Тема 7. Обеспечение доступности информации на рабочих станциях

«Доверенная загрузка» – это загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: **проверки целостности технических и программных средств ПК** (с использованием механизма пошагового контроля целостности) **и идентификации/аутентификации** пользователя.

Доверенная загрузка компьютера необходима для того, чтобы воспрепятствовать несанкционированному запуску ПЭВМ, загрузке операционной системы и получению возможности доступа к конфиденциальной информации. Обеспечение конфиденциальности данных пользователя обычно достигается различными средствами в несколько этапов, начиная от защиты параметров BIOS от изменений до защиты памяти программ пользователя на уровне операционной системы, и выполняется программно-аппаратными средствами.

В область действия средств доверенной загрузки входят этапы работы компьютера от запуска микропрограммы BIOS до начала загрузки операционной системы.

Доверенная загрузка обычно включает в себя:

- Аутентификацию;
- Контроль устройства, с которого BIOS начинает загрузку операционной системы (жёсткий диск компьютера или устройство чтения сменного носителя, загрузки по сети и т.п.);
- Контроль целостности и достоверности загрузочного сектора устройства и системных файлов запускаемой операционной системы;
- Шифрование/расшифрования загрузочного сектора, системных файлов операционной системы, либо шифрование всех данных устройства.

Аутентификация, шифрование и хранение секретных данных, таких как ключи, контрольные суммы и хэш-суммы, выполняются на базе аппаратных средств.

Аутентификация пользователя может производиться различными способами и на разных этапах загрузки компьютера.

Для подтверждения личности запускающего компьютер могут требоваться различные факторы:

- Секретный логин и пароль пользователя;
- Дискета, компакт-диск, флэш-карта с аутентификационной информацией;
- Аппаратный ключ, подключаемый к компьютеру через USB-порт, последовательный или параллельный порты;
- Аппаратный ключ, либо биометрическая информация, считываемые в компьютер с помощью отдельно выполненного аппаратного модуля.

Аутентификация может быть многофакторной. Также аутентификация может быть многопользовательской с разделением прав доступа к компьютеру. Так, один пользователь сможет только запустить операционную систему с жёсткого диска, в то время как другому будет доступно изменение конфигурации BIOS и выбор загрузочного устройства.

Аутентификация может происходить:

- Во время выполнения микропрограммы BIOS;
- Перед загрузкой главной загрузочной записи (MBR) либо загрузочного сектора операционной системы;
- Во время выполнения программы загрузочного сектора.

Выполнение аутентификации на разных стадиях загрузки имеет свои преимущества.

- **Выполнение микропрограммы BIOS**. На этом этапе могут быть реализованы: проверка целостности микропрограммы BIOS, проверка целостности и подлинности настроек BIOS Setup, аутентификация (защита от запуска компьютера в целом, либо только от изменения конфигурации BIOS или выбора загрузочного устройства), контроль выбора загрузочного устройства. Этот этап загрузки должен быть полностью выполнен в микропрограмме BIOS производителем материнской платы;
- **Передача управления загрузочному устройству**. На этом этапе BIOS, вместо продолжения загрузки, может передать управление аппаратному модулю доверенной загрузки. Аппаратный модуль может выполнить аутентификацию, выбор загрузочного устройства, дешифрование и проверку целостности и достоверности загрузочных секторов и системных файлов операционной системы. При этом дешифрование загрузочного сектора операционной системы может быть выполнено только на этом этапе. Микропрограмма BIOS должна поддерживать передачу управления аппаратному модулю, либо аппаратный модуль должен эмулировать отдельное загрузочное устройство, выполненного в виде жёсткого диска, сменного носителя либо устройства загрузки по сети;

• **Выполнение загрузочного сектора операционной системы**. На этом этапе также может быть выполнена проверка целостности, достоверности загрузчика, системных файлов операционной системы и аутентификация. Однако исполняемый код загрузочного сектора ограничен в функциональности вследствие того, что имеет ограничение на размер и размещение кода, а также выполняется до запуска драйверов операционной системы.

