Резервное копирование и восстановление данных

Выполнил :обучающийся группы № 23

Шабалин В.Ю

Проверила: Турусинова И. П

Содержание

- Резервное копирование
- Основы резервного копирования файловых ресурсов
- Типы резервного копирования файлов
- Обратные изменения
- Точки мгновенного восстановления
- Планирование архивации данных
- Выбор архивных устройств и носителей
- Хранение резервной копии
- Резервная копия состояния системы
- Учетные записи пользователей
- Настройка Антивируса Dr.Web

Резервное копирование

Резервное копирование (англ. backup) — процесс создания копии данных на носителе, предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

Причины потери информации:

- аппаратные сбои устройств;
- действия вредоносных программ и вирусов;
- ошибки пользователей.

Наиболее часто делают резервные копии:

- файлов с важными документами;
- баз данных;
- состояния операционной системы.

Основы резервного копирования файловых ресурсов

В практически любой файловой системы существуют механизмы облегчающие резервное копирование.

При резервном копировании файлов используются их свойства – атрибуты. Наиболее часто используется атрибут, хранящий дату и время последнего изменения файла, а также (характерно для ОС семейства Windows) специальный атрибут «Архивный».

При любом изменении файла дата последнего изменения меняется на текущую, и для файла устанавливается атрибут «Архивный».

Для резервного копирования используют специальное ПО, часто встроенное поставляемое с ОС.

Типы резервного копирования файлов

- Нормальный
- Добавочный
- Разностный
- Зеркальное копирование

Нормальный (normal)

- Архивируются все файлы, отмеченные для архивации. В Windows при этом у всех заархивированных файлов очищается атрибут «архивный».
- необходим для создания полных резервных копий каких-либо больших файловых ресурсов. компании или организации имеются достаточные ресурсы, то можно ежедневно осуществлять полное архивирование данных.
- Для восстановления информации на момент нормального копирования достаточно восстановить последний сделанный архив.

Добавочный (Incremental)

- Из файлов, отмеченных для архивирования, архивируются файлы, измененный с момента последнего по времени добавочного или нормального копирования (для Windows – те, которые имеют атрибут «архивный», при этом данный атрибут очищается).
- В случае утери информации для восстановления данных потребуется сначала восстановить данные из последней Нормальной копии, а затем последовательно из всех Добавочных копий, созданных после Нормальной.

Разностный (Differential)

- Из файлов, отмеченных для архивирования, архивируются только те, которые были изменены с момента последнего нормального архива (для Windows – имеют атрибут архивный, при этом после копирования атрибут не сбрасывается). Использование Обычного и Разностного архивирования позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий.
- В случае утери информации требуется выполнения двух операций восстановления — сначала восстановление Нормальной копии, а затем из последней Разностной резервной копии.

Зеркальное копирование (Copy)

- Архивируются все файлы, отмеченные для архивации, вне зависимости от атрибутов и без их изменения. В Windows при этом у всех заархивированных файлов не очищается атрибут «архивный».
- Данный вид архивирования необходим для создания полных резервных копий каких-либо больших файловых ресурсов. Для восстановления информации на момент Зеркального копирования достаточно восстановить последний сделанный архив, при этом план резервного копирование не меняется.

Обратные изменения (reverse delta)

- Хранится разница между текущими версиями отмеченных для архивирования файлов и их предыдущими состояниями. После сохранения полной резервной копии периодически составляются списки последних изменений содержимого файлов.
- В зависимости от стратегии может быть аналогичен разностному или добавочному копированию, с разницей в том, что хранятся не целиком файлы, а лишь изменения в них. Процесс восстановления аналогичен разностному или добавочному копированию.

Точки мгновенного восстановления

- Резервные копии создаются не по расписанию, а путем создания автоматической копии, после каждого изменения данных.
- Когда данные записываются на диск, они также асинхронно записываются в другой точке, обычно ей служит другой компьютер поверх сети. Это вносит определенную нагрузку на операции записи диска, но устраняет необходимость расписания созданий резервных копий.
- Позволяет восстановить данные на любой момент вре

Планирование архивации данных

Выбор стратегии резервного копирования зависит от следующих факторов:

- какие именно ресурсы будут архивироваться;
- минимальный промежуток времени для восстановления данного ресурса при возникновении аварии;
- какой объем данных будет архивироваться;
- какова емкость носителей для хранения резервных копий и скорость записи на эти носители;
- сколько времени будет занимать архивирование каждого ресурса;
- как часто будет производиться архивация каждого ресурса;
- если резервные копии записываются на ленты, то как часто будет производиться перезапись лент;
- по какому графику будет производиться тестовое восстановление данных.

