**Процедуры безопасности**

**Защита данных**

Программный межсетевой экран — это программа, запускаемая на компьютере для разрешения или запрета обмена трафиком между компьютером и другими компьютерами, к которым он подключен. Программный межсетевой экран применяет набор правил для передачи данных с помощью проверки и фильтрации пакетов данных. Межсетевой экран Windows — это пример программного межсетевого экрана. Он устанавливается по умолчанию при установке ОС.

Любая связь по протоколу TCP/IP связана с номером порта. Например, HTTP по умолчанию использует порт 80. Как показано на рис. 1, программный межсетевой экран может защищать компьютер от вторжений через порты данных. Можно контролировать тип данных, отправляемых на другой компьютер, выбирая порты, которые будут открыты или заблокированы. Необходимо создать исключения, чтобы разрешить подключение к компьютеру для определенного трафика или приложений. Межсетевые экраны блокируют входящие и исходящие сетевые подключения, кроме случаев, когда для открытия и закрытия портов, необходимых для работы этой программы, определены исключения.

Для отключения портов в брандмауэре Windows в Windows 7, как показано на рис. 2, выполните следующие действия:

**Этап 1.**Выберите**Пуск > Панель управления > Брандмауэр Windows > Дополнительные параметры**.

**Этап 2.**На левой панели выберите настройку правил для входящих или исходящих подключений, затем щелкните пункт **Новое правило** на правой панели.

**Этап 3.**Выберите переключатель **Порт** и нажмите кнопку**Далее**.

**Этап 4.**Выберите **TCP**или **UDP**.

**Этап 5.**Выберите **Все локальные порты** или**Определенные локальные порты**, чтобы определить отдельные порты или диапазон портов, затем нажмите кнопку **Далее**.

**Этап 6.**Выберите **Блокировать подключение**, затем нажмите кнопку**Далее**.

**Этап 7.**Выберите, когда применяется правило, затем нажмите кнопку**Далее**.

**Этап 8.**Укажите имя и дополнительное описание для правила, затем нажмите кнопку**Готово**.

Для отключения портов в брандмауэре Windows в Windows Vista выполните следующие действия:

**Этап 1.**Выберите**Пуск > Панель управления > Брандмауэр Windows > Изменить параметры > Продолжить > Исключение > Добавить порт**.

**Этап 2.**Укажите имя и номер или диапазон портов.

**Этап 3.**Выберите TCP или UDP и нажмите кнопку**ОК**.

Для отключения портов в брандмауэре Windows в Windows XP выполните следующие действия:

**Этап 1.**Выберите**Пуск > Панель управления > Брандмауэр Windows > Исключения > Добавить порт**.

**Этап 2.**Укажите имя и номер или диапазон портов.

**Этап 3.**Выберите TCP или UDP и нажмите кнопку**ОК**.

**ПРИМЕЧАНИЕ**. В защищенной сети включите внутренний межсетевой экран ОС, чтобы обеспечить дополнительную безопасность. Если межсетевой экран настроен неверно, некоторые приложения могут работать неправильно.

# Процедуры безопасности

## Защита данных

В системах биометрической безопасности при проверке подлинности пользователей сравниваются физические характеристики и сохраненные профили. Профиль — это файл данных, содержащий известные характеристики пользователя. Примеры биометрических данных — отпечаток пальца, как показано на рис. 1, шаблон лица или скан сетчатки, как показано на рис. 2. Теоретически биометрическая защита более надежна, чем другие меры обеспечения безопасности, такие как пароли или смарт-карты, поскольку пароли можно узнать, а смарт-карты можно украсть. В число распространенных доступных биометрических устройств входят считыватели отпечатков пальцев, сканеры сетчатки и устройства распознавания лица и голоса. Если характеристики пользователя совпадают с сохраненными параметрами и указана верная информация для входа в систему, пользователю предоставляется доступ.

Биометрические устройства, измеряющие физическую информацию о пользователе, идеально подходят для высокосекретных областей в сочетании с дополнительными мерами обеспечения безопасности, такими как пароль или PIN-код. Однако для большинства небольших организаций стоимость этого типа решения чрезмерно высока.

**Обеспечение безопасности с использованием смарт-карт**

Смарт-карта — это небольшая пластиковая карта размером с кредитную карту с небольшим встроенным чипом, как показано на рис. 3. Чип — это интеллектуальное средство переноса данных, которое может обрабатывать, хранить и защищать данные. На смарт-картах хранится личная информация, такая как номера банковских счетов, информация, удостоверяющая личность, медицинская документация и цифровые подписи. Смарт-карты обеспечивают проверку подлинности и шифрование для защиты данных.

**Ключ-брелок безопасности**

Ключ брелок-безопасности — это небольшое устройство в виде украшения на кольце для ключей, как показано на рис. 4. Оно оснащено модулем радиосвязи для связи с компьютером на небольшом расстоянии. Брелок имеет небольшой размер, позволяющий просто носить его на кольце для ключей. Перед принятием имени пользователя и пароля компьютер должен определить сигнал ключа.

# Процедуры безопасности

## Защита данных

При выполнении резервного копирования данных компьютера копия информации сохраняется на съемном носителе для резервных копий, который можно сохранить в надежном месте.? Резервное копирование данных — один из самых эффективных способов защиты данных от потери. Данные могут потеряны или повреждены в таких случаях, как кражи, сбои оборудования или аварии. В случае сбоя компьютерного оборудования данные могут быть восстановлены из резервной копии на работающем оборудовании.

Резервное копирование данных следует выполнять регулярно и включать в план безопасности. Последняя резервная копия данных обычно сохраняется автономно, чтобы защитить носителя с резервными копиями на случай, если что-либо произойдет в основном помещении. Носители с резервными копиями часто используются повторно для экономии затрат на носители. Всегда следуйте правилам организации по замене носителей.

Ниже приведены некоторые соображения по резервному копированию данных.

* **Частота**— резервное копирование может длиться очень долго. Иногда проще выполнять полное резервное копирование ежемесячно или еженедельно, а затем выполнять частые частичные резервные копирования данных, измененных с момента полного резервного копирования. Однако чем больше частичных копий, тем больше затрачивается времени на восстановление данных.
* **Хранение** — чтобы обеспечить дополнительную безопасность, необходимо переносить резервные копии в автономное хранилище ежедневно, еженедельно или ежемесячно в соответствии с политикой безопасности.
* **Безопасность** — резервные копии должны быть защищены паролями. Пароль вводится до того, как данные на резервном носителе могут быть восстановлены.
* **Проверка** — всегда проверяйте резервные копии для обеспечения целостности данных.

**Процедуры безопасности**

**Защита данных**

Шифрование часто используется для защиты данных. Шифрование — это преобразование данных с использованием сложного алгоритма, чтобы сделать их нечитаемыми. Для преобразования нечитаемой информации в читаемые данные необходимо использовать специальный ключ. Программные продукты применяются для шифрования файлов, папок и даже дисков целиком.

