Содержание:

Введение

В этом случае информация, идентифицирующая и аутентифицирующая пользователя, хранится на внешнем носителе информации, который может представлять собой обычную дискету, электронный ключ, пластиковую карту и т.д. При входе в систему пользователь подключает к компьютеру носитель ключевой информации, и операционная система считывает с него идентификатор пользователя и соответствующий ему ключ.

Поскольку ключ, хранящийся на внешнем носителе, может быть сделан гораздо более длинным, чем пароль, подобрать такой ключ практически невозможно. Однако угроза утери или кражи ключевой информации по-прежнему остается актуальной. Если процедура аутентификации не предусматривает дополнительных мер защиты, любой обладатель носителя ключевой информации, в том числе и злоумышленник, укравший этот носитель у легального пользователя системы, может войти в систему с правами пользователя, которому принадлежит носитель.

Поэтому данный механизм аутентификации, как правило, используется в совокупности с дополнительным защитным кодом. При этом пользователь, входя в систему, должен не только "предъявить" компьютеру носитель ключевой информации, но и ввести соответствующий этому носителю пароль. Ключевая информация на носителе информации хранится зашифрованной на этом пароле, что не позволяет случайному обладателю ключа воспользоваться им.

Основной угрозой при использовании описываемого механизма аутентификации является угроза кражи носителя ключевой информации с последующим его копированием и подбором пароля на доступ к ключу. Если этот ключ выбирается случайно и не содержит проверочных полей (контрольных сумм и т.д.), подбор пароля на доступ к ключу вне атакуемой операционной системы невозможен - злоумышленник просто не сможет сформулировать критерий, позволяющий отличать правильно расшифрованный ключ от неправильно расшифрованного и, следовательно, правильный пароль от неправильного. А если злоумышленник

станет опробовать этот пароль, делая попытки использовать ключевой носитель для аутентификации, от этой угрозы надежно защищают процедуры блокировки

Однако во многих случаях без проверочных полей ключа обойтись невозможно. В этой ситуации пароль на доступ к ключу может быть подобран с помощью методов подбора паролей. Для затруднения такого подбора используются следующие меры защиты:

-защита ключевого носителя от копирования;

-блокировка или уничтожение ключевой информации после определенного количества неудачных попыток ввода пароля на доступ к ключу.

Если в качестве носителя ключевой информации применяются ключевые дискеты, электронные ключи TouchMemory или пластиковые карты MemoryCard, эти меры защиты неприменимы. Хотя существующие средства защиты от копирования и позволяют несколько затруднить копирование носителя информации, любой из перечисленных носителей может быть скопирован за несколько минут, в отдельных случаях -за несколько часов. Поскольку проверку правильности пароля на доступ к ключу осуществляет операционная система, то, если злоумышленник подбирает пароль с помощью специальной программы, подсчитывать количество неудачных попыток также невозможно.

В отличие от перечисленных носителей информации интеллектуальные пластиковые карты SmartCardпомимо энергонезависимой памяти содержат микропроцессор, способный выполнять криптографические преобразования информации. Поэтому интеллектуальные карты способны самостоятельно проверять правильность пароля на доступ к ключевой информации, и при аутентификации пользователя с использованием интеллектуальной карты проверку пароля на доступ к карте производит не операционная система, а сама карта. Интеллектуальная карта может быть запрограммирована на стирание хранимой информации после превышения максимально допустимого количества неправильных попыток ввода пароля, что не позволяет подбирать пароль без частого копирования карты, а это весьма дорого.

