Услуга «Антивирус Dr.Web»

для

Содержание

Введение

Заблуждение №1

Современные вирусные угрозы

Вирусы пишут хакеры-одиночки

Раньше создателями вредоносного ПО действительно были программисты-одиночки. Современные вредоносные программы разрабатываются вирусописателями-профессионалами, и это хорошо организованный криминальный бизнес, вовлекающий в свою преступную деятельность высококвалифицированных системных и прикладных разработчиков ПО.

Структурные элементы некоторых преступных сообществ

В ряде случаев роли злоумышленников внутри преступных сообществ могут быть разделены следующим образом:

1. Организаторы — лица, которые организовывают и руководят процессом создания и использования вредоносного ПО. Использование вредоносного ПО может происходить как непосредственно, так и путем его продажи другим преступникам или их объединениям.
2. Участники:
   - Разработчики вредоносного ПО.
   - Тестировщики созданного ПО (оно тестируется в том числе и на предмет его детектирования известными антивирусными программами).
   - Исследователи уязвимостей в операционных системах и прикладном ПО в преступных целях.
   - «Специалисты» по использованию вирусных упаковщиков и шифрованию.
   - Распространители вредоносного ПО, специалисты по социальной инженерии.
   - Системные администраторы, обеспечивающие распределенную безопасную работу внутри преступного сообщества и управление бот-сетями.

Внимание!

Физическое лицо, воспользовавшееся вредоносным ПО (разработанным на заказ или скаченным из Интернета), т. е. компьютерной программой либо иной компьютерной информацией, заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, также является преступником и несет уголовную ответственность согласно ч. 1 ст. 273 УК РФ.

Благодаря четкой организации криминальных групп, занимающихся разработкой и распространением вирусов, производство вирусов было поставлено на поток, что обеспечило взрывной рост числа создаваемых злоумышленниками вредоносных программ. Это не замедлило сказаться на количестве ежедневных сигнатурных записей, добавляемых в вирусные базы.

Факты

- Служба вирусного мониторинга Dr.Web производит сбор образцов вирусов по всему миру.
- Ежесуточно в антивирусную лабораторию «Доктор Веб» поступает в среднем не менее 60 000 образцов вредоносных программ.
- 28 ноября 2012 года был поставлен своеобразный «рекорд» — на анализ поступило более 300 000 образцов. И это далеко не все, что создается за сутки вредоносного.

Вирусные аналитики — не волшебники, и мгновенно обработать многие тысячи ежедневно поступающих подозрительных файлов не могут. Поэтому важнейшим элементом противодействия вредоносным программам становятся автоматизированные системы обработки входного потока подозрительных файлов. Качество работы этих систем имеет не меньшее значение, чем качество работы коммерческих продуктов, работающих на компьютерах пользователей.

Антивирус должен обнаруживать 100% вирусов

Предыстория возникновения заблуждения

В антивирусной отрасли давно существуют т. н. сравнительные тестирования на обнаружение, которые проводят независимые тестеры. Для таких тестов берется коллекция вирусов и вредоносных программ, антивирусы обновляются до актуального состояния и прогоняются по коллекции. Чтобы победить в тесте, надо обнаружить 100% вирусов из коллекции.

Особенностями этих тестирований является то, что:

- ни один тестировщик не может гарантировать, что в его коллекции только вредоносные программы;
- такие тесты показывают только одну из функций антивируса — обнаружение (детектирование) угроз;
- в таких тестах оценивается качество только одного компонента из множества компонентов антивируса — файлового монитора или сканера — т. е. тестируется борьба антивируса с **известными** угрозами;
- такие тесты не показывают, насколько хорошо ведет себя антивирус в реальных условиях заражения компьютера вирусом, как он умеет тот или иной вирус лечить;
- такие тесты не показывают, умеет ли антивирус обнаруживать **неизвестные** угрозы.

Именно такие тесты и породили это опасное заблуждение.

Факты

- Технологически сложные и особо опасные вирусы, в том числе руткиты, создаются для извлечения коммерческой выгоды. Вирусописатели проверяют их на обнаружение всеми антивирусами, перед тем как выпустить такой вирус в «живую природу». Ведь им необходимо, чтобы вирус действовал на инфицированной машине как можно дольше. Если вирус легко обнаружить — это плохой вирус, с точки зрения его создателей. Именно поэтому до поступления образцов вредоносных программ в антивирусную лабораторию многие из них не обнаруживаются антивирусом.
- Вирус может проникнуть на компьютер через уязвимости нулевого дня (т. н. 0day exploits — уязвимость, о которой пока известно только вирусописателю или для исправления которой производитель ПО пока еще не выпустил «заплатку»), либо с использованием методов социальной инженерии — т. е. будет запущен самим пользователем, который в том числе может отключить самозащиту антивируса.

Антивирусы ловят вирусы по сигнатурам (записям в вирусных базах)

Если бы это было так, антивирус был бы беспомощен перед лицом неизвестных угроз.

Однако антивирус не перестал быть лучшим и единственным эффективным средством защиты от всех типов вредоносных угроз — и что особенно важно — как **известных**, так и **неизвестных** вирусной базе антивируса.

В продуктах Dr.Web для обнаружения и обезвреживания неизвестного вредоносного ПО применяется множество эффективных несигнатурных технологий, сочетание которых позволяет обнаруживать новейшие (неизвестные) угрозы до внесения записи в вирусную базу. Остановимся лишь на некоторых из них.

- **Технология Fly-Code** — обеспечивает качественную проверку упакованных исполняемых объектов, распаковывает любые (даже нестандартные) упаковщики методом виртуализации исполнения файла, что позволяет обнаружить вирусы, упакованные даже неизвестными антивирусному ПО Dr.Web упаковщиками.
- **Технология Origins Tracing** — при сканировании исполняемого файла он рассматривается как некий образец, построенный характерным образом, после чего производится сравнение полученного образа с базой известных вредоносных программ. Технология позволяет с высокой долей вероятности распознавать вирусы, еще не добавленные в вирусную базу Dr.Web.
- **Технология анализа структурной энтропии** — обнаруживает неизвестные угрозы по особенностям расположения участков кода в защищенных криптоупаковщиками проверяемых объектах.
- **Технология ScriptHeuristic** — предотвращает исполнение любых вредоносных скриптов в браузере и PDF-документах, не нарушая при этом функциональности легитимных скриптов. Защищает от заражения неизвестными вирусами через веб-браузер. Работает независимо от состояния вирусной базы Dr.Web совместно с любыми веб-браузерами.
- **Традиционный эвристический анализатор** — содержит механизмы обнаружения неизвестных вредоносных программ. Работа эвристического анализатора опирается на знания (эвристики) об определенных особенностях (признаках) вирусов — как характерных именно для вирусного кода, так и наоборот, крайне редко встречающихся в вирусах. Каждый из таких признаков характеризуется своим «весом» — числом, модуль которого определяет важность, серьезность данного признака, а знак, соответственно, указывает на то, подтверждает он или опровергает гипотезу о возможном наличии неизвестного вируса в анализируемом коде.
- **Модуль эмуляции исполнения** — технология эмуляции исполнения программного кода необходима для обнаружения полиморфных и сложношифрованных вирусов, когда непосредственное применение поиска по контрольным суммам невозможно либо крайне затруднено (из-за невозможности построения надежных сигнатур). Метод состоит в имитации исполнения анализируемого кода эмулятором — программной моделью процессора (и, отчасти, компьютера и ОС).

Факты

- У антивируса Dr.Web — рекордно малое число вирусных записей в базе, поэтому всего одна запись в вирусной базе Dr.Web позволяет определять десятки, сотни и даже тысячи подобных вирусов. Принципиальное отличие вирусной базы Dr.Web от вирусных баз других программ в том, что даже при меньшем числе записей она позволяет детектировать такое же (и даже большее) число вирусов и вредоносных программ.
- Даже если записи о вирусе нет в вирусной базе Dr.Web, он с большой долей вероятности будет обнаружен благодаря использованию многочисленных технологий, применяемых в антивирусном ядре.
- Устройство антивирусных баз Dr.Web таково, что при добавлении новых записей скорость проверки не снижается!

Что дают пользователю малый размер базы Dr.Web и меньшее, чем у конкурентов, число записей в ней?

- Экономия места на диске.
- Экономия оперативной памяти.
- Экономия трафика при обновлении баз.
- Высокая скорость анализа вирусов.
- Возможность определять вирусы, которые появятся в будущем путем модификации уже существующих версий.

Внимание!

Миллионы людей в мире ежедневно пользуются уникальным продуктом Dr.Web CureIt!, созданным специально для лечения зараженных вирусами компьютеров, на которых работают другие антивирусные продукты.

Так вирусов же давно нет!

Действительно, свыше 90% современных угроз вирусами в строгом понимании этого термина назвать нельзя, т. к. они не имеют механизмов саморепликации (самостоятельного размножения без участия пользователя). Подавляющее количество современных угроз — это троянские программы. Они относятся к категории вредоносных программ и могут нанести серьезный ущерб владельцу инфицированного компьютера.

Опасные троянцы:

1. Не видны ни пользователю, ни некоторым антивирусным программам.
2. Способны похищать конфиденциальную информацию, в том числе пароли, данные для доступа к банковским и платежным системам, денежные средства с банковских счетов.
3. Могут загружать другие вредоносные программы и даже вывести операционную систему из строя.
4. Могут полностью парализовать работу компьютера по команде злоумышленника.

Такие программы на момент создания чаще всего не обнаруживаются антивирусами. Более того, некоторые из них предпринимают попытки удаления антивируса.

Внимание!

Никакое другое программное обеспечение, **кроме антивируса**, не способно вылечить систему от уже проникшего троянца.

Факты

До 70% случаев заражений локальных сетей компаний, изолированных от сети Интернет, происходят из-за инфекций на съемных носителях — люди собственноручно переносят троянцев на флешках.

Действие вируса на компьютере всегда заметно. Если мой компьютер будет заражен, я сразу это пойму и приму меры

Факты

- Современные вредоносные программы зачастую действуют незаметно для пользователя и даже не определяются на момент их создания многими антивирусными программами.
- Задачей современных вирусописателей является создание вредоносного ПО, которое должно как можно дольше оставаться в системе необнаруженным — как со стороны пользователя системы, так и специальными программами (антивирусами).
- Например, **Trojan.Carberp**, созданный для хищений денежных средств, запускаясь на инфицированной машине, предпринимает целый ряд действий для того, чтобы обмануть средства контроля и наблюдения. После успешного запуска троянец внедряется в другие работающие приложения, а свой основной процесс завершает. Таким образом, вся его дальнейшая работа происходит частями, внутри сторонних процессов.

Миф о том, что появление любого вируса можно заметить, изжил себя окончательно.

Даже если произойдет заражение компьютера, дешевле восстановить Windows из резервной копии, чем покупать антивирус

Угроза

Вредоносная программа может скрываться в файлах, хранящихся на других разделах жесткого диска и съемных носителях. В этом случае переустановка Windows ничего не даст: при обращении к такому файлу вредоносное ПО активизируется снова.

Внимание!

Антивирус является единственным программным средством, способным вылечить компьютер от проникшего в него вируса.

Даже если у вас нет резервной копии каждой рабочей станции — не проблема! Если до установки Dr.Web ваша система оказалась заражена, Dr.Web вылечит ее, и компьютер снова будет работать нормально. Для лечения активного заражения достаточно выполнить быструю проверку компьютера, и все найденные угрозы будут нейтрализованы. Лечение даже нескольких компьютеров в сети займет меньшее время, чем восстановление системы из резервной копии! При этом выполняется:

- лечение зараженных файлов;
- автоматическое исправление реестра Windows;
- автоматическое удаление вредоносных служб;
- автоматическое удаление руткитов и буткитов.

Основной источник заражения вирусами — электронная почта

Факты

Основные источники заражения вирусами корпоративной сети (в порядке убывания количества случаев заражений):

- личные / домашние ПК / ноутбуки / мобильные устройства сотрудников;
- ноутбуки / мобильные устройства клиентов;
- съемные устройства — а это не только флешки!
- легитимные (необходимые для выполнения должностных обязанностей и поэтому неблокируемые) сайты, инфицированные злоумышленниками;
- фишинговые и специально созданные вредоносные сайты;
- электронная почта;
- уязвимости операционных систем и прикладного ПО.

Время «собирать камни»

В истории антивирусной индустрии был период, когда программисты в разных странах почему-то решили, что могут создавать программы с громким названием «антивирус». В 1994 году широкое распространение полиморфного вируса Phantom-1, который не мог обнаруживать ни один антивирус, кроме Dr.Web, расставило всех по своим местам и выбросило на свалку отрасли бесполезные антивирусные поделки.

В июле 2001 года разразилась эпидемия CodeRed. Оказалось, что только один антивирус в мире — Dr.Web — был способен обнаружить этот вирус в памяти компьютера. Даже сейчас лишь немногие антивирусы умеют лечить подобные угрозы.

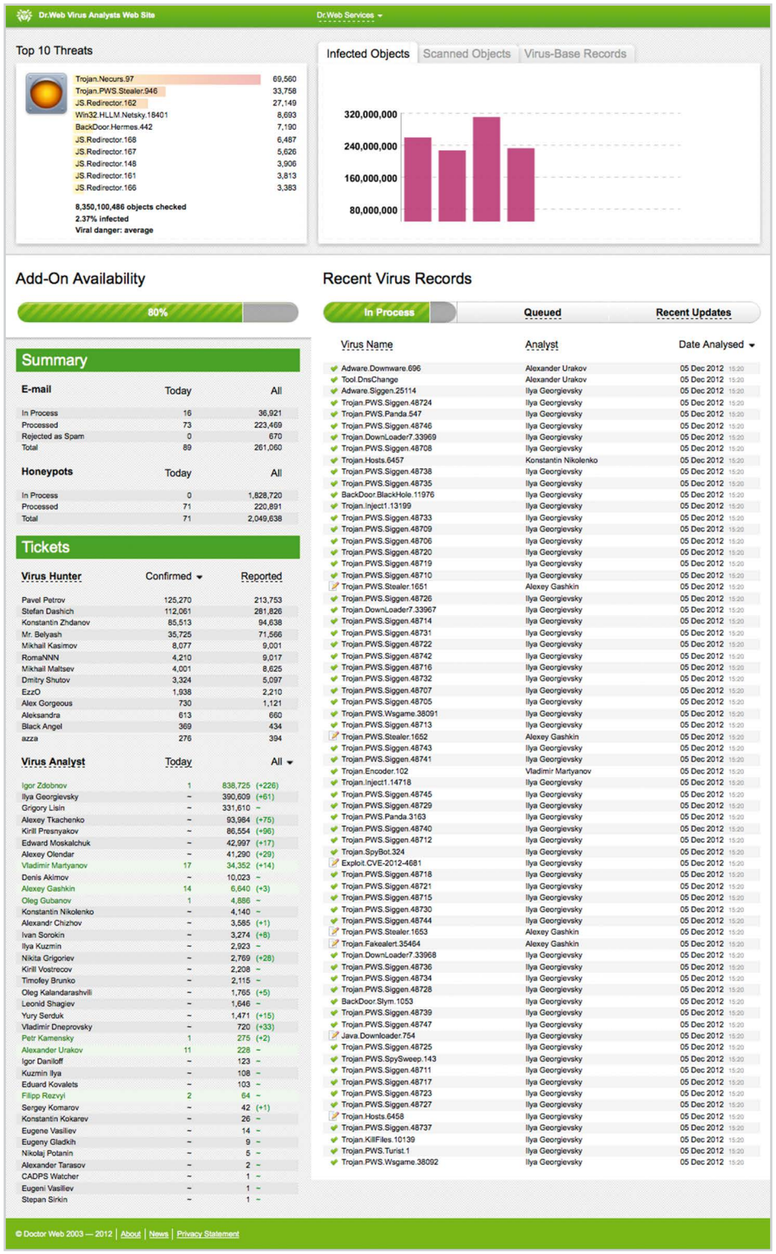
И вот сегодня, похоже, антивирусная отрасль еще раз готова очиститься, сбросить балласт. В будущем на рынке останутся только те немногие антивирусы, которые:

- будут определять и обезвреживать вирусы не только по сигнатурам и эвристическим технологиям — т. е. будут обладать функционалом, позволяющим не пропускать вредоносный объект внутрь системы, даже если его сигнатура еще не добавлена в вирусную базу;
- будут иметь непробиваемую систему самозащиты — чтобы не позволить вывести себя из строя новому неизвестному вирусу, какими-то путями пробравшемуся в систему;
- будут способны качественно очищать системы от проникшей вредоносной программы в условиях, когда эта программа активна, сопротивляется, препятствует обнаружению и действует во вред пользователю — иными словами, **лечить систему в реальных условиях**, успешно восстанавливать ее работоспособное состояние, т. к. только в условиях реального заражения и проверяется качество антивирусных технологий;
- будут располагать системой сбора информации, позволяющей максимально быстро передавать в антивирусную лабораторию всю необходимую для решения проблемы информацию;
- будут иметь мощную инфраструктуру разработки, собственную службу вирусного мониторинга, антивирусную лабораторию и службу поддержки пользователей;
- будут способны моделировать новые виды угроз раньше вирусописателей и использовать технологии борьбы с ними (которые точно будут несигнатурными).