Шифрующая файловая система (EFS) — это функция Windows для шифрования данных. EFS напрямую связана с определенной учетной записью пользователя. После шифрования с помощью EFS данные будут доступны только пользователю, выполнившему шифрование. Для шифрования данных с помощью EFS выполните следующие действия:

**Этап 1.**Выберите один или несколько файлов или папок.

**Этап 2.**Щелкните выбранные данные правой кнопкой мыши и выберите пункт**Свойства**.

**Этап 3.**Перейдите на вкладку**Дополнительно**.

**Этап 4.**Установите флажок **Шифровать содержимое для защиты данных**.

**Этап 5.**Файлы и папки, зашифрованные с использованием EFS, отображаются зеленым цветом, как показано на рисунке.

В состав Windows 7, Windows Vista Ultimate и Enterprise входит функция BitLocker для шифрования тома жесткого диска целиком. Функция BitLocker также может использоваться для шифрования съемных дисков. Для использования функции BitLocker на жестком диске должны быть хотя бы два тома. Системный том остается незашифрованным и должен иметь размер не менее 100 Мб. На этом томе содержатся файлы, необходимые для загрузки Windows. Windows 7 создает этот том по умолчанию при установке.

При использовании функции BitLocker в Windows Vista можно задействовать специальное средство подготовки диска для BitLocker для сжатия тома, содержащего операционную систему. После сжатия тома может быть создан системный файл в соответствие с требованиями BitLocker.

После создания системного тома необходимо инициализировать модуль TPM. TPM — это специальный модуль, установленный на материнской плате компьютера и используемый для программной и аппаратной проверки подлинности. В модуле TPM сохраняется информация, относящаяся к системе размещения, такая как ключи шифрования, цифровые сертификаты и пароли. Приложения, использующие шифрование, могут задействовать модуль TPM для защиты данных проверки подлинности, защиты лицензий на ПО и зашифрованных файлов, папок и дисков. Встроенные аппаратные средства обеспечения безопасности, например модуль TPM, вместе с программными, обеспечивают гораздо более безопасную компьютерную систему, чем при использовании только соответствующих программных средств.

Для инициализации модуля TPM выполните следующие действия:

**Этап 1.**Включите компьютер и войдите в программу настройки BIOS.

**Этап 2.**Перейдите к пункту **TPM** на экранах настройки BIOS. Для поиска верного экрана ознакомьтесь с руководством по материнской плате.

**Этап 3.**Выберите **Enable** (Включить) и нажмите клавишу **Ввод**.

**Этап 4.**Сохраните изменения настройки BIOS.

**Этап 5.**Перезагрузите компьютер.

Для включения BitLocker выполните следующие действия:

**Этап 1.**Нажмите кнопку **Пуск > Панель управления > Безопасность > Шифрование диска BitLocker**.

**Этап 2.**При появлении сообщения**Контроль учетных записей** нажмите кнопку **Продолжить**.

**Этап 3.**На странице **Шифрование диска BitLocker** выберите пункт**Включить BitLocker** для тома операционной системы.

**Этап 4.**Если модуль TPM не инициализирован, откроется мастер оборудования безопасности для TPM. Для инициализации TPM следуйте указаниям мастера. Перезагрузите компьютер.

**Этап 5.**На странице сохранения пароля восстановления имеются следующие возможности:

* **Сохранить пароль на USB-диске**— сохранение пароля на накопителе для порта USB.
* **Сохранить пароль в папке** — сохранение пароля на сетевом диске или в другом местоположении.
* **Напечатать пароль** — печать пароля.

**Этап 6.**После сохранения пароля восстановления нажмите кнопку **Далее**.

**Этап 7.**На странице **Encrypt the selected disk volume** (Шифрование выбранного тома диска) установите флажок**Запустить проверку системы Bitlocker**.

**Этап 8**. Нажмите кнопку **Продолжить**.

**Этап 9**. Нажмите кнопку **Перезагрузить сейчас**.

**Этап 10**. Появится индикатор состояния**Выполняется шифрование**.

**Процедуры безопасности**

**Защита от вредоносного ПО**

При определенных типах атак, например, осуществляемых с помощью шпионского ПО или фишинга, собираются данные о пользователе, которые могут использоваться злоумышленником для получения конфиденциальной информации.

Необходимо использовать программы поиска вирусов и шпионского ПО для обнаружения и удаления нежелательного ПО. Сейчас в состав многих обозревателей входят специальные средства и параметры предотвращения выполнения определенных форм вредоносного ПО. Для удаления всего вредоносного ПО может потребоваться использовать несколько различных программ и выполнять поиск несколько раз. Запускайте только одну программу защиты от вредоносного ПО одновременно.

* **Защита от вирусов**— антивирусная программа обычно запускается автоматически в фоновом режиме и отслеживает проблемы. При обнаружении вируса программа уведомляет об этом пользователя и пытается удалить вирус или поместить его на карантин, как показано на рис. 1.
* **Защита от шпионского ПО** — антишпионские программы проверяют наличие клавиатурных шпионов, сохраняющих последовательность нажатия клавиш, и другого вредоносного ПО для его удаления с компьютера, как показано на рис. 2.
* **Защита от рекламного ПО** — программы защиты от рекламного ПО выполняют поиск программ, отображающих рекламу на компьютере.
* **Защита от фишинга** — программы защиты от фишинга блокируют IP-адреса известных фишинговых веб-сайтов и уведомляют пользователя о подозрительных веб-сайтах.

**ПРИМЕЧАНИЕ**. Вредоносное ПО может встраиваться в операционную систему. Доступны специальные средства удаления, выпускаемые компаниями разработки программного обеспечения безопасности для очистки операционной системы.

**Лжеантивирусное ПО**

При работе в Интернете часто можно встретить рекламу продуктов и программного обеспечения. Эта реклама может использоваться для заражения компьютера пользователя. На некоторой рекламе отображаются сообщения с указанием на то, что компьютер пользователя заражен вирусом или иным вредоносным ПО. Реклама или всплывающее окно может выглядеть как действительное предупреждение Windows, сообщающее, что компьютер заражен и должен быть очищен, как показано на рис. 3. При выборе "Remove" (Удалить), "Clean" (Очистка), "OK" или даже "Cancel" (Отмена) или "Exit" (Выход) может начаться загрузка и установка вредоносного ПО. Этот тип атаки называется лжеантивирусным ПО.

При появлении подозрительного окна с предупреждением никогда не щелкайте это окно. Закройте вкладку или обозреватель, чтобы убрать окно с предупреждением. Если вкладка или обозреватель не закрываются, нажмите сочетание клавиш **ALT**+**F4**, чтобы закрыть окно, или используйте диспетчер задач для завершения работы программы. Если окно с предупреждением не закрывается, проверьте компьютер, используя известную действительную программу защиты от вирусов и рекламы, чтобы убедиться, что он не заражен.

**Восстановление зараженных систем**

Когда программа защиты от вредоносного ПО обнаруживает, что компьютер заражен, она удаляет угрозу или помещает ее на карантин. Однако, скорее всего, компьютер по-прежнему находится под угрозой. Первый этап восстановления зараженного компьютера — удаление компьютера из сети, чтобы не произошло заражения других компьютеров. Извлеките все сетевые кабели из компьютера и отключите все беспроводные подключения.

Затем следуйте указаниям применимых политик управления инцидентами. В их число может входить уведомление сотрудников отдела ИТ, сохранение файлов журналов на съемных носителях или выключение компьютера. Домашним пользователям необходимо обновить установленные программы защиты от вредоносного ПО или выполнить полную проверку всех установленных на компьютере носителей. Многие антивирусные программы могут быть настроены на запуск до загрузки Windows. Это предоставляет программе доступ ко всем областям диска без воздействия операционной системы или какого-либо вредоносного ПО.

