Лабораторная работа № 1

Тема работы: Основные термины, определения и мероприятия по защите пользовательских данных.

Цель работы: научиться защищать информацию с использованием следующих методов: резервное копирование данных, антивирусная защита, проверка исправности оборудования.

Теоретическая часть:

В связи с все возрастающей ролью информации в жизни общества вопросы информационной безопасности занимают особое место и требуют к себе все большего внимания. Первичным является понятие информационной безопасности - это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации.

Безопасность данных - такое состояние хранимых, обрабатываемых и принимаемых данных, при которых невозможно их случайное или преднамеренное получение, изменение или уничтожение.

Защита данных - совокупность целенаправленных действий и мероприятий по обеспечению безопасности данных. Таким образом, защита данных есть процесс обеспечения безопасности данных, а безопасность - состояние данных, конечный результат процесса защиты. Защита данных осуществляется с использованием методов (способов) защиты.

Метод (способ) защиты данных - совокупность приемов и операций, реализующих функции защиты данных. Примерами их могут служить, например, методы шифрования и паролирования.

На основе методов защиты создаются средства защиты (например, устройства шифрации/дешифрации, программы анализа пароля, датчики охранной сигнализации и т.д.).

Механизм защиты - совокупность средств защиты, функционирующих совместно для выполнения определенной задачи по защите данных (криптографические протоколы, механизмы защиты операционных систем и т.д.). Система обеспечения безопасности данных (СОБД) - совокупность средств и механизмов защиты данных.

Концептуальная модель безопасности информации представлена на рис. 1.

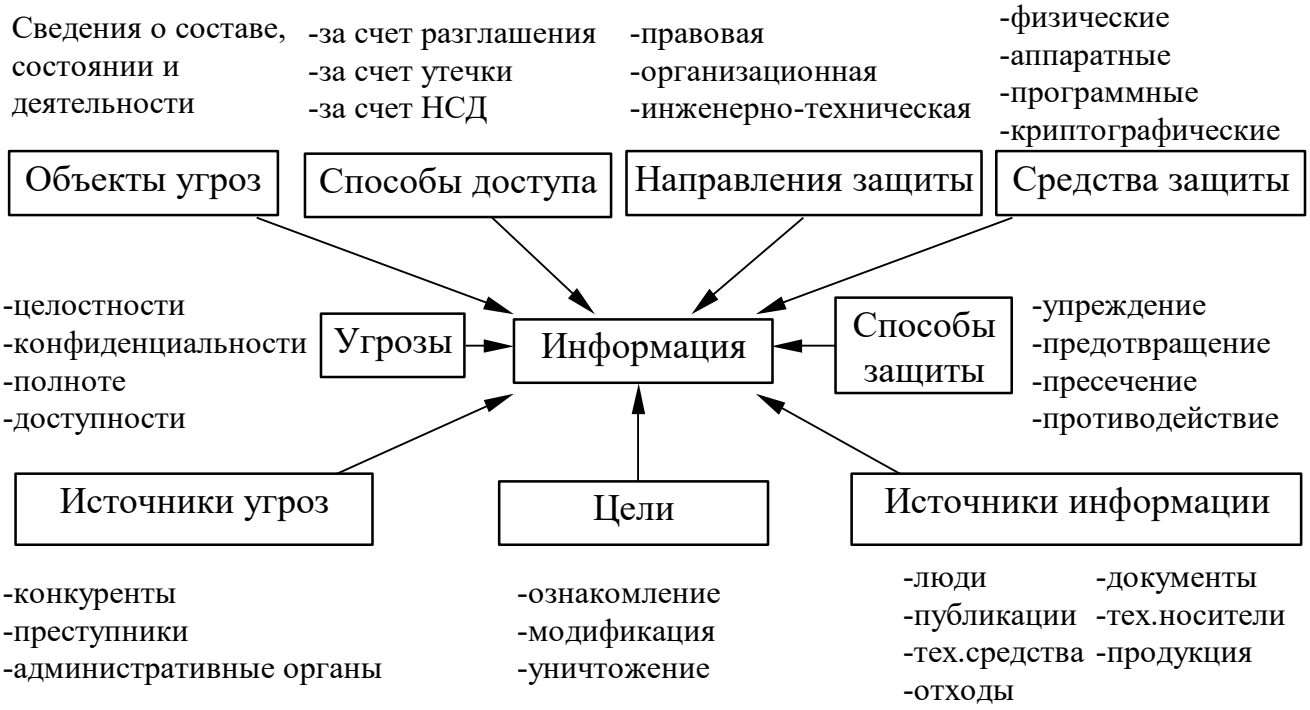

Рис. 1. Концептуальная модель безопасности информации

Основные угрозы безопасности данных

Для того чтобы сформулировать главную цель защиты данных, необходимо определить потенциально существующие возможности нарушения безопасности хранимых, обрабатываемых и передаваемых данных. Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно используют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения информационной безопасности.

Под угрозой безопасности данных будем понимать потенциально существующую возможность случайного или преднамеренного действия или бездействия, в результате которого может быть нарушена безопасность данных. Несанкционированный доступ к данным (НСД) - злоумышленное или случайное действие, нарушающее технологическую схему обработки данных и ведущее к получению, модификации или уничтожению данных. НСД может быть пассивным (чтение, копирование) и активным (модификация, уничтожение).

Классификация угроз безопасности данных приведена на рис. 2.

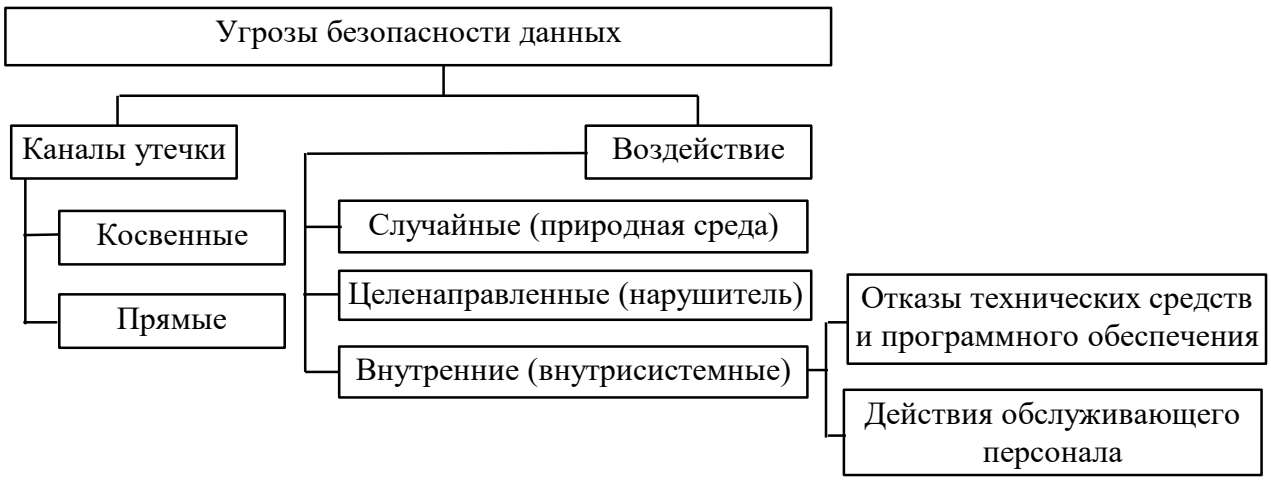

Рис. 2. Классификация угроз безопасности данных

Воздействия, в результате которых может быть нарушена безопасность данных, включают в себя:

- случайные воздействия природной среды (ураган, пожар и т.п.);
- целенаправленные воздействия нарушителя (шпионаж, разрушение компонентов информационной системы, использование прямых каналов утечки данных);
- внутренние возмущающие факторы (отказы аппаратуры, ошибки в математическом и программном обеспечении, недостаточная подготовка персонала и т.д.).