Все эти качества уже есть у современного антивируса Dr.Web.

Всегда живой, всегда открытый

http://live.drweb.com — это открытый ресурс, который показывает работу антивирусной лаборатории «вживую». Там вы увидите, как обрабатываются поступающие экземпляры вредоносных программ и какие вирусы на данный момент наиболее распространены.



Введение

Безопасность — это услуга

Антивирусное ПО используется на всех участках бизнеса — в процессе управления предприятием, при ведении бухгалтерского и финансового учета, на производстве. Эффективный антивирус способствует обеспечению бесперебойности бизнес-процессов предприятия и является одним из самых главных факторов, влияющих на снижение совокупной стоимости владения ИТ-инфраструктурой в целом.

Как показывает практика, из всего спектра продукции антивирусных фирм небольшие и средние компании в большинстве своем используют только персональные продукты.

Какой антивирус чаще всего приобретает предприятие? Самый лучший на рынке? Тот, что более всего подходит к специфическим условиям предприятия? Вовсе нет! Покупается лицензия на тот антивирус, с которым умеет работать его системный администратор. Причем многие функции программного обеспечения могут просто не использоваться из-за незнания либо об их существовании, либо о том, как их использовать. В итоге информационная безопасность предприятия становится заложником субъективной оценки и квалификации администратора.

Серьезным фактором, затрудняющим реализацию задачи эффективного функционирования ИТ-инфраструктуры предприятия, является нехватка системных администраторов, способных грамотно управлять системой информационной защиты предприятия, что требует специальных знаний, которые отсутствуют у большинства ИТ-администраторов. Это создает угрозы для информационной безопасности компании и в итоге значительно повышает совокупную стоимость владения антивирусом, приводит к проблемам в исполнении требований законодательства в части информационной безопасности.

Особенно остро эта проблема стоит для малых и средних предприятий. Как правило, системные администраторы там либо приходящие (обслуживают сразу несколько компаний), либо недостаточно квалифицированные. Снижение зависимости предприятия от этих факторов — важная задача, стоящая перед руководством.

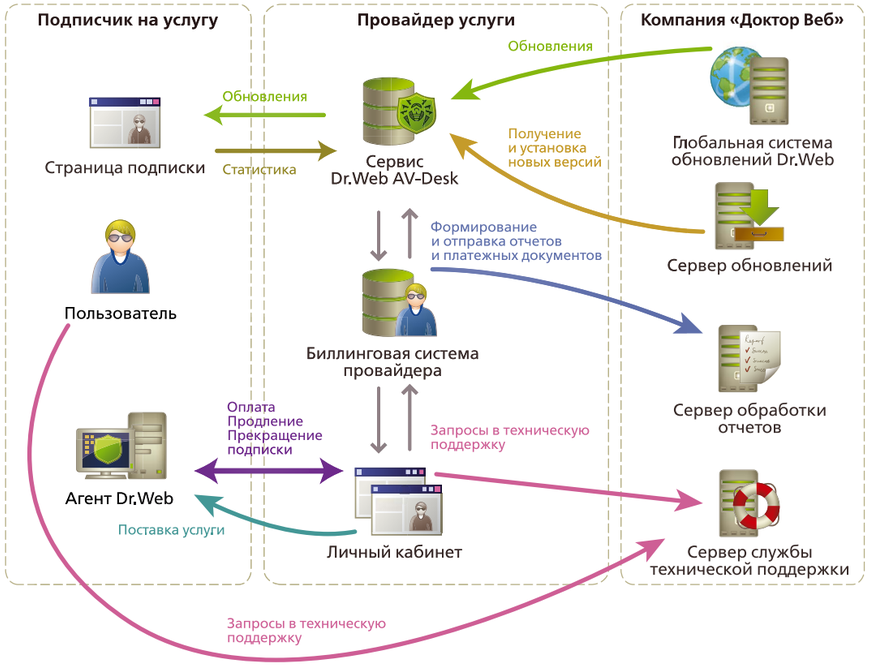
ПО как услуга (Software as a service)

Software as a service (SaaS) — давно и широко используемая за пределами России модель предоставления программного обеспечения в качестве услуги.

В России до 2007 года ее использование в антивирусной отрасли сдерживалось банальным отсутствием отечественных решений подобного класса. С выпуском в мае 2007 года интернет-сервиса Dr.Web AV-Desk, разработанного российской компанией «Доктор Веб», на рынке ИТ-услуг России появился новый сегмент — сегмент услуг антивирусной защиты.

Поставщиками таких услуг являются провайдеры ИТ-услуг, установившие у себя интернет-сервис Dr.Web AV-Desk, с помощью которого они оказывают услугу по защите компаний от интернет-угроз — «Антивирус Dr.Web».

Как это работает?



1. Поставщик услуги «Антивирус Dr.Web» устанавливает ПО интернет-сервиса Dr.Web AV-Desk на своих серверах и организует подписку на услугу «Антивирус Dr.Web».
2. Клиенты оформляют подписку, производят установку ПО Dr.Web, самостоятельно управляют параметрами подписки.
3. «Доктор Веб» обеспечивает поставщика услуги актуальными обновлениями вирусных баз и программных модулей Dr.Web, оказывает техническую поддержку поставщикам и подписчикам услуги.
4. Поставщик взимает с клиентов плату за пользование услугой, мониторит состояние антивирусной сети, поставляет подписчикам обновления вирусных баз, собирает статистическую информацию о вирусных заражениях.

Использование услуги «Антивирус Dr.Web» позволит компаниям построить антивирусную систему защиты в соответствии с требованиями российского законодательства. Услуга способна обеспечить выполнение требований Федерального закона № 152-ФЗ «О персональных данных» в части антивирусной защиты. Поэтому вам не придется нанимать специалиста по информационной безопасности, труд которого стоит дорого в условиях острой нехватки достаточного количества специалистов такого класса.

Если в компании нет штатного системного администратора

Решить задачу эффективного обеспечения безопасности в условиях дефицита квалифицированных системных администраторов позволяет использование антивируса Dr.Web в качестве услуги через поставщика ИТ-сервисов.

- Ваше предприятие будет обеспечено квалифицированным администрированием процесса информационной защиты.
- Специалисты поставщика услуги — это профессионалы, сертифицированные компанией «Доктор Веб», которые обладают полными знаниями об администрируемом продукте и максимально используют эти знания для управления информационной защитой.
- Обеспечивается неукоснительное соблюдение политик безопасности на всех защищаемых объектах предприятия — путем частичного ограничения возможности персонала вмешиваться в настройки или полного запрета возможности таких изменений.
- Благодаря квалифицированному управлению услугой, грамотной реакции на вирусные угрозы и профессиональным действиям специалистов поставщика по восстановлению работоспособности сети после вирусных атак непредвиденные расходы снижаются до минимума, в том числе за счет отсутствия затрат на серверное оборудование и наем высокооплачиваемых профессионалов в области информационной защиты.

Внешнее администрирование услуги «Антивирус Dr.Web» — это гарантия высокой надежности функционирования ИТ-инфраструктуры и непредвзятого анализа вирусного состояния сети предприятия.

Антивирусная система защиты Dr.Web

Заблуждение №8

Компоненты антивирусной системы защиты

Централизованное управление антивирусной системой защиты

Если в вашей компании есть штатный или приходящий системный администратор, поставщик услуги может передать ему функции управления антивирусной системой защиты через Центр управления. Это обеспечит предприятие еще большими возможностями по управлению информационной защитой антивирусной сети.

Продукты enterprise-класса с центром управления стоят дороже однопользовательских версий. Их управление крайне сложное, что требует найма специалиста по информационной безопасности.

Факты

Поставка серверных продуктов Dr.Web enterprise-класса по модели SaaS позволила существенно снизить стоимость таких продуктов и сделать их доступными для потребителей. Центр управления в составе услуги «Антивирус Dr.Web»:

1. Лицензируется бесплатно.
2. С его управлением справится специалист любой квалификации.
3. Максимально автоматизирует работу по защите локальной сети при минимальных затратах на сопровождение, т. к. настройки для всех станций или групп станций производятся в 2–3 клика и так же легко могут быть изменены, если необходимо.

Использование возможностей Центра управления услуги «Антивирус Dr.Web» способствует бесперебойной работе компании и в итоге минимизирует расходы на бизнес-процедуры.

Соответствие российскому законодательству

Использование Центра управления услуги «Антивирус Dr.Web» обеспечивает соответствие системы антивирусной защиты предприятия Федеральному закону № 152-ФЗ «О персональных данных» в части централизованного управления антивирусной системой защиты.

Федеральный закон № 152-ФЗ «О персональных данных»

Наличие централизованной комплексной защиты требуется подзаконными актами регуляторов Федерального закона № 152-ФЗ.

Выдержки из Приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»:

«2.4. При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с методами и способами, указанными в пункте 2.1 настоящего Положения, основными методами и способами защиты информации от несанкционированного доступа являются:

<...> **централизованное управление** системой защиты персональных данных информационной системы».

Центр управления в составе услуги «Антивирус Dr.Web» позволяет управлять защитой:

- рабочих станций Windows и Mac OS X,
- файловых серверов Windows,
- мобильных устройств Android.

Удобство и реальная экономия средств

- Центр управления услуги «Антивирус Dr.Web» — это возможность единого «взгляда сверху» на всю антивирусную сеть предприятия любого масштаба с одного рабочего места.
- Центр управления сокращает до минимума время на обслуживание системы, позволяет оперативно управлять системой защиты локальной сети в любой момент времени, из любой точки мира, с компьютера под управлением любой операционной системы просто через браузер и без необходимости установки дополнительного программного обеспечения.
- Наличие удобного веб-интерфейса позволяет централизованно устанавливать, обновлять и настраивать компоненты антивирусной системы защиты, включать компьютеры в «мобильном» режиме.
- При его использовании снижается нагрузка на локальные станции за счет сжатия сетевого трафика и шифрования данных — они станут работать продуктивней, исчезнут жалобы персонала на якобы тормозящий антивирус.

Гарантия высокого уровня информационной безопасности предприятия

Централизованное управление антивирусной системой защиты в составе услуги «Антивирус Dr.Web» позволяет:

- реализовать необходимые для конкретного предприятия политики безопасности — без необходимости настройки защиты на каждой отдельной рабочей станции;
- гарантировать невозможность отключения антивируса или его отдельных компонентов персоналом, что неизбежно повлекло бы снижение уровня защиты;
- гарантировать работу антивируса с теми настройками, которые задал администратор сети;
- планировать и удаленно запускать регулярные сканирования — как по команде администратора, так и по расписанию;
- контролировать регулярность обновлений и невозможность их отключения;
- собирать и анализировать информацию о состоянии антивирусной системы защиты, а также создавать отчеты за необходимый период времени;
- уведомлять администраторов и пользователей о состоянии системы защиты;
- оперативно реагировать на возникающие проблемы вирусного характера, что, в свою очередь, снизит риск заражения сети и финансовых потерь компании из-за простоя сотрудников, потери данных, отключения от Интернета, заражения партнеров по бизнесу.

Внимание!

- Невозможность перехвата трафика и его подмены обеспечивает безопасное администрирование любого количества рабочих станций — вне зависимости от того, в какой точке мира они находятся.

Прокси-сервер

Услуга «Антивирус Dr.Web» может предоставляться даже в случае использования сложной топологии сети, например, если антивирусные агенты не имеют прямого доступа к серверу услуги (серверу Dr.Web AV-Desk) и между ними отсутствует маршрутизация пакетов (логически изолированная от Интернета внутренняя локальная сеть).

Для организации прямого доступа в этом случае предоставляется отдельный компонент антивирусной сети — прокси-сервер. Прокси-сервер можно использовать также для значительного снижения сетевого трафика (оптимизация трафика) и уменьшения времени получения обновлений антивирусными агентами, поскольку он поддерживает кеширование обновлений и компонентов антивирусных агентов.

Использование технологии сжатия трафика (опция на сервере услуги) не является препятствием для использования прокси-сервера. Обработка пересылаемой информации осуществляется вне зависимости от того, сжимается трафик или нет.

Внимание!

В состав антивирусной сети может входить как один, так и несколько прокси-серверов.

Установка по сети (удаленная установка)

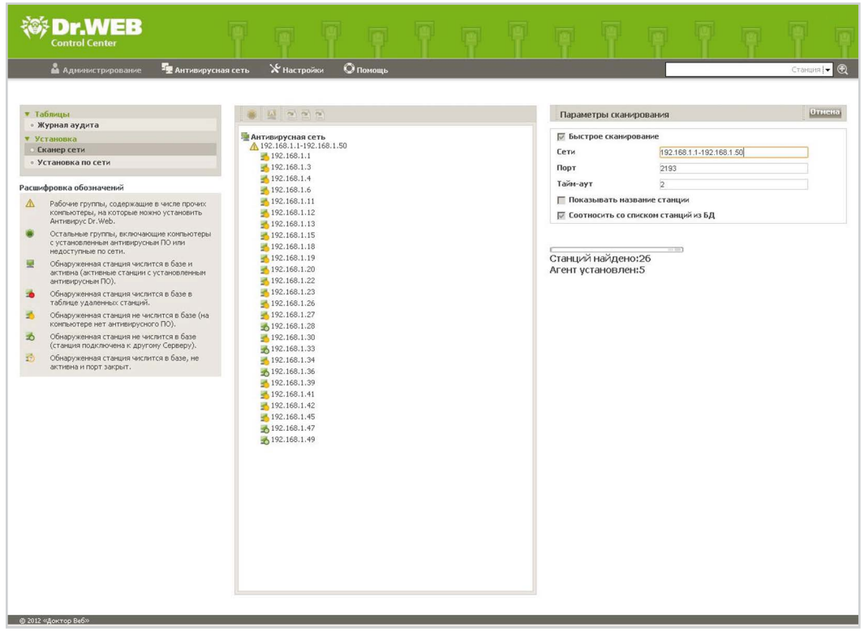
Услуга «Антивирус Dr.Web» обладает всеми преимуществами продуктов enterprise-класса с централизованным управлением антивирусной системы защиты. Одним из таких преимуществ является возможность выявления компьютеров в рамках локальной сети, на которых отсутствует антивирусная защита, и возможность удаленной установки Dr.Web на незащищенные компьютеры.