Удаление с компьютера вирусов и червей может быть трудным процессом. Для удаления вирусов и восстановление компьютерного кода, измененного вирусом, требуются программные средства. Эти программные средства предоставляются производителями операционной системы и компаниями, выпускающими ПО обеспечения безопасности. Эти средства необходимо загрузить с доверенного сайта.

Загрузите компьютер в безопасном режиме, чтобы избежать загрузки большинства драйверов. Установите дополнительные программы защиты от вредоносного ПО и выполните полную проверку, чтобы удалить дополнительное вредоносное ПО или поместить его на карантин. Для полной очистки компьютера может потребоваться обратиться к специалисту. В некоторых случаях может потребоваться переформатирование компьютера и его восстановление из резервной копии или же переустановка операционной системы.

Служба восстановления системы может включать зараженные файлы в точку восстановления. После удаления вредоносного ПО на компьютере необходимо удалить файлы восстановления системы. Если для восстановления компьютера используется восстановление системы, то точки восстановления, содержащие зараженные файлы, не будут указаны в списке доступных и поэтому не приведут к повторному заражению компьютера.

Для удаления текущих файлов восстановления системы в Windows 7 выполните следующие действия:

**Этап 1.**Правой кнопкой мыши щелкните**Компьютер > Свойства > Защита системы**.

**Этап 2.**Выберите диск, содержащий точки восстановления, которые необходимо удалить.

**Этап 3.**Нажмите кнопку **Настройка**.

**Этап 4.**Нажмите кнопку **Удалить** рядом с пунктом**Удаление всех точек восстановления, включая параметры системы и предыдущие версии файлов**.

В Windows Vista и Windows XP выполните следующие действия:

**Этап 1.**Создайте точку восстановления.

**Этап 2.**Правой кнопкой мыши щелкните диск, содержащий точки восстановления, которые необходимо удалить.

**Этап 3.**Выберите **Свойства > Общие > Очистка диска**.

**Этап 4.**Windows выполнит анализ диска.

**Этап 5.**В окне **Очистка диска (C:)**перейдите на вкладку **Дополнительные параметры** **> Очистка**.

**Этап 6.**Нажмите кнопку **Удалить** в окне**Очистка диска**, чтобы удалить все точки восстановления, кроме последней.

# Процедуры безопасности

## Защита от вредоносного ПО

Стратегии безопасности постоянно меняются, как и технологии, используемые для защиты оборудования и данных. Новые уязвимости обнаруживаются каждый день. Злоумышленники постоянно ищут новые способы проникновения в компьютерные системы и сети. Производители программного обеспечения должны регулярно создавать и выпускать новые исправления для устранения ошибок и уязвимостей в продуктах. Если инженер оставит компьютер незащищенным, злоумышленник может получить доступ к нему. Незащищенные компьютеры в Интернете могут стать инфицированными за несколько минут.

Всегда присутствуют угрозы безопасности со стороны вирусов и червей. Поскольку постоянно разрабатываются новые вирусы, программное обеспечение безопасности должно постоянно обновляться. Этот процесс может выполняться автоматически, но инженер должен знать, как обновлять любые типы программного обеспечения безопасности и все клиентские программы вручную.

Программы защиты от вирусов, шпионского и рекламного ПО ищут шаблоны в коде программного обеспечения на компьютере. Эти шаблоны определяются путем анализа вирусов, перехваченных в Интернете и локальных сетях. Эти шаблоны кода называются сигнатурами. Издатели защитного ПО компилируют сигнатуры в таблицы определений вирусов. Перед обновлением файлов сигнатур для защиты от вирусов и шпионских программ сначала убедитесь, что файлы сигнатур являются последними версиями. Для проверки состояния файла выберите пункт «О программе» в защитном ПО или запустите средство обновления защитного ПО.

Чтобы обновить файл сигнатур, выполните следующие действия:

**Этап 1.**Создайте точку восстановления Windows. Если загруженный файл поврежден, настройка точки восстановления позволяет вернуться к нужному моменту.

**Этап 2.**Откройте антивирусную или антишпионскую программу. Если программа настроена на автоматическое выполнение или получение обновления, может потребоваться выключить функцию автоматического обновления, чтобы выполнить эти действия вручную.

**Этап 3.**Нажмите кнопку **Update**(Обновить).

**Этап 4.**После обновления программы используйте ее для проверки компьютера.

**Этап 5.**После завершения проверки прочтите отчет, чтобы найти вирусы или другие проблемы, которые не могли быть устранены, чтобы удалить их самостоятельно.

**Этап 6.**Установите антивирусную или антишпионскую программу на автоматические обновление и регулярный запуск.

Всегда получайте файлы сигнатур с веб-сайта производителя, чтобы обеспечить подлинность обновления и отсутствие повреждений, вызванных вирусами. Это может создать большую нагрузку на веб-сайт производителя, особенно при появлении новых вирусов. Чтобы избежать создания чрезмерного трафика для одного веб-сайта, некоторые производители выпускают файлы сигнатур для загрузки на нескольких сайтах. Эти сайты загрузки называются зеркалами.

**ВНИМАНИЕ!** При загрузке файлов сигнатур с зеркала убедитесь, что сайт зеркала являются легальным. Всегда переходите на сайт зеркала с веб-сайта производителя.

# Процедуры безопасности

## Методы безопасности

**Использование хэш-кода (контрольной суммы)**

Использование хэш-кода, или хэширование гарантирует отсутствие повреждения или фальсификации сообщений во время передачи. Хэширование использует математическую функцию для подсчета числового значения, которое является уникальным для передаваемых данных. Если изменить даже один символ, то результат функции, называемый контрольной суммой, будет другим. Однако это односторонняя функция. Знание контрольной суммы не позволяет злоумышленнику получить сообщение, что затрудняет перехват и изменение сообщений. Использование хэширования показано на рис. 1. Наиболее популярные алгоритмы хэширования — Secure Hash Algorithm (SHA), Message Digest 5 (MD5) и Data Encryption Standard (DES).

**Симметричное шифрование**

Для симметричного шифрования необходимо, чтобы на обеих сторонах зашифрованной связи использовался ключ для шифрования и расшифровки данных. Отправитель и получатель должны использовать одинаковые ключи. Симметричное шифрование показано на рис. 2. Примеры симметричного шифрования — DES и 3DES.

**Асимметричное шифрование**

Для асимметричного шифрования требуются два ключа, секретный и открытый. Открытый ключ может свободно распространяться, включая отправку по электронной почте в незашифрованном виде или размещение в Интернете. Секретный ключ сохраняется пользователем и не должен раскрываться другим лицам. Эти ключи могут использоваться двумя способами.

Шифрование открытым ключом используется, если одной организации необходимо получить зашифрованный текст из нескольких источников. Открытый ключ может широко распространяться и использоваться для шифрования сообщений. Предполагаемый получатель — это единственная сторона, имеющая секретный ключ, используемый для расшифровки сообщений.

