руб. Данный факт занесен в международный реестр правонарушений подобного рода и явился своеобразной отправной точкой в развитии нового вида преступлений в нашей стране.

На данный момент не существует общепризнанного определения таких преступлений, а сам термин «компьютерное преступление» носит операционный характер.

Вместе с тем исследователи выделяют три категории явлений, относимых к этому понятию:

- злоупотребление компьютером – ряд мероприятий с использованием компьютера для извлечения выгоды, которые нанесли или могли нанести ущерб;

- прямое незаконное использование компьютеров в совершении преступления;

- любое незаконное действие, для успешного осуществления которого необходимо знание компьютерной техники.

Наряду с этим в практический оборот введен термин «киберпреступность», охватывающий любое преступление, которое может совершаться с помощью компьютерной системы (сети) или в рамках компьютерной системы (сети). В принципе он охватывает любое преступление, которое может быть совершено в электронной среде. Как результат анализа ООН, существуют две категории киберпреступлений:

а) киберпреступление в узком смысле: любое противоправное деяние, осуществляемое посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных;

б) киберпреступление в широком смысле: любое противоправное деяние, совершаемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное хранение, предложение или распространение информации посредством компьютерной системы или сети.

3.2 Субъекты компьютерных преступлений

Обстановка совершения преступлений в сфере компьютерной информации характеризуется рядом существенных факторов. Для нее характерно несовпадение между местом совершения противоправных действий и местом наступления общественно опасных последствий. Рассматриваемые преступления совершаются, как правило, в специфически интеллектуальной области профессиональной деятельности и с использованием специализированного оборудования. Все эти преступления обычно совершаются в условиях различных нарушений установленного порядка работы с ЭВМ, о которых лицам становится известно в ходе их соответствующей профессиональной подготовки. Для правонарушителей в данной области обычно достаточно ясен механизм возможных нарушений правил пользования информационными ресурсами и связь с событиями, повлекшими наступление криминального результата.

Следовательно, относительно объекта преступного посягательства двух мнений быть не может – им, естественно, является информация, а действия преступника следует рассматривать как покушение на информационные отношения общества.

Субъекты данных преступлений нередко владеют специальными навыками не только в области управления ЭВМ и ее устройствами, но и специальными знаниями в области обработки информации в информационных системах в целом. При этом для корыстных преступлений, связанных с использованием информационных систем, характерны и специальные познания в соответствующих финансовых и иных информационных технологиях. Для нарушений правил эксплуатации ЭВМ и действий с ВЦ характерны специальные познания в узкой предметной профессиональной области устройств ЭВМ и программного обеспечения.

Лица, совершающие компьютерные преступления, могут быть объединены в три большие группы:

а) лица, не связанные трудовыми отношениями с организацией жертвой, но имеющие некоторые связи с нею;

б) сотрудники организации, занимающие ответственные посты;

в) сотрудники – пользователи ЭВМ, злоупотребляющие своим положением.

Кроме того, субъекты компьютерных преступлений могут различаться как по уровню их профессиональной подготовки, так и по социальному положению.

В частности, выделяют следующие их виды[[41]](#footnote-41):

а) «хакеры» – лица, рассматривающие защиту компьютерных систем как личный вызов и взламывающие их для получения полного доступа к системе и удовлетворения собственных амбиций;

б) «шпионы» – лица, взламывающие компьютеры для получения информации, которую можно использовать в политических, военных и экономических целях;

в) «террористы» – лица, взламывающие информационные системы для создания эффекта опасности, который можно использовать в целях политического воздействия;

г) «корыстные преступники» – лица, вторгающиеся в информационные системы для получения личных имущественных или неимущественных выгод;

д) «вандалы» – лица, взламывающие информационные системы для их разрушения;

е) психически больные лица, страдающие новым видом психических заболеваний – информационными болезнями или компьютерными фобиями.

Западные специалисты подразделяют представляющий опасность персонал на категории в соответствии со сферами деятельности[[42]](#footnote-42):

1. Операционные преступления. Совершаются операторами ЭВМ, операторами периферийных устройств ввода информации в ЭВМ и операторами, обслуживающими линии телекоммуникации.
2. Преступления, основанные на использовании программного обеспечения, обычно совершаются лицами, в чьем ведении находятся библиотеки программ; системными программистами; прикладными программистами; хорошо подготовленными пользователями.
3. Для аппаратурной части компьютерных систем опасность совершения преступлений представляют: инженеры системщики, инженеры по терминальным устройствам, инженеры-связисты, инженеры-электронщики.
4. Определенную угрозу совершения компьютерных преступлений представляют и сотрудники, занимающиеся организационной работой: управлением компьютерной сетью; руководством операторами; управлением базами данных; руководством работой по программному обеспечению.
5. Определенную угрозу могут представлять также разного рода клерки, работники службы безопасности, работники, контролирующие функционирование ЭВМ.

Особую опасность могут представлять специалисты в случае вхождения ими в сговор с руководителями подразделений и служб самой коммерческой структуры или связанных с ней систем, а также с организованными преступными группами, поскольку в этих случаях причиняемый ущерб от совершенных преступлений и тяжесть последствий значительно увеличиваются.

Например, около 90% злоупотреблений в финансовой сфере, связанных с нарушениями в области информационной безопасности, происходит при прямом или косвенном участии действующих или бывших работников банков. При этом на преступный путь часто становятся самые квалифицированные, обладающие максимальными правами в автоматизированных системах категории банковских служащих – системные администраторы и другие сотрудники служб автоматизации банков.

## 3.3. Особенности квалификации преступлений в сфере компьютерной

## информации

Анализируя динамику преступности в сфере высоких технологий, специалисты прогнозируют рост организованной преступности, связанной с использованием в корыстных целях различных электронных средств, входящих в состав телекоммуникационных систем. При этом предполагается, что в ближайшее время различные учреждения и организации все больше в производственной и коммерческой деятельности ориентируются на применение новых информационных технологий.

По мере развития компьютерных технологий и сетей у преступных групп и сообществ возникает желание обогатиться в нетрадиционной области. Виды преступной деятельности, в которой компьютерная информация выступает в качестве орудия совершения преступления или предмета преступного посягательства, настолько разнообразны, что компьютерная преступность по новому уголовному законодательству Российской Федерации стала объектом исследования многих юридических наук, в частности, криминологии, криминалистики, оперативно-розыскной деятельности. Однако по-прежнему существует много проблем как в квалификации, так и в расследовании компьютерных преступлений.

В настоящее время большая часть преступлений, подпадающих под категорию компьютерных, объединены законодателем в отдельную главу 28 УК РФ «Преступления в сфере компьютерной информации».

По статистическим данным МВД России, в 1997 г. было зарегистрировано 7 преступлений в сфере компьютерной информации, в 1998 г. – 66 преступлений, в 1999 г. – 294 преступления, в 2000 г. – 800, в 2001 г. – 1379, в 2002 г. – 2143, в 2003 г. – 4914, в 2004 г. – 7268, в 2005 г. – 14810 преступлений. В 2006 году было некоторое снижение количества преступлений в сфере компьютерной информации – 8889 преступлений, но, тем не менее, уровень остается высоким.

Исходя из статистики видно, что общее количество преступлений в сфере компьютерной информации имеет тенденцию к росту. И так происходит не только в России, но и во всем мире, поэтому можно уверенно прогнозировать продолжение роста компьютерной преступности и ее дальнейшее качественное развитие в обозримом будущем.

Следует отметить, что динамика роста может иметь более удручающий характер, если учесть, что подобные преступления – емкое понятие, оно охватывает и правонарушения, которые являются логическим продолжением преступлений, перечисленных в главе 28 УК РФ и многих других, например, связанных с нарушением законов, устанавливающих правоотношения в производственных сферах, базирующихся на информационных технологиях. В связи с этим уместно вспомнить, что еще более пятнадцати лет тому назад международными экспертами по информационным технологиям было предложено понимать под компьютерными преступлениями любое незаконное поведение, связанное с автоматизированной обработкой или передачей данных.

Наличие компьютерной информации потенциально связано с ее утечкой, разрушением, риском противоправного использования, изъятия или дополнением необъективной информацией. Преступник, совершая свои действия, посягает на права и интересы граждан, предприятий, учреждений, организаций в областях ответственного хранения, обладания, авторства, а также использования автоматизированных систем.

На сегодняшний день в юридической практике доминирует подход, предполагающий квалификацию лишь предметов преступного посягательства (гл. 28 УК РФ): компьютерная информация, средства ее защиты, программное обеспечение и компьютерные технологии. В случаях, когда они сопровождаются совершением других, сопутствующих им преступлений, с иным предметом преступного посягательства, уголовная ответственность наступает по правилам идеальной совокупности[[43]](#footnote-43). По нашему мнению, такой подход не совсем точно отражает значение компьютерных технологий в совершении преступлений. Статистика и основанный на ее данных анализ уголовных дел убедительно свидетельствует, что при совершении ряда других преступлений активно и весьма эффективно используются информационные технологии.

Так, по данным Следственного комитета МВД России, с начала 90-х годов значительную распространенность и повышенную общественную опасность получили различного рода хищения, совершаемые с применением подложных электронных идентификаторов, модификации данных фискальной памяти систем учета платежей, кредитных карточек, по технической функции являющихся носителями охраняемой законом компьютерной информации. Тем не менее, как свидетельствует Хвоевский С.А., до сих пор существует мнение, что их «трудно отнести к неправомерному доступу к компьютерной информации, так как непонятно, действительно ли речь идет об охраняемой законом компьютерной информации... Среди них наибольшее число вопросов вызывают «взломы» систем спутникового телевидения и изменение фискальной памяти контрольно-кассовых машин»[[44]](#footnote-44).

В 1996 году за подделку кредитных (пластиковых) карт «к уголовной ответственности было привлечено 25 человек, совершивших 300 хищений денежных средств с использованием пластиковых кредитных карточек и поддельных слипов на сумму 600 тыс. долларов. Стоит отметить, что при проведении экспертизы названных платежных документов специалисты были удивлены столь высоким качественным уровнем их подделки»[[45]](#footnote-45).

С технической точки зрения, большее удивление вызывает квалификация преступления, как «подделка платежных документов», когда в действительности (в терминах действующих законов)[[46]](#footnote-46) на основе «несанкционированного доступа» к «персональным данным» совершалось дублирование «машинных носителей информации», входящих в «информационно-телекоммуникационную сеть» расчетно-банковской информационной системы. Если в последствии дубликат банковской карты использован для нарушения «правил обращения с компьютерной информацией, установленных собственником или владельцем информации», то происходит хищение денежных средств собственника.

В действительности злоумышленник получил тайный доступ к информации, находящейся на пластиковой карте, скопировал реквизиты карты и данные, записанные на носителе. Выяснив идентификационный пароль, вошел в банковскую информационную систему и снял со счета денежные средства потерпевшего. При этом расшифровка данных, записанных на карте, производится с помощью специального адаптера, подключенного к компьютеру, оснащенного специальным программным обеспечением. Печать клонируемой карты и внесение информационных кодов данных производится с помощью специального оборудования, работающего под микропроцессорным управлением.

Иначе говоря, злоумышленник заранее запланировал хищение денежных средств, подготовил технические средства (орудие преступления) и сознательно совершил преступление. Таким образом, умысел в совершении кражи денежных средств банковской платежной системы присутствует только в области информационных технологий и в плоскости модификации компьютерной информации. При этом лишь компьютер, выполняющий операции управления периферийным оборудованием «чист перед законом»[[47]](#footnote-47), остальное программное и аппаратное обеспечение преступной технологии свидетельствует не только об умысле, но и о преступном сговоре с производителями указанного технологического оборудования. Сам компьютер служил лишь технологическим звеном реализации преступного деяния и хранителем следов этой деятельности.

Таким образом, на основании терминов законодательства можно говорить о применении в отношении данного преступления целого ряда статей действующего УК, например:

- Статья 272. Неправомерный доступ к компьютерной информации;

- Статья 187. Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов;

- Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети;

- Статья 158. Кража;

- Статья 69. Назначение наказания по совокупности преступлений.

Стоит отметить, что при необходимости можно добавить термин «база данных»[[48]](#footnote-48) и соответствующую квалификацию правонарушений связанных с неправомерным доступом и к ней. Это вполне возможно, так как в зависимости от конкретной технологии, применяемой в различных банковских сетях, пластиковые карты могут представлять собой и возобновляемый (при каждой транзакции) массив данных о счете, и комбинацию микропроцессора с электронным хранилищем данных, и хранилище электронных данных о зарегистрированном клиенте.

Подобные размышления возможны и на этапе расследования подобных преступлений. Отсутствие четкой законодательной терминологии вызывает не только серьезные затруднения в документировании преступной деятельности, но и в выявлении преступников, требует специального толкования экспертов, привлечения специалистов в области вычислительной техники, новейших средств электросвязи и защиты конфиденциальной информации.

К примеру, в настоящее время в МВД России функционируют департаменты и отделы по борьбе с преступлениями в банковской и финансовой системах; по борьбе с преступлениями в сфере высоких технологий; по борьбе с преступлениями в сфере телекоммуникаций и компьютерной информации; однако, до сих пор идут научные дискуссии и практические терзания по вопросу «что такое высокие технологии».

В законодательстве, регулирующем сферу информационных технологий выделены 11 информационных процессов, защищаемых от преступных посягательств:

- 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.

Тем не менее, многие противозаконные действия, совершаемые в указанных ситуациях (совершенные путем кражи, вымогательства, мошенничества или злоупотребления служебным положением) с трудом вписываются в них, так как многие (особенно технические) термины в законодательстве отсутствуют или имеют двусмысленное значение.

Приведем пример. Одной из основных задач на этапе проведения оперативно-розыскных мероприятий (ОРМ) является документирование фактов преступных действий. Исходя из нового закона «Об информации, информационных технологиях и о защите информации» «…документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель».

Если учесть, что в России «документированием называется процесс создания документов по установленным правилам»[[49]](#footnote-49), а под документами понимается ряд «материальных объектов, используемых для закрепления и хранения на нем речевой, звуковой или изобразительной информации, в том числе в преобразованном виде»[[50]](#footnote-50), то в России различается 10 видов документов[[51]](#footnote-51), из них в оперативно-разыскной деятельности используется 4:

Аудиовизуальный документ – это документ, содержащий изобразительную и звуковую информацию, созданный видео- или кинематографическим способом.

Фотодокумент – это изобразительный документ, созданный фотографическим способом.

Фонодокумент – это документ, содержащий звуковую информацию, зафиксированную любой системой звукозаписи.

Документ на машинном носителе – это документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.

Государственный стандарт определил термины, однако в юридической практике редко встретишь подобное толкование документа и безусловное признание их юридического значения. Тем более это касается «установленных правил». Так, давно назрел вопрос о так называемых правилах документирования в оперативно-розыскной деятельности, отменен устаревший приказ о порядке применения технических средств при проведении оперативно-розыскных мероприятий (ОРМ), однако новая инструкция с учетом современного технического развития до сих пор не разработана.

Повсеместное внедрение цифровых технологий фактически поставило крест на использовании аналоговых средств в области подготовки и функционирования средств массовой информации, звукозаписи, кино- и фотосъемки, видео- и звукозаписи. Прогресс неумолим, но достижения одних часто приводят к стремлению присвоить плоды чужого труда, пусть в виртуальном, но зато весьма прибыльном пространстве, тем более, что пробелы в законодательстве делают подобные деяния практически недоказуемыми и ставят перед криминалистами новые сложные задачи по оценке достоверности информационных ресурсов и соответствующих цифровых носителей этой информации.

Другой проблемой является явная тенденция заменить простые термины юридической казуистикой, например, персональные данные, как «информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения….»[[52]](#footnote-52), при этом законодательно допускается лишь три законные реализации доступа к ним:

- согласие субъекта персональных данных на проведение «обработки персональных данных», то есть ОРМ;

- обработка персональных данных отнесена к сведениям, составляющим государственную тайну;

- обработка персональных данных необходима в связи с осуществлением правосудия.

Таким образом, основаниями для проведения оперативно-розыскных мероприятий (т.е. сбора и обработки персональных данных), соблюдая федеральные законы «О персональных данных» и «Об информации, информационных технологиях и о защите информации», остались:

- наличие возбужденного уголовного дела;

- поручения следователя, органа дознания, указания прокурора или определения суда по уголовным делам, находящимся в их производстве;

- постановления о применении мер безопасности в отношении защищаемых лиц, в порядке, предусмотренном законодательством Российской Федерации;

- запросы международных правоохранительных организаций и правоохранительных органов иностранных государств в соответствии с международными договорами Российской Федерации.

Излишняя регламентация термина, не отражая физического (материального) смысла понятий, сузила область применения законов «Об оперативно-розыскной деятельности», «О связи», отдельные ведомственные нормативные акты ОВД. Вместе с тем многие неясные, а порой спорные вопросы практического исполнения закона «Об оперативно-розыскной деятельности» требуют совсем другой коррекции. Новые технологии должны по-новому описываться, не вызывая кривотолков и разночтений.

Например, мероприятия по проведению прослушивания телефонных переговоров должны четко определять, что данное действие связано с фиксацией электрического сигнала связи низкочастотной телефонной линии. Любая другая технология контроля передачи звуковых сообщений (ADSL-коммутация, IP-телефония, частотное или временное уплотнение канала связи, канал сотовой связи) связана с декодированием канала и поэтому должна быть отнесена к мероприятию по контролю технических каналов связи.

Аудио-контроль при проведении ОРМ – это процесс фиксации звуковых колебаний упругой среды в зоне распространения интересующего разговора на материальный носитель. При непрописанности данных объективных ситуаций порой возникают непреодолимые препятствия для использования результатов, полученных с немалым трудом, в качестве доказательства вины.

Иллюстрацией необходимости пересмотра технических аспектов, упоминаемых в законодательстве, может служить недавний случай, произошедший в г. Уфе в 2006 году. Результатом доказательства найма «исполнителя» для совершения убийства служила магнитофонная запись разговора по сотовому телефону стандарта GSM, произведенная в салоне личного автомобиля оперативного работника с ведома «исполнителя». Защита опротестовала данное доказательство, мотивируя тем, что на прослушивание телефонных переговоров не было предписания следователя. Казус заключается не только в том, что канал связи GSM является абсолютно техническим по сути, но и в том, что к контролю канала телефонной связи оперативные работники умышленно не обращались для обеспечения конспиративности.

В плане предложений по совершенствованию законодательства в сфере борьбы с преступлениями в области высоких технологий можно рекомендовать введение терминов и разъяснений по присущим им особенностям не только в ведомственных инструкциях, но и на законодательном уровне. Это не только избавит от необходимости привлекать экспертов для определения таких понятий, как сотовый телефон (обращение имеет место), но и упростит работу как сотрудников оперативных подразделений, так и следственных и судебных органов.

Так, сфера высоких технологий характеризуется как взаимосвязанное множество физических принципов действия, алгоритмических подходов и соответствующих технических решений, обеспечивающих реализацию потребностей человека методами компьютерного управления и процессами, недоступными для непосредственного контроля органами чувств человека.

В такой постановке использование «неконтролируемых» органами чувств человека технологических процессов вполне логично объясняет причины и необходимость введения ограничений всех видов (лицензионных, сертификационных, аттестационных и т.п.), налагаемых на их использование и функциональные возможности.

Для конкретизации и однозначной квалификации правонарушений в сфере высоких технологий необходимо законодательно определить понятийный аппарат, например, в предлагаемом ниже контексте.

Информация – это события или опосредованные факты реальной действительности, отраженные в человеческом сознании.

Информационный сигнал – представление отдельных свойств, событий или фактов в виде изменения физических параметров среды распространения (хранения).

Формализованные данные – это материальное отражение информационного сигнала.

Цифровая информация – это формализованные данные, представленные в виде последовательности двоичных символов.

Компьютер – это программируемое электронное устройство, способное обрабатывать данные и производить вычисления, а также выполнять другие задачи манипулирования символами[[53]](#footnote-53).

Компьютерная информация – это цифровая информация, описывающая принадлежность, пространственно-временные и информационные характеристики информационного сигнала.

Микропроцессор (процессор) – устройство математической обработки данных и управления внешними устройствами, содержащее набор фиксированных операций преобразования поступающих управляющих и обрабатываемых данных.

Машинные носители компьютерной информации – это электронные цифровые запоминающие устройства.

Компьютерные сети – каналы связи, организованные между ЭВМ для обмена компьютерной информацией.

Протокол обмена – соглашение о форме взаимодействия информационными сигналами с целью обеспечения доступности, целостности и конфиденциальности информационных систем.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Под целостностью подразумевается актуальность и непротиворечивость информации.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Документированная информация – это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Даже неполный перечень предлагаемых терминов уже позволяет уточнить умысел, преступное действие и последствия его совершения в каждом из компонентов компьютерной информационной системы. По аналогии с перечнем правонарушений, уже включенных в государственное уголовное законодательство, более подробное членение и толкование компонентов информационных систем позволяет, в частности, наиболее адекватно разработать:

1) терминологический аппарат, позволяющий однозначно трактовать объекты, субъекты, факты и последствия преступной деятельности в сфере высоких технологий;

2) критерии правомерности и допустимости проведения отдельных следственных действий с целью выявления доказательств совершения компьютерного преступления (преступления в сфере высоких технологий);

3) условия возможности оценки полученной информации в качестве доказательственной;

4) тактику проведения следственных действий, проводимых при расследовании дел данной категории;

5) характер уголовно-правовой оценки противодействия расследованию, совершенного способом, аналогичным способу совершения преступления (как повторность преступного деяния, или как воспрепятствование расследованию).

## 3.4 Проблемы уголовно-правовой квалификации преступлений в сфере

## высоких технологий

Российское законодательство, предусматривающее ответственность за совершение преступлений в сфере высоких технологий, включает:

1) Уголовный кодекс РФ;

2) Закон РФ «О милиции» ст.10 и ст.11;

3) Федеральные законы РФ:

- «О связи»;

- «Об информации, информационных технологиях и о защите информации»;

- «О персональных данных»;

- «Об электронно-цифровой подписи»;

- «О коммерческой тайне»;

- «О государственной тайне»;

- «О Безопасности»;

4) Кодекс РФ об административных правонарушениях (административные правонарушения в области связи и информации);

5) Гражданский кодекс РФ. Часть 4 (отношения в области авторского права);

6) Постановления правительства Российской Федерации:

- № 30 от 15 января 1993 г. «Об упорядочении использования радиоэлектронных средств (высокочастотных устройств) на территории Российской Федерации»;

- №157 от 25 февраля 2000 г. «О внесении изменений и дополнений в особые условия приобретения радиоэлектронных средств и высокочастотных устройств»;

- № 770 от 1 июля 1996 г. «Об утверждении положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности»;

- № 643 от 5 июня 1994 г. «О порядке изготовления, приобретения, ввоза в Российской Федерации радиоэлектронных средств (высокочастотных устройств)»;

- № 832 от 17 июля 1996 г. «Об утверждении особых условий приобретения радиоэлектронных средств и высокочастотных устройств»;

- № 909 от 7 августа 1998 г. «О внесении изменений и дополнений в особые условия приобретения радиоэлектронных средств и высокочастотных устройств»;

- № 1235 от 26 сентября 1997 г. «Об утверждении правил оказания услуг телефонной связи»;

Административные правонарушения в области связи и информации (см. Кодекс РФ об административных правонарушениях):

- Статья 7.12. «Нарушение авторских и смежных прав, изобретательских и патентных прав»;

- Статья 13.1. «Самовольные установка или эксплуатация узла проводного вещания»;

- Статья 13.2. «Самовольное подключение к сети электрической связи оконечного оборудования»;

- Статья 13.3. «Самовольные проектирование, строительство, изготовление, приобретение, установка или эксплуатация радиоэлектронных средств и (или) высокочастотных устройств»;

- Статья 13.4. «Нарушение правил проектирования, строительства, установки, регистрации или эксплуатации радиоэлектронных средств и (или) высокочастотных устройств»;

- Статья 13.6. «Использование несертифицированных средств связи либо предоставление несертифицированных услуг связи»;

- Статья 13.7. «Несоблюдение установленных правил и норм, регулирующих порядок проектирования, строительства и эксплуатации сетей и сооружений связи»;

- Статья 13.8. «Изготовление, реализация или эксплуатация технических средств, не соответствующих стандартам или нормам, регулирующим допустимые уровни индустриальных радиопомех»;

- Статья 13.9. «Самовольные строительство или эксплуатация сооружений связи»;

- Статья 13.12. «Нарушение правил защиты информации»;

- Статья 13.13. «Незаконная деятельность в области защиты информации»;

- Статья 13.15. «Злоупотребление свободой массовой информации»;

- Статья 13.18. «Воспрепятствование уверенному приему радио- и телепрограмм»;

- Статья 20.23. «Нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации»;

- Статья 20.24. «Незаконное использование специальных технических средств, предназначенных для негласного получения информации, в частной детективной или охранной деятельности».

Такие дела отличаются широким разнообразием, однако условно их можно разделить на несколько групп.

1. Неправомерный доступ к сетевым ресурсам. Неправомерный доступ в компьютерную сеть, чужой компьютер, базу данных или к любой другой охраняемой законом компьютерной информации является серьезным правонарушением. Подобного рода преступлений очень много. Как показала практика, достать чужие пароли способен даже подросток, при этом искушение бесплатно воспользоваться сервисом связи очень велико.

2. Создание, использование и распространение вредоносных программ для ЭВМ и нарушение правил эксплуатации ЭВМ. Такого рода дела встречаются довольно редко, но факты случаются. В 2006 году в г. Челябинск по этой статье был осужден студент вуза, который послал 10 тысячам абонентов сети сообщение с нецензурной бранью. За эту нелепую шутку студент получил год условно и 3 тысячи рублей штрафа.

3. Защита неприкосновенности личной жизни, тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

4. Незаконный оборот специальных технических средств. Пресечение незаконного оборота специальных технических средств, использование которых невозможно без специального разрешения, каких много: всевозможные прослушивающие устройства, системы скрытого видеонаблюдения и т.п.

5. Незаконный доступ к ресурсам оператора связи. Незаконный доступ к операторам и ресурсам связи, в том числе сотовой, международной и междугородней, до сих пор встречается довольно часто. Мошенники действуют предельно просто: заходят в подъезд, подключаются к чужим телефонным клеммам.

6. Преступления, посягающие на интеллектуальную собственность. Это является важным направлением в борьбе с «пиратами», точнее, преступлениями, посягающими на интеллектуальную собственность (авторское право).

7. Распространение запрещенной информации. Борьба с распространителями порнографии и пиратских дисков не только на прилавках магазинов, но и в Интернете. Владельцев подобных интернет-ресурсов вынуждают закрыть сайт, а российским хостинг-компаниям запрещено размещать и поддерживать ресурсы подобного характера.

8. Борьба с кардингом. Профилактика и пресечение краж баз данных кредитных карт с полной информацией о владельце, отмывания денег и получения незаконно купленного товара.

9. Выявление и пресечение взлома и нарушения работы интернет-сайтов. Уголовных дел по факту взлома интернет-сайтов в России пока не так много, однако, появилась новая тенденция – интернет-шантаж. Хакеры, используя огромные мощности, 24 часа в сутки атакуют известные интернет-ресурсы, тем самым препятствуя его полноценной работе. За прекращение атаки шантажисты, как это водится, требуют денежное вознаграждение.

Контрольные вопросы

1. Что такое компьютерное преступление?

2. Каковы субъекты компьютерных преступлений?

3. Каковы особенности квалификации преступлений в сфере компьютерной информации?

4. Какие нормативно-правовые акты предусматривают ответственность за совершение преступлений сфере высоких технологий?

ГЛАВА 4. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КЛАССИФИКАЦИИ

ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

##

## 4.1 Обзор отечественного и международного опыта

4.1.1 Международная классификация

Обращение к российской истории разработки уголовно-правовых норм ответственности в сфере компьютерных преступлений показывает, что они возникали в ходе постоянной борьбы мнений и не сумели отразить всю специфику регулируемых правоотношений. Опубликованные проекты УК РФ содержали более совершенные и более детальные уголовно-правовые нормы[[54]](#footnote-54).

Названные проблемы уже привели к ряду затруднений с квалификацией некоторых преступных деяний[[55]](#footnote-55). Например, расширение возможностей отечественных информационных сетей, облегчение их подключения к сети Интернет привели к появлению и распространению в Российском сегменте как порнографических, так и экстремистских материалов. При этом рассылке подлежат не сами материалы, а лишь электронные адреса (указатели) на серверы, где хранятся порнографические изображения и материалы. В связи с этим названные деяния «в чистом виде» не подпадают ни под одну из статей главы 28, ни под диспозицию ст. 242 «Незаконное распространение порнографических материалов или предметов» и т.п.

Серьезные проблемы возникают с квалификацией действий, связанных с неправомочным использованием чужих идентификационных номеров в системах сотовой связи. Особенность данной ситуации заключается в том, что эти идентификационные номера свободно передаются через эфир и могут быть получены практически любым лицом, имеющим необходимый набор технических средств, причем этот набор может быть приобретен на вполне законных основаниях и за умеренную плату.

Весьма значительный опыт уголовно-правовой классификации преступлений в сфере компьютерной информации накоплен в ведущих промышленно развитых государствах мира, который вылился в появление так называемых «Минимального списка нарушений» и «Необязательного списка нарушений», разработанных государствами-участниками Европейского сообщества и официально оформленных как «Руководство Интерпола по компьютерной преступности». Так, «Минимальный список нарушений» содержит восемь основных видов компьютерных преступлений: компьютерное мошенничество, подделка компьютерной информации, повреждение данных ЭВМ или программ ЭВМ, компьютерный саботаж, несанкционированный доступ, несанкционированный перехват данных, несанкционированное использование защищенных компьютерных программ, несанкционированное воспроизведение схем.

«Необязательный список» включает в себя четыре вида компьютерных преступлений: изменение данных ЭВМ или программ ЭВМ, компьютерный шпионаж, неразрешенное использование ЭВМ, неразрешенное использование защищенной программы ЭВМ.

Одной из наиболее распространенных из существующих классификаций преступлений в сфере компьютерной информации является кодификатор компьютерных преступлений Генерального секретариата Интерпола, который был положен в основу автоматизированной информационно-поисковой системы, созданной в начале 90-х гг. В соответствии с названным кодификатором все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с латинской буквы Q[[56]](#footnote-56):

1. QA – несанкционированный доступ и перехват:

1) QAH – «Компьютерный абордаж» (hacking). Доступ в компьютер или сеть без права на то. Этот вид компьютерных преступлений обычно используется преступниками для проникновения в чужие информационные сети.

2) QAI – «Перехват» (interception). Перехват при помощи технических средств, без права на то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи.

К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup). Современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата.

Для характеристики методов несанкционированного доступа и перехвата информации рассмотрим используемую специфическую терминологию.

«Жучок» (bugging). Характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала.

«Откачивание данных» (data leakage). Отражает возможность сбора информации, необходимой для получения основных данных в частности о технологии ее прохождения в системе.

«Уборка мусора» (scavening). Характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет два варианта – физический и электронный. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и прочих технологических отходов. Электродный вариант требует исследования данных, оставленных в памяти ЭВМ.

«За дураком» (piggbacking). Состоит в несанкционированном проникновении в пространственные (охраняемые помещения) либо в электронные (программные) закрытые зоны.

«За хвост» (between the lines entry). Заключается в несанкционированном негласном подключении к линии электросвязи законного пользователя в момент его работы в сети ЭВМ. Когда ничего не подозревающий пользователь заканчивает работу и отключает свою ЭВМ от сети, негласно подключенный компьютер преступника продолжает работу в сети по его идентификаторам (паролю доступа в сеть).

«Неспешный выбор» (browsing). В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем ЭВМ. Однажды обнаружив их, правонарушитель может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости.

«Поиск бреши» (trapdoor entry). Используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно.

«Люк» (trapdoor). Является развитием предыдущего алгоритма преступления. В найденной «бреши» программа «разрывается» и туда встраиваются определенное коды управляющих команд. По мере необходимости «люк» открывается, а встроенные команды автоматически обеспечивают несанкционированный доступ к данным;

«Маскарад» (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя.

«Мистификация» (spoofing). Используется при случайном подключении «чужой» системы. Правонарушитель, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него конфиденциальную информацию, например коды доступа в сеть ЭВМ либо сведения, позволяющие идентифицировать пользователя.

3) QAT – «Кража времени». Заключается в неоплате услуг доступа в систему или сеть ЭВМ.

4) QAZ – прочие виды несанкционированного доступа и перехвата.

2. QD – изменение компьютерных данных:

1) QDL/QDT –изменение компьютерных данных без права на то путем внедрения троянской программы.