В целом использование для аутентификации пользователей не только паролей, но еще и внешних носителей информации позволяет заметно повысить защищенность операционной системы. В наибольшей мере защищенность системы повышается при использовании интеллектуальных карт. Учитывая постоянное удешевление как самих интеллектуальных карт, так и устройств для их считывания, можно ожидать,

что в ближайшие 5-10лет интеллектуальные карты станут основным средством аутентификации в операционных системах, используемых для хранения и обработки конфиденциальной информации.
Средства идентификации и аутентификации –электронные идентификаторы– являются частью аппаратно-программных систем идентификации и аутентификации (СИА), в которые входят также устройства ввода-вывода и соответствующее ПО.
Идентификация представляет собой процесс распознавания пользователя по присущему или присвоенному ему идентификационному признаку.
Аутентификация– процесс проверки принадлежности пользователю предъявленного им идентификационного признака.
электронные идентификаторы предназначены для хранения уникальных идентификационных признаков, а также для хранения и обработки конфиденциальных данных. Устройства ввода-вывода и ПО осуществляют обмен данными между идентификатором и защищаемым компьютером.
Идентификационные признаки представляются в виде цифрового кода, хранящегося в памяти идентификатора
По способу обмена данными между идентификатором и устройством ввода-вывода электронные СИА подразделяются на:
Контактные– при непосредственном соприкосновении идентификатора с устройством ввода-вывода;
бесконтактные– при отсутствии четкого позиционирования идентификатора и устройства ввода-вывода (чтение / запись данных происходит при поднесении идентификатора на определенное расстояние к устройству ввода-вывода).
Современные электронные СИА разрабатываются на базе следующих идентификаторов:

- смарт-карт;
- радиочастотных, или RFID-идентификаторов;
- идентификаторов iButton;
- USB-ключей, или USB-токенов.

Контактные идентификаторы подразделяются на идентификаторы iButton, смарт-карты и USB-ключи.

Идентификатор iButton представляет собой встроенную в герметичный стальной корпус микросхему, питание которой обеспечивает миниатюрная литиевая батарейка. Основу чипа составляют мультиплексор и память. Помимо этого некоторые типы идентификаторов содержат дополнительные компоненты.

Контактные смарт-карты делиться на процессорные карты и карты с памятью. Выпускаются в виде пластиковых карточек. Основу внутренней структуры современной процессорной смарт-карты составляет чип, в состав которого входят процессор (или несколько процессоров), оперативная память RAM, постоянная память ROM и энергонезависимая программируемая постоянная память PROM.

USB-ключи предназначаются для работы с USB-портом компьютера. Конструктивно изготавливаются в виде брелоков, выпускаемых в цветных корпусах и имеющих световые индикаторы работы. Каждый идентификатор имеет прошиваемый при изготовлении уникальный 32/64-разрядный серийный номер.

Бесконтактные идентификаторы разделяются на идентификаторы Proximity и смарт-карты. Конструктивно они изготавливаются в виде пластиковых карточек, брелоков, жетонов, дисков, меток и т. п. Основными компонентами идентификаторов являются чип и антенна. Каждый идентификатор имеет уникальный 32/64-разрядный серийный номер.

Достоинством радиочастотных идентификаторов, смарт-карт и USB-ключей являются защищенная энергонезависимая память и криптографический процессор, позволяющие повысить уровень защиты устройств, входящие в их состав.

Прежде чем получить доступ к ресурсам, пользователь должен пройти процесс представления компьютерной системе, который включает две стадии:

идентификацию - пользователь сообщает системе по ее запросу свое имя (идентификатор);

аутентификацию - пользователь подтверждает идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль).

Для проведения процедур идентификации и аутентификации пользователя необходимо наличие:

- программы аутентификации;
- уникальная информация о пользователе.

Различают две формы хранения информации о пользователе: внешняя (например, пластиковая карта) и внутренняя (например, запись в базе данных).

Процедуры идентификации и аутентификации пользователя могут базироваться не только на секретной информации, которой обладает пользователь (пароль, секретный ключ, персональный идентификатор и т.п.). В последнее время все большее распространение получает биометрическая идентификация и аутентификация, позволяющая уверенно идентифицировать потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.

