**КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

**КУРСОВАЯ РАБОТА**

ПО ТЕМЕ:

**«Компьютерная безопасность,   
компьютерная преступность и государственная служба»**

*Выполнил:*

*MDV*

*Научный руководитель:*

Ростов-на-Дону

**СОДЕРЖАНИЕ**

Введение

1. Компьютерная преступность

2. Предупреждение компьютерных преступлений

2.1. Защита данных в компьютерных сетях

2.2. Физическая защита данных

2.2.1. Кабельная система

2.2.2. Системы электроснабжения

2.2.3. Системы архивирования и дублирования информации

2.2.4. Защита от стихийных бедствий

2.3. Программные и программно-аппаратные методы защиты

2.3.1. Защита от компьютерных вирусов

2.3.2. Защита от несанкционированного доступа

2.3.3. Защита информации при удаленном доступе

3. Компьютерная безопасность, компьютерная преступность и государственная служба

Заключение

Список использованных источников и литературы

# Введение

Изменения, происходящие в экономической жизни России - создание финансово-кредитной системы, предприятий различных форм собственности и т.п. - оказывают существенное влияние на вопросы защиты информации. Долгое время в нашей стране существовала только одна собственность - государственная, поэтому информация и секреты были тоже только государственные, которые охранялись мощными спецслужбами.

Проблемы информационной безопасности постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и, прежде всего вычислительных систем. Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением.

Каждый сбой работы компьютерной сети это не только "моральный" ущерб для работников предприятия и сетевых администраторов. По мере развития технологий платежей электронных, "безбумажного" документооборота и других, серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике. На сегодняшний день сформулировано два базовых принципа информационной безопасности, которая должна обеспечивать:

- целостность данных - защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных.

- конфиденциальность информации и, одновременно, ее доступность для всех авторизованных пользователей.

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

# 1. Компьютерная преступность

Попытаемся кратко обрисовать явление, которое как социологическая категория получила название "компьютерная преступность". Компьютерные преступления условно можно подразделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, и, преступления, использующие компьютеры как необходимые технические средства.

Перечислим основные виды преступлений, связанных с вмешательством в работу компьютеров:

1. Несанкционированный доступ к информации, хранящейся в компьютере. Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Несанкционированный доступ к файлам законного пользователя осуществляется также нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз, как покупатель рассматривает товары на витрине.

Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого приема. Самый простейший путь его осуществления - получить коды и другие идентифицирующие шифры законных пользователей. Это может делаться:

- приобретением (обычно подкупом персонала) списка пользователей со всей необходимой информацией;

- обнаружением такого документа в организациях, где не налажен достаточный контроль за их хранением;

- подслушиванием через телефонные линии.

Несанкционированный доступ может осуществляться в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных. Все происходит так, словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В таком случае он может проникнуть в чужие сейфы и похитить все, что в них хранится.

2. Ввод в программное обеспечение "логических бомб", которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему.

Способ "троянский конь" состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. С помощью "троянского коня" преступники, например, отчисляют на свой счет определенную сумму с каждой операции. Компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен, тысяч, а иногда и миллионов команд. Поэтому "троянский конь", состоящий из нескольких десятков команд, вряд ли может быть обнаружен, если, конечно, нет подозрений относительно этого. Но и в последнем случае экспертам-программистам потребуется много дней и недель, чтобы найти его.

Есть еще одна разновидность "троянского коня". Ее особенность состоит в том, что в безобидно выглядящей кусок программы вставляются не команды, собственно, выполняющие "грязную" работу, а команды, формирующие эти команды и после выполнения уничтожающие их. В этом случае программисту, пытающемуся найти "троянского коня", необходимо искать не его самого, а команды его формирующие.

3. Разработка и распространение компьютерных вирусов.

Вирус - это довольно сложная и изощрённая программа. Попав в компьютер, он может самостоятельно "размножаться". Вирус прикрепляется к рабочим программам, копирует и переносит себя на диски и дискеты. При этом он нарушает нормальное функционирование компьютера.