Под каналом утечки данных будем понимать потенциальную возможность нарушителю получить доступ к НСД, которая обусловлена архитектурой, технологической схемой функционирования информационной системы, а также существующей организацией работы с данными. Все каналы утечки данных можно разделить на косвенные и прямые.

Косвенными называются такие каналы утечки, использование которых для НСД не требует непосредственного доступа к техническим устройствам информационной системы. Они возникают, например, вследствие недостаточной изоляции помещений, просчетов в организации работы с данными и предоставляют нарушителю возможность применения подслушивающих устройств, дистанционного фотографирования, перехвата электромагнитных излучений, хищения носителей данных и отходов и т.п.).

Прямые каналы утечки данных требуют непосредственного доступа к техническим средствам информационной системы и данным. Наличие прямых каналов утечки обусловлено недостатками технических и программных средств защиты, ОС, СУБД, математического и программного обеспечения. Прямые каналы утечки данных позволяют нарушителю подключиться к аппаратуре информационной системы, получить доступ к данным и выполнить действия по анализу, модификации и уничтожению данных.

С учетом физической природы путей переноса информации каналы утечки данных можно классифицировать на следующие группы:

- визуально-оптические – источником информации здесь служит, как правило, непосредственное или удаленное наблюдение (в том числе и телевизионное);
- акустические - источником информации здесь служат речь и шумы, средой распространения звука являются воздух, земля, вода, строительные конструкции (кирпич, железобетон, металлическая арматура и др.);
- электромагнитные (включая магнитные и электрические) – источником информации здесь служат различные провода и кабели связи, создающие вокруг себя магнитное и электрическое поле, информацию с которых можно перехватить путем наводок на другие провода и элементы аппаратуры в ближней зоне их расположения;
- материально-вещественные (бумага, фото, магнитные носители и т.д.).

Любая информационная система состоит из источника информации, передатчика, канала (среды) передачи информации, приемника и получателя сведений. Передатчик, канал передачи информации и приемник представляют собой возможный канал утечки информации к нарушителю.

Следует отметить, что технические средства и системы могут не только непосредственно излучать в пространство сигналы, содержащие обрабатываемую информацию, но и улавливать за счет своих магнитофонных или антенных свойств излучения, преобразовывать их в электрические сигналы и передавать по своим линиям связи, как правило, бесконтрольно, что еще в большей степени повышает опасность утечки информации. Отдельные технические средства имеют в своем составе помимо подобных «микрофонов» и «антенн» высокочастотные или импульсные генераторы, излучения которых мо-

гут быть промодулированными различными сигналами, содержащими конфиденциальную информацию.

Рассмотрим основные способы НСД к конфиденциальной информации через технические средства информационных систем.

Незаконное подключение. Самым простым способом незаконного подключения является контактное подключение, например параллельное подключение телефонного аппарата. Но контактное подключение такого типа легко обнаруживается за счет существенного падения напряжения, приводящего с ухудшению слышимости в основном телефоне за счет подключения параллельного. Более совершенным является подключение к линии связи с помощью специальных согласующих устройств типа согласующих трансформаторов или интерфейсных плат ЭВМ.

Бесконтактное подключение к линии связи осуществляется двумя путями: за счет электромагнитных наводок на параллельно проложенные провода или с помощью сосредоточенной индуктивности, охватывающей контролируемую линию. В обоих случаях подслушивание реализуется за счет электромагнитной индукции.

Контактное и бесконтактное подключение возможно и к линиям волоконно-оптической связи. Для контактного подключения, в частности, удаляют защитные слои кабеля, стравливают светоотражающую оболочку и изгибают оптический кабель на необходимый угол. При таком подключении обнаружить утечку информации за счет ослабления мощности излучения бывает очень трудно, так как при существующих приемных устройствах НСД достаточно отобрать всего 0.001% передаваемой мощности, чтобы подслушать переговоры.

Высокочастотное навязывание. Это способ, при котором в телефонную линию в сторону прослушиваемого телефона подаются от специального генератора высокочастотные колебания. Эти колебания взаимодействуют с речевыми сигналами при разговоре и выполняют роль модулятора. Излучение модулированного сигнала в свободное пространство обеспечивается телефонным шнуром. Высокочастотное навязывание может использоваться и на громкоговорители, и на другие элементы, обладающие микрофонным эффектом.

Перехват электромагнитных излучений. Это получение информации за счет приема сигналов электромагнитной энергии пассивными средствами, расположенными, как правило, на достаточно безопасном расстоянии от источника информации. Нарушители осуществляют перехват радиостанций и систем связи, радиолокационных и радионавигационных систем, систем телеуправления, сигналов компьютера, возникающих при выдаче информации на экран монитора и т.д. Перехват электромагнитных излучений базируется на широком использовании самых разнообразных радиоприемных средств, средств анализа и регистрации информации и других.

Перехват информации обладает рядом особенностей по сравнению с другими способами добывания информации:

- информация добывается без непосредственного контакта с источником;
- реализуется скрытно и очень трудно обнаруживается;
- дальность перехвата ограничивается только особенностью распространения радиоволн соответствующих диапазонов.

Таким образом, можно выделить уязвимые места информационных систем с точки зрения информационной безопасности, которые потенциально предоставляют нарушителю возможность НСД (см. рис. 3).