При использовании цифровых подписей для шифрования сообщений требуется секретный ключ, а открытый ключ требуется для расшифровки сообщения. Этот подход позволяет получателю быть уверенным в источнике сообщения, поскольку с помощью открытого ключа может быть расшифровано только сообщение, зашифрованное с помощью исходного секретного ключа. В асимметричном шифровании используются цифровые подписи, как показано на рис. 3. RSA — наиболее популярный пример асимметричного шифрования.

# Процедуры безопасности

## Методы безопасности

Поскольку для передачи данных в беспроводных сетях используются радиоволны, злоумышленники могут просто отслеживать и собирать данные без физического подключения к сети. Злоумышленники могут получать доступ к сети, находясь в диапазоне действия незащищенной беспроводной сети. Инженеру требуется настроить соответствующий уровень безопасности на точках доступа и беспроводных сетевых платах.

При установке беспроводных служб необходимо немедленно применить методы безопасности беспроводной связи для предотвращения нежелательного доступа к сети. Для беспроводных точек доступа должны быть настроены базовые параметры безопасности, совместимые с существующей безопасностью сети.

Идентификатор набора услуг (SSID) — это имя беспроводной сети. Беспроводной маршрутизатор или точка доступа по умолчанию вещает имя сети, позволяя беспроводным устройствам обнаружить беспроводную сеть. Если вещание имени сети отключено на беспроводном маршрутизаторе или точке доступа, для подключения к беспроводной сети введите имя сети на беспроводных устройства вручную.

Для отключения вещания имени сети используйте следующий путь, как показано на рисунке.

**Wireless > Basic Wireless Settings >**(Беспроводная связь > Основные параметры беспроводной сети), выберите**Disabled** (Отключено) для вещания имени сети **> Save Settings > Continue**(Сохранить параметры > Продолжить)

Отключение вещания имени сети обеспечивает очень небольшой уровень безопасности. Если вещание имени сети отключено, все пользователи компьютеров, которым необходимо подключиться к беспроводной сети, должны ввести имя сети вручную. При поиске беспроводной сети компьютер вещает имя сети. Опытный злоумышленник может просто перехватить эту информацию и использовать ее, чтобы выдать себя за ваш маршрутизатор и перехватить учетные данные.

# Процедуры безопасности

## Методы безопасности

Фильтрация по MAC-адресам — это метод, используемый для развертывания безопасности на уровне устройств в беспроводных ЛВС. Поскольку каждое беспроводное устройство имеет уникальный MAC-адрес, беспроводные маршрутизаторы и точки доступа могут отказать в подключении к сети беспроводным устройствам, если MAC-адреса этих устройств не являются авторизованными. Для применения фильтрации по MAC-адресам введите MAC-адрес каждого беспроводного устройства.

Для настройки фильтра MAC-адресов, как показано на рисунке, выполните следующие действия:

**Этап 1.**Выберите **Wireless > Wireless MAC Filter** (Беспроводная связь > Фильтр беспроводных MAC-адресов).

**Этап 2.**Выберите **Enabled** (Включено).

**Этап 3.**Выберите **Prevent** (Запретить) или **Permit** (Разрешить), чтобы установить тип ограничения доступа.

**Этап 4.**Щелкните **Wireless Client List**(Список беспроводных клиентов).

**Этап 5.**Выберите клиент.

**Этап 6.**Щелкните **Save to MAC Address Filter List > Add > Save Settings > Continue** (Сохранить в списке фильтра по MAC-адресам> Добавить > Сохранить параметры > Продолжить).

Повторите приведенные выше действия для добавления других беспроводных клиентов к списку фильтра по MAC-адресам.

Для получения MAC-адреса интерфейсной платы беспроводной связи введите **ipconfig /all** в командной строке. MAC-адрес обозначен в выходных данных как **Physical Address**(Физический адрес). Для других устройств, отличных от компьютеров, MAC-адрес обычно напечатан на наклейке на устройстве или внутри руководства, предоставляемого производителем.

Настройка фильтрации по MAC-адресам может быть утомительным процессом, если к сети подключено множество устройств. Кроме того, при использовании фильтрации по MAC-адресам злоумышленник может прочитать MAC-адрес, используя беспроводные средства взлома. Если злоумышленнику известен MAC-адрес, он может использовать его для выдачи себя за компьютер, утвержденный через фильтрацию по MAC-адресам. Вместо этого необходимо использовать технологию стойкого шифрования.

**Процедуры безопасности**

**Методы безопасности**

Используйте систему беспроводного шифрования, чтобы зашифровать отправляемую информацию и предотвратить нежелательный перехват и использование данных. Обе стороны одного канала связи должны использовать один стандарт шифрования.

Большинство беспроводных точек доступа поддерживают несколько различных режимов безопасности. Ниже приведены наиболее распространенные из них.

* **Wired Equivalent Privacy (WEP)** — стандарт защиты для беспроводной связи первого поколения. Злоумышленники быстро обнаружили, что шифрование WEP было слишком слабым. Ключи шифрования, используемые для шифрования сообщений, могли быть обнаружены программами мониторинга. После получения этих ключей можно было просто расшифровать сообщения.
* **Wi-Fi Protected Access (WPA)** — улучшенная версия WEP. WPA охватывает весь стандарт 802.11i (уровень безопасности для беспроводных систем). В WPA используется гораздо более стойкое шифрование, чем в WEP.
* **Wi-Fi Protected Access 2 (WPA2)** — улучшенная версия WPA. В этом протоколе представлены более высокие уровни безопасности, чем в WPA. WPA2 поддерживает надежное шифрование, предоставляя безопасность правительственного уровня. WPA2 имеет две версии: Personal (проверка подлинности с помощью пароля) и Enterprise (серверная проверка подлинности).

**Дополнения к WPA и WPA2**

К стандарту WPA добавлены другие реализации безопасности.

* **Temporal Key Integrity Protocol (TKIP)** — эта технология меняет ключ шифрования для каждого пакета и предоставляет способ проверки целостности сообщений.
* **Extensible Authentication Protocol (EAP)** — для повышения безопасности используется централизованный сервер проверки подлинности.
* **Protected Extensible Authentication Protocol (PEAP)** — протокол, не использующий сервер сертификатов.
* **Advanced Encryption Standard (AES)** — метод шифрования с использованием симметричного ключа добавлен только к WPA2.

Для добавления безопасности беспроводной связи используйте следующий путь, как показано на рисунке:

**Wireless > Wireless Security >**(Беспроводная связь > Безопасность беспроводной связи), выберите **Security Mode**(Метод безопасности) **>**, выберите**Encryption Type**(Тип шифрования) **>**, введите**Pre-shared Key (Предварительный ключ) >** и установите**Key Renewal > Save Settings > Continue** (Обновление ключа > Сохранение параметров > Продолжить)

**Процедуры безопасности**

**Методы безопасности**

**Беспроводные антенны**

Диаграмма направленности приема и передачи антенны, подключенной к беспроводной точке доступа, может влиять на зону приема сигнала. Избегайте передачи сигналов за пределами области сети, установив антенну с соответствующей диаграммой направленности, обслуживающей пользователей сети.

Некоторые беспроводные устройства позволяют изменять уровень мощности радиосигнала. Это может быть выгодно в двух аспектах.