Удаленная установка возможна как в случае, если рабочая станция входит в домен под учетной записью администратора, так и в случае, если удаленная станция не входит в домен или используется локальная учетная запись.

Внимание!

В случае если удаленная станция не входит в домен или используется локальная учетная запись на удаленном компьютере, для некоторых версий операционных систем MS Windows необходимо произвести ряд настроек. Это описано в Руководстве администратора.

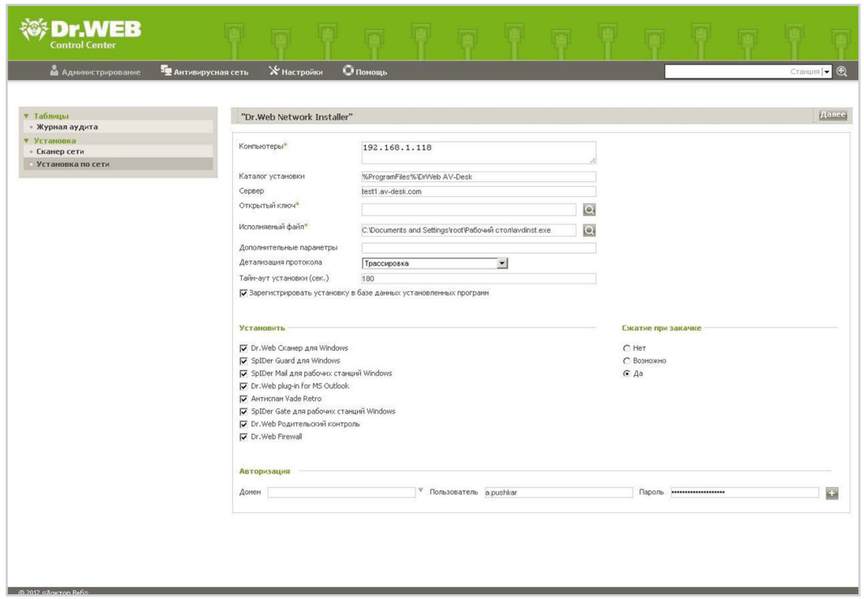
В состав Центра управления услугой «Антивирус Dr.Web» входит Сканер сети, который осуществляет поиск компьютеров по IP-адресам в рамках локальной сети, результатом работы которого будет иерархический список компьютеров с указанием, на каких из них установлено антивирусное ПО, а на каких нет.



Установка может осуществляться как на один, так и на несколько незащищенных компьютеров путем формирования соответствующего задания в панели инструментов.

Внимание!

Удаленная установка возможна СТРОГО в маршрутизируемых сетях.



Администраторы системы

Если в компании есть штатный системный администратор, или если компания использует услуги внешнего администратора, он может самостоятельно управлять антивирусной системой защиты Dr.Web через удобный и дружественный Центр управления, самостоятельно принимать и реализовывать решения по соблюдению политик безопасности, оперативно реагировать на вирусозависимые инциденты — т. е. иметь все рычаги влияния на информационную безопасность компании.

Типы администраторов

- **Администратор групп с полными правами** — сотрудник имеет доступ к Центру управления и может оперировать любыми настройками системы. Таким администратором рекомендуется назначить либо руководителя предприятия (если предприятие небольшое, у него нет системного администратора и руководитель совмещает функцию управляющего антивирусной системы защиты), либо системного администратора, уполномоченного должностной инструкцией администрировать антивирусную систему защиты.

Внимание!

Если компания использует услуги внешнего администратора, необходимо тщательно взвесить, можно ли ему в этом объеме делегировать управление системой антивирусной защиты, т. к. данная роль дает полный контроль над системой.

- **Администратор групп с полными правами (только чтение)** — сотрудник имеет доступ к Центру управления, может получать статистику работы системы, но не может менять что-либо в настройках. Такой ролью можно наделить сотрудника, уполномоченного вести анализ статистики работы системы и проводить аудиты системы безопасности.
- **Администратор групп с ограниченными правами** — сотрудник имеет доступ к Центру управления и может оперировать любыми настройками в рамках прав, разрешенных ему администратором групп с полными правами, за исключением функций управления подписками (создание/приостановка/возобновление/удаление). Данная роль полезна 1) для клиентов поставщиков услуги «Антивирус Dr.Web» на аутсорсинге и 2) для администраторов абонентов поставщиков услуг доступа. Если групп несколько, каждой группе может быть назначен свой администратор.

Важно!

Для назначения администраторов системы вам должен быть предоставлен доступ к соответствующему функционалу — обратитесь за этим к вашему поставщику услуги.

Группы. Управление группами

В средних и крупных компаниях для облегчения управления защитой используется механизм группирования, что обеспечивает услуге «Антивирус Dr.Web» исключительную масштабируемость. Группирование позволяет:

- создавать группы, объединять защищаемые станции в группы, добавлять/удалять станции из группы;
- применять различные политики безопасности для различных групп (допустим, для группы Бухгалтерия может быть назначено задание запрета отмены обновлений, а для группы Менеджеры могут отсутствовать жесткие ограничения на использование сети Интернет);
- задавать одной командой задания для всех защищаемых станций группы, а также инициировать выполнение на них заданий;
- устанавливать для разных групп индивидуальные графики обновлений и сканирований, что позволит распределять нагрузку на сеть;
- составлять отчеты по группам;
- отсылать оповещения — на отдельные станции, отдельные группы или все группы.

Если у компании более 15 подписок на услугу «Антивирус Dr.Web», имеет смысл создать группы в системе антивирусной защиты и применить разные политики безопасности для этих групп, используя многообразные настройки Центра управления.

Системный администратор имеет возможность расширить или ограничить права по управлению агентами — отдельным пользователям, группе пользователей или всем группам пользователей:

- разрешить самостоятельно изменять настройки;
- частично ограничить возможность изменения настроек;
- полностью запретить изменение настроек;
- управлять набором компонентов Dr.Web, установленных на компьютерах пользователей;
- устанавливать/удалять компоненты на ПК пользователей;
- запускать задания на защищаемых станциях;
- принудительно обновлять давно не обновлявшиеся агенты;
- принудительно запускать сеансы сканирования на защищаемых станциях в фоновом режиме.

Тарифные пакеты и компоненты защиты Dr.Web

Подписка на услугу производится в виде тарифных пакетов. В состав каждого тарифного пакета входят компоненты для защиты рабочих станций, файловых серверов Windows и мобильных устройств.

Выбирайте тарифные пакеты, исходя из реальной производственной необходимости, требований к информационной защите и текущей финансовой ситуации предприятия.

	Dr.Web Классик Минимально необходимая защита от вирусов	Dr.Web Премиум Комплексная защита от интернет-угроз
Защита рабочих станций		
ОС Windows	8/7/Vista/XP/2000 SP4	
Mac OS X	10.10-10.15	
Антивирус, антишпион, антируткит	✔	✔
Антиспам		✔
Веб-антивирус		✔
Родительский контроль		✔
Брандмауэр	✔	✔
Защита файловых серверов		
ОС Windows		Windows Server 2003/2008
Все компоненты защиты Dr.Web Премиум	✔	
Защита мобильных устройств		
ОС Android		1.6/2.0/2.1/2.2/2.3/ 3.0/3.1/3.2/4.0/4.1
Антивирус	✔	✔
Антивор		✔
Антиспам		✔
Базовая техническая поддержка		
Обновления вирусных баз	✔	✔
Обновления программных модулей Dr.Web	✔	✔
Количество обращений в техническую поддержку	Не ограничено	
Другие сервисы		
Бесплатный переход на другой тарифный пакет	✔	✔
Приостановка подписки (на 1, 2 или 3 месяца)	✔	✔

От каких угроз защищает услуга «Антивирус Dr.Web»?

	Dr.Web Классик	Dr.Web Премиум
Вирусы	✔	✔
Троянские программы	✔	✔
Клавиатурные шпионы	✔	✔
Программы — похитители паролей	✔	✔
Шпионское ПО (spyware)	✔	✔
Руткиты	✔	✔
Потенциально опасное ПО (riskware)	✔	✔
Полиморфные вирусы	✔	✔
Почтовые черви	✔	✔
Программы-люки	✔	✔
Программы-шутки	✔	✔
Программы платного дозвона	✔	✔
Хакерские утилиты	✔	✔
Спам		✔
Фишинг		✔
Фарминг		✔
Скамминг		✔
Технический спам		✔
Похищение конфиденциальной информации		✔
Киберпреступность, направленная против детей		✔
Несанкционированный доступ по сети	✔	✔

Только антивирус сегодня уже не панацея!

Почему только антивируса недостаточно? Ведь еще недавно все было не так!

Внимание!

Сегодняшняя антивирусная система защиты не равна вчерашнему файловому антивирусу.

Современная антивирусная система защиты среди прочего обязана включать в себя:

- эффективный антиспам — так как спам является одним из основных переносчиков вредоносного ПО;
- средства фильтрации HTTP-трафика для защиты от проникновений вредоносных кодов с интернет-страниц;
- систему ограничения доступа к сменным носителям и внутрисетевым ресурсам (Офисный контроль);
- персональный брандмауэр.

Внимание!

Данный функционал есть только в тарифном пакете Dr.Web Премиум.

При правильном использовании данных компонентов (с соблюдением рекомендаций данной брошюры) исключена необходимость закупок дополнительных продуктов с аналогичными возможностями. Это позволяет реализовать систему антивирусной защиты в условиях ограниченного бюджета.

Лучший опыт

- Настраивая доступы пользователей к компонентам в Центре управления, сохраните права на запуск каждого из компонентов, но запретите редактировать конфигурацию компонентов и останавливать их.
- Мнение пользователя о том, какие компоненты антивирусной системы защиты должны быть установлены на его ПК, должно ИГНОРИРОВАТЬСЯ.

Вы платите только за то, чем пользуетесь

«Платить только за то, что нужно в данный момент» — главный принцип философии лицензирования услуги, которое способно приспосабливаться под нужды предприятия для оплаты только необходимого в данный момент объема услуг. **Оплачивается только фактическое количество подписок, причем это количество может гибко изменяться как в сторону увеличения, так и в сторону уменьшения.**

Это позволяет максимально точно планировать расходы на информационную безопасность в краткосрочной и долгосрочной перспективах на основании фактических бизнес-потребностей компании, исключает непрогнозируемый рост затрат и дает полное понимание возможных будущих расходов на информационную защиту.

Преимущества лицензирования услуги «Антивирус Dr.Web»

- Тарификация от 1 месяца. Оплачивается только фактическое количество подписок в отчетном периоде.
- Подключение новых станций производится немедленно.
- При уменьшении количества персонала производится отключение от услуги ненужных станций.

Снижайте затраты на ИБ, когда они не нужны, и увеличивайте их только по мере возникновения реальной производственной необходимости.

Скидки

Оформив подписку на услугу «Антивирус Dr.Web», вы начинаете экономить на информационной защите с первого месяца пользования.

Подпишитесь на услугу и получайте скидки….

за количество защищаемых объектов...

от 10 до 40 % — в зависимости от количества защищаемых объектов, для которых оформлена подписка

Кол-во ПК	Скидка, %
1–25	Базовая цена тарифа
26–50	10
51–100	20
101–200	25
201–300	30
301–400	35
401–500	40

...и за срок пользования услугой

от 5 до 15 % — особая дополнительная скидка для тех, кто пользуется услугой непрерывно*

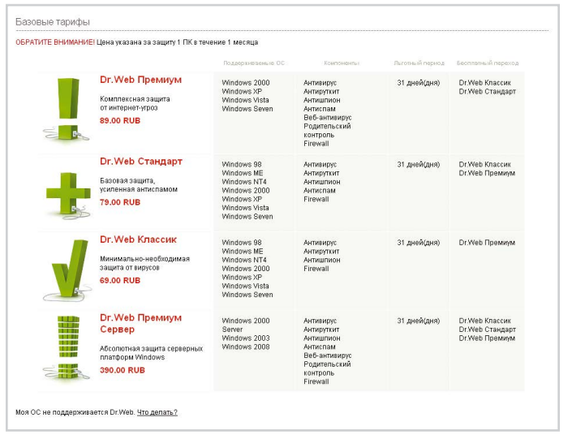
Срок подписки	Скидка, %
1 год	5
3 года	10
5 лет	15

* *Без приостановки или отмены подписки. Начисляется с 13, 37 и 61 месяца соответственно.*

Гибкое лицензирование услуги — ключ к реальной экономии затрат на ИТ.

Центр управления подпиской (ЦУП)

Доступ к Центру управления подпиской предоставляется клиенту поставщиком услуги. ЦУП дает возможность клиенту самостоятельно контролировать процесс подписки и ее продления, переходить на другие тарифные пакеты, получать вирусную статистику и статистику работы услуги, получать новости компании «Доктор Веб» в режиме реального времени, обращаться в службу технической поддержки.

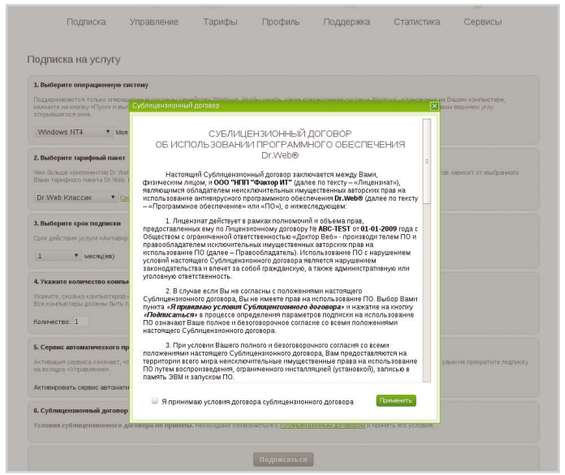


Подписка

Через Центр управления подпиской можно в любой момент подключать к услуге новые станции (расширять лицензию) или отключать ненужные станции, когда этого требует производственная необходимость.

Для оформления подписки необходимо:

1. Указать используемую ОС.
2. Выбрать тарифный пакет.
3. Указать количество ПК.
4. Указать срок подписки (от 1 месяца).
5. Принять условия сублицензионного соглашения.
6. Нажать на кнопку «Подписаться».



Внимание!

Галочка пункта «Сервис автоматического продления активирован» должна быть нажата — тогда подписка будет автоматически продлеваться каждый месяц.

