**Министерство сельского хозяйства**

**Российской федерации**

**Фгоу впо «воронежский государственный**

**аграрный университет имени К.Д. Глинки»**

**Кафедра информационного обеспечения**

**и моделирования агроэкономических систем**

Курсовая работа

на тему:

**«Компьютерные преступления и методы защиты информации»**

Выполнил: студент

заочной формы обучения

**Асташова Т.К.**

Шифр АБ/08392

Руководитель: к.э.н., доц.

**Кусмагамбетов С.М.**

Усмань 2009

**Содержание**

1. Общие сведения о компьютерных преступлениях

1.1. Основные направления компьютерных преступлений

1.2. Классификация компьютерных преступлений

1.3. Методы защиты информации

2. Обзор современных программных средств, обеспечивающих обслуживание устройств ПК

2.1. Norton Utilities (Norton System Works)

2.2. Acronis Power Utilities

2.3. System Mechanic

Выводы и предложения

Список использованной литературы

**Введение**

Проблема обеспечения информационной безопасности актуальна с тех пор, как люди стали обмениваться информацией, накапливать ее и хранить. Во все времена возникала необходимость надежного сохранения наиболее важных достижений человечества с целью передачи их потомкам. Аналогично возникала необходимость обмена конфиденциальной информацией и надежной ее защиты.

В современном обществе проблема информационной безопасности особенно актуальна, поскольку информация стала частью жизни современного общества. Развитие современного общества во многом определяется теми информационными процессами, которые в нем протекают.

Быстро развивающиеся информационные технологии вносят заметные изменения в жизнь общества. Информация стала товаром, который можно приобрести, продать, обменять. При этом стоимость информации часто во много раз превосходит стоимость аппаратных средств, в которых она хранится. От степени безопасности информационных технологий зависит благополучие, а порой и жизнь многих людей.

С началом массового применения компьютеров проблема информационной безопасности приобрела особую остроту. С одной стороны, компьютеры стали носителями информации и, как следствие, одним из каналов ее получения как санкционированного, так и несанкционированного. С другой стороны, компьютеры как любое техническое устройство подвержены сбоям и ошибкам, которые могут привести к потере информации. Под *информационной безопасностью* понимается защищенность информации от случайного или преднамеренного вмешательства, наносящего ущерб ее владельцам или пользователям.

С повышением значимости и ценности информации соответственно растет и важность ее защиты. С одной стороны, информация стала товаром, и ее утрата или несвоевременное раскрытие наносит материальный ущерб. С другой стороны, информация - это сигналы управления процессами в обществе, в технике, а несанкционированное вмешательство в процессы управления может привести к катастрофическим последствиям.

Для анализа возможных угроз информационной безопасности рассмотрим составные части автоматизированной системы обработки информации:

* аппаратные средства - компьютеры и устройства обмена информацией между ними (внутренние и внешние устройства, устройства связи и линии связи);
* программное обеспечение — системное и прикладное программное обеспечение;
* данные (информация) — хранимые временно и постоянно на внутренних и внешних носителях, печатные копии, системные журналы;
* персонал — обслуживающий персонал и пользователи.

*Опасные воздействия* на информационную систему подразделяются на случайные и преднамеренные.

Причинами *случайных воздействий* являются:

аварийные ситуации вследствие стихийных бедствий и нарушения электропитания;

отказы и сбои аппаратуры;

ошибки в программном обеспечении;

ошибки в работе пользователей;

помехи в линиях связи из-за воздействий внешней среды.

*Преднамеренные воздействия* — это целенаправленные действия нарушителя, обусловленные не только материальными, но и психологическими факторами, например, недовольство служебным положением, любопытство, конкурентная борьба и т. п.

*Защита информации* — это комплекс мер по ограничению доступа к информации пользователей и программ, по обеспечению ее подлинности, целостности в процессе передачи (обмена) и хранения.[4]

Цель данной работы – раскрыть понятие компьютерных преступлений и рассмотреть методы защиты информации.

Для достижения поставленной цели необходимо решить следующие задачи:

* рассмотреть основные направления компьютерных преступлений;
* дать классификацию компьютерным преступлениям;
* охарактеризовать методы защиты информации;
* сделать обзор программных средств, обеспечивающих обслуживание устройств ПК.

В ходе написания работы использовался монографический метод, графический метод.

Курсовая работа оформлена в текстовом процессоре MS Word с использованием технических средств: компьютер Intel (R) Celeron (R) CPU 3.06 GHz, 248 МБ ОЗУ, принтер Samsung ML-1610.

1. **Общие сведения о компьютерных преступлениях**
	1. **Основные направления компьютерных преступлений**

*Компьютерные преступления* - это предусмотренные уголовным кодексом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть. Компьютерные преступления условно можно разделить на две большие категории:

* преступления, связанные с вмешательством в работу компьютеров;
* преступления, использующие компьютеры как необходимые технические средства.

Перечислим основные виды преступлений, связанные 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.

Хакер, «компьютерный пират», - лицо, совершающее систематические несанкционированные доступы в компьютерные системы и сети с целью развлечения, мошенничества или нанесения ущерба (в том числе и путем распространения компьютерных вирусов). С одной стороны «хакер» - это человек, который прекрасно знает компьютер и пишет хорошие программы, а с другой, - незаконно проникающий в компьютерные системы с целью получения информации.

Английский глагол «to hack» применительно к компьютерам может означать две вещи - взломать систему или починить ее. В основе этих действий лежит нечто общее - понимание того, как устроен компьютер и программы, которые на нем работают.

Таким образом, слово «хакер» совмещает в себе, по крайней мере, два значения: одно - окрашенное негативно («взломщик»), другое - нейтральное или даже хвалебное («ас», «мастер»). Другими словами, хакеров можно разделить на «плохих» и «хороших».

«Хорошие» хакеры двигают технический прогресс и используют свои знания и умения на благо человечества. Ими разработано большое число новых технических и программных систем.

Им, как водится, противостоят «плохие»: они читают чужие письма, воруют чужие программы и всеми доступными способами вредят прогрессивному человечеству.

«Плохих» хакеров можно условно разделить на четыре группы. Первая, состоящая в основном из молодежи, - люди, взламывающие компьютерные системы просто ради собственного удовольствия. Они не наносят вреда, а такое занятие весьма полезно для них самих - со временем из них получаются превосходные компьютерные специалисты.

Вторая группа - пираты. Они взламывают защиту компьютеров для похищения новых программ и другой информации.