Выбор архивных устройств и носителей

Определив, какие данные и как часто архивировать, можно выбрать аппаратные средства архивации и необходимые носители.

Выбор подходящего оборудования для организации зависит от многих факторов:

- Емкость.
- Надежность аппаратных средств и носителей.
- Расширяемость решения.
- Скорость архивации и восстановления.
- Цена архивации.

Хранение резервной копии

- Ленточные накопители;
- магнитные диски (резервное копирование на дискеты ZIP, JAZ, MO);
- оптические накопители (компакт-диски);
- съемные или стационарные дисковые накопители;
- флэш-накопители;
- копия в «облаке» - запись резервных данных по «облачной» технологии через онлайн-службы специальных провайдеров.

Резервная копия состояния системы

В Windows предусмотрена возможность создания специальной резервной копии, которая позволит восстановить работоспособность и все настройки операционной системы в случае потери данных или прекращения функционирования.

При этом архивируются следующие данные:

- системный реестр;
- база данных зарегистрированных классов объектов;
- системные загрузочные файлы;
- база данных служб сертификатов (только на серверах, на которых установлена служба сертификатов);
- база данных Active Directory и папка SYSVOL (на контроллерах доменов).

Учетные записи пользователей

Учетная запись

Применение учетной записи

Типы учетных записей

Преимущества записей

Учетная запись

Учётная запись, содержит сведения, необходимые для идентификации пользователя при подключении к системе, информацию для авторизации и учёта.

Это имя пользователя и пароль (или другое аналогичное средство аутентификации — например, биометрические характеристики) .

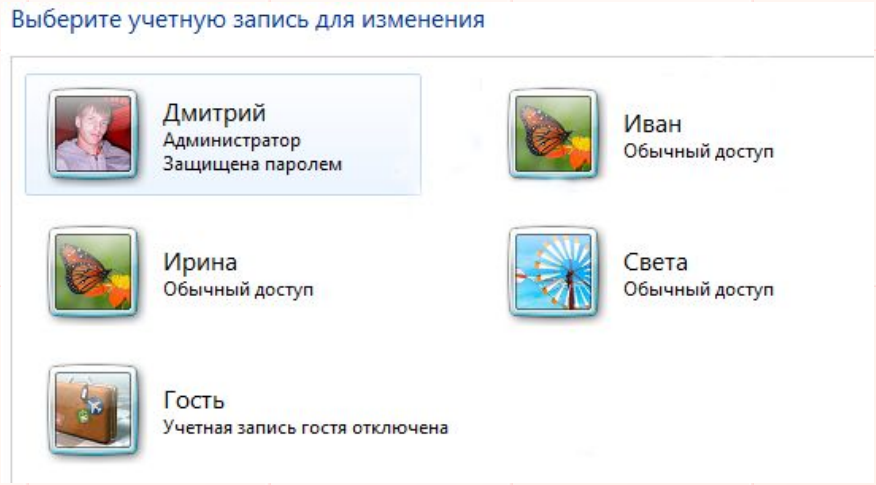
Пароль или его аналог, хранится в зашифрованном или хешированном виде (в целях его безопасности) .

Применение учетной записи

- Применение учетных записей позволяет нескольким пользователям работать на одном компьютере с использованием собственных файлов и параметров.
- Для доступа к учетной записи используется имя пользователя и пароль.
- Пользователи могут воспринимать учётную запись как личную страничку, профиль, кабинет, место хранения личных и других сведений на определённом Интернет-ресурсе.

Типы учетных записей

- обычные учетные записи пользователей предназначены для повседневной работы;
- учетные записи администратора предоставляют полный контроль над компьютером и применяются только в необходимых случаях;
- учетные записи гостя предназначены для временного доступа к компьютеру.