Логическая бомба (logic bomb) – тайное встраивание в программу для ЭВМ потерпевшего вредоносной программы для ЭВМ (программного модуля), которая должна сработать лишь однажды при наступлении определенных логических условий. При этом «бомба» автоматически ликвидируется при окончании исполнения заданного преступником вредоносного алгоритма.

Троянский конь (trojan horse). Заключается в тайном введении в чужое программное обеспечение вредоносной программы для ЭВМ, которая позволяют негласно осуществлять иные, не планировавшиеся разработчиком программы функции. Эти средства совершения преступления используют для негласного добывания конфиденциальных сведений, например, логина и пароля доступа в сеть ЭВМ «Интернет».

Троянская матрешка – автоматический конструктор для создания вредоносных программ для ЭВМ по заданному преступником алгоритму. Она камуфлируется под обычные программы для ЭВМ (новые версии известных программ, обновления, демонстрационные версии программных продуктов и т.д.). При попадании в программную среду компьютера потерпевшего автоматически срабатывает алгоритм, по которому начинают создаваться модули, из которых впоследствии будет создана вредоносная программа для ЭВМ. После их создания и «привязки» к системному программному обеспечению первоначальная программа – «мать» самоуничтожается. Одновременно с этим запускается алгоритм построения собственно вредоносной программы. После ее создания, модули опять же «привязывают» ее к системным программам и самоликвидируются. Такие циклы могут повторяться многократно (количество «реинкарнаций» определяется преступником), как матрешки, встроенные друг в друга.

2) QDV – «Вирус» (virus). Вредоносная программа для ЭВМ, которая заведомо приводит к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, их системы или сети без предварительного предупреждения пользователя о характере действия программы и не запрашивающая его разрешения на реализацию программой своего назначения (ст. 273 УК РФ).

3) QDW – «Червь» (worm). Саморазмножающийся и самораспространяющийся вирус, который специально создан для функционирования в сети ЭВМ. В отличие от обычного вируса, распространяемого в виде отдельного файла данных, эта вредоносная программа для ЭВМ хранит свои модули на нескольких компьютерах – рабочих станциях сети. При уничтожении одного или нескольких модулей на соответствующем числе рабочих станций она автоматически воссоздает их после каждого подключения «вылеченного» компьютера к сети – как разрезанный на части дождевой червь отращивает новые, недостающие участки тела. Червь, помимо своего оригинального алгоритма, может являться «средством передвижения» (распространения) обычных вирусов, троянских коней и матрешек, а также логических бомб.

4) QDZ – прочие виды изменения данных.

3. QF – компьютерное мошенничество (computer fraud):

1) QFC – компьютерные мошенничества, связанные с хищением наличных денег из банкоматов.

2) QFF – компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (пластиковых карт, сотовых «двойников» и пр.).

3) QFG – мошенничества и хищения, связанные с игровыми автоматами.

4) QFM – манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них путем манипуляции программами.

В этот вид компьютерных преступлений включается метод «Подмены данных (кода)» (data diddling, code change), который обычно осуществляется при вводе-выводе данных. Это простейший и потому очень часто применяемый способ. Для совершения своих преступных деяний современный компьютерный преступник широко использует «нетрадиционные» методы. Обычно компьютерное преступление начинается с искажения входных данных или изъятия важных входных документов. Таким образом можно заставить ЭВМ оплачивать несостоявшиеся услуги, переводить платежи и не имевшие место закупки, формировать ложный курс на бирже и т.д.

5) QFP – компьютерные мошенничества и хищения, связанные с платежными средствами. К этому виду относятся самые распространенные компьютерные преступления, связанные с хищением денежных средств, которые составляют около 45% всех преступлений, связанных с использованием ЭВМ.

6) QFT – телефонное мошенничество (фрикинг): доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих системы электросвязи.

7) QFZ – прочие компьютерные мошенничества.

4. QR – незаконное копирование («пиратство»):

1) QRG/QRS – незаконное копирование, распространение или опубликование компьютерных игр и другого программного обеспечения, защищенного законом об авторском праве и смежных правах (контрафактной продукции).

2) QRT – незаконное копирование топологии полупроводниковых изделий: копирование без права на то, защищенной законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью без права на то, топографии или самого полупроводникового изделия, произведенного с использованием данной топографии.

3) QRZ – прочее незаконное копирование.

5. QS – компьютерный саботаж:

1) QSH – саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ; вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы.

2) QSS – компьютерный саботаж с программным обеспечением: стирание, повреждение, ухудшение или подавление компьютерных данных или программ без права на то.

3) QSZ – прочие виды саботажа.

6. QZ – прочие компьютерные преступления:

1) QZB – использование электронных досок объявлений (BBS) для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности.

2) QZE – хищение информации, составляющей коммерческую тайну: приобретение незаконными средствами или передача информации, представляющей коммерческую тайну без права на то или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества.

3) QZS – использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера.

4) QZZ – прочие компьютерные преступления.

В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска и в настоящее время доступен подразделениям Национальных центральных бюро Международной уголовной полиции «Интерпол» более чем в 120-ти странах мира.

Однако уголовно-правовое регулирование зарубежным законодательством вопросов уголовной ответственности за рассматриваемые преступления не в полной мере укладывается в рамки приведенных классификаций, также обстоит дело и в отечественном законодательстве. Законодательство об уголовной ответственности за эти преступления в различных странах мира существенно отличается друг от друга. Не во всех государствах законодательство в должной мере адаптировано к постоянно возрастающим потребностям усиления уголовно-правовой охраны правоотношений, связанных с использованием компьютерных технологий и информации.

Несмотря на кажущуюся логичность и стройность предложенной классификации, по некоторым мнениям подобные «системы классификации, в погоне за всеобщей универсальностью и гибкостью приобрели существенный недостаток. Ввод литеры «Z» привел к хаотическому (с точки зрения криминалистики) смешению уголовно-правовых начал и технических особенностей автоматизированной обработки информации, что, несомненно, приведет к существенным проблемам при формулировании частных целей и задач расследования преступлений в сфере компьютерной информации»[[57]](#footnote-57).

Однако, в криминалистике «систему взаимообусловленных, подвижно детерминированных действий, направленных на подготовку, совершение и сокрытие преступления, связанных с использованием соответствующих орудий и средств, а также времени, места и других обстоятельств объективной обстановки совершения преступления»[[58]](#footnote-58) называют «способом совершения преступления», что нисколько не противоречит ни приведенной классификации, ни криминалистической теории расследования преступлений в сфере информации[[59]](#footnote-59).

Есть мнение, что «сложность в формулировке этого понятия существует как по причине невозможности выделения единого объекта преступного посягательства, так и множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны»[[60]](#footnote-60), поэтому в поисках истинного юридического значения выражения «компьютерное преступление» многие ученные и практики разошлись во мнениях.

Так, по мнению В.В. Крылова, классификация информационных преступлений подразумевает их деление на противоправные действия по месту, занимаемому в системе ИТ:

а) с компьютерной информацией;

б) в области телекоммуникаций;

в) с информационным оборудованием;

г) с иной информацией[[61]](#footnote-61).

В.А. Копылов подчеркивает значимость аспекта информационной безопасности и подразделяет информационные преступления с позиции интересов субъектов общественных правоотношений:

- «национальной безопасности (например, от распространения инструкций по изготовлению взрывчатых устройств, производству наркотиков, террористической деятельности, призывами к свержению власти);

- несовершеннолетних (оскорбительные формы маркетинга, насилие и порнография);

- человеческого достоинства (расовая дискриминация и расистские оскорбления);

- информации и информационных ресурсов (например, от неправомерного доступа, злонамеренного хакерства и т.п.);

- тайны личной жизни (несанкционированный доступ к персональным данным, электронные оскорбления);

- репутации («навешивание ярлыков», незаконная сравнительная реклама);

- интеллектуальной собственности (несанкционированное распространение защищенных авторским правом работ, например, программного обеспечения, музыки, неправомерное использование торговых марок в качестве доменных имен и т.п.)»[[62]](#footnote-62).

Добавим от себя ряд существенных преступлений в отношении хозяйствующих субъектов в сфере информационных технологий:

- электронных платежных систем (компрометация клиентской базы, подделка кредитных карт, фальсификация электронных платежей, блокирование работы автоматизированных систем);

- средств автоматизированной маркировки (подделка или модификация кодов маркировки, принадлежности, дат и сроков реализации товара);

- фискальных систем тарификации и зачисления платежей (данных электронных кассовых аппаратов и счетчиков тарификации энергетических ресурсов);

- телекоммуникационных и телематических служб (обход тарификации услуг хостинга и телекоммуникационных сервисов обслуживания абонентов, подделка или модификация идентификационных признаков абонентов сетей связи).

Многие авторы подчеркивают проблемы классификации преступлений в сфере компьютерной информации в связи с невозможностью «выделения единого объекта преступного посягательства» и «множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны»[[63]](#footnote-63). Однако мы поддерживаем точку зрения А.П. Полежаева, согласно которой понятие «компьютерная преступность» охватывает преступления, совершаемые с помощью компьютеров, информационно-вычислительных систем и средств телекоммуникаций[[64]](#footnote-64), а также согласны с мнением В.Н. Дранникова, выделяющим их, как «негативное социальное явление в сфере информационных отношений, состоящее из совокупности правонарушений в отношении … информации, … технологий и … систем (информационных) в целях достижения криминальных целей и субъектов, их совершающих»[[65]](#footnote-65).

Поэтому, учитывая сложившееся в криминалистике определение понятия «способ совершения преступления», а также особенности среды совершения преступлений, основой криминалистической классификации преступлений в сфере информационных технологий является анализ объекта преступного посягательства – информации «как сложного многоуровневого объекта на основе выявления набора элементарных операций на каждом из его уровней»[[66]](#footnote-66).

Существующая противоречивость мнений исходит из того, что многие авторы суть нового явления в уголовном праве пытаются понять через призму понятий уголовной науки. Но компьютерное преступление по своей сути очень специфично и своими корнями уходит вглубь профессиональной среды специалистов в области информационных технологий. Единственный путь для уголовно-правовой науки видится в том, чтобы на основе глубокого анализа правонарушений в различных видах информационных технологий пытаться смоделировать юридические понятия и в дальнейшем грамотно регулировать отношения в данной области.

В качестве базовых ИТ мы будем рассматривать четыре основных вида:

- технологии связи;

- технологии автоматизированной обработки информации;

- технологии электронных платежей;

- технологии производства мультимедийной продукции.

В качестве объектов преступного посягательства выделим следующие системообразующие виды:

- сервисы связи и управления;

- компьютерная информация;

- электронные идентификаторы.

Общепризнано, что действия, которые «совершаются по корыстным мотивам и в целях неосновательного обогащения за счет этого имущества, причем без использования субъектами своего служебного положения, не связаны с нарушением хозяйственных связей и отношений в сфере экономики»[[67]](#footnote-67) называются преступлениями против собственности.

Предвидя возражения, которые могут возникнуть в связи с применением в сфере ИТ «вещного права», отметим, что законодательство РФ[[68]](#footnote-68) рассматривает понятия «интеллектуальной собственности», «авторского права» и «права собственности на информацию» и как самостоятельные объекты гражданских прав, и отождествляя вещное и интеллектуальное право собственности на информацию. Еще большее противоречие вносят дефиниции законов о связи прав собственности на информацию в зависимости от прав собственности на материальный носитель.

В отсутствии компромисса в законодательстве полагаем, что вправе предложить в отношении объектов преступлений в сфере информационных технологий квалифицировать правонарушения в соответствии с вызвавшими их побудительными причинами и наличием умысла.

В настоящее время, пожалуй, только Соединенные Штаты обладают набором законодательных актов, более или менее соответствующих современному положению дел. Например, в главе 47 18-го свода законов США есть 1029 статья «Мошенничество по отношению к средствам доступа», которая запрещает мошенническое использование поддельных средств доступа (идентификационных номеров, кредитных карт, номеров учетных записей, различных электронных идентификаторов). Под эту статью подпадают, в том числе, нарушения, связанные с использованием, производством, продажей или владением телекоммуникационным оборудованием, модифицированным или измененным для несанкционированного использования телекоммуникационных услуг, а также действия со сканирующими приемниками, оборудованием или программным обеспечением для модификации телекоммуникационной аппаратуры, направленные на достижение той же цели. Оба типа правонарушений караются штрафом в размере 50 000 долларов или в размере двукратной стоимости причиненного ущерба и/или до 15 лет тюремного заключения. При повторном совершении преступления наказание возрастает до 100 000 долл. и/или до 20 лет лишения свободы[[69]](#footnote-69).

4.1.2 Классификация компьютерных преступлений в соответствии с

законодательством России

В соответствии с законодательством России компьютерные преступления классифицируются следующим образом: компьютерные преступления в сфере оборота компьютерной информации; в сфере телекоммуникаций; в сфере информационного оборудования; в сфере защиты охраняемой законом информации;

Рассмотрим данную классификацию более подробно.

1. Преступления в сфере оборота компьютерной информации:

а) неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ);

б) операции с вредоносными программами для ЭВМ (ст. 273 УК РФ);

в) нарушение авторских и смежных прав в отношении программ для ЭВМ и баз данных, а также иных объектов авторского и смежного права, находящихся в виде документов на машинном носителе (ст. 146 УК РФ);

г) незаконные изготовление в целях распространения или рекламирования, распространение, рекламирование порнографических материалов на машинных носителях, в системе или сети ЭВМ, а равно незаконная торговля ими (ст. 242 УК РФ).

д) изготовление и оборот материалов с порнографическими изображениями несовершеннолетних (ст. 242-1 УК РФ).

2. В сфере телекоммуникаций (ст. 138 УК РФ, ст. 159 УК РФ, ст. 183 УК РФ):

а) незаконное прослушивание телефонных переговоров и иных сообщений;

б) незаконный перехват и регистрация информации с технических каналов связи;

в) неправомерный контроль электронных почтовых сообщений и отправлений;

г) обман потребителей (мошенничество) и др.

Более подробно эту категорию преступлений рассмотрим в п.4.2.

3. В сфере информационного оборудования:

а) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ);

б) незаконный оборот специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации (ч.ч. 2 и 3 ст. 138 УК РФ);

в) незаконный оборот специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения (изменения, уничтожения) информации с технических средств ее создания, обработки, хранения и передачи (ч.ч. 2 и 3 ст. 138 УК РФ);

г) незаконное изготовление в целях сбыта или сбыт поддельных кредитных либо расчетных карт (ст. 187 УК РФ);

д) нарушение авторских прав в отношении топологий интегральных микросхем (ст. 146 УК РФ).

4. В сфере защиты охраняемой законом информации:

а) незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, в том числе персональных данных – любой информации, относящейся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (ст. 137 УК РФ);

б) разглашение охраняемой законом информации: государственной тайны (ст. 276 УК РФ; ст. 283 УК РФ); служебной тайны и профессиональной тайны (ст. 155 УК РФ; ст. 310 УК РФ; ст. 311 УК РФ; ст. 320 УК РФ);

в) незаконные собирание, разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ);

г) незаконные экспорт или передача иностранной организации или ее представителю научно-технической информации, которая может быть использована при создании вооружения и военной техники и в отношении которой установлен экспортный контроль (ст. 189 УК РФ).

5. В сфере информационных правоотношений:

а) распространение заведомо ложной информации (ст. 129 УК РФ; ст. 182 УК РФ);

б) неправомерный отказ в предоставлении или уклонение от предоставления информации (ст. 140 УК РФ; ст. 185.1 УК РФ; ст. 287 УК РФ);

в) сокрытие или искажение информации (ст. 237 УК РФ; ст. 198 УК РФ).

6. В сфере экономики и компьютерной информации:

а) мошенничество в сфере предоставления услуг электросвязи и доступа к информационным ресурсам сети «Интернет» (ст. ст. 165 и 272 УК РФ, 159 и 272 УК РФ, ст. 200 УК РФ);

б) мошенничество в сфере электронного перевода денежных средств (ст. ст. 159, 165, 187, 272 и 273 УК РФ);

в) незаконная деятельность в сфере предоставления услуг электросвязи и доступа к информационным ресурсам сети «Интернет» (ст. ст. 171, 171.1, 173, 178 УК РФ);

г) иные преступления, совершенные в сфере экономики и компьютерной информации (ст. ст. 169, 175, 186, 194, 198, 199 УК РФ).

Практика расследования преступлений, сопряженных с использованием компьютерных средств, свидетельствует о значительном преобладании количества уголовных дел по другим статьям УК РФ над делами, относящихся по своему составу к главе 28 УК РФ. К ним относятся преступления, предусмотренные:

ст. 129 – клевета (в случае размещения в сети Интернет заведомо ложных сведений, порочащих честь и достоинство определенного лица);

ст. 137 – нарушение неприкосновенности частной жизни (при размещении информации, которая относится к категории личной или семейной тайны);

ст. 138 – нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (здесь речь идет об уголовной ответственности за чтение чужих электронных писем).

ст. 146 – нарушение авторских и смежных прав (в части защиты авторских прав на программы для ЭВМ и баз данных);

ст. 159 – мошенничество;

ст. 165 – причинение имущественного ущерба путем обмана или злоупотребления доверием;

ст. 174 – легализация (отмывание) денежных средств или иного имущества, приобретенного незаконным путем (в случае, если преступник перевел деньги со счета зарубежного банка на свой счет в российском банке и получает по этому вкладу начисляемые проценты);

ст. 183 – незаконное получение или разглашение сведений, составляющих коммерческую или банковскую тайну (здесь под категорию коммерческой тайны подпадает список пользователей компьютерной системы с их паролями);

ст. 187 – изготовление и сбыт поддельных кредитных либо расчетных карт и иных платежных документов;

ст. 292 – служебный подлог. Проведение следственных действий по ряду статей УК РФ сопряжено с защитой безопасности интересов государства. Это, в первую очередь:

ст. 207 – заведомо ложное сообщение об акте терроризма (например, в случае ложного сообщения о заминированных объектах посредством сети Интернет);

ст. 276 – шпионаж;

ст. 283 – разглашение государственной тайны, устанавливает ответственность за предание огласке или распространение с нарушением установленного порядка (правил) сведений, составляющих государственную тайну, вследствие чего они становятся известны другим лицам (например, неограниченному числу пользователей Интернет).

## 4.2 Преступления в сфере телекоммуникаций

Как мы упоминали, не всякая информационная технология содержит в своем составе компьютер (хотя практика последних лет свидетельствует о тотальном внедрении цифровых технологий во все без исключения технические устройства). Тем не менее в сфере ИТ существует ряд особенностей, позволяющих приносить незаконную выгоду путем совершения преступлений, связанных с:

- с нарушением лицензионных ограничений на право изготовления, ввоза и продажи;

- с нарушением правил использования радиочастотного диапазона;

- с нарушением авторских прав;

- с незаконным доступом к охраняемой информации;

- с незаконным доступом к сервисам связи;

- с нарушением (блокированием) работы телекоммуникационных систем;

- с обманом потребителей.

Из перечисленных разновидностей преступлений в настоящее время наибольшую опасность представляют, пожалуй, телефонные мошенники. Они пробивают огромные бреши в бюджетах операторов. По оценкам экспертов, размер потерь составляет 3–5% общей суммы доходов, причем данный показатель особенно высок у молодых поставщиков телекоммуникационных услуг и операторов сотовой связи, а ниже всего он у традиционных операторов фиксированной связи. За последние пять лет количество зарегистрированных преступлений в данной области в России увеличилось практически в 10 раз. В 2000 г. таких преступлений было зафиксировано 1,3 тыс., в 2003 г. – 10,9 тыс., в 2005 г. их количество выросло до 14,8 тыс., из которых 2400 являются телекоммуникационными[[70]](#footnote-70). При этом истинные сведения о преступной активности до сих пор остаются скрытыми, латентность преступности в рассматриваемой сфере достигает порядка 90 %.

Наиболее «безобидный» для операторов связи вид преступлений – это мошеннический доступ (access fraud) – несанкционированное использование услуг связи путем перепрограммирования серийных (ESN, Electronic Serial Number) или идентификационных (MIN, Mobile Identification Number) номеров сотовых телефонов, а также мошенничество с украденным телефоном (stolen phone fraud) – использование украденного или потерянного сотового телефона. Существует мнение, что данные преступления даже выгодны салонам связи и операторам сетей связи (вызывает увеличение продаж). Однако это не совсем так. Так, согласно сведениям, опубликованным в журнале Mobile Europe, в 2002 году убытки от телефонного мошенничества по всему миру превысили 13 млрд долл., а в 2003 г. они достигли уже 28 млрд долл. При этом распространены следующие способы мошенничества:

- клонирование терминалов;

- использование услуг связи без намерения платить;

- блокирование линии связи перегрузкой запросами множеством международных переговоров;

- переадресация вызовов дальней связи на собственные каналы;

- проникновение в компьютерную систему для переконфигурации системы базовых станций.

### Клонирование

### Клонирование – это технология, позволяющая на основе одной официально купленной у оператора SIM-карты произвести любое количество SIM-карт с зарегистрированным на них одним и тем же телефонным номером, и которые можно использовать в сотовой сети одного оператора связи. Сначала необходимо объяснить, почему такое возможно. Зашифрованные данные абонента GSM хранятся в небольшой смарт-карте, которая вставляется в телефон. Без карты, называемой также модулем идентификации пользователя (SIM – Subscriber Identification Module), аппарат представляет собой бесполезную оболочку. Карту, идентифицирующую владельца, можно использовать с любым стандартным телефоном. Обнаруженная дыра в безопасности позволяет извлечь секретную информацию из одного SIM и переписать ее в другой, создав точную копию первого телефона. В апреле 1998 г. группа компьютерных экспертов из Калифорнии широко объявила и продемонстрировала, что ей удалось клонировать мобильный телефон стандарта GSM. Ранее всеми по умолчанию предполагалось, что цифровые сети GSM гораздо надежнее защищены от этой напасти, приносящей миллионные убытки сетям аналоговой сотовой телефонии.

Несанкционированный доступ к системам связи стал одной из главных угроз операторам мобильных телекоммуникаций и их абонентам. Он причиняет колоссальный материальный ущерб. По оценкам специалистов, от 10 до 30 % трафика операторов связи приходится на нелегальные звонки. Согласно исследованиям, проведенным специально созданным в США органом – Ассоциацией по контролю за мошенничеством в телекоммуникациях (CFCA), общие потери сотовых операторов от противозаконных действий злоумышленников за период 2003–2005 гг. составили около 54,4 – 60 миллиардов долларов (приблизительно 5 % годового дохода)[[71]](#footnote-71).

Наиболее известным типом мошенничества в сотовой телефонии является клонирование терминалов, особенно распространенное в сетях аналоговых стандартов. Этим термином обозначают программирование параметров легально зарегистрированного сотового аппарата на другом терминале. Известны случаи, когда для одного телефона было создано сразу несколько клонированных копий. Надо ли объяснять, что счета за разговоры с клонированного телефона придется оплачивать владельцу трубки-прототипа.

Хакерское мошенничество (hacking fraud) – проникновение хакеров в компьютерную систему защиты для удаления механизмов защиты или переконфигурации системы в своих целях.

Техническое мошенничество (technical fraud) – неправомочное изготовление (клонирование) телефонных трубок или платежных телефонных карт с фальшивыми идентификаторами абонентов, номеров и платежных отметок.

### No Intention To Pay

NITP – No Intention To Pay – использование услуг связи без намерения платить за них. Контракт (договор на оказание услуг связи) заключается без намерения оплачивать услуги. Данное деяние распространено в основном в регионах, где компании реализуют сотовые телефонные аппараты в кредит. Механизм таков, что злоумышленник приобретает телефонный аппарат в кредит чаще всего по подложным документам. Затем производит максимально возможное количество звонков (сам или предоставляет другим), а затем скрывается. Данное преступление возможно там, где не проверяются удостоверяющие личность данные. В России в настоящее время операторы сотовой связи заключают договор на оказание услуг связи только на основании паспортных данных. Это, безусловно, способствует совершению подписного мошенничества.

По оценкам самих операторов, средний размер ущерба от мошенничества данного типа составляет около 600 долл. за один раз. Основная проблема с выявлением подобных действий злоумышленников – необходимость отличать их от случаев несостоятельности клиента, возникших в связи с непредвиденными обстоятельствами.

Гораздо более популярны среди телефонных пиратов две другие разновидности мошенничества. Это продажа дорогостоящих чужих услуг по демпинговым ценам без оплаты счетов, приходящих от реального оператора (Call Selling), и получение прибыли путем незаконного перевода вызовов на дорогостоящие каналы связи (Premium Rate Service, PRS).

### Call Selling

Действия, попадающие в категорию Call Selling, сегодня поставлены на индустриальную основу и контролируются крупными международными структурами. С целью «максимизировать» собственную прибыль мошенники интенсивно используют одну и ту же линию для множества международных переговоров – до тех пор, пока эта линия не будет отключена. В результате средний ежедневный ущерб оператора в пересчете на одну телефонную линию составляет 15 тыс. долл.

### Premium Rate Service, PRS

Переадресация вызовов дальней связи на собственные каналы PRS, развернутые в других странах, позволяет мошенникам получать за счет оператора, из сети которого поступил вызов, внешне законную прибыль. Действительно, к поставщику дорогостоящей услуги деньги поступают от этого оператора независимо от того, оплатил абонент данную услугу или нет. Именно таким образом хакерская фирма, переводившая вызовы из Англии в собственные каналы в Израиле, в течение месяца «выкачала» из одного британского оператора 750 тыс. долл.

Мошенничество при использовании льготного тарифа включает два действия абонента-нарушителя: получение права пользования льготным тарифом некоторой службы и приобретение абонентом-нарушителем (или группой таких абонентов) нескольких номеров телефонов для того, чтобы звонить по номеру этой службы. В зависимости от схемы оплаты службы с льготным тарифом видоизменяются механизм мошенничества и его отличительные признаки. Если такая служба получает часть доходов от сети, то на ее номер поступают длительные повторяющиеся звонки. Если доход такой службы зависит от количества получаемых звонков, то ей поступает большое количество коротких звонков. Звонки на этот номер не будут оплачены.

Почти классический случай произошел недавно с одним из российских GSM-операторов. Злоумышленники зарегистрировали подставную компанию, арендовали платный номер во Франции и купили у российского оператора 50 телефонов, подключенных по кредитному тарифному плану. Затем они перевезли эти телефоны во Францию и поставили их на автодозвон до арендованного платного номера. Так они сгенерировали огромное количество очень дорогого трафика, приходящего на этот номер. В конце месяца France Telecom выплатил арендаторам номера несколько сотен тысяч долларов. Единственным пострадавшим от мошенников оказался российский сотовый оператор, которому французская компания выставила астрономические роуминговые счета – его ущерб составил около полумиллиона долларов.

### Hacking fraud

Hacking fraud – проникновение в компьютерную систему защиты для удаления механизмов защиты или переконфигурации системы базовых станций в целях использования (либо последующей продажи) имеющихся в системе функциональных возможностей. Так как компьютерная информация системы сотовой связи (ESN и MIN номера) содержится в базовой станции и коммутаторе, то следующий способ неправомерного копирования может осуществляться через компьютерные сети. Данный способ во всех его вариациях очень широко описывался в научной литературе.

Низкочастотные телефонные сети также являются объектом пристального внимания мошенников, среди наиболее распространенных видов преступной деятельности является клонирование (эмуляция) карт оплаты, срыв системы тарификации трафика, перехват управления сервисом и банальное подключение к телефонной линии связи.

Все угрозы, направленные на средства электросвязи и вызванные сознательной деятельностью злоумышленника, можно условно разделить на две группы:

- перехват (кража) информации (техническая разведка);

- несанкционированное использование ресурсов систем связи.

### Перехват (кража) информации

В эпоху межпланетных полетов и персональных компьютеров перехват информации происходит, как правило, по техническим каналам утечки информации. Под таким каналом подразумевается совокупность объекта разведки, технического средства разведки и физической среды, в которой распространяется информационный сигнал. В зависимости от вида каналов связи (радио или проводные), различают следующие технические каналы утечки информации:

- электромагнитный (перехват электромагнитных излучений передатчиков систем и средств связи);

- электрический (съем информации путем контактного подключения к кабельным линиям);

- индукционный (бесконтактный съем информации с кабельных линий).

Электромагнитный канал широко используется для прослушивания систем подвижной радиосвязи, к которым относятся: системы беспроводных телефонов (Cordless Telephony); системы сотовой подвижной связи (Cellular Radio Systems); профессиональные (частные) системы подвижной связи (PMR, PAMR); системы персонального радиовызова (Paging Systems).

Для перехвата пейджинговых сообщений могут использоваться как специализированные программно-аппаратные комплексы, так и системы, которые хорошо подготовленный радиолюбитель может собрать в домашних условиях. Кроме ПК со звуковой картой и программы-декодера, в состав таких «облегченных» комплексов могут входить: сканирующий приемник, доработанный бытовой приемник (с возможностью настройки на частоты пейджинговых компаний), некоторые типы TV-тюнеров для ПК и обычные пейджеры.

Кроме перехвата сообщений, большой ущерб абонентам и компаниям-операторам приносит клонирование, для чего определяется кэпкод (capcode) пейджера, который с помощью программатора «прошивается» во второй (третий и т.д.) пейджер. Некоторые пользователи намеренно «размножают» один пейджер и таким образом превращаются в «группового» абонента (при неизменной оплате услуг).

Для перехвата факсимильных передач используются специализированные комплексы типа 4600-FAX-INT, 4605-FAX-INT, ФАКС-02 и т.п. Система 4600-FAX-INT предназначена для перехвата в реальном масштабе времени любого числа страниц, передаваемых по факсу, всех форм и видов сигналов, поступающих со скоростью от 300 до 9600 двоичных единиц в секунду. Комплекс ФАКС-02 перехватывает факсимильную передачу, сохраняет сигналы на жестком диске компьютера в виде звуковых файлов, производит их демодуляцию и цифровую обработку с целью устранения помех.

### Фрикинг телефонных карточек

Чип, который стоит в телефонных карточках зависит от производителя карточки. Телефонную карточку восстановить нельзя. Карта устроена таким образом, что деньги на ней можно только уменьшать. Для этого обычно используется восьмеричный счетчик с хитрой логикой управления, позволяющей записывать только значения, которые меньше текущего значения счетчика, однако можно сымитировать работу чипа памяти с помощью эмулятора карточки – устройства, собранного на микроконтроллере, эмулирующего работу телефонной карточки.

### Подмена номера звонящего абонента

Это сделать не сложно: если позвонить с телефона, с которого не определяется номер, и послать в нужный момент ложный сигнал-ответ АОН, содержащий номер и категорию абонента. Этот сигнал длительностью 360 мс постоянно повторяется 2-4 раза при стандартном определении номера на АТС.

Сигнал можно сгенерировать с помощью специальной программы Blue box generator или в программе Sound Forge.

Ниже приведены сведения о некоторых устройствах, используемых при совершении рассматриваемой категории правонарушений.

Russian GrayBox – устройство для подмены номера по запросу АО междугородней АТС. На некоторых типах АТС возможно создать ситуацию, когда запрос АОН междугородней АТС попадает непосредственно на абонентский комплект, а не блокируется станционной аппаратурой. Russian GrayBox эмулирует ответ АТС и посылает ложный безинтервальный пакет с чужим номером. В этом случае АТС считает, что звонок по межгороду идет с другого номера (который подставлен в безынтервальном пакете) и счет за переговоры приходит на другой номер. Кроме описанного устройства, специальная техника, предназначенная для проведения телефонного фрикинга, включает и другие конструкции:

Blast Box – усилитель телефонного микрофона;

Blue Box – подражает настоящему оператору, перекрывая магистраль с тоном в 2600 Гц;

Brown Box – создает единую телефонную линию из двух;

Bud Box – создает подсоединение к телефонной линией соседей;

Chartreuse Box – использует электричество вашей телефонной линии;

Chrome Box – манипулирует сигналами дистанционного управления;

Divertor Box – переадресует исходящие или входящие звонки на другой телефон;

Green Box – подражает сигналам «монета опущена», «возврат монеты» и ring back номеру;

Static Box – сохранят высокое напряжение на телефонной линии;

White Box – переносная вспомогательная DTMF-клавиатура;

Yellow Box – добавляет параллельный телефон.

Типология действий, характерных для совершения «мошенничества» в сетях связи, позволяет обозначить для них соответствующие типовые следовоспринимающие объекты и следы, закономерно на них отражающиеся.