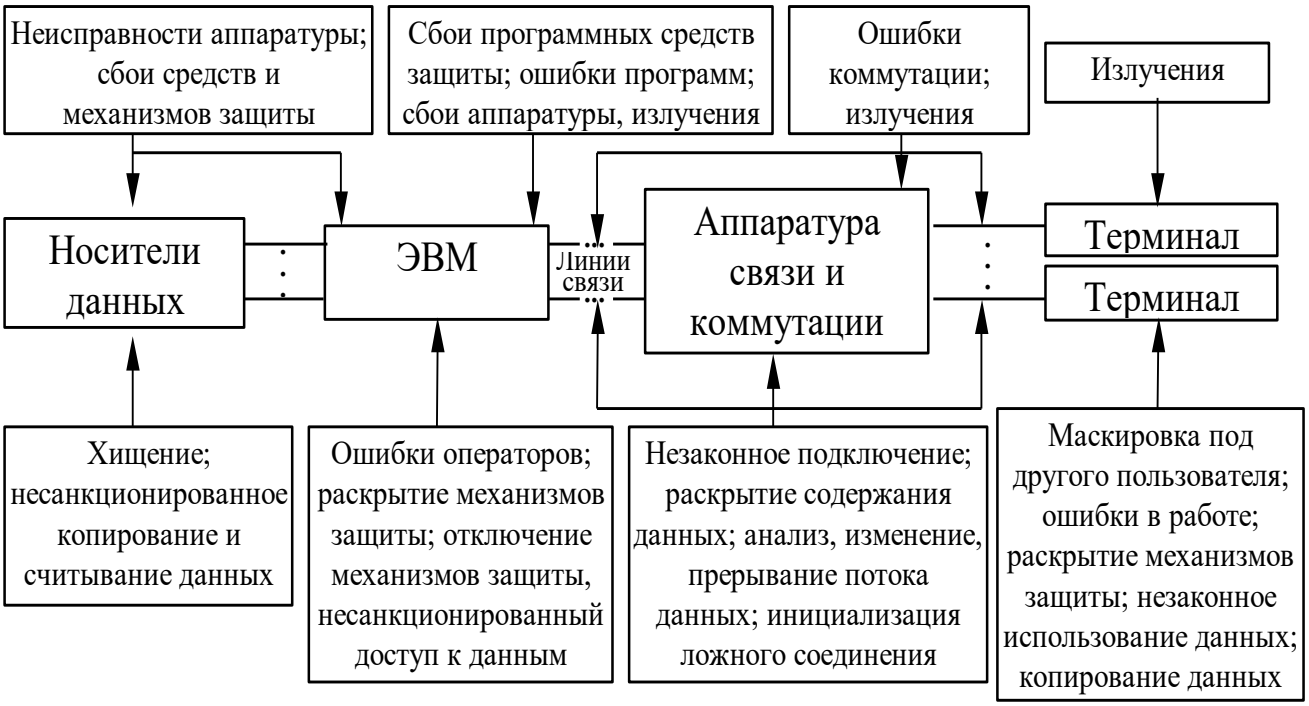

Рис. 3. Возможные уязвимые места информационной системы

Основные методы и средства защиты данных

На первом этапе развития концепций обеспечения безопасности данных преимущество отдавалось программным средствам защиты. Когда практика показала, что для обеспечения безопасности данных этого недостаточно, интенсивное развитие получили всевозможные устройства и системы. Постепенно, по мере формирования системного подхода к проблеме обеспечения безопасности данных, возникла необходимость комплексного применения методов защиты и созданных на их основе средств и механизмов защиты. Обычно на предприятиях в зависимости от объема хранимых, передаваемых и обрабатываемых конфиденциальных данных за информационную безопасность отвечают отдельные специалисты или целые отделы.

Рассмотрим кратко основные методы защиты данных. Классификация методов и средств защиты данных представлена на рис. 4.

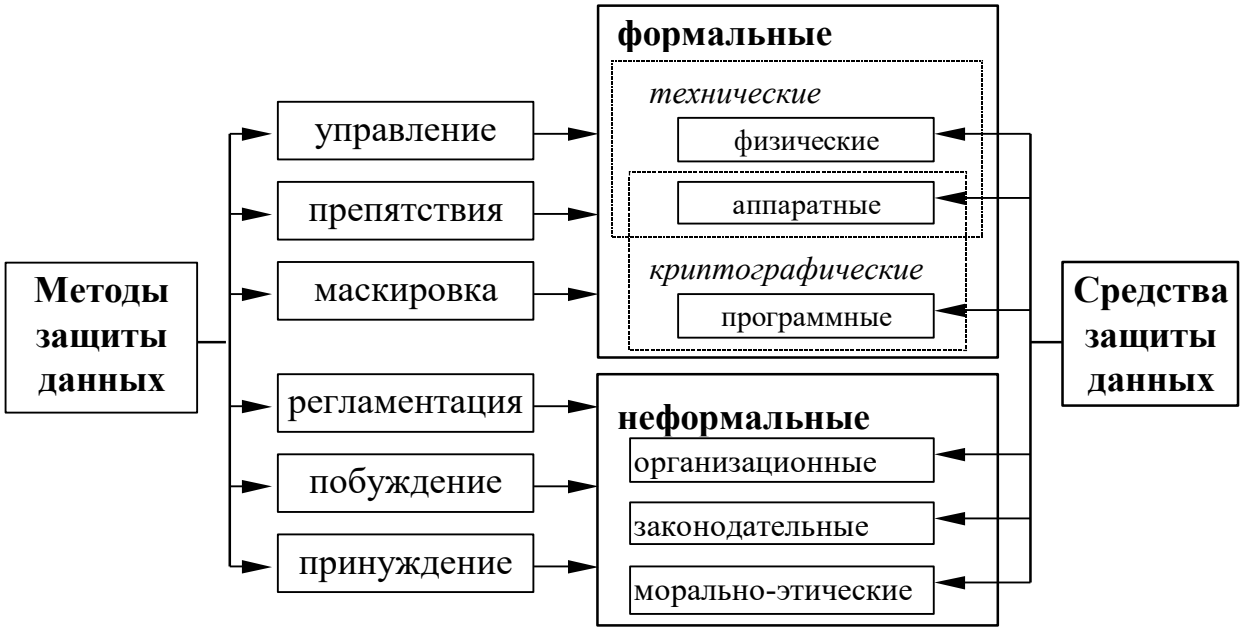

Рис. 4. Классификация методов и средств защиты данных

Управление представляет собой регулирование использования всех ресурсов системы в рамках установленного технологического цикла обработки и передачи данных, где в качестве ресурсов рассматриваются технические средства, ОС, программы, БД, элементы данных и т.п.

Препятствия физически преграждают нарушителю путь к защищаемым данным.

Маскировка представляет собой метод защиты данных путем их криптографического закрытия.

Регламентация как метод защиты заключается в разработке и реализации в процессе функционирования информационной системы комплексов мероприятий, создающих такие условия технологического цикла обработки данных, при которых минимизируется риск НСД к данным. Регламентация охватывает как структурное построение информационной системы, так и технологию обработки данных, организацию работы пользователей и персонала.

Побуждение состоит в создании такой обстановки и условий, при которых правила обращения с защищенными данными регулируются моральными и нравственными нормами.

Принуждение включает угрозу материальной, административной и уголовной ответственности за нарушение правил обращения с защищенными данными.

На основе перечисленных методов создаются средства защиты данных. Все средства защиты можно разделить на формальные и неформальные.

Формальные средства защиты

Формальными называются такие средства защиты, которые выполняют свои функции по заранее установленным процедурам без вмешательства человека. Они подразделяются на технические и программные средства.

К техническим средствам защиты относятся все устройства, которые предназначены для защиты данных. В свою очередь, технические средства защиты можно разделить на физические и аппаратные.

Физические средства защиты создают препятствия для нарушителей на путях к защищаемым данным, например, на территорию, на которой располагаются объекты информационной системы, в помещение с аппаратурой и носителями данных и т.д. Физические средства защиты не входят в состав аппаратуры информационной системы и вы-

полняют следующие основные функции: охрана территории и зданий, охрана внутренних помещений, охрана оборудования и наблюдение за ним, контроль доступа в защищаемые зоны, нейтрализация излучений и наводок, создание препятствий визуальному наблюдению и подслушиванию, противопожарная защита, блокировка действий нарушителя и т.п.

Под аппаратными средствами защиты понимаются специальные средства, непосредственно входящие в состав технического обеспечения информационной системы и выполняющие функции защиты как самостоятельно, так и в комплексе с другими средствами. Аппаратные средства защиты данных можно условно разбить на группы согласно типам аппаратуры, в которых они используются: средства защиты процессора, памяти, терминалов, устройств ввода-вывода, каналов связи и т.д.

Программными называются средства защиты данных, функционирующие в составе программного обеспечения информационной системы. Они выполняют функции защиты данных самостоятельно или в комплексе с другими средствами защиты. Отдельную группу формальных средств составляют криптографические средства, которые реализуются в виде программных, аппаратных и программно-аппаратных средств защиты.

Классификация программных средств защиты по функциональному назначению приведена на рис. 5.