Установка ПО услуги на отдельной станции

Ссылка на установочный пакет Dr.Web доступна в ЦУП немедленно после оформления подписки. Необходимо скачать установочный пакет, запустить его на исполнение и дождаться окончания установки Dr.Web. По завершении установки в правом нижнем углу монитора появится зеленая иконка с паучком на щите, на фоне которой будет мигать желтый треугольник с восклицательным знаком. Необходимо перегрузить компьютер и дождаться соединения с антивирусным сервером — процесс подключения к услуге на этом завершен.

Внимание!

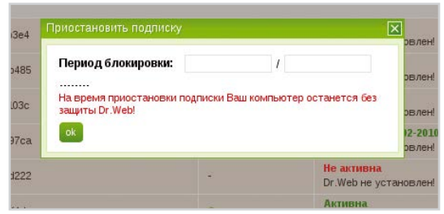
1. Перед установкой надо убедиться, что на ПК нет других антивирусных программ, так как имеющиеся в их составе резидентные модули могут привести к конфликтам несовместимости различного ПО.
2. Защита антивирусной системы Dr.Web начинает действовать после установки ПО услуги «Антивирус Dr.Web».

Продление

Специально заботиться о продлении не нужно. Продление услуги производится автоматически, если при подписке не была снята галочка с пункта «Сервис автоматического продления активирован».

Приостановка подписки

Если необходимо, в любой момент можно приостановить действие подписки — на срок до 3 месяцев.



Чтобы приостановить подписку, на вкладке «Управление» выберите «Приостановить подписку».

Внимание!

В случае приостановки подписки вы теряете право на накопительные скидки за срок пользования услугой (см. раздел Скидки).

Начало действия приостановки

- При посуточной тарификации — с даты приостановки.
- При помесячной тарификации — с 1-го числа следующего календарного месяца.

Окончание действия приостановки

- По истечении заданного периода приостановки. Одновременно включается сервис автоматического продления, если он был активирован до приостановки подписки.

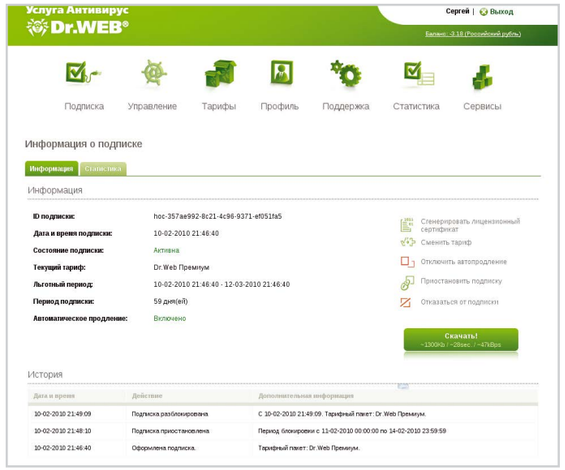
Автоматическое возобновление подписки после приостановки

Происходит в том случае, если до момента приостановки подписки был активирован сервис автоматического продления. Подписка возобновляется на тех же условиях, которые действовали до момента приостановки.

Прекращение подписки

В любой момент можно отказаться от пользования услугой. При этом:

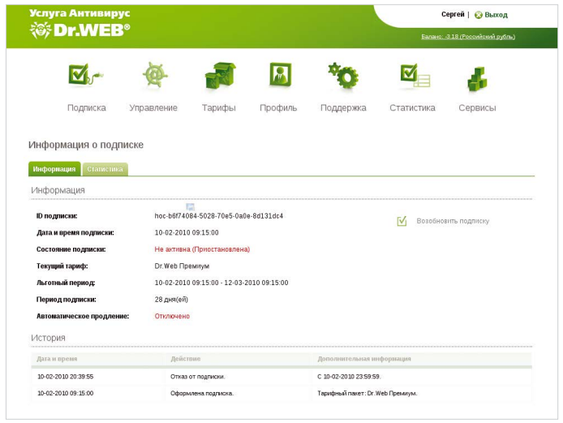
- при посуточной тарификации подписка прекращается немедленно;
- при помесячной тарификации подписка активна до конца текущего календарного месяца. Средства, уплаченные авансом и не израсходованные на момент прекращения подписки, не возмещаются.



Чтобы остановить подписку, на вкладке «Управление» выберите «Отказаться от подписки».

Ручное возобновление подписки после отказа от нее

Подписка возобновляется с момента выбора действия «Возобновить подписку», ссылка на скачивание установочного файла Dr.Web вновь становится доступна. Фактически это новая подписка. Одновременно включается сервис автоматического продления, если он был активирован до приостановки подписки.



На вкладке «Управление» выберите «Возобновить подписку».

Лицензионный сертификат — онлайн

В Центре управления подпиской вы можете самостоятельно создать лицензионный сертификат Dr.Web и подтвердить проверяющим органам лицензионность использования ПО Dr.Web.

Статистика

Центр управления подпиской предоставляет разнообразные отчеты о действиях, произведенных Dr.Web на защищаемых рабочих станциях. Это делает работу ПО услуги прозрачной для пользователя.

Доступна информация о параметрах каждой подписки и группы подписок, а также совокупные данные обо всех подписках. В любой момент (даже когда подписка приостановлена) можно проверить статус подписки, информацию о каждой подписке или обо всех подписках, динамику использования подписок (по группам и тарифам).

Вирусная статистика

Информацию о том, как антивирус Dr.Web защищает рабочие станции — статистику о найденных Dr.Web вирусах и вредоносных программах — можно найти в наглядной форме диаграмм и рейтингов на вкладке «Статистика».

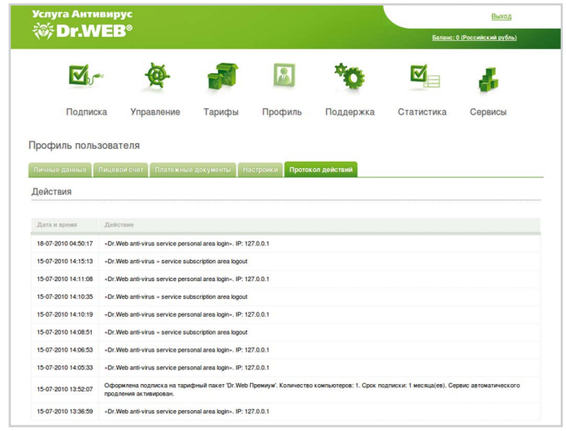
Для каждой станции за любой (настраиваемый) период отображаются:

- сводные данные об обнаруженных антивирусом Dr.Web вредоносных объектах;
- десятка наиболее часто обнаруживаемых вирусов.

Журнал действий

В журнале представлена исчерпывающая информация (история) о действиях клиента в Центре управления подпиской:

- действия за текущий месяц по каждой подписке и по всем подпискам (подписка, отказ, приостановка, вход в кабинет и т. д.);
- действия с лицевым счетом клиента за текущий месяц (пополнение, списание и возврат денег).



Антивирусная система защиты Dr.Web

Задача №1

Политики информационной безопасности

Создание единой экосистемы защиты

Как показывает практика, именно рабочие станции и серверы являются наиболее уязвимыми местами локальной сети. Именно с них распространяются вирусы, а зачастую и спам.

При этом на сами компьютеры вирусы могут попадать самыми различными путями — с флеш-карт пользователей, из защищенных паролем архивов, вложенных в почтовые сообщения и избежавших вследствие этого проверки на сервере, с зараженных сайтов, на которые пользователи перешли по ссылкам из пришедших к ним писем.

В соответствии с существующими стандартами антивирусная система защиты каждой рабочей станции должна включать эффективный антивирус и систему ограничения доступа к локальным ресурсам в целях исключения случаев умышленного или непредумышленного доступа к данным и нарушения нормальной работы системы.

Распространенным заблуждением является то, что в силу относительно малого количества вредоносных программ, работающих под операционными системами типа Linux и Unix, необходимо защищать только рабочие станции и серверы, работающие на операционных системах типа Windows. В результате применения такой политики «защиты» вредоносные программы получают безопасное убежище на незащищенных машинах — даже если они не могут заразить сами операционные системы и работающие приложения, она могут использовать их в качестве источника заражения — например, через открытые для общего доступа сетевые ресурсы.

Внимание!

Центр управления услуги «Антивирус Dr.Web» позволяет централизованно контролировать антивирусную систему защиты любого количества рабочих станций под управлением Windows и Mac OS X.

Защита файлового сервера

Угроза

Как правило, организации защищают только рабочие компьютеры сотрудников, оставляя без защиты серверы, мобильные устройства, домашние компьютеры сотрудников. В итоге проникший на рабочие станции вирус вырывается на свободу, с легкостью проникая на серверы с критически важной информацией.

Почему важно защищать серверы?

- Пользователь может заразить сервер неизвестным на момент заражения вирусом (принеся его или запустив из хранилища). Установленный антивирус сразу поймает его, основываясь на эвристических механизмах. В крайнем случае пролечит вирус при очередном обновлении.
- Сервер может быть взломан хакерами. Установленный антивирус не допустит этого: он отследит и уничтожит вредоносные программы. Если сервер находится под контролем централизованной системы управления, то администратор мгновенно получит уведомление об изменении состояния станции (например, о попытке остановить систему защиты).
- Современный мир пронизан цифровыми технологиями. Пользователи могут работать не только в офисе, но и дома, хранить данные на файловых серверах компании — и на серверах сети Интернет. Использовать свои флеш-диски — и переданные им знакомыми и коллегами по работе. На них могут быть вирусы.
- Современные сотовые телефоны по своим возможностям и количеству уязвимостей могут сравниться с компьютерами — там используются операционные системы и приложения, которые тоже могут быть поражены. А с них в корпоративную сеть могут попасть вирусы и добраться до сервера.

Лучший опыт

Если в вашей компании есть выделенный файловый сервер, он тоже должен быть защищен.

Решение

Для защиты файлового сервера подойдет тарифный пакет Dr.Web Премиум, который поддерживает Microsoft Windows 2003/2008.

Защита сервера услугой «Антивирус Dr.Web» обойдется вашей компании по цене защиты станций, в отличие от стандартных дорогостоящих серверных антивирусных продуктов. И это еще одно из многочисленных преимущества услуги.

Внимание!

Центр управления услуги «Антивирус Dr.Web» позволяет централизованно контролировать антивирусную систему защиты любого количества файловых серверов под управлением Windows.

Защита личных устройств сотрудников

Сегодня большая часть компьютеров, находящихся в пределах помещений компании, ей не принадлежит — это собственность сотрудников — их ноутбуки и смартфоны. Увлеченные сотрудники работают не только в рабочее время, но и в дороге и дома. Они нередко жертвуют часами отдыха, все время находясь на связи. И бизнес с удовольствием использует преимущества таких перемен. А еще многие компании с успехом используют удаленных сотрудников — это тоже дает существенную экономию.

Но на каждый плюс находится свой минус — другими словами, за все нужно платить. При старом, уходящем в прошлое методе организации работы компания могла в любой момент времени гарантировать соблюдение заданного уровня безопасности — ведь системные администраторы контролировали все до одного устройства в компании. Теперь это невозможно.

Угрозы

- Почти две трети работников (63,3%) имеют удаленный доступ к корпоративной информации с личных устройств, включая мобильные.
- До 70% случаев заражений локальных сетей происходят с личных ноутбуков, нетбуков и ультрабуков, мобильных устройств сотрудников, а также сменных носителей (флешек), принесенных в том числе из дома.
- 60% домашних компьютеров не имеют никакой защиты! А значит, вне офиса люди никак не защищены от атак хакеров, используемые ими приложения могут иметь уязвимости, на компьютерах могут быть вирусы и троянцы. При этом эти люди регулярно ходят в локальную сеть компании.
- Это создает возможность утечки, подмены или компрометации важных для компании данных.

Факты

Являясь отличными специалистами в своей области, сотрудники компании не являются экспертами в сфере антивирусной безопасности, часто находятся в плену мифов.

В интересах самой компании обеспечить защищенность всех устройств, на которых работают ее сотрудники, — где бы сотрудники на них ни работали и кому бы эти устройства ни принадлежали.

Для этого компаниям необходимо средство, позволяющее гарантировать:

- защиту любой информации на устройствах пользователей;
- невозможность распространения вирусов и троянцев с устройств пользователей;
- защиту для любых типов устройств, включая мобильные — даже одно устройство, оставшееся без защиты, служит лазейкой для киберпреступников.

Но личные устройства используются сотрудниками и в личных целях!

А в личных целях можно позволить ребенку посидеть за ноутбуком, провести вечерок в кишащей вирусами соцсети, скачать и установить музыкальный файл с сомнительного сайта... Какая уж тут безопасность корпоративных данных!

С услугой «Антивирус Dr.Web» можно сделать почти невозможное — защитить любое устройство так, чтобы это было выгодно всем — и компании, и ее сотрудникам.

Лучший опыт

- Приобретите для личных устройств ваших сотрудников подписку на услугу «Антивирус Dr.Web» — тогда все компьютеры, имеющие доступ к локальной сети вашей компании, будут иметь защиту одного производителя.
- С помощью Центра управления услуги обеспечьте соблюдение политики информационной безопасности вашего предприятия и на личных устройствах сотрудников, включая невозможность отключения ими обновлений, регулярных сканирований и удаления отдельных компонентов защиты.
- Мнение сотрудника о том, какой антивирус должен быть установлен на его личном устройстве, должно ИГНОРИРОВАТЬСЯ — до тех пор, пока это устройство входит в корпоративную сеть. В противном случае такое устройство должно быть объявлено «недоверенным» и не должно пропускаться в сеть.

Только при соблюдении этих условий можно гарантировать, что с личных компьютеров сотрудников в сеть не попадет ничего вредоносного.

Выгоды для компании

- Лояльность сотрудников. Антивирус в подарок — это отличный бонус!
- Удешевление организации защиты.
- Возможность контроля любых защищенных машин из единственной точки.
- Возможность работы сотрудников в любом месте мира с равной защищенностью.
- Гарантия безопасности данных (в том числе персональных) в любой момент времени.
- Снижение простоев по причине заражения.

Сотрудники давно вышли за периметр защиты компании, и вернуть их в его рамки уже невозможно. Да и не стоит. Логичней расширить рамки офисного периметра и включить в него личное пространство каждого сотрудника.

Защита офисных и личных мобильных устройств сотрудников

Сейчас самые распространенные устройства функционируют на базе ОС Android.

Угрозы

- Количество угроз для ОС Android растет катастрофическими темпами вместе с ростом количества используемых устройств.
- Уже существуют банковские троянцы под Android.
- Мобильные устройства подвержены огромному риску потери/кражи. Информация (включая пароли и логины доступа к корпоративным ресурсам) может попасть в не всегда дружелюбные руки.

Решение

В состав тарифного пакет Dr.Web Премиум входит бесплатная подписка на Dr.Web для Android. Система содержит следующие компоненты защиты:

- **Антивирус** – он позволит не допустить на устройство вредоносные файлы, в том числе предназначенные для контроля за перемещением владельца устройства, а также его контактами и переговорами.
- **Антивор** – система защиты от утери мобильного устройства. Если же устройство похищено или пропало, можно удаленно стереть с него все данные.
- **Антиспам** – защита от нежелательных сообщений и звонков, а также разорительных СМС-троянцев.

Внимание!