## 4.3 Особенности криминального использования компьютерной техники

## в экономической сфере и материальном производстве

Предотвращение незаконного доступа к информационным ресурсам в сфере высоких технологий – не единственное направление правоохранительной деятельности. Как мы уже подчеркивали, универсальность инструментальных возможностей компьютерных технологий позволяет использовать их для фальсификации продуктов интеллектуального труда, объектов авторского права и платежных документов. Об этом свидетельствуют факты[[72]](#footnote-72): «нельзя не отметить, что производители контрафактной продукции начинают использовать более изощренные методы сокрытия признаков подделки: растет качество упаковки поддельных товаров, в контрафактном производстве используются передовые технологии.

Так же в последнее время значительная доля контрафакта (в основном, нелицензионное программное обеспечение для ЭВМ, аудио и видеопродукция) распространяется через Интернет.

В 2006 году в открытом сегменте Интернет было выявлено 13 сайтов. Деятельность 8 из них была направлена на поиск клиентов для сбыта контрафактной продукции, 3 располагались вне российского сегмента сети и представляли ссылки на ресурсы, содержащие контрафактную продукцию, и только 2 осуществляли непосредственное распространение нелицензионной продукции. По данным фактам возбуждено 4 уголовных дела, направлено 9 предписаний на прекращение деятельности ресурсов.

В 2007 году выявлена и прекращена деятельность 18 таких ресурсов, имеющих отношение к распространению контрафактной аудиовизуальной продукции, фонограмм и программного обеспечения.

Надо отметить, что по мнению государственных органов РФ и правообладателей, уровень распространения контрафакта на территории России имеет устойчивую тенденцию к снижению (по видео-, аудиопродукции на 15 %; по промышленным и продовольственным товарам на 20%). Так же, по данным ВSА, в этом году Россия покинула список первых 20 стран с самым высоким уровнем пиратства в сфере программного обеспечения».

### 4.3.1 Подлог документированной информации фискальных систем

Одним из наиболее распространенных видов нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети является нарушение работы контрольно-кассовой машины (ККМ) путем использования недокументированных возможностей с применением специальных средств и программного обеспечения, уничтожающих либо модифицирующих компьютерную информацию, хранящуюся в памяти ККМ. Это позволяет недобросовестным субъектам предпринимательской деятельности сокращать налогооблагаемую базу, формировать неучтенную выручку в виде наличных денег, чем в результате наносить серьезный ущерб государству.

При квалификации подобных деяний следует особо отметить то, что контрольно-кассовая машина согласно абзацу 1 раздела 1 «Общие положения» «Типовых правил эксплуатации контрольно-кассовых машин при осуществлении денежных расчетов с населением» является «счетно-суммирующим, вычислительным и чекопечатающим устройством».

Таким образом, поскольку ККМ служит для обработки информации (выполняет вычислительные функции) и получения результата в необходимой форме (регистрирует на бумажной ленте и в фискальной памяти), а также учитывая, что ее основные функциональные устройства выполнены на электронных компонентах, ККМ полностью соответствует данному определению ЭВМ и является таковой.

Фискальная память – комплекс программно-аппаратных средств в составе контрольно-кассовой техники, обеспечивающих некорректируемую ежесуточную (ежесменную) регистрацию и энергонезависимое долговременное хранение итоговой информации, необходимой для полного учета наличных денежных расчетов и (или) расчетов с использованием платежных карт, осуществляемых с применением контрольно-кассовой техники в целях правильного исчисления налогов.

Контрольно-кассовая машина как имущественный объект, находится в собственности граждан, однако информация, которую они содержат на машинном носителе в фискальной памяти, охраняется законом, доступ к ней действующим законодательством ограничен, а неправомерный доступ или внесение в нее изменений запрещен. Кроме того, Федеральным законом от 22 мая 2003 г. № 54–ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт» специально утвержден порядок ведения кассовых операций в кредитных организациях на территории Российской Федерации (Положение ЦБР от 9 октября 2002 г. № 199–П), определяющий правила эксплуатации данного вида ЭВМ.

Таким образом, модификацию либо уничтожение компьютерной информации в фискальной памяти ККМ лицом, имеющим доступ к данному виду ЭВМ в случае причинения существенного вреда в следствии нарушения ее правил эксплуатации следует квалифицировать по ст. 274 УК РФ. Если же данное деяние совершено третьими лицами – то по ст. 272 как несанкционированный доступ, либо в случае использования специальных программ – по ст. 273 УК РФ. Кроме того, в случаях, предусмотренных уголовным законом требуется дополнительная квалификация по ст. 199.2. УК РФ, предусматривающую ответственность за сокрытие денежных средств либо имущества организации или индивидуального предпринимателя, за счет которых в порядке, предусмотренном законодательством Российской Федерации о налогах и сборах, должно быть произведено взыскание недоимки по налогам и/или сборам, совершенное собственником или руководителем организации либо иным лицом, выполняющим управленческие функции в этой организации, или индивидуальным предпринимателем в крупном размере.

### 4.3.2 Преступления в сфере безналичных расчетов

В настоящее время в мире насчитывается около миллиарда банковских пластиковых карточек, это средство расчетов предоставляет всем использующим ее лицам и организациям множество преимуществ. Как и всякий высокодоходный бизнес, а в особенности в сфере денежного оборота, банковские пластиковые карточки давно стали мишенью для преступных посягательств. Прежде чем дать характеристику преступлений, совершаемых с использованием банковских карт, рассмотрим некоторые базовые понятия и технологии использования этого платежного инструмента.

Под банковской картой понимается средство для составления расчетных и иных документов, подлежащих оплате за счет клиента. Главная особенность платежной карты заключается в том, что она хранит определенный набор и объем информации, который позволяет ей служить одним из средств организации кредитных и/или дебетовых безналичных расчетов.

С точки зрения технических возможностей пластиковые карточки можно классифицировать на магнитные и микропроцессорные.

Магнитная банковская карточка – это только отражение банковского счета владельца: ее магнитный индикатор содержит лишь информацию об имени владельца и номере его счета в банке. Поэтому при расчетах с использованием этой карты каждый раз необходимо обращаться к центральному компьютеру для получения информации о наличии на счете необходимой для оплаты товаров (работ, услуг) суммы денег.

Чиповая карточка содержит микропроцессор (чип) – маленький квадратик или овал на лицевой стороне, в памяти которого содержится вся информация о банковском счете ее владельца: о количестве денег на счете, максимальном размере суммы, которую можно снять со счета единовременно, об операциях, совершенных в течение дня. Чиповая карточка – это одновременно и кошелек, и средство расчета, и банковский счет. И это все благодаря микропроцессору, главным достоинством которого является его высокая способность при постоянстве памяти надежно сохранять и использовать большие объемы информации.

Участниками сделок по банковским карточкам выступают:

- банк, эмитирующий карточку;

- клиент, который пользуется карточкой;

- точка обслуживания карточки, где расплачивается клиент – владелец карточки;

- процессинговая (расчетная) компания – организация, которая поддерживает информационные потоки внутри системы по обслуживанию значительного количества банков и торговых точек.

При предоставлении услуг в начале проводится авторизация карточки клиента. Авторизация карты заключается в проверке по списку утраченных (арестованных) карт, ее платежеспособности, идентификации владельца карты. Данная стадия является наиболее уязвимой в криминальном плане. Похищенная (утраченная) карточка нередко предъявляется к оплате лицом, не являющимся ее владельцем, в результате халатности операторов или в сговоре с ними. После авторизации владелец карты дополнительно санкционирует сделку путем набора в кассовый терминал известного только ему персонального идентификационного номера (PIN).

По данным Главного информационного центра МВД, в 1997 г. было зарегистрировано 53 преступления (в Москве – 12), подпадающих под действие ст. 159 УК «Мошенничество», а сумма причиненного ущерба составила почти 1,6 млн. деноминированных рублей. К уголовной ответственности были привлечены 36 человек. В том же году было зарегистрировано 16 преступлений, квалифицируемых по ст. 187 УК «Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов»[[73]](#footnote-73).

В 1998 г. было зарегистрировано 98 мошеннических действий с пластиковыми карточками (в Москве – 12), и ущерб от них исчислялся суммой 88,2 млн. рублей. К уголовной ответственности были привлечены 122 человека. Фактов изготовления или сбыта поддельных кредитных либо расчетных карточек в том году было зарегистрировано 43, к уголовной ответственности были привлечены четыре человека.

По данным ГУВД г. Москвы, в 1996 году убытки от преступлений, которые понесли банки, использующие на российском рынке пластиковые карточки, составили около $3,5 млн., что примерно в 1,5 раза ниже аналогичного показателя за 1995 год (около $5,5 млн.)[[74]](#footnote-74).

По данным еженедельника «Коммерсантъ», в конце 80-х – начале 90-х годов потери от мошенничеств с карточками в России достигали 5% от общего объема операций. Этот показатель превышал пороговый уровень, равный 3%, за пределами которого данный вид деятельности становится для банков убыточным[[75]](#footnote-75). Ситуацию усугубляет тот факт, что в последние годы происходят качественные изменения в преступности. Увеличивается доля преступлений в сфере оборота банковских карточек, совершаемых хорошо организованными группировками и преступными сообществами (численностью до 50 человек). Эти группировки оснащены самой современной техникой, имеют все необходимые для прикрытия документы, в их состав входят квалифицированные специалисты[[76]](#footnote-76).

По данным Главного информационно-аналитического центра МВД РФ, за 6 месяцев 2007 года было выявлено около 1000 преступлений, связанных с подделкой банковских карт. По данным Следственного комитета МВД РФ общий ущерб составил около 100 млн. рублей.

Преступления, совершаемые с использованием банковских карт, могут быть объединены в следующие категории:

- изготовление поддельных банковских карт;

- сбыт поддельных банковских карт;

- злоупотребления с товарными чеками (слипами);

- использование поддельных банковских карт.

Злоупотребления с подлинными банковскими картами. Данные злоупотребления возможны в случае их попадания в чужие руки, при наличии преступного умысла их законного владельца, а также со стороны руководителей обслуживающих карты лжефирм. К таким преступлениям относятся, например, операции с украденной или потерянной карточкой; превышение счета (получения законным владельцем карты денежных сумм значительно превышающих размеры лимита); ложное заявление о краже или потере банковской карты; временное изъятие карточки у законного владельца для присвоения товаров; незаконное использование карты в период между открытием счета и доставкой карточки владельцу для совершения операций по ней; хищение денежных средств под прикрытием фиктивных предприятий и с использованием корпоративных банковских карт.

Изготовление поддельных банковских карт. Различают полную и частичную подделку карт.

Полная подделка. На сегодняшний день из известных видов мошенничеств полная подделка карточек наиболее распространена. При полной подделке на заготовки поддельных карточек наносятся логотип эмитента, поле для проставления подписи, точно воспроизводятся все степени защиты (используются подлинные реквизиты реально существующих карточек).

Часто используемый преступниками прием – изъятие на время из поля зрения клиента его карту и снятие с нее оттиска. При этом используется простое в изготовлении приспособление. Выплаченные банками деньги из банкомата или за фактически не производившиеся сделки похищаются. По информации МВД России в России действуют более 150 самых различных структур, поставляющих информацию мошенникам с пластиковыми картами.

Использование «белого пластика». Эта мошенническая схема появилась в конце 70-х гг. и получила широкое распространение. Поддельные карточки не имеют внешних реквизитов, по которым возможна их идентификация (логотипа банка-эмитента и платежной системы, голограммы и других степеней защиты). На чистый лист пластмассы переносятся данные уже существующих карточек. Разновидностью преступлений с «белым пластиком» является подделка преступниками полученных в результате неосторожности держателей карточек реквизитов этих карточек, в случае карточек с магнитной полосой или перехват этих реквизитов и PIN-кодов в случае микропроцессорных карточек и их использования для снятия денег через банкоматы.

Частичная подделка. Ее целью является удаление с подлинной карты отмеченных там данных и внесение новых.

Сбыт поддельных кредитных или расчетных карт. Злоупотребления с платежными квитанциями (слипами). Они имеют место при осуществлении или имитации расчетов с карточками. Такие операции могут осуществляться только с участием сотрудников фирм, обслуживающих клиентов по карточкам. При этом возможны следующие варианты действий:

- слипы изготавливаются при помощи чужих подлинных или поддельных карт;

- к оплате предъявляются слипы, полученные ранее при обслуживании законного владельца карточки, но в количестве, превышающем необходимое.

Определенной спецификой отличаются злоупотребления с пластиковыми карточками, используемыми в банкоматах для получения наличных денег.

Известен случай, когда в Венгрии через банкоматы, расположенные в разных концах Будапешта, преступники в течение нескольких минут, используя около 1,5 тыс. поддельных карточек, сняли со счетов 1,5 млн. форинтов. В мошенничестве принимало участие около 150 человек.

В Англии преступники изготовили фальшивый банкомат, который был внешне оформлен как многие другие. При пользовании им законные держатели карточек оставляли свои реквизиты, включая данные о счетах, с помощью которых затем злоумышленники изготавливали поддельные карточки, после чего получали наличные деньги через действующие банкоматы.

С развитием электронной коммерции, появлением виртуальных Интернет-магазинов, где можно сделать заказ на получение товара по почте с персонального компьютера, появляются и новые способы криминальных посягательств с использованием банковских карт (интернет-кардинг). Мошенники пользуются простотой технологии осуществления сделок и несовершенством систем защиты информации в сети.

Следует заметить, что число разновидностей и количество приемов мошеннических действий в этой области неуклонно растет. Это вызывает серьезные опасения.

### 4.3.3 Преступления в сети Интернет

В настоящее время известно уже около 30 видов противоправных действий с помощью Интернета, которые могут практически безнаказанно использоваться мошенниками. По классификации ООН к наиболее опасным относятся:

- промышленный шпионаж. Воровство хакерами промышленных секретов (техническая документация, информация о новой продукции и маркетинговой стратегии). Часто хакеры делают это в интересах корпораций. В области экономических преступлений, таких как мошенничество или промышленный шпионаж, чаще всего задействованы сами сотрудники компаний. По данным ООН, ими совершается свыше 90% таких преступлений;

- саботаж. Главную угрозу представляют так называемые «почтовые бомбы»: преступники терроризируют владельцев электронной почты, парализуя работу их почты мегабайтами мусора;

- вандализм. Хакеры получают доступ к веб-сайтам и базам данных и изменяют их или уничтожают;

- перехват паролей. Воровство паролей у пользователей Интернета с целью совершения преступления под чужим именем. Для этого используется специальное программное обеспечение;

- спуфинг. «Спуферы» используют всевозможные технические хитрости, чтобы взломать защиту чужих компьютеров и получить доступ к хранящейся в них информации. Этим способом воспользовался известный хакер Кевин Митник в 1996 году, взломав домашний компьютер эксперта по компьютерной безопасности ФБР Цутому Шимомуры;

- распространение детской порнографии. Масштабы этой проблемы в Сети увеличиваются в геометрической прогрессии. В последние годы, отмечают эксперты, количество подобных преступлений в США ежегодно увеличивается в четыре раза. Причем преступники наловчились использовать криптографию, с помощью которой шифруют распространяемые порноматериалы;

- азартные игры. Электронные азартные игры за последние годы стали серьезным бизнесом. Проблема в том, что через Интернет доступ к таким игровым сайтам получают граждане тех стран, где азартные игры запрещены или требуют лицензирования;

- мошенничество. От этого вида преступлений, прежде всего, страдает электронная коммерция, торговля акциями и ценными бумагами, а также продажа и покупка товаров через Интернет[[77]](#footnote-77).

Рассмотрим более подробно такой вид противоправных действий с помощью Интернета, как использование компьютерных технологий в сферах торговли людьми и распространения детской порнографической продукции.

Распространение детской порнографической продукции, сводничество, установление и поддержание каналов торговли людьми трансформировались в новые формы. Намечается тенденция к использованию информационных технологий организованными преступными группами (ОПГ) и распространение их деятельности на межгосударственный уровень.

Анализ предпринимаемых органами внутренних дел страны мер, направленных против обозначенных общественно-опасных явлений, позволяет выделить следующие направления противоправного использования сети Интернет при осуществлении торговли людьми[[78]](#footnote-78):

1) размещение объявлений о предоставлении высокооплачиваемой работы за пределами Российской Федерации с целью последующей вербовки для сексуальной эксплуатации;

2) использование служб и сервисов сети Интернет (E-mail, форумы и чаты) для осуществления связи с лицами, идущими на вербовку;

3) использование служб и сервисов сети Интернет (E-mail, форумы и чаты) в качестве оперативного средства связи между членами международных организованных преступных групп, занимающихся торговлей людьми.

Статья 242 УК РФ предусматривает уголовную ответственность за незаконное изготовление в целях распространения или рекламирования, распространение, рекламирование порнографических материалов на машинных носителях, в системе или сети ЭВМ, а равно незаконная торговля ими.

Оценка активности лиц, изготавливающих и распространяющих детскую порнографию в России, показывает, что распространение производится двумя способами:

- непосредственно на носителях (CD, DVD-дисках либо через файлы в Интернет);

- организацией платных WEB-сайтов, содержащих материалы порнографического характера, оплата доступа к которым происходит с использованием электронных платежных средств (кредитные карточки Visa, MasterCard, система E-Gold и т.д.).

Активная борьба с контрафактной продукцией на CD, DVD-дисках в настоящее время перекрыла каналы поставок продукции порнографического характера на Российский рынок. Однако, дилеры разработали новую схему распространения компакт-дисков посредством подачи объявлений на разных сайтах в сети Интернет. Содержимое для них подбирается при помощи Интернет-форумов, на которых отдельные лица обмениваются файлами с фото- и видеоизображениями. Доступ к таким сайтам, как правило, ограничен узким кругом знакомств. Интернет-форумы постоянно перемещаются между серверами.

Лица, занимающиеся распространением детской порнографии в сети Интернет, посредством платных ресурсов по характеру своей деятельности делятся на следующие категории:

- владельцы фотостудий;

- Web-мастера;

- рекламные агенты («адверты»);

- сотрудники «биллинговых» систем (сотрудники операторов сотовой связи и т.п.).

**Их функции заключаются в следующем.**

Фотостудии непосредственно изготавливают фото- и видеоизображения с участием несовершеннолетних, обрабатывают их с использованием компьютерных технологий для получения товарного вида. В дальнейшем эти материалы продаются Web-мастерам, которые размещают эти изображения в Интернет на разработанных ими страницах. Каждый Web-мастер вступает в соглашение с группой рекламных агентов, которые рекламируют сайт с детской порнографией путем размещения рекламы на других сайтах, а также путем рассылки рекламных писем (спама) по E-mail большому количеству адресатов.

Заинтересованные лица просматривают титульные страницы сайта с детской порнографией. В случае, если заинтересованному лицу понравилось оформление и примеры наполнения порносайта, то он путем заполнения полей ввода на специальной странице отсылают свои платежные реквизиты «биллинговой» компании (оператору сотовой связи и т.п.), которая снимает определенную сумму со счета потребителя и затем распределяет ее между Web-мастерами и рекламными агентами, предварительно отчислив себе некоторый процент денежных средств в качестве оплаты своей услуги.

Следует учитывать, что работники фотостудий, Web-мастера, рекламные агенты и сотрудники «биллинговой» компании тесно связаны между собой, общаются друг с другом посредством сети Интернет на различных специализированных форумах и чатах. Они могут представлять одну устойчивую организованную преступную группу.

Анализ ситуации в области распространения порнографии показывает, что в настоящее время существует один основной риск для детей, связанный с информационными технологиями – получение доступа к сайтам Интернет, а также файлообменным сетям, которые содержат материалы порнографического характера (как с участием несовершеннолетних, так и нет). Другие формы риска (втягивание в развратные действия с использованием чатов и форумов и т.д.) пока не получили широкого развития.

Однако стоит отметить, что за последние годы возросло количество публикаций заведомо ложных клеветнических сообщений о якобы оказании сексуальных услуг, которые размещаются на сайтах знакомств, как самими несовершеннолетними, так и в отношении несовершеннолетних и других граждан. Подобные сообщения размещаются с целью мести знакомым по различным мотивам. Несмотря на то, что в этих случаях дети непосредственно не испытывают насилия, страдает их репутация и они получают значительный моральный вред.

Нарушение авторского права. Весьма значительный интерес злоумышленников вызывает не только материальное имущество, но и интеллектуальная собственность. В связи с этим важнейшее значение приобретает защита интеллектуальной собственности от различных посягательств. К интеллектуальной собственности, нуждающейся в защите от различного рода посягательств, могут относиться, прежде всего, товарные знаки, знаки обслуживания, наименования мест происхождения товаров, изобретения, полезные модели, промышленные образцы, авторские права, программы для электронных вычислительных машин, базы данных и прочие информационные ресурсы и продукты, создаваемые или функционирующие, как правило, с применением компьютерных систем.

4.3.4 Применение полиграфических компьютерных технологий

Компьютерная техника вооружила принципиально новыми возможностями разного рода фальсификаторов, в частности, стала возможной подделка печатной продукции в промышленных масштабах. Более двух десятков лет идет непрерывная борьба между разработчиками защитных технологий и изобретателями различных способов их подделки.

Как способов защиты от подделки, так и соответствующих подделок чрезвычайно много, и их число растет с каждым годом. Чтобы не пытаться объять необъятное, остановимся лишь на тех из них, которые пытаются реализовать с помощью компьютерных технологий. Рассмотрим воспроизводство защитных изображений и имитация защитных способов печати.

Защитные изображения можно разделить на три группы:

- тонкая графика и микрографика;

- скрытые изображения;

- переменная информация.

Воспроизведение сложных композиций из графических элементов малой толщины является одним из наиболее распространенных методов защиты печатной продукции – это системы пересекающихся кривых, тонких линий, образующих фоновые рисунки, которые из-за малой толщины линий не могут быть корректно сосканированы, а значит, и воспроизведены с помощью копировальной техники.

Скрытые изображения представляют собой графические элементы, специально спрятанные в оформлении печатной продукции, например, в композициях тонкой графики. Скрытые изображения становятся видимыми либо при рассматривании оттиска под определенным углом, либо при контроле с использованием специальных инструментов. При фальсификации документа скрытые изображения либо разрушаются и становятся невидимыми на копии, либо наоборот – проявляются, свидетельствуя о подделке. Примером второй разновидности таких изображений являются рисунки или надписи, проявляющиеся при фальсификации документа с помощью копировально-множительной техники.

Одним из способов идентификации изделия и упрощения обнаружения подделок может быть печать переменной информации, то есть персонализация документации, разновидностью которой является нумерация иили штриховое кодирование.

Для повышения степени защиты изображений от подделки могут быть использованы специальные краски и лаки, которые делятся на следующие группы:

- обладающие специальными оптическими свойствами в видимом свете;

- обладающие специальными оптическими свойствами в УФ- и ИК-излучении;

- обладающие магнитными или токопроводящими свойствами;

- чувствительные к изменениям температуры (термохромные);

- ароматические;

- изменяющие объем.

Печатные технологии характеризуются различиями в реализации работы с различными красками и реализации изобразительных возможностей по воспроизведению защитной графики. Разными возможностями по нанесению печати обладают трафаретная печать, технологии офсетной (плоской, высокой или глубокой) печати, орловский способ и ирисовая печать[[79]](#footnote-79).

Унификация и автоматизация учета товарно-материальных ценностей добавили в копилку производственных секретов технологию штрих-кодирования. Сегодня штриховое кодирование применяется во множестве различных систем: системах оптовой и розничной торговли, в охранных системах и системах аутентификации, в системах автоматизированного ввода и учета документов, в производственных системах контроля и т.д. Подделав штрих-код, злоумышленник может добиться каких-то собственных целей в обход устанавливаемых правил. Обслуживающий персонал таких систем склонен чересчур доверять технологии штрих-кодирования, полагая, что подделка штрих-кода – весьма сложная задача. Однако, штрих-коды, созданные по закрытым стандартам, поддаются расшифровке путем их анализа. Для создания и печати штрих кода достаточно воспользоваться программной утилитой «Barcode for Office», позволяющей создавать 25 наиболее распространенных видов линейных кодов. Встраивается в приложения Microsoft Office, что позволяет вставлять в них рисунок штрих-кода прямо из меню: Вставка => Объект… => Bocai Barcode. В настоящее время наиболее широко распространены (и успешно фальсифицируются) следующие виды штрих-кода:

EAN-13 CountryFinder – определяет региональную принадлежность или принадлежность к определенным видам печатной продукции товарного кода EAN-13 по первым трем цифрам;

UCC/EAN 128 – создан для автоматизации логистических операций, повсеместно применяется в сетях оптовой и розничной торговли (существует три набора символов данного кода (A, B и C));

Двухмерные штрих-коды – в их основе лежит идея независимой базы данных, содержащей информацию об определенном объекте.

PDF417 – происходит от сокращения Portable Data File (Портативный Файл Данных). Его штрих-кодовый символ состоит из 17 модулей, каждый из которых содержит 4 штриха и пробела (отсюда номер 417). Этот штрих-код открыт для общего пользования. Структура данного кода поддерживает кодирование максимального числа от 1000 до 2000 символов в одном коде при информационной плотности от 100 до 340 символов. Каждый такой код содержит стартовую и стоповую группы штрихов, увеличивающие высоту штрих-кода. Существует также разновидность этого кода – Micro PDF417.

Aztec Code был введен в 1995 году и открыт для общего использования, представляет собой квадратную матрицу с концентрическими квадратами в центре, которые служат для определения позиции кода относительно сканера и мерной линейкой по краю кода. Наименьший штрих-код Aztec имеет площадь 15x15 модулей, наибольший – 151x151. Минимальный код Aztec кодирует 13 цифр или 12 букв, а максимальный – 3832 цифры или 3067 букв или 1914 байт данных. Символика этого кода не требует свободной зоны вокруг штрих-кода. Существуют 32 градации размера кода с возможностью пользовательской установки защиты от ошибок по методу Рида-Соломона (Reed-Solomon) от 5% до 95% от области кода.

Код Data Matrix – двухмерный код от фирмы CiMatrix, разработанный для размещения большого объема информации на ограниченной площади поверхности. Data Matrix может хранить от одного до 500 символов. Data Matrix имеет теоретическую максимальную плотность 500 миллионов символов на дюйм! На практике плотность, конечно, ограничивается разрешающей способностью печатающих устройств и сканеров. Наиболее популярными применениями Data Matrix является маркировка небольших предметов, таких как электронные элементы и печатные платы электронных приборов[[80]](#footnote-80).

4.4 Неправомерный доступ к компьютерной информации

Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к охраняемой законом информации (информации на машинном носителе, в ЭВМ или сети ЭВМ), если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем.

Преступное деяние должно носить характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств, позволяющих преодолеть установленные системы защиты; незаконного применения действующих паролей или маскировки под видом законного пользователя для проникновения в компьютер, хищения носителя информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

Непосредственным объектом преступления является право владельца компьютерной системы на неприкосновенность содержащейся в ней информации.

Объективная сторона данного преступления состоит в неправомерном доступе к охраняемой законом компьютерной информации, т.е. к информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Под информацией в данном случае понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, содержащиеся в информационных системах. Эта информация должна быть чужой для осуществляющего неправомерный доступ лица и защищенной от произвольного копирования.

Доступ к охраняемой законом компьютерной информации – это приобретение и использование лицом возможности получать информацию, вводить ее либо влиять на процесс обработки информации.

Неправомерным следует считать такой доступ, когда лицо действует без разрешения владельца этой системы или сети либо законного полномочия.

Обязательным признаком объективной стороны этого преступления является наступление вредных последствий для собственника или хранителя информации в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Это означает, что сам по себе просмотр информации, хранящейся в оперативной памяти компьютера или на машинном носителе (дискете, CD-R диске), состава преступления не образует.

Под уничтожением информации понимается не простое удаление файлов, а только то, которое приведет к невозможности их восстановления.

Модификация информации – существенное ее видоизменение, совершенное без согласия собственника информации и затрудняющее законное пользование ею.

Блокирование информации – это создание препятствий к свободному ее использованию при сохранности самой информации.

Нарушение работы ЭВМ, системы ЭВМ или их сети имеет место в том случае, если компьютерная система не выполняет своих функций, выполняет их не должным образом или в случае заметного уменьшения производительности системы. Между действиями и последствиями обязательно должна быть установлена причинная связь.

Вопрос о том, когда окончено данное деяние должен решаться так: моментом его окончания является момент отсылки пользователем последней интерфейсовой команды вызова хранящейся информации, независимо от наступления дальнейших последствий. Однако преступлением это деяние станет лишь при наличии последнего условия. При ненаступлении указанных последствий все совершенные до этого действия будут подпадать под признаки неоконченного преступления.

Субъективная сторона преступления характеризуется виной в форме умысла: лицо сознает, что осуществляет неправомерный (несанкционированный) доступ к охраняемой законом компьютерной информации, предвидит, что в результате производимых им действий могут наступить или неизбежно наступят указанные в законе вредные последствия, и желает (прямой умысел) или сознательно допускает (косвенный умысел) их наступление либо относится к ним безразлично.

Мотивы и цели этого преступления могут быть разными: корыстный мотив, желание получить какую-либо информацию либо желание причинить вред. Мотив и цель не являются признаками состава данного преступления и не влияют на квалификацию.

Субъект – лицо, достигшее 16-летнего возраста.

Квалифицирующие признаки:

1. Совершение данного преступления группой лиц по предварительному сговору.
2. Совершение данного преступления организованной группой.
3. Совершение данного преступления лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Если описание первых двух признаков дано в ст. 35 УК РФ, то специальный субъект двух последних можно трактовать как отдельных должностных лиц, программистов, операторов ЭВМ, наладчиков оборудования, специалистов-пользователей специализированных рабочих мест и т.д. Лицом, «имеющим доступ к ЭВМ, системе ЭВМ или их сети» является как лицо, которому в силу разрешения владельца системы или служебного полномочия разрешено получать информацию в компьютерной системе, вводить ее или производить с ней операции, так и лицо, осуществляющее техническое обслуживание компьютерного оборудования и на иных законных основаниях имеющее допуск к компьютерной системе. Лицо, имеющее допуск к компьютерной системе может совершить это преступление лишь в случае доступа к информации, допуска к которой оно не имеет. В случае, когда существенный вред причиняется действиями лица, имеющего правомерный доступ (имеющее допуск) к компьютерной информации, ответственность наступает по ст. 274 УК РФ.

4.5 Создание, использование и распространение вредоносных программ

для ЭВМ

Статья 273 УК РФ предусматривает уголовную ответственность за создание программ для ЭВМ или их модификацию, заведомо приводящее к несанкционированному уничтожению, блокированию и модификации, либо копированию информации, нарушению работы информационных систем, а равно использование таких программ или машинных носителей с такими программами.

Непосредственным объектом данного преступления являются общественные отношения по безопасному использованию ЭВМ, ее программного обеспечения и информационного содержания. Состав части 1 ст. 273 УК РФ формальный и предусматривает совершение одного из следующих действий:

1. Создание программ для ЭВМ, заведомо для создателя приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы аппаратной части.
2. Внесение в существующие программы изменений, обладающих аналогичными свойствами.
3. Использование двух названных видов программ.
4. Их распространение.
5. Использование машинных носителей с такими программами.
6. Распространение таких носителей.

Рассмотрим понятия, введенные в данной статье.

Понятие «вредоносная программа». С точки зрения законодателя, любая программа, специально разработанная или модифицированная для несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения обычной работы ЭВМ собственником информационной системы является вредоносной, и лица, создавшие, использовавшие и распространявшие ее должны быть привлечены к уголовной ответственности.

Существуют различные классификации вирусных программ, но не все они могут иметь значение для криминалистических исследований.

Понятие «создание вредоносных программ». Под созданием вредоносных программ в смысле ст. 273 УК РФ понимаются программы, специально разработанные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций, для которых эти программы предназначены, определенные в документации на программу.

Создание вредоносных программ – целенаправленная деятельность, включающая (в общем виде):

- постановку задачи, определение среды существования и цели программы;

- выбор средств и языков реализации программы;

- отладку программы;

- 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.

Понятие «использование вредоносных программ». Использование вредоносных программ подразумевает применение разработанных иным лицом вредоносных программ при эксплуатации ЭВМ и обработке информации.

Под использованием понимается выпуск в свет, воспроизведение, распространение и иные действия по введению программ в оборот. Использование может осуществляться путем записи в память ЭВМ, на материальный носитель, распространения по сетям, либо путем иной передачи другим лицам.

Уголовная ответственность по этой статье возникает уже в результате создания программы, независимо от того, использовалась программа или нет. По смыслу ст. 273 УК РФ 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 в необходимых 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.

Понятие «распространение вредоносных программ». В соответствии с Законом «О правовой охране программ» (ст.1) под распространением программ понимается «предоставление доступа к воспроизведенной в любой материальной форме, программе для ЭВМ или базе данных, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи в наем, предоставления взаймы, включая импорт для любой их этих целей».