Основные достоинства биометрических методов идентификации и аутентификации:

высокая степень достоверности идентификации по биометрических признакам из-за их уникальности;

неотделимость биометрических признаков от дееспособной личности;

трудность фальсификации биометрических признаков.

В качестве биометрических признаков, которые могут быть использованы для идентификации потенциального пользователя, используются:

- узор радужной оболочки и сетчатки глаз;
- отпечатки пальцев;
- геометрическая форма руки;
- форма и размеры лица;
- термограмма лица;
- форма ушей;
- особенности голоса;
- ДНК;

биомеханические характеристики рукописной подписи;

биомеханические характеристики "клавиатурного почерка".

При регистрации пользователь должен продемонстрировать один или несколько раз свои характерные биометрические признаки. Эти признаки (известные как подлинные) регистрируются системой как контрольный "образ" законного пользователя. Этот образ пользователя хранится в электронной форме и используется для проверки идентичности каждого, кто выдает себя за соответствующего законного пользователя.

Системы идентификации по узору радужной оболочки и сетчатки глаз могут быть разделены на два класса:

- использующие рисунок радужной оболочки глаза;
- использующие рисунок кровеносных сосудов сетчатки глаза.

Поскольку вероятность повторения данных параметров равна 10-78, эти системы являются наиболее надежными среди всех биометрических систем. Такие средства применяются, например, в США в зонах военных и оборонных объектов.

Системы идентификации по отпечаткам пальцев являются самыми распространенными. Одна из основных причин широкого распространения таких систем заключается в наличии больших банков данных по отпечаткам пальцев. Основными пользователями таких систем во всем мире являются полиция, различные государственные организации и некоторые банки.

Системы идентификации по геометрической форме руки используют сканеры формы руки, обычно устанавливаемые на стенах. Следует отметить, что подавляющее большинство пользователей предпочитают системы именно этого типа.

Системы идентификации по лицу и голосу являются наиболее доступными из-за их дешевизны, поскольку большинство современных компьютеров имеют видео- и аудиосредства. Системы данного класса широко применяются при удаленной идентификации в телекоммуникационных сетях.

Системы идентификации по динамике рукописной подписи учитывают интенсивность каждого усилия подписывающегося, частотные характеристики написания каждого элемента подписи и начертания подписи в целом.

Системы идентификации по биомеханическим характеристикам "клавиатурного почерка" основываются на том, что моменты нажатия и отпускания клавиш при наборе текста на клавиатуре существенно различаются у разных пользователей. Этот динамический ритм набора ("клавиатурный почерк") позволяет построить достаточно надежные средства идентификации.

Следует отметить, что применение биометрических параметров при идентификации субъектов доступа автоматизированных систем пока не получило надлежащего нормативно-правового обеспечения, в частности в виде стандартов. Поэтому применение систем биометрической идентификации допускается только в

системах, обрабатывающих и хранящих персональные данные, составляющие коммерческую и служебную тайну.

Наиболее действенными методами защиты от несанкционированного доступа по компьютерным сетям являются виртуальные частные сети (VPN – VirtualPrivateNetwork) и межсетевое экранирование. Рассмотрим их подробно.

Виртуальные частные сети

Виртуальные частные сети обеспечивают автоматическую защиту целостности и конфиденциальности сообщений, передаваемых через различные сети общего пользования, прежде всего, через Интернет. Фактически, VPN – это совокупность сетей, на внешнем периметре которых установлены VPN-агенты. VPN-агент – это программа (или программно-аппаратный комплекс), собственно обеспечивающая защиту передаваемой информации путем выполнения описанных ниже операций.

Перед отправкой в сеть любого IP-пакета VPN-агент производит следующее:

Из заголовка IP-пакета выделяется информация о его адресате. Согласно этой информации на основе политики безопасности данного VPN-агента выбираются алгоритмы защиты (если VPN-агент поддерживает несколько алгоритмов) и криптографические ключи, с помощью которых будет защищен данный пакет. В том случае, если политикой безопасности VPN-агента не предусмотрена отправка IP-пакета данному адресату или IP-пакета с данными характеристиками, отправка IP-пакета блокируется.