Центр управления услуги «Антивирус Dr.Web» позволяет централизованно контролировать антивирусную систему защиты любого количества мобильных устройств под ОС Android (начиная с версии 6.2).

Регулярные обновления вирусных баз и программных модулей

Угроза

Антивирус, обновления которого могут отключаться пользователями, или которые производятся от случая к случаю, не способен качественно защищать.

Факты

- Вирусные базы Dr.Web обновляются несколько раз в сутки.
- Ежесуточно компания «Доктор Веб» добавляет в вирусные базы порядка 200 новых записей, что позволяет обнаруживать большую часть поступивших на анализ угроз.
- «Горячие» обновления выпускаются немедленно после анализа новой вирусной угрозы.
- Перед выпуском обновления тестируются на огромном количестве чистых файлов, что позволяет избежать ложных срабатываний.
- Обновления поступают к пользователям с нескольких серверов, находящихся в разных точках земного шара.

Лучший опыт

- Для обеспечения **актуальности** и **целостности** антивирусной системы защиты необходимо своевременно устанавливать все обновления вирусных баз и программных модулей антивируса.
- Мнение пользователя по поводу отмены перезагрузки в связи с обновлением антивирусной системы защиты должно ИГНОРИРОВАТЬСЯ.
- Задачу обеспечения регулярных обновлений и актуального состояния компонентов защиты системой антивирусной защиты можно решить только с помощью **централизованного** управления.
- Мониторинг обновлений должен производиться ЕЖЕДНЕВНО – не исключено появление вирусов, способных отключать обновления или блокировать доступ к серверу обновлений.

Внимание!

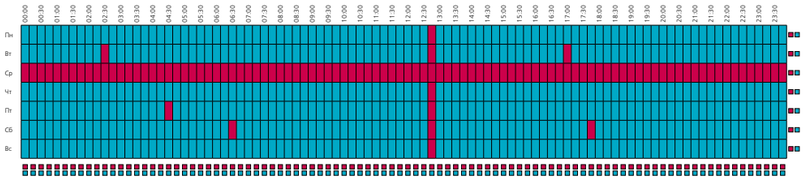
Ни один программный продукт не требует столь частой актуализации, как антивирус. Новые вирусы пишутся постоянно, и вирусные базы обновляются с очень высокой частотой.

Ни в коем случае не отключайте автоматическое обновление!

Решение

Центр управления услугой «Антивирус Dr.Web» всего двумя-тремя настройками позволяет навсегда исключить возможность отмены обновления рабочей станции сотрудником, отключать от сети необновленного агента, а значит, предотвращать распространение эпидемий внутри локальной сети и за ее пределы, а также:

- задать режим обновлений компонентов Dr.Web на защищаемых станциях, распределив нагрузку на разные промежутки времени;



- проводить мониторинг вирусных баз и состояния станций;
- распространить настройки обновлений одной станции на другую станцию или на целую группы (группы).

Обновления «мобильных агентов»

Угроза

Всего один, пусть даже защищенный лицензионным антивирусом, но не обновляемый регулярно ПК, представляет потенциальную опасность для всей локальной сети. А еще на этом путешествующем компьютере может стоять система «Клиент-Банк»...

Решение

Если ноутбук в течение долгого времени не будет находиться в пределах локальной сети, установите мобильный режим агента для связи с сервером для обновлений. «Мобильный режим» агента услуги «Антивирус Dr.Web» позволяет получать обновления даже за пределами локальной сети компании, что особенно актуально для командированных сотрудников.

Регулярные сканирования рабочих станций

Угрозы

- Антивирус не знает 100% вирусов в любой произвольный момент времени.
- Между появлением нового вируса и внесением сигнатуры в вирусную базу могут проходить дни и даже месяцы.
- Даже если внесенная в базу сигнатура способна детектировать вирус, это не значит, что она будет способна вылечить этот вирус — на изобретение лечения может потребоваться много времени.

Факты

- После очередного обновления в результате сканирования на компьютере может быть выявлено значительное количество ранее не известных антивирусу угроз.
- Проверка сканером проводится на большую глубину, чем проверка фоновым файловым монитором — именно поэтому иногда случается, что сканер обнаруживает вирусы, не увиденные файловым монитором.

Лучший опыт

- Сканирования должны проводиться не реже одного раза в неделю.
- Папка Карантин, в которую перемещаются подозрительные объекты, также должна регулярно сканироваться, т. к. в ней могут быть ранее неизвестные вирусы или файлы, перемещенные в результате ложных срабатываний антивируса.
- Мнение персонала о том, как часто надо проводить регулярные сканирования, должно ИГНОРИРОВАТЬСЯ.

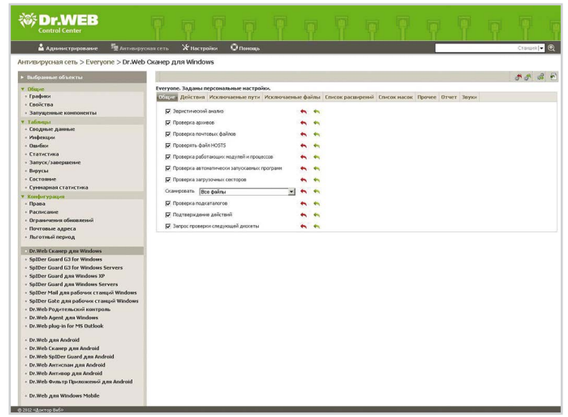
Решение

Настройка регулярных сканирований на уровне отдельной рабочей станции производится в Планировщике, который позволяет:

- запускать сканирования без вмешательства оператора рабочей станции;
- задавать графики сканирований с любой необходимо частотой — т. е. проводить сканирования в удобное для персонала время;
- запускать обязательное сканирование после старта компьютера;
- задавать пути сканирований (области, диски и папки, которые будут проверены в обязательном порядке) и исключения;
- задавать последовательность автоматических действий для обнаруженных вредоносных и подозрительных объектов.

Внимание!

Настройки сканирования по умолчанию, установленные разработчиками Dr.Web, являются наиболее оптимальными. Без крайне необходимости их не следует изменять.



Централизованный контроль за регулярными сканированиями рабочих станций

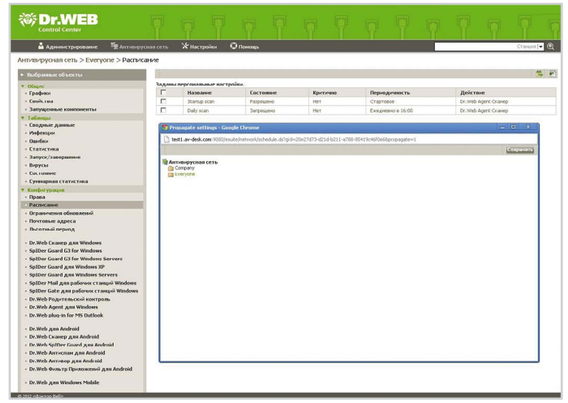
Лучший опыт

- Единственным способом обеспечить проведение регулярных сканирований всеми станциями локальной сети является **централизованный запрет** возможности отключения сканирования.

Решение

Центр управления услуги «Антивирус Dr.Web» позволяет централизованно контролировать соблюдение политики безопасности в части проведения регулярных сканирований:

- запускать/останавливать сканирования без вмешательства оператора рабочей станции;
- задавать пути сканирований;
- задавать групповые и индивидуальные графики сканирований с любой необходимой частотой — т. е. проводить сканирования в удобное для персонала время.



Дополнительно в Центре управления предусмотрена возможность запуска/останова любых компонентов агента (кроме SplDer Guard).

Ограничение доступа к съемным устройствам

Внимание!

Данный функционал есть только в тарифном пакете Dr.Web Премиум.

Угроза

- Ежедневно появляется так много вирусов, что антивирус не может знать их все — риск заражения неизвестным вирусом есть всегда.
- Даже в очень защищенных информационных системах основной источник распространения вирусов уже давно не электронная почта, а вирусы на съемных носителях, чаще всего флешках.

Внимание!

К съемным носителям относятся не только флеш-карты, но и вообще **любые устройства, которые используют USB порт для подключения к ПК!** Передать вирус с одного компьютера на другой можно даже через фотоаппарат или MP3-плеер.

- Большинство современных угроз — троянцы. Это полностью вредоносные программы, которые не имеют механизма саморазмножения и не способны распространяться самостоятельно. Люди собственноручно переносят троянцев от компьютера к компьютеру на флешках.
- По различным оценкам от 7 до 22% случаев утери данных происходят вследствие деятельности вирусов.
- Результатом деятельности вирусов может стать утечка важной информации, отключение компании от сети Интернет, простои сотрудников компании во время восстановления работоспособности компьютеров, пораженных вирусами.
- Постоянная угроза проникновения вирусов в сеть компании отвлекает системных администраторов от выполнения других задач, необходимых для развития компании.

Соответствие Российскому законодательству

Использование Офисного контроля услуги «Антивирус Dr.Web» обеспечивает соответствие системы антивирусной защиты предприятия Федеральному закону № 152-ФЗ «О персональных данных» в части управления доступом.

Федеральный закон № 152-ФЗ «О персональных данных»

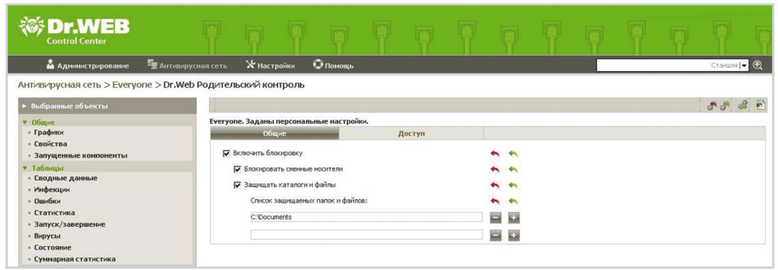
Наличие средств разграничения доступа требуется подзаконными актами регуляторов Федерального закона № 152-ФЗ.

Выдержки из Приказа Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»:

«2.2. В системе защиты персональных данных информационной системы в зависимости от класса информационной системы и исходя из угроз безопасности персональных данных, структуры информационной системы, наличия межсетевого взаимодействия и режимов обработки персональных данных с использованием соответствующих методов и способов защиты информации от несанкционированного доступа реализуются **функции управления доступом**, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений».

Решение

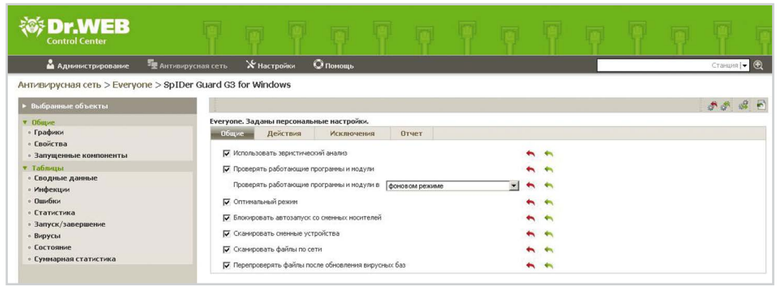
Если нужно полностью запретить использование съемных носителей на рабочих станциях, включите опцию «Блокировать сменные носители» в настройках компонента Офисный контроль Dr.Web. Применение Офисного контроля перекрывает один из основных каналов поступления вирусов — через съемные носители.



Система ограничения доступа Офисного контроля Dr.Web:

- определяет файлы и папки в локальной сети, к которым может иметь доступ сотрудник, и запрещает те, которые должны быть ему недоступны — т. е. позволяет обезопасить данные и важную информацию от умышленного или намеренного повреждения, удаления или похищения злоумышленниками или инсайдерами (сотрудниками компании, стремящимися получить доступ к конфиденциальной информации);
- ограничивает или полностью запрещает доступ к ресурсам сети Интернет и съемным устройствам, а значит, исключает возможность проникновения вирусов через эти источники.

Дополнительным механизмом защиты от вирусов, которые распространяются через съемные носители, является режим запрета выполнения автозапуска в файловом мониторе SpIDer Guard. При включении опции «Блокировать автозапуск со сменных носителей» можно продолжать использование флеш-накопителей в случаях, когда отказ от их использования затруднен.



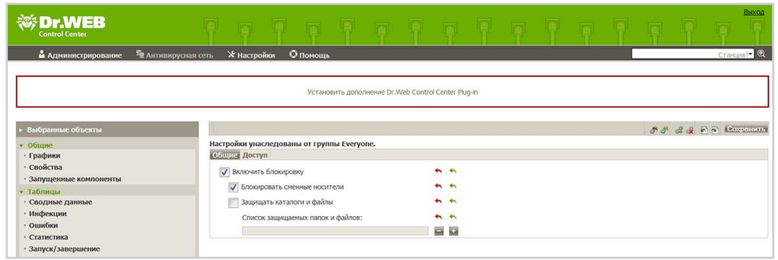
Перечисленные выше меры действенны, но они недостаточны, так как эти настройки может найти и отключить сотрудник.

Лучший опыт

Пользователь или вредоносная программа от его имени не должны иметь доступ ни к каким локальным и сетевым ресурсам, кроме необходимы для выполнения рабочих обязанностей. Убеждать персонал, что флешки опасны — бесполезно. Гораздо проще централизованно запретить возможность доступа к ним.

Решение

Централизованная настройка ограничения доступа к съемным устройствам производится в Центре управления услуги «Антивирус Dr.Web».



Ограничение доступа к интернет-сайтам

Защита от заражений вредоносными программами и защита от фишинга

Угроза

Людям необходимо для работы читать новости и быть в курсе событий. Опасность в том, что большинство офисных сотрудников:

- выходит в Интернет с рабочего компьютера;
- работает под Windows с правами администратора;
- работает, используя простые пароли, взлом которых не представляет труда;
- не производит обновления безопасности всего программного обеспечения, установленного на их ПК.

Бесконтрольное посещение сотрудниками сайтов создает возможность утечки данных, подмены или компрометации важных материалов.

Какие сайты чаще всего являются источниками вредоносного ПО и фишинговых атак (в порядке убывания частоты инцидентов)?

- Сайты, посвященные технологиям и телекоммуникациям.
- Бизнес-сайты: бизнес-СМИ, порталы деловых новостей, бухгалтерские сайты и форумы, интернет-курсы/лекции, сервисы для повышения эффективности бизнеса.
- Порнографические сайты.

Лучший опыт

Необходимо проверять антивирусной системой все ссылки, по которым предлагается загрузка каких-либо ресурсов из сети, и весь трафик до его попадания на компьютер.

Решение

Для защиты от заражения при посещении вредоносного сайта рекомендуем комбинированную защиту.

Внимание!

Возможности антивирусной системы защиты Dr.Web позволяют:

- частично ограничить доступ к сети Интернет;
- вести черные и белые списки адресов, чтобы не ограничивать полностью доступ сотрудника к сети Интернет, если он ему необходим для выполнения служебных обязанностей;
- полностью ограничить доступ к сети Интернет там, где это жизненно необходимо (например, на компьютерах с бухгалтерскими системами);
- сделать невозможным отмену ограничений сотрудником на станции.