Главные преимущества аппаратных средств:

- Высокая степень защищённости секретной информации о паролях, ключах и контрольных суммах системных файлов. В условиях стабильной работы такого модуля не предусмотрено способа извлечения такой информации.
- Возможная засекреченность алгоритмов шифрования, выполняемых аппаратно;
- Невозможность запустить компьютер, не вскрывая его содержимого;
- В случае шифрования загрузочного сектора, невозможно запустить операционную систему пользователя, даже после извлечения аппаратного модуля;
- В случае полного шифрования данных, невозможность получить любые данные после извлечения аппаратного модуля.

Примеры существующих аппаратных средств

Аппаратный модуль доверенной загрузки "Аккорд-АМДЗ"

Представляет собой аппаратный контроллер, предназначенный для установки в слот PCI/PCI Express. Модули «Аккорд-АМДЗ» обеспечивают доверенную загрузку операционных систем (ОС) любого типа с файловой структурой FAT12, FAT16, FAT32, NTFS, HPFS, Free BSD, Linux EXT2FS.

Вся программная часть модулей (включая средства администрирования), журнал событий и список пользователей размещены в энергонезависимой памяти контроллера. Таким образом, функции идентификации/аутентификации пользователей, контроля целостности аппаратной и программной среды, администрирования и аудита выполняются самим контроллером до загрузки ОС.

Основные возможности:

- идентификация и аутентификация пользователя с использованием ТМ-идентификатора и пароля длиной до 12 символов;
- блокировка загрузки ПЭВМ с внешних носителей;
- ограничение времени работы пользователей;
- контроль целостности файлов, аппаратуры и реестров;
- регистрация входа пользователей в систему в журнале регистрации;
- администрирование системы защиты (регистрация пользователей, контроль целостности программной и аппаратной части ПЭВМ).

Дополнительные возможности:

- контроль и блокировка физических линий;
- интерфейс RS-232 для применения пластиковых карт в качестве идентификатора;
- аппаратный датчик случайных чисел для криптографических применений;
- дополнительное устройство энергонезависимого аудита.

Модуль доверенной загрузки «Криптон-замок/PCI»

Предназначен для разграничения и контроля доступа пользователей к аппаратным ресурсам автономных рабочих мест, рабочих станций и серверов локальной вычислительной сети. Позволяют проводить контроль целостности программной среды в ОС, использующих файловые системы FAT12, FAT16, FAT32 и NTFS.