С помощью выбранного алгоритма защиты целостности формируется и добавляется в IP-пакет электронная цифровая подпись (ЭЦП), имитоприставка или аналогичная контрольная сумма.

С помощью выбранного алгоритма шифрования производится зашифрование IP-пакета.

С помощью установленного алгоритма инкапсуляции пакетов зашифрованный IP-пакет помещается в готовый для передачи IP-пакет, заголовок которого вместо исходной информации об адресате и отправителе содержит соответственно информацию о VPN-агенте адресата и VPN-агенте отправителя. Т.е. выполняется трансляция сетевых адресов.

Пакет отправляется VPN-агенту адресата. При необходимости, производится его разбиение и поочередная отправка результирующих пакетов.

При приеме IP-пакета VPN-агент производит следующее:

Из заголовка IP-пакета выделяется информация о его отправителе. В том случае, если отправитель не входит в число разрешенных (согласно политике безопасности) или неизвестен (например, при приеме пакета с намеренно или случайно поврежденным заголовком), пакет не обрабатывается и отбрасывается.

Согласно политике безопасности выбираются алгоритмы защиты данного пакета и ключи, с помощью которых будет выполнено расшифрование пакета и проверка его целостности.

Выделяется информационная (инкапсулированная) часть пакета и производится ее расшифрование.

Производится контроль целостности пакета на основе выбранного алгоритма. В случае обнаружения нарушения целостности пакет отбрасывается.

Пакет отправляется адресату (по внутренней сети) согласно информации, находящейся в его оригинальном заголовке.

VPN-агент может находиться непосредственно на защищаемом компьютере. В этом случае с его помощью защищается информационный обмен только того компьютера, на котором он установлен, однако описанные выше принципы его действия остаются неизменными.

Основное правило построения VPN – связь между защищенной ЛВС и открытой сетью должна осуществляться только через VPN-агенты. Категорически не должно быть каких-либо способов связи, минующих защитный барьер в виде VPN-агента. Т.е. должен быть определен защищаемый периметр, связь с которым может осуществляться только через соответствующее средство защиты.

Политика безопасности является набором правил, согласно которым устанавливаются защищенные каналы связи между абонентами VPN. Такие каналы обычно называют туннелями, аналогия с которыми просматривается в следующем:

Вся передаваемая в рамках одного туннеля информация защищена как от несанкционированного просмотра, так и от модификации.

Инкапсуляция IP-пакетов позволяет добиться сокрытия топологии внутренней ЛВС: из Интернет обмен информации между двумя защищенными ЛВС виден как обмен информацией только междуих VPN-агентами, поскольку все внутренние IP-адреса в передаваемых через Интернет IP-пакетах в этом случае не фигурируют.

Правила создания туннелей формируются в зависимости от различных характеристик IP-пакетов, например, основной при построении большинства VPN протокол IPSec (SecurityArchitecturefor IP) устанавливает следующий набор входных данных, по которым выбираются параметры туннелирования и принимается решение при фильтрации конкретного IP-пакета:

IP-адрес источника. Это может быть не только одиночный IP-адрес, но и адрес подсети или диапазон адресов.

IP-адрес назначения. Также может быть диапазон адресов, указываемый явно, с помощью маски подсети или шаблона.

Идентификатор пользователя (отправителя или получателя).

Протокол транспортного уровня (TCP/UDP).

Номер порта, с которого или на который отправлен пакет.

Межсетевое экранирование

Межсетевой экран представляет собой программное или программно-аппаратное средство, обеспечивающее защиту локальных сетей и отдельных компьютеров от несанкционированного доступа со стороны внешних сетей путем фильтрации двустороннего потока сообщений при обмене информацией. Фактически, межсетевой экран является «урезанным» VPN-агентом, не выполняющим шифрование пакетов и контроль их целостности, но в ряде случаев имеющим ряд дополнительных функций, наиболее часто из которых встречаются следующие:

- антивирусное сканирование;
- контроль корректности пакетов;
- контроль корректности соединений (например, установления, использования и разрыва TCP-сессий);
- контент-контроль.