Это определение можно распространить и на вредоносные программы. Субъективная сторона преступления характеризуется прямым умыслом.

Лицо сознает, что создает программу-вирус или модифицирует, доводя до такого качества обычную программу, предвидит возможность или неизбежность наступления при ее использовании другими пользователями ЭВМ вредных последствий и желает их наступления.

Мотив и цель не являются признаками состава этого преступления и не влияют на его квалификацию.

Субъект преступления – лицо, достигшее 16-летнего возраста.

Законодательство РФ предусматривает возможность применения в административном порядке к лицам, совершившим общественно-опасные деяния, но не достигшим возраста, с которого может наступать уголовная ответственность, принудительных мер воспитательного характера.

4.6 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Статья 274 УК РФ устанавливает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ним, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред.

Непосредственным объектом этого преступления является интерес владельца компьютерной системы или сети относительно правильной эксплуатации системы или сети.

Объективная сторона преступления характеризуется действием или бездействием, заключающемся в нарушении правил эксплуатации компьютерной системы или сети, последствием в виде существенного вреда и причинной связью между действием и последствием (материальный состав). Фактически это выражается в несоблюдении или прямом игнорировании определенных правил, обеспечивающих безопасность компьютерной системы или сети (например, непроверке вновь используемых машинных носителей на наличие «вирусных» программ).

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-сотрудников, на которых может быть возложена ответственность в соответствии со ст. 274 УК РФ.

Применительно к данной статье под сетью понимается только внутренняя сеть ведомства или организации, на которую может распространяться его юрисдикция; эта статья распространяется только на локальные сети и ее применение невозможно в глобальных сетях типа «Интернет».

Итак, существует как минимум два вида правил эксплуатации ЭВМ, которыми должны руководствоваться в своей деятельности лица, работающие с ЭВМ.

Первый вид правил – инструкции по работе с ЭВМ и машинными носителями информации, разработанные изготовителем ЭВМ и периферийных технических устройств, поставляемых вместе с данным экземпляром ЭВМ. Эти правила обязательны к соблюдению пользователем ЭВМ под угрозой, самое меньшее, потери прав на гарантийный ремонт и обслуживание.

Второй вид правил – правила, установленные собственником или владельцем информационных ресурсов, информационных систем, технологий и средств их обеспечения, определяющие порядок пользования ЭВМ, системой ЭВМ и сетью ЭВМ, а также иными машинными носителями.

Нарушение и тех и других видов правил, повлекшее причинение предусмотренного уголовным законом вреда собственнику информационного ресурса, является уголовно наказуемым.

1. Уничтожение информации

Уничтожение информации – наиболее опасное явление, поскольку при этом собственнику информационной системы наносится максимальный реальный вред.

Наиболее опасным, разрушающим информационные системы, фактором чаще всего являются действия людей: умышленные или неосторожные действия лиц, имеющих возможность воздействовать на эту информацию.

Причины программно-технического характера, связанные с недостатками или сбоями в работе устройств и систем, встречаются реже и связаны главным образом с эксплуатационными ошибками или бракованными элементами устройств.

В юридической литературе уже, однако, наметились тенденции различной трактовки термина «уничтожение информации», введенного УК РФ.

Некоторые ученые считают, что уничтожение информации представляет собой ее удаление с физических носителей, а также несанкционированные изменения составляющих ее данных, кардинально меняющие ее содержание (например, внесение ложной информации, добавление, изменение, удаление записей).

Другие полагают, что под уничтожением информации следует понимать ее утрату при невозможности ее восстановления.

Ряд специалистов рассматривают уничтожение как приведение информации либо полностью, либо в существенной части в непригодное для использования по назначению состояние[[81]](#footnote-81).

Исходя из базовых определений, В.В. Крылов делает вывод, что под уничтожением компьютерной информации следует понимать полную физическую ликвидацию информации или ликвидацию таких ее элементов, которые влияют на изменение существенных идентифицирующих информацию признаков[[82]](#footnote-82).

2. Модификация информации

Вопрос о модификации информации является весьма сложным. В специализированных словарях термин «модификация» используется для обозначения изменений, не меняющих сущности объекта. Подобные действия над компьютерной информацией напрямую связаны с понятиями «адаптации» и «декомпиляции» программ, уже существующими в действующем законодательстве.

В главе 4 Гражданского кодекса РФ установлено, что лицо, правомерно владеющее экземпляром программы для ЭВМ или экземпляром базы данных (пользователь), вправе без разрешения автора или иного правообладателя и без выплаты дополнительного вознаграждения:

1. Внести в программу для ЭВМ или базу данных изменения исключительно в целях их функционирования на технических средствах пользователя и осуществлять действия, необходимые для функционирования таких программ или базы данных в соответствии с их назначением, в том числе запись и хранение в памяти ЭВМ (одной ЭВМ или одного пользователя сети), а также осуществить исправление явных ошибок, если иное не предусмотрено договором с правообладателем.

2. Изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования. При этом копия программы для ЭВМ или базы данных не может быть использована в иных целях, чем цели, указанные выше, и должна быть уничтожена, если владение экземпляром таких программы или базы данных перестало быть правомерным.

3. Изучать, исследовать или испытывать функционирование такой программы в целях определения идей и принципов, лежащих в основе любого элемента программы для ЭВМ, путем осуществления действий, предусмотренных законом.

4. Воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, при соблюдении следующих условий:

- информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;

- указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;

- информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления другого действия, нарушающего исключительное право на программу для ЭВМ (ст. 1280 ГК РФ).

Таким образом, законом санкционированы следующие виды легальной модификации программ, баз данных (а следовательно, информации) лицами, правомерно владеющими этой информацией:

а) модификация в виде исправления явных ошибок;

б) модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя;

в) модификация в виде частичной декомпиляции программы для достижения способности к взаимодействию с другими программами.

Анализ законодательства показывает, что под модификацией информации следует понимать внесение в нее любых изменений, обусловливающий ее отличие от той, которую включил в систему и которой владеет собственник информационного ресурса.

Вопрос о легальности произведенной модификации информации следует решать с учетом положений законодательства об авторском праве.

3. Копирование информации

Термин «копирование» как изготовление копии объекта не требует дополнительных пояснений.

Правовое регулирование копирования информации имеет ряд специфических особенностей.

Прежде всего следует отметить, что Гражданским кодексом предусмотрен ряд случаев, когда копирование информации и программ является легальным.

Как уже указывалось выше, Гражданским кодексом установлено, что лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без получения дополнительного разрешения правообладателя осуществлять любые действия, связанные с функционированием программы для ЭВМ или базы данных в соответствии с ее назначением, в том числе запись и хранение в памяти ЭВМ.

Запись и хранение в памяти ЭВМ допускаются в отношении одной ЭВМ или одного пользователя в сети, если иное не предусмотрено договором с правообладателем.

Лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без согласия правообладателя и без выплаты ему дополнительного вознаграждения изготавливать или получать изготовление копии программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей и при необходимости (в случае, когда оригинал утерян, уничтожен) для замены правомерно приобретенного экземпляра.

Таким образом, легальному пользователю копирование и перенос информации на машинные носители разрешены:

а) для целей использования информации;

б) для хранения архивных дубликатов.

В иных случаях копирование информации без явно выраженного согласия собственника информационного ресурса независимо от способа копирования, вероятно, является уголовно наказуемым.

Способ копирования, по всей видимости, не имеет существенного значения (от руки, путем фотографирования с экрана, перехват излучений ЭВМ и др.), поскольку защите в данном случае подлежит информация, в каком бы месте она ни находилась.

4. Блокирование информации

Некоторые юристы полагают, что блокирование информации – это невозможность ее использования при сохранности такой информации.

Другие указывают, что блокирование компьютерной информации – это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением.

Наконец, ряд специалистов считают, что блокирование представляет собой создание условий (в том числе и с помощью специальных программ), исключающих пользование компьютерной информацией ее законным владельцем.

Фактически, если незаконное воздействие на ЭВМ или программы для ЭВМ стало причиной остановки («зависания») действовавших элементов или программ ЭВМ, ее устройств и связанных систем, налицо элемент «блокировки» ЭВМ.

«Блокирование» – полагает В.В. Крылов, – результат воздействия на ЭВМ и ее элементы, повлекшего временную или постоянную невозможность осуществлять какие-либо операции над компьютерной информацией[[83]](#footnote-83).

5. Нарушение работы ЭВМ

В литературе указывается, что нарушение работы ЭВМ, системы ЭВМ или их сети может выразиться в их произвольном отключении, в отказе выдать информацию, в выдаче искаженной информации при сохранении целостности ЭВМ, системы ЭВМ или их сети; в возникновении ошибочных команд.

Вероятнее всего в понятие нарушения работы ЭВМ следует включать любую нестандартную (нештатную) ситуацию с ЭВМ или ее устройствами, находящуюся в причинной связи с неправомерными действиями и повлекшую уничтожение, блокирование, модификацию или копирование информации.

6. Иные последствия воздействия на компьютерную информацию

Иными последствиями, указанными в Законе, являются тяжкие последствия (ч. 2 ст. 273, ч. 2 ст. 274 УК РФ) и существенный вред (ч. 1 ст. 274 УК РФ).

Оба понятия являются оценочными, и установление объема причиненного собственнику информационной системы вреда в результате воздействия вредоносных программ или нарушения правил эксплуатации ЭВМ будет осуществляться судом с учетом совокупности полученных данных.

Субъективная сторона преступления характеризуется умышленной виной (исходя из положения, установленного ч. 2 ст. 24 УК РФ). Виновный сознает, что нарушает правила эксплуатации, предвидит возможность или неизбежность уничтожения, блокирования или модификации охраняемой законом информации и причинения существенного вреда, желает или сознательно допускает причинение такого вреда или относится к его наступлению безразлично. Часть 2 ст. 274 УК РФ предусматривает ответственность за те же деяния, повлекшие по неосторожности тяжкие последствия. Понятие таких последствий раскрывалось при анализе ч. 2 ст. 273 УК РФ.

Субъект преступления – специальный, то есть лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети (законный пользователь).

Контрольные вопросы

1. На какие виды подразделяются преступления в сфере компьютерной информации по международной классификации?

2. Каковы проблемы классификации преступлений в сфере компьютерной информации?

3. Как классифицируются компьютерные преступления в соответствии с законодательством России?

4. Назовите и охарактеризуйте наиболее распространенные виды преступлений в сфере телекоммуникаций?

5. Каковы особенности криминального использования компьютерной техники в экономической сфере и материальном производстве?

6. Приведите примеры противоправных действий в отношении документированной информации фискальных систем.

7. Приведите примеры противоправных действий в сфере безналичных расчетов.

8. Какие виды противоправных действий совершаются в сети Интернет?

9. Какие виды противоправных действий совершаются с применением полиграфических компьютерных технологий?

10. Охарактеризуйте преступные деяния, предусмотренные главой 28 УК РФ «Преступления в сфере компьютерной информации».

# РАЗДЕЛ 2. БОРЬБА С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ

# КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ГЛАВА 5. КОНТРОЛЬ НАД ПРЕСТУПНОСТЬЮВ СФЕРЕ ВЫСОКИХ

ТЕХНОЛОГИЙ

5.1 Контроль над компьютерной преступностью в России

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

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

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

К программно-техническим мерам можно отнести защиту от несанкционированного доступа к системе, профилактику от компьютерных вирусов, резервирование особо важных компьютерных подсистем, применение конструктивных мер защит от хищений, саботажа диверсий, взрывов, установку резервных систем электропитания, оснащение помещения 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. По мнению В.А. Минаева, к наиболее значимым следует отнести следующие факторы[[84]](#footnote-84):

- 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;

- серьезное отставание отечественной индустрии средств и технологий информатизации и информационной безопасности от мирового уровня.

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

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

- организацию взаимодействия и координации усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой;

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

- координацию 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.

5.2 Уголовно-правовой контроль над компьютерной преступностью в

России

В целях борьбы с компьютерной преступностью российским законодательством (глава 28 УК РФ) предусмотрена уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ). Содержание этих статей достаточно подробно рассматривалось в главе 4 данного учебного пособия.

Исходя из анализа главы 28 УК РФ, в соответствии со ст. 272 УК РФ, преступлением является неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

В соответствии со ст. 273 УК РФ, преступлением является создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

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

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

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

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

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

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

В целях повышения эффективности борьбы с компьютерной преступностью осуществляется координация деятельности национальных правоохранительных органов в рамках Интерпола.

### 5.3 Особенности оперативно-разыскной деятельности при

### расследовании преступлений в сфере высоких технологий

Прогресс в науке и технике идет в направлении новых информационных технологий. Чем больше компьютерные технологии вовлекаются в коммерческий оборот, тем больше возникает потребность в их защите от противоправных действий. Возникли понятия компьютерной преступности (кибер-преступности), Интернет-преступности. Предметом преступной деятельности стала информация. Стремительно растет число преступлений в сфере интеллектуальной собственности и компьютерной информации. Перед правоохранительными органами России стала неотложная задача: на высоком профессиональном уровне раскрывать преступления в сфере высоких технологий.

Как показывает практика, оперативно-розыскная деятельность (ОРД) по раскрытию преступлений в сфере компьютерной информации должна осуществляться с учетом особой специфики этих преступлений.

Залог успешного осуществления оперативно-розыскных мероприятий состоит прежде всего в том, что стратегию и тактику выявления и раскрытия противоправных деяний необходимо строить на основе хороших знаний специфики состава преступления. Другими словами, сотрудники правоохранительных органов должны обладать хорошими знаниями в области компьютерных технологий, кибернетики, психологии, психолингвистики. Понятно, что в настоящее время такой подход реализовать довольно трудно ввиду слабой подготовки сотрудников МВД в области современных информационных технологий.

В данном разделе рассматриваются некоторые концептуальные положения по осуществлению оперативно-розыскной деятельности при предупреждении и раскрытии преступлений в сфере компьютерной информации.

Учитывая неотложность решения задачи по раскрытию и пресечению преступлений в рассматриваемой предметной области оперативно-розыскная деятельность должна базироваться на следующих принципах[[85]](#footnote-85):

- стратегия и тактика ОРД в области компьютерной информации должны строиться на основе самого широкого использования современных достижений в области информационных технологий;

- на этапе разработки стратегии и тактики ОРД в области компьютерной информации гласно и негласно должны привлекаться высококвалифицированные специалисты по информационным технологиям;

- необходимо существенно пересмотреть качественный состав субъектов при установлении конфиденциального сотрудничества (при осуществлении агентурной работы);

- арсенал оперативной техники необходимо комплектовать современными техническими приборами и устройствами (в т.ч. компьютерными программами), разработанными и успешно применяемыми в информационно-технологической сфере народнохозяйственного комплекса;

- личный состав специализированных оперативных подразделений должен проходить соответствующую подготовку (переподготовку) по применению современных технологий и программных средств.

Без использования самых современных технических и программных средств эффективность оперативно-розыскной деятельности в сфере компьютерной информации резко снизится.

В деятельности подразделений органов внутренних дел может использоваться как универсальное, так и специальное программное обеспечение. Универсальные программы (информационно-поисковой системы, редакторы, электронные таблицы и т.п.) общего назначения не только повышают производительность труда и эффективность работы по выявлению, раскрытию и расследованию преступлений, но и поднимают ее на качественно новый уровень. Специализированные программы могут быть ориентированы на непосредственное их применение при осуществлении оперативно-розыскных мероприятий в направлении борьбы с информационной (в т.ч. компьютерной) преступностью. Остановимся на краткой характеристике таких программных средств.

В настоящее время существуют программные средства, позволяющие[[86]](#footnote-86):

- контролировать процесс попыток взлома компьютерной системы или сети;

- определять индивидуальный почерк работы программиста и идентификационных характеристики разработанных им программ;

- определять перечень электронных адресов (IP) и сайтов Интернет с которыми работал пользователь, список организаций и их географическое местоположение, сведения о лицах, за которыми адреса зарегистрированы;

- негласно регистрировать перечень программ, с которыми работает пользователь;

- определять путь, а в некоторых случаях и конкретный адрес исходящей угрозы для компьютерных систем;

- осуществлять негласный контроль над программистом, определяя характер разрабатываемых продуктов (программы-шпионы и т.п.);

- обнаруживать латентную и закодированную информации в автоматизированных рабочих местах, серверах и сетях передачи данных;

- проводить идентификацию компьютерных систем по следам применения на различных материальных носителях информации;

- осуществлять исследование следов деятельности пользователей в целях его идентификации;

- осуществлять диагностику устройств и систем телекоммуникаций на возможность осуществления несанкционированного доступа к ним;

- исследовать материальные носители с целью поиска заданной информации;

- осуществлять исследование компьютерных технологий для установления возможности решения конкретных преступных задач (крекинг, хакинг, фрикинг и т.п.);

- исследовать программы для ЭВМ и базы данных для определения их возможного предназначения для преступных действий (наличие программных закладок, подпрограмм класса «троянский конь» и т.п.).

Это далеко не полный перечень возможностей существующего программного обеспечения, которое с успехом может использоваться при осуществлении ОРД.

Поисковые программные средства могут найти широкое применение в оперативно-разыскной деятельности (непроцессуальная форма), в том числе и до возбуждения уголовного дела. Факт обнаружения объектов (программ закладок, программного обеспечения для изготовления вирусов или для осуществления взлома компьютерных сетей и т.п.) может послужить основанием для возбуждения дела и производства расследования. В процессуальной форме поисковые программные средства могут найти применение при проведении следственных действий, таких как следственный осмотр (все его виды), выемка предметов, документов и электронной почтовой корреспонденции, следственный эксперимент, выполняемый с целью опытной проверки показаний.

В оперативно-розыскной деятельности в области расследования компьютерных преступлений целесообразно применять криминологическое прогнозирование индивидуального и преступного группового поведения. Определенную информацию можно извлечь, анализируя сетевой трафик локальных и региональных компьютерных сетей. Полезную информацию могут дать и анализ платежей клиентов за телефонные услуги. Прогнозирование может успешно осуществляться в основе первичных материалов оперативного учета, так как его банки информации создаются на основе прогноза вероятности преступного поведения определенных криминогенных контингентов. Именно прошлое (судимость, правонарушения, антиобщественные поступки, большие успехи в области программирования), настоящее (поддержание криминальных связей, паразитизм, склонность к антиобщественным занятиям, склонность создавать программы-«вандалы») их поведение дают основания для прогностических выводов о вероятном противоправном поведении в будущем. Принимаются во внимание социальные оценки, даваемые лицу, представляющему оперативный интерес, роль для него мнения представителей криминогенной и преступной среды. Все это в совокупности является элементами методики криминологического прогнозирования, которое вплетается в оперативно-розыскные мероприятия при реализации форм ОРД (поиске, профилактике, разработке). Естественно, вопросы моделирования и прогнозирования необходимо решать, используя современные информационные технологии и программные средства.

В ряде составов информационных преступлений мотивация поведения преступника имеет особое значение. Преступные мотивы есть по сути своей модификации обычных человеческих мотивов, но направленные на цели, запрещенные законом или связанные с использованием противоправных средств, являются основополагающими в раскрытии и пресечении противоправных действий нарушителей, с помощью методов оперативно-розыскной деятельности. Такое понимание мотивации преступного поведения исключает представление об обреченности человека на преступное поведение, о неисправимости преступников. Поэтому для осуществления ОРД в области компьютерной информации определенный интерес представляют социологические и психологические исследования молодежи, обучающейся компьютерным наукам. Для профилактической деятельности по предотвращению компьютерных преступлений важно проводить изучения мотивов поступков человека. Особый интерес представляет определение уровня ценностно-ориентационного единства (ЦОЕ) в молодежной аудитории. По уровню ЦОЕ можно определить факторы, влияющие на поведение человека в группах и, в какой-то степени, спрогнозировать его стремление к противоправным действиям. Данная методика определения ЦОЕ, которую можно использовать при прогнозировании компьютерной преступности в молодежной аудитории, разработана Маклаковым Г.Ю.[[87]](#footnote-87)

При выявлении и раскрытии преступлений, совершенных с использованием компьютеров, вычислительных систем или иной электронной техники, оперативный сотрудник сталкивается с нетрадиционными следами преступной деятельности или вещественными доказательствами. Поэтому для грамотного использования фактических данных, полученных в ходе осуществления оперативно-розыскных мероприятий по таким преступлениям, базовой юридической подготовки может оказаться недостаточно.

Для успешного осуществления ОРД сотрудникам правоохранительным органам необходимо хорошее знание психологии нарушителя, возможных тактик проведения им атак на компьютерные системы, уровень его знаний и возможность их пополнения.

Для ОРД в области информационных технологий целесообразно привлекать специалистов в области комплексной защиты объектов информатизации, например, сотрудников центров защиты информации в регионах, а также преподавателей и специалистов, обеспечивающий учебный процесс в высших учебных заведениях по направлениям защиты компьютерной информации. При подготовке резерва кадров для оперативных подразделений имеет смысл привлекать молодых специалистов, окончивших высшие учебные заведения по специальностям «Компьютерные системы и сети», «Комплексная защита объектов информатизации» с последующим получением ими второго высшего (юридического) образования либо прохождением курсов первоначальной подготовки в системе МВД России. Интересную информацию для правоохранительных органов могут дать различные социологические и психологические исследования (типа: «Цель хакера», «Какие сайты «Интернет» в сфере информационных технологий, компьютерной информации часто посещаемы?» и т.п.) в молодежной аудитории. Дело в том, что в настоящее время все больше исследователей склоняются к тому, что хакер – это одно из направлений молодежной культуры, как раньше рокеры, металлисты, нудисты. Вопрос спорный, тем не менее, ряд социологических исследований позволил выявить некоторые взгляды молодежи о хакерах. Оказалось, что кто-то занимается хакерством из спортивного интереса, кто-то ради самоутверждения, кто-то ради извлечения материальной выгоды. Такие исследования позволят углубить знания по тактике проведения и философии (психологии) противоправных действий в сфере компьютерной информации и информационных технологий.

Хотелось бы еще остановиться на одном любопытном факте, который необходимо, на наш взгляд, учитывать при расследовании преступлений в сфере информационных технологий. Хорошо известно, что многие, так сказать «традиционные» преступления совершаются в состоянии алкогольного или наркотического опьянения. Существует достаточно количество методических руководств, алгоритмов по проведению операций, по предотвращению преступлений. Однако, мало кому известно, что существует понятие «информационной наркомании» («internet-addiction», «pathological internet use»). В сети Интернет практически открыто предлагаются специально созданная музыка («psychedelic music») и компьютерные программы («psychedelic software»), способные вызвать у человека состояние наркотического опьянения. Складывается парадоксальный факт: если человек распространяет наркотик традиционным путем, то против него может быть возбуждено уголовное дело по соответствующей статье уголовного кодекса, а аналогичное деяние, совершаемое в сети Интернет по распространению «информационных» наркотиков остается безнаказанным. Точнее, тоже может быть возбуждено уголовное дело по соответствующим статьям уголовного кодекса, но вся беда в том, что большинство сотрудников правоохранительных органов даже не знают о возможностях деструктивной информации. А ряд сект (взять хотя бы для примера «Белое Братство») умело пользуются возможностями современных информационных технологий для воздействия на сознание и подсознание человека[[88]](#footnote-88). Действительно, современные информационные технологии могут оказать деструктивное воздействие на сознание и подсознание человека. Проблема Интернет-наркомании стала реальностью. Интернет-наркомания, подобно хроническому алкоголизму или азартной игре, имеет разрушительные последствия на человека, его семью, работу, учебу, а в некоторых случаях, провоцирует на преступления. По мнению профессора Питсбургского университета Кимберли Янг, проблема Интернет-наркомании в США достигла эпидемических размеров, причем число наркоманов («сетеголиков») продолжает расти. В международную классификацию психических расстройств (Diagnostic and Statistical Manual of Mental Disorders – Fourth Edition «DSM-IV», American Psychiatric Association, 1995) внесено заболевание «кибернетические расстройства».

Собственно говоря, в сети Интернет имеется практически открытая информация по изготовлению синтетических наркотиков, но это отдельная тема для изложения. Можно только сослаться на исследования Роганова С.А., специализирующегося на расследовании уголовных дел, связанных с незаконным оборотом наркотиков, который прямо указывает, что методы синтеза наркотиков часто берутся из сети Интернет[[89]](#footnote-89).

Все вышеизложенное еще раз подчеркивает необходимость контакта между правоохранительными органами и специалистами в области биологической кибернетики и информационных технологий.

Сегодня Интернет представляет злоумышленнику большую возможность для проведения разведывательных мероприятий (операций). Анализ сайтов Интернет показывает, что такая работа активно ведется рядом зарубежных государств. Следует обратить внимание на то, что уже давно существует такое понятие, как «компьютерная разведка». В начале 90-х годов аналитики спецслужб США обратили внимание на то, что большая часть необходимой информации без особого труда может быть получена через Интернет. Это позволило пересмотреть структуру финансирования спецслужб в сторону значительного увеличения средств, выделяемых на «компьютерную разведку». Теперь подразделения по исследованию и использованию сети Интернет появились в ЦРУ, ФБР, СИС, МОССАД и других спецслужбах развитых государств. Сфера их деятельности – легальная разведка в глобальной сети, организация каналов связи с агентурой, сбор материалов по оперативно значимым ситуациям, проведение акций «информационной войны», изучение личностных характеристик политиков, ученых, военных, а также важнейших секретоносителей в качестве возможных кандидатов на вербовку или агентов влияния. Подобную разведывательную функцию работники оперативных подразделений ОВД вправе осуществлять в соответствии с Федеральным законом РФ «Об оперативно-розыскной деятельности».

Получение любой информации о преступной деятельности требует определенных тактических усилий и организационных форм: действий негласных сотрудников, оперативно-поисковых групп, оперативных контактов с гражданами. И все же многие сведения о традиционных преступлениях (кражи, вывоз похищенных материальных ценностей, владение оружием), по сравнению со сведениями о преступлениях в сфере высоких технологий, как бы лежат на поверхности: их можно визуально фиксировать, видеть предметы. Преступления в области информационных технологий довольно часто можно получить лишь изучением отношений, то есть глубинных явлений, часто никак не фиксируемых визуально и по материальным следам. В качестве примера можно привести факт. Сведения о преступлениях в сфере электронной торговли не принято афишировать коммерческими структурами. Часто они предпочитают понести убыток, чем потерять свою репутацию.

Учитывая, что основным местом преступления является Интернет (или с использованием Интернета), то процесс сбора оперативной информации легко автоматизировать путем использования специальных программ, называемых интеллектуальными агентами (в среде программистов еще называемы «пауками»). Они способны проводить анализ сайтов, проводить целевой поиск информации в сети Интернет и тем самым находить потенциальных преступников.

Так, недавно ФБР приняло на вооружение новую технологию мониторинга Интернета вместо устаревшей системы Carnivore. Возможности «новорожденного» значительно шире – они позволяют отслеживать сетевую активность подозреваемых в совершении преступлений, одновременно вести базу данных о вполне законопослушных гражданах, а также фиксировать интернет-трафик, включая IP-адреса, просмотры отдельных страниц и электронную почту.

По результатам оперативно-аналитического поиска в оперативных подразделениях целесообразно формировать компьютерные базы данных, используемые:

- для последующей оперативной проверки преступных групп и организаций; для проведения оперативно-профилактических мер;

- для внедрения оперативных работников и негласных сотрудников в среду компьютерной преступности с целью углубления оперативных позиций, необходимых для успешного продолжения стратегической разведки.

Оперативно-аналитический поиск дает возможность использования компьютерного моделирования для раскрытия преступлений в сфере высоких технологий. Одним из перспективных направлений компьютерной инженерии является использование имитационных моделей. Такая модель предусматривает организацию информационных потоков внутри моделируемых систем, воспроизведение на компьютере операций подмены, перераспределения, взаимодействия между отдельными структурными элементами системы и поэтому является достаточно эффективным средством изучения и прогнозирования компьютерной преступности.

Повышение эффективности работы правоохранительных органов по раскрытию и расследованию преступлений в сфере высоких технологий в настоящее время невозможно без интеграции в криминалистику новых информационных технологий.

Контрольные вопросы

1. Какие меры контроля над компьютерной преступностью используются в России?

2. Какие меры уголовно-правового контроля над компьютерной преступностью предусмотрены в законодательстве России?

3. Каковы базовые направления повышения эффективности контроля над компьютерной преступностью в Росси?

4. Каковы особенности оперативно-розыскной деятельности при расследовании преступлений в сфере высоких технологий?

ГЛАВА 6. РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ

КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

6.1 Основные следственные версии, выдвигаемые при расследовании

преступлений в сфере компьютерной информации

При выдвижении версий совершения преступлений в сфере компьютерной информации необходимо учитывать, что они совершаются обычно группой из двух и более человек, хотя не исключена возможность работы преступника – одиночки. В таком случае он сам или, если действует группа, один из ее членов является либо сотрудником данного учреждения, либо имеет свободный доступ к компьютерам (представитель службы технической или программной поддержки, программист, работающий по контракту и т.д.), умеет работать с вычислительной техникой, хорошо представляет, какая информация и где расположена в компьютере. Интерес обычно представляет информация, содержащая государственную или коммерческую тайну (например, информация базы данных передвижении оружия, наркотиков и т.д.).

В основном, как правило, информация преступниками копируется на магнитный носитель, хотя не исключена возможность передачи ее по сетям телекоммуникации, распечатки на бумаге, кино-, фото-, видеосъемки изображения экрана и действий оператора или перехват с помощью специальных технических средств. Копирование может осуществляться как на портативный компьютер (Notebook) с подключением его к локальной вычислительной сети, так и непосредственно к последовательному или параллельному порту конкретной ЭВМ с помощью специального кабеля.

Преступление обычно происходит в рабочее время и внешне не отличается от обычной работы в учреждении. Похищенная информация используется в дальнейшем самими преступниками для подготовки хищений или может быть продана заинтересованным лицам.

Учитывая конкретные обстоятельства, следователем могут быть выдвинуты и проверены следующие общие версии:

1. Преступление совершено сотрудником данного учреждения, либо лицом, имеющим свободный доступ к компьютерной технике.

2. Преступление совершено сторонним лицом, входящим в круг родственников, друзей, знакомых сотрудников учреждений.

3. Преступление совершено группой лиц по предварительному сговору или организованной группой с участием сотрудника данного учреждения, либо лица, имеющего свободный доступ к компьютерной технике и в совершенстве владеющего навыками работы с ней.

4. Преступление совершено лицом или группой лиц, не связанных с деятельностью учреждения и не представляющих ценность компьютерной информации.

Приведенный перечень следственных версий является общим, и в зависимости от конкретной ситуации, может быть расширен.

6.2 Методика расследования преступлений в сфере компьютерной

информации

Хорошо известно, что одними мерами предупреждения не всегда удается предотвратить преступное посягательство. В связи с этим возникает необходимость заниматься не только вопросами защиты средств компьютерной техники, но и решать вопросы расследования компьютерных преступлений.

Принципиальная схема организации взлома защитных механизмов информационных систем достаточно однотипна. Профессиональные компьютерные взломщики обычно работают только после тщательной предварительной подготовки. Они снимают квартиру на подставное лицо, подкупают сотрудников организации, знакомых с деталями электронных платежей и паролями, и работников телефонной станции, чтобы обезопаситься на случай поступления запроса от служб безопасности. Нанимают охрану из бывших сотрудников МВД России. Чаще всего взлом компьютерной сети осуществляется рано утром, когда дежурный службы безопасности теряет свою бдительность, а вызов помощи затруднен. Может быть предложена некоторая общая схема расследования преступления, связанного с неправомерным (несанкционированным) доступом к компьютерной информации.

В ходе расследования основные следственные задачи целесообразно решать в такой последовательности:

1. Установление факта неправомерного доступа к информации в компьютерной системе или сети.
2. Установление места несанкционированного проникновения в компьютерную систему или сеть.
3. Установление времени совершения преступления.
4. Установление надежности средств защиты компьютерной информации.
5. Установление способа несанкционированного доступа.
6. Установление лиц, совершивших неправомерный доступ, их виновности и мотивов преступления.
7. Установление вредных последствий преступления.
8. Выявление обстоятельств, способствовавших преступлению.