"Жизненный цикл" и принцип действия вируса представляют собой сложную систему. Все неприятности начинаются с того, что вирус встраивается, вживается в какую-либо программу, загружаемую в компьютер. После запуска этой программы автоматически запускается механизм действия вируса. Обычно он проявляет себя не сразу, этому предшествует "инкубационный период", который может продолжаться от нескольких дней до нескольких месяцев. Разрушительное действие вируса проявляется после завершения "инкубационного периода". За это время он поражает память компьютера, записывая свои копии в подходящие для этого программы. Каждый вирус совместим лишь с программами определённого типа. Сегодня различают следующие типы вирусов:

- операционные, заражающие операционную систему;

- прикладные, заражающие прикладные или системные программы;

- компиляторные, заражающие объектную библиотеку компилятора;

- драйверные, заражающие драйверы локальной сети.

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

Каковы способы распространения компьютерного вируса? Они основываются на способности вируса использовать любой носитель передаваемых данных в качестве "средства передвижения". То есть с начала заражения имеется опасность, что ЭВМ может создать большое число средств передвижения и в последующие часы вся совокупность файлов и программных средств окажется зараженной. Таким образом, дискета или магнитная лента, перенесенные на другие ЭВМ, способны заразить их. И наоборот, когда "здоровая" дискета вводится в зараженный компьютер, она может стать носителем вируса. Удобными для распространения обширных эпидемий оказываются телекоммуникационные сети. Достаточно одного контакта, чтобы персональный компьютер был заражен или заразил тот, с которым контактировал. Однако самый частый способ заражения - это копирование программ, что является обычной практикой у пользователей персональных ЭВМ. Так скопированными оказываются и зараженные программы.

Есть предположения, что ежедневно создаётся от 3 до 5 вирусов. Естественно, что против них принимаются чрезвычайные меры, приведшие к созданию текстовых программ-антивирусов. Защитные программы подразделяются на три вида:

- фильтрующие (препятствующие проникновению вируса),

- противоинфекционные (постоянно контролирующие процессы в системе),

- противовирусные (настроенные на выявление отдельных вирусов).

Справедливости ради следует отметить, что распространение компьютерных вирусов имеет и некоторые положительные стороны. В частности, они являются, по-видимому, лучшей защитой от похитителей программного обеспечения. Зачастую разработчики сознательно заражают свои дискеты каким-либо безобидным вирусом, который хорошо обнаруживается любым антивирусным тестом. Это служит достаточно надежной гарантией, что никто не рискнет копировать такую дискету.

4. Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

Проблема неосторожности в области компьютерной техники сродни неосторожной вине при использовании любого другого вида техники, транспорта и т.п.

Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна, а в ряде случаев почти не достижима.

5. Подделка компьютерной информации.

По-видимому, этот вид компьютерной преступности является одним из наиболее свежих. Он является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, причем имеющий достаточно высокую квалификацию.

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосования, референдумов и т.п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы. Естественно, что подделка информации может преследовать и другие цели.

Рассмотрим теперь вторую категорию преступлений, в которых компьютер является "средством" достижения цели. Здесь можно выделить разработку сложных математических моделей, входными данными в которых являются возможные условия проведения преступления, а выходными данными - рекомендации по выбору оптимального варианта действий преступника.

Вот один из примеров, когда компьютер является "средством" для совершения преступления. В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз до тех пор, пока на счете не оказывается приличная сумма (фактически она постоянно "перескакивает" с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются, а владелец счета исчезает.

Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике в такую игру включают большое количество банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

Можно представить себе создание специализированного компьютера-шпиона, который, будучи подключен к разведуемой сети, генерирует всевозможные запросы, фиксирует и анализирует полученные ответы.

# 2. Предупреждение компьютерных преступлений

При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на предупреждение преступления. Выделим из них:

- технические,

- организационные,

К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

К организационным мерам отнесем охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

## 2.1. Защита данных в компьютерных сетях

При рассмотрении проблем защиты данных в сети, прежде всего, возникает вопрос о классификации сбоев и нарушений, прав доступа, которые могут привести к уничтожению или нежелательной модификации данных. Среди таких потенциальных "угроз" можно выделить:

1. Сбои оборудования:

- сбои кабельной системы;

- перебои электропитания;

- сбои дисковых систем;

- сбои систем архивации данных;

- сбои работы серверов, рабочих станций, сетевых карт и т.д.

2. Потери информации из-за некорректной работы персонального оборудования (ПО):

- потеря или изменение данных при ошибках ПО;

- потери при заражении системы компьютерными вирусами.

3. Потери, связанные с несанкционированным доступом:

- несанкционированное копирование, уничтожение или подделка информации;

- ознакомление с конфиденциальной информацией, составляющей тайну, посторонних лиц;

4. Потери информации, связанные с неправильным хранением архивных данных.