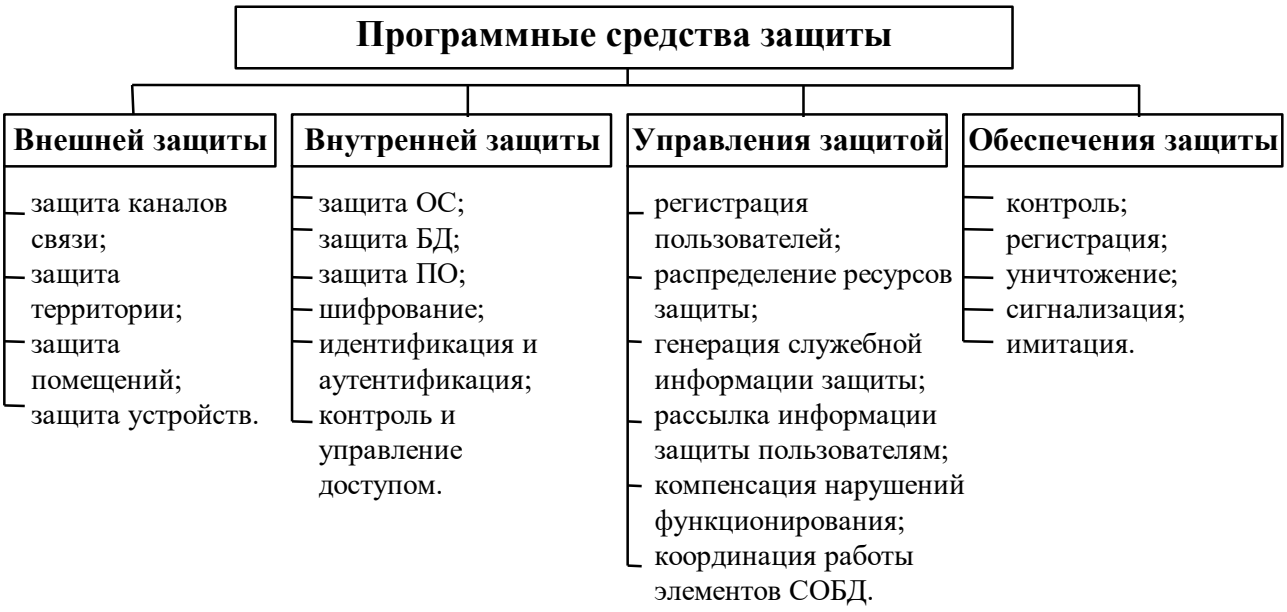

Рис. 5. Классификация программных средств защиты

Программные средства внешней защиты включают программные средств обеспечения функционирования физических средств, защиты территории, помещений, отдельных каналов связи и устройств информационной системы. В настоящее время выпускается множество систем охранной сигнализации, содержащих микропроцессоры и ЭВМ. Программные средства используются также в устройствах опознания личности по различным характеристикам, таким как голос, отпечатки пальцев и т.д. Основным методом защиты данных, передаваемых по каналам связи, является криптографическое закрытие данных, которое реализуется программными, аппаратными и программно-аппаратными средствами.

Программные средства внутренней защиты охватывают совокупность средств и механизмов защиты данных, находящихся в аппаратуре информационных систем. Их

основным назначением является регулирование и контроль использования данных и ресурсов системы в строгом соответствии с установленными правами доступа.

Типичная схема функционирования этих программных средств включает следующие основные этапы:

- установление подлинности пользователя, обращающегося к ресурсам системы;
- проверка соответствия характера запроса предоставленным полномочиям данного пользователя;
- принятие решения в соответствии с результатом проверки полномочий.

Регулирование использования технических средств обычно осуществляется по таким параметрам как время доступа и запрашиваемое действие при доступе. Защита программного обеспечения осуществляется такими методами, как, например, контрольное суммирование и шифрование.

Программные средства управления защитой выполняют три основных класса задач:

- задачи управления пользователями (регистрация пользователей, генерация служебной информации для пользователей, рассылка служебной информации пользователям);
- задачи управления СОБД (распределение ресурсов защиты, координация работы элементов и подсистем СОБД);
- задачи принятия решений в нештатных ситуациях (система поддержки принятия решения администратором СОБД, выработка управляющих воздействий для компенсации нарушения функционирования СОБД).

Программные средства обеспечения защиты включают средства, выполняющие функции контроля, регистрации, уничтожения, сигнализации и имитации. Средства контроля осуществляют тестирование элементов СОБД, а также постоянный сбор информации о функционировании элементов СОБД. Эта информация служит исходными данными для средств поддержки принятия решения и выработке управляющих воздействий. Средства регистрации обеспечивают сбор, хранение, обработку и выдачу данных о состоянии СОБД. Средства уничтожения предназначены для уничтожения остаточных данных и могут предусматривать аварийное уничтожение данных в случае прямой угрозы НСД, которая не может быть блокирована системой. Средства сигнализации предназначены для предупреждения пользователей при их обращении к защищенным данным и для предупреждения администратора СОБД при обнаружении факта НСД к данным, искажения программных средств защиты, выходе или выводе из строя аппаратных средств защиты и т.п. Средства имитации имитируют работу с нарушителями при обнаружении попытки НСД к защищаемым данным. Имитация позволяет увеличить время на определение места и характера НСД, что особенно важно в территориально распределенных информационных системах, и «увести» нарушителя в сторону от защищаемых данных.

Неформальные средства защиты

Неформальными называются такие средства защиты, которые реализуются в результате деятельности людей, либо регламентируют эту деятельность. Неформальные средства включают организационные, законодательные и морально-этические меры и средства.

Под организационными средствами защиты понимаются организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации информационной системы для обеспечения безопасности данных.

Организационные средства защиты охватывают все структурные элементы информационной системы на всех этапах ее жизненного цикла.

Можно выделить следующие принципы организации работ, которые способствуют обеспечению безопасности данных:

- минимизация данных, доступных персоналу (этот принцип означает, что каждый сотрудник должен знать только те детали процесса обеспечения безопасности данных, которые необходимы ему для выполнения своих обязанностей);
- минимизация связей персонала (организация технологического цикла сбора, обработки и передачи данных, по мере возможности, должна исключать или минимизировать контакты обслуживающего персонала);
- разделение полномочий (в системах с высокими требованиями по обеспечению безопасности данных ответственные процедуры выполняются, как правило, после подтверждения их необходимости двумя сотрудниками);
- минимизация доступных данных требует ограничения количеств данных, которые могут быть доступны персоналу и пользователям;
- дублирование контроля (контроль важнейших операций нельзя поручать одному сотруднику).

Особенности организации обеспечения безопасности данных отражаются в эксплуатационной документации и функциональных обязанностей персонала, которые разрабатываются с учетом целей и задач, стоящих перед информационной системой, и требований по защите данных в ней.

Законодательные меры позволяют сдерживать потенциальных преступников, причем под законодательными мерами понимаются законодательные акты, которыми регламентируются правила использования данных ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

К морально-этическим нормам защиты относятся всевозможные нормы, которые традиционно сложились или складываются по мере развития информатизации общества. Такие нормы не являются обязательными, однако их несоблюдение ведет, как правило, к потере авторитета, престижа человека, группы лиц или целой организации. Морально-этические нормы могут быть неписанными (например, общепринятые нормы честности) и оформленными в качестве свода правил и предписаний (кодексов).

Необходимые мероприятия по защите информации для пользователя

Таким образом, очевидно, что в современном мире информация имеет определенную, а часто и очень высокую ценность. Как и любую ценность ее нужно защищать. С точки зрения конечного пользователя можно выделить следующие основные направления и соответствующие мероприятия по обеспечению информационной безопасности (см. рис. 6).