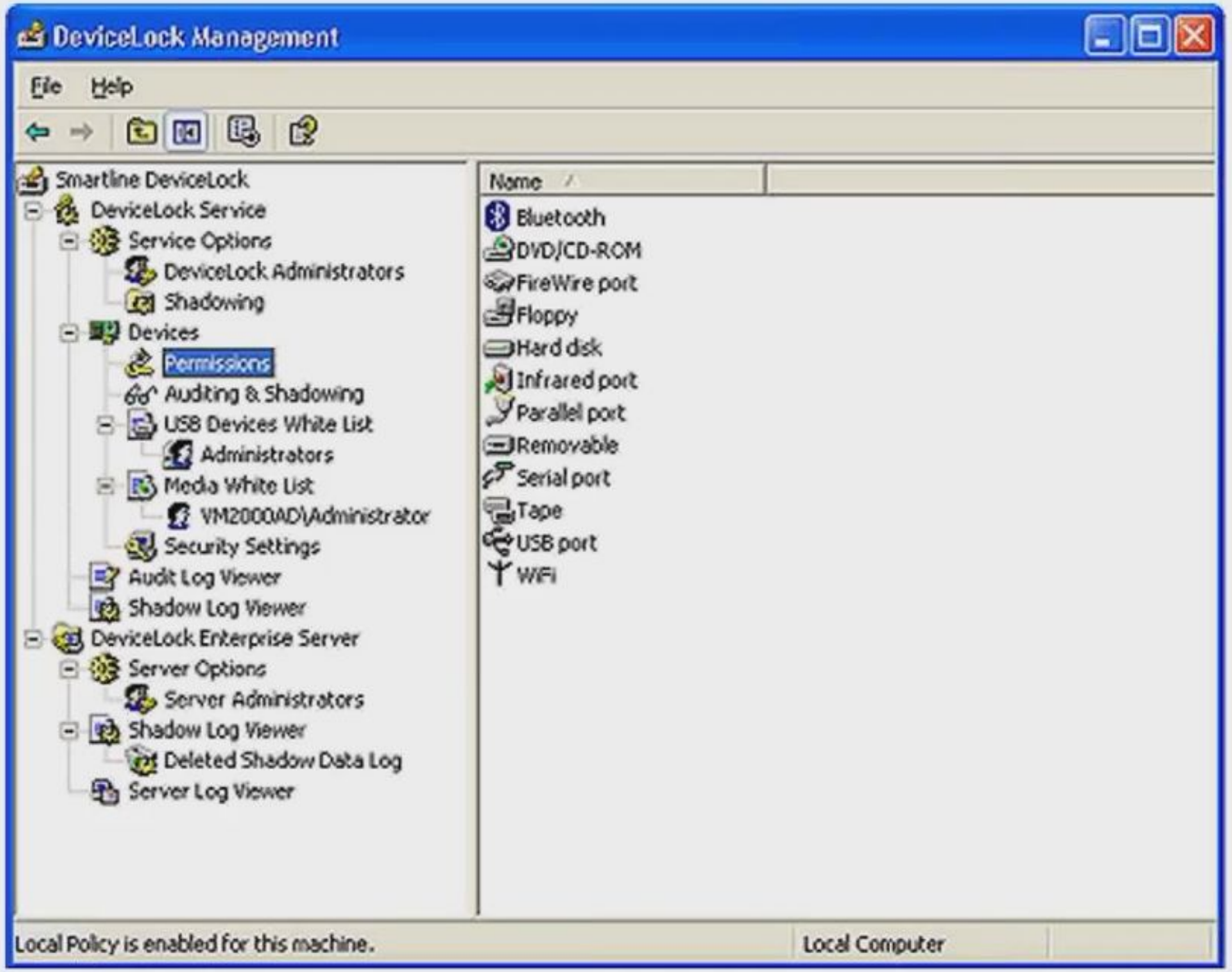
Особенности:

- идентификация и аутентификация пользователей до запуска BIOS при помощи идентификаторов Touch Memory;
- разграничение ресурсов компьютера, принудительная загрузка операционной системы (ОС) с выбранного устройства в соответствии с индивидуальными настройками для каждого пользователя;
- блокировка компьютера при НСД, ведение электронного журнала событий в собственной энергонезависимой памяти;
- подсчет эталонных значений контрольных сумм объектов и проверка текущих значений контрольных сумм, экспорт/импорт списка проверяемых объектов на гибкий магнитный диск;
- возможность интеграции в другие системы обеспечения безопасности (сигнализация, пожарная охрана и др.).

Обзор DeviceLock - программы для управления доступом к устройствам

При помощи DeviceLock администратор компьютера или домена может контролировать доступ пользователей к дисководам, DVD/CD-ROM, другим сменным устройствам, адаптерам WiFi и Bluetooth, а также к USB, FireWire, инфракрасным, COM- и LPT-портам. Кроме функции контроля доступа, DeviceLock позволяет осуществлять протоколирование и аудит использования устройств на локальном компьютере как отдельными пользователями, так и группами. Для хранения записей аудита DeviceLock использует стандартный журнал Windows, что позволяет просматривать их как с помощью стандартной программы просмотра событий, так и встроенного средства.