* Размер беспроводной сети может быть уменьшен, чтобы исключить возможное покрытие нежелательных областей. Используйте портативный компьютер или мобильное устройства для определения области покрытия. Уменьшайте уровень мощность радиосвязи, пока область покрытия не достигнет необходимого размера.
* Увеличьте уровень мощности в областях со множеством беспроводных сетей, чтобы минимизировать возможные помехи от других сетей и помочь заказчикам всегда оставаться на связи.

**Доступ сетевых устройства**

Многие беспроводные устройства, выпущенные определенным производителем, по умолчанию настроены с одинаковыми именами пользователей и паролями для доступа к беспроводным настройкам сети. Если оставить все без изменений, несанкционированные пользователи могут просто подключиться к точке доступа и изменить параметры. При первом подключении сетевого устройства измените имя пользователя и пароль по умолчанию. Некоторые устройства позволяют изменять имя пользователя и пароль, в то время как другие устройства позволяют изменять только пароль.

Для изменения пароля по умолчанию, как показано на рисунке, используйте следующий путь:

**Administration > Management >**(Администрирование > Управление), введите новый пароль маршрутизатора, **> Re-enter to confirm > Save Settings**(Снова введите для подтверждения > Сохранить параметры)

**Настройка защиты Wi-Fi**

Для множества пользователей настройка беспроводного маршрутизатора и ручной ввод настроек — это трудный процесс. Ранее множество пользователей просто подключали устройства и использовали параметры по умолчанию. Эти параметры обеспечивали простоту подключения устройств, но оставляли ряд брешей в безопасности, таких как отсутствие шифрования, использование имени сети по умолчанию и использование пароля администратора по умолчанию. Стандарт WPS был разработан, чтобы помочь пользователям и обеспечить простую, быструю и безопасную настройку беспроводной сети.

При использовании WPS самый распространенный способ подключения пользователя — это использование PIN-кода. При использовании PIN-кода беспроводной маршрутизатор имеет установленный производителем PIN-код, напечатанный на наклейке или отображаемый на дисплее. Если беспроводное устройство пытается подключаться к беспроводному маршрутизатору, маршрутизатор запрашивает PIN-код. После ввода пользователем PIN-кода беспроводное устройство подключается к сети, и включается безопасность.

WPS имеет значительный недостаток в безопасности. Было разработано программное обеспечение для перехвата трафика и восстановления PIN-кода WPS и предварительно согласованного ключа шифрования. Для обеспечения безопасности рекомендуется отключить WPS на беспроводном маршрутизаторе, если это возможно.

**Процедуры безопасности**

**Методы безопасности**

Аппаратный межсетевой экран — это физический компонент фильтрации, проверяющий пакеты данных из сети перед тем, как они попадут на компьютеры и другие устройства в сети. Аппаратный межсетевой экран — это отдельное устройство, которое не использует и защищает ресурсы компьютеров, тем самым не влияя на производительность обработки. Межсетевой экран может быть настроен на блокирование нескольких отдельных портов, диапазона портов или даже трафика определенного приложения. Беспроводной межсетевой экран Linksys E2500 тоже является аппаратным межсетевым экраном.

Аппаратный межсетевой экран пропускает в сеть два типа трафика:

* Ответный трафик на трафик, сгенерированный из внутренней сети.
* Трафик к порту, который намеренно оставлен открытым

Существует несколько типов настройки программных межсетевых экранов:

* **Фильтр пакетов** — пакеты могут пройти через межсетевой экран, только если они соответствует набору правил, настроенных на межсетевом экране. Фильтрация трафика может осуществляться на основе различных атрибутов, таких как IP-адрес отправителя, порт отправителя или IP-адрес или порт назначения. Фильтрация трафика также может быть выполнена на основе служб назначения или протоколов, таких как WWW и FTP.
* **Анализ пакетов с поддержкой состояния** — это межсетевой экран, отслеживающий состояние сетевых подключений, проходящих через него. Пакеты, не относящиеся к известным подключениям, удаляются.
* **Прикладной уровень** — все пакеты, исходящие от приложения или предназначенные ему, перехватываются. Весь нежелательный входящий трафик не достигает защищенных устройств.
* **Прокси** — это межсетевой экран, установленный на прокси-сервере, проверяющий весь трафик и разрешающий или отклоняющий пакеты на основе настроенных правил. Прокси-сервер — это сервер ретрансляции между клиентом и сервером назначения в Интернете.

Программные и аппаратные межсетевые экраны защищают данные и оборудование в сети от несанкционированного доступа. Помимо программного обеспечения безопасности, необходимо использовать межсетевой экран. На рис. 1 приведено сравнение программных и аппаратных межсетевых экранов.

Для настройки параметров аппаратного межсетевого экрана на Linksys E2500, как показано на рис. 2, используйте следующий путь:

**Security > Firewall >** (Безопасность > Межсетевой экран), выберите **Enable**(Включить) для защиты межсетевого экрана SPI. Затем выберите другие интернет-фильтры и веб-фильтры, необходимые для защиты сети. Щелкните**Save Settings > Continue** (Сохранить параметры > Продолжить)

**ПРИМЕЧАНИЕ**. Даже в защищенной сети для обеспечения дополнительной безопасности необходимо включить встроенный межсетевой экран операционной системы. Некоторые приложения могут правильно работать только при настройке для них межсетевого экрана.

**Демилитаризованная зона**

DMZ — это подсеть, предоставляющая службы недоверяемой сети. В DMZ часто размещаются почтовые серверы, веб-серверы или серверы FTP, тем самым трафик , используемый сервером, не отправляется из локальной сети. Это защищает внутреннюю сеть от атак с трафика из внешней сети, но никак не защищает серверы в DMZ. Трафик в DMZ и из нее часто защищается межсетевым экраном или прокси.

На Linksys E2500 можно создать DMZ для одного устройства путем пересылки трафика всех портов из Интернета на определенный IP или MAC-адрес. В DMZ может находиться сервер, игровой компьютер или веб-камера, чтобы эти устройства были доступны всем. Однако устройство в DMZ подвержено атакам хакеров через Интернет.

# Процедуры безопасности

## Методы безопасности

Аппаратные межсетевые экраны могут использоваться для блокирования портов с целью предотвращения несанкционированного доступа на вход в ЛВС и выход из нее. Однако в некоторых случаях необходимо открыть некоторые порты, чтобы определенные программы и приложения могли связываться с устройствами в различных сетях. Переадресация портов — это способ направления трафика между устройствами в различных сетях на основе правил. Этот способ обеспечивает доступность устройств из Интернета гораздо безопаснее, чем DMZ.

Когда трафик достигает маршрутизатора, маршрутизатор определяет, должен ли трафик пересылаться определенному устройству, на основе номера порта, найденного в трафике. Номера портов связаны с определенными службами, такими как FTP, HTTP, HTTPS и POP3. Правила определяют, какой трафик направляется в ЛВС. Например, маршрутизатор может быть настроен на пересылку порта 80, который связан с HTTP. Когда маршрутизатор получает пакет с портом назначения 80, он пересылает трафик серверу в сети, обслуживающему веб-страницы.

Для добавления переадресации портов, как показано на рисунке, выполните следующие действия:

**Этап 1.** Выберите **Applications & Gaming > Single Port Forwarding**(Приложения и игры > Переадресация одного порта).

**Этап 2**. Выберите или введите имя приложения. Может потребоваться ввести номер внешнегопорта, номер порта Интернета и тип протокола.