Третья группа - хакеры, использующие свои познания действительно во вред всем и каждому. Они уничтожают компьютерные системы, в которые им удалось прорваться, читают чужие письма, а потом издеваются над их авторами. Когда читаешь в телеконференциях их рассказы о взломах, складывается впечатление, что это люди с ущемленным чувством собственного достоинства. Есть и еще одна группа - хакеры, которые охотятся за секретной информацией по чьим-либо заказам.

Русские хакеры. На сегодняшний день западные спецслужбы озабочены нашествием хакеров с востока. По данным Интерпола, ежегодно на военных компьютерах США фиксируется несколько тысяч атак российских хакеров.

Во время экономических потрясений, которые пережила наша страна в последние годы, огромное количество действительно высококлассных специалистов осталось не у дел. В этот период и было написано то великое множество вирусов, которыми прославилась Россия. В большинстве своем отечественные хакеры не получают выгоды от взломов, хотя есть и исключения.

Среди российского хакерства выделяются четыре основных типа.

Первый - романтики-одиночки. Они, как правило, взламывают базы данных из чистого любопытства. В целом они довольно безопасны и бескорыстны, но и наиболее талантливы. Поэтому массовые взломы компьютерных сетей какой-либо фирмы обычно начинаются после того, как на нее набредет кто-то из «романтиков» и похвастается этим в своей сети.

Второй - прагматики, или классики. Работают как в одиночку, так и группами. Воруют, как говорится, что придется - игры, программы, электронные версии разных изданий. Например, еще в сентябре 1995 г. фирма «Майкрософт» с большой помпой представляла в Москве «WINDOWS 95». По оценкам западной прессы, на рекламу нового продукта ушло около 300 миллионов долларов и фирмачи потом долго не могли понять, почему в России эта новейшая база раскупается так плохо. А дело в Том, что наши хакеры еще в апреле взломали главный компьютер «Майкрософта», украли оттуда засекреченный тогда «WINDOWS 95» и наладили продажу его по ценам дешевле фирменных

Третий - разведчики. Сегодня в любой уважающей себя фирме имеется хакер, оформленный обычно как программист. Его задача - взламывать сети конкурентов и красть оттуда самую разную информацию. Этот тип пользуется сейчас наибольшим спросом.

Четвертый - кибергангстеры. Это уже профессиональные компьютерные бандиты, работают они в основном на мафиозные структуры. Их задачи конкретные - блокировка и развал работы компьютерных сетей разных «неугодных» российских и западных фирм, а также кража денег с банковских счетов. Дело это дорогое и небезопасное, зато самое высокооплачиваемое.

Нахальство наших компьютерных хулиганов не в последнюю очередь обусловлено фактическим отсутствием борьбы с ними на Родине.

Только в Москве выявлено более 360 человек, незаконно оплачивающих коммуникационные услуги. Юридическая тонкость момента, сидя Дома, человек совершает преступление на территории США. Привлечь их к ответственности в соответствии с законодательством США очень сложно: тут можно годами разбираться.

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

«Временная бомба» - разновидность «логической бомбы», которая срабатывает по достижении определенного момента времени.

Способ «троянский конь» состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять 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» 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 стоит в том, что в безобидно выглядящий 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. Развивая эту идею, можно представить себе команды, которые создают команды и т.д. (сколь угодно большое число раз), создающие «троянского коня».

*3. Разработка и распространение компьютерных вирусов.*

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

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 недостижима.

*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, голосований, референдумов и т.п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

*6. Хищение компьютерной информации.*

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

Рассмотрим теперь вторую категорию преступлений, в которых компьютер является «средством» достижения цели.

1. Разработка сложных математических моделей, входными данными в которых являются возможные условия проведения преступления, а выходными данными - рекомендации по выбору оптимального варианта действий преступника.

2. Преступления с общим названием «воздушный змей». В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз («воздушный змей» поднимается все выше и выше) до тех пор, пока на счете не оказывается приличная сумма (фактически она постоянно «перескакивает» с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются, а владелец счета исчезает. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике в такую игру включают большое количество банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.[2]

* 1. **Классификация компьютерных преступлений**

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. Ниже приведены
названия способов совершения подобных преступлений, соответствующие
кодификатору Генерального Секретариата Интерпола. В 1991 году данный
кодификатор был интегрирован в автоматизированную систему поиска и в
настоящее время доступен НЦБ более чем 100 стран.

Все коды, характеризующие компьютерные преступления, имеют идентификатор, начинающийся с буквы Q. Для характеристики преступлений может использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного.

*QA - Несанкционированный доступ и перехват:*

QAH - компьютерный абордаж,

QAI - перехват,

QAT - кража времени,

QAZ - прочие виды несанкционированного доступа и перехвата.

*QD - Изменение компьютерных данных:*

QUL - логическая бомба,

QDT - троянский конь,

QDV - компьютерный вирус,

QDW - компьютерный червь,

QDZ - прочие виды изменения данных.

*QF - Компьютерное мошенничество:*

QFC - мошенничество с банкоматами,

QFF - компьютерная подделка,

QFG - мошенничество с игровыми автоматами,

QFM - манипуляции с программами ввода-вывода,

QFP - мошенничества с платежными средствами,

QFT - телефонное мошенничество,

QFZ - прочие компьютерные мошенничества.

*QR - Незаконное копирование:*

QRG - компьютерные игры,

QRS - прочее программное обеспечение,

QRT - топография полупроводниковых изделий,

QRZ - прочее незаконное копирование,

*QS - Компьютерный саботаж:*

QSH - с аппаратным обеспечением,

QSS - с программным обеспечением,

QSZ - прочие виды саботажа,

*QZ - Прочие компьютерные преступления:*

QZB - с использованием компьютерных досок объявлений,

QZE - хищение информации, составляющей коммерческую тайну, *i*

QZS - передача информации конфиденциального характера,

QZZ - прочие компьютерные преступления,

Кратко охарактеризуем некоторые виды компьютерных преступлений согласно приведенному кодификатору.

*Несанкционированный доступ и перехват информации (QA) включает в себя следующие виды компьютерных преступлений.*

QAH - «Компьютерный абордаж» (хакинг - hacking) - доступ в компьютер или сеть без права на то. Этот вид компьютерных преступлений обычно используется хакерами для проникновения в чужие информационные сети.