DeviceLock


DeviceLock Management
File
Help
Smartline DeviceLock
DeviceLock Service
Service Options
DeviceLock Administrators
Shadowing
Devices
Permissions
Auditing & Shadowing
USB Devices White List
Administrators
Media White List
VM2000AD\Administrator
Security Settings
Audit Log Viewer
Shadow Log Viewer
DeviceLock Enterprise Server
Server Options
Server Administrators
Shadow Log Viewer
Deleted Shadow Data Log
Server Log Viewer
Name
Bluetooth
DVD/CD-ROM
FireWire port
Floppy
Hard disk
Infrared port
Parallel port
Removable
Serial port
Tape
USB port
WiFi
Local Policy is enabled for this machine.
Local Computer

Хотя наличие журнала аудита и позволяет администратору отслеживать все действия пользователя, в том числе и по копированию файлов, только вот сами файлы пользователь, после копирования на носитель, может уничтожить или просто переименовать, и администратор безопасности уже не сможет сказать, была ли информация разрешена для копирования или нет.

При использовании функции теневого копирования (ее можно включить для отдельных пользователей или групп) все файлы и данные, копируемые пользователем на внешние носители и передаваемые через COM- и LPT-порты, будут "зеркалироваться" и сохраняться для последующего просмотра администратором. Сохраняются полные копии файлов и данных. Если в локальной сети установлено несколько сервисов DeviceLock, для каждого из них можно задавать имена одного или нескольких серверов, куда будут пересылаться данные теневого копирования.

Программа состоит из трех элементов: агента (DeviceLock Service), сервера (DeviceLock Enterprise Server) и консоли управления. Ядром системы является агент, устанавливаемый на каждый контролируемый компьютер. Консоли управления требуются для удаленного управления агентами, DeviceLock-сервером. Эти элементы обязательны, а вот сервер - элемент дополнительный, используемый для централизованного сбора и хранения данных теневого копирования и журналов. При значительной нагрузке на сервер (когда в сети свыше нескольких сотен контролируемых компьютеров) их может быть установлено несколько.

Для того чтобы не зависеть от учетных записей, под которыми будет запускаться сервер, предусмотрена организация его доступа к контролируемым компьютерам с помощью цифровых сертификатов. Закрытый ключ устанавливается на сервере, а на каждый компьютер, к которому должен подключаться сервер, устанавливается соответствующий ему открытый ключ.

Если DeviceLock Enterprise Server лишь обрабатывает поступающие данные и дает возможность их просмотра, то сбором и передачей данных занимается агент DeviceLock, для чего требуется его дополнительная настройка. В число параметров входит раздел на диске, где будут временно размещаться данные, и размер выделяемого пространства (задается в процентах от общего размера логического диска). Но даже выделив под сохраняемые копии многогигабайтный раздел, когда-то вы достигнете предела и его наполнения. Поэтому в качестве дополнительного параметра предусмотрена установка ограничения на наполнение этого раздела. В этом случае при достижении предельных цифр копирование данных в раздел прекращается.

Для предотвращения умышленного наполнения раздела и попытки копирования файлов во время, когда он отключен, предусмотрена возможность установки запрета на любое копирование данных в это время на контролируемые устройства.

Задачу администратора можно облегчить, если использовать еще один параметр настройки - разрешить автоматическое удаление старых файлов, помещенных в это хранилище. Если сервер для сбора данных не установлен, остается лишь риск того, что администратор может не проверить вовремя, что же копировалось на носители. Если же используется связка с сервером, то данные сами без администратора закачиваются на сервер и удаляются из локального хранилища.

В настройках аудита можно включить протоколирование всех заданий по копированию для гибких дисков, CD/DVD-ROM, последовательных и параллельных портов, съемных носителей. Для этих устройств в настройках аудита есть специальный параметр - включение режима теневого копирования. Файлы, копируемые на гибкие и съемные носители, сохраняются со своими первоначальными именами. Для сохранения информации, записываемой на CD/DVD или передаваемой через порты, DeviceLock в процессе копирования формирует собственные имена.