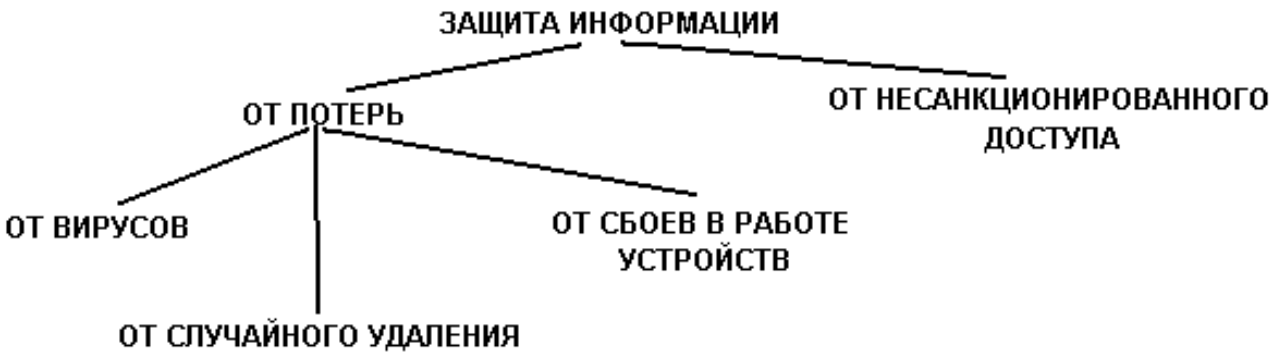

Рис. 6. Основные направления по обеспечению информационной безопасности

Под мероприятиями по защите информации от несанкционированного доступа имеются в виду те, что связаны с ее секретностью. К их числу относятся самые разнообразные способы защиты, начиная от простейших, но очень эффективных защит паролем до использования сложнейших технических систем.

Как показывает практика, вероятность взлома современных средств защиты информации гораздо ниже, чем вероятность доступа к секретной информации в их обход. Поэтому особое внимание следует обращать не столько на системы защиты, сколько на различные организационные вопросы - подбор персонала, допускаемых к секретной информации, тщательное соблюдение правил работы с ней и т.д. При этом следует учитывать, что никакая система защиты информации не обеспечивает 100%-ю надежность. Достаточно надежной считается такая система защиты информации, которая обеспечивает ее защиту в течение весьма продолжительного периода времени. Иными словами, система защита информации должна быть такой, чтобы на ее взлом потребовалось больше времени, чем время, которое эта информация должна оставаться секретной.

Под мероприятиями по защите информации от потерь имеются в виду те, которые позволяют восстановить необходимую информацию при случайном или намеренном ее удалении или изменении. Один из наиболее действенных и эффективных методов защиты информации от потерь является резервное копирование данных.

Существует ряд программных средств резервного копирования. Но, во-первых, это затруднительно делать регулярно для очень больших объемов информации, а во-вторых, та информация, которая появилась или изменилась после копирования, будет все-таки потеряна. Поэтому процесс резервного копирования данных часто автоматизируют и выполняют в тот период времени, когда информационная система наименее занята (например, в ночное время).

Действительно, если имеется резервная копия какого-то файла, например на дискете, магнитной ленте или магнитооптическом диске, то в случае порчи или потери основного файла его можно будет легко заменить. Очевидно, что резервное копирование требует дополнительных устройств хранения информации, а значит определенных (а часто - весьма больших) финансовых затрат. Поэтому резервное копирование, как правило, применяют только для наиболее ценной информации, потеря которой приведет к серьезным последствиям.

Если вся информация, с которой ведется работа, очень ценная, то альтернативой может быть использование отказоустойчивых устройств, обычно путем их дублирования (жесткие диски, блоки питания, оперативная память и т.д.).

Кроме финансовых затрат на защиту информации от потерь следует учитывать и человеческий фактор. Бывает, пользователь экономит несколько минут на создание резервной копии важного файла, а в результате теряет часы и дни работы на восстановление потерянной информации.

К мероприятиям по защите информации от потерь, кроме резервного копирования данных, относятся мероприятия по защите:

- от компьютерных вирусов;
- от случайного удаления;
- от сбоев в работе устройств.

Компьютерный вирус – небольшая программа, которая без ведома пользователя, приписывая себя к другим программам, проникает на диск через приносимые на компь-

ютер диски или по компьютерной сети, распространяется на нем и производит какие-то вредные действия (например, портит данные, нарушает нормальную работу программ и т.п.).

Иногда компьютерный вирус приписывает себя не к файлам, а к загрузочному сектору (имеющемуся на каждом диске, в котором содержится служебная информация о структуре файлов и каталогов на нем).

Написание компьютерного вируса - не очень сложная работа, доступная профессиональным программистам среднего уровня. Люди, которые занимаются написанием компьютерных вирусов (хакеры) делают это потому, что либо не могут найти более достойного применения своим знаниям, либо из желания (а иногда и политики) нанести вред какой-либо фирме или организации, либо просто из баловства.

Бывают относительно «безобидные» компьютерные вирусы, которые приводят к тому, что в ходе работы зараженной программы (т.е. программы, к которой приписался вирус) на экран выводятся какие-то сообщения, ее работа прерывается паузами и т.п. Однако в любом случае такие вирусы не позволяют продолжить нормальную работу пользователя с компьютером.

Существуют и очень опасные компьютерные вирусы, которые способны безвозвратно уничтожать информацию на диске. Заражение компьютерным вирусом может привести к очень серьезным последствиям. Например, в 1989 году вирус, написанный американским студентом Моррисом, вывел из строя тысячи компьютеров, часть из которых принадлежала министерству обороны США.

Наибольшая опасность компьютерных вирусов заключается в том, что они распространяются без ведома пользователя. Для борьбы с ними нужно четко представлять, когда может произойти заражение вирусом. Это может случиться, если на компьютере хотя бы раз была выполнена зараженная программа, например, принесенная с другого компьютера. Компьютерные вирусы не могут совершать сверхъестественных действий, поэтому не стоит преувеличивать их возможностей. Известны комичные случаи «вирусофобии», когда из-за боязни заражения компьютерными вирусами пользователи при хранении дискет прокладывали между ними листы бумаги «чтобы вирусы не перескочили с одной дискеты на другую».

Мероприятия по защите информации от компьютерных вирусов

1. Предотвращение доступа к компьютеру посторонних лиц. Бывает, что заражение вирусом происходит, когда на компьютер пустили поработать какого-то человека, который принес свои дискеты со своими программами, оказавшимися зараженными.
2. Использование только надежного лицензионного программного обеспечения. Не следует без разбора копировать на свой компьютер понравившиеся или нелицензионные программы. В особенности это касается компьютерных игр, именно с ними компьютерные вирусы и передаются чаще всего.
3. Отслеживание любых изменений в работе компьютера для возможно более быстрого обнаружения компьютерного вируса. К таким изменениям относятся: нарушения работы программ, которые раньше работали нормально, появление каких-либо посторонних сообщений на экране и т.п. Чем раньше удастся обнаружить компьютерный вирус, тем больше шансов, что он не успел сильно распространиться на диске и заразить много программ, а значит, последствия заражения вирусом будут минимальными. Важно иметь в виду, что некоторые компьютерные вирусы характеризуются «инкубационным периодом», т.е. после проникновения на диск в течение определенного времени они только распространяются на нем, не производя никаких вредных дей-

ствий, а проявляют себя только потом, когда зараженным оказывается не один десяток файлов.

4. Размещение наиболее ценной информации на защищенных от записи дисках. Если запись на диск запрещена, то, очевидно, компьютерный вирус не может приписать себя к файлам на нем, и заражение защищенного диска будет невозможным.
5. Использование антивирусных программ для постоянной и периодической проверки компьютера. Важно помнить, что антивирусные программы быстро устаревают, так как новые компьютерные вирусы появляются быстрее их, также как яд всегда появляется раньше противоядия.

Случайное удаление файла - ошибка, свойственная далеко не только начинающим пользователям, способным совершить ее по незнанию. Бывает, что опытные пользователи, которые довели свои действия при работе с компьютером до автоматизма, могут удалить файл, например случайно задев другую клавишу, и не заметить этого.