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 используется следующая специфическая терминология:

1. *"Жучок"* (bugging) характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала;
2. *"Откачивание данных"* (data leakage)отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе;
3. *"Уборка мусора"* (scavening) характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.д. Электронный вариант требует исследования данных, оставленных в памяти машины;
4. метод следования *"За дуракам*" (piggbacking), характеризующий несанкционированное проникновение как в пространственные, так и в электронные закрытые зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним;
5. метод *"За хвост"* (between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний закончит активный режим, осуществлять доступ к системе;
6. метод *"Неспешного выбора"* (browsing). В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости;
7. метод *"Поиск бреши"* (trapdoor entry), при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;
8. метод *"Люк"* (trapdoor), являющийся развитием предыдущего. В найденной "бреши" программа "разрывается", и туда вставляется определенное число команд. По мере необходимости "люк" открывается, а встроенные команды автоматически осуществляют свою задачу;
9. метод *"Маскарад"* (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;
10. метод «*Мистификация»* (spoofing)*,* который используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коду пользователя.

QAT - кража времени - незаконное использование компьютерной системы или сети с намерением неуплаты.

*Изменение компьютерных данных (QD) включает в себя следующие виды преступлений:*

QDL/QDT - логическая бомба (logic bomb), троянский конь (trojan horse) - изменение компьютерных данных без права на то путем внедрения логической бомбы или троянского коня.

Логическая бомба заключается в тайном встраивании в программа набора команд, который должен сработать лишь однажды, но при определенных условиях.

Троянский конь заключается в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

QDV - вирус (virus) - изменение компьютерных данных или программ без права на то путем внедрения или распространения компьютерного вируса.

**Компьютерный вирус** - это специально написанная программа, которая может «приписать» себя к другим программам (т.е. «заражать» их), размножаться и порождать новые вирусы для выполнения различных нежелательных действий на компьютере.

QDW - червь - изменение компьютерных данных или программ без права на то путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть.

*Компьютерные мошенничества (QF) объединяют в своем составе разнообразные способы совершения компьютерных преступлений:*

QFC - компьютерные мошенничества, связанные с хищением наличных денег из банкоматов.

QFF - компьютерные подделки - мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и пр.).

QFG - мошенничества и хищения, связанные с игровыми автоматами.

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.

QFP - компьютерные мошенничества и хищения, связанные с.платежными средствами. К этому виду относятся самые распространенные
компьютерные преступления, связанные с кражей денежных средств, которые составляют около 45% всея преступлений, связанных с использованием ЭВМ.

QFT - телефонное мошенничество - доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.

*Незаконное копирование информации (QR) составляют следующие виды компьютерных преступлений:*

QRG/QRS - незаконное копирование, распространение или опубликование компьютерных игр и другого программного обеспечения, защищенного законом.

QRT - незаконное копирование топографии 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.

*Компьютерный саботаж (QS) составляют следующие виды преступлении.*

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.

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

*К прочим видам компьютерных преступлений (QZ) в классификаторе отнесены следующие:*

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

QZE -хищение информации, составляющей коммерческую тайну -приобретение .незаконными средствами или передача информации, представляющей коммерческую тайну без права на то или другого иконного обоснования с намерением причинить экономический ущерб иди получить незаконные экономические преимущества;

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

Некоторые специалисты по компьютерной преступности в особую группу выделяют методы манипуляции, которые имеют специфические жаргонные названия.

«Временная бомба» - разновидность логической бомбы, которая срабатывает при достижении определенного момента времени.

«Асинхронная атака» (asynchronous attack) состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей.

«Моделирование» (simulation modelling) используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления. Таким образом, осуществляется «оптимизация» способа совершения преступления.[2]

1.3 **Методы защиты информации**

Для решения проблем защиты информации в сетях прежде всего нужно уточнить возможные причины сбоев и нарушений, способные привести к уничтожению или нежелательной модификации данных. К ним, в частности, относятся:

сбои оборудования (кабельной системы, электропитания, дисковых систем, систем архивации данных, работы серверов, рабочих станций, сетевых карт и т.д.);

потери информации из-за некорректной работы ПО;

заражение системы компьютерными вирусами;

ущерб, наносимый организации несанкционированным копированием, уничтожением или подделкой информации, доступом посторонних лиц к конфиденциальным данным;

потери информации, связанные с неправильным хранением архивных данных;

ошибки обслуживающего персонала и пользователей (случайное уничтожение или изменение данных, некорректное использование программного и аппаратного обеспечения).

Меры защиты от названных нарушений можно разделить на три основные группы:

средства физической защиты (кабельной системы, электропитания, аппаратуры архивации данных, дисковых массивов и т.д.);

программные средства (антивирусные программы, системы разграничения полномочий, программные средства контроля доступа к информации);

административные меры (охрана помещений, разработка планов действий в чрезвычайных ситуациях и т.п.).

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

Концентрация информации в компьютерных системах (аналогично концентрации наличных денег и других материальных ценностей в банках) заставляет все более усиливать контроль за ее сохранностью как в частных, так и в правительственных организациях. Работы в этом направлении привели к появлению новой дисциплины: безопасность информации. Специалист в этой области отвечает за разработку, реализацию и эксплуатацию системы обеспечения информационной безопасности; в его функции входит обеспечение как физической (технические средства, линии связи, удаленные компьютеры), так и логической защиты информационных ресурсов (данные, прикладные программы, операционная система).

Обеспечение безопасности информации обходится дорого, и не столько из-за затрат на закупку или установку соответствующих средств, сколько из-за того, что трудно точно определить границы разумно безопасности и объем ресурсов, требуемых для поддержания системы в работоспособном состоянии. Так, если локальная сеть разрабатывалась в целях совместного использования лицензионных программных средств, дорогих принтеров или больших файлов общедоступной информации, нет никакой необходимости даже в минимальных затратах на системы шифрования/дешифрования данных.

Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока не произведен анализ имеющихся рисков и связанных с ними потерь. При этом нужно учитывать многие факторы (подверженность системы сбоям, вероятность появления нарушений ее работы, ущерб от возможных коммерческих потерь, снижение коэффициента готовности сети, отношения в коллективе, юридические проблемы) и собрать разнообразную информацию для определения подходящих типов и уровней безопасности. Коммерческие организации сейчас все больше переносят критическую корпоративную информацию с закрытых внутренних систем в открытую среду (в том числе связанную с Интернетом) и встречаются с новыми сложными проблемами при реализации и эксплуатации систем безопасности. Растет популярность распределенных баз данных и приложений типа «клиент-сервер» при управления бизнесом. Это также увеличивает риск неавторизованного доступа к данным и их искажения.

