Оренбургский государственный институт менеджмента

Реферат на тему:

**Обязательный набор программ безопасности на персональном компьютере**

Оренбург – 2004

**Содержание**

Введение

1. Основные понятия компьютерной безопасности

1.1 Защита от компьютерных вирусов

1.2 Защита от несанкционированного доступа

1.3 Защита информации при удаленном доступе

2. Антивирус Касперского

Заключение

Список литературы

**Введение**

Если информация, которая содержится на вашем компьютере, представляет для вас определенную ценность, вы должны позаботиться об ее сохранности. Причин для этого несколько.

* Во-первых, данные могут быть уничтожены в результате заражения системы вирусом.
* Во-вторых, ваша информация может кануть в лету по причине поломки винчестера или поврежденного носителя.
* И в-третьих, информацию могут попросту выкрасть (например, во время вашего отсутствия на рабочем месте).

В данной работе будет рассмотрен обязательный набор программ безопасности на персональном компьютере.

# 1. Основные понятия компьютерной безопасности

Для того чтобы рассматривать в дальнейшем вопросы безопасности, необходимо ввести основные понятия, которыми оперирует теория компьютерной безопасности.

Итак, *угроза* безопасности компьютерной системы - это потенциально возможное происшествие, неважно, преднамеренное или нет, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней. Уязвимость компьютерной системы - это некая ее неудачная характеристика, которая делает возможным возникновение угрозы. Другими словами, именно из-за наличия уязвимостей в системе происходят нежелательные события. Наконец, *атака* на компьютерную систему - это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости. Таким образом, атака - это реализация угрозы. Заметим, что такое толкование атаки (с участием человека, имеющего злой умысел), исключает присутствующий в определении угрозы элемент случайности, но, как показывает опыт, часто бывает невозможно различить преднамеренные и случайные действия, и хорошая система защиты должна адекватно реагировать на любое из них.

Далее, исследователи обычно выделяют три основных вида угроз безопасности - это угрозы раскрытия, целостности и отказа в обслуживании. Угроза *раскрытия* заключается том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда вместо слова "раскрытие" используются термины "кража" или "утечка". Угроза *целостности* включает в себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе целостности - деловые или коммерческие. Угроза *отказа в обслуживании* возникает всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или оно может вызвать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

## 1.1 Защита от компьютерных вирусов

Вряд ли найдется хотя бы один пользователь или администратор сети, который бы ни разу не сталкивался с компьютерными вирусами. 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 появляется 100-150 новых штаммов ежемесячно. Наиболее распространенными методами зашиты 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. Корпорация Intel в 1994 году 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.

## 1.2 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.

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.

Одним из удачных примеров создания комплексного решения для контроля доступа в открытых системах, 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 предмет получения того или иного вида сетевых услуг.

Авторизационный сервер, получая запрос от пользователя, обращается к базе данных и определяет, имеет ли пользователь право на совершение данной операции. Примечательно, что пароли пользователей по сети не передаются, что также повышает степень зашиты 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 также в зашифрованном по алгоритму DES виде. После получения и расшифровки "пропуска" сервер выдачи разрешений проверяет запрос и сравнивает ключи затем дает "добро" 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 Mulovendor Environment), предназначенную для использования в крупных гетерогенных сетях.

## 1.3 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. Компания Datapro свидетельствует, что уже в 1995 году только в США число работников постоянно или временно использующих удаленный доступ к компьютерным сетям, составит 25 миллионов "человек. 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 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, TO) 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, 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 поставило разработчиков радиосистем перед необходимостью защиты информации от "хакеров", вооруженных разнообразными сканирующими устройствами. Были применены разнообразные технические решения. Например, в радиосети компании RAM Mobil Data информационные пакеты передаются через разные каналы и базовые станции, что делает практически невозможным для посторонних собрать всю передаваемую информацию воедино. Активно используются в радио сетях и технологии шифрования данных при помощи алгоритмов DES и RSA.

**2. Антивирус Касперского**

Работая с интернетом, электронной почтой и различными документами, вы должны быть уверены в надежной защите вашей информации. Вам необходимо эффективное программное обеспечение, контролирующее все возможные источники проникновения вирусов на ваш компьютер. Антивирус Касперского® Personal Pro разработан специально для опытных пользователей. Он обеспечивает полномасштабную защиту всех приложений и содержит новые уникальные компоненты и технологии, теперь доступные и для домашних пользователей.

Надежный контроль над всеми вирусоопасными источниками

Антивирус Касперского® Personal Pro постоянно контролирует все источники проникновения вирусов: электронную почту, интернет, дискеты, компакт-диски и т.п. Программа не допустит присутствия вирусов ни в одном из возможных мест, включая системную память, загрузочные сектора, файлы и почтовые базы. Решение также содержит уникальные технологии защиты документов формата MS Office.