Мероприятия по защите информации от случайного удаления

1. Аккуратность и внимательность при работе.
2. Размещение наиболее ценной информации на защищенных от записи дисках. Понятно, что с защищенных дисков даже специально удалить информацию невозможно.
3. Своевременное удаление ненужных файлов и рациональное размещение файлов по каталогам. С течением времени на диске появляется все больше и больше файлов, таким образом, диск забивается. Постепенно пользователь забывает, что в каком файле находится, и в каких каталогах (папках) содержится нужная информация. В результате, когда возникнет необходимость освободить место на диске, могут быть удалены файлы, содержащие ценную информацию. Поэтому необходимо периодически приводить диски в порядок.
4. Быстрое восстановление ошибочно удаленных файлов при помощи специальных программ. Дело в том, что при удалении файла информация с диска не стирается, просто на его место разрешается запись другой информации. Если пользователь быстро обнаружил свою ошибку, у него остаются шансы восстановить случайно удаленную информацию, причем, если после удаления он не копировал, не перемещал другие файлы, не запускал другие программы или не перезапускал компьютер, эти шансы будут выше. Для восстановления ошибочно удаленных файлов существуют специальные программы. В операционной системе Windows копии удаленных файлов автоматически помещаются в специальную папку (каталог) – «Корзина», откуда в случае необходимости их можно восстановить.

Мероприятия по защите информации от сбоев в работе устройств

1. Периодическая проверка исправности оборудования (в частности поверхности жесткого диска) при помощи специальных программ. Такие программы позволяют обнаружить дефектные участки на поверхности диска и соответствующим образом их пометить, чтобы при записи информации эти участки были обойдены.
2. Периодическая оптимизация (дефрагментация) диска для рационального размещения файлов на нем, ускорения работы и уменьшения его износа. При записи на диск части файла могут оказаться записанными в разных, удаленных друг от друга секторах диска, что связано с тем, что информация может быть записана только в свободные сектора. Для того чтобы объединить эти фрагменты файлов и тем самым уменьшить износ диска и затраты времени на считывание информации, следует периодически про-

изводить оптимизацию (дефрагментацию) диска при помощи соответствующих программ.

3. Наличие загрузочных (системных) дискет, с которых можно запустить компьютер (т.е. загрузить операционную систему) в случае сбоев с основным системным диском. Для того чтобы компьютер заработал, необходимо загрузить в оперативную память операционную систему, основная часть которой находится в виде файлов на одном из дисков, называемом системным. Если с системным диском или с какой-то его частью, где находятся файлы операционной системы, что-то произошло, запустить компьютер с него не удастся, поэтому и нужно иметь резервные системные дискеты или диск с соответствующими файлами.

В случае обнаружения заражения вирусами также следует перезапустить компьютер с резервной системной дискеты, поскольку операционная система на основном системном диске также может оказаться зараженной и, следовательно, при каждом включении компьютера и каждой загрузке с основного системного диска операционной системы в оперативной памяти будут находиться вирусы. В такой ситуации борьба с вирусами, например с помощью антивирусных программ, будет бессмысленной, поскольку, скорее всего, любая запускаемая программа будет заражена. Кстати, антивирусные программы тоже следует собирать и хранить на отдельной дискете, чтобы избежать их заражения.

Лабораторная работа

Тема работы: защита данных.

Цель работы: научиться защищать информацию с использованием следующих методов: резервное копирование данных, антивирусная защита, проверка исправности оборудования.

Подготовка к работе:

1. Изучите теоретические основы защиты информации, рассмотренные в лекционном курсе, методических указаниях или других источниках информации.
2. Ответьте на контрольные вопросы к лабораторной работе.
3. Подготовьте отчет к оформлению хода выполнения работы.

Порядок выполнения работы:

1. Запустите программу резервного копирования, например, «Архивация данных», WinRar, Хранитель V и т.п.
2. Выберите необходимые документы для резервного копирования (см. рис. 7).

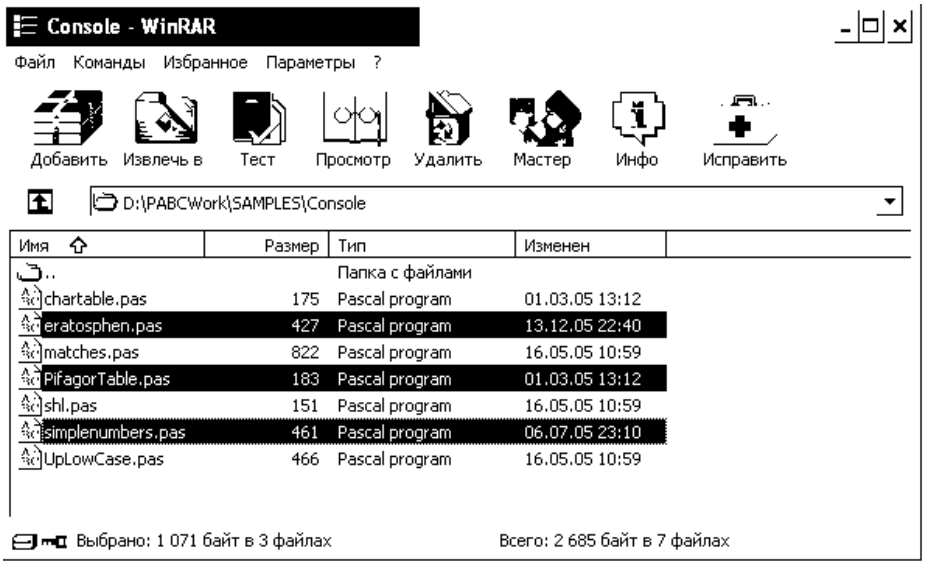

Рис. 7. Основное окно программы WinRar

3. Нажмите кнопку «Добавить» (см. рис. 7).
4. На вкладке «Общие» укажите имя архивного файла (см. рис. 8).

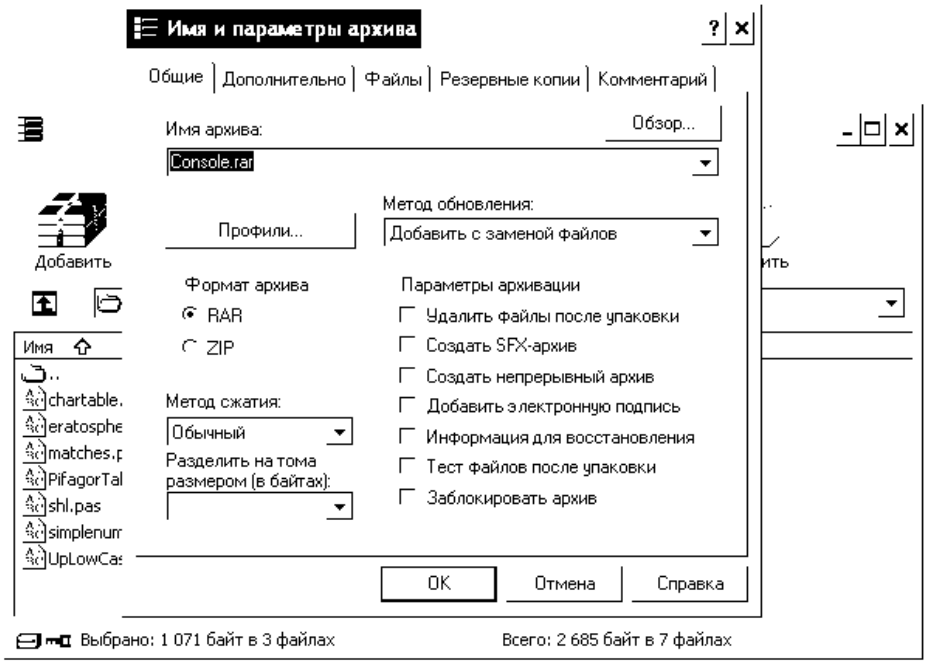

Рис. 8. Вкладка «Общие» окна «Имя и параметры архива» программы WinRar

5. Выберите необходимый метод сжатия (см. рис. 8).
6. На вкладке «Дополнительно» нажмите кнопку «Установить пароль» и в открывшемся окне укажите пароль для выбранных файлов, добавляемых в указанный архив (см. рис. 9).
7. Ознакомьтесь с остальными параметрами, расположенными на вкладках «Общие», «Дополнительно», «Резервные копии», «Комментарии» окна «Имя и параметры архива» программы WinRar. Задайте необходимые параметры.
8. Нажмите кнопку «OK», после чего в заданный архив будут добавлены выбранные файлы (см. рис. 7).
9. Убедитесь, что для просмотра содержимого добавленных файлов архива, необходимо ввести пароль.