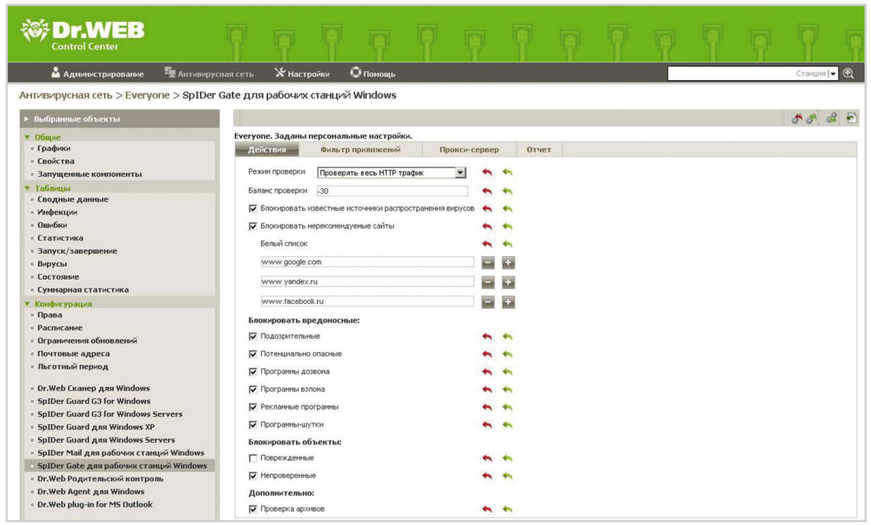
Защита средствами антивирусного ядра Dr.Web

- **Технология ScriptHeuristic** – предотвращает исполнение любых вредоносных скриптов в браузере и PDF-документах, не нарушая при этом функциональности легитимных скриптов.
- **Обнаружение новых угроз средствами эвристического анализа** – для определения новых, ранее неизвестных вирусов, информации о которых нет в базе антивируса.
- **Технология Fly-Code** – обнаружение скрытых под неизвестными упаковщиками известных вирусов.

- **Подсистема фонового сканирования и нейтрализации активных угроз в рамках Антируткита Dr.Web (Anti-rootkit API, arkapi)** – подсистема постоянно находится в памяти и осуществляет поиск активных угроз в следующих критических областях Windows: объекты автозагрузки, запущенные процессы и модули, эвристики системных объектов, оперативная память, MBR/VBR дисков, а также в системной BIOS компьютера. При обнаружении угроз подсистема осуществляет лечение и блокирует опасные воздействия.

Защита средствами программных компонентов на уровне отдельной станции

- **Файловый монитор SpIDer Guard** – защита от активных заражений, действующих в системе.
- **Офисный контроль Dr.Web** – проверка по обновляемой базе опасных и нежелательных сайтов 10 категорий (соцсети, азартные игры и т. д.).
- **HTTP-монитор SpIDer Gate®** – проверка по сигнатурам и проверка эвристическими методами – до поступления трафика в браузер.
- Модуль SpIDer Gate в режиме реального времени прозрачно сканирует входящий HTTP-трафик, перехватывает все HTTP/HTTPS-соединения, производит фильтрацию данных, автоматически блокирует зараженные страницы в любых веб-браузерах, проверяет файлы в архивах (например, загружаемые через менеджеров загрузки, и многие другие приложения, обменивающиеся данными с веб-серверами), защищает от фишинговых и других опасных интернет-ресурсов.
- Возможно отключение проверки исходящего или входящего трафика, а также формирование списка тех приложений, HTTP-трафик которых будет проверяться в любом случае и в полном объеме (черный список). Также существует возможность исключения из проверки трафика отдельных приложений (белый список).
- Работа SpIDer Gate не зависит от используемого браузера.
- Фильтрация практически не сказывается на производительности ПК, скорости работы с Интернетом и количестве передаваемых данных.
- В режиме «по умолчанию» не требуется никакой настройки: SpIDer Gate начинает сканирование сразу же после установки в системе.



Внимание!

Эти компоненты есть только в тарифном пакете Dr.Web Премиум.

Экономия на расходах на Интернет и контроль за действиями сотрудников

Угроза

- Всего один час в день использования Интернета в личных целях каждым сотрудником компании составляет 12,5% от всех расходов компании на заработную плату.
- В отдельные периоды рабочего дня (например, обеденный перерыв) сотрудники компании занимают до 80% пропускной способности канала на задачи, не связанные с работой.

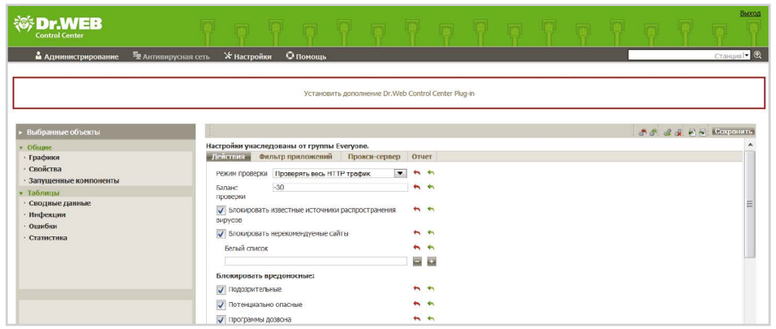
Лучший опыт

- В рабочее время персонал должен иметь доступ только к нужным, с точки зрения работы, интернет-ресурсам.
- Запретите **централизованно** возможность доступа персонала к ненужным интернет-ресурсам.
- Мнение персонала о вредоносности тех или иных сайтов должно ИГНОРИРОВАТЬСЯ.

Решение

Централизованное управление услугой «Антивирус Dr.Web» дает возможность:

- прописывать политики доступа к веб-ресурсам для групп пользователей или отдельных пользователей;
- пресекать попытки посещения сотрудниками нежелательных страниц — например, социальных сетей, интернет-магазинов, игровых сайтов.



Защита от спама

Внимание!

Данный функционал есть только в тарифном пакете Dr.Web Премиум.

Сокращение спам-трафика и устранение до 99% угроз, распространяющихся через спам

Угрозы

1. Почтовый трафик является основным **переносчиком** вирусов и спама. В случае заражения компьютера вредоносные программы могут получить доступ к адресной книге сотрудника, а там могут быть не только адреса ваших коллег, но и адреса ваших клиентов и партнеров — т. е. распространение заражения начнется не только по локальной сети вашей компании, но и за ее пределы.
2. Небрежность, халатность и простое незнание основ компьютерной безопасности сотрудников компании зачастую являются причинами того, что компьютеры компании становятся частью бот-сетей и сами становятся источником спама, что вредит имиджу компании и может привести к внесению компании в черные списки и отключению от сети Интернет за рассылку спама.

Риски использования антивируса без антиспама

Вирусозависимые риски	Репутационные риски
▪ Возможность инфицирования компьютера и превращения его в узел бот-сети и объект для хакерских атак — вплоть до отказа в обслуживании. ▪ Возможность компрометации компании путем внесения ее в черные списки и отключения от сети Интернет за рассылку спама в случае попадания в бот-сеть. ▪ Увеличение затрат на ИТ-инфраструктуру (оплата «паразитного» трафика/затраты на хранение почты, в том числе и спама), повышение платы за трафик.	▪ Блокирование получения почты партнерами за счет внесения компании в черные списки. ▪ Ухудшение репутации в глазах потребителей и партнеров . ▪ Мнение о компании как о технологически отсталой. ▪ Уход клиентов — отказ от услуг компании.

Заблуждение

Антиспам требует постоянного обучения.

Факты

Интеллектуальная система фильтрации спама Dr.Web не требует настроек и обучения — в противовес обучаемым антиспам-системам, использование которых требует ежедневной работы системного администратора.

Лучший опыт

- Проверка почтового трафика должна производиться до попадания письма в почтовую программу, чтобы исключить возможность эксплуатации ее уязвимостей вредоносным кодом.
- Только комплексные решения для электронной почты, сочетающие в себе **антивирус** и **антиспам**, могут обеспечить ее полноценную защиту и снижение непроизводительных расходов компании — т. е. потерь, возникающих вследствие недостатков организации и управления производством.

Решение

Антиспам Dr.Web, входящий в состав почтового монитора SpIDer Mail, проверяет почту до поступления письма в почтовый клиент и не дает вредоносным программам — разносчиком которых является спам — воспользоваться уязвимостями в программном обеспечении. Его работа практически не сказывается на вычислительных ресурсах системы. При этом эффективность отсева спама достигает 97–99%.

Преимущества антиспама Dr.Web

- **Антиспам не требует обучения** — в противовес обучаемым антиспам-системам, использование которых требует ежедневной работы системного администратора, интеллектуальная система фильтрации спама Dr.Web не требует настроек и начинает автоматически действовать с приемом первого сообщения.
- **Высокий процент отсева спама** — разные технологии фильтрации обеспечивают высокую вероятность распознавания спама, фишинг-, фарминг-, скамминг- и bounce-сообщений.
- **Защита от попадания в ботнеты** — поставщик не отключит вашей компании доступ к Интернету за рассылку спама.
- **Почта не пропадет** — отфильтрованные письма не удаляются, а перемещаются в специальную папку почтовой программы (при условии настройки этой папки на локальной станции), где в случае необходимости их можно просмотреть на наличие ложных срабатываний.
- **Экономия трафика** — модуль спам-анализатора абсолютно автономен; для его работы не требуется связь с внешним сервером или доступ к какой-либо базе данных.
- Всегда актуальный — уникальные технологии распознавания нежелательной почты на основе нескольких тысяч правил позволяют производить обновления не чаще одного раза в сутки.
- **Не нагружает систему** — работа антиспама не оказывает заметной нагрузки на систему и не увеличивает время приема почты.

Повышение производительности труда сотрудников

Во времена перепроизводства информации человеческое внимание — ценный и почти невозобновляемый ресурс. Обилие и даже переизбыток информации, ее большая доступность в связи с наличием Интернета поглощают внимание людей. Чистка почтового ящика от спама, закрытие вплывающих окон и рекламных баннеров — все эти факторы рассеивают внимание, снижают уровень концентрации, негативно влияют на эмоциональное и психическое состояние человека. В итоге стоимость внимания сотрудника оказывается для предприятий дороже стоимости средств борьбы с отвлекающими факторами.

Угрозы

1. Один офисный работник в среднем тратит на просмотр и удаление спама от 6 до 11 минут рабочего времени в день.
2. Чем выше служебное положение такого работника, тем больше теряет предприятие на оплате его труда.

Риски

Использование антивируса без антиспама:

- снижает производительность труда всех сотрудников компании, получающих почту и вынужденных заниматься чисткой ящиков от спама;
- приводит к потерям рабочего времени — к задержкам в выполнении сотрудниками должностных обязанностей, а значит, к задержкам в выполнении обязательств компании перед клиентами и партнерами;
- влияет на снижение внимательности и повышение утомляемости от переизбытка отвлекающих факторов;
- вызывает раздражение и недовольство персонала неспособностью руководства справиться с проблемой (высокий репутационный риск для руководства!).

Решение

Использование антиспама в составе Dr.Web Премиум является эффективным средством борьбы с многочисленными отвлекающими факторами, сокращающим потери рабочего времени:

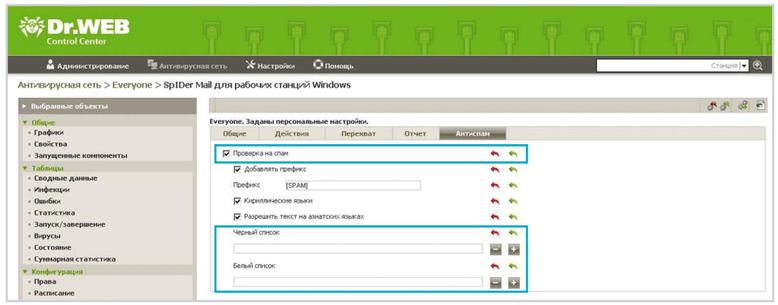
- за счет стабильной и безопасной работы компьютера (без вирусов и спама в почтовом трафике);
- за счет отсутствия в почте сотрудников спама, на чистку которого может уходить немало времени.

Настройка спам-фильтрации на отдельной станции

Включение антиспама производится в программном компоненте Dr.Web SpIDer Mail.

Черные и белые списки

При необходимости можно создать списки доверенных и запрещенных адресов, почта с которых будет нужным образом отфильтрована по умолчанию.



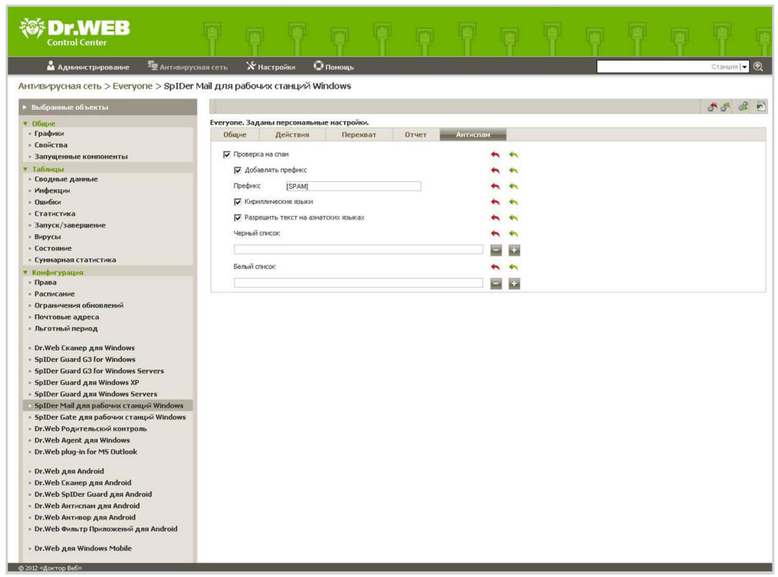
Централизованный контроль за невозможностью отключения антиспама

Лучший опыт

Единственной действенной мерой, позволяющей исключить возможность отключения антиспама или редактирования черных и белых списков персоналом, является централизованный запрет возможности доступа к настройкам антиспама.

Решение

Централизованная настройка параметров антиспама производится в Центре управления услуги «Антивирус Dr.Web».



Защита от вирусозависимых атак на устройства с установленной системой дистанционного банковского обслуживания

Напоминаем!

1. Современные угрозы создаются хорошо организованными криминальными группировками, и вовсе не для оттачивания мастерства программистов, а для отъема денег у тех, кто умеет их зарабатывать.
2. Уязвимости есть в любом ПО, включая системы дистанционного банковского обслуживания.

Сценарии современных атак, направленных на хищения средств

Для проникновения/внедрения вирусов в систему, используемую для работы в системе «Клиент-Банк», используются:

- Фишинговые сайты.
- Создание подложных сайтов.
- Взлом сайтов и ресурсов сети Интернет с высокой посещаемостью.
- Методы социальной инженерии.
- Взлом компьютеров.
- Виды атак, направленных на хищения средств.
- Вирусное заражение ПК через веб-инжект (иногда с переадресацией на фишинговый сайт).
- Атака на каналы передачи данных – производится перехват http-запросов с целью получения логина/пароля или передаваемых значений экранных форм.
- Вирусные атаки на сервер – их целями могут быть поиск уязвимостей на стороне сервера обслуживающего ДБО либо сокрытие фактов хищения средств.
- Атаки на компьютер через Интернет с целью кражи секретного ключа ЭЦП, паролей.
- Атаки на компьютер через Интернет с целью захвата удаленного управления ресурсами компьютера.
- Атака с целью подмены документа при передаче его на подпись.
- Атака с целью подмены части или всего использующегося ПО Внедрение программных закладок или троянских программ.