**Этап 3**. Введите IP-адрес компьютера для получения запросов.

**Этап 4**. Выберите **Enable > Save Settings > Continue** (Включить > Сохранить параметры > Продолжить).

Включение портов позволяет маршрутизатору временно переадресовывать данные через входящие порты определенному устройству. Включение портов можно использовать для переадресации данных на компьютер, только если назначенный диапазон портов используется для создания исходящего запроса. Например, видеоигра может использовать порты 27000 – 27100 для связи с другими игроками. Это запускающие порты. Клиент чата может использовать порт 56 для связи с этими же игроками, чтобы они могли общаться друг с другом. Если в этом примере существует игровой трафик на исходящем порту с диапазоном запускающих портов, входящий трафик чата на порту 56 переадресуется на компьютер, используемый для видеоигры и общения с друзьями. Когда игра завершается и запускающие порты больше не используются, порту 56 больше не будет разрешено пересылать какой-либо трафик этому компьютеру.

Чтобы добавить включение портов, выполните следующие действия:

**Этап 1**. Выберите **Applications & Gaming > Port Range Triggering**(Приложения и игры > Включение диапазона портов).

**Этап 2**. Введите **имя приложения**. Введите **starting and ending port numbers** (начальный и конечный номера портов) диапазона запускающих портов и начальный и конечный номера портов диапазона переадресованных портов.

**Этап 3**. Выберите **Enable > Save Settings > Continue** (Включить > Сохранить параметры > Продолжить).

**Процедуры безопасности**

**Защита физического оборудования**

Физическая безопасность так же важна, как и безопасность данных. При хищении компьютера также происходит кража данных. Важно ограничить доступ к помещениям с помощью заборов, замков и дверей. Защитите инфраструктуру сети, например кабели, телекоммуникационное оборудование и сетевые устройства, с помощью следующих мер:

* Защищенные телекоммуникационные комнаты, отсеки для оборудования и кожухи
* Кабельные замки и защитные винты для оборудования
* Беспроводное определение несанкционированных точек доступа
* Аппаратные межсетевые экраны
* Система управления сетью, определяющая изменения в коммутациях и коммутационных панелях

**Отключение автоматического выполнения**

Другой способ обеспечения защиты оборудования — отключение функции автоматического выполнения операционной системы. Функция автоматического выполнения следует инструкциям в специальном файле с именем autorun.inf, если он обнаруживается на новом носителе. Функция автоматического запуска отличается от автоматического выполнения. Функция автоматического запуска — удобный способ определения установки или подключения к компьютеру новых носителей, таких как оптические диски, внешние жесткие диски или флэш-накопители. Функция автоматического запуска запрашивает у пользователя выбор действия на основе содержимого нового носителя, например запустить программу, включить воспроизведение музыки или просмотр мультимедиа.

В Windows сначала запускается функция автоматического выполнения, если она не отключена. Если функция автоматического выполнения не отключена, она выполняет команды в файле autorun.inf. В Windows Vista и Windows 7 функция автоматического выполнения не может миновать функцию автоматического запуска. Однако в Windows XP функция автоматического выполнения минует функцию автоматического запуска и может запускать приложение без запроса пользователя. Это представляет угрозу безопасности, поскольку вредоносные программы могут автоматически выполняться и подвергать систему угрозам, поэтому рекомендуется отключить функцию автоматического выполнения.

Чтобы отключить функцию автоматического выполнения в Windows XP, выполните следующие действия:

**Этап 1.**Выберите **Пуск > Выполнить**.

**Этап 2.**Введите **regedit**и нажмите кнопку**ОК**.

**Этап 3.**Перейдите к**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom**.

**Этап 4.**Дважды щелкните **AutoRun**. В текстовом поле «Значение» введите**0** и нажмите кнопку **ОК**, как показано на рис. 1.

**Этап 5.**Закройте редактор реестра.

**Этап 6.**Чтобы это изменение вступило в силу, может потребоваться выйти из системы и снова войти в нее.

**Двухфакторная проверка подлинности**

Оборудование и данные компьютера могут быть защищены с использованием перекрывающихся методов защиты, чтобы предотвратить несанкционированный доступ к конфиденциальным данным. Пример перекрывающейся защиты — использование пароля и смарт-карты для защиты актива. Это называется двухфакторной проверкой подлинности, как показано на рис. 2. При выборе программы безопасности стоимость реализации должна быть сбалансирована с учетном ценности защищаемого оборудования или данных.

**Процедуры безопасности**

**Защита физического оборудования**

Защитное оборудование помогает предотвратить нарушения безопасности и потерю данных или оборудования. В число мер физического контроля доступа входят замки, видеонаблюдение и охрана. Ключ-карты защищают физические области. При утере или краже ключ-карты должна быть деактивирована только отсутствующая карта. Система ключ-карты более дорога, чем замки безопасности, но при утере обычного ключа необходимо заменить или перекодировать замок.

Сетевое оборудование должно быть смонтировано в защищенных областях. Все кабели должны находиться в трубопроводе или быть проложены в стенах для предотвращения несанкционированного доступа или повреждения. Трубопровод защищает инфраструктурные носители от повреждения и несанкционированного доступа. Неиспользуемые сетевые порты должны быть отключены.

Биометрические устройства, измеряющие физические характеристики пользователя, идеально подходят для областей с высокой безопасностью. Однако для небольших организаций этот тип решения является слишком дорогостоящим.

В политике безопасности должно определяться аппаратное обеспечение и оборудование, которое может использоваться для предотвращения краж, вандализма или потери данных. Физическая безопасность включает в себя четыре взаимосвязанных аспекта: доступ, данные, инфраструктура и физический компьютер.

Существует несколько способов физической защиты компьютерного оборудования, как показано на рис. 1 и 2:

* Использование кабельных замков для оборудования.
* Закрытие телекоммуникационных помещений.
* Оснащение оборудования защитными винтами.
* Использование защитных кожухов для оборудования.
* Отметка и установка датчиков, таких как наклейки радиочастотной идентификации, на оборудовании.
* Установка физической сигнализации с датчиками определения движения.
* Использование веб-камер с программным обеспечением определения движения и наблюдения.

Существует несколько средств защиты доступа к помещениям:

* Ключ-карты, на которых сохранены данные пользователя, включая уровень доступа
* Биометрические датчики для определения физических характеристик пользователя, таких как отпечатки пальцев и сетчатка глаза
* Охрана
* Датчики, такие как наклейки RFID, для отслеживания оборудования

Использование корпусов с замками, кабельных замков и замков для док-станций портативных компьютеров для защиты компьютеров от переноса. Использование запираемых контейнеров для переноса жестких дисков, а также надежное хранение и перевозка резервных носителей для защиты данных и носителей от хищения.

**Защита используемых данных**

Для пользователей, которым требуется доступ к конфиденциальным сетевым ресурсам, может использоваться маркер для двухфакторной проверки подлинности. Маркер может быть аппаратного типа, например PIN-карта, как показано на рис. 3, или программного типа, например программный маркер, как показано на рис. 4. Маркер назначается для компьютера и в нужные моменты создает уникальный код. Пользователь при доступе к сетевому ресурсу вводит PIN-код и номер, отображаемый маркером. Номер, отображаемый маркером, вычисляется с помощью внутренних часов и случайного числа, закодированного в маркере на заводе. Это число проверяется в базе данных, которой известен номер маркера и которая может его вычислить.