5. Ошибки обслуживающего персонала и пользователей:

- случайное уничтожение или изменение данных;

- некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных.

В зависимости от возможных видов нарушений работы сети (под нарушением работы я также понимаю и несанкционированный доступ) многочисленные виды защиты информации объединяются в три основных класса:

- средства физической защиты, включающие средства защиты кабельной системы, систем электропитания, средства архивации, дисковые массивы и т.д.

- программные средства защиты, в том числе: антивирусные программы, системы разграничения полномочий, программные средства контроля доступа.

- административные меры защиты, включающие контроль доступа в помещениях, разработку стратегии безопасности фирмы, планов действий в чрезвычайных ситуациях и т.д.

Следует отметить, что подобное деление достаточно условно, поскольку современные технологии развиваются в направлении сочетания программных и аппаратных средств защиты. Наибольшее распространение такие программно-аппаратные средства получили, в частности, в области контроля доступа, защиты от вирусов и т.д.

Концентрация информации в компьютерах - аналогично концентрации наличных денег в банках - заставляет все более усиливать контроль в целях защиты информации. Юридические вопросы, частная тайна, национальная безопасность - все эти соображения требуют усиления внутреннего контроля в коммерческих и правительственных организациях. Работы в этом направлении привели к появлению новой дисциплины: безопасность информации. Специалист в области безопасности информации отвечает за разработку, реализацию и эксплуатацию системы обеспечения информационной безопасности, направленной на поддержание целостности, пригодности и конфиденциальности накопленной в организации информации. В его функции входит обеспечение физической (технические средства, линии связи и удаленные компьютеры) и логической (данные, прикладные программы, операционная система) защиты информационных ресурсов.

Сложность создания системы защиты информации определяется тем, что данные могут быть похищены из компьютера и одновременно оставаться на месте; ценность некоторых данных заключается в обладании ими, а не в уничтожении или изменении.

Обеспечение безопасности информации - дорогое дело, и не столько из-за затрат на закупку или установку средств, сколько из-за того, что трудно квалифицированно определить границы разумной безопасности и соответствующего поддержания системы в работоспособном состоянии.

Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока не произведен соответствующий анализ. Анализ риска должен дать объективную оценку многих факторов (подверженность появлению нарушения работы, вероятность появления нарушения работы, ущерб от коммерческих потерь, снижение коэффициента готовности системы, общественные отношения) и предоставить информацию для определения подходящих типов и уровней безопасности.

Шифрование данных традиционно использовалось правительственными и оборонными департаментами, но в связи с изменением потребностей и многие компании начинают использовать возможности, предоставляемые шифрованием для обеспечения конфиденциальности информации. Шифрование данных может осуществляться в режимах On-line (в темпе поступления информации) и Off-line (автономном).

## 2.2. Физическая защита данных

### 2.2.1. Кабельная система

Кабельная система остается главной "ахиллесовой пятой" большинства локальных вычислительных сетей: по данным различных исследований, именно кабельная система является причиной более чем половины всех отказов сети. В связи с этим кабельной системе должно уделяться особое внимание с самого момента проектирования сети.

Наилучшим образом избавить себя от "головной боли" по поводу неправильной прокладки кабеля является использование получивших широкое распространение в последнее время так называемых структурированных кабельных систем, использующих одинаковые кабели для передачи данных в локальной вычислительной сети, локальной телефонной сети, передачи видеоинформации или сигналов от датчиков пожарной безопасности или охранных систем.

Понятие "структурированность" означает, что кабельную систему здания можно разделить на несколько уровней в зависимости от назначения и месторасположения компонентов кабельной системы. Вот пример одной из кабельных систем, она состоит из:

- Внешней подсистемы (campus subsystem)

- Административной подсистемы (administrative subsystem)

- Магистрали (backbone cabling)

- Горизонтальной подсистемы (horizontal subsystem)

- Рабочих мест (work location subsystem)

Наилучшим способом защиты кабеля от физических (а иногда и температурных, и химических воздействий, например, в производственных цехах) является прокладка кабелей с использованием в различной степени защищенных коробов. Другая важная проблема правильной инсталляции и безотказной работы кабельной системы - соответствие всех ее компонентов требованиям международных стандартов.