Раздел, в который копируются файлы и данные на локальном компьютере, недоступен для пользователя. Но администратор, используя модуль управления агентом, может получить доступ к просмоторщику, в котором в виде записей будет выведена информация о том, кто, когда, на какой носитель скопировал файл или передал информацию, какой программой при этом воспользовался. А если выбрать заинтересовавшую вас запись, то соответствующий ей файл или данные можно сохранить на диске в доступном разделе, после чего эти данные можно просматривать через соответствующие типу файла приложения. Впрочем, у пользователя остается возможность запрета доступа к скопированным файлам (но не тем, что передавались через порты COM или LPT). Для этого достаточно зашифровать файл, а таких возможностей сейчас имеется достаточно.

Авторизация носителей информации.

Авторизованные носители формируют так называемый "белый" список медианосителей. Этот список позволяет идентифицировать, к примеру, определенный CD/DVD- диск на основе записанных на него данных и разрешить его использование, даже если сам CD/DVD-привод заблокирован. (Но использование - не полное, поскольку на основе "белого" списка пользователю можно предоставить доступ только на чтение, но не на запись.) Изменение данных на носителе приводит к изменению его уникального идентификатора, и, следовательно, этот носитель уже не будет распознан как разрешенный (авторизованный). "Белый" список авторизованных носителей можно экспортировать и устанавливать на любой пользовательский компьютер. Разрешив пользователю доступ к такому носителю, вы предоставляете для него возможность чтения данных даже в том случае, если устройства для него недоступны.

Управление электропитанием рабочих станций и серверов.

Ни для кого не секрет, что проблемы с электропитанием компьютеров могут привести не только к потере информации, но и к повреждению оборудования. Чтобы защитить оборудование компании от таких проблем не-обходимо использование источников бесперебойного питания (ИБП, или UPS – Uninterruptible Power Source).

Мощность ИБП

Часто цифры, указываемые в названии ИБП, соответствуют полной мощности этого источника, измеряемой в вольт-амперах (ВА, VA). Соответствующее ему значение в Вт обычно указывается в спецификации устройства. Мощность импульсного блока питания компьютера в Вт соответствует мощности в ВА с коэффициентом 0,6-0,8. Кроме того, производители рекомендуют использовать ИБП с 20% запасом по мощности нагрузки.

Например, модель APC Smart-UPS 620 рассчитана на максимальную мощность 390 Вт, а модель APC Smart-UPS 1500 рассчитана на максимальную мощность 980 Вт.

Время автономной работы для ИБП зависит от подключенной к нему нагрузки и обычно указывается в спецификации устройства. Например, типичное время работы с нагрузкой 260 Вт (400 ВА) для модели APC Smart-UPS 620 составляет 9 мин., а для модели APC Smart-UPS 1500 – 58 мин.

Программное управление ИБП

Защита компьютеров с помощью ИБП является только частью решения задачи предотвращения потери данных в случае возникновения проблем с энергоснабжением. В случае продолжительного отсутствия электропитания, необходимо наличие программного обеспечения для корректного выключения компьютера в такой ситуации. Каждый производитель ИБП предлагает своё программное обеспечение для этой задачи. Кроме того, в Windows входит встроенная поддержка ИБП, которая была разработана компанией APC.

Существует несколько конфигураций для программного обеспечения ИБП:

- один компьютер – один ИБП;
- два или три компьютера – один ИБП;
- три и более компьютера – один ИБП.

В зависимости от используемой конфигурации, применяют различные способы взаимодействия ИБП с компьютером (последовательное, USB-, Ethernet- подключение).

Обзор средств активной защиты информации от утечки по сети электропитания.

Информативный сигнал в сети электропитания имеет достаточную для перехвата злоумышленником мощность и широкий частотный диапазон, что усложняет задачу защиты информации, обрабатываемой ПЭВМ и ЛВС. Таким образом, при соблюдении определенных энергетических и временных условий может возникнуть электромагнитный канал утечки конфиденциальной информации, обрабатываемой ПЭВМ и циркулирующей в ЛВС. Эти условия можно представить в виде:

$$\frac{P_{ис}}{P_ш} \geq \left(\frac{P_c}{P_ш}\right)_{пред} \qquad \Delta t \cong \Delta T,$$

где Рис – мощность информативного сигнала в точке приема; Рш – мощность шумов в точке приема; $\left(\frac{P_c}{P_ш}\right)_{пред}$ – предельное отношение мощности сигнала к мощности шума,при котором сигнал может быть перехвачен техническим средством злоумышленника; Т, - время обработки конфиденциальной информации; t - время работы средства перехвата информации.