На признаки несанкционированного доступа или подготовки к нему могут указывать следующие очевидные обстоятельства:

- появление в компьютере фальшивых данных;

- не обновление в течение длительного времени в автоматизированной информационной системе кодов, паролей и других защитных средств;

- частые сбои в процессе работы компьютеров; участившиеся жалобы клиентов компьютерной системы или сети;

- осуществление сверхурочных работ без видимых на то причин;

- немотивированные отказы некоторых сотрудников, обслуживающих компьютерные системы или сети, от отпусков;

- неожиданное приобретение сотрудником домашнего дорогостоящего компьютера;

- чистые дискеты либо диски, принесенные на работу сотрудниками компьютерной системы под сомнительным предлогом перезаписи программ для компьютерных игр;

- участившиеся случаи перезаписи отдельных данных без серьезных на то причин; чрезмерный интерес отдельных сотрудников к содержанию чужих распечаток (листингов), выходящих из принтеров и т.д.

Определить место и время непосредственного применения технических средств удаленного несанкционированного доступа, не входящих в данную информационную систему или сеть, на практике бывает достаточно трудно. Для установления этих данных необходимо привлекать специалистов. Способ несанкционированного доступа может быть установлен путем производства информационно-технической судебной экспертизы. Перед экспертом следует поставить вопрос: «Каким способом мог быть совершен несанкционированный доступ в данную компьютерную систему?». Целесообразно представить эксперту всю проектную документацию на исследуемую систему (если таковая имеется), а также имеющиеся данные о ее сертификации.

Несанкционированный доступ к закрытой компьютерной системе или сети является технологически весьма сложным действием. Совершить такую акцию могут только специалисты, имеющие достаточно высокую квалификацию. Поэтому поиск подозреваемых следует начинать с технического персонала пострадавших компьютерных систем или сетей (разработчиков соответствующих систем, их руководителей, операторов, программистов, инженеров связи, специалистов по защите информации и других).

Следственная практика показывает, что чем сложнее в техническом отношении способ проникновения в компьютерную систему или сеть, тем легче выделить подозреваемого, поскольку круг специалистов, обладающих соответствующими способностями, обычно весьма ограничен.

При расследовании компьютерных преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ, целесообразно применять следующую последовательность действий:

1. Установление факта и способа создания вредоносной программы для ЭВМ.
2. Установление факта использования и распространения вредоносной программы.
3. Установление лиц, виновных в создании, использовании и распространении вредоносных программ для ЭВМ.
4. Установление вреда, причиненного данным преступлением.
5. Установление обстоятельств, способствовавших совершению расследуемого преступления.

При расследовании нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, необходимо прежде всего доказать факт нарушения определенных правил, повлекший уничтожение, блокирование или модификацию охраняемой законом компьютерной информации и причинивший существенный вред. Кроме того, необходимо установить и доказать:

- место и время (период времени) нарушения правил эксплуатации ЭВМ;

- характер компьютерной информации, подвергшейся уничтожению, блокированию или модификации вследствие нарушения правил эксплуатации компьютерной системы или сети;

- способ и механизм нарушения правил;

- характер и размер ущерба, причиненного преступлением;

- факт нарушения правил определенным лицом;

- виновность лица, допустившего преступное нарушение правил эксплуатации ЭBM;

- обстоятельства, способствовавшие совершению расследуемого преступления.

Кроме того, следователю необходимо знать, что существует много особенностей, которые должны учитываться при производстве отдельных следственных действий. Приведем некоторые из них.

Если следователь располагает информацией, что на объекте обыска находятся средства компьютерной техники, расшифровка данных с которых может дать доказательства по делу, он должен заранее подготовиться к их изъятию. Необходимо обеспечить участие в ходе обыска специалиста по компьютерной технике. По прибытии на место обыска следует сразу же принять меры к обеспечению сохранности ЭВМ и имеющихся на них данных и ценной информации. Для этого необходимо:

- не разрешать кому бы то ни было из лиц, работающих на объекте обыска или находящихся здесь по другим причинам (персоналу), прикасаться к ЭВМ с любой целью;

- не разрешать кому бы то ни было из персонала выключать электроснабжение объекта;

- в случае, если на момент начала обыска электроснабжение объекта выключено, то до его восстановления следует отключить от электросети всю компьютерную технику, находящуюся на объекте;

- самому не производить никаких манипуляций со средствами компьютерной техники, если результат этих манипуляций заранее неизвестен.

После принятия указанных выше неотложных мер можно приступать к непосредственному обыску помещения и изъятию средств компьютерной техники.

При этом следует принять во внимание следующие неблагоприятные факторы:

- возможные попытки со стороны персонала повредить ЭВМ с целью уничтожения информации и ценных данных;

- возможное наличие на компьютерах специальных средств защиты от несанкционированного доступа, которые, не получив в установленное время специальный код, автоматически уничтожат всю информацию;

- возможное наличие на ЭВМ иных средств защиты от несанкционированного доступа;

- постоянное совершенствование компьютерной техники, следствием чего может быть наличие на объекте программно-технических средств, незнакомых следователю.

В целях недопущения вредных последствий перечисленных факторов следователь может придерживаться следующих рекомендаций:

1. Перед выключением питания по возможности корректно закрыть все используемые программы, а в сомнительных случаях просто отключить компьютер (в некоторых случаях некорректное отключение компьютера – путем перезагрузки или выключения питания без предварительного выхода из программы и записи информации на постоянный носитель – приводит к потере информации в оперативной памяти и даже к стиранию информационных ресурсов на данном компьютере).
2. При наличии средств защиты ЭВМ от несанкционированного доступа принять меры к установлению ключей доступа (паролей, алгоритмов и т. д.).
3. Корректно выключить питание всех ЭВМ, находящихся на объекте (в помещении).
4. Не пытаться на месте просматривать информацию, содержащуюся в компьютерах.
5. В затруднительных случаях не обращаться за консультацией (помощью) к персоналу, а вызывать специалиста, не заинтересованного в исходе дела.
6. Следует изъять все носители ЭВМ, обнаруженные на объекте.
7. При обыске не подносить ближе, чем на 1 м к компьютерной технике металлоискатели и другие источники магнитного поля, в т. ч. сильные осветительные приборы и некоторую специальную аппаратуру.
8. Поскольку многие, особенно неквалифицированные, пользователи записывают процедуры входа-выхода при работе с компьютерной системой, а также пароли доступа, на отдельных бумажных листках, следует изъять также все записи, относящиеся к работе с ЭВМ.
9. Так как многие коммерческие и государственные структуры прибегают к услугам нештатных и временно работающих специалистов по обслуживанию средств компьютерной техники, следует записать паспортные данные у всех лиц, находящихся на объекте, независимо от их объяснений цели пребывания на объекте.
10. При изъятии средств компьютерной техники необходимо обеспечить строгое соблюдение требований действующего уголовно-процессуального законодательства. Для этого необходимо акцентировать внимание понятых на всех производимых действиях и их результатах, давая им при необходимости пояснения, поскольку многим участникам следственного действия могут быть непонятны производимые манипуляции. Кроме того, следует опечатывать ЭВМ так, чтобы исключить возможность работы с ними, разукомплектования и физического повреждения основных рабочих компонентов в отсутствие владельца или эксперта. При опечатывании компьютерных устройств следует наложить один лист бумаги на разъем электропитания, расположенный на задней панели, второй – на переднюю панель вверху с захлестом на верхнюю панель и закрепить их края густым клеем. На листах бумаги должны быть подписи следователя, понятых и представителя персонала. При изъятии магнитного носителя машинной информации нужно помнить, что они должны перемещаться в пространстве и храниться только в специальных опломбированных и экранированных контейнерах или в стандартных дискетных или иных алюминиевых футлярах заводского изготовления, исключающих разрушающее воздействие различных электромагнитных и магнитных полей и «наводок», направленных излучений.
11. В случае, когда необходимо сослаться непосредственно на определенный физический носитель, следует указать в протоколе его серийный (заводской) номер, тип, название (если есть) или провести его точное описание (размеры, цвет, класс, надписи, физические повреждения). При отсутствии четких внешних признаков физический носитель запечатывается в отдельную коробку (ящик, конверт), о чем обязательно делается отметка в протоколе проведения следственного действия.
12. В случае невозможности изъятия и приобщения к делу в качестве вещественного доказательства средства компьютерной техники (например, если компьютер является сервером или рабочей станцией компьютерной сети) в обязательном порядке после его осмотра необходимо блокировать не только соответствующее помещение, но и отключать источники энергопитания аппаратуры или, в крайнем случае, создать условия лишь для приема информации с одновременным опломбированием всех необходимых узлов, деталей, частей и механизмов компьютерной системы. Если же возникла необходимость изъятия информации из оперативной памяти компьютера (непосредственно из оперативного запоминающего устройства – ОЗУ), то сделать это возможно только путем копирования соответствующей машинной информации на физический носитель с использованием стандартных паспортизированных программных средств, с соответствующим документальным приложением и в порядке, установленном следующими нормативными документами: Государственный стандарт (ГОСТ) № 6104–84 от 01.07.87 «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения» и Постановление Госстандарта № 2781 от 24.09.86 «Методические указания по внедрению и применению ГОСТ 6104–84». Только с использованием указанных нормативных документов машинная информация будет относиться к разряду «документированной информации», как требует того закон.

К сожалению, практика работы органов прокуратуры и следствия показывает, что рассмотренные рекомендации в большинстве случаев следователями в практической деятельности по расследованию компьютерных преступлений не применяются. В результате неправильного изъятия средств компьютерной техники добытая информация зачастую не может являться доказательством в судебном процессе.

В зарубежных государствах накоплен обширный опыт борьбы с компьютерной преступностью. Однако в России большинство уголовных дел по компьютерным преступлениям остаются нераскрытыми. И дело не в том, что плохо работают сыщики или российские компании экономят на защите своих компьютерных сетей. К сожалению, при высоком техническом оснащении и тщательной подготовке компьютерного преступления поймать преступника очень сложно.

6.3 Типичные следственные ситуации и действия следователя на

первоначальном этапе расследования преступлений в сфере

компьютерной информации

Раскрывать преступления в сфере компьютерной информации сложно, так как нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния многочисленными объективными и субъективными причинами, которые действительно могут иметь место (например, сбой в работе ЭВМ и программного обеспечения, средств электросвязи, энергообеспечивающего оборудования; замыкания в электропроводке и т.п.).

Перечень неотложных следственных действий и оперативных мероприятий, очередность их проведения будут определяться конкретной следственной ситуацией, в которой начинается расследование[[90]](#footnote-90).

Следственная ситуация характеризуется прежде всего объемом и достоверностью исходной криминалистически значимой информации, имеющейся в распоряжении следователя и оперативного работника.

Поводами и основаниями для возбуждения уголовных дел чаще всего служат:

- заявления граждан (конкретных потерпевших);

- сообщения руководителей предприятий, учреждений, организаций и должностных лиц (базирующиеся, как правило, на материалах контрольно-ревизионных проверок и сообщениях служб безопасности);

- сведения, полученные в результате проведения оперативно-розыскных мероприятий;

- непосредственное обнаружение следователем, прокурором или судом признаков преступления;

- статьи, заметки и письма, опубликованные в средствах массовой информации, а также в сети Интернет.

Как правило, возбуждению уголовного дела предшествует предварительная проверка материалов, поступивших в правоохранительные органы. В связи с этим, следователь может заблаговременно ознакомиться с собранными по делу материалами, совместно с оперативным сотрудником выбрать в тактическом отношении наиболее оптимальный момент для возбуждения дела, а также определить характер и последовательность первоначальных следственных действий, организационных и иных мероприятий. Успех расследования преступления в сфере компьютерной информации во многом обеспечивают: быстрота и решительность действий следователя и оперативного сотрудника в самые первые часы производства по делу; организованное взаимодействие с различными подразделениями правоохранительных органов; наличие специалиста в области компьютерной обработки информации (возможно, пользователя ЭВМ).

В ходе предварительной проверки материалов при решении вопроса о возбуждении уголовного дела следователь должен, прежде всего, получить четкое и полное представление о предмете посягательства, месте его нахождения и условиях охраны; о характере деятельности и структуре объекта, где возможно было совершено преступление; об особенностях технологии производства; изучить конкретные условия деятельности данного объекта, существующий там порядок учета и отчетности, систему товаро- и документооборота, коммуникативные и иные тактико-технические характеристики используемой компьютерной техники, организацию охраны. Необходимо также хорошо знать служебные обязанности лиц, имеющих прямые или косвенные отношения к орудиям обработки и компьютерной информации, которые стали предметом преступного посягательства.

К типичным признакам подготовки, совершения и сокрытия преступления в сфере компьютерной информации относятся: появление в ЭВМ, системе ЭВМ или их сети фальшивых данных; несанкционированные изменения структуры файловой системы, программного обеспечения и конфигурации ЭВМ, системы ЭВМ или их сети; необычные (нестандартные) проявления в работе СВТ и их программного обеспечения; частые сбои в работе аппаратуры; жалобы клиентов на предоставление некачественного доступа к ЭВМ, системе ЭВМ, их сети или компьютерной информации; сверхурочная работа некоторых сотрудников на ЭВМ, в системе ЭВМ или их сети, нарушение установленного графика их эксплуатации; нерегламентированный доступ к ЭВМ, системе ЭВМ, их сети и к компьютерной информации отдельных субъектов; нарушение правил работы с компьютерной информацией и несанкционированные манипуляции с ней; чрезмерный интерес отдельных субъектов (клиентов, сотрудников) к содержанию чужих распечаток (листингов) и компьютерной информации определенной категории; случаи перезаписи отдельных данных и компьютерной информации без серьезных требуемых на то причин; применение на рабочем месте и вынос с работы личных машинных носителей информации под различными предлогами (записи игр и т.п.); исследование мусорных корзин (контейнеров) с технологическими отходами компьютерной обработки информации; случаи утечки конфиденциальной информации, либо обнаружение негласных устройств ее получения; нарушение установленных правил оформления документов при работе с ЭВМ, системой ЭВМ, их сетью или компьютерной информацией; создание копий определенной категории данных и компьютерной информации, не предусмотренных технологическим процессом; несоответствие данных, содержащихся в первичных (исходных) документах, данным машинограмм и иным более поздним по времени создания документам; подозрительно частое обращение одного и того же пользователя к данным и компьютерной информации определенной категории.

Чтобы детально разобраться в особенностях деятельности потерпевшего (физического или юридического лица), следователю и оперативному сотруднику необходимо ознакомиться с соответствующей справочной литературой, изучить ведомственные нормативные акты. Исключительно важное значение имеют консультации со специалистами. Для этих целей могут быть привлечены любые лица, обладающие необходимыми знаниями и опытом для дачи консультаций по делу. Как правило, это квалифицированные сотрудники различных организаций, осуществляющих свою деятельность в сфере информации, информатизации и защиты информации. Наиболее предпочтительны сотрудники: Федеральной службы по техническому и экспортному контролю (ФСТЭК); центров защиты информации; оперативно-технических подразделений правоохранительных органов; подразделений «К» при УСТМ МВД России; специалисты межрегиональных Центров защиты информации, функционирующих на базе гражданских высших учебных технических заведений; научные работники исследовательских институтов и лабораторий, а также учебных заведений.

Для преступлений в сфере компьютерной информации типичны три ситуации первоначального этапа расследования:

1. Сведения о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя отсутствуют.

2. Имеются сведения о причинах возникновения преступления, способе его совершения, но нет сведений о личности преступника.

3. Известны причины возникновения преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

В первых двух следственных ситуациях обычно планируют и осуществляют следующие неотложные следственные действия, оперативно-розыскные, организационные и иные мероприятия:

1) получение объяснения (допрос) заявителя или лиц, на которых указано в исходной информации как на возможных свидетелей (очевидцев);

2) вызов и инструктаж необходимых специалистов для участия в осмотре места происшествия;

3) осмотр места происшествия (с осмотром, предварительным исследованием и изъятием машинных носителей и компьютерной информации, средств вычислительной техники (СВТ), документов и т. п.);

4) проведение оперативно-розыскных мероприятий в целях установления причин совершения преступления, выявления лиц, виновных в его совершении, определения рабочего места преступника, обнаружения следов и других вещественных доказательств;

5) изучение справочной литературы, ведомственных нормативных актов, положений, инструкций, правил эксплуатации конкретного СВТ и порядка работы с компьютерной информацией, а также консультации с соответствующими специалистами;

6) наведение справок в контролирующих, инспектирующих и лицензирующих организациях и их структурных подразделениях ФСТЭК России, налоговой инспекции, Комитете по контролю за использованием радиочастот, Энергонадзоре, Госпожнадзоре, КРУ, торговой инспекции и т.п.);

7) истребование материалов контрольных проверок, инвентаризаций и ревизий (соблюдения правил обработки информации, системы защиты конфиденциальной информации, оборота электронных документов и др.) за интересующий следствие период, в случае необходимости – организовать их производство (в т.ч. повторно);

8) выемку и последующий осмотр недостающих документов (в том числе находящихся в электронной форме на машинных носителях информации), характеризующих производственную операцию, в ходе которой по имеющимся данным совершены преступные действия, а также орудий (СВТ, программ для ЭВМ, компьютерной информации, предметов, материалов и др.), с помощью которых они, возможно, были изготовлены;

9) допросы подозреваемых и/или свидетелей, ответственных за данный участок работы, конкретную производственную операцию и защиту конфиденциальной информации;

10) обыски на рабочих местах и по месту проживания подозреваемых;

11) назначение экспертиз – программно-технической, радиотехнической, технической, бухгалтерской, полимерных материалов и изделий из них и иных.

Дальнейшие действия планируются с учетом дополнительной информации, полученной при производстве вышеуказанных действий.

При наличии третьей следственной ситуации необходимо:

1) изучить поступившие материалы с позиций их полноты, соблюдения норм уголовно-процессуального законодательства и порядка их передачи в органы предварительного следствия. При необходимости следует принять меры к получению недостающей процессуальной информации;

2) решить вопрос о возможности задержания преступника с поличным и о необходимых в связи с этим мероприятиях;

3) личный обыск задержанного;

4) осмотр места происшествия с участием соответствующих заранее приглашенных специалистов;

4) допрос задержанного;

5) обыски на рабочем месте и по месту проживания задержанного;

6) установление связей задержанного и лиц, причастных к совершению преступления;

7) допрос свидетелей (очевидцев);

8) допрос подозреваемого;

9) выемка и осмотр следующих вещественных доказательств и документов:

- подлинных документов, удостоверяющих личность преступника и наличие у него соответствующих специальных познаний, характеризующих те производственные операции, в процессе которых допущены нарушения и преступные действия (в том числе документов, находящихся в электронной форме на машинных носителях информации);

- орудий подготовки, совершения и сокрытия преступления;

- предмета преступления;

10) допрос лиц, названных в документах, переданных в следственные органы, как допустивших нарушения, ответственных за конкретный участок работы по фактам установленных нарушений;

11) истребование, а при необходимости производство выемки нормативных актов и документов, характеризующих порядок и организацию работы в данном подразделении с конфиденциальной информацией, с бланками строгой отчетности, компьютерной информацией, ЭВМ, системой ЭВМ, их сетью и т. п.;

12) допрос свидетелей, причастных к соответствующим производственным операциям или подозреваемых в связях с преступником;

13) анализ полученной информации и решение вопроса о необходимости назначения судебных экспертиз, проведения ревизии, инвентаризации или контрольной проверки (в том числе повторной).

В очередность перечисленных следственных действий, оперативных и организационных мероприятий могут быть внесены коррективы в зависимости от изменения ситуации.

Контрольные вопросы

1. Перечислите и охарактеризуйте основные следственные версии, выдвигаемые при расследовании преступлений в сфере компьютерной информации.

2. В какой последовательности целесообразно решать основные следственные задачи в ходе расследования преступления, связанного с неправомерным (несанкционированным) доступом к компьютерной информации?

3. Какие обстоятельства могут указывать на признаки несанкционированного доступа или подготовки к нему?

4. Какую последовательность действий целесообразно применять при расследовании компьютерных преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ?

5. Что необходимо установить и доказать при расследовании нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети?

6. Какие особенности должны учитываться при производстве следственных действий по расследованию преступлений в сфере компьютерной информации?

7. Какие неблагоприятные факторы следует принять во внимание при производстве следственных действий?

8. Каких рекомендаций должен придерживаться следователь в целях недопущения вредных последствий неблагоприятных факторов?

9. Каковы типичные следственные ситуации и действия следователя на первоначальном этапе расследования преступлений в сфере компьютерной информации?

ГЛАВА 7. ОСОБЕННОСТИ ТАКТИКИ РАССЛЕДОВАНИЯ

ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

7.1 Осмотр места происшествия

Все следственные действия по делам о преступлениях в сфере компьютерной информации проводятся в строгом соответствии с правилами, регламентированными действующим уголовно-процессуальным законодательством, но с учетом следующих основных особенностей:

- следственное действие должно быть заблаговременно подготовлено и детально спланировано; в каждом следственном действии должны принимать участие специалисты, четко представляющие свои задачи, права и обязанности;

- понятые должны обладать минимально необходимыми специальными познаниями в области обработки компьютерной информации (на уровне бытовых пользователей персонального компьютера), следователь и специалисты – познаниями в части полной сохранности (неизменяемости) компьютерной информации, содержащейся на осматриваемом (изымаемом) средстве электронно-вычислительной техники; для осмотра, обыска и выемки компьютерной информации и ее носителей заранее должны быть подготовлены необходимые СВТ и материалы.

При осмотре места происшествия в состав следственно-оперативной группы в зависимости от конкретной следственной ситуации, помимо следователя, должны входить:

- специалист-криминалист, знающий особенности работы со следами по преступлениям данной категории;

- специалист по СВТ;

- сотрудник ФСТЭК, Центра защиты информации [при наличии на месте происшествия конфиденциальной компьютерной информации, машинных носителей с ней, специальных средств защиты от НСД и(или) технических средств негласного получения (уничтожения, блокирования) компьютерной информации];

- специалист по сетевым технологиям (в случае наличия периферийного оборудования удаленного доступа или локальной компьютерной сети);

- специалист по системам электросвязи (при использовании для дистанционной передачи данных каналов электросвязи);

- оперативные сотрудники (отдела «К» или ОБЭП);

- участковый оперуполномоченный, обслуживающий данную территорию;

- инспектор отдела вневедомственной охраны (в случае, когда место происшествия или СВТ, находящееся на нем, одновременно является охраняемым объектом);

- специалист для проведения цветной фото- или видеосъемки следственного действия.

При необходимости в состав СОГ могут быть включены незаинтересованные в деле специалисты, знающие специфику работы осматриваемого объекта (инженеры-электрики, бухгалтеры со знанием СВТ, специалисты спутниковых систем связи, операторы компьютерных систем и сетей электросвязи, др.).

7.2 Особенности тактики производства обыска при расследовании

преступлений в сфере предоставления услуг сети Интернет

Известно, что обыск как самостоятельное процессуальное действие имеет свое определенное место и играет специфическую роль в сфере правоприменительной деятельности полномочных органов в рамках уголовного судопроизводства. Решаемые с его помощью задачи во многом обусловлены той или иной следственной ситуацией, складывающейся в ходе предварительного расследования. Своевременное и грамотное проведение обыска способствует достижению целей отправления правосудия. Результаты данного следственного действия могут быть положены, как в основу обвинительного приговора, так и послужить основанием для исключения факта необоснованного привлечения лица к уголовной ответственности.

По делам о преступлениях в сфере предоставления услуг «Интернет» рассматриваемое следственное действие, как правило, носит неотложный характер. Основанием для его производства является наличие достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться орудия преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела (ст. 182 УПК РФ).

Цели обыска: обнаружение, фиксация и изъятие перечисленных выше объектов, а также выявление и задержание разыскиваемых и подозреваемых лиц.

В криминалистике в зависимости от объекта выделяют различные виды обыска. По делам о преступлениях в сфере предоставления услуг сети Интернет типичными являются обыск в помещении (жилище) и личный обыск подозреваемого (обвиняемого), который там находится. Эти следственные действия имеют определенную специфику, которая обусловлена как предметом, так и орудием преступного посягательства – компьютерной информацией. Характерные особенности последней накладывают отпечаток на все стадии проведения указанного следственного действия. Рассмотрим их подробнее.

Представляется, что подготовительный этап обыска играет главенствующую роль во всем процессе реализации замысла следственного действия. Тщательная и глубокая проработка всех нюансов сложившейся накануне обыска следственной ситуации во многом определяет его результативность. Практика показывает, что многое зависит от тесного взаимодействия следователя со специализированным органом дознания – Отделом «К» при Управлении специальных технических мероприятий (УСТМ) МВД (УВД) республики, края (области). С его помощью обеспечивается должная оперативная осведомленность следователя об обстоятельствах, связанных с проведением обыска, которая помогает избежать ряда тактических ошибок, а также грамотно решить вопрос о привлечении к его проведению высококвалифицированных специалистов в области компьютерной техники и понятых, имеющих определенные знания в этой сфере.

В работе Илюшина Д.А.[[91]](#footnote-91) перечислены мероприятия, которые необходимо осуществить следователем на подготовительном этапе обыска:

1. Определить месторасположение и планировку помещения, которое должно быть подвергнуто обыску. Выяснить характер охраны объекта. Определить пути возможного отхода подозреваемого (обвиняемого).

2. С помощью специалиста в области телекоммуникаций определить расположение в данном помещении узлов связи, локализацию разводки коммуникационных сетей. Рассмотреть возможность наличия на объекте средств радиосвязи, используемых подозреваемым (обвиняемым). Установить их идентификационные характеристики: абонентский номер, позывной, рабочую частоту, логин и пароль доступа для работы в сети Интернет.

3. Выяснить, какие средства электронно-вычислительной техники (далее по тексту «СВТ») находятся в помещении, в котором предполагается провести обыск (по возможности установить их технические характеристики). Данные сведения могут быть получены у провайдера сети Интернет или оператора электросвязи. При этом во многих случаях требуется консультация с соответствующим специалистом. В дальнейшем полученная информация будет использована для определения границ места, подлежащего обыску, и внесет определенность относительно искомых предметов (документов).

4. Установить, какие средства защиты информации и СВТ от несанкционированного доступа находятся по месту, где предполагается провести обыск; выяснить источники их питания и рассмотреть возможность их обесточивания до момента начала обыска. Это позволит исключить факты преднамеренного уничтожения искомых документов или предметов.

5. Установить тип источников электропитания СВТ и расположение пунктов их обесточивания для предотвращения возможных попыток уничтожения искомой компьютерной информации, содержащейся в оперативной памяти компьютерных устройств.

6. Пригласить специалистов, обладающих достаточными знаниями, умениями и навыками для оказания действенной помощи следователю при подготовке и в ходе производства обыска. Для этих целей наиболее подходят универсальные специалисты в области цифровых средств электросвязи и компьютерной техники.

7. Подготовить соответствующие СВТ, специальную аппаратуру и материалы для поиска, осмотра, фиксации и изъятия искомой компьютерной информации, документов и предметов.

8. Определить дату, время и место проведения обыска, его продолжительность, а также меры, направленные на обеспечение его скоротечности и конфиденциальности. Наиболее благоприятной ситуацией является момент отсутствия подозреваемого (обвиняемого) на месте обыска. Это обстоятельство позволяет исключить активное противодействие с его стороны и предоставляет возможность следователю быстро обнаружить и грамотно изъять искомые объекты. При этом следует отметить, что присутствие на месте обыска сослуживцев или близких родственников подозреваемого (обвиняемого), как правило, формирует у них определенное негативное отношение к совершенному преступному деянию. Данное обстоятельство может быть использовано для определения тактики проведения последующих следственных действий, например, допросов свидетелей.

9. Провести инструктаж лиц, привлекаемых к участию в обыске, с постановкой конкретных персональных задач.

10. Изучить личность подозреваемого (обвиняемого). Особое внимание следует обратить на уровень его профессиональных умений и навыков в области компьютерных технологий.

11. Пригласить понятых, обладающих определенными знаниями в сфере компьютерной информации и телекоммуникаций.

По прибытии на место проведения обыска специфика действий следователя будет состоять в следующем:

1. Определить места возможного отхода подозреваемого (обвиняемого) или выноса предметов и документов, имеющих значение для уголовного дела (запасный выход, окна и другие). Принять меры к установлению наблюдения за ними.

2. Быстро и внезапно войти в обыскиваемое помещение (жилище). Если их несколько – одновременно войти во все. На наш взгляд, нельзя согласиться с доводами отдельных авторов, полагающих, что «в некоторых случаях, когда это возможно или целесообразно, непосредственно перед входом в обыскиваемое помещение следует обесточить его».[[92]](#footnote-92) Представляется, что при внезапном отключении электропитания в помещении (жилище) и наличии предположений у преступника о намерении сотрудников правоохранительных органов провести обыск, последним могут быть предприняты меры по уничтожению следов преступного посягательства. Таким образом, теряется не только фактор внезапности, но и ценные вещественные доказательства.

3. В случае оказания активного сопротивления со стороны лиц, находящихся на объекте обыска, принять меры по нейтрализации противодействия и скорейшему проникновению в обыскиваемое помещение (жилище).

4. Организовать охрану места обыска и наблюдение за ним. Охране подлежат: периметр обыскиваемых площадей; СВТ; хранилища машинных носителей информации (МНИ); все пункты (пульты) связи, охраны и электропитания, находящиеся на объекте обыска (в здании, помещении, на производственной площади); специальные средства защиты от несанкционированного доступа; хранилища ключей (кодов, паролей) аварийного и регламентного доступа к СВТ, помещениям и другим объектам (пультам, пунктам, стендам, сейфам и т. п.), попавшим в зону обыска.

По поводу дальнейших действий следователя на месте обыска в современной криминалистической литературе дискутируются различные точки зрения.[[93]](#footnote-93) Мы, в свою очередь, полагаем, что после реализации вышеуказанных мероприятий следователь должен перейти к обзорной стадии обыска и выполнить следующие действия:

1. Определить местонахождение подозреваемого (обвиняемого) на объекте обыска (если обыск осуществляется в его присутствии). При обнаружении – принять меры к отстранению его от пультов управления техническими устройствами, дистанцировать от них и организовать охрану.

2. Определить и отключить специальные средства защиты информации и СВТ от несанкционированного доступа, особенно те, которые автоматически уничтожают компьютерную информацию и МНИ при нарушении процедуры доступа к ним, порядка их использования и (или) установленных правил работы с ними; принять меры к установлению пароля (кода) санкционированного доступа и ключа шифрования-дешифрования информации.

3. Установить наличие телекоммуникационной связи между СВТ, СВТ и каналами электросвязи. При наличии компьютерной сети любого уровня технической организации в первую очередь должна быть осмотрена и подвергнута обыску управляющая ЭВМ – сервер, который хранит в своей оперативной и постоянной памяти наибольшую часть компьютерной информации, управляет другими СВТ, имеет с ними прямую и обратную связь. В этом случае следует учитывать то обстоятельство, что у сообщников подозреваемого (обвиняемого) или у него самого (если обыск производится в его отсутствие) имеется реальная возможность уничтожения искомой компьютерной информации дистанционно с помощью СВТ, находящихся вне периметра обыскиваемой зоны (в другом помещении, здании, населенном пункте и т. д.). Применительно к этому положению вызывает недоумение утверждение некоторых авторов о том, что «… подключением компьютера к телефонной или телетайпной линиям невозможно уничтожить или изменить информацию на нем. Эта информация может быть лишь пополнена или куда-либо передана»[[94]](#footnote-94).

Для предупреждения вышеуказанных негативных последствий необходимо в зависимости от ситуации и рекомендаций специалиста временно или на длительный срок, частично или полностью отключить СВТ или локальную вычислительную сеть от технических устройств, находящихся за периметром обыскиваемой зоны. Отключение может быть произведено как на программном, так и аппаратном уровне. Если СВТ работает в режиме «электронной почты», то предпочтительнее оставить его до конца обыска в работающем состоянии в режиме «приема почты», исключив возможность какой-либо обработки и обратной передачи информации. Эту работу может сделать только квалифицированный специалист. Все выполняемые им действия должны быть зафиксированы с помощью видеозаписи и отражены в протоколе рассматриваемого следственного действия.

4. Определить СВТ, находящиеся во включенном состоянии, характер выполняемых ими операций и название программ. Особое внимание необходимо уделить печатающим и видеоотображающим устройствам (принтерам и мониторам). Распечатки информации (листинги) при необходимости должны быть изъяты и приобщены к протоколу следственного действия; изображение на экране монитора – видеограмма[[95]](#footnote-95) изучено и детально описано в протоколе (можно также зафиксировать его на видеопленку либо сделать распечатку на бумаге с использованием специальных сканирующих программ).

Если специалист установит, что на момент обыска на каком-либо СВТ происходит уничтожение информации либо ее машинного носителя, необходимо срочно всеми возможными способами приостановить этот процесс и начать обследование с данного места или СВТ.