*Средства физической защиты данных*

*Кабельная система* остается главной «ахиллесовой пятой» большинства ЛВС: по данным различных исследований, именно из-за нее происходит более половины всех отказов сети. Поэтому надежности кабельной системы должно уделяться особое внимание с самого начала проектирования.

Наилучшим образом избавить себя от проблем, связанных с неправильной прокладкой кабеля, позволяет использование получивших широкое распространение структурированных кабельных систем (например, SYSTIMAX SCS фирмы AT&T, OPEN DECconnect компании Digital, кабельной системы корпорации ЮМ). В них используются одинаковые кабели для передачи данных в локальной вычислительной сети, локальной телефонной сети, видеоинформации, сигналов от датчиков пожарной безопасности или охранных систем. Структурированность в данном случае означает, что кабельную систему здания можно разделить на несколько уровней в зависимости от назначения и месторасположения ее компонентов. Например, кабельная система SYSTIMAX SCS включает внешнюю (campus subsystem), административную (administrative subsystem) и горизонтальную подсистемы (horizontal subsystem), аппаратную (equipment room), магистраль (backbone cabling) и подсистему рабочих мест (work location subsystem).

Внешняя подсистема состоит из медного или оптоволоконного кабеля, устройств электрической защиты и заземления, и связывает коммуникационную и обрабатывающую аппаратуру в здании (или комплексе зданий). Кроме того, в эту подсистему входят устройства сопряжения внешних кабельных линий с внутренними.

Аппаратные служат для размещения различного коммуникационного оборудования, необходимого для обеспечения работы административной подсистемы. Последняя предназначена для быстрого и легкого управления кабельной системой SYSTIMAX SCS при изменении планов размещения персонала и отделов. В ее состав входят кабельная система (неэкранированная витая пара и оптоволокно), устройства коммутации и сопряжения магистрали и горизонтальной подсистемы, соединительные шнуры, маркировочные средства и т.д.

Магистраль состоит из медного кабеля или комбинации медного и оптоволоконного кабеля и вспомогательного оборудования. Она связывает между собой этажи здания или большие площади одного и того же этажа.

Горизонтальная подсистема на базе витого медного кабеля расширяет основную магистраль от входных точек административной системы этажа к розеткам на рабочем месте.

И, наконец, оборудование рабочих мест включает в себя соединительные шнуры, адаптеры, устройства сопряжения и обеспечивает механическое и электрическое соединение с горизонтальной кабельной подсистемой.

Наилучшим способом защиты кабеля от физических воздействий (а иногда также от температурных и химических воздействий - например, в производственных цехах) является прокладка кабелей с использованием защищенных коробов. При прокладке сетевого кабеля вблизи источников электромагнитного излучения необходимо соблюдать следующие требования:

неэкранированная витая пара должна отстоять минимум на 15—30 см от электрического кабеля, розеток, трансформаторов и т.п.;

расстояние от коаксиального кабеля до электрических линий или электроприборов должно быть не менее 10-15 см.

Другая важная проблема кабельной системы - соответствие всех ее компонентов требованиям международных стандартов. Наибольшее распространение в настоящее время получил стандарт EIA/TIA 568. Он был разработан совместными усилиями UL, American National Standarts Institute (ANSI) и Electronic Industry Association/Telecommunications Industry Association, подгруппой TR41.8.1 для кабельных систем на витой паре (UTP).

В дополнение к стандарту EIA/TIA 568 существует документ DIS 118-01, разработанный International Standard Organization (ISO) и International Electrotechnical Commission (IEC). Данный стандарт использует термин «категория» для отдельных кабелей и термин «класс» для кабельных систем.

Необходимо также отметить, что требования стандарта EIA/TIA 568 относятся только к сетевому кабелю. Но в систему, помимо кабеля, входят также соединительные разъемы, розетки, распределительные панели и другие элементы. Поэтому использование только кабеля категории 5 не гарантирует создания кабельной системы этой категории. Все перечисленное выше оборудование должно быть сертифицировано аналогичным образом.

*Системы электроснабжения.* Наиболее надежным средством предотвращения потерь информации при кратковременных отключениях электроэнергии в настоящее время остаются источники бесперебойного питания. Различные по своим техническим и потребительским характеристикам, они могут обеспечить питание всей локальной сети или отдельного компьютера в течение времени, достаточного для восстановления подачи напряжения или, по крайней мере, для сохранения информации на внешних носителях.

Большинство источников бесперебойного питания одновременно выполняет функции стабилизатора напряжения, что также повышает устойчивость системы. Многие современные сетевые устройства (серверы, концентраторы, мосты и др.) оснащаются автономными 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 из них электроснабжение осуществляется с резервной подстанции.

*Системы архивирования и дублирования информации.* Организация надежной и эффективной системы архивации данных - одна из важнейших задач защиты информации. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях лучше использовать для этой цели специализированный архивационный сервер.

Носители архивной информации, представляющей особую ценность, должны находиться в отдельном охраняемом помещении.

*Защита от стихийных бедствий.* Основным и наиболее распространенным методом защиты информации от различных стихийных бедствий (пожаров, землетрясений, наводнений и т.п.) является хранение дубликатов архивных копий или размещение некоторых сетевых устройств (например, серверов баз данных) в специальных защищенных помещениях, расположенных, как правило, в других зданиях, а иногда в другом районе города или даже в другом городе.

*Программные и программно-аппаратные методы защиты*

*Шифрование данных* традиционно использовалось спецслужбами и оборонными ведомствами; сейчас, в связи с ростом возможностей компьютерной техники, многие коммерческие компании и даже частные лица начинают использовать средства шифрования для обеспечения конфиденциальности данных. Прежде всего речь идет о финансовых службах крупных компаний, часто предъявляющих особые требования к алгоритму, используемому в процессе шифрования. В то же время рынок коммерческих систем не всегда требует такой строгой защиты, как правительственные или оборонные ведомства, поэтому возможно применение продуктов и другого типа, например PGP (Pretty Good Privacy).

Шифрование данных может осуществляться в режимах on-line (в темпе поступления информации) и off-line (автономном). Остановимся подробнее на первом режиме, представляющем наибольший интерес. Для него чаще всего используются два алгоритма - DES и RSA.