С помощью защитного экрана можно гарантировать, что посторонние не подсмотрят информацию, отображаемую на мониторе. Защитный экран представляет собой панель, часто изготовляемую из пластика. Он препятствует прохождению света при острых углах падения, поэтому экран может видеть только пользователь, смотрящий на него прямо. Например, в самолете пользователь может защитить экран портативного компьютера от лица, сидящего рядом.

**Правильное сочетание средств безопасности**

В число факторов, определяющих наиболее эффективное оборудование безопасности, используемое для защиты оборудования и данных, входят следующие:

* Способ использование оборудования
* Местоположение компьютерного оборудования
* Необходимый тип доступа пользователя к данным

Например, для компьютера в популярном общественном месте, таком как библиотека, требуется дополнительная защита от кражи и вандализма. В активно работающем центре обработки вызовов сервер должен быть установлен в закрытой комнате для оборудования. При необходимости использования портативного компьютера в общественном месте аппаратный ключ безопасности, как показано на рис. 5, обеспечивает блокировку системы, если пользователь отходит от компьютера.

**Стандартные методы профилактического обслуживания для обеспечения безопасности**

**Обеспечение безопасности**

Исправления — это обновления кода, выпускаемые производителями для предотвращения атак новых обнаруженных вирусов и червей. Периодически производители объединяют исправления и обновления в комплексные приложения обновления, которые называются пакетами обновления. Многие разрушительные атаки вирусов могли быть менее серьезными, если бы большее число пользователей загрузило и установило последний пакет обновления.

Операционная система Windows регулярно проверяет наличие на веб-сайте Центра обновления Windows высокоприоритетных обновлений для защиты компьютера от последних угроз безопасности. В число этих обновлений входят обновления безопасности, критические обновления и пакеты обновления. В зависимости от выбранного варианта Windows автоматически загружает и устанавливает высокоприоритетные обновления, необходимые компьютеру, или уведомляет о наличии таких обновлений.

Обновления должны быть установлены, а не только загружены, как показано на рисунке. При использовании режима «Автоматически» можно запланировать день и время. В противном случае по умолчанию новые обновления устанавливаются в 3 часа ночи, если компьютер включен или находится в энергосберегающем режиме. Если компьютер выключен во время запланированного обновления, обновления устанавливаются при следующем запуске компьютера. Также можно выбрать, чтобы Windows уведомляла о доступности нового обновления, для его последующей самостоятельной установки.

В свете постоянно меняющихся угроз безопасности инженеры должны знать, как устанавливать обновления и исправления. Они должны узнавать о наличии новых обновлений и исправлений. Некоторые производители выпускают обновления в один и тот же день каждого месяца, а критические обновления — при возникновении необходимости. Другие производители предоставляют службы автоматического обновления для обновления программного обеспечения при каждом включении компьютера или уведомления о выпуске новых обновлений и исправлений по электронной почте.

Чтобы установить пакет обновления или исправление безопасности в операционной системе, выполните следующие действия:

**Этап 1.**Перед установкой обновления создайте точку восстановления.

**Этап 2.**Проверьте наличие обновлений, чтобы убедиться в том, что располагаете их новейшими версиями.

**Этап 3.**Загрузите обновления, используя функцию автоматического обновления или посетив веб-сайт производителя операционной системы.

**Этап 4.**Установите обновление.

**Этап 5.**При необходимости перезагрузите компьютер.

**Этап 6.**Убедитесь в правильности работы компьютера.

По умолчанию Windows автоматически загружает и устанавливает обновления операционной системы. Однако обновления могут противоречить политике безопасности организации или другим параметрам компьютера. Следующие параметры Windows позволяют установить время обновления программного обеспечения:

* **Автоматически —**автоматическая загрузка и установка обновлений без участия пользователя.
* **Only download updates** (Только загружать обновления) — обновления загружаются автоматически, но устанавливаются пользователем.
* **Notify me** (Уведомлять) — пользователь получает уведомление о доступности обновлений и имеет возможность загрузить и установить их.
* **Turn off automatic updates**(Отключение автоматического обновления) — проверка наличия обновлений не выполняется.

Для настройки Центра обновления Windows перейдите по следующему пути:

**Пуск > Все программы > Центр обновления Windows > Изменить параметры**

Если пользователь находится в сети коммутируемого доступа, использование Центра обновления Windows должно быть отключено или он должен быть настроен на уведомление о доступных обновлениях. Пользователю с коммутируемым доступом может потребоваться управлять обновлением, выбрав время, когда обновление не мешает другим сетевым действиям или использует доступные ограниченные ресурсы.

В корпоративной среде в политиках управления исправлениями указывается загрузка и автономное тестирование обновлений до развертывания на отдельных компьютерах в сети.

**Стандартные методы профилактического обслуживания для обеспечения безопасности**

**Обеспечение безопасности**

Можно выполнить резервное копирование Windows вручную или запланировать частоту автоматического резервного копирования. Для успешного резервного копирования и восстановления данных в Windows требуются соответствующие права и разрешения пользователя.

* Все пользователи могут выполнять резервное копирование собственных файлов и папок. Они также могут выполнять резервное копирование файлов, на которые у них имеется разрешение на чтение.
* Все пользователи могут восстанавливать файлы и папки, на которые у них имеется разрешение на запись.
* Члены группы администраторов, операторы архива и операторы сервера (если присоединены к домену) могут выполнять резервное копирование и восстановление всех файлов независимо от назначенных разрешений. По умолчанию члены этих группы имеют права на резервное копирование и восстановление файлов и каталогов.

Для первого запуска мастера резервного копирования файлов Windows 7 перейдите по следующему пути:

**Пуск** **> Все программы > Обслуживание >** **Резервное копирование и восстановление >Настройка архивации**

Чтобы изменить параметры архивации в Windows 7 после завершения работы мастера резервного копирования файлов, перейдите по следующему пути:

**Пуск** **> Все программы > Обслуживание >** **Резервное копирование и восстановление >Изменить параметры > Изменить параметры архивации файлов > Продолжить**

Чтобы восстановить резервную копию файла в Windows 7, перейдите по следующему пути:

**Пуск** **> Все программы > Обслуживание** **>** **Резервное копирование и восстановление** **>Восстановить мои файлы**

Чтобы запустить мастер резервного копирования файлов Windows Vista, перейдите по следующему пути:

**Пуск** **> Все программы > Обслуживание >** **Центр архивации и восстановления** **>** **Архивировать файлы**

Чтобы изменить параметры резервного копирования, перейдите по следующему пути:

**Пуск** **> Все программы > Обслуживание >** **Центр архивации и восстановления** **>** **Изменить параметры > Изменить параметры архивации файлов > Продолжить**

Чтобы восстановить резервную копию файла в Windows Vista, перейдите по следующему пути:

**Пуск** **> Все программы > Обслуживание** **>** **Центр архивации и восстановления** **>** **Восстановить файлы**

Файлы резервных копий в Windows 7 или Windows Vista имеют расширение .zip. Архивированные данные автоматически сжимаются, и каждый сжатый файл должен иметь размер не более 200 МБ. Можно сохранить файлы резервных копий Windows 7 и Windows Vista на жестком диске, на записываемом носителе или на другом компьютере или сервере, подключенном к сети. Резервная копия может быть создана только из раздела NTFS. Целевой жесткий диск должен иметь файловую систему NTFS или FAT.