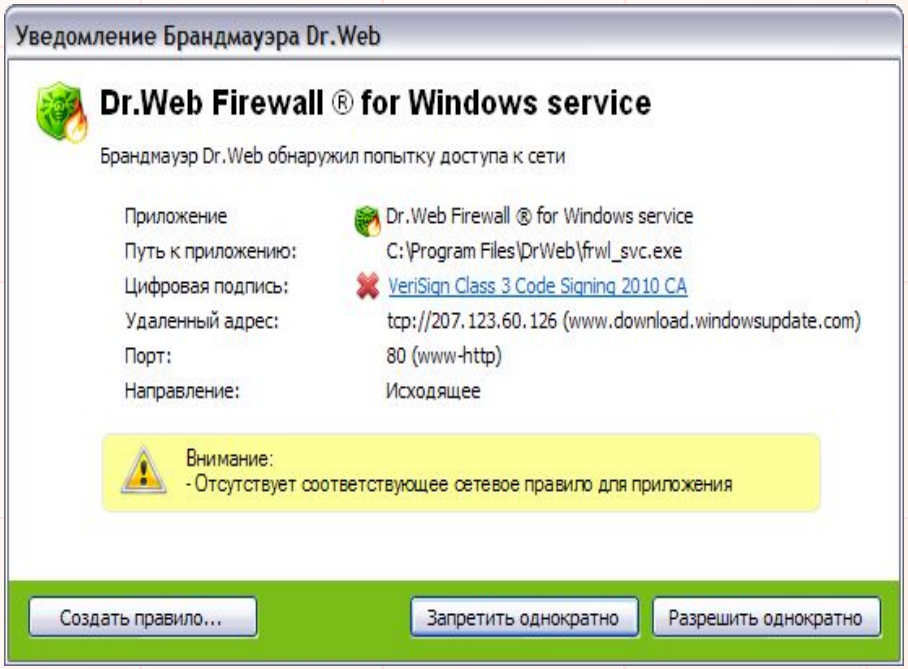


Преимущества записей

- Защита от ошибочных действий
- Конфиденциальность
- Родительский контроль
- Общий контроль

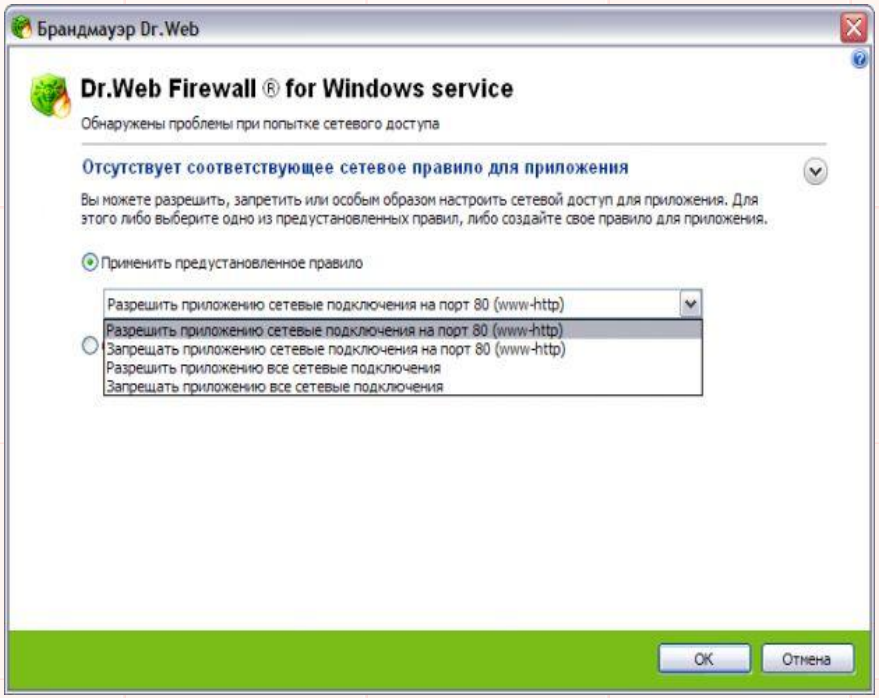
Настройка Антивируса Dr.Web

Антивирус уведомит вас о блокировании приложения, желающего вырваться во внешний мир, и предложит создать для него правило. Для этого нажмите одноименную кнопку «Создать правило» в окне с уведомлением.