*Стандарт шифрования данных DES* (Data Encryption Standart) был разработан фирмой ЮМ в начале 70-х годов и в настоящее время является правительственным стандартом для шифрования цифровой информации. Он рекомендован Ассоциацией американских банкиров. Сложный алгоритм DES использует ключ длиной 56 бит и 8 бит проверки на четность и требует от злоумышленника перебора 72 квадриллионов возможных ключевых комбинаций, обеспечивая высокую степень защиты при небольших расходах. При частой смене ключей алгоритм удовлетворительно решает проблему превращения конфиденциальной информации в недоступную.

*Алгоритм RSA* был изобретен Ривестом, Шамиром и Альдеманом в 1976 г. и представляет собой значительный шаг в развитии криптографии. Этот алгоритм также был принят в качестве стандарта Национальным Бюро Стандартов.

В отличие от DES, RSA является ассиметричным алгоритмом, то есть он использует разные ключи при шифровании и дешифровании. Пользователи имеют два ключа и могут широко распространять свой открытый ключ. Он используется для шифрования сообщения пользователем, но только определенный получатель может дешифровать его своим секретным ключом; открытый ключ бесполезен для дешифрования. Это делает ненужными секретные соглашения о передаче ключей между корреспондентами.

DES определяет длину данных и ключа в битах, a RSA может быть реализован при любой длине ключа. Чем длиннее ключ, тем выше уровень безопасности (но одновременно возрастает время шифрования и дешифрования). Если ключи DES можно сгенерировать за микросекунды, то типичное время генерации ключа RSA- десятки секунд\*. Поэтому открытые ключи RSA предпочитают разработчики программных средств, а секретные ключи DES - разработчики аппаратуры.

*Защита от компьютерных вирусов.* По данным исследования, проведенного фирмой Creative Strategies Research, 64% из 451 опрошенного специалиста испытали «на себе» действие вирусов. На сегодняшний день дополнительно к тысячам уже известных вирусов ежемесячно появляется 100-150 новых. Наиболее распространенными методами защиты от них остаются антивирусные программы.

В качестве перспективного подхода в последние годы все чаще применяется сочетание программных и аппаратных средств защиты. Среди аппаратных устройств такого плана можно отметить специальные антивирусные платы, которые вставляются в стандартные слоты расширения компьютера. Корпорация Intel еще в 1994 г. предложила перспективную технологию защиты от вирусов в компьютерных сетях. Flash-память сетевых адаптеров Intel EtherExpress PRO/10 содержит антивирусную программу, сканирующую все системы компьютера еще до его загрузки.

*Защита от несанкционированного доступа.* Проблема защиты информации от несанкционированного доступа обострилась в связи с широким распространением локальных и особенно глобальных компьютерных сетей. Очень часто ущерб наносят не злоумышленники, а сами пользователи, которые из-за элементарных ошибок портят или удаляют важные данные. Поэтому, помимо контроля доступа, необходимым элементом защиты информации в сетях является разграничение полномочий пользователей. Обе задачи могут быть успешно решены за счет встроенных средств сетевых операционных систем. Например, в ОС NetWare 4.1, помимо стандартных средств ограничения доступа, таких, как система паролей и разграничения полномочий, предусмотрен ряд новых возможностей, обеспечивающих наивысший уровень защиты данных. Новая версия NetWare позволяет, в частности, шифровать данные по методу открытого ключа (алгоритм RSА) с формированием электронной подписи для передаваемых по сети пакетов.

Но и в такой системе защиты имеется 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 сеть в последнее время все чаще используется комбинированный подход: пароль плюс идентификация пользователя по персональному ключу. В качестве такого ключа может применяться пластиковая карта (магнитная или со встроенной микросхемой - smart-card) или различные устройства для идентификации личности по биометрической информации (радужной оболочке глаза, отпечаткам пальцев, размерам кисти руки и др.). Для доступа к компьютеру пользователь должен вставить смарт-карту в устройство чтения и ввести свой персональный код (примерно так, как это делается в банкоматах).

Программное обеспечение позволяет установить несколько уровней безопасности, которые управляются системным администратором. Возможен и комбинированный подход с вводом дополнительного пароля, причем принимаются специальные меры от перехвата пароля с клавиатуры. Такие системы аутентификации значительно надежнее паролей; если пароль стал известен постороннему лицу, пользователь может об этом и не знать, а если пропала пластиковая карта, можно принять меры незамедлительно.

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.

Одним из удачных примеров комплексного решения проблемы контроля доступа, основанного как на программных, так и на аппаратных средствах защиты, стала система Kerberos. В основе этой схемы авторизации лежат три компонента:

база данных, содержащая информацию по всем сетевым ресурсам, пользователям, паролям, шифровальным ключам и т.д.;

авторизационный сервер (authentication server), обрабатывающий все запросы пользователей на доступ к тому или иному виду сетевых услуг. Получив такой запрос, сервер обращается к базе данных и определяет, имеет ли пользователь право на совершение данной операции. При этом пользовательские пароли по сети не передаются, что также повышает степень защиты информации;

Ticket-granting server (сервер выдачи разрешений) получает от авторизационного сервера «пропуск», содержащий имя пользователя и его сетевой адрес, время запроса и ряд других параметров, а также уникальный сессионный ключ. Пакет, содержащий пропуск, передается в зашифрованном по алгоритму DES виде. После получения и расшифровки пропуска сервер выдачи разрешений проверяет запрос и сравнивает ключи, после чего дает разрешение на использование сетевой аппаратуры или программ.

Среди других подобных комплексных схем можно отметить разработанную Европейской ассоциацией производителей компьютеров (ЕСМА) систему Sesame (Secure European System for Applications in Multivendor Environment), предназначенную для использования в крупных гетерогенных сетях.

*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. Компания Datapro свидетельствует, что уже в 1995 г. только в США число работников, постоянно или временно осуществляющих удаленный доступ к компьютерным сетям, составляло 25 млн человек. Чаще всего с этой целью используются кабельные линии (обычные телефонные или выделенные) и радиоканалы. Естественно, защита информации, передаваемой по таким каналам, требует особого подхода.

В частности, в мостах и маршрутизаторах удаленного доступа применяется сегментация пакетов - их разделение и передача параллельно по двум линиям, что делает невозможным перехват данных при подключении хакера к одной из линий. Используемая при передаче данных процедура сжатия также затрудняет их расшифровку при перехвате. 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.