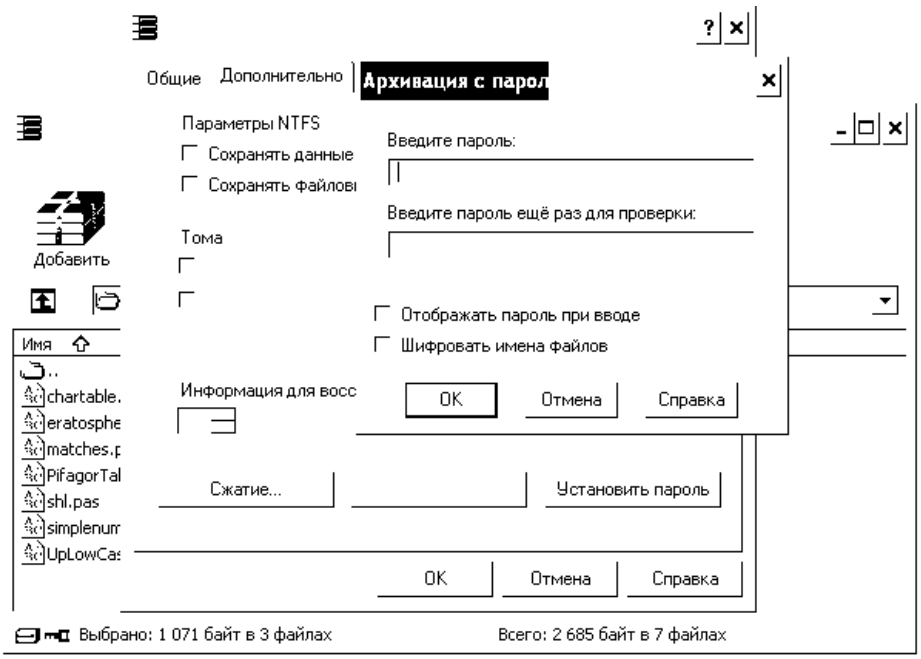

Рис. 9. Окно «Архивация с паролем» программы WinRar

Для того чтобы автоматизировать процесс резервного копирования данных, необходимо настроить запуск программы архивации в определенное время, например на два часа ночи. При этом удобно все документы, требующие резервного копирования располагать на одном диске в одной папке, например «D:\Документы».

10.Запустите программу «Мастер планирования заданий» (см. рис. 10).

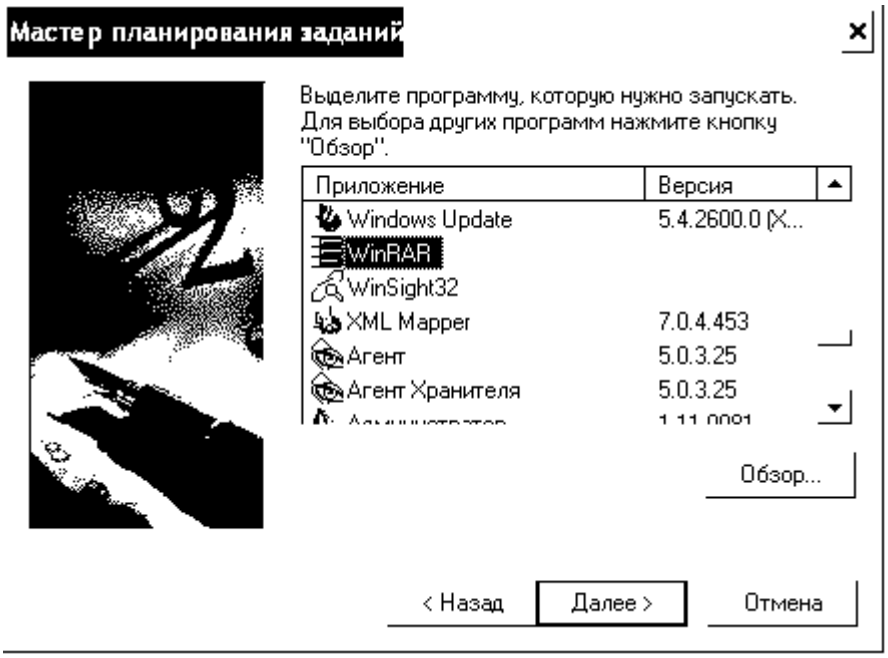

Рис. 10. Окно «Выбор программы» приложения «Мастер планирования заданий»

Для того чтобы настроить запуск любой программы в назначенное время, необходимо нажать кнопку «Пуск», выбрать пункт меню «Программы» | «Стандартные» | «Служебные» | «Назначенные задания» и в открывшемся окне запустить «Добавить задание».

11.Выберите программу «WinRar» (см. рис. 10)

12.Укажите имя создаваемого задания и периодичность его выполнения (см. рис. 11).

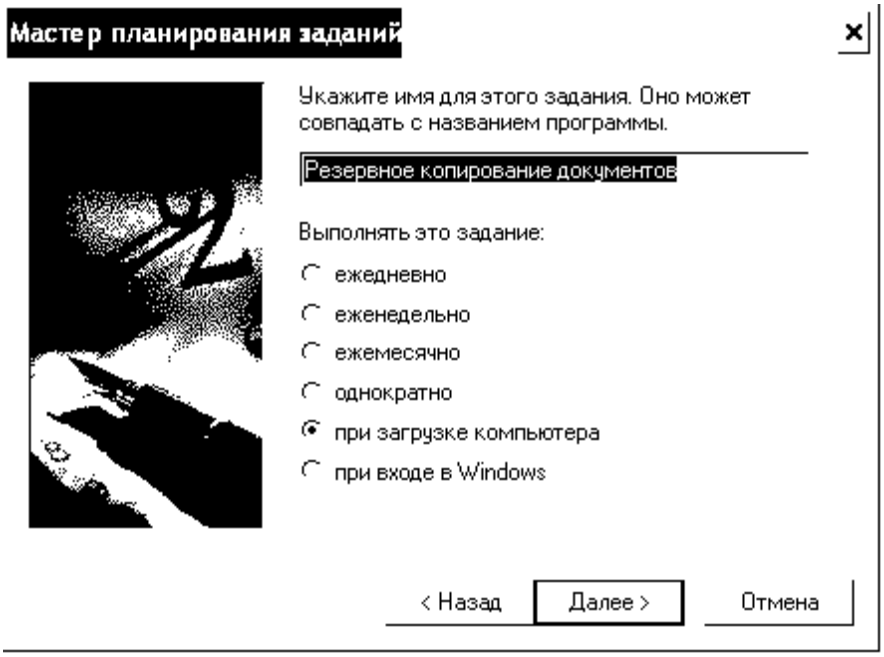

Рис. 11. Окно «Имя и время выполнения задания» приложения «Мастер планирования заданий»

Периодичность задается в зависимости от ценности архивируемых данных и частоте их изменения. Если компьютер не выключается в ночное время, то можно выбрать период «ежедневно» и впоследствии указать ночное или обеденное время (т.е. время, когда с компьютером никто не работает). Если выбрать период «при загрузке компьютера», то данные будут архивироваться при каждом включении компьютера. Таким образом, в случае отказа оборудования в архиве будут храниться данные за предыдущий рабочий день.