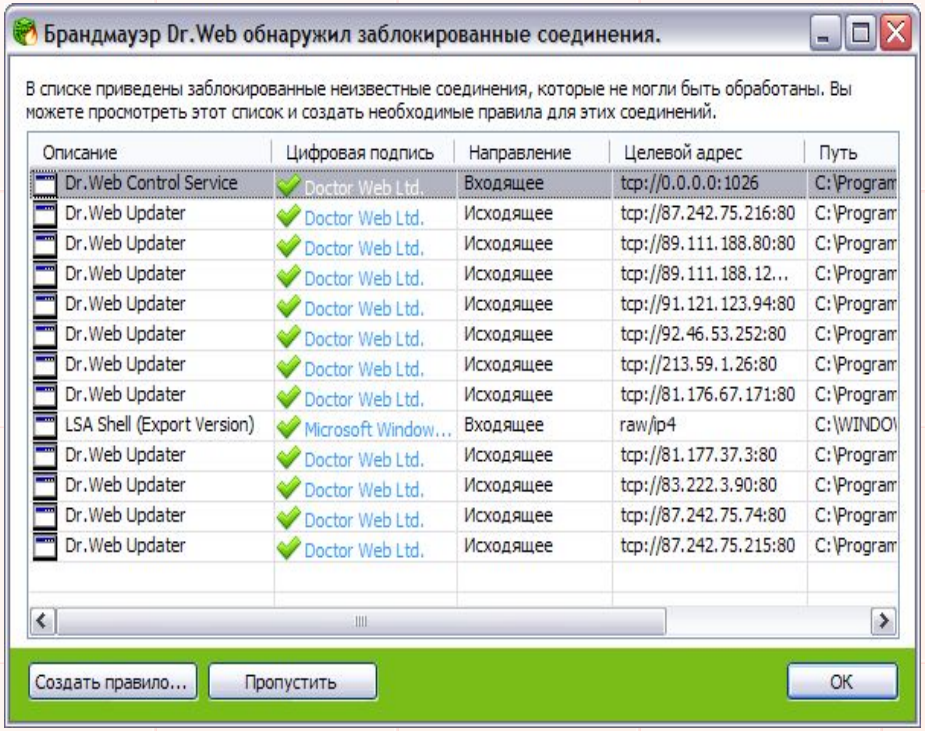
Настройка Антивируса Dr.Web

«Применить предустановленное правило» и выберите правило из списка. Для добропорядочных приложений это будет «Разрешить приложению сетевые подключения….», а далее - нюансы настроек для конкретной программы. Если вас эти нюансы не беспокоят, можете дать программе абсолютную свободу выхода в сеть, выбрав пункт «Разрешать приложению все сетевые подключения».