Обработка архивированных и сжатых файлов

Вирусы, находящиеся внутри архивированных и упакованных файлов, часто просто "невидимы" для антивируса. Антивирус Касперского Pro проверку архивированных и упакованных файлов более 900 версий, а также лечит файлы в архивах форматов ZIP, CAB, RAR, ARJ. Кроме того, программа позволяет обнаружить вирусную программу даже в файле, подвергавшемся сжатию несколько раз.

Эффективная защита вашего компьютера

Антивирус Касперского® Personal Pro защищает ваш компьютер в режиме реального времени, проверяя все файлы непосредственно в момент их запуска, создания или копирования. Антивирус Касперского® Personal Pro дает возможность проводить полномасштабную проверку всего содержимого локальных и сетевых дисков по требованию пользователя или автоматически по расписанию.

Полномасштабная защита электронной почты

Программа автоматически проверяет все входящие почтовые сообщения на присутствие вирусов до их поступления в почтовый ящик, и при необходимости осуществляет лечение. Исходящие сообщения также подвергаются проверке в режиме реального времени. Кроме того, программа позволяет проверять почтовые базы различных почтовых клиентов, а также осуществлять лечение в почтовых базах MS Outlook и Outlook Express по требованию.

Проактивная защита документов от макровирусов

Антивирус Касперского® Personal Pro обеспечивает постоянный контроль над выполняемыми макросами в документах формата MS Office, пресекая все подозрительные действия. Это дает полную защиту от любых макровирусов, в том числе неизвестных, не оставляя им ни единого шанса нанести вашему компьютеру вред.

Оптимизация производительности.

Совместное использование уникальных технологий iChecker™ и iStreams™, интегрированных в Антивирус® Касперского, позволило повысить производительность программы в три раза при одновременном снижении объема требуемой оперативной памяти в два раза по сравнению с предыдущей версией.

Поддержка мобильных пользователей.

Решение обеспечивает гарантированную доставку обновлений при разрыве или смене соединений. Пр этом та часть обновлений, которая уже была получена пользователем до разрыва соединений, повторно не скачивается. Также предусмотрено продление срока эксплуатации батареи за счет отмены сканирования компьютера по расписанию при низком уровне заряда. Антивирусная проверка в режиме реального времени при этом сохраняется.

Защита от riskware.

Антивирус® Касперского Personal Pro - мощный барьер против потенциально опасных программ, предназначенных для удаленного наблюдения и управления компьютером, но не классифицируемых как вирусы. Это достигается за счет существенного расширения набора баз данных, определяющих программы класса riskware.

Уникальная система перехвата скрипт-вирусов.

Классические антивирусные мониторы не способны защитить от действия скрипт-вирусов в оперативной памяти компьютера. Универсальный перехватчик скрипт-вирусов Script Checker, входящий в состав Антивируса КасперскогоPersonal Pro, полностью решает эту проблему, интегрируясь в систему в качестве фильтра между скриптом и его обработчиком. Это обеспечивает антивирусную проверку всех запускаемых скриптов еще до того, как они будут выполнены

Полная автоматизация вирусной защиты.

Вы иногда забываете проверить сканером все диски? Антивирус КасперскогоPersonal Pro предоставляет пользователям удобные инструменты администрирования, позволяющие создавать гибкое расписание и задавать порядок работы компонентов программы.

**Заключение**

# На этом, пожалуй, можно завершить наш обзор. Остается только повторить, что выборочное применение тех или иных средств, конечно, в целом усилит безопасность вашей информационной системы, но для построения достаточно эффективной комплексной системы защиты вашей сети целесообразней привлечь профессионалов.

Основные выводы о способах использования рассмотренных выше средств, методов и мероприятий защиты, сводится к следующему:

1. Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты.
2. Механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы.
3. Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации.
4. Необходимо осуществлять постоянный контроль функционирования механизма защиты.

**Список литературы**

1. Теория и практика обеспечения информационной безопасности, под редакцией Зегжды П.Д., Изд. "Яхтсмен", 1996. Гайкович В., Першин А..
2. Безопасность электронных банковских систем., Изд. "Единая Европа", 2004.
3. Клименко С., Уразметов В., Internet. Среда обитания информационного общества, Российский Центр Физико-Технической Информатики, 1995.

4. Козлов Д.А., Парандовский А.А., Парандовский А.К. Энциклопедия компьютерных вирусов.- М: Солон-Р, 2002.- 458 с.