Межсетевые экраны, не обладающие описанными выше функциями и выполняющими только фильтрацию пакетов, называют пакетными фильтрами.

По аналогии с VPN-агентами существуют и персональные межсетевые экраны, защищающие только компьютер, на котором они установлены.

Межсетевые экраны также располагаются на периметре защищаемых сетей и фильтруют сетевой трафик согласно настроенной политике безопасности.

Взаимная проверка подлинности пользователей

Обычно стороны, вступающие в информационный обмен, нуждаются во взаимной аутентификации. Этот процесс выполняется в начале сеанса связи.

Для проверки подлинности применяют следующие способы:

- механизм запроса-ответа;
- механизм отметки времени ("временной штемпель").

Механизм запроса-ответа. Если пользователь А хочет быть уверен, что сообщения, получаемые им от пользователя В, не являются ложными, он включает в посылаемое для В сообщение непредсказуемый элемент - запрос X (например, некоторое случайное число). При ответе пользователь В должен выполнить над этим числом некоторую заранее оговоренную операцию (например, вычислить некоторую функцию f(X)). Это невозможно осуществить заранее, так как пользователю В неизвестно, какое случайное число X придет в запросе. Получив ответ с результатом действий В, пользователь А может быть уверен, что В - подлинный. Недостаток этого метода - возможность установления закономерности между запросом и ответом.

Механизм отметки времени подразумевает регистрацию времени для каждого сообщения. В этом случае каждый пользователь сети может определить насколько "устарело" пришедшее сообщение и не принимать его, поскольку оно может быть ложным.

В обоих случаях для защиты механизма контроля следует применять шифрование, чтобы быть уверенным, что ответ послан не злоумышленником.

При использовании отметок времени возникает проблема допустимого временного интервала задержки для подтверждения подлинности сеанса. Ведь сообщение с "временным штемпелем" в принципе не может быть передано мгновенно. Кроме того, компьютерные часы получателя и отправителя не могут быть абсолютно синхронизированы.

Для взаимной проверки подлинности обычно используют процедуру "рукопожатия", которая базируется на указанных выше механизмах и заключается во взаимной проверке ключей, используемых сторонами. Иначе говоря, стороны признают друг друга законными партнерами, если докажут друг другу, что обладают правильными ключами. Процедуру "рукопожатия" применяют в компьютерных сетях при организации связи между пользователями, пользователем и хост-компьютером, между хост-компьютерами и т.д.

Программы от несанкционированного доступа

Здесь мы кратно рассмотрим 3 программы, с помощью которых возможно защитить свои данные он несанкционированного доступа.

CryptoExpert

CryptoExpert 2008 Professional от компании SecureAction— это программа для шифрования данных в режиме реального времени на компьютере. Она совместима с операционными системами семействаWindows, включая WindowsVista 32-bit и 64-bit.

Программа CryptoExpert 2008 Professional позволяет создавать виртуальные логические диски (контейнеры), в которых информация сохраняется в зашифрованном виде. CryptoExpertсуществуютвдвухвариантах: CryptoExpert 2007 Lite иCryptoExpert 2008 Professional. Программа CryptoExpert 2007 Lite является бесплатной и отличается от CryptoExpert 2008 Professional урезанной функциональностью. В частности, в CryptoExpert 2007 Lite размер виртуального контейнера составляет 50 Мбайт, тогда как в программе CryptoExpert 2008 Professional он ограничен лишь свободным пространством на жестком диске. Еще одно различие между версиями заключается в том, что в программе CryptoExpert 2007 Lite используется только один алгоритм шифрования — CAST 128 bit, а в программе CryptoExpert 2008 Professional поддерживаются четыре типа

шифрования: AES (256 bit), CAST (128 bit), Blowfish (448 bit) и 3DES (168 bit). Есть и другие различия, однако, чтобы понять, о чем идет речь, необходимо научиться работать с программой.