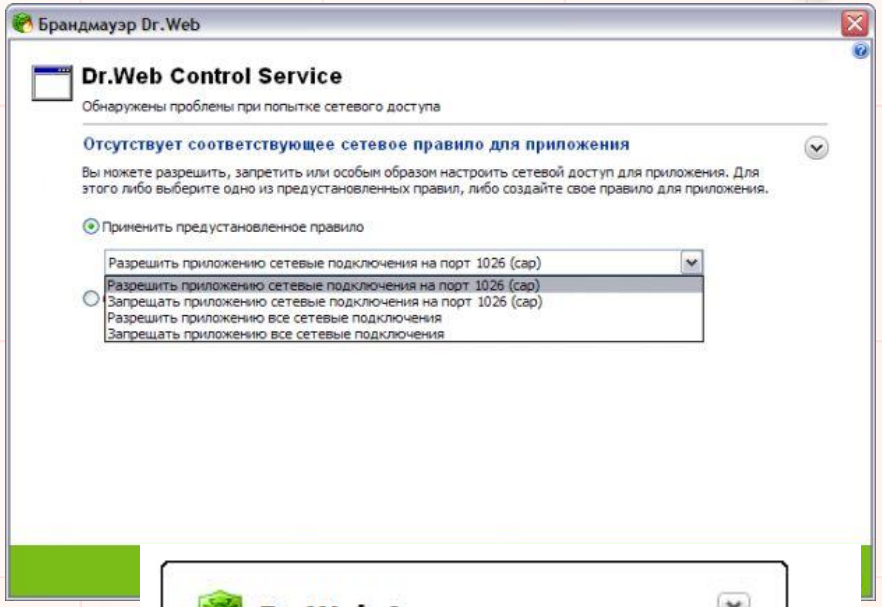
Настройка Антивируса Dr.Web

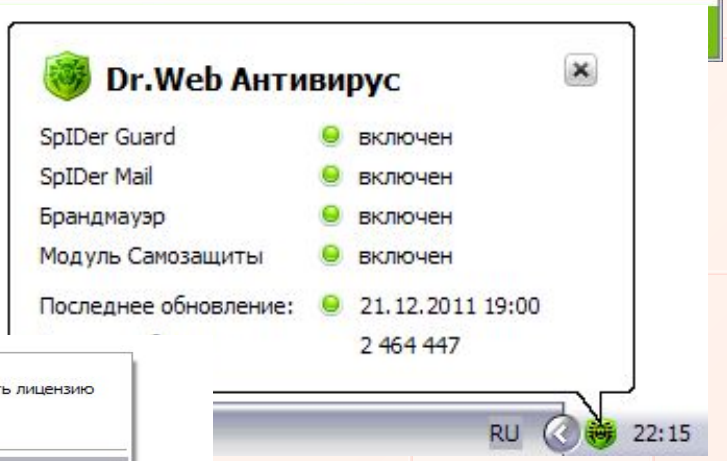
Список заблокированных страдальцев может быть довольно внушителен. Выделите каждый пункт в этом списке и нажмите кнопку «Создать правило».



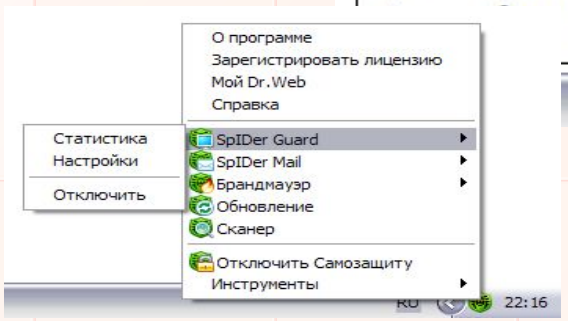
Настройка Антивируса Dr.Web

Разобравшись с первичной настройкой Брандмауэра Dr.Web, попробуем посмотреть состояние антивируса. Для этого наведите курсор мыши на иконку симпатичного зеленого паучка в трее. Все модули антивируса должны быть включены, а антивирусные базы иметь свежую дату обновления



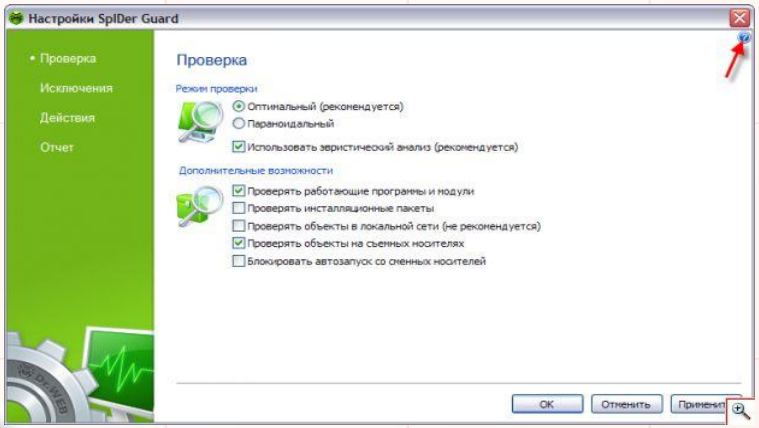


Кликнув правой кнопкой мыши по той же иконке, вы увидите контекстное меню программы. Здесь можно изменить настройки любого модуля, просто наведя на него курсор мыши и выбрав пункт «Настройки».