5. При обследовании персонального компьютера необходимо:

а) установить последнюю исполненную программу и (или) операцию, а при возможности – все, начиная с момента включения компьютера;

б) произвести экспресс-анализ компьютерной информации, содержащейся на жестком диске и в оперативной памяти с целью получения данных, имеющих значение для следствия (их скорейшее получение позволит скорректировать тактику обыска и порядок производства последующих следственных действий).

6. В случае совершения преступления выделенной категории с помощью портативного или малогабаритного (мобильного) СВТ, например, коммуникатора или сотового радиотелефона, организовать производство личного обыска подозреваемого (обвиняемого) или лиц, находящихся в обыскиваемом помещении. Это возможно лишь в тех случаях, когда у следователя имеются достаточные основания полагать, что лицо скрывает при себе предметы либо документы, которые могут иметь значение для уголовного дела (ч. 2 ст. 184 УПК РФ). Личный обыск такого лица производится по правилам, изложенным в ч. 3 ст. 184 УПК РФ.

Детальный этап обыска является очень трудоемким и требует слаженной работы всех участников следственного действия. Необходимо четко организовать поисковые мероприятия, направленные на выявление тайников, в которых могут находиться предметы и документы. Ими могут быть и сами компьютерные устройства – аппаратные и программные модули, входящие в состав ЭВМ, системы ЭВМ или их сети.

Следует также уделить внимание действиям, направленным на обнаружения записей, которые содержат сведения о чужих логинах и паролях доступа в компьютерную сеть «Интернет». Например, в 2002 году при производстве обыска у подозреваемого Б. сотрудниками Отдела «К» при УСТМ ГУВД Самарской области были изъяты листы бумаги, содержащие 19 конфиденциальных реквизитов пользователей сети Интернет (логинов и паролей), напротив каждого из которых стояли даты и время. В ходе дальнейшего расследования уголовного дела, возбужденного по ст. 165 ч. 1 и ст. 272 ч. 1 УК РФ, было установлено, что записи выполнены собственноручно Б. и полностью соответствуют реквизитам протокола провайдера, отражающим все сеансы работы пользователей в сети Интернет. Эти вещественные доказательства в совокупности с другими доказательствами, даже с учетом активного противодействия следствию со стороны Б., позволили привлечь его к уголовной ответственности за совершение 38 преступлений.

На заключительном этапе обыска составляются: протокол следственного действия и описи к нему; вычерчиваются планы обыскиваемых помещений, схемы расположения СВТ относительно друг друга, инженерно-технических коммуникаций, а также схема соединения СВТ между собой и с другими техническими устройствами; проводится дополнительная фотосъемка или видеозапись.

7.3 Осмотр средств вычислительной техники

Осмотр СВТ обычно приводит к необходимости их изъятия для последующего экспертного исследования и(или) приобщения к делу в качестве вещественного доказательства.

В протоколе осмотра СВТ фиксируют:

- его тип (назначение), марку (название), конфигурацию, цвет и заводской номер (серийный, инвентарный или учетный номер изделия);

- тип (назначение), цвет и другие индивидуальные признаки соединительных и электропитающих проводов; состояние на момент осмотра (выключено или включено);

- техническое состояние – внешний вид, целостность корпуса, комплектность (наличие и работоспособность необходимых блоков, узлов, деталей и правильность их соединения между собой), наличие расходных материалов, тип используемого машинного носителя информации;

- тип источника электропитания, его тактико-технические характеристики и техническое состояние (рабочее напряжение, частота тока, рабочая нагрузка, наличие предохранителя, стабилизатора, сетевого фильтра, количество подключенного к нему электрооборудования, количество питающих электроразъемов-розеток и т.д.);

- наличие заземления («зануления») СВТ и его техническое состояние; наличие и техническая возможность подключения к СВТ периферийного оборудования и(или) самого СВТ к такому оборудованию либо к каналу электросвязи; имеющиеся повреждения, не предусмотренные стандартом конструктивные изменения в архитектуре строения СВТ, его отдельных деталей (частей, блоков), особенно те, которые могли возникнуть в результате преступления, а равно могли спровоцировать возникновение происшествия;

- следы преступной деятельности (следы орудий взлома корпуса СВТ, проникновения внутрь корпуса, пальцев рук, несанкционированного подключения к СВТ сторонних технических устройств и др.);

- расположение СВТ в пространстве, относительно периферийного оборудования и других электротехнических устройств;

- точный порядок соединения СВТ с другими техническими устройствами;

- категорию обрабатываемой информации (общего пользования или конфиденциальная);

- наличие или отсутствие индивидуальных средств защиты осматриваемого СВТ и обрабатываемой на нем информации от несанкционированного доступа и манипулирования.

Если на момент осмотра СВТ находится в рабочем состоянии, необходимо детально описать:

- расположение его рабочих механизмов и изображение на его видеоконтрольном устройстве (экране, мониторе, дисплее);

- основные действия, производимые специалистом при осмотре СВТ (порядок корректного приостановления работы и закрытия исполняемой операции или программы, выключения СВТ, отключения от источника электропитания, рассоединения (или соединения) СВТ, отсоединения проводов, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т.п.).

7.4 Осмотр документов и их носителей

Осмотр машинного носителя и компьютерной информации проводят по принципу «от общего к частному». Вначале описывают внешние индивидуальные признаки носителя: его цвет, размер, тип, вид, название, марка, заводской и индивидуальный номер, наличие наклейки и надписей на ней, наличие или отсутствие физических повреждений корпуса и следов на нем, положение элемента защиты от записи/стирания компьютерной информации. Затем переходят к осмотру компьютерной информации, содержащейся на машинном носителе информации (МНИ).

Перед началом ее осмотра необходимо указать в протоколе следственного действия:

- индивидуальные признаки используемого для осмотра средства электронно-вычислительной техники и основные реквизиты его программного обеспечения (тип, вид, марку, название, заводской или регистрационный номер, номер версии, юридический адрес и(или) автора программного продукта);

- юридические реквизиты программы, с помощью которой СВТ и его программное обеспечение в присутствии понятых было тестировано специалистом на предмет отсутствия вредоносных программно-аппаратных средств.

После этого на указанный предмет проверяется и осматриваемая компьютерная информация.

Анализируя содержащуюся на осматриваемом носителе компьютерную информацию, надо установить сведения, имеющие отношение к расследуемому событию. Для оптимизации процесса осмотра большого объема информации можно применять функции автоматизированного поиска по конкретному слову (реквизиту), входящие в состав стандартного программного обеспечения ЭВМ. Ход осмотра должен дополнительно фиксироваться на цветной фото- или видеопленке. При обнаружении следов преступления необходимо сделать распечатку всей или части компьютерной информации и приложить ее к протоколу следственного действия с указанием в протоколе индивидуальных признаков использованного для этого печатающего устройства (тип, вид, марку, название, номер).

В протоколе осмотра, также необходимо отразить:

- наличие, индивидуальные признаки защиты носителя от несанкционированного использования (голография, штрих-код, эмбоссинг, флуоресцирование, перфорация, ламинирование личной подписи и(или) фотографии владельца, их размеры, цвет, вид и т.п.);

- признаки материальной подделки МНИ и его защиты; внутреннюю спецификацию носителя – серийный номер и(или) метку тома либо код, размер разметки (для дисков – по объему записи информации, для лент – по продолжительности записи);

- размер области носителя свободной от записи и занятой под информацию;

- количество и номера сбойных зон, секторов, участков, кластеров, цилиндров;

- количество записанных программ, файлов, каталогов (структура их расположения на МНИ, название, имя и(или) расширение, размер (объем), в том числе тот, который занимают их названия, дата и время создания (или последнего изменения), а также специальная метка или флаг (системный, архивный, скрытый, только для чтения или записи и т.д.);

- наличие скрытых или ранее стертых файлов (программ) и их реквизиты (название, размер, дата и время создания или уничтожения).

Готовясь к проведению обыска, следователь должен решить, что и где он будет искать. Для этого необходимо тщательно изучить обстоятельства дела и собрать ориентирующую информацию о предмете обыска, месте его проведения и личности обыскиваемого. По делам о преступлениях в сфере компьютерной информации предметом обыска могут быть не только разнообразные СВТ, машинные носители и содержащаяся на них компьютерная информация, но и документы, средства электросвязи, разработанные и приспособленные специальные технические устройства, бытовые электротехнические устройства и оборудование, материалы и инструменты.

В ходе обыска следует обращать внимание на литературу, методические материалы и рекламные проспекты по компьютерной технике, обработке, защите, передаче и негласному получению компьютерной информации, а также на аудио-, видеокассеты, распечатки машинной информации и документы о соответствующем образовании. Особое внимание нужно уделять предметам, содержащим коды, пароли доступа, идентификационные номера, названия, электронные адреса пользователей конкретных компьютерных систем и сетей, алгоритмы входа и работы в системах и сетях. Необходимо также перлюстрировать записные (телефонные) книжки, справочники и каталоги, в том числе электронные, находящиеся в памяти телефонных аппаратов, пейджеров и других компьютерных устройств.

Ценные доказательства могут быть обнаружены и при личных обысках подозреваемых (обвиняемых).

Предметом выемки в подавляющем большинстве случаев совершения преступления в сфере компьютерной информации являются персональные компьютеры, машинные носители информации (включая распечатки на бумаге, аудио- и видеокассеты, пластиковые карты) и всевозможные документы (в том числе и электронные), отражающие и регламентирующие различные операции, технологические процессы, связанные с обработкой, накоплением, созданием, передачей и защитой компьютерной информации, использованием ЭВМ, системы ЭВМ и их сети. Последние находятся по месту работы (учебы) подозреваемого (обвиняемого), в рабочих кабинетах должностных лиц и других служебных (учебных) помещениях.

Помимо вышеуказанного, могут быть изъяты специальные технические средства для негласного получения, модификации и уничтожения информации, свободные образцы почерка, бланки и фрагменты документов, заготовки машинных носителей информации, исходные тексты программ для ЭВМ, черновики и иные образцы для сравнительного исследования. Перед изъятием магнитных носителей информации они должны быть в обязательном порядке упакованы в алюминиевый материал (алюминиевую фольгу или специальный контейнер), предохраняющий МНИ и его содержимое от внешнего электромагнитного и магнитного воздействия.

Контрольные вопросы

1. Какие основные особенности должны учитываться при проведении следственных действий по делам о преступлениях в сфере компьютерной информации?

2. Каков должен быть состав следственно-оперативной группы при осмотре места происшествия?

3. Каковы особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг сети Интернет?

4. Что фиксируют в протоколе осмотра средств вычислительной техники?

5. Что необходимо зафиксировать в протоколе при осмотре документов и их носителей?

ГЛАВА 8. НАЗНАЧЕНИЕ КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ

ЭКСПЕРТИЗ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ

ВЫСОКИХ ТЕХНОЛОГИЙ

8.1 Механизм следообразования в компьютерных средствах и системах

Под механизмом следообразования следует понимать специфическую конкретную форму протекания процесса, конечная фаза которого представляет собой образование следа-отображения. Элементами этого механизма являются объекты следообразования – следообразующий, следовоспринимающий и вещество следа, следовой контакт как результат взаимодействия между ними вследствие приложения энергии к объектам следообразования.

Для преступлений, сопряженных с использованием компьютерных средств, одной из первых, представляющих практический интерес, была предложена следующая следовая картина:

1) следы на компьютерных средствах (в т.ч. носителях компьютерной информации), посредством которых действовал преступник на своем рабочем месте (в файловой системе, ОЗУ, аппаратно-программная конфигурация) и вне носителей информации (рукописные записи и распечатки с принтера – коды доступа, тексты программ, телефонные счета и пр.);

2) следы на «транзитных» (коммуникационных) носителях информации, посредством которых преступник осуществлял связь с информационными ресурсами, подвергавшимися неправомерному доступу (следы в линиях электросвязи: документированная информация о трафике через оператора телематических услуг, результаты наблюдения в ходе проведения ОРМ и следствия);

3) следы в компьютерной системе (в т.ч. на носителях информации компьютерной системы), в которую осуществлен неправомерный доступ, либо иные противоправные действия (изменения в файловой системе, ОЗУ, аппаратно-программной конфигурации и пр.);

4) следы на компьютерных средствах, которые сопряжены с иными (не только в сфере компьютерной информации) преступлениями – криминалистически значимая информация в компьютерах, органайзерах, мобильных телефонах, смарт-картах и пр.

8.2 Типовые следообразующие признаки преступной деятельности в

сфере телекоммуникации

Анализ преступлений, совершенных в сфере телекоммуникации, показывает, что при организации доступа к сети сотовой связи характерны следы, следообразующие и следовоспринимающие объекты, типовые для хищений, подделки документов, неправомерного доступа к охраняемой законом компьютерной информации и другие. Характерные следы преступного пользования ресурсами связи зависят от технологических особенностей их построения, например, в результате криминального пользования ресурсами сотовой связи типовые следы остаются на следующих типовых объектах[[96]](#footnote-96):

1. Объекты, находящиеся в ведении преступника:

- похищенная у легального пользователя подвижная абонентская станция;

- клонированная подвижная абонентская станция;

- подвижная абонентская станция, доработанная на техническом и программном уровне для осуществления сканирования идентификационных данных (номеров) легальных пользователей (ESN, MIN и др.);

- сканирующие технические устройства, мониторы сотовой связи (кустарного или промышленного изготовления) и т.д.;

- технический комплекс, представляющий собой комбинацию сканнера, компьютера и сотового телефона (так называемый сотовый кэш-бокс)

- средства компьютерной техники: гибкий (floppy) диск (дискета); дисковод; накопитель на жестких магнитных дисках («винчестер»); компактные диски (CD ROM); программаторы;

- бумажные носители (рукописные записи, распечатки).

На указанных объектах возникают следующие типовые следы:

1) материальные следы:

- следы пальцев, микрочастицы и т.п. (на клавиатуре, дискетах, внутри абонентской подвижной станции и т.д.);

- установленные кустарным способом дополнительные микросхемы в абонентскую подвижную станцию;

- конструктивно-технические изменения электронных схем абонентской подвижной станции;

- инструкции, связанные с использованием технического оборудования, выступающего в качестве орудий преступления (сканирующие приемники, мониторы сотовой связи кустарного или промышленного изготовления и т.д.);

- инструкции по вводу и выводу из электронной записной книжки абонентской подвижной станции идентификационных данных (номеров) легальных пользователей и т.д.

2) виртуальные следы[[97]](#footnote-97):

- специальное программное обеспечение и идентификационные данные (номера) легальных пользователей в энергонезависимой памяти EPROM (Erasable Programmable Read Only Memory – стираемая программируемая постоянная память) абонентской подвижной станции, сканирующего технического устройства и т.д.;

- компьютерная информация на материальных носителях компьютерной техники (программное обеспечение, с помощью которого осуществляется сканирование, декодирование, запись и хранение необходимых данных, подделка документов, продукты применения указанных специальных программ и т.п.).

3) идеальные следы, находящиеся в памяти виновного.

2. Объекты, находящиеся в ведении собственника, абонента сотовой связи:

- средства компьютерной техники коммутаторов сотовой связи;

- средства компьютерной техники сотовой связи, применяемые для выявления нелегальной абонентской активности. Системы проверки записей звонков на предмет обнаружения почти одновременных звонков из различных зон (сот), формирования профиля легального абонента и т.д. Указанные системы способны накапливать данные о вызовах каждого конкретного легального абонента и создавать на этой основе их индивидуальные профили. Они затем дополняются, анализируются по мере совершения новых звонков и способны немедленно обнаруживать аномальную активность.

К системам обнаружения криминальной абонентской активности относятся: система FraudBuster, система Signature Fraud Management System (Signature FMS), система визуального анализа информации Watson и др. Поскольку инфраструктура не связана с концепцией системы защиты, то она подходит для систем GSM, AMPS, CDMA, TDMA и др.

На указанных объектах возникают следующие типовые следы:

1) материальные следы практически отсутствуют, так как действия по пользованию ресурсами сотовой связи (абонентская активность) осуществляются «внутри» системы сотовой связи: абонентская подвижная станция – радиоинтерфейс – система базовых станций и т.д. («среда-посредник»).

2) виртуальные следы представляют собой компьютерную информацию коммутаторов сотовой связи и систем по выявлению и предотвращению «мошенничества», характеризующие абонентскую активность и, в частности, исходящие и входящие соединения.

Исходящие соединения. Легальный абонент компании сотовой связи, как правило, знает круг своих телефонных контактов, поэтому можно установить номера, на которые он соединения не производил. В частности, указывают на присутствие нелегального пользователя: трафик исходящих номеров легального абонента, когда его абонентская подвижная станция была отключена; появление в трафике иногородних и международных исходящих номеров, неизвестных легальному абоненту и другие показатели криминальной активности.

Исходящая криминальная абонентская активность может быть классифицирована по нескольким основаниям:

а) по географическому признаку:

- локальные соединения из области подключения;

- междугородние соединения из области подключения;

- международные соединения из области подключения;

- мобильные локальные соединения извне области подключения;

- мобильные междугородние соединения извне области подключения;

- мобильные международные соединения извне области подключения;

- порядок передвижения соединений в рамках одной ячейки (соты) или в рамках пространства занимаемых несколькими ячейками (сотами) за определенный интервал времени;

б) по временным факторам:

- по времени суток (например, с 7-00 до 19-00, с 19-00 до 7-00);

- по дням недели (рабочие дни, выходные дни);

- по особым периодам и событиям (Новый год, Рождество и т.д.);

- по количеству соединений за определенный интервал(ы) времени;

- по длительности соединений за определенный интервал(ы) времени;

- по общему времени соединений за определенный интервал времени (начиная с первого соединения);

в) по направленности исходящих соединений:

- повторяющиеся соединения с одними и теми же номерами проводной сети связи;

- повторяющиеся соединения с одними и теми же номерами сотовой подвижной связи;

- повторяющиеся соединения с одними и теми же номерами иных видов связи;

- повторяющиеся соединения с одними и теми же номерами льготных тарифов;

- повторяющиеся соединения с одними и теми же freefone номерами;

- общее соотношение входящих и исходящих соединений за определенный интервал времени;

г) по типу мобильного соединения:

- соединения конференции;

- активация и дезактивация дополнительных услуг.

Входящие соединения. На абонентскую подвижную станцию нелегального пользователя можно позвонить, но обычно этого не делают, так как звонок раздается у обоих абонентов (легального и нелегального), а говорить сможет тот, кто первый ответит на входящий вызов. Обычно в данном случае абонентская подвижная станция легального абонента блокируется, что может вызвать подозрение у легального абонента.

Входящая криминальная абонентская активность также может быть классифицирована по нескольким основаниям:

а) по географическому признаку:

- входящие мобильные локальные соединения (из той же области подключения);

- входящие мобильные междугородние соединения;

- входящие мобильные международные соединения;

б) по временным факторам:

- по времени суток;

- по дням недели;

- по особым периодам и событиям;

- по количеству входящих соединений за определенный интервал(ы) времени;

- по длительности входящих соединений за определенный интервал(ы) времени;

- по общему времени входящих соединений за определенный интервал времени (начиная с первого соединения в рамках определенного временного интервала);

в) по направленности входящих соединений:

- повторяющиеся соединения, исходящие от одного и того же номера проводной сети связи;

- повторяющиеся соединения, исходящие от одного и того же номера сотовой подвижной связи;

- повторяющиеся соединения, исходящие от одного и того же номера иных видов связи;

- повторяющиеся соединения, исходящие от одного и того же номера или разных номеров льготного тарифа;

- повторяющиеся соединения, исходящие от одного и того же freefone номера или разных freefone номеров;

г) по типу мобильного соединения – входящие соединения – конференции.

3. Идеальные следы остаются в памяти свидетелей и потерпевших, в числе которых сотрудники компании-оператора, легальные пользователи и др.

Следы при совершении рассматриваемого вида криминальных действий редко остаются в виде изменений внешней среды, что должно учитываться при сборе доказательств и поиске так называемых «традиционных» следов. Поэтому одной из основных задач успешного раскрытия и расследования «мошенничества» в сети сотовой связи является обеспечение следователем и другими уполномоченными лицами сохранности доказательственной информации, сбор и фиксация следов на стадии рассмотрения сообщения о возбуждении уголовного дела и первоначальном этапе расследования.

8.3 Экспертные исследования

В зависимости от стоящих перед следствием задач и спецификой объектов исследования для установления конструктивных особенностей и состояния компьютеров, периферийных устройств, магнитных носителей и пр., компьютерных сетей, причин возникновения сбоев в работе указанного оборудования, а также изучения информации, хранящейся в компьютере и на магнитных носителях, назначается компьютерно-техническая экспертиза. Рассмотрим методические рекомендации по расследованию преступлений в сфере компьютерной информации[[98]](#footnote-98).

8.3.1 Объекты компьютерно-технической экспертизы

К объектам компьютерно-технической экспертизы относятся:

1. Компьютеры в сборке, их системные блоки.

2. Периферийные устройства (дисплеи, принтеры, дисководы, модемы, клавиатура, сканеры, манипуляторы типа «мышь», джойстики и пр.), коммуникационные устройства компьютеров и вычислительных сетей.

3. Магнитные носители информации (жесткие и флоппи-диски, оптические диски, ленты).

4. Словари поисковых признаков систем (тезаурусы), классификаторы и иная техническая документация, например, технические задания и отчеты.

5. Электронные записные книжки, пейджеры, телефонные аппараты с памятью номеров, иные электронные носители текстовой или цифровой информации, техническая документация к ним.

В системе Министерства внутренних дел России в настоящее время нет специальных экспертных подразделений, которые производят компьютерно-технические экспертизы носителей машинной информации, программного обеспечения, баз данных и аппаратного обеспечения ЭВМ. В связи с этим они могут быть назначены специалистам соответствующей квалификации из внеэкспертных учреждений. В частности, такие специалисты могут быть в информационных центрах, учебных и научно-исследовательских заведениях МВД России. Кроме того, для производства этого вида экспертиз можно привлекать специалистов учебных и научно-исследовательских заведений, не относящихся к системе МВД России, фирм и организаций, занимающихся разработкой программного и аппаратного обеспечения для компьютеров, их эксплуатацией и ремонтом. Данный вид экспертиз может быть поручен специалистам в области эксплуатации ЭВМ (системным программистам, инженерам по обслуживанию, непосредственно работающим с данного вида носителями и др.) и программистам, которые обладают соответствующей квалификацией.

При вынесении постановления о назначении компьютерно-технической экспертизы следователем в постановлении о ее назначении обязательно указываются серийный номер компьютера и его индивидуальные признаки (конфигурация, цвет, надписи на корпусе и т.д.).

Учитывая, что компьютерно-техническая экспертиза – новый формирующийся род судебных экспертиз, необходимость в которых обусловливается широким внедрением компьютерных технологий практически во все сферы человеческой деятельности, полезным будет дать краткую характеристику ее возможностей.

В настоящее время в рамках таких экспертиз выделяются два вида:

- техническая экспертиза компьютеров и их комплектующих, которая проводится в целях изучения конструктивных особенностей и состояния компьютера, его периферийных устройств, магнитных носителей и пр., компьютерных сетей, а также причин возникновения сбоев в работе вышеуказанного оборудования;

- экспертиза данных и программного обеспечения, осуществляемая в целях изучения информации, хранящейся в компьютере и на магнитных носителях.

8.3.2 Вопросы, выносимые на разрешение компьютерно-технической

экспертизы

Вопросы, выносимые на разрешение компьютерно-технической экспертизы, в зависимости от вида экспертизы также подразделяются на следующие группы:

1. Вопросы, разрешаемые технической экспертизой компьютеров и их комплектующих (диагностические):

1. Компьютер какой модели представлен на исследование? Каковы технические характеристики его системного блока и периферийных устройств? Каковы технические характеристики данной вычислительной сети?

2. Где и когда изготовлен и собран данный компьютер и его комплектующие? Осуществлялась ли сборка компьютера в заводских условиях или кустарно?

3. Соответствует ли внутреннее устройство компьютера и периферии прилагаемой технической документации? Не внесены ли в конструкцию компьютера изменения (например, установка дополнительных встроенных устройств: жестких дисков, устройств для расширения оперативной памяти, считывания оптических дисков и пр., иные изменения конфигурации)?

4. Исправен ли компьютер и его комплектующие? Каков их износ? Каковы причины неисправности компьютера и периферийных устройств? Не содержат ли физических дефектов магнитные носители информации?

5. Не производилась ли адаптация компьютера для работы с ним специфических пользователей (левша, слабовидящий и пр.)?

6. Каковы технические характеристики иных электронных средств приема, накопления и выдачи информации (пейджер, электронная записная книжка, телефонный сервер)? Исправны ли эти средства? Каковы причины неисправностей?

2. Диагностические вопросы, разрешаемые экспертизой данных и программного обеспечения:

1. Какая операционная система установлена в компьютере?

2. Каково содержание информации, хранящейся на внутренних и внешних магнитных носителях, в том числе какие программные продукты там находятся? Каково назначение программных продуктов? Каков алгоритм их функционирования, способа ввода и вывода информации? Какое время проходит с момента введения данных до вывода результатов при работе данной компьютерной программы, базы данных?

3. Являются ли данные программные продукты лицензионными (или несанкционированными) копиями стандартных систем или оригинальными разработками?

4. Не вносились ли в программы данного системного продукта какие-либо коррективы (какие), изменяющие выполнение некоторых операций (каких)?

5. Соответствует ли данный оригинальный компьютерный продукт техническому заданию? Обеспечивается ли при его работе выполнение всех предусмотренных функций?

6. Использовались ли для ограничения доступа к информации пароли, скрытые файлы, программы защиты и пр.? Каково содержание скрытой информации? Не предпринимались ли попытки подбора паролей, взлома защитных средств и иные попытки несанкционированного доступа?

7. Возможно ли восстановление стертых файлов? Возможно ли восстановление дефектных магнитных носителей информации? Каково содержание восстановленных файлов?

8. Каков механизм утечки информации из локальных вычислительных сетей, глобальных сетей и распределенных баз данных?

9. Имеются ли сбои в функционировании компьютера, работе отдельных программ? Каковы причины этих сбоев? Не вызваны ли сбои в работе компьютера влиянием вируса (какого)? Распространяется ли негативное влияние вируса на большинство программ или он действует только на определенные программы? Возможно ли восстановить в полном объеме функционирование данной программы (текстового файла), поврежденного вирусом?

10. Каково содержание информации, хранящейся на пейджере, в электронной записной книжке и пр.? Имеется ли в книжке скрытая информация и каково ее содержание?

11. Когда производилась последняя корректировка данного файла или инсталляция данного программного продукта?

12. Каков был уровень профессиональной подготовки в области программирования и работы с компьютерной техникой лица, произведшего данные действия с компьютером и программным обеспечением?

3. Вопросы идентификационного характера, разрешаемые компьютерно-технической экспертизой:

1. Имеют ли комплектующие компьютера (печатные платы, магнитные носители, дисководы и пр.) единый источник происхождения?

2. Не написана ли данная компьютерная программа определенным лицом (решается комплексно при производстве компьютерно-технической и автороведческой экспертиз)?

Кроме приведенного выше перечня вопросов, разрешаемых компьютерно-технической экспертизой, для использования на практике, в зависимости от объекта исследования и конкретной обстановки, можно привести дополнительные примеры, расширяющие перечень вопросов, подлежащих выяснению при исследовании таких объектов, как носители информации, программное обеспечение, базы данных и аппаратное обеспечение ЭВМ.

8.3.3 Перечень вопросов, разрешаемых при исследовании носителей

машинной информации

При исследовании носителей машинной информации разрешаются следующие вопросы:

1. Каков тип носителя, его технические характеристики (на каких типах ЭВМ может быть использован, максимально допустимая емкость записи и пр.)?

2. Имеет ли носитель механические повреждения?

3. Как размечен носитель, в каком формате информация записана на него?

4. Какая информация записана на данный носитель?

5. Как информация физически размещена на носителе (для лент – последовательность записи, для дисков – сектора, дорожки, цилиндры и пр.)?

6. Как информация размещена логически на носителе (файлы, каталоги, логические диски)?

7. Имеются ли повреждения информации (плохие сектора, потерянные блоки и пр.)?

8. Возможна ли коррекция информации на носителе?

9. Имеется ли на носителе компьютерный вирус, если да, то какой, какие изменения вносит и возможна ли его нейтрализация без ущерба для информации?

10. Являются ли изменения на носителе результатом действия вируса?

11. Возможно ли копирование информации с данного носителя и возможно ли физическое копирование носителя в целом?

12. При повреждении носителя возможно ли восстановление информации?

13. Какая информация ранее была записана на данный носитель (отмечена как стертые файлы) и возможно ли ее восстановление?

14. Какой объем занимает вся информация на носителе, ее отдельные части и сколько имеется свободного места?

15. Какое время занимает копирование данной информации с учетом типа ЭВМ?

16. Требуются ли для работы с информацией на носителе специальные аппаратные или программные средства дешифрации и перекодировки?

17. Нет ли на носителе специальных программ, уничтожающих информацию в случае несанкционированного доступа, отсутствия ключей и паролей или использования на другом компьютере, стоит ли счетчик возможных инсталляций и другие средства защиты, возможен ли их обход и каким образом?

8.3.4 Перечень вопросов, разрешаемых при исследовании

программного обеспечения

Под программным обеспечением (программами для ЭВМ) понимается совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата.

Программное обеспечение обычно хранится на магнитных, оптических или электронных (непосредственно установлено в микросхемах памяти компьютера) носителях машинной информации и управляет работой вычислительной системы. Кроме того, коды программ, входные, выходные и промежуточные данные могут находиться на бумажном носителе (перфолента, перфокарта). Вся информация, относящаяся к программному обеспечению, независимо от формы носителя, является объектом экспертизы и должна быть представлена эксперту.

При исследовании программного обеспечения разрешаются следующие вопросы:

1. Каково назначение данного программного обеспечения?

2. Кто разработчик данного обеспечения?

3. Каким образом данное программное обеспечение распространяется, кто является владельцем данной копии, имеется ли лицензия или разрешение на использование данного продукта. Каков серийный номер данной копии программного обеспечения?

4. С какими входными и выходными данными оно работает, каким образом и в какой форме эти данные вводятся в ЭВМ, создаются ли (а если создаются, то где) временные файлы и файлы статистики и их содержание, в какой форме выдается, где хранится или куда передается выходная информация?

5. Требует ли данная программа при своей работе ввода паролей и наличия ключей (дискет, заглушек и пр.). Если требует, то каким образом они хранятся и кодируются, имеется ли возможность прочитать файл с паролем с помощью простейших редакторов?

6. Возможен ли обход паролей при запуске программы через отладчик?

7. Имеются ли на машинном носителе исходные коды программ на языке программирования?

8. Когда последний раз вносились изменения в программу (например, по дате и времени создания или внесения изменений в файлы)?

9. Имеются ли в программе изменения по сравнению с исходной версией, что было изменено, к каким последствиям данные изменения приводят?

10. Имеются ли в программе враждебные функции, которые влекут уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети? Каким образом эти функции осуществляются и к каким последствиям приводят?

11. Возможно ли самопроизвольное распространение данной программы, т.е. является ли данная программа компьютерным вирусом?

12. Возможно ли осуществление копирования информации или требуется инсталляция?

13. Были ли внесены в программу изменения, направленные на преодоление защиты?

14. Количественные (занимаемый объем, требуемое количество дискет, количество файлов и пр.) и качественные (назначение конкретных файлов, требование к оборудованию и пр.) характеристики программы?

15. Соответствие алгоритма работы конкретной программы требованиям, указанным в техническом задании или заявленных в инструкции по эксплуатации?

16. Имеются ли ошибки при проведении расчетов с помощью данной программы (правильно ли происходит округление чисел, правильный ли алгоритм расчета конкретных данных и пр.?

17. Определить тип ЭВМ (системы ЭВМ), совместимый с программным и аппаратным обеспечением данного компьютера, если ее нет, то каким образом это влияет на нормальную работу программы?

18. Имеется ли полная совместимость конкретного программного обеспечения с другими программами, выполняемыми на данном компьютере, если нет, то каким образом это влияет на нормальное функционирование системы?

8.3.5 Перечень вопросов, разрешаемых при исследовании баз данных

Под базами данных понимается форма представления и организации совокупности данных (статей, расчетов и т.д.), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ. С точки зрения организации базы данных могут представлять собой информацию в текстовых файлах и информацию в файлах со специальной структурой, которые обрабатываются специальными программами (системами управления базами данных, сокращенно СУБД), именно их в компьютерной терминологии называют базами данных.