К сожалению, описание к программе на русском языке отсутствует, да и интерфейс только английский, к тому же его нельзя назвать простым и интуитивно понятным — прежде чем воспользоваться этой программой, придется изучить инструкцию.

Если кратко, то основные принципы работы с программой следующие. Сначала создаются виртуальные контейнеры, для каждого из которых устанавливается размер, выбирается алгоритм шифрования и задается пароль (рис. 8). Контейнер может находиться в двух состояниях: подключенном и отключенном. С подключенным контейнером можно работать как с обычным логическим диском. Естественно, что для подключения контейнера необходимо знать пароль. В программе CryptoExpert 2008 Professional одновременно можно подключать неограниченное число контейнеров, а в программе CryptoExpert 2007 Lite поддерживается только один подключенный контейнер. Кроме того, версия CryptoExpert 2008 Professional поддерживает работу с USB-носителями, а также возможность создавать и подключать контейнеры, созданные на общих ресурсах локальной сети

Программа также позволяет удалять файлы без возможности их восстановления. Причем поддерживается невосстанавливаемое удаление файлов как из логических контейнеров, так и из обычных папок.

Из недостатков программы CryptoExpert 2008 отметим нестабильность ее в работе. Мы тестировали программу с операционной системой WindowsVista 32-bit, и она частенько зависала.

Графическое оформление программы представлено в приложении

FineCrypt

Утилита FineCrypt предназначена для шифрования данных с целью их дальнейшего безопасного хранения на компьютере или передачи через Интернет. Она

поддерживает только английский язык и совместима со всеми операционными системами семейства Windows. С сайта компании можно скачать бесплатную демо-версию программы, которая отличается от полной версии урезанной функциональностью. К сожалению, толковое описание к программе типа «Howto…» отсутствует поэтому осваивать утилиту придется методом проб и ошибок. Но ничего сложного в этом нет. После инсталляции на ПК программа интегрируется в оболочку Windows и в контекстном меню появляется соответствующий пункт После этого достаточно выделить мышкой любой файл, щелкнуть по нему правой кнопкой мыши и, выбрав соответствующий пункт меню, зашифровать или расшифровать файл.

Программа FineCrypt поддерживает шифрование как отдельных файлов, так и целых папок. При этом поддерживается как симметричное шифрование с использованием пароля, так и шифрование с помощью секретных ключей. Кроме того, поддерживается асимметричное шифрование на основе публичного и секретного ключей.

Дляшифрованияможнопримен ятьследующиеалгоритмы: AES (256 bit), Blowfish (576 bit), CAST (256 bit), GOST (256 bit), Square (128 bit), Mars (448 bit), RC-6 (2040 bit), Serpent (256 bit), TripleDES (192 bit) иTwofish (256 bit)

В случае симметричного шифрования при наборе пароля, который программно преобразуется в ключ шифрования нужной длины, специальный индикатор напомнит о стойкости вводимого пароля (чем длиннее пароль, тем лучше)

Если требуется обеспечить наивысший уровень безопасности данных, то вместо пароля рекомендуется применять секретный ключ. Программа FineCrypt позволяет генерировать и сохранять секретные ключи шифрования. Кроме того, при генерации секретного ключа пользователь может полностью управлять вектором инициализации ключа. Напомним, что вектор инициализации не является секретной информацией и используется для реализации блочного алгоритма шифрования. В программе FineCrypt вектор инициализации ключа шифрования сохраняется вместе с ключом, а не в зашифрованном файле.

Кроме генерирования ключа и вектора инициализации ключа программа FineCrypt позволяет создавать ключ и вектор инициализации вручную.