Разработаны и специальные устройства контроля доступа к компьютерным сетям по коммутируемым линиям. Например, фирмой AT&T предлагается модуль Remote Port Security Device (PRSD), представляющий собой два блока размером с обычный модем: RPSD Lock (замок), устанавливаемый в центральном офисе, и RPSD Key (ключ), подключаемый к модему удаленного пользователя. RPSD Key и Lock позволяют установить несколько уровней защиты и контроля доступа к информации, в частности:

шифрование данных, передаваемых по линии при помощи генерируемых цифровых ключей;

контроль доступа в зависимости от дня недели или времени суток (всего 14 ограничений).

Широкое распространение радиосетей в последние годы потребовало от разработчиков оборудования создания систем защиты информации от хакеров, оснащенных самыми современными сканирующими устройствами. Были найдены различные технические решения. Например, в радиосети компании RAM Mobil Data информационные пакеты передаются через разные каналы и базовые станции, что делает для постороннего лица практически невозможным свести всю передаваемую информацию воедино. Активно используются в радиосетях и технологии шифрования данных при помощи алгоритмов DES и RSA.

В настоящее время защита данных обеспечивается законодательными актами на международном и национальном уровнях. Еще в 1981 г. Совет Европы одобрил Конвенцию по защите данных, в Великобритании подобный закон был принят в 1984 г. В России базовые нормы защиты информации содержатся в законах «Об информации, информатизации и защите информации» и «О правовой охране программ для электронных вычислительных машин и баз данных», изданных соответственно в 1995 и 2002 гг.

Эти правовые акты устанавливают нормы, регулирующие отношения в области формирования и потребления информационных ресурсов, создания и применения информационных систем, информационных технологий и средств их обеспечения, защиты информации и защиты прав граждан в условиях массовой информатизации общества.

На федеральном уровне принимаются следующие меры для обеспечения информационной безопасности:

осуществляется формирование и реализация единой государственной политики по обеспечению защиты национальных интересов от угроз в информационной сфере;

устанавливается баланс между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;

совершенствуется законодательство РФ в сфере обеспечения информационной безопасности;

координируется деятельность органов государственной власти по обеспечению безопасности в информационной среде;

защищаются государственные информационные ресурсы на оборонных предприятиях;

развиваются отечественные телекоммуникационные и информационные структуры;

совершенствуется информационная структура развития новых информационных технологий;

унифицируются средства поиска, сбора, хранения, обработки и анализа информации для вхождения в глобальную информационную инфраструктуру.

Вопросы информационной безопасности государства оговариваются в «Концепции национальной безопасности Российской Федерации», созданной в соответствии с Указом президента РФ от 17 декабря 1997 г.

Некоторые меры по защите информации предусмотрены в главе 28 УК РФ «Преступления в сфере компьютерной информации». В ст. 272 «Неправомерный доступ к компьютерной информации», состоящей, как и две последующие, из двух частей, содержится достаточно много признаков, обязательных для объекта, объективной и субъективной сторон данного состава преступления. Непосредственным объектом ее являются общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ, их системы или сети.

Состав преступления сформулирован как материальный, причем если само деяние определено однозначно (неправомерный доступ к охраняемой законом компьютерной информации), то последствия, хотя они и обязательны, могут быть весьма разнообразны: уничтожение информации, ее блокирование, модификация, копирование, нарушение работы ЭВМ, систем ЭВМ и их сети.

Часть 2 ст. 272 предусматривает в качестве квалифицирующих признаков несколько новых, характеризующих объективную сторону и субъект состава преступления. Это совершение деяния: группой лиц по предварительному сговору; организованной группой; лицом с использованием своего служебного положения; лицом, имеющим доступ к ЭВМ, их системе или сети.

Ст. 273 имеет название «Создание, использование и распространение вредоносных программ для ЭВМ». Непосредственным объектом данного преступления являются общественные отношения по безопасному использованию ЭВМ, ее программного обеспечения и информационного содержания. Статья предусматривает наказания при совершении одного из следующих действий: создание программ для ЭВМ, заведомо приводящих (приводящей) к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы аппаратной части; внесение в существующие программы изменений, обладающих аналогичными свойствами; использование двух названных видов программ; их распространение; использование машинных носителей с такими программами; распространение таких носителей.

Ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» касается неисполнения пользователями своих профессиональных обязанностей, приводящему к нарушению целостности хранимой и перерабатываемой информации. Непосредственный объект преступления, предусмотренного этой статьей, - отношения по соблюдению правил эксплуатации ЭВМ, системы или их сети, то есть аппаратно-технического комплекса. Под таковыми правилами понимаются, во-первых, Обще- российские временные санитарные нормы и правила для работников вычислительных центров, во-вторых, техническая документация на приобретаемые компьютеры, в-третьих, конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка.[1]

1. **Обзор современных программных средств, обеспечивающих обслуживание устройств ПК**

* 1. **Norton Utilities (Norton System Works)**

Norton SystemWorks 2003 Professional Edition - универсальный интегрированный набор самых совершенных программных средств для решения проблем, возникающих в ходе работы с компьютером, и оптимизации его производительности.

Набор программных компонентов "логически" разбит на четыре основных модуля: Norton Utilities, Norton AntiVirus, Norton CleanSweep и Norton Ghost - объедененных в оболочку.

Компания Symantec давно завоевала лидирующее место среди производителей системных утилит, модуль Norton Utilities явное тому подтверждение. По функциональности компоненты модуля разбиты на группы: Optimize Performance включает утилиты Speed Disk и Norton Optimization Wizard, оптимизируют дисковое пространство и системный реестр для ускорения доступа и запуска программ; Find and Fix Problems состоит из программ Norton System Doctor, UnErase Wizard, Norton Disk Doctor, Norton WinDoctor отслеживает и "ремонтирует на лету" возникающие дисковые и системные проблемы, восстанавливает потеряные данные; System Maintenance содержит утилиты System Information, Wipe Info, Image, Norton File Compare предоставляет полнейшую информацию о системной конфигурации, "подчистую" удаляет дисковые данные, так что их невозможно восстановить ни одной программой, делает резервное копирование критичных данных; Registry Management с помощью утилит Norton Registry Editor и Norton Registry Tracker предоставляет функции управления реестром.

*Speed Disk*

В ходе работы компьютера постепенно происходит фрагментация хранимых на диске файлов. Это существенно сказывается на скорости работы компьютера, особенно на старых и медленных машинах. Время от времени необходимо проводить дефрагментацию раздела или диска. Дефрагментацию выполняет утилита Speed Disk, функции которой аналогичны штатной программе Windows "Дефрагментация диска". Однако возможности программы от Symantec гораздо шире.