Базы данных обычно хранятся на магнитных, оптических или электронных носителях машинной информации, а также могут быть непосредственно установлены в микросхемах памяти компьютера. Кроме того, коды баз данных, входные, выходные и промежуточные данные могут находиться на бумажном носителе (распечатки исходных текстов программ баз данных, перфолента, перфокарта). Вся информация, относящаяся к базам данных, независимо от формы носителя, является объектом экспертизы и должна быть представлена эксперту.

Перечень вопросов:

1. Каким образом организована база данных?

2. В каком формате записана информация и какие СУБД могут ее обрабатывать?

3. Какая информация записана в данной базе?

4. Информация в базе записана обычным образом или закодирована?

5. Когда последний раз обновлялась информация?

6. Имеются ли в данной базе скрытые (помеченные для удаления) поля и их содержание?

7. Имеются ли повреждения или изменения в записях базы по сравнению с эталоном или резервной копией, если да, то какие?

8. Сколько записей в базе?

9. Имеется ли в данной базе запись конкретного содержания?

10. Возможно ли внести изменение в данную базу с помощью простейших программных средств (например, текстовых редакторов и пр.)?

8.3.6 Перечень вопросов, разрешаемых при исследовании аппаратного

обеспечения ЭВМ

Под аппаратным обеспечением ЭВМ понимается комплекс технических средств, предназначенных для автоматизированной обработки информации, обеспечения хранения и передачи ее по каналам связи, ведения диалога с пользователем и выполнения других функций в составе компьютерной системы. Аппаратное обеспечение в свою очередь подразделяется на следующие устройства:

1. Центральные устройства ЭВМ (центральный процессор; оперативное и постоянное запоминающие устройства; системную шину; другие устройства для обеспечения работы вычислительной системы – контроллеры, таймер, тактовый генератор, различные буферы и пр.).

2. Периферийные устройства (видеоподсистема; накопители различных типов; устройства вывода информации; устройства ввода информации; устройства организации ЛВС и телекоммуникации; другие устройства, сопряженные с компьютером и которые функционируют под его управлением).

3. Вспомогательные устройства (устройства электропитания; различные фильтры – сетевые, экранные и пр.; аппаратура защиты, работающая автономно от центрального процессора – генераторы помех и пр.).

Вопросы, которые необходимо поставить экспертам:

1. Каковы тип устройства и его технические характеристики?

2. Исправно ли данное устройство или нет, тип неисправности (отказ или сбой), как она влияет на работу системы в целом?

3. Полностью ли совместимы между собой компоненты данного устройства, если нет, то как это сказывается на его работе?

4. Полностью ли совместимо данное устройство с каким-либо конкретным устройством, если нет, то как сказывается это на их работе?

5. Имеются ли на устройстве следы ремонта, повреждений, демонтажа микросхем, замены блоков?

6. Соответствует ли комплектация устройства технической документации, если нет, то какие компоненты были изменены, демонтированы?

7. Нет ли в данном устройстве дополнительных блоков (жучков) с враждебными функциями, если есть, то каково их предназначение?

8. Возможно ли на данном оборудовании решать какие-либо конкретные задачи?

9. Какой уровень излучений у данного устройства, возможен ли его прием специальными техническими средствами для последующей расшифровки информации, если возможен, то на каком расстоянии?

10. Возможно ли отключение аппаратных средств защиты и как это влияет на работу системы?

11. Соблюдались ли правила эксплуатации?

12. Могла ли данная проблема возникнуть в результате несоблюдения правил технической эксплуатации?

Следует отметить, что приведенные выше вопросы носят рекомендательный характер. Конкретность их постановки будет зависеть от фабулы преступления.

Контрольные вопросы

1. Какова следовая картина преступлений, сопряженных с использованием компьютерных средств?

2. Каковы типовые следообразующие признаки преступной деятельности в сфере телекоммуникации?

3. Как классифицируется исходящая криминальная абонентская активность?

4. Как классифицируется входящая криминальная абонентская активность?

5. Что относится к объектам компьютерно-технической экспертизы?

6. Какие вопросы выносятся на разрешение компьютерно-технической экспертизы?

7. Какие вопросы разрешаются при исследовании носителей машинной информации?

8. Какие вопросы разрешаются при исследовании баз данных?

9. Какие вопросы разрешаются при исследовании аппаратного обеспечения ЭВМ?

ГЛАВА 9. ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ

ВЫСОКИХ ТЕХНОЛОГИЙ

9.1 Организационно-технические меры предупреждения компьютерных

преступлений

Международный опыт борьбы с преступностью свидетельствует о том, что одним из приоритетных направлений решения задачи эффективного противодействия современной преступной деятельности является активное использование правоохранительными органами различных мер профилактического характера.

Большинство зарубежных специалистов прямо указывают на то, что предупредить компьютерное преступление всегда намного легче и проще, чем его раскрыть и расследовать.

Как уже отмечалось, обычно выделяются две основные группы мер предупреждения компьютерных преступлений: правовые и организационно-технические.

Одной из основных проблем, затрудняющих предупреждение и расследование компьютерных преступлений, является дефицит квалифицированных специалистов МВД России (редкий следователь обладает глубокими познаниями процессов, происходящих в компьютере, не говоря уже о расследовании компьютерных преступлений) и отсутствие наработок в этой области (методических рекомендаций по изъятию, обыску, осмотру места происшествия и т.п.).

Ввиду того, что компьютерные преступления все больше приобретают транснациональный характер, усиливается международное сотрудничество в этой области. Что касается Российской Федерации, то, к сожалению, приходится признать, что большая часть компьютерных преступлений совершается в большей мере вследствие недостаточности организационных мер в предприятиях и организациях, слабой защиты данных от несанкционированного доступа, недостаточной конфиденциальности, слабой проверки и инструктажа персонала.

Анализ сведений о совершенных компьютерных преступлениях позволяет сделать вывод о том, что основными причинами и условиями, способствующими их совершению, в большинстве случаев стали:

1) неконтролируемый доступ сотрудников к клавиатуре компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе осуществления финансовых операций;

2) бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать ПК в качестве орудия совершения преступления;

3) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

4) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

5) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации и ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа;

6) отсутствие разграничения допуска сотрудников к документации строгой финансовой отчетности, в т.ч. находящейся в форме машинной информации;

7) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной информации ограниченного доступа.

Зарубежный опыт показывает, что наиболее эффективной защитой от компьютерных правонарушений является введение в штатное расписание организаций должности специалиста по компьютерной безопасности (администратора по защите информации) либо создание специальных служб как частных, так и централизованных, исходя из конкретной ситуации. Наличие такого отдела (службы) в организации, по оценкам зарубежных специалистов, снижает вероятность совершения компьютерных преступлений вдвое.

Помимо организационно-управленческих мер, существенную роль в борьбе с компьютерными преступлениями могут играть меры технического характера (аппаратные, программные и комплексные).

Аппаратные методы предназначены для защиты компьютерной техники от нежелательных физических воздействий и закрытия возможных каналов утечки конфиденциальной информации. К ним относятся источники бесперебойного питания, устройства экранирования аппаратуры, шифрозамки, устройства идентификации личности и т.п.

Средства регистрации, средства контроля доступа к информационным ресурсам также относятся к эффективным мерам противодействия попыткам несанкционированного доступа:

1) программы регистрации первичных данных, исключающие возможность пропуска обязательных реквизитов данных и содержащие условия блокировки ввода-вывода информации и подсказку пропущенных реквизитов;

2) подтверждение личности, регистрирующей первичные данные (авторизация данных), основанное на идентификации личности, производящей ввод-вывод данных, и предусматривающее возможность блокировки средств компьютерной техники при выполнении предъявляемых условий идентификации;

3) программы защиты зарегистрированных данных от преднамеренного или случайного их искажения, уничтожения, а также от несанкционированного получения сведений о зарегистрированных данных. Исправлять машинную запись первичных данных может только лицо, имеющее специальные полномочия, а основным подтверждением достоверности машинной записи при этом является однозначное доказательное определение личности, производившей регистрацию первичных данных.

Программные методы защиты предназначаются для непосредственной защиты информации. Для защиты информации при ее передаче обычно используют различные методы шифрования данных. Как показывает практика, современные методы шифрования позволяют достаточно надежно скрыть смысл сообщения. Например, в США в соответствии с директивой Министерства финансов начиная с 1984 г. все общественные и частные организации были обязаны внедрить процедуру шифрования коммерческой информации по системе DES (Data Encryption Standard), официально утвержденной Национальным бюро стандартов США еще в 1978 г.

В России в июле 1991 г. также был введен в действие ГОСТ криптографирования информации, представляющий собой единый алгоритм криптографического преобразования данных для системы обработки информации в сетях ЭВМ, отдельных вычислительных комплексах и ЭВМ, функционирующий на базе отечественного алгоритма Kryption, аналогичного по своим основным техническим параметрам DES. Российский стандарт свободен от недостатков стандартов DES и в то же время обладает всеми его преимуществами.

При рассмотрении вопросов, касающихся программной защиты информационных ресурсов, особо выделяется проблема их защиты от компьютерных вирусов как способа совершения компьютерного преступления. В настоящее время разрабатываемые отечественные и зарубежные программные антивирусные средства позволяют с определенным успехом (примерно 97%) опознать зараженные программные средства и их компоненты.

Наиболее эффективным направлением в предупреждении подобных посягательств является комплексное использование различных мер предупреждения компьютерных преступлений: организационных, аппаратных и программных. Например, для уменьшения опасности вирусных посягательств на СВТ, по мнению специалистов, необходимо предпринять следующие комплексные организационно-технические меры, которые могут быть сокращены или расширены по своему содержанию исходя из каждой конкретной ситуации.

1. Информировать всех сотрудников учреждения, организации, использующих СВТ, об опасности и возможном ущербе в случае совершения вирусного посягательства.
2. Не осуществлять неофициальные связи с другими организациями, связанные с обменом программных средств. Запретить сотрудникам приобретение и использование на рабочем месте программными средствами (ПС) «со стороны». Должны использоваться только официально распространяемые ПС, содержащиеся на оттестированных и опломбированных носителях машинной информации.
3. Запретить сотрудникам использование и хранение на носителях и в памяти ЭВМ компьютерных игр, являющихся источником повышенной опасности для безопасности компьютерных систем.

Общепризнанно мнение о том, что профилактика любого, в том числе и компьютерного, преступления должна носить комплексный характер и относиться к компетенции государственных органов, а не различных коммерческих охранных структур, что имеет место в нашей стране. Этому учит нас и опыт зарубежных государств, где (с момента совершения первого компьютерного преступления) стали серьезно заниматься этими проблемами на государственном уровне. В частности, помимо основных правовых актов были предприняты и другие законодательные мероприятия, направленные на обеспечение общей безопасности информационных ресурсов и возлагающие ответственность за их сохранность на несколько федеральных ведомств. Например, в США в 1965 г. был принят соответствующий Вrooks Act.

В настоящее время в зарубежных странах уже действует развитая система обеспечения компьютерной безопасности, осуществляемая государственными силами и средствами, включающая в себя законодательные, организационные и технические мероприятия, проводимые по единому комплексному плану и направленные на предупреждение компьютерных преступлений.

9.2 Правовые меры предупреждения компьютерных преступлений

К правовым мерам предупреждения компьютерных преступлений в первую очередь относятся нормы законодательства, устанавливающие уголовную ответственность за указанные выше противоправные деяния.

История развития законодательства зарубежных стран в этом направлении показывает, что впервые подобный шаг был предпринят законодательными собраниями американских штатов Флорида и Аризона уже в 1978 году. Принятый закон назывался «Computer crime act of 1978» и был первым в мире специальным законом, устанавливающим уголовную ответственность за компьютерные преступления. Затем практически во всех штатах США (в 45 штатах) были приняты аналогичные специальные законодательства.

Эти правовые акты стали фундаментом для дальнейшего развития законодательства в целях осуществления мер предупреждения компьютерных преступлений. Отечественное законодательство движется в этом направлении очень робкими шагами.

Первым из них по праву можно считать издание 22 октября 1992 года двух Указов Президента РФ «О правовой охране программ для ЭВМ и баз данных» и «О правовой охране топологий интегральных микросхем», регламентирующих порядок установления и правовую защиту авторских прав на программные средства компьютерной техники и топологии интегральных микросхем с 1 января 1994 года.

Вторым прогрессивным шагом является принятие Государственной Думой и Федеральным Собранием сразу двух законов: 20 января 2005 г. «О связи» и 25 января 1995 г. «Об информации, информатизации и защите информации»[[99]](#footnote-99). Данные нормативные акты дают юридическое определение основных компонентов информационной технологии как объектов правовой охраны; устанавливают и закрепляют права и обязанности собственника на эти объекты; определяют правовой режим функционирования средств информационных технологий; определяют категории доступа определенных субъектов к конкретным видам информации; устанавливают категории секретности данных и информации.

Решающим законодательным шагом можно считать принятие в июне 1996 года Уголовного кодекса Российской Федерации, выделяющего информацию в качестве объекта уголовно-правовой охраны.

Этим актом отечественное уголовное законодательство приводится в соответствие с общепринятыми международными правовыми нормами развитых в этом отношении зарубежных стран.

Следует отметить, что Государственная дума России постоянно пересматривает перечень нормативных правовых актов в сфере информационной безопасности и преступлений в области высоких технологий. Поэтому ряд законов были отменены, а основные правые нормы перенесены в Гражданский кодекс РФ (часть 4).

Контрольные вопросы

1. Перечислите и охарактеризуйте организационно-технические меры предупреждения компьютерных преступлений.

2. Каковы наиболее эффективные направления в предупреждении компьютерных преступлений?

3. Какие меры необходимо принимать для уменьшения опасности вирусных посягательств на средства вычислительной техники?

4. Каковы правовые меры предупреждения компьютерных преступлений?

ЗАКЛЮЧЕНИЕ

Анализ существующего состояния законодательства России и зарубежных стран позволяет обозначить некоторые основные направления развития законодательства в целях борьбы с компьютерной преступностью.

1. Предстоит обеспечить правовое регулирование распространения массовой информации, размещенной на сайтах Интернета, в том числе обеспечить реализацию конституционного запрета на пропаганду или агитацию, возбуждающую социальную, расовую, национальную и религиозную вражду, распространение порнографической информации и др., а также закрепить обязанность государственных органов защищать официальную информацию, размещаемую на их сайтах в Интернете.

2. Требуется законодательно закрепить механизм отнесения объектов информационной инфраструктуры к критически важным и обеспечить их информационную безопасность, включая разработку и принятие требований к техническим и программным средствам, используемым в информационной инфраструктуре этих объектов.

3. Серьезная работа должна быть проведена по совершенствованию законодательства об оперативно-розыскной деятельности в части:

- создания необходимых условий для проведения оперативно-розыскных мероприятий в целях выявления, предупреждения, пресечения и раскрытия компьютерных преступлений и преступлений в сфере высоких технологий;

- усиления контроля за сбором, хранением и использованием информации о частной жизни граждан, сведений, составляющих личную, семейную, служебную и коммерческую тайны;

- уточнения состава оперативно-розыскных мероприятий.

4. Необходимо усиление ответственности за преступления в сфере компьютерной информации и уточнение составов преступлений с учетом Европейской конвенции о киберпреступности.

5. Совершенствование уголовно-процессуального законодательства должно создать условия правоохранительным органам оперативно и эффективно действовать в случаях угроз безопасности, осуществляемых с использованием инфокоммуникационных технологий, единообразно оформлять доказательства, полученные с использованием компьютерных систем и телекоммуникаций.

6. Законодательство в области связи также требует совершенствования по ряду аспектов. Оно должно обеспечить:

- возможность перехвата информации, передаваемой по сетям электросвязи;

- раскрытие компетентным органам достаточного количества данных о потоках информации с целью идентификации поставщиков услуг и путей передачи информации;

- оперативное получение от поставщиков услуг связи сведений об абонентах (вид и время оказанных услуг, личность пользователя, адрес, телефон, сведения о платежах и другие сведения), не связанных с содержанием передаваемой ими информации.

7. Необходимо устранить правовую неопределенность в части использования работодателями средств визуального наблюдения, средств контроля телефонных переговоров, электронных сообщений, использования средств доступа в Интернет, поскольку эти средства могут быть использованы для противоправных действий.

8. В последнее время в связи с массовым распространением пиратства, порнографии, угрозами кибертерроризма, спама и множеством других реальных угроз все чаще поднимается вопрос о необходимости ужесточения контроля за пользователями в сети Интернет. Существующая относительная анонимность пользователя влечет множество отрицательных последствий и ее границы объективно придется сужать.

ЛИТЕРАТУРА

1. Конституция Российской Федерации от 12 декабря 1993 года. Электронный ресурс системы Гарант.
2. Закон РФ «О безопасности» от 05.03.92,. № 2446–1. Электронный ресурс системы Гарант.
3. Закон РФ «Об информации, информатизации и защите информации» от 20.02.95, №24–ФЗ. Электронный ресурс системы Гарант.
4. Закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2007, №149–ФЗ. Электронный ресурс системы Гарант.
5. Закон РФ «О персональных данных» от 27.07.2006, № 152–ФЗ. Электронный ресурс системы Гарант.
6. Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92, № 3523–1. Электронный ресурс системы Гарант.
7. Закон РФ «О государственной тайне» от 21.07.93, №5485–1. Электронный ресурс системы Гарант.
8. Патентный закон Российской Федерации от 23.09.92, №3717–1. Электронный ресурс системы Гарант.
9. Уголовный кодекс РФ от 13.06.96, №63–ФЗ. Электронный ресурс системы Гарант.
10. Постановление Правительства РФ от 11 октября 1993 г. № 1030 (в ред. от 04.02.2005 «О контроле за выполнением обязательств по гарантиям использования импортируемых и экспортируемых товаров и услуг двойного назначения в заявленных целях». Электронный ресурс системы Гарант.
11. ГОСТ Р 51141–98 «Делопроизводство и архивное дело. Термины и определения». Электронный ресурс системы Гарант.
12. Аналитическая деятельность и компьютерные технологии: Учебное пособие /Под ред. проф. В.А. Минаева. – М.: МЦ при ГУК МВД России, 1996.
13. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2001.
14. Баев О.Я., Мещеряков В.А. Проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации //Конфидент. 1998. № 7(23).
15. Батурин Ю.М. Проблемы компьютерного права. – М.: Юриздат, 1991.
16. Борьба с компьютерной преступностью за рубежом (на примере США, Великобритании, Франции, Польши): Обзорная информация. Зарубежный опыт. Вып.14. – М.: ГИЦ МВД РФ, 2003.
17. Быстряков Е.Н., Иванов А.Н., Климов В.Л. Расследование компьютерных преступлений. – Саратов, 2000.
18. Вехов В.Б., Попова В.В., Илюшин Д.А. Тактические особенности расследования преступлений в сфере компьютерной информации: Научно-практическое пособие. – 2-е изд., доп. и испр. – М.: ЛексЭст, 2004.
19. Вехов В.Б., Рогозин В.Ю. Методика расследования преступлений в сфере компьютерной информации. 2002 г. Компьютерный ресурс. Режим доступа: http: //www. crime.vl.ru /books.
20. Виды интернет-преступлений (по классификации ООН). Издательство «Семь Дней», 2000. Компьютерный ресурс. Режим доступа: //w3s.nsf\Archive\Archive.html.
21. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: Юрлитинформ, 2002.
22. Гаврилов О.А. Курс правовой информатики: Учебник для вузов. М.: НОРМА, 2000.
23. Громаков Ю.А. Сотовые системы подвижной радиосвязи. – М.: Эко-Трендз, 1994.
24. Дранников В.Н. Некоторые детерминанты компьютерной преступности в свете современной уголовной политики: /Материалы научно-практической конференции. – Таганрог: ТГРУ, 2006.
25. Илюшин Д.А. Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг «Интернет»//Вестник Муниципального института права и экономики (МИПЭ). – Вып. 1. – Липецк: Интерлингва, 2004.
26. Коншин А.А. Защита полиграфической продукции от фальсификации. – М.: Синус, 2000.
27. Копылов В.А. Информационное право: Учебник для вузов. – 2-е изд. – М.: Юристъ, 2005.
28. Крылов В.В. Информация как элемент криминальной деятельности //Вестник Московского университета. Серия 11. – Право, 1998.
29. Крылов В.В. Информационные компьютерные преступления. – М.: ИНФРА-М, НОРМА, 1997.
30. Крылов В.В. Расследование преступлений в сфере информации. – М.: ИНФРА-М, НОРМА, 1998.
31. Курс криминалистики. В 3 т. Т. 3. Криминалистическая методика. Методика расследования преступлений в сфере экономики, взяточничества и компьютерных преступлений: Учебник /Под ред. О.Н. Коршуновой, А.А. Степанова. – СПб.: Юридический центр Пресс, 2004.
32. Крылов В.В. Информация как элемент криминальной деятельности //Вестник Московского университета. Серия 11. – Право. – 1998.
33. Курушев В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. – М.: Новый юрист, 1998.
34. Лавникевич Д. Самые распространенные интернет-аферы 2004 года //Техника – молодежи. 2005. № 2.
35. Лазарева И.В. Некоторые проблемы расследования несанкционированного доступа к сетям сотовой радиотелефонной связи //«Черные дыры» в Российском законодательстве. 2007. № 1.
36. Лучин И.Н., Шурухнов Н.Г. Методические рекомендации по изъятию компьютерной информации при проведении обыска //Информационный бюллетень СК МВД России. 1996. № 4(89).
37. Левин М., Библия хакера. Книга 2. – М.: Майор, 2003.
38. Маклаков Г.Ю., Рыжков Э.В. Особенности оперативно-розыскной деятельности при расследовании преступлений в сфере высоких технологий. Компьютерный ресурс. Режим доступа: //http://www.crimeresearch.org.
39. Малая советская энциклопедия. – М.: Знание, 1960.
40. Малокостов В. О преступности в области пластиковых карточек //Мир карточек. 1999. № 12.
41. Мамлеев Р.Р. Обеспечение защиты информации при использовании технических систем обработки: Учебное пособие. – Уфа: УЮИ МВД РФ, 2003.
42. Мамлеев Р.Р., Обеспечение неотслеживаемости каналов передачи данных вычислительных систем //Безопасность информационных технологий. №2. – М.: МИФИ, 1999.
43. Мещеряков В.А. Криминалистическая классификация преступлений в сфере компьютерной информации //Конфидент. 1999. №4-5.
44. Методическое пособие по расследованию преступлений в сфере компьютерной информации и осуществлению прокурорского надзора за исполнением законов при их расследовании. – М.: Ген. прокуратура РФ, НИИ проблем укрепления законности и правопорядка, 2001.
45. Мошенничества с пластиковыми карточками. Компьютерный ресурс. Режим доступа: www.bizcom.ru/cards/security/1999-12/02-01.html.
46. Муромцев Ю.Л., Орлова Л.П., Муромцев Д.Ю., Тютюнник В.М. Информационные технологии проектирования. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2004.
47. Наумов А.В. Комментарий к Уголовному кодексу РФ. – М.: Институт государства и права РАН, 1996.
48. Наумов А.В. Российское уголовное право: Курс лекций. В 2 т. –М., 2004.
49. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях. Международный опыт: Монография. – М.: Норма, 2004.
50. Петров В.А., Пискарев А.С., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах: Учебное пособие. Изд. 2-е, испр. – М.: МИФИ, 1995.
51. Правовые аспекты борьбы с кибернетическими преступлениями в ЕС //Борьба с преступностью за рубежом. – М., 2003.
52. Преступления в кредитно-финансовой системе: Обзорная информация. Зарубежный опыт. – Вып. 2. – М.: ГИЦ МВД России, 1996.
53. Преступления в сфере компьютерной информации за рубежом: Обзорная информация. Зарубежный опыт. Вып. 2 /Сост. М.А. Головешкина. – М.: ГИЦ МВД России, 2004.
54. Приказ Росархива № 68 «Об утверждении Типовой инструкции по делопроизводству в федеральных органах исполнительной власти» от 27.11.2000. Электронный ресурс системы Гарант.
55. Расследование неправомерного доступа к компьютерной информации: Учебное пособие /Под ред. Шурухнова Н.Г. – 2-е изд., доп. и перераб. – М.: Московский университет МВД России, 2005.
56. Расследование неправомерного доступа к компьютерной информации/Под ред. Н.Г. Шурухнова. – М., 1999.
57. Расследование преступлений повышенной общественной опасности: Пособие для следователей /Под ред. Н.А. Селиванова, А.И. Дворкина. – М., 1998.
58. Расследование преступлений в сфере компьютерной информации: Методические рекомендации //Остроушко А.В., Прохоров А.С., Задорожко С.М., Тронин М.Ю., Гаврилюк С.В. Компьютерный ресурс. Режим доступа: http://zakon.kuban.ru/uk/272`274.htm.
59. Растегаев А.А. Анализ общеуголовной корыстной преступности //Методика анализа преступности. – М.: Инфо-М, 1986.
60. Ривкин К. Преступления с кредитными карточками //Экономика и жизнь. 1997. № 2.
61. Роганов С.А. Синтетические наркотики: вопросы расследования преступлений. – СПб: Питер, 2001.
62. Рогозин В.Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной информации: Учеб. пособие /Под ред. А.А. Закатова. – Волгоград, 2000.
63. Россинская Е.Р. Проблемы становления компьютерно-технической экспертизы как нового рода инженерно-технических экспертиз //Криминалистика в XXI веке. Материалы международной научно-практической конференции. – М., 2001.
64. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. – М.: Право и закон, 2001.
65. Розенфельд Н. Общая характеристика умышленных компьютерных преступлений //Право Украины. 2002. № 10.
66. Рыжков Э.В. Энергоинформационная безопасность общества и государства с позиции деятельности правоохранительных органов //Злочини проти особистої волі людини: Збірник матеріалів міжнародного науково-практичного семінару (Харків, 19-20 вересня 2000 р.). – Харків: «Книжкове видавництво» Лествиця Марії, 2002.
67. Сальников В.П., Ростов К.Т., Морозова Л.А., Бондуровский В.В. Компьютерная преступность: уголовно-правовые и криминологические проблемы: Международная научно-практическая конференция //Государство и право. 2000. № 9.
68. Семенов Г.В., Бирюков П.Н. Ответственность за «мошенничество» в сетях сотовой связи: Учебное пособие. – Воронеж: Воронежский государственный университет, 2002.
69. Скрипников. С. Черви, сети и виртуальные девушки //Эксперт. 2005. № 10
70. Сорокин. А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. Компьютерный ресурс. Режим доступа: //http://kurgan.unets.ru/~procur/my\_page.htm, 1999.
71. Старостина Е.В., Фролов Д.Б. Защита от компьютерных преступлений и кибертерроризма: вопросы и ответы. – М.: Эксмо, 2005.
72. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учебное пособие. – М.: ИНФРА-М, 2001.
73. Толковый словарь по вычислительным системам /Под ред. В. Иллингуотера и др. – М.: Машиностроение, 1990.
74. Хвоевский С.А., Исаева Л.М., Дьяков Ф.С., Вайле С.П. Выявление, пресечение и документирование фактов неправомерного доступа к охраняемой законом информации в контрольно-кассовых машинах при осуществлении предпринимательской деятельности: Методические рекомендации. – М.: ВНИИ МВД России, 2005.
75. Шурухнов Н.Г., Левченко И.П., Лучин И.Н. Специфика проведения обыска при изъятии компьютерной информации //Актуальные проблемы совершенствования деятельности ОВД в новых экономических и социальных условиях. – М., 1997.
76. Яблоков Н.П. Криминалистика: Учебник. – М.: ЛексЭст, 2006.
77. Ярочкин В.И. Информационная безопасность: Учебник для вузов. – М.: Академический Проект, Фонд «Мир», 2003.
78. Computing & Multimedia: Словарь. – М.: Внешсигма, 1996.

СЛОВАРЬ специальных ТЕРМИНОВ

BIOS – базовая система ввода/вывода, которая является частью операционной системы, постоянно хранящейся в постоянном запоминающем устройстве машины.

COM – тип исполняемого файла, в котором привязка уже выполнена и поэтому все адреса уже правильно записаны в файле перед его загрузкой.

CONFIG.SYS – имя специального файла, который система просматривает при загрузке. Этот файл содержит информацию о параметрах системы и драйверах устройств, которые должны быть установлены, что позволяет установить требуемую конфигурацию системы.

EXE – тип исполняемого файла, который требует привязки при загрузке. Не все адреса программы могут быть установлены до тех пор, пока неизвестно ее положение в памяти. EXE-файлы имеют заголовок, который содержит информацию об этой привязке. Эти файлы загружаются немного дольше и требуют больше места на диске, чем файлы типа COM.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ (АСУ) – это организованная совокупность правил работы, баз данных и пакетов прикладных программ, обеспечивающая с помощью ЭВМ рациональное управление деятельностью.

АЛГОРИТМ – последовательность команд (инструкций) для выполнения поставленной задачи. В данном случае команд для ЭВМ.

АРХИТЕКТУРА ЭВМ – общее описание структуры и функций ЭВМ на уровне, достаточном для понимания принципов работы и системы команд ЭВМ.

АТАКА НА КОМПЬЮТЕРНУЮ СИСТЕМУ – это действие, предпринимаемое злоумышленником, которое заключается в поиске той или иной уязвимости. Таким образом, атака – реализация угрозы.

АУТЕНТИЧНОСТЬ (authenticity) – свойство данных быть подлинными и свойство систем быть способными обеспечивать подлинность данных. Подлинность данных означает, что они были созданы законными участниками информационного процесса и не подвергались случайным или преднамеренным искажениям.

АУТЕНТИФИКАЦИЯ (authentication) – процедура проверки подлинности данных и субъектов информационного взаимодействия.

БАЗА ДАННЫХ – это объективная форма представления и организации совокупности данных (например, статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

БАНК ДАННЫХ – это совокупность баз данных, объединенных общностью применения.

БЕСПЕРЕБОЙНЫЕ ИСТОЧНИКИ ПИТАНИЯ. См. РЕЗЕРВНЫЕ ИСТОЧНИКИ ПИТАНИЯ.

БИБЛИОТЕКА – это организованная совокупность программ или алгоритмов, хранящаяся обычно во внешней памяти ЭВМ.

БЛОКИРОВАНИЕ – результат воздействия на ЭВМ и ее элементы, повлекшие временную или постоянную невозможность осуществлять какие-либо операции над компьютерной информацией.

##### ВИНОВНЫЕ В СОВЕРШЕНИИ КОМПЬЮТЕРНОГО ПРЕСТУПЛЕНИЯ – злоумышленники и неправомочные приобретатели записанной в устройство памяти компьютера информации, специально защищенной от несанкционированного доступа.

##### ВИРУС – это программа (некоторая совокупность выполняемого кода/инструкций), способная создавать свои копии, не обязательно полностью совпадающие с оригиналом, и внедрять их в различные объекты/ресурсы компьютерных систем, сетей и т.д., а также выполнять некоторые деструктивные действия.

##### ВОССТАНОВЛЕНИЕ ДАННЫХ – процесс восстановления потерянной (поврежденной, случайно стертой и др.) информации на магнитных носителях с помощью специального программного обеспечения.

ВРЕДОНОСНАЯ ПРОГРАММА – специально разработанная или модифицированная для несанкционированного собственником информационной системы уничтожения, блокирования, модификации либо копирования информации, нарушения обычной работы ЭВМ, является вредоносной.

ВРЕМЕННЫЙ ФАЙЛ – специальные файл, в котором во время работы программы хранятся промежуточные данные. При корректном завершении программы этот файл автоматически уничтожается.

ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА – ассортимент вычислительных машин, вычислительных устройств и приборов, используемых для ускорения решения задач, связанных с обработкой информации, путем частичной или полной автоматизации вычислительного процесса.

ГИБКИЙ МАГНИТНЫЙ ДИСК (ГМД). См. ДИСКЕТА.

ДАННЫЕ – информация, представленная в формальном виде, который обеспечивает возможность ее хранения, обработки или передачи.

ДЕФЕКТНЫЕ СЕКТОРЫ – место на магнитном носителе информации с поврежденным покрытием, где невозможно хранение данных.

ДИСК МАГНИТНЫЙ – вид внешней памяти, в котором носителем информации является вращающийся металлический или пластмассовый диск, покрытый слоем магнитного материала.

ДИСКЕТА – это гибкий магнитный диск внешней памяти ЭВМ, представляющий собой тонкий упругий диск, покрытый слоем магнитного материала в пластмассовом или пленочном корпусе.

ДИСКОВОД – внешнее устройство ЭВМ, предназначенное для ввода-вывода информации с магнитных дисков в память ЭВМ.

ДИСПЛЕЙ (МОНИТОР) – внешнее устройство ЭВМ для отображения графической и текстовой информации.