Мишени атак

- офисные ПК;
- личные устройства сотрудников;
- личные устройства клиентов организации-цели.

Цели атак

- хищение и подмена средств аутентификации доступа (логина и пароля) к системе интернет-банкинга;
- выполнение банковских проводок с использованием удаленного доступа – в уже имеющейся или параллельной сессии;
- проникновение в защищаемую сеть компании.

Способы хищений

- Создание в удаленном режиме несанкционированного платежа непосредственно с компьютера клиента с использованием вредоносного ПО.
- Отправка платежного поручения злоумышленником через компьютер клиента одновременно с сессией работы клиента в системе «Клиент-Банк» (с возможностью подписания документа ключом, хранящимся на отчуждаемом носителе – eToken, iKey и т. п.).

Возмущенный клиент

«Антивирус купили, админ тоже не зря свой хлеб ест, системы обновляются... А деньги пропали! Кто виноват?»

Факты

3. В большинстве малых и средних компаний право подписи платежных поручений имеет только руководитель. А ведь две ЭЦП — руководителя и бухгалтера — значительно сокращают риски вирусозависимых хищений.
4. Заходы в систему «Банк-Клиент» производятся не только с офисного компьютера. Это делают и с домашних ПК, и с мобильных устройств (чаще всего под ОС Android), на которых, как правило, вообще нет никакого антивируса, а если и есть — то бесплатная, сильно ограниченная в функционале версия.

В Росси не существует единой статистики фактов вирусозависимых хищений средств через ДБО. Часто пострадавшие даже не обращаются в правоохранительные органы, считая, что средства вернуть невозможно, а мороки с хождениями по инстанциям будет больше. Жертвы не знают, с чего начать действовать в кризисной ситуации, не знают процедуры инициирования расследования по возврату средств, теряют драгоценное время.

Угрозы

1. Современные успешные троянцы нацелены на хищение денежных средств компаний и частных лиц.
2. Самый успешный и опасный из них — **Trojan.Carberp** — распространяется с использованием набора эксплойтов Black Hole Exploit Kit — коллекции уязвимостей, эксплуатирующих ошибки и недокументированные возможности современного ПО, в частности, браузеров и операционных систем.
3. Разработкой и «продвижением» **Trojan.Carberp** занимается организованная преступная группа: разработчики находятся в одной стране, серверы, с которых распространяется троянец — в другой, организаторы — в третьей, «партнеры», которые покупают часть бот-сети для собственного преступного использования, — в нескольких странах.
4. Троянская программа имеет возможность скачивать специальные встраиваемые модули (плагины). На данный момент имеются версии плагинов под большинство известных банковских систем. Среди команд, которые способен выполнять **Trojan.Carberp**, имеются директивы запуска произвольных файлов на инфицированном компьютере, команда установки сеанса удаленного рабочего стола по протоколу RDP, и даже удаления на зараженном ПК операционной системы. Благодаря наличию удаленного управления и плагинов возможна организации атаки на конкретную компанию по заказу извне. Какими будут действия троянца против вашей компании, зависит от «заказчика».
5. Вирусы семейства **Carberp** проникают на компьютеры пользователей **просто во время просмотра взломанных сайтов, в том числе новостных и бухгалтерских**, которые потенциальные жертвы посещают ежедневно. Не нужно предпринимать вообще никаких действий для того, чтобы «получить троянца»: **заражение происходит автоматически**.
6. Троянцу необходимо всего 1–3 минуты, чтобы похитить пароли и денежные средства со счета жертвы.
7. Ежедневно в вирусные базы Dr.Web добавляется несколько записей этого троянца — программа постоянно совершенствуется его авторами. Пример количества новых троянцев всего за один день:

```
Trojan.Carberp.14(2) Trojan.Carberp.15(7) Trojan.Carberp.194 Trojan.Carberp.195
Trojan.Carberp.196 Trojan.Carberp.197 Trojan.Carberp.198 Trojan.Carberp.199 Trojan.Carberp.200
Trojan.Carberp.201 Trojan.Carberp.202 Trojan.Carberp.203 Trojan.Carberp.204 Trojan.Carberp.205
Trojan.Carberp.206 Trojan.Carberp.207 Trojan.Carberp.208(14) Trojan.Carberp.209
Trojan.Carberp.210 Trojan.Carberp.211 Trojan.Carberp.212 Trojan.Carberp.214 Trojan.Carberp.215
Trojan.Carberp.216 Trojan.Carberp.217 Trojan.Carberp.218 Trojan.Carberp.219 Trojan.Carberp.220
Trojan.Carberp.221 Trojan.Carberp.222 Trojan.Carberp.224 Trojan.Carberp.225 Trojan.Carberp.226
Trojan.Carberp.227 Trojan.Carberp.228 Trojan.Carberp.229 Trojan.Carberp.230 Trojan.Carberp.231
Trojan.Carberp.232 Trojan.Carberp.233 Trojan.Carberp.234 Trojan.Carberp.235 Trojan.Carberp.236
Trojan.Carberp.237 Trojan.Carberp.238 Trojan.Carberp.239 Trojan.Carberp.240 Trojan.Carberp.241
Trojan.Carberp.242 Trojan.Carberp.243Trojan.Carberp.244 Trojan.Carberp.245 Trojan.Carberp.246
Trojan.Carberp.247 Trojan.Carberp.248 Trojan.Carberp.249 Trojan.Carberp.250 Trojan.Carberp.251
Trojan.Carberp.252 Trojan.Carberp.253 Trojan.Carberp.254 Trojan.Carberp.255 Trojan.Carberp.256
Trojan.Carberp.257 Trojan.Carberp.258 Trojan.Carberp.259 Trojan.Carberp.260 Trojan.Carberp.261
Trojan.Carberp.262 Trojan.Carberp.263 Trojan.Carberp.264 Trojan.Carberp.265 Trojan.Carberp.266
Trojan.Carberp.267 Trojan.Carberp.29(14) Trojan.Carberp.33(10) Trojan.Carberp.45(4)
Trojan.Carberp.5(3) Trojan.Carberp.60(6) Trojan.Carberp.61 Trojan.Carberp.80
```

А ведь это только один троянец...

Что может противопоставить этому компания, имея в наличии только файловый антивирус без средств комплексной антивирусной защиты? — НИЧЕГО.

Лучший опыт

1. Только антивируса для защиты от подобных атак недостаточно. Чтобы значительно снизить риск заражения, в состав антивирусной системы защиты должны входить:
   - Система лечения активных заражений — чтобы погасить активность проникших какими-то путями в систему вредоносных программ и очистить ее.
   - Лучшая система самозащиты — чтобы нормально функционировать до поступления обновления, позволяющего пролечить заражение.
   - Офисный контроль — он имеет механизм ограничения доступа к интернет-сайтам (напомним, что троянец распространяется именно через сайты).
   - Модуль проверки интернет-ссылок (HTTP-монитор).
   - Центр управления — система не должна позволять сотрудникам изменять настройки самостоятельно под предлогом, что «все тормозит».
2. Практика показывает, что платежи могут осуществляться не только с машин, расположенных в бухгалтерии, но и с личных домашних ПК, а также с мобильных устройств. Таким образом, нужно защищать все машины и мобильные устройства, с которыми работают сотрудники компании.
3. Компьютер, на котором установлена бухгалтерская система или системами «Банк-Клиент», должен быть полностью отключен от сети Интернет. На нем должна быть ЦЕНТРАЛИЗОВАННО заблокирована возможность использования съемных устройств*.
4. Мнение бухгалтера о предпринимаемых мерах защиты такого компьютера должно полностью ИГНОРИРОВАТЬСЯ.

** Это производится с помощью компонента Офисный контроль в составе тарифного пакета Dr.Web Премиум.*

Факты

Уже существует первый банковский троянец для платформы Android — Android.SpyEye.1.

Что делать если, похищены средства из системы ДБО

Увы, но о фактах хищения жертвы узнают, когда все уже произошло. И в этот момент исключительно важной становится правильная реакция на инцидент. Прежде чем следовать нашим рекомендациям, убедитесь, что хищение произошло именно в результате действия вируса. Для этого достаточно бегло опросить сотрудников, имеющих доступ к системе ДБО. Если вы сами или они не проводили подозрительной, с вашей точки зрения, операции — скорее всего, действовал вирус или проникший в систему злоумышленник.

Внимание!

- Не пытайтесь обновить антивирус или запустить сканирование — так вы уничтожите следы злоумышленников в системе!
- Не пытайтесь переустановить операционную систему!
- Не пытайтесь удалить с диска какие-либо файлы или программы!
- **Не пользуйтесь компьютером**, с которого предположительно произошла утечка средств аутентификации к системе ДБО — даже если в нем есть острая производственная необходимость!

Ваши действия должны быть быстрыми и решительными:

1. Немедленно перезвоните в свой банк — возможно, платеж еще получится остановить. Даже если платеж уже ушел, попросите заблокировать все операции по скомпрометированному счету до выдачи вам новых средств аутентификации доступа (логина и пароля, etoken и т. д.).
2. Напишите заявление в свой банк (банк отправителя платежа) и отправьте его по факсу. Распечатайте заявление в ТРЕХ экземплярах и занесите их в банк. Попросите поставить регистрационный номер на двух экземплярах — один останется у вас, другой будет приложен к вашему заявлению в полицию. На принятом у вас заявлении должны быть дата и порядковый номер входящего документа, принятого секретарем.
3. Напишите заявление в банк получателя платежа с вашего счета, отправьте его по факсу. Аналогично предыдущему пункту надо сделать ТРИ экземпляра и повторить процедуру регистрации.
4. Напишите заявление в полицию и приложите к нему заявления в два банка (получателя и отправителя платежа). Для этого надо посетить ближайшее отделение.

Внимание!

Против вас совершено противоправное действие — могут присутствовать признаки преступлений, предусмотренных по ст. ст. 159, 159.6, 165, 272 и 273 УК РФ.

Для возбуждения в отношении злоумышленников уголовного дела правоохранительным органам необходим процессуальный повод — ваше заявление о преступлении.

Если у вас откажутся принять заявление — получите письменный отказ и обращайтесь с жалобой в вышестоящий орган полиции (к начальнику полиции вашего города или области). Установленный факт хищения является достаточным основанием для возбуждения уголовного дела.

5. Напишите заявление вашему провайдеру с просьбой предоставить логи сетевых подключений за период, когда произошло хищение.

Внимание!

Провайдеры хранят логи сетевых подключений не более двух суток — у вас мало времени!

Важно!

Образцы заявлений находятся на сайте «Доктор Веб» в разделе «Правовой уголок»: http://legal.drweb.com.

Распечатайте все образцы заявлений, чтобы в трудный час они были у вас под рукой, а не в Интернете, к которому у вас может не быть доступа.

Все это должно быть сделано в течение 1–2 суток с момента обнаружения хищения!

Защита от хакерских атак

Виды хакерских атак

Существует огромное количество видов сетевых атак. Как правило, для проведения атак используются уязвимости операционной системы или иного установленного программного обеспечения, ограничения вычислительных мощностей жертвы. Среди сетевых атак можно выделить несколько наиболее распространенных:

- **DoS или DDoS-атаки** (атаки, вызывающие отказ в обслуживании) направлены на временное выведение атакуемой системы из строя.
- **Парольные атаки**, направленные на выявление используемых паролей — методом перебора или с помощью социальной инженерии.
- **Спуфинг** — вставка ложной информации или вредоносных команд в обычный поток данных, перенаправление трафика на ложный IP-адрес и/или его подмена.
- **Сниффинг** — перехват трафика (например, всех почтовых сообщений жертвы) для его последующего анализа.
- **Перехват TCP-сеанса** (TCP Session Hijacking).
- **Man-in-the-Middle.** Атакующий находится как бы между двумя хостами в сети и по сути выступает в роли прокси-сервера, просматривая передаваемую информацию и имея возможность изменять ее в своих целях. Данные атаки проводятся с целью кражи информации, перехвата текущей сессии и получения доступа к частным сетевым ресурсам, анализа трафика и получения информации о сети и ее пользователях, проведения атак типа DoS, искажения передаваемых данных и ввода несанкционированной информации в сетевые сессии.

И это далеко не все. К числу сетевых атак можно отнести все методы разведки, проводимой по сетевым каналам, злоупотребления доверием и несанкционированного доступа. Например, сканирование портов — угроза этого вида не является атакой, но обычно ей предшествует, поскольку это один из основных способов получить сведения об удаленном компьютере. Полученная в результате сканирования информация («слепок» системы) дает злоумышленнику представление о типе операционной системы на удаленном компьютере, а значит, о специфических для данной ОС уязвимостях.

Постоянно появляются новые типы атак. В частности, переход компаний в «облака» вызвал активизацию атак на каналы передачи данных, а внедрение протокола IPv6 — создание новых видов атак, связанных с уязвимостями этого еще пока несовершенного в реализации протокола.

Последствия атак

- Повреждение или разрушение информационных ресурсов и, следовательно, невозможность их использования, простои.
- Утечки конфиденциальных данных, включая пароли, почту и вообще любые данные, которые можно похитить.
- Репутационные риски — задержки или невозможность выполнения обязательств перед клиентами и партнерами.

Внимание!

Атаки на внедрение вредоносных программ, как правило, остаются незамеченными жертвами, компьютеры которых становятся подконтрольны злоумышленникам.

Цели атак

- Политические мотивы.
- Заказ конкурентов (в том числе промышленная разведка, месть).
- Хулиганство.

Решение

Брандмауэр в составе услуги «Антивирус Dr.Web»:

- защищает от инсайдеров путем запрета возможности сканирования сети или подключения к удаленному рабочему столу;
- препятствует хакерским проникновениям через незакрытые порты;
- защищает от несанкционированного доступа;
- снижает риск взлома через уязвимости;

- предотвращает утечки важных данных по сети;
- блокирует подозрительные соединения на уровне пакетов и приложений;
- контроль подключений на уровне приложений позволяет контролировать доступ конкретных программ и процессов к сетевым ресурсам и регистрировать информацию о попытках доступа в журнале приложений;
- фильтрация на уровне пакетов позволяет контролировать доступ к сети Интернет вне зависимости от программ, инициирующих подключение. Журнал пакетного фильтра хранит информацию о пакетах, переданных через сетевые интерфейсы.

Внимание!

По умолчанию брандмауэр Dr.Web не устанавливается. Чтобы установить этот компонент, необходимо во время установки отметить соответствующую галочку напротив его названия.

Защита от проникновений через уязвимости

Угроза

- Уязвимость — недостаток в программном обеспечении, используя который можно нарушить целостность ПО или вызвать его неработоспособность.
- Уязвимости есть в каждом ПО. Не существует ПО, в котором не было бы уязвимостей.
- Современные вирусописатели эксплуатируют уязвимости для проникновения на локальный компьютер не только в операционных системах, но и в прикладных программах (браузерах, офисных продуктах, например Adobe Acrobat Reader и плагинах для браузеров для отображения flash).

Внимание!

Никакое современное ПО, кроме антивирусного, не умеет очистить систему от вредоносного ПО, проникшего через уязвимости.