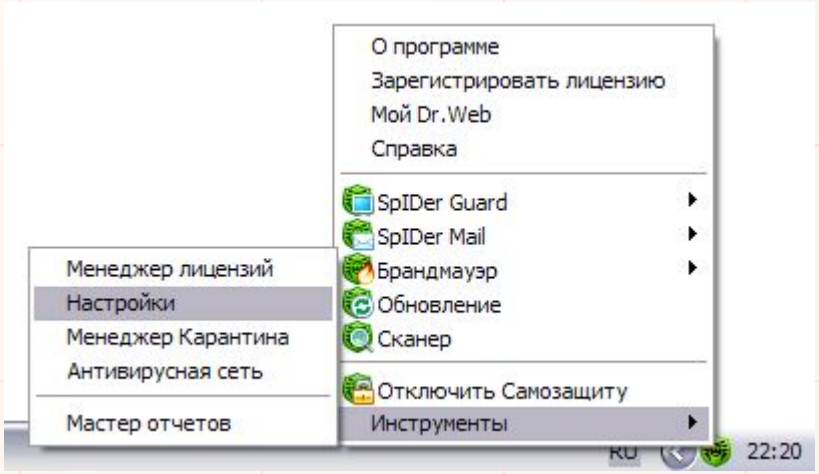


Настройка Антивируса Dr.Web

В качестве примера взглянем на параметры файлового монитора SpIDer Guard. Все опции выставлены в оптимальном режиме. Если же вы решите изменить параметры, прежде ознакомьтесь со справочными материалами выбранного раздела настроек, кликнув по иконке «Справка» в правом верхнем углу окна.



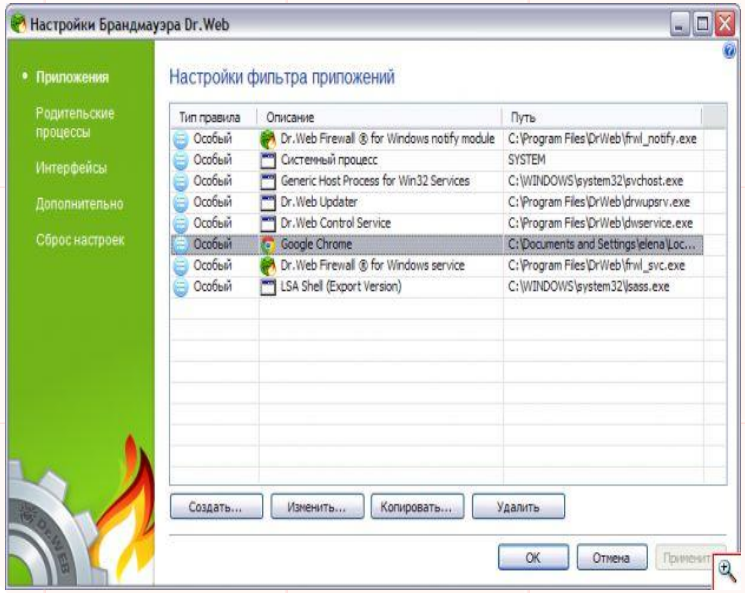
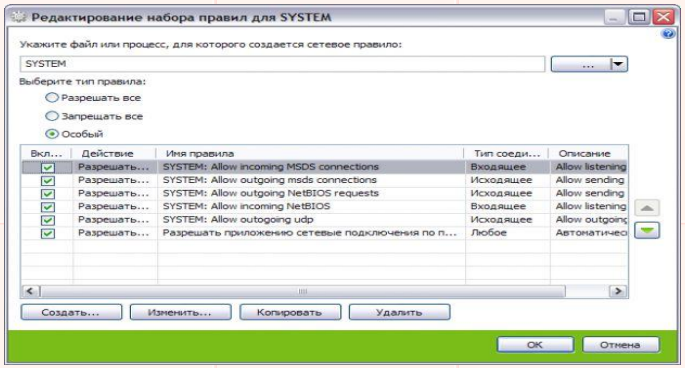
Для изменения общих настроек антивируса зайдите в меню «Инструменты» - «Настройки».



В разделе «Приложения» будет представлен список программ, которым требуется выход в сеть. Для того чтобы изменить правила для приложения, достаточно дважды кликнуть по нему.

Настройка Антивируса Dr.Web

Для того чтобы изменить то или иное правило, также дважды кликните по нему мышью.



- Настройки сетевых правил для программы включают стандартные параметры:
- Имя правила – наименование правила для программы;
- Описание – краткая информация о правиле;
- Состояние – применяется правило или нет;
- Тип соединения – входящее (из сети на ваш компьютер) или исходящее (с вашего компьютера в сеть);