Для каждого из установленных на компьютере дисков можно:

* провести оптимизацию размещения файлов (функция Optimization map);
* просмотреть статистику использования диска (функция Analysis);
* задать размещение необходимых файлов в начале, либо конце HDD (функция Drive options);
* задать режим автоматической оптимизации диска (Schedule options).

Дефрагментация может проводиться в фоновом режиме. Но при этом необходимо помнить, что если в процессе дефрагментации будет сделана запись на диск, то весь этот долгий процесс начнется заново. В настройках утилиты можно задать повышенный или пониженный приоритет процесса дефрагментации и уровень использования оперативной памяти. Это позволяет регулировать нагрузку на систему во время фонового режима работы. Настройки программы сведены к минимуму в сравнении с предыдущими версиями утилиты.

*Norton System Doctor*

Norton System Doctor - утилита постоянного мониторинга состояния компьютера. Всего в утилите предусмотрено 25 самых различных функций мониторинга, разбитых на шесть групп: memory (мониторинг параметров оперативной памяти и файла подкачки), disks (мониторинг параметров дисков), system (мониторинг параметров системы), internet/network (мониторинг параметров Интернета и локальной сети), performance (мониторинг различных процессов, выполняемых ОС) и information (информация о других параметрах). Каждый из датчиков можно настроить по внешнему виду, уровню срабатывания датчика, установить действия датчика при превышении уровня срабатывания, настроить режим измерения.

Утилита работает в фоновом режиме. При возникновении ситуации, требующей вмешательства пользователя, она может либо выдать сигнал, либо самостоятельно устранить проблему.

*UnErase Wizard*

UnErase Wizard - утилита восстановления удаленных файлов. Средство восстановления файлов, не попавших в корзину - например, удаленных автоматически во время работы приложений или в сеансе MS-DOS. Утилита может восстановить только те файлы, на место физического размещения которых не было еще произведено записи информации.

*Norton Disk Doctor*

Norton Disk Doctor - утилита проверки диска. Утилита по назначению аналогична стандартной программе Windows ScanDisk, но обладает расширенными, по сравнению со ScanDisk, возможностями.

Особенностью Norton Disk Doctor является возможность самостоятельного определения параметров жесткого диска (число цилиндров, секторов, объем), которые сравниваются с данными, хранящимися в энергонезависимой памяти CMOS. Благодаря этому исключаются ошибки, связанные с неправильным заданием параметров жесткого диска при настройке BIOS. Запуск Norton Disk Doctor возможен в автоматическом режиме - например, при запуске Windows. Утилита может выполнять проверку дисков в фоновом режиме, что особенно актуально при проверке качества поверхности, занимающей продолжительное время.

Найденные ошибки можно автоматически исправлять. Эта функция рассчитана, прежде всего, на начинающих пользователей и производит исправление по заданному программой алгоритму. Опытные пользователи могут воспользоваться ручными настройками.

*Norton WinDoctor*

Norton WinDoctor - средство для проверки операционной системы (системного реестра и системных файлов Windows) и выявления наиболее характерных ошибок, например: несоответствие записей реестра; ярлыков, указывающих на несуществующие файлы и других.

Утилита допускает полное или выборочное сканирование любым из 15 тестов. При выборочном сканировании пользователь может задать дополнительные параметры анализаторов, координирующих действия программы в случае обнаружения неисправности. После сканирования неисправности можно исправить как "оптом" (все сразу) в автоматическом режиме, так и индивидуально. Утилита ведет журнал вносимых изменений, что позволяет в любой момент отменить внесенные изменения.

*System Information*

System Information - утилита, собирающая данные о программной части компьютерной системы: об используемой операционной системе, драйверах, устройствах ввода/вывода, мультимедийных компонентах и других.

Назначение закладок ясно из их названия и в комментариях не нуждается. При необходимости можно распечатать отчет о системе или сохранить его в файле на компьютере.

*Wipe Info*

Wipe Info - служебная утилита, предназначенная для обеспечения режима секретности хранения данных. Она производит не только обычное удаление файлов, но и фактическое уничтожение информации, сохранившейся после удаления файлов и папок путем записи новых данных поверх удаленных файлов. По умолчанию поверх стираемых данных записывается комбинация "00", но пользователь может установить и другую.[5]

2.2 **Acronis Power Utilities**

*Acronis Power Utilities* — это все, что нужно для управления безопасностью системы, жесткими дисками и данными. Acronis Power Utilities — долгожданный сборник утилит, в который вошли четыре популярных системных программы: Acronis Privacy Expert Suite, Acronis Migrate Easy, Acronis Disk Editor, Acronis Recovery Expert.

*Acronis Privacy Expert Suite* предназначен для гарантированного удаления данных, хранящихся на компьютере. Он позволяет удалить следы работы за компьютером, блокировать всплывающие окна, пресекать работу некоторых программ–шпионов и гарантированно удалить информацию с жестких дисков компьютера без возможности восстановления. При удалении данных с диска Acronis Privacy Expert Suite использует наиболее распространенные алгоритмы уничтожения информации. На то место, где ранее находились файлы, в несколько проходов записываются случайные данные. Алгоритм выбора этих данных определяется алгоритмом уничтожения информации, который может быть предварительно выбран из списка. После такой записи на диск восстановление ранее хранившихся файлов на нем становится невозможным.

*Acronis Migrate Easy* — программа перенесет абсолютно все данные, включая операционную систему, программы, настройки, почту, документы, контакты и все остальное на новый жесткий диск за считанные минуты. Понятный пользовательский интерфейс с пошаговыми инструкциями делает сложную работу по миграции данных доступной даже неспециалистам.

**Возможности Acronis Migrate Easy позволяют:**

* Переносить данные в автоматическом или ручном режиме;
* Устанавливать новый диск в качестве загрузочного или дополнительного хранилища данных;
* Устанавливать старый диск в качестве дополнительного хранилища данных;
* Работать с жесткими дисками объемом более 180Гб;
* Управлять разделами на новом диске, включая изменение размера переносимых разделов, создание, копирование, передвижение и удаление (для поддерживаемых разделов);
* Оперировать посекторным переносом данных (для поддерживаемых разделов);
* Для удобства пользователей в Acronis Migrate Easy предусмотрена работа с отложенными операциями и сценариями, когда операция начинает выполняться только после создания сценария. Причем, в ходе выполнения операции миграции данные на старом диске могут быть сохранены либо гарантировано удалены.