13. Укажите имя пользователя (от имени которого будет выполняться задание) и его пароль (см. рис. 12).

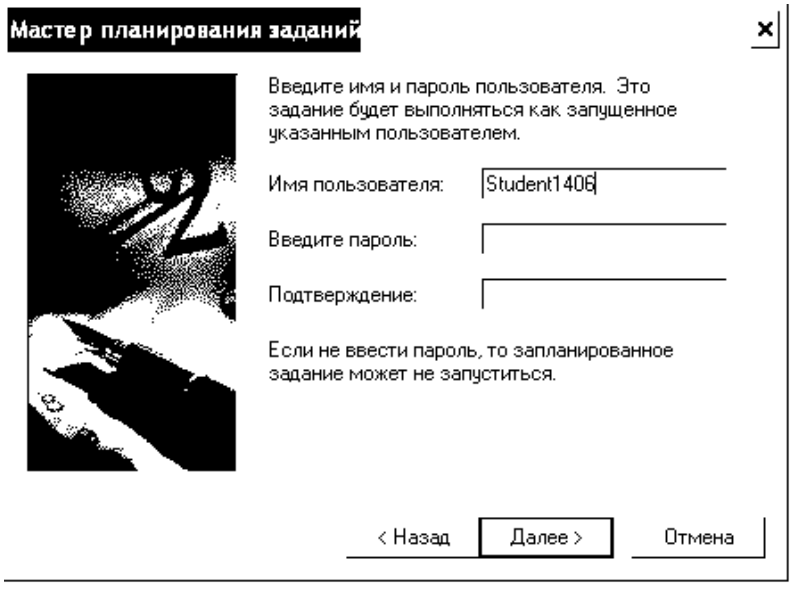

Рис. 12. Окно «Ввод пароля» приложения «Мастер планирования заданий»

14. Установите галочку задания дополнительных параметров и нажмите кнопку «Готово» (см. рис. 13).

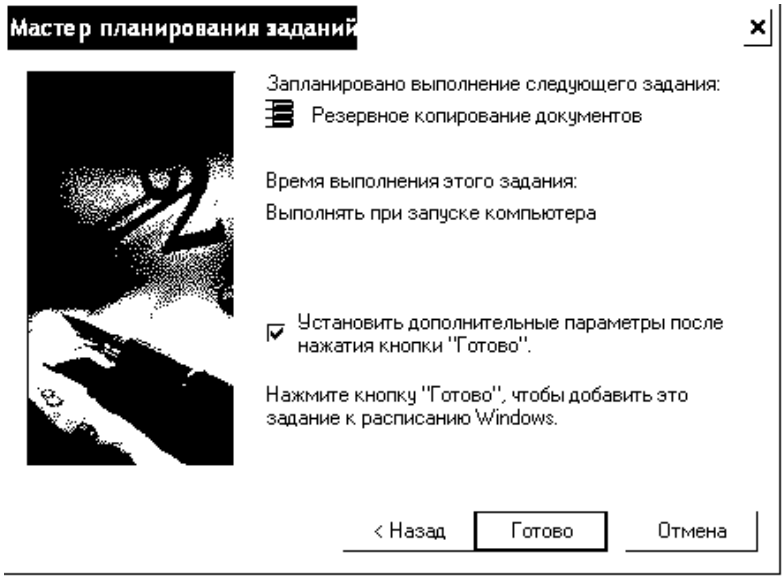

Рис. 13. Окно «Завершение» приложения «Мастер планирования заданий»

15. В дополнительных параметрах на вкладке «Задания» в поле «Выполнить» укажите параметры запуска программы WinRar: полное имя программы, команда добавления в архив, полное имя архива и шаблон архивируемых файлов (например, «C:\Program Files\WinRAR\WinRar.exe a D:\Arhive D:\Документы» см. рис. 14).

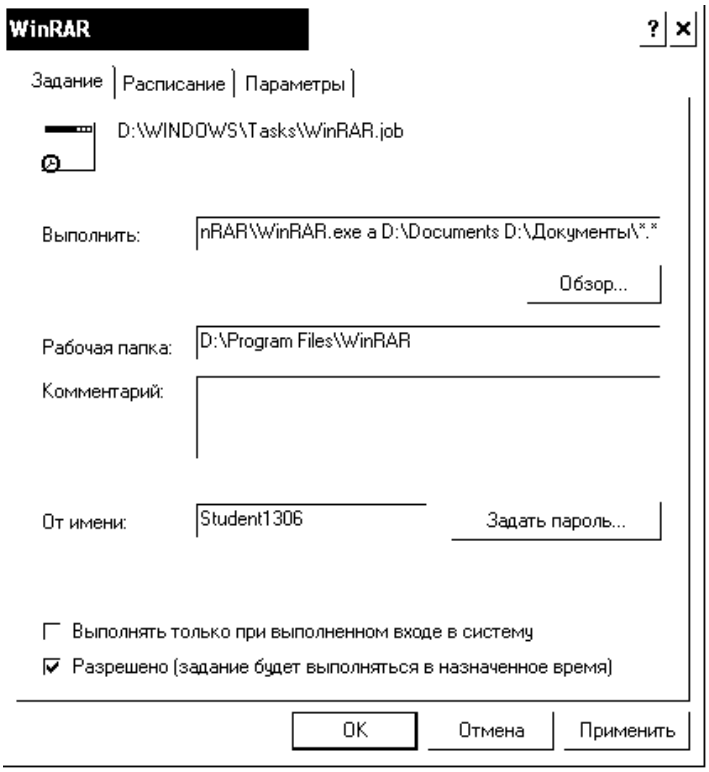

Рис. 14. Окно «Параметры» приложения «Мастер планирования заданий»

Вообще архивы рекомендуется хранить на другом компьютере, желательно в другом помещении, чтобы в случае кражи, пожара и т.п. сохранилась резервная копия данных.

16. Ознакомьтесь с дополнительными параметрами на вкладках «Расписание» и «Параметры» и нажмете кнопку «OK» (см. рис. 14).
17. Перезагрузите компьютер и проверьте наличие созданного архива.
18. Измените дополнительные параметры запуска программы WinRar так, чтобы при повторном добавлении файлов в архив старые файлы удалялись.

19. Запустите программу антивирус, например Kaspersky AntiVirus, и проверьте компьютер на наличие вирусов. Если в процессе работы программы были обнаружены вирусы, то необходимо «вылечить» или удалить зараженные файлы.
20. Запустите программу «Проверка диска» (кнопка «Пуск» | «Программы» | «Стандартные» | «Служебные» | «Проверка диска») и проверьте жесткие диски компьютера на наличие ошибок.
21. Запустите программу «Дефрагментация диска» (кнопка «Пуск» | «Программы» | «Стандартные» | «Служебные» | «Дефрагментация диска») и оптимизируйте жесткие диски компьютера.
22. Оформите отчет о ходе выполнения лабораторной работы.

Контрольные вопросы

1. Что понимается под информационной безопасностью, безопасностью и защитой данных?
2. В чем различие между понятиями: методы, средства и механизм защиты данных?
3. Перечислите основные угрозы безопасности данных.
4. Назовите основные способы несанкционированного доступа к конфиденциальной информации.
5. Перечислите уязвимые места информационных систем с точки зрения безопасности данных.
6. Перечислите основные методы защиты данных.
7. Перечислите основные средства защиты данных.
8. Какие программные средства защиты Вы знаете?
9. Назовите основные направления по обеспечению информационной безопасности для конечного пользователя.
10. Перечислите основные мероприятия по защите от компьютерных вирусов.
11. Перечислите основные мероприятия по защите информации от случайного удаления.
12. Перечислите основные мероприятия по защите информации от сбоев в работе различных устройств компьютера.