Программа FineCrypt также поддерживает использование асимметричного RSA-шифрования на основе публичного и секретного ключей. Напомним, что асимметричное шифрование применяется при необходимости передачи

информации в зашифрованном виде другим пользователям. При этом информация шифруется с помощью публичного ключа, а расшифровать ее можно, только имея секретный ключ. Программа FineCrypt позволяет генерировать пары ключей, публичный и секретный , а также отсылать другим пользователям публичные ключи. Для простоты управления секретным и публичным ключами при их генерации осуществляется привязка к имени пользователя и его почтовому адресу. Кроме того, секретный ключ защищается паролем. Сгенерированный публичный ключ можно отправить по почте другому пользователю.

Как и большинство программ, предназначенных для обеспечения конфиденциальности данных, утилита FineCrypt позволяет не просто удалять файлы, а удалять их без возможности дальнейшего восстановления в соответствии со стандартом DoD 5200.28-STD (стандарт Министерства обороны США).

Ну и последнее, о чем хотелось бы упомянуть, — это возможность создания самораспаковывающихся зашифрованных архивов. В этом случае расшифровать данные можно даже на компьютере, где программа FineCrypt не установлена.

DekartPrivateDisk 2.10

Программа DekartPrivateDisk 2.10 от компании Dekart — это разработка молдавских программистов. Она совместима с операционными системами семейства Windows, включая WindowsVista 32 bit и 64 bit.

Стоимость программы DekartPrivateDisk 2.10 составляет 45 долл., а на сайте производителя можно скачать ее ознакомительную полнофункциональную 30-дневную версию. Отметим, что с сайта производителя можно загрузить программу с русскоязычным интерфейсом, причем на русском языке написана и подробная инструкция по ее использованию.

Итак, программа DekartPrivateDisk 2.10 предназначена для шифрования информации с целью ее безопасного хранения на компьютере или на съемных носителях. Она позволяет создавать виртуальные логические диски, в которых информация сохраняется в зашифрованном виде. С виртуальными логическими дисками можно работать точно так же, как и с обычными. Виртуальный зашифрованный диск представляет собой обычный файл — так называемый файл-образ диска. Файл-образ виртуального зашифрованного диска может иметь любые имя, расширение и путь доступа.

Работа с программой начинается с создания виртуального контейнера, для которого необходимо указать размер и местоположение файла-образа, а также задать пароль доступа. Минимальный размер виртуального диска — 1 Мбайт, а максимальный — 1 Тбайт (для ОС Windows NT/2000/XP/2003/Vista).

Каждый созданный контейнер может находиться в двух состояниях: подключенном и отключенном. При смонтированном состоянии контейнера с ним можно работать как с обычным логическим диском. Естественно, для подключения контейнера необходимо знать пароль.

После того как виртуальный контейнер создан и смонтирован, зашифровать данные очень просто — надо лишь перенести их на новый логический диск. В программе DekartPrivateDisk 2.10 используется алгоритм шифрования AES с длиной ключа 256 бит.

Нужно отметить, что программа DekartPrivateDisk 2.10 обладает очень широкими возможностями по настройке, а также разнообразными дополнительными функциями.

Среди возможностей по настройке отметим назначение горячих клавиш и иконок, создание списка программ, которым разрешен доступ к виртуальному диску, и списка программ, которые автоматически запускаются при подключении и отключении виртуального диска.

Кроме того, в программе DekartPrivateDisk 2 предусмотрена возможность создания резервной копии виртуального диска и зашифрованной резервной копии ключа шифрования. Можно даже попытаться восстановить забытый пароль к виртуальному диску, используя для этого метод перебора возможных комбинаций символов пароля. При попытке восстановления пароля возможно задание набора символов и указание длины пароля. Хотя, конечно, если пароль забыт, то пытаться восстановить его — дело безнадежное, поэтому данная функция скорее демонстрирует надежность защиты, нежели имеет практическое значение.