Работая как в ручном, так и автоматическом режиме установки Acronis Migrate Easy может либо свести процедуру обновления жесткого диска к нескольким щелчкам мышки, либо предоставит Вам полный контроль над процессом. Вы сможете изменить размер и положение на диске переносимых разделов, создать новые разделы, установить новый жесткий диск как загрузочный и как дополнительный носитель, сохранить или, наоборот, надежно уничтожить данные на старом диске (если этого требуют соображения конфиденциальности).

*Acronis Disk Editor* предназначен для редактирования содержимого секторов жесткого диска и позволяет при наличии достаточной квалификации пользователя производить резервное копирование и восстановление загрузочных секторов и других важных областей данных на жестком диске, поиск и извлечение случайно удаленной или потерянной в результате сбоев информации, восстановление работоспособности компьютера после разрушительного воздействия вирусов и многое другое.

Acronis Disk Editor 6.0 представляет собой профессиональный редактор жестких дисков и предназначен, прежде всего, для опытных пользователей, знакомых со структурой хранения информации на жестких дисках.
Acronis Disk Editor может быть использован в учебных целях: в различных режимах просмотра он предоставляет исключительно наглядное представление структур хранения данных на жестком диске.

*Acronis Recovery Expert* — программа восстановления разделов жесткого диска, удаленных случайно в результате пользовательской ошибки, программного или аппаратного сбоя, воздействия компьютерного вируса или хакерской атаки.

Восстановление удаленных разделов выполняется в автоматическом или ручном режимах, в последнем случае под полным контролем пользователя.[6]

* 1. **System Mechanic**

Компактная и умелая программа System до сентября 2003 г. служила скорее дополнением к офисным грандам типа Norton SystemWorks, чем их прямым конкурентом. Ситуация резко изменилась с выходом четвертой версии программы, когда System Mechanic впервые за много лет полностью переменила обличье и существенно расширила набор своих умений.

Сегодня программа поставляется в двух версиях: стандартная — это и есть System Mechanic с рядом дополнительных функций и Pro.

Остановимся на возможностях главной, базовой программы — она в обеих версиях System Mechanic одинакова. Все сервисы SM разнесены по следующим категориям-разделам:

*Раздел «Clean» (Чистка).*

Здесь вы найдете кнопки удаления «мусорных» файлов, поиска файлов-дубликатов, быстрой очистки следов работы в Интернете (списка закладок, журнала посещения сайтов, сохраненных на диске страниц Интернета для автономного просмотра и так далее). Здесь же находится программа-блокиратор «всплывающих окон» вашего браузера — отличное средство для избавления от сетевой рекламы.

*Раздел «Fix» (Исправить).*

Программа для чистки и исправления системного реестра, поиск «мертвых» ярлыков, очистка папки *Установка и удаление программ* от «мертвых душ»... И здесь же интересная программа для восстановления данных на жестком диске.

*Раздел «Maintain» (Обслуживание).*

Главная программа в этом разделе — PC Maintenance Wizard**,** комплексный уборщик, который позволяет запустить все утилиты, входящие в предыдущие разделы, одним нажатием кнопки. Можно сделать это вручную, а можно — в полностью автоматическом режиме (с помощью программы-планировщика). Utility Bar **-** панель быстрого доступа к программам System Mechanic.

*Раздел «Optimize» (Оптимизация).*

Этот раздел — настоящая выставка новинок, которыми обзавелась последняя версия System Mechanic. В программе появился собственный дефрагментатор жестких дисков (Speed Up Hard Drive).А для тех пользователей, чьи компьютеры оборудованы небольшим объемом оперативной памяти (менее 256 Мб) будет полезен и новый «дефрагментатор памяти».

Программа NetBoosterувеличивает скорость передачи данных по интернет-каналу (за счет тонкой подстройки ряда параметров Windows)... Хотя и не слишком сильно — в лучшем случае выигрыш составит несколько процентов.

Tweak Manager— тонкая подстройка около 100 параметров, спрятанных в реестре Windows. Если что-то сделали не так — всегда можно восстановить значения параметров «по умолчанию» с помощью одноименной кнопки.

Startup Managerпозволяет увидеть и отредактировать список программ, которые запускаются автоматически сразу после «старта» Windows.

*Раздел «Protect» (Защита).*

Невероятно полезная новинка — встроенный «чистильщик» жесткого диска от программ-«паразитов» — рекламных и шпионских модулей, которые тихой сапой проносят на ваш диск некоторые «бесплатные» программы.

Среди других программ этого раздела — средство для безвозвратного удаления важной информации (актуально для бизнесменов), программа для создания «снимков» системы (благодаря им вы можете отследить все параметры, измененные при установке на ваш компьютер новых программ).[3]

**Выводы и предложения**

Защита информации является ключевой задачей в современных условиях взаимодействия глобальных и корпоративных компьютерных сетей. В реальном мире много внимания уделяется физической безопасности, а в мире электронного обмена информацией необходимо заботиться также о средствах защиты данных.

Усложнение методов и средств организации машинной обработки, повсеместное использование глобальной сети Интернет приводит к тому, что информация становится все оболе уязвимой. Этому способствуют такие факторы, как постоянно возрастающие объемы обрабатываемых данных, накопление и хранение данных в ограниченных местах, постоянное расширение круга пользователей, имеющих доступ к ресурсам, программам и данным, недостаточный уровень защиты аппаратных и программных средств компьютеров и коммуникационных систем и т.п.

Учитывая эти факты, защита информации в процессе ее сбора, хранения, обработки и передачи приобретает исключительно важное значение.

**Список использованной литературы**

1. Информатика / Курносов А.П., Кулев С.А., Улезько А.В. и др.; под ред А.П. Курносова. – М.: КолосС, 2005.
2. Компьютерные сети и средства защиты информации: Учебное пособие/ Камалян А.К., Кулев С.А., Назаренко К.Н., Ломакин С.В., Кусмагамбетов С.М.; Под ред. д.э.н., профессора А.К. Камаляна. – Воронеж: ВГАУ, 2003.
3. Леонтьев В. П. Новейшая энциклопедия персонального компьютера 2005. – М.: ОЛМА-ПРЕСС Образование, 2005.
4. Черняков М.В., Петрушин А.С. Основы информационных технологий. Учебник для вузов: - М.: ИКЦ «Академкнига», 2007.
5. http://soft/compulenta/ru
6. http://litek.ru/catalog/acronis/homeRe.html