### 2.2.2. Системы электроснабжения

Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии в настоящее время является установка источников бесперебойного питания. Различные по своим техническим и потребительским характеристикам, подобные устройства могут обеспечить питание всей локальной сети или отдельного компьютера в течение промежутка времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитные носители. Большинство источников бесперебойного питания одновременно выполняет функции и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства - серверы, концентраторы, мосты и т.д. - оснащены собственными дублированными системами электропитания. Некоторые корпорации имеют собственные аварийные электрогенераторы или резервные линии электропитания. Эти линии подключены к разным подстанциям, и при выходе из строя одной них электроснабжение осуществляется с резервной подстанции.

### 2.2.3. Системы архивирования и дублирования информации

Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер.

Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия.

### 2.2.4. Защита от стихийных бедствий

Основной и наиболее распространенный метод защиты информации и оборудования от различных стихийных бедствий - пожаров, землетрясений, наводнений и т.д. - состоит в хранении архивных копий информации или в размещении некоторых сетевых устройств, например, серверов баз данных, в специальных защищенных помещениях, расположенных, как правило, в других зданиях или, реже, даже в другом районе города или в другом городе.

## 2.3. Программные и программно-аппаратные методы защиты

### 2.3.1. Защита от компьютерных вирусов

Вряд ли найдется хотя бы один пользователь или администратор сети, который бы ни разу не сталкивался с компьютерными вирусами. На сегодняшний день дополнительно к тысячам уже известных вирусов появляется 100-150 новых ежемесячно. Наиболее распространенными методами защиты от вирусов по сей день остаются различные антивирусные программы.

Однако в качестве перспективного подхода к защите от компьютерных вирусов в последние годы все чаще применяется сочетание программных и аппаратных методов защиты. Среди аппаратных устройств такого плана можно отметить специальные антивирусные платы, которые вставляются в стандартные слоты расширения компьютера.

### 2.3.2. Защита от несанкционированного доступа

Проблема защиты информации от несанкционированного доступа особо обострилась с широким распространением локальных и, особенно, глобальных компьютерных сетей. Необходимо также отметить, что зачастую ущерб наносится не из-за "злого умысла", а из-за элементарных ошибок пользователей, которые случайно портят или удаляют жизненно важные данные. В связи с этим, помимо контроля доступа, необходимым элементом защиты информации в компьютерных сетях является разграничение полномочий пользователей.

В такой системе организации защиты все равно остается слабое место: уровень доступа и возможность входа в систему определяются паролем. Не секрет, что пароль можно подсмотреть или подобрать. Для исключения возможности неавторизованного входа в компьютерную сеть в последнее время используется комбинированный подход – пароль+идентификация пользователя по персональному "ключу". В качестве "ключа" может использоваться пластиковая карта (магнитная или со встроенной микросхемой - smart-card) или различные устройства для идентификации личности по биометрической информации - по радужной оболочке глаза или отпечатков пальцев, размерам кисти руки и так далее.

Оснастив сервер или сетевые рабочие станции, например, устройством чтения смарт-карточек и специальным программным обеспечением, можно значительно повысить степень защиты от несанкционированного доступа. В этом случае для доступа к компьютеру пользователь должен вставить смарт-карту в устройство чтения и ввести свой персональный код. Программное обеспечение позволяет установить несколько уровней безопасности, которые управляются системным администратором. Возможен и комбинированный подход с вводом дополнительного пароля, при этом приняты специальные меры против "перехвата" пароля с клавиатуры. Этот подход значительно надежнее применения паролей, поскольку, если пароль подглядели, пользователь об этом может не знать, если же пропала карточка, можно принять меры немедленно.

Смарт-карты управления доступом позволяют реализовать, в частности, такие функции, как контроль входа, доступ к устройствам персонального компьютера, доступ к программам, файлам и командам. Кроме того, возможно также осуществление контрольных функций, в частности, регистрация попыток нарушения доступа к ресурсам, использования запрещенных утилит, программ, команд DOS.

### 2.3.3. Защита информации при удаленном доступе

По мере расширения деятельности предприятий, роста численности персонала и появления новых филиалов, возникает необходимость доступа удаленных пользователей (или групп пользователей) к вычислительным и информационным ресурсам главного офиса компании. Чаще всего для организации удаленного доступа используются кабельные линии (обычные телефонные или выделенные) и радиоканалы. В связи с этим защита информации, передаваемой по каналам удаленного доступа, требует особого подхода.