##### ДОСТУП К ИНФОРМАЦИИ – в узком смысле – операция записи, модификации, передачи или чтения данных.

##### ДОСТУП К ЭВМ – это санкционированное и упорядоченное собственником информационной системы взаимодействие лица с устройствами ЭВМ и (или) ознакомление лица с данными, содержащимися на машинных носителях или в ЭВМ.

##### ДОСТУП К ИНФОРМАЦИИ – в широком смысле – операционный тип взаимодействия между субъектом и объектом, в результате которого создается поток информации от одного к другому.

ЕМКОСТЬ – количество информации, содержащейся в запоминающем устройстве.

ЗЛОУМЫШЛЕННИК (intruder) – субъект, оказывающий на информационный процесс воздействия с целью вызвать его отклонение от условий нормального протекания. Злоумышленник идентифицируется набором возможностей по доступу к информационной системе, работу которой он намеревается отклонить от нормы. Считается, что в его распоряжении всегда есть все необходимые для выполнения его задачи технические средства, созданные на данный момент.

ИГРА КОМПЬЮТЕРНАЯ – это техническая игра, в которой игровое поле находится под управлением компьютера и воспроизводится обычно на экране дисплея.

ИЗЪЯТИЕ СРЕДСТВ КОМПЬЮТЕРНОЙ ТЕХНИКИ – традиционные способы совершения «некомпьютерных» преступлений, в которых преступник, попросту говоря, изымает чужое имущество. Чужое имущество – средства компьютерной техники.

ИНТЕРНЕТ – это всемирная сеть, использующая для взаимодействия набор протоколов TCP/IP (Transmission Control Protocol/Internet Protocol).

ИНТЕРФЕЙС – это средства и способы установления и поддержания информационного обмена между исполнительными устройствами автоматической системы или системы человек–машина.

##### ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – по законодательству РФ – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

##### Информационная безопасность имеет три основные составляющие:

##### 1. Конфиденциальность – защита чувствительной информации от несанкционированного доступа.

##### 2. Целостность – защита точности и полноты информации и программного обеспечения.

##### 3. Доступность – обеспечение доступности информации и основных услуг для пользователя в нужное для него время.

##### ИНФОРМАЦИОННАЯ СИСТЕМА – по законодательству РФ – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

##### Информационная система предназначена для хранения, обработки, поиска, распространения, передачи и предоставления информации.

ИНФОРМАЦИЯ (ДОКУМЕНТ) – это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

ИНФОРМАЦИОННОЕ ПРАВООТНОШЕНИЕ – отношения, в которых информация передается непосредственно и воля субъектов направлена на передачу исключительно информации.

КАНАЛ СВЯЗИ – это техническое устройство, в котором сигналы, содержащие информацию, распространяются от передатчика к приемнику.

КЛАВИАТУРА – внешнее устройство ЭВМ и других технических средств, служащее для ручного ввода информации как при передаче сообщений, так и в целях управления.

КОД – это набор выполняемых инструкций, составляющих программу, в отличие от данных, над которыми выполняются операции. Иначе говоря, кодом называется последовательность машинных инструкций, которые производит транслятор или ассемблер из текста программы.

КОДИРОВАНИЕ – процесс записи или преобразования информации в соответствии с правилами, заданными некоторым кодом.

КОМАНДА – это типовое предписание, записанное на языке машины, определяющее действия ЭВМ при выполнении отдельной операции или части вычислительного процесса.

КОМПЬЮТЕР – то же, что ЭВМ. Чаще употребляется в применении к персональным ЭВМ.

КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ – идентифицируемый, имеющий собственника элемент информационной системы – сведения, знания или набор команд (программа), хранящийся в ЭВМ или управляющий ею.

##### КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ – в уголовном праве РФ – преступления, посягающие на нормальное, безопасное функционирование компьютерных информационных систем.

##### Компьютерное преступление как уголовно-правовое понятие – это 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.

##### В Уголовном кодексе РФ компьютерные преступления классифицируются следующим образом:

##### - нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети;

##### - неправомерный доступ к компьютерной информации;

##### - создание, использование и распространение вредоносных программ для ЭВМ.

##### КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ – документированная (то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать) информация, доступ к которой ограничивается в соответствии с законодательством РФ.

КОПИРОВАНИЕ – изготовление копии объекта. Копирование информации без явно выраженного согласия собственника информационного ресурса независимо от способа копирования подпадает под действие уголовного закона. Важным вопросом является проблема мысленного запечатления полученной информации в процессе ознакомления с нею в памяти человека, без которого, кстати, невозможно ее разглашение.

КРАКЕРЫ (crackers) – специалисты, способные снять защиту от копирования с лицензионного программного обеспечения.

ЛАЗЕРНЫЙ ДИСК (CD диск, оптический диск, компакт-диск) – носитель информации, принцип работы которого основывается на отражении и рассеивании света от различных поверхностей. Источником света служит лазер. Запись информации на данный диск происходит, в основном, в заводских условиях. В персональном компьютере происходит только считывание информации (при отсутствии специального записывающего дисковода).

ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ (ЛВС) – объединение компьютеров с помощью специальных устройств (сетевого оборудования) с целью взаимного использования вычислительных ресурсов, обмена информацией и использования одной базы данных.

МАГНИТООПТИЧЕСКИЕ ДИСКИ – это носители информации, в которых используется принцип изменения магнитного поля при воздействии на поверхность из специального магнитного материала лучом лазера. Используется в компьютерах для записи и считывания информации.

МАШИННАЯ ИНСТРУКЦИЯ – числовые коды, используемые процессором.

МАШИННЫЕ НОСИТЕЛИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ – устройства памяти ЭВМ, периферийные устройства ЭВМ, компьютерные устройства связи, сетевые устройства и сети электросвязи.

МАШИННЫЙ ЯЗЫК – это инструкции в специальных компьютерных кодах, непосредственно используемых процессором (самый сложный уровень программирования).

МОДИФИКАЦИЯ ИНФОРМАЦИИ – внесение в нее любых изменений, обусловливающих ее отличие от той, которую включил в систему и владеет собственник информационного ресурса. Вопрос о легальности произведенной модификации информации следует решать с учетом положений законодательства об авторском праве.

НАРУШЕНИЕ РАБОТЫ ЭВМ – любая нестандартная (нештатная) ситуация с ЭВМ или ее устройствами, находящаяся в причинной связи с неправомерными действиями и повлекшая уничтожение, блокирование, модификацию или копирование информации.

НОСИТЕЛЬ ИНФОРМАЦИИ – это физическое тело или среда для записи, хранения и воспроизведения информации.

ОБЪЕКТ ПРЕСТУПЛЕНИЯ – общественные отношения, охраняемые правом, той или иной отраслью.

ОБЪЕКТИВНАЯ СТОРОНА – внешняя характеристика поступка: само деяние и его противоправность.

ОПЕРАЦИИ В РЕАЛЬНОМ ВРЕМЕНИ – это программные операции, которые должны выполняться в определенный момент, а не тогда, когда компьютер окажется способным их выполнить. Мультипликация, сигналы тревоги и роботы используют работу в реальном времени.

ОПЕРАЦИОННАЯ СИСТЕМА – комплекс программ, постоянно находящихся в памяти ЭВМ, позволяющих организовать управление устройствами машины и ее взаимодействие с пользователями.

ПАКЕТ ПРИКЛАДНЫХ ПРОГРАММ – это организованная совокупность программ постоянного применения для решения некоторых классов однотипных задач.

ПАМЯТЬ – устройство ЭВМ, предназначенное для хранения обрабатываемой информации.

ПАМЯТЬ ВИРТУАЛЬНАЯ – способ управления памятью ЭВМ, позволяющей программе использовать объем оперативной памяти, существенно превышающей емкость микросхем оперативной памяти в ЭВМ.

ПАМЯТЬ ВНЕШНЯЯ – память ЭВМ, организуемая внешними запоминающими устройствами (жесткие и гибкие магнитные диски, магнитные ленты, перфокарты и т.д.).

ПАМЯТЬ ВНУТРЕННЯЯ – память ЭВМ, реализуемая через запоминающее устройство, непосредственно связанное с процессором и содержащее данные, непосредственно участвующие в его операциях.

ПАМЯТЬ ОПЕРАТИВНАЯ – часть внутренней памяти ЭВМ, реализуемая оперативным запоминающим устройством (ОЗУ) и предназначенная для временного хранения команд, данных, результатов в процессе выполнения арифметических и логических операций. После отключения питания ЭВМ информация, хранящаяся в оперативной памяти, автоматически удаляется.

ПАМЯТЬ ПОСТОЯННАЯ – часть внутренней памяти ЭВМ, предназначенная для хранения стандартных программ и данных для управления ЭВМ и решения типовых задач, реализуемая обычно на базе специальных микросхем.

ПАРОЛЬ (ЛОГИН) – это специальная комбинация клавиш, без набора которой невозможно получить доступ к информации и ресурсам вычислительной системы.

ПОЛЬЗОВАТЕЛЬ – человек, работающий на ЭВМ.

ПОРТ – путь, по которому происходит обмен данными между процессором и внешними устройствами.

ПРОГРАММА ДЛЯ ЭВМ – объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин и других компьютерных устройств с целью получения определенного результата. Программы для ЭВМ являются разновидностью компьютерной информации. Программы фактически существуют в двух видах:

- в виде «исходного текста», т.е. описанного с помощью языков программирования алгоритма обработки данных или управления ими, и в виде «объектного кода»;

- исходного текста, компилированного в набор машиночитаемых символов. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЭВМ – это совокупность программных средств управления работой вычислительной машины и совокупность инструментальных программных средств, используемых для создания новых программ.

ПРОЦЕССОР – основное устройство вычислительных машин, выполняющее заданные программы преобразования информации и осуществляющее управление всем вычислительным процессом в ЭВМ.

РАЗДЕЛ – это область жесткого диска. Жесткий диск может быть разбит на разделы с тем, чтобы он использовался несколькими операционными системами.

РЕЗЕРВНОЕ КОПИРОВАНИЕ – процесс создания специальных (резервных) копий с информации по окончании работы или для долговременного хранения.

РЕЗЕРВНЫЕ ИСТОЧНИКИ ПИТАНИЯ (UPS) – это источники питания, способные обеспечить кратковременную работу вычислительной системы при полном отключении электропитания.

РЕЗИДЕНТНАЯ ПРОГРАММА – программа, остающаяся в памяти после завершения. Система предохраняет ее от порчи другими загружаемыми программами, которые могут иметь доступ к содержащимся в данной программе процедурам через вектора прерывания.

СЕТИ ЭВМ – компьютеры, объединенные между собой сетями электросвязи.

##### СЕРВЕР – в информационных сетях – компьютер или программная система, предоставляющие удаленный доступ к своим службам или ресурсам с целью обмена информацией.

##### Сервер работает по заданиям клиентов. После выполнения задания сервер посылает полученные результаты клиенту, инициировавшему это задание.

##### Обычно связь между клиентом и сервером поддерживается посредством передачи сообщений, и при этом используется определенный протокол для кодирования запросов клиента и ответов сервера.

##### СЕТЕВОЙ КЛИЕНТ – компьютер или программа, имеющие доступ к услугам сервера; получающие или обменивающиеся с ним информацией.

##### Сетевой клиент является инициатором и проводит с сервером транзакции либо использует электронную почту.

##### СИСТЕМА ЗАЩИТЫ – это комплекс программно-аппаратных средств, ограничивающих доступ пользователей к определенной информации или ресурсам вычислительной системы.

СИСТЕМА ОПЕРАЦИОННАЯ: См. ОПЕРАЦИОННАЯ СИСТЕМА.

СИСТЕМА ЭВМ – комплексы, в которых хотя бы одна ЭВМ является элементом системы либо несколько ЭВМ составляют систему.

СКРЫТЫЙ ФАЙЛ – это статус, который может быть присвоен файлу установкой его байта атрибутов. Скрытые файлы не выводятся при выводе каталога файлов.

СУБЪЕКТ ПРЕСТУПЛЕНИЯ – лицо старше 16 лет (в некоторых случаях – 14 лет).

СУБЪЕКТИВНАЯ СТОРОНА – осознание лицом, совершающим противоправное деяние, того, что оно нарушает требования правовых норм, и это может повлечь вредные последствия. Обязательный признак – вина.

ТЕКСТ ПРОГРАММЫ – это исходный вариант программы в том виде, как она выглядит до того, как она была переведена в машинный язык.

УГРОЗА БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СИСТЕМЫ – это потенциально возможное происшествие, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней.

УНИЧТОЖЕНИЕ ИНФОРМАЦИИ – наиболее опасное явление, поскольку при этом собственнику информации или информационной системы наносится максимальный реальный вред. Наиболее опасным разрушающим информационные системы фактором чаще всего являются действия людей: уничтожение информации осуществляется умышленными и неосторожными действиями лиц, имеющих возможность воздействия на эту информацию. Существование возможности восстановления уничтоженной неправомерным воздействием информации не является исключающим ответственность фактором.

УСТРОЙСТВО – устройством называется любое оборудование, которое хранит, выводит или обрабатывает информацию, такое как дисковый накопитель, видеодисплей или принтер.

УЯЗВИМОСТЬ КОМПЬЮТЕРНОЙ СИСТЕМЫ – это некоторые ее неудачные характеристики, которые дают возможность возникновения угрозы. Именно из-за уязвимости в системе происходят нежелательные явления.

ФАЙЛ – это последовательность записей, размещаемая на внешних запоминающих устройствах и рассматриваемая в процессе пересылки и обработки как единое целое.

ФАРМИНГ – метод онлайнового мошенничества, заключающийся в изменении DNS (Domain Name System) адресов так, чтобы веб-страницы, которые посещает пользователь, были не оригинальными, а другими, специально созданными кибер-мошенниками для сбора конфиденциальной информации, особенно относящейся к онлайновым банкам.

ФИШИНГ – это опасная техника, используемая для сбора конфиденциальной информации, прикрываясь личностью легитимного лица или организации (обычно путем мошеннических писем, направляющих пользователей на фальсифицированную веб-страницу).

ФЛОППИ-ДИСК: См. ДИСКЕТА.

ХАКЕР – злоумышленник, специализирующийся на взломе защиты отдельных компьютеров и распределенных систем.

ЭВМ (ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНАЯ МАШИНА) есть комплекс электронных устройств, позволяющий осуществлять предписанные программой и (или) пользователем информационные процессы, в том числе последовательности действий по обработке информации и управлению устройствами, над документированной и иной (символьной, образной) информацией и выполнять ее ввод-вывод, уничтожение, копирование, модификацию, передачу информации в сети ЭВМ и другие действия.

1. Муромцев Ю.Л., Орлова Л.П., Муромцев Д.Ю., Тютюнник В.М. Информационные технологии проектирования: Основные понятия, архитектура, принципы. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2004. [↑](#footnote-ref-1)
2. Белозеров Б.И. Техническое творчество. Методические проблемы. – Ульяновск: Приволжское книжное издание, 1975. [↑](#footnote-ref-2)
3. Миронов С.М. Применение высоких технологий в промышленности – стратегические цели и задачи развития России //Высокие технологии, фундаментальные и прикладные исследования, образование. Т.1: Сборник трудов Первой Международной научно-практической конференции «Исследования, разработка и применение высоких технологий в промышленности». – СПб.: Изд-во Политехн. ун-та, 2005. [↑](#footnote-ref-3)
4. Утрачивает силу с 01.01.2008 согласно ФЗ РФ от 18 декабря 2006 г. № 231–ФЗ «О введении в действие части четвертой Гражданского кодекса Российской Федерации». [↑](#footnote-ref-4)
5. Постановление Правительства РФ от 11 октября 1993 г. № 1030 (в ред. от 04.02.2005 «О контроле за выполнением обязательств по гарантиям использования импортируемых и экспортируемых товаров и услуг двойного назначения в заявленных целях». [↑](#footnote-ref-5)
6. Richard Szafranski «Theory of Information Warfare», USAF, 2002. [↑](#footnote-ref-6)
7. Гаврилов О. А. Курс правовой информатики: Учебник для вузов. М.: НОРМА, 2000. [↑](#footnote-ref-7)
8. Наумов А.В. Российское уголовное право: Курс лекций. В 2 т. –М., 2004. [↑](#footnote-ref-8)
9. Наумов А.В. Комментарий к Уголовному кодексу РФ. – М.: Ин-т государства и права РАН, 1996. [↑](#footnote-ref-9)
10. Тоффлер Э. Третья волна. – М., 1999. [↑](#footnote-ref-10)
11. Анисимов А.П. Компьютерная лингвистика для всех: Мифы. Алгоритмы. Язык – Киев: Наук. думка, 1991. [↑](#footnote-ref-11)
12. Россинская Е.Р. Проблемы становления компьютерно-технической экспертизы как нового рода инженерно-технических экспертиз //Криминалистика в XXI веке. Материалы международной научно-практи­ческой конференции. – М., 2001. [↑](#footnote-ref-12)
13. Голдман С. Теория информации. Пер. с англ. – М., 1957. [↑](#footnote-ref-13)
14. Малая советская энциклопедия. – М.: Знание, 1960. [↑](#footnote-ref-14)
15. Толковый словарь по вычислительным системам /Под ред. В. Иллингуотера и др. – М.: Машиностроение, 1990. [↑](#footnote-ref-15)
16. Бордовский Г.А. Информатика в понятиях и терминах. – М.: Просвещение, 1991. [↑](#footnote-ref-16)
17. Каган Б.М. Электронные вычислительные машины и системы. – М.: Энергоатомиздат, 1985. [↑](#footnote-ref-17)
18. Тюкин В.Н. Теория управления: Конспект лекций. Часть 1. – Вологда: ВоГТУ, 2000. [↑](#footnote-ref-18)
19. Мамлеев Р.Р. Обеспечение защиты информации при использовании технических систем обработки: Учебное пособие. – Уфа: УЮИ МВД РФ, 2003. [↑](#footnote-ref-19)
20. ###  Мальков В.И., Мартынов Ю.М. Информация и связь в системах управления. – М.: Московский рабочий, 1973.

 [↑](#footnote-ref-20)
21. ###  Каган Б.М. Электронные вычислительные машины и системы. – М.: Энергоатомиздат, 1985.

 [↑](#footnote-ref-21)
22. Английское понятие «*computer*» гораздо шире, чем понятие «компьютер» в русском языке. В английском языке компьютером называют любое устройство, способное производить математические расчеты, вплоть до логарифмической линейки. В связи с чем для обозначения того, что мы понимаем под словом компьютер, в англо-говорящих странах употребляют «*personal computer*». [↑](#footnote-ref-22)
23. *Computing & Multimedia*. Словарь. – М.: Внешсигма, 1996. [↑](#footnote-ref-23)
24. Фолкберри Л.М. Справочное пособие по ремонту электрических и электронных схем. – М.: Энергоатомиздат, 1989. [↑](#footnote-ref-24)
25. Кирмайер М. Мультимедиа. – СПб., 1994. [↑](#footnote-ref-25)
26. Europe Towards 90. Banking. – Digital Equipment Corp., 1992. [↑](#footnote-ref-26)
27. Васильченко А.И., Денисьева О.М., Жарков М.А. и др. Система телефонной сигнализации по общему каналу (система ОКС). – М.: Связь, 1980. [↑](#footnote-ref-27)
28. Термин заимствован из зарубежной печати. Он касается двухпроводной линии между телефонным аппаратом (ТА) и устройствами аналого-цифровых преобразователей. Информация в последней «миле» передается в аналоговой форме. [↑](#footnote-ref-28)
29. Область пространства, ограниченная дальностью установления связи для беспроводных телефонных аппаратов (между стационарным и переносным блоком), а также ячейка действия сотового телефона. [↑](#footnote-ref-29)
30. Левин М., Библия хакера. Книга 2. – М.: Майор, 2003. [↑](#footnote-ref-30)
31. Громаков Ю.А. Сотовые системы подвижной радиосвязи. Технологии электронных коммуникаций. – М.: Эко-Трендз, 1994. [↑](#footnote-ref-31)
32. Существуют две разновидности алгоритма: A5/1 – «сильная» версия шифра и A5/2 – ослабленная. [↑](#footnote-ref-32)
33. Громаков Ю.А. Организация физических и логических каналов в стандарте *GSM* //Электросвязь, 1993. № 10. [↑](#footnote-ref-33)
34. Громаков Ю.А. Сотовые системы подвижной радиосвязи. – М.: Эко-Трендз, 1994. [↑](#footnote-ref-34)
35. Муромцев Ю.Л., Орлова Л.П., Муромцев Д.Ю., Тютюнник В.М. Информационные технологии проектирования. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2004. [↑](#footnote-ref-35)
36. Мамлеев Р.Р., Обеспечение неотслеживаемости каналов передачи данных вычислительных систем //Безопасность информационных технологий. №2. – М.: МИФИ, 1999. [↑](#footnote-ref-36)
37. Петров В.А., Пискарев А.С., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах: Учебное пособие. Изд. 2-е, испр. – М.: МИФИ, 1995. [↑](#footnote-ref-37)
38. *Gadget* (англ.) – техническое устройство. [↑](#footnote-ref-38)
39. Витвитская С.А. Охотники за чужими головами //Щит и меч. 13.10.2005. [↑](#footnote-ref-39)
40. Ястребов, Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового примерного анализа) //Государство и право, 2005. № 1. С.53–63. [↑](#footnote-ref-40)
41. Яблоков Н.П. Криминалистика: Учебник. – М.: ЛексЭст, 2006. [↑](#footnote-ref-41)
42. Бекряшев А.К., Белозеров И.П., Бекряшева Н.С. Теневая экономика и экономическая преступность. 2003. Компьютерный ресурс. Режим доступа: *http://kiev-security.org.ua*. [↑](#footnote-ref-42)
43. Наумов А.В. Комментарий к Уголовному кодексу РФ. – М.: Институт государства и права РАН, 1996. [↑](#footnote-ref-43)
44. Хвоевский С.А., Исаева Л.М., Дьяков Ф.С., Вайле С.П. Выявление, пресечение и документирование фактов неправомерного доступа к охраняемой законом информации в контрольно-кассовых машинах при осуществлении предпринимательской деятельности: Методические рекомендации. – М.: ВНИИ МВД России, 2005. [↑](#footnote-ref-44)
45. Лучин И.Н., Шурухнов Н.Г. Методические рекомендации по изъятию компьютерной информации при проведении обыска //Информационный бюллетень СК МВД России. 1996. № 4(89). С. 22-28. [↑](#footnote-ref-45)
46. Федеральные законы «Об информации, информационных технологиях и о защите информации» и «О персональных данных». [↑](#footnote-ref-46)
47. При условии легальности операционной системы, что весьма сомнительно в данных обстоятельствах. Прим. авт. [↑](#footnote-ref-47)
48. Встречается во всех законах, прямо или косвенно касающихся компьютерной информации. Прим. авт. [↑](#footnote-ref-48)
49. Приказ Росархива № 68 «Об утверждении Типовой инструкции по делопроизводству в федеральных органах исполнительной власти» от 27 ноября 2000 г. [↑](#footnote-ref-49)
50. Постановление Госстандарта России № 28 «Государственный стандарт РФ ГОСТ Р 51141–98 «Делопроизводство и архивное дело. Термины и определения», 1998 г. [↑](#footnote-ref-50)
51. ГОСТ Р 51141–98 «Делопроизводство и архивное дело. Термины и определения». [↑](#footnote-ref-51)
52. Федеральный закон «О персональных данных» от 27 июля 2006 года № 152–ФЗ. [↑](#footnote-ref-52)
53. *Computing & Multimedia*: Словарь. – М.: Внешсигма, 1996. [↑](#footnote-ref-53)
54. Проект Уголовного кодекса Российской Федерации //Российская газета .25 января 1995 г. [↑](#footnote-ref-54)
55. Баев О.Я., Мещеряков В.А. Проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации //Конфидент. 1998. № 7(23). [↑](#footnote-ref-55)
56. Ястребов, Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового примерного анализа) //Государство и право. 2005. № 1. С.53-63. [↑](#footnote-ref-56)
57. Мещеряков В.А. Криминалистическая классификация преступлений в сфере компьютерной информации //Конфидент. 1999. №4-5. [↑](#footnote-ref-57)
58. Зуйков Г.Г. Установление способа совершения преступления. – М.: МВШ МВД СССР, 1970. [↑](#footnote-ref-58)
59. Крылов В.В. Основы криминалистической теории расследования преступлений в сфере информации: Автореферат диссертации на соискание ученой степени доктора юридических наук. – М.: НИИ проблем укрепления законности и правопорядка Генеральной прокуратуры РФ, 1998. [↑](#footnote-ref-59)
60. Сорокин. А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. Компьютерный ресурс. Режим доступа: *//http://kurgan.unets.ru/~procur/ my\_page.htm*, 1999. [↑](#footnote-ref-60)
61. Крылов В.В. Указанная работа. [↑](#footnote-ref-61)
62. Копылов В.А. Информационное право: Учебник. 2-е изд. – М.: Юристь, 2002. [↑](#footnote-ref-62)
63. Сорокин. А.В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. Компьютерный ресурс. Режим доступа: *//http://kurgan.unets.ru/~procur my\_page.htm*, 1999. [↑](#footnote-ref-63)
64. Аналитическая деятельность и компьютерные технологии: Учебное пособие /Под ред. проф. В.А. Минаева. – М.: МЦ при ГУК МВД России, 1996. [↑](#footnote-ref-64)
65. Дранников В.Н. Некоторые детерминанты компьютерной преступности в свете современной уголовной политики //Материалы научно-практической конференции. – Таганрог: ТГРУ, 2006. [↑](#footnote-ref-65)
66. Мещеряков В.А., Герасименко В.Г. Пути и средства обеспечения доказуемости правонарушений в сфере компьютерной информации //Материалы конференции. «Безопасность информации». Москва, 14-18 апреля 1997. [↑](#footnote-ref-66)
67. Растегаев А.А. Анализ общеуголовной корыстной преступности //Методика анализа преступности. – М.: «Инфо-М», 1986. [↑](#footnote-ref-67)
68. См. Гражданский кодекс РФ ст. 138, Закон РФ «О государственной тайне» ст. 10, Закон «О правовой охране программ для ЭВМ и баз данных» в ст. 2, Закон РФ «Об информации, информационных технологиях и о защите информации» ст. 11, Таможенный кодекс РФ ст. 20 и т.п. [↑](#footnote-ref-68)
69. Мотуз О. Алло! Вы безопасность гарантируете? //Конфидент. 1998. № 5. [↑](#footnote-ref-69)
70. Лазарева И.В. Некоторые проблемы расследования несанкционированного доступа к сетям сотовой радиотелефонной связи //«Черные дыры» в Российском законодательстве. 2007. № 1. [↑](#footnote-ref-70)
71. Материалы официального сайта *CFCA*. Компьютерный ресурс. Режим доступа: *//http://www.cfca.org*. [↑](#footnote-ref-71)
72. См. Пресс-релиз к брифингу ДЭБ МВД России «О мерах, предпринимаемых Департаментом экономической безопасности МВД России по защите прав интеллектуальной собственности, пресечению производства и распространения фальсифицированной и контрафактной продукции». Компьютерный ресурс. Режим доступа: /http://www.mvd.rupress/release/4881/4881/. [↑](#footnote-ref-72)
73. Ривкин К. Преступления с кредитными карточками //Экономика и жизнь. 1997. № 2. [↑](#footnote-ref-73)
74. Малокостов В. О преступности в области пластиковых карточек //Мир карточек. 1999. № 12. [↑](#footnote-ref-74)
75. Киселева Е. От крапленых карт до тузов в рукаве //Коммерсантъ. 1995. № 28. [↑](#footnote-ref-75)
76. Ривкин К. Указанная работа. [↑](#footnote-ref-76)
77. Виды интернет-преступлений (по классификации ООН). Издательство «Семь Дней», 2000. Компьютерный ресурс. Режим доступа: *//w3s.nsf\Archive\Archive.html*. [↑](#footnote-ref-77)
78. #  *Козлов В.Е., Пармон И.О. О некоторых результатах осуществления противодействия использованию компьютерных технологий в сферах торговли людьми и распространения детской порнографической продукции в республике Беларусь. Режим доступа:* http://www.crime-research.ru*.*

 [↑](#footnote-ref-78)
79. Коншин А.А. Защита полиграфической продукции от фальсификации. – М.: ООО «Синус», 2000. [↑](#footnote-ref-79)
80. Жуки в полоску //Хакер. 2005. № 84. [↑](#footnote-ref-80)
81. Беляев В. Безопасность в распределительных системах //Открытые системы. 1995. № 3. [↑](#footnote-ref-81)
82. Крылов В.В. Информация как элемент криминальной деятельности //Вестник Московского университета. Серия 11. – Право, 1998. [↑](#footnote-ref-82)
83. Крылов В.В. Информация как элемент криминальной деятельности //Вестник Московского университета. Серия 11. – Право, 1998. [↑](#footnote-ref-83)
84. Минаев В.А., Саблин В.Н. Основные проблемы борьбы с компьютерными преступлениями в России. Экономика и производство. Компьютерный ресурс. Режим доступа: *http://www.mte.ru/www/toim.nsf.* [↑](#footnote-ref-84)
85. ###  Маклаков Г.Ю., Рыжков Э.В. Особенности оперативно-разыскной деятельности при расследовании преступлений в сфере высоких технологий. Компьютерный ресурс. Режим доступа: //http://www.crime-research.org.

 [↑](#footnote-ref-85)
86. ###  Маклаков Г.Ю., Рыжков Э.В. Особенности оперативно-разыскной деятельности при расследовании преступлений в сфере высоких технологий. Компьютерный ресурс. Режим доступа: //http://www.crime-research.org.

 [↑](#footnote-ref-86)
87. Маклаков Г.Ю. Анализ сплоченности студенческой группы в работе куратора //Сб. Структурно-системный подход в обучении и воспитании. – Днепропетровск: ДГУ, 1984. С. 129-131. [↑](#footnote-ref-87)
88. Рыжков Э.В. Энергоинформационная безопасность общества и государства с позиции деятельности правоохранительных органов //Злочини проти особистої волі людини: Збірник матеріалів міжнародного науково-практичного семінару (Харків, 19-20 вересня 2000 р.). – Харків: «Книжкове видавництво» Лествиця Марії, 2002. С. 83 – 88. [↑](#footnote-ref-88)
89. Роганов С.А. Синтетические наркотики: вопросы расследования преступлений. – СПб: Питер, 2001. [↑](#footnote-ref-89)
90. Вехов В.Б., Рогозин В.Ю. Методика расследования преступлений в сфере компьютерной информации. 2002. Компьютерный ресурс. Режим доступа: *http: //www. crime.vl.ru /books*. [↑](#footnote-ref-90)
91. Илюшин Д.А. Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг «Интернет» //Вестник Муниципального института права и экономики (МИПЭ). Вып. 1. – Липецк: Издательство НОУ «Интерлингва», 2004. С. 77 – 86. [↑](#footnote-ref-91)
92. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. – М.: ООО Изд. «Юрлитинформ», 2001. [↑](#footnote-ref-92)
93. Например, см.: Рогозин В.Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной информации: Учеб. пособие /Под ред. А.А. Закатова. – Волгоград, 2000. С. 38-41; Шурухнов Н.Г., Левченко И.П., Лучин И.Н. Специфика проведения обыска при изъятии компьютерной информации //Актуальные проблемы совершенствования деятельности ОВД в новых экономических и социальных условиях. – М.: 1997. С. 208-216. [↑](#footnote-ref-93)
94. Расследование неправомерного доступа к компьютерной информации /Под ред. Н.Г. Шурухнова. – М., 1999. [↑](#footnote-ref-94)
95. Видеограммой документа называется его изображение на экране средства видеоотображения информации ЭВМ – см.: п. 18 ч. 2 ГОСТа Р 51141–98 «Делопроизводство и архивное дело. Термины и определения» (введен в действие с 01.01.99 г. Постановлением Госстандарта России от 27.02.98 г. № 28). [↑](#footnote-ref-95)
96. Семенов Г.В., Бирюков П.Н. Ответственность за «мошенничество» в сетях сотовой связи: Учебное пособие. – Воронеж: Воронежский государственный университет, 2002. [↑](#footnote-ref-96)
97. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. – Воронеж, 2002. [↑](#footnote-ref-97)
98. Расследование преступлений в сфере компьютерной информации: Методические рекомендации //Остроушко А.В., Прохоров А.С., Задорожко С.М., Тронин М.Ю., Гаврилюк С.В. Компьютерный ресурс. Режим доступа: *http://zakon.kuban.ru/uk/272`274.htm*. [↑](#footnote-ref-98)
99. 27 июля 2006 г. принят Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, отменивший указанный закон. [↑](#footnote-ref-99)