Лучший опыт

Поддерживать установленное на компьютере программное обеспечение в актуальном состоянии не менее важно, чем обновлять ОС. Теоретически абсолютно любую ошибку в программе можно использовать для причинения вреда системе в целом. Будет это кратковременный сбой или серьезная порча данных — в данном случае не важно. Чтобы этого избежать, важно следить за состоянием имеющегося ПО и своевременно скачивать обновления или новые версии.

Решение

Использование HTTP-монитора SpIDer Gate и почтового монитора SpIDer MailD позволяет исключить проникновение вредоносных объектов из-за уязвимости программ (таких как браузеры, Adobe Flash и Adobe Acrobat, почтовые клиенты), поскольку весь трафик, включая шифрованный, проверяется до его поступления в соответствующую программу.

Защита от заражений методами социальной инженерии

Самый страшный вирус — пользователь.

Народная мудрость

Большая часть современных вредоносных программ из «дикой природы» не имеет механизма саморазмножения — они умышленно рассчитаны на распространение самими пользователями.

Именно пользователи — не знающие основ компьютерной безопасности, просто уставшие или невнимательные — неумышленно или по халатности нарушая политики безопасности, способствуют проникновению вирусов в сеть компании (используют USB-устройства, автоматически открывают почту от неизвестных отправителей, бесконтрольно путешествуют по Интернету в рабочее время и пр.).

Чтобы распространять троянцев руками пользователей, вирусописатели используют методы социальной инженерии — хитроумные уловки, которые заставляют пользователя собственноручно запустить файл вредоносной программы. Уловок для пользователей множество: фишинговые ссылки, ложные письма из банков или администрации каких-либо сетевых ресурсов и многое другое. Различные виды социальной инженерии всегда направлены на одно и то же: получить личные данные пользователя, будь то пароли от веб-сервисов или конфиденциальная информация и банковские данные.

Лучший опыт

Чтобы справиться с мошенниками, использующими данный метод атаки, требуется немного. Соблюдение простых правил помогает заметно снизить вероятность потери информации:

1. Если вы получили письмо с требованием сообщить или подтвердить ваш пароль от любого ресурса — удаляйте его, какие бы страшные угрозы в нем ни содержались (удаление аккаунта, обнуление счета и т. д.). **Администрации сетевых ресурсов, а уж тем более банки, НИКОГДА не запрашивают у пользователя какие-либо данные.**
2. Если вы получили якобы от своего знакомого письмо или сообщение странного содержания, к тому же имеющее ссылки на какие-то ресурсы — свяжитесь с ним любым другим способом (например, по телефону) и уточните, что и зачем он вам отправил. Не исключено, что его аккаунт взломан и используется злоумышленниками.
3. Если какие-либо сторонние ресурсы предлагают перейти на страницу, где вам придется ввести свои данные (например, ссылка на сайт vkontakte.ru) — потратьте время, чтобы вручную ввести текст ссылки в окно браузера — это полностью исключит возможность попадания на фишинговый сайт (существует много методов маскировки истинных путей ссылок). Прежде чем вводить ссылку в браузере, посмотрите, соответствует ли доменное имя сайта оригинальному доменному имени (чтобы заманить вас в ловушку, вредоносная ссылка, например, вместо vk.ru может содержать vkontacte.ru).
4. Прочитав в Интернете про «жареный» факт — например, про новый способ чтения чужих СМС — лучше не проверяйте это в действии. Хакеры никогда не афишируют, какие уязвимости им удалось найти. В данном случае они играют на любопытстве пользователей, чтобы заставить перейти на нужный зараженный ресурс.
5. Не отключайте в антивирусе HTTP-монитор (веб-антивирус) — это намного обезопасит любые ваши действия в сети.

Важно!

Не отключайте файловый монитор SpIDer Guard. Он должен постоянно находиться в памяти компьютера и предотвращать заражения, проверяя файлы перед их запуском, а также все системные процессы и при каждом обновлении антивируса. SpIDer Guard эффективен против любых известных и многих неизвестных угроз, поскольку использует методы эвристического анализа. Даже если новый вирус не будет обнаружен SpIDer Guard, выполнить вредоносное действие он все равно не сможет.

Снижение вирусозависимых простоев

Вирусы и спам являются основными угрозами информационной безопасности для организаций любого типа и размера. Анализ состояния корпоративной сети, работы по предотвращению вирусных атак и действия по преодолению последствий вирусных инцидентов — задачи, которыми приходится заниматься ИТ-персоналу каждый день. Снижение простоев, вызванных действиями вредоносных объектов, — одна из важнейших задач системных администраторов, от успеха решения которой зависят эффективность функционирования бизнес-процессов целого предприятия и его имидж надежного партнера.

Угроза

- Простои составляют в среднем 2 часа в месяц на одного пользователя.
- Чем выше служебное положение такого пользователя, тем выше стоимость его простоя.

Время простоя тратится на ожидание устранения проблемы или самостоятельные попытки устранить ее, что может привести к непредсказуемым последствиям, вплоть до полной потери данных.

Решение

При условии использования антивируса в качестве услуги:

- апгрейды и обновления ПО производятся автоматически и администрируются централизованно — поставщиком услуги или системным администратором предприятия;
- простои, вызванные неквалифицированной реакцией пользователей на вирусное заражение, которые приводят к невозможности выполнения рабочих задач, исключены полностью — в случае отключения возможности изменения настроек на защищаемой рабочей станции.

Антивирусная система защиты Dr.Web

Сервисы

Услуга «Антивирус Dr.Web» — мощный инструмент снижения простоев, вызванных действиями вирусов и вредоносных объектов.

Оповещения

Реализована система оповещений администратора о проблемах, возникающих в антивирусной сети, например, сообщения о вирусных атаках, системные предупреждения, уведомления пользователей о результатах сканирования. Оповещения производятся по электронной почте или с использованием стандартных широковещательных средств операционных систем Windows. Тексты сообщений кастомизируются.

Сервис отправки мгновенных сообщений

Интерфейс отправки сообщений пользователям сервиса позволяет администратору системы отправлять информационные сообщения отдельным пользователям или группам пользователей. Данная возможность может быть использована, например, для рассылки сообщений об эпидемиях и о порядке действий в случае заражения вредоносными программами, для рассылки технических сообщений о неполадках в сети или для поздравлений с праздниками.

Статистика и отчеты

Система позволяет администраторам получать исчерпывающую информацию о состоянии антивирусной сети:

- обнаруженные вирусы (перечень зараженных объектов, вирус, действия антивируса и т. п.);
- сведения об обнаружении вирусов на станциях, сгруппированные по типам вирусов;
- информация об установленных вирусных базах: название файла, содержащего конкретную вирусную базу; версия вирусной базы; количество записей в вирусной базе; дата создания вирусной базы;
- список ошибок сканирования на выбранной рабочей станции за определенный период;
- список компонентов, запускавшихся на рабочей станции;
- сведения о необычном и (возможно) требующем вмешательства состоянии рабочих станций за определенный период;
- список заданий, назначенных для рабочей станции в заданный период;
- подробная информация обо всех модулях антивируса Dr.Web: описание модуля — его функциональное название; файл, определяющий отдельный модуль продукта; полная версия модуля и т. д.;
- список установок ПО на рабочую станцию;
- суммарная статистика.

Возможность графического представления информации о состоянии защищаемой сети позволяет производить регулярный сбор и анализ информации о вирусных событиях на каждом защищаемом ПК и представлять наглядные статистические отчеты по результатам проведенного мониторинга.

Журнал аудита действий

Дает возможность отслеживать все действия системного администратора по установке и настройке системы. В случае возникновения вопросов по хронологии или оправданности производимых действий администратор всегда может представить полный отчет о проделанной работе — это гарантирует высокую прозрачность его действий.

Важно!

При расследовании компьютерных инцидентов журнал аудита действий является одним из элементов доказательной базы.

Заключение

О компании «Доктор Веб»

Компания «Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Наши продукты разрабатываются с 1992 года. «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Наши разработчики уделяют огромное внимание развитию технологий защиты как от известных, так и от неизвестных угроз. Антивирусная система защиты Dr.Web позволяет информационным системам наших клиентов эффективно противостоять любым, даже еще неизвестным угрозам. Решения Dr.Web полностью удовлетворяют бизнес-потребности компаний в защите от вредоносных программ.

«Доктор Веб» является автором инновационных бизнес-моделей на основе собственных разработок. В 2007 году мы стали первой компанией, предложившей на российском рынке новую модель дистрибьюции антивируса в качестве услуги. С этого момента начинается SaaS-эра в истории антивирусной индустрии России, а «Доктор Веб» по сей день продолжает оставаться безусловным лидером этого сегмента рынка.

Продукты Dr.Web имеют сертификаты соответствия ФСТЭК России и ФСБ России. Это позволяет использовать их в организациях с повышенными требованиями к уровню безопасности. Dr.Web сертифицирован Министерством обороны РФ. Dr.Web полностью соответствует требованиям Федерального закона № 152-ФЗ «О персональных данных», предъявляемым к антивирусным продуктам, и может применяться в сетях, соответствующих максимально возможному уровню защищенности.

Ежегодные темпы роста продаж «Доктор Веб» превышают средние показатели по отрасли. Домашние пользователи из всех регионов мира, небольшие организации, крупные предприятия и системообразующие корпорации доверяют продуктам Dr.Web в течение многих лет. Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

Лицензии и сертификаты

1. В отличие от большинства конкурирующих решений, программные продукты Dr.Web имеют сертификаты соответствия ФСТЭК России и ФСБ России. Это позволяет использовать их в организациях с повышенными требованиями к уровню безопасности.
2. Dr.Web сертифицирован Министерством обороны РФ.
3. Dr.Web сертифицирован ФСТЭК России на соответствие:
   - ТУ и НДВ 4 на применение в составе подсистемы антивирусной защиты в информационных системах персональных данных (ИСПДн) класса К1;
   - требованиям (по уровню контроля не ниже 4) руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по 2 уровню контроля отсутствия недекларированных возможностей» и требованиям технических условий.
4. **Dr.Web полностью соответствует требованиям закона «О персональных данных», предъявляемым к антивирусным продуктам** в части защиты от несанкционированного доступа и централизованной защиты каналов передачи данных, и может применяться в сетях, соответствующих максимально возможному уровню защищенности.

Компания «Доктор Веб» имеет следующие лицензии, сертификаты и свидетельства:

- лицензии Федеральной службы по техническому и экспортному контролю (ФСТЭК России) на проведение работ, связанных с созданием средств защиты информации, а также на деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
- лицензия Министерства обороны Российской Федерации на деятельность в области создания средств защиты информации;
- лицензии ФСБ России на проведение работ, связанных с использованием сведений, составляющих государственную тайну;
- лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на разработку и (или) производство средств защиты конфиденциальной информации;
- сертификаты соответствия ФСБ России;
- сертификаты соответствия ФСТЭК России.

Все лицензии и сертификаты «Доктор Веб»:

http://company.drweb.com/licenses_and_certificates

Обучение и сертификация

Самыми частыми причинами возникновения любого рода компьютерных инцидентов является недостаточная образованность персонала в области компьютерной безопасности. Только знание и понимание сотрудниками основ компьютерной безопасности может сократить количество инцидентов и гарантировать эффективность работы средств антивирусной системы защиты.

- **Обучение системных администраторов**
  Для эффективной работы систем информационной безопасности, построенных на базе продуктов Dr.Web®, разработаны программы обучения и сертификации специалистов в области защиты компьютерных сетей предприятия. Обучающие курсы создаются при непосредственном участии разработчиков компании «Доктор Веб». В ходе обучения специалисты приобретают действительно необходимые навыки работы с продуктами Dr.Web, что позволяет объективно оценить уровень знаний ИТ-специалистов.
- **Обучение пользователей продуктов Dr.Web**
  Знания принципов функционирования антивирусов Dr.Web, которые пользователи могут приобрести в ходе изучения обучающих курсов, помогают лучше справляться с компьютерными угрозами.

Мы предлагаем обучение и сертификацию по следующим курсам:

Шифр курса	Название курса	Квалификация	Целевая аудитория
DWCERT-007	Анализ активных заражений и лечение инфицированных систем с помощью антивирусного ПО Dr.Web	Сертифицированный специалист по анализу активных заражений и лечению инфицированных систем с помощью антивирусного ПО Dr.Web	Системные администраторы
DWCERT-004	Dr.Web AV-Desk v.6	Сертифицированный специалист по администрированию Dr.Web AV-Desk v.6	Системные администраторы
DWCERT-001	Dr.Web для рабочих станций и файловых серверов Windows v.7	Сертифицированный специалист по администрированию Dr.Web для Widows v.7	Системные администраторы
DWCERT-030-5	Dr.Web LiveCD (Dr.Web LiveUSB)	Сертифицированный пользователь Dr.Web LiveCD (Dr.Web LiveUSB)	Системные администраторы
DWCERT-030-2	Dr.Web для Windows	Сертифицированный пользователь Dr.Web для Windows	Пользователи
DWCERT-030-3	Dr.Web для Mac OS X	Сертифицированный пользователь Dr.Web для Mac OS X	Пользователи
DWCERT-030-10	Основы антивирусной безопасности. Защита личных ПК/ноутбуков/ нетбуков/ ультрабуков и мобильных устройств	Знаток основ антивирусной безопасности	Пользователи Системные администраторы

И это далеко не весь список обучающих курсов «Доктор Веб».

Все курсы «Доктор Веб»:

http://training.drweb.com

Контакты

Россия

ООО «Доктор Веб»

125124, Москва, 3-я улица Ямского поля, вл. 2, корп.12 А

Телефон: +7 (495) 789-45-87 (многоканальный)

Факс: +7 (495) 789-45-97

Бесплатный телефон технической поддержки:
8-800-333-7932

www.drweb.com | www.av-desk.com | www.freedrweb.com | mobi.drweb.com

Германия

Doctor Web Deutschland GmbH

Rodenbacher Chaussee 6, D-63457 Hanau

Телефон: +49 (6039) 939-5414

Факс: +49 (6039) 939-5415

www.drweb-av.de

Казахстан

ТОО «Доктор Веб – Центральная Азия»

050009, Алматы, ул. Шевченко / уг. ул. Радостовца, 165б/72г, офис 910

Телефон: +7 (727) 323-62-30, 323-62-31, 323-62-32

www.drweb.kz

Китай

Doctor Web Software Company (Tianjin), Ltd.

Тяньцзинская зона экономического и технического развития,
4 проспект, д. 80, технопарк «Тяньда», северный софт-корпус
天津市经济技术开发区第四大街80号软件大厦北楼112

Телефон: +86-022-59823480

Факс: +86-022-59823480

E-mail: D.Liu@drweb.com

www.drweb.com

Украина

ООО «Центр технической поддержки «Доктор Веб»

01001, Киев, ул. Костельная, 4, офис 3

Телефон/факс: +38 (044) 238-24-35, 279-77-70

www.drweb.ua

Франция

Doctor Web France

333 b Avenue de Colmar, 67100 STRASBOURG

Телефон: +33 (0) 3-90-40-40-20

Факс: +33 (0) 3-90-40-40-21

www.drweb.fr

Япония

Doctor Web Pacific, Inc.

NKF Kawasaki building 2F, 1-2, Higashida-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa-ken
210-0005, Japan

Телефон: +81 (0) 44-201-7711

www.drweb.co.jp