Средства активной защиты информации от утечки по сети электропитания

Генератор шума по сети 220В и телефонной линии "РИАС-4"

“РИАС-4” предотвращает возможность использования устройств с передачей информации по сети 220В и устройств съёма информации с телефонной линии. Генерация помех телефонной линии и электросети для блокировки несанкционированно установленных устройств, передающих информацию.

Устройство для защиты от утечки информации по ПЭМИН "Октава-РС"

Устройство "Октава-РС" предназначено для защиты объектов ЭВТ (объектов информатизации) 1, 2 и 3 категории от утечки информации за счёт побочных электромагнитных излучений и наводок (ПЭМИН). Защита объектов осуществляется путем формирования и излучения в окружающее пространство электромагнитного поля шума (ЭМПШ) в диапазоне частот от 10 кГц до 2000МГц, а также индукцией напряжения шума в сеть электропитания 220В/50Гц, шину заземления и слаботочные линии связи в диапазоне частот от 10 кГц до 1000МГц.

Генератор для защиты от ПЭМИН и по сети 220 В "ЛГШ-503"

Генератор ЛГШ-503 предназначен для активной защиты объектов информатизации от утечки по сети электропитания ("фаза", "ноль" и "защитное заземление"), и для противодействия средствам несанкционированного съема информации по каналам ПЭМИ путем создания широкополосной шумовой помехи в диапазоне частот от 0,01 МГц до 2000 МГц.

Аппаратура дистанционного управления "Соната-ДУ".

Устройства "Соната-ДУ" предназначены для дистанционного включения/отключения аппаратуры защиты офисных и жилых помещений от негласного съема информации.

Генератор шума "Гном-3М"

Стационарный генератор шума для радиотехнической маскировки и защиты цепей электропитания.

Широкополосный генератор помех для силовой сети электропитания "Октава-С"

Защита электросетей переменного тока 220 В. 50 Гц от несанкционированного их использования для передачи речевой информации.

Тема 8. Обеспечение доступности информации на рабочих станциях в локальных сетях.

Межсетевой экран (firewall) - это устройство контроля доступа в сеть, предназначенное для **блокировки всего трафика, за исключением разрешенных данных**. Этим оно отличается от маршрутизатора, функцией которого является доставка трафика в пункт назначения в максимально короткие сроки.

Существует мнение, что маршрутизатор также может играть роль межсетевого экрана. Однако между этими устройствами существует одно принципиальное различие: маршрутизатор предназначен для быстрой маршрутизации трафика, а не для его блокировки. Межсетевой экран представляет собой средство защиты, которое пропускает определенный трафик из потока данных, а маршрутизатор является сетевым устройством, которое можно настроить на блокировку определенного трафика.

Кроме того, межсетевые экраны, как правило, обладают большим набором настроек. Прохождение трафика на межсетевом экране можно настраивать по службам, IP-адресам отправителя и получателя, по идентификаторам пользователей, запрашивающих службу. Межсетевые экраны позволяют осуществлять централизованное управление безопасностью. В одной конфигурации администратор может настроить разрешенный входящий трафик для всех внутренних систем организации. Это не устраняет потребность в обновлении и настройке систем, но позволяет снизить вероятность неправильного конфигурирования одной или нескольких систем, в результате которого эти системы могут подвергнуться атакам на некорректно настроенную службу.

Определение типов межсетевых экранов

Существуют два основных типа межсетевых экранов: межсетевые экраны **прикладного уровня** и межсетевые экраны **с пакетной фильтрацией**. В их основе лежат различные принципы работы, но при правильной настройке оба типа устройств обеспечивают правильное выполнение функций безопасности, заключающихся в блокировке запрещенного трафика.