В частности, в мостах и маршрутизаторах удаленного доступа применяется сегментация пакетов - их разделение и передача параллельно по двум или нескольким линиям, что делает невозможным "перехват" данных при незаконном подключении "хакера" к одной из линий. К тому же используемая при передаче данных процедура сжатия передаваемых пакетов гарантирует невозможности расшифровки "перехваченных" данных. Кроме того, мосты и маршрутизаторы удаленного доступа могут быть запрограммированы таким образом, что удаленные пользователи будут ограничены в доступе к отдельным ресурсам сети главного офиса.

Широкое распространение радиосетей в последние годы поставило разработчиков радиосистем перед необходимостью защиты информации от "хакеров", вооруженных разнообразными сканирующими устройствами. Были применены разнообразные технические решения. Например, в радиосетях некоторых компаний информационные пакеты передаются через разные каналы и базовые станции, что делает практически невозможным для посторонних собрать всю передаваемую информацию воедино.

# 3. Компьютерная безопасность, компьютерная преступность и государственная служба

На данном этапе нашей жизни происходит массовое (тотальное) осознание и понимание того, что гос. службе должно уделяться не малое значение, чего нельзя сказать о времени до 1992 года. Например, с 1992 года начала активно развиваться наука о государственном и муниципальном управлении, впервые введена специальность "Государственное и муниципальное управление". До этого момента подготовка кадров осуществлялась узкопрофильно и исследования в области государственного и муниципального управления, как таковые, не велись.

Поскольку в наш век развиваются и постоянно улучшаются средства обработки, хранения информации и обмена ей - это не могло не коснуться государства. Если взять различные сферы этого политического образования: правоохранительную, финансовую, образовательную, то здесь, по большому счету, во всех крупных учреждениях используются ЭВМ различных модификаций, а также многие другие атрибуты информационных технологий.

В связи с этим проблемы компьютерной безопасности и компьютерной преступности прочно и глубоко внедряются в государственную службу. Практически каждый человек, будь то управляющий или подчинённый, находящийся на попечительстве у государства, должен знать и, по крайней мере, иметь представление о том, что такое компьютер и "с чем его едят". Ведь передача данных по сети или простейшая обработка информации, по средствам специально написанных для этого программ, не может осуществляться людьми, знающими об ЭВМ только то, что это монитор, клавиатура и "мышка".

# Заключение

Подводя итоги, хотелось бы отметить, что проблемам компьютерной безопасности и компьютерной преступности в гос. службе должно придаваться особое значение. Правильно иерархически построенная система доступа к данным на гос. уровне, современное оборудование, штат квалифицированных работников, отвечающих за компьютерную безопасность - это гарант безопасности государственной информации, а вместе с тем и государства. В этом нельзя сомневаться. Как-то один мудрец сказал: "Чем больше вы даёте, тем больше к вам возвращается". И правда, - чем больше будет уделено внимания проблемам компьютерной безопасности и компьютерной преступности, тем больше будет уверенности в том, что данные гос. важности не будут потеряны при малейшем сбое в работе оборудования или при несанкционированном доступе. Так же подчеркну, что никакие аппаратные, программные и любые другие средства, и организаторские работы различных видов не смогут гарантировать абсолютную надежность и безопасность данных, но в то же время свести риск потерь к минимуму возможно лишь при осознанном, комплексном подходе к вопросам компьютерной безопасности и компьютерной преступности.

# Список использованных источников и литературы

1. Фигурнов В.Э. IBM PC для пользователя. Москва, 1995.
2. Рааб М. (M. Raab). Защита сетей: наконец-то в центре внимания // Компьютеруорлд, Москва, 1994, №29.
3. Волошина В.В., Титов К.А. Государственная служба в Российской Федерации. Москва, 1995.
4. Феоктисов Г.Г. Информационная безопасность общества, личность и средства массовой информации // Информатика и вычислительная техника, 1996, №1-2.
5. Дергачёва Е.В. Роль информационного противоборства в современных условиях // Информатика и вычислительная техника, 1996, №1-2.
6. Хакеры: Компьютерная преступность. Можно ли ей противостоять? // Мир безопасности, 1997, №11.
7. Информация защищена. Нет проблем? // Мир безопасности, 1997, №11.

8. Островский А.К. Компьютерные вирусы / Приложение к газете «Первое сентября», Москва, 1996, №4.