**ПРИМЕЧАНИЕ**. В мастере резервного копирования и восстановления Windows 7 и Windows XP можно исключить каталоги вручную. Эта возможность не поддерживается в мастере резервного копирования файлов Windows Vista.

Чтобы запустить мастер резервного копирования и восстановления Windows XP, перейдите по следующему пути:

**Пуск** **> Все программы > Стандартные > Служебные** **> Архивация данных**

Запустится мастер резервного копирования и восстановления. Чтобы изменить параметры резервного копирования, перейдите по следующему пути:

**Пуск** **> Все программы > Стандартные > Служебные** **> Архивация данных > Расширенный режим > Сервис > Параметры**

Чтобы восстановить файл резервной копии в Windows XP с помощью мастера резервного копирования и восстановления, перейдите по следующему пути:

**Далее > Восстановление файлов и параметров > Далее**. Выберите файл резервной копии и нажмите кнопки **Далее > Готово**

Мастер резервного копирования и восстановления и другие приложения для архивации позволяют выполнять некоторые из следующих типов резервного копирования:

Файлы мастера резервного копирования и восстановления Windows XP имеют расширение .bkf. Можно сохранить файл .bkf на жестком диске, диске DVD или на любом другом записываемом носителе. Исходное местоположение и целевой диск могут иметь файловую систему NTFS или FAT.

В Windows XP можно выполнить операции резервного копирования из командной строки или с помощью пакетного файла, используя команду **NTBACKUP**. Параметры по умолчанию для команды**NTBACKUP** установлены в программе резервного копирования Windows XP. Параметры, которые необходимо переопределить, должны быть указаны в командной строке. Можно восстановить файлы из командной строки, используя команду **NTBACKUP**.

В Windows 7 и Windows Vista используйте команду **WBADMIN**. Можно использовать резервные копии, созданные с помощью команды**NTBACKUP** в Windows XP, и восстанавливать их с помощью команды**WBADMIN** в Windows 7 и Windows Vista. Для восстановления копий из Windows XP в Windows 7 или Windows Vista загрузите специальную версию команды**NTBACKUP** Microsoft.

Сочетание типов резервного копирования позволяет эффективно архивировать данные. Типы резервного копирования описаны на рисунке. Резервное копирование данных занимает некоторое время, поэтому рекомендуется выполнять его при низкой загрузке компьютера и сети.

**Стандартные методы профилактического обслуживания для обеспечения безопасности**

**Обеспечение безопасности**

Межсетевой экран выборочно отклоняет трафик, предназначенный компьютеру или сегменту сети. Межсетевые экраны работают путем открытия и закрытия портов, используемых различными приложениями. Запрещающая политика безопасности реализуется путем открытия только тех портов, которые необходимы. Отклоняются все пакеты, не имеющие явного разрешения. В отличие от этого разрешающая политика безопасности разрешает доступ к портам, за исключением явно закрытых портов. В прошлом программное обеспечение и оборудование поставлялись с разрешительными параметрами. Поскольку пользователи пренебрегали настройкой своего оборудования, разрешительные параметры, установленные по умолчанию, открывали злоумышленникам доступ к множеству устройств. Теперь большинство устройств по возможности поставляются с запрещающими параметрами и с возможностью простой настройки.

Настройка брандмауэра Windows 7 или Windows Vista может быть выполнена двумя способами:

* **Автоматически** — пользователю выдается предложение**Блокировать**, **Разблокировать** или**Отложить** несанкционированные запросы. Эти запросы могут исходить из допустимых приложений, которые не были настроены ранее, или от вирусов и червей, заразивших систему.
* **Управление параметрами безопасности** — пользователь вручную добавляет программу или порты, необходимые приложениям для использования в сети.

Чтобы предоставить программам доступ через брандмауэр Windows в Windows 7, перейдите по следующему пути:

**Пуск > Панель управления > Брандмауэр Windows > Разрешить запуск программы или компонента через брандмауэр Windows > Разрешить другую программу**

Чтобы предоставить программам доступ через брандмауэр Windows в Windows Vista, перейдите по следующему пути:

**Пуск > Панель управления > Центр безопасности > Брандмауэр Windows > Изменить параметры > Продолжить > Исключения > Добавить программы**

Чтобы предоставить программам доступ через брандмауэр Windows в Windows XP, перейдите по следующему пути:

**Пуск > Панель управления > Центр безопасности > Брандмауэр Windows > Исключения > Добавить программы**

Чтобы отключить брандмауэр Windows в Windows 7, перейдите по следующему пути:

**Пуск > Панель управления > Брандмауэр Windows > Включение и отключение брандмауэра Windows > Отключить брандмауэр Windows (не рекомендуется) > OК**

Чтобы отключить брандмауэр Windows в Windows Vista, перейдите по следующему пути:

**Пуск > Панель управления > Центр безопасности > Брандмауэр Windows > Включение и отключение брандмауэра Windows > Продолжить > Выключить (не рекомендуется) > ОК**

Чтобы отключить брандмауэр Windows в Windows XP, перейдите по следующему пути:

**Пуск > Панель управления > Центр обеспечения безопасности > Брандмауэр**

# Стандартные методы профилактического обслуживания для обеспечения безопасности

## Обеспечение безопасности

Сотрудникам организации часто требуются различные уровни доступа к данным. Например, руководитель или бухгалтер могут быть единственными сотрудниками организации с доступом к платежным ведомостям.

Сотрудники могут группироваться по требованиям к работе, и им может предоставляться доступ к файлам в соответствии с разрешениями группы. Этот процесс помогает управлять доступом сотрудников к сети. Для сотрудников, которым требуется кратковременный доступ, можно настроить временные учетные записи. Точное управление сетевым доступом помогает ограничить области уязвимости, которые могут быть использованы вирусами или вредоносным программным обеспечением для проникновения в сеть.

**Прекращение доступа сотрудников**

Когда сотрудник уходит из организации, его доступ к данным и оборудованию сети должен быть немедленно прекращен. Если бывший сотрудник имеет сохраненные файлы в личном месте на сервере, необходимо закрыть доступ, отключив учетную запись. Если новому сотруднику, заменившему прежнего, требуется доступ к приложению и личному месту для хранения данных, можно снова настроить учетную запись и изменить имя на имя нового сотрудника.

**Гостевые учетные записи**

Временным сотрудникам и гостям может потребоваться доступ к сети. Например, посетителям может потребоваться доступ к электронной почте, Интернету и принтеру в сети. Эти ресурсы могут быть предоставлены с помощью специальной учетной записи, которая называется гостевой. При наличии гостей им может быть назначена гостевая учетная запись. При отсутствии гостей учетная запись может быть отключена до появления новых гостей.

Для некоторых гостевых учетных записей требуется расширенный доступ к ресурсам, например для консультантов или финансового аудитора. Этот тип доступа должен предоставляться только на время выполнения работы.

Для настройки всех пользователей и групп на компьютере введите**lusrmgr.msc** в поле «Поиск» или запустите служебную программу командной строки.



