Dr.WEB®
Антивирус

Защити созданное

Обеспечение информационной безопасности

Рекомендации

Общие принципы обеспечения информационной безопасности

Требования в области информационной безопасности

Варианты построения системы информационой безопасности. Оптимизация систем защиты

Защита удаленных пользователей и подразделений

Содержание

Общие положения по обеспечению информационной безопасности локальных сетей

На данный момент ситуация на рынке информационной безопасности такова, что заражен (либо изменен так, чтобы открыть доступ вирусам к компьютерам и сетям) может быть файл практически любого формата, а не только исполняемый, как было ранее. Вредоносные коды могут проникать в систему через почту и скачиваемые программы, уязвимости и на флеш-дисках. По статистике, достаточно в среднем 15 минут работы в Интернете на незащищенном компьютере для его заражения.

Тенденцией современных угроз является то, что современных вирусописателей интересует информация, хранящаяся на компьютере, в первую очередь музыка и пароли к программам и электронным счетам, а также использование компьютера в качестве основы для ботнета. Последствием заражения является не только замедление работы компьютера и нарушение нормальной работы установленных на нем программ, но и пропажа денег со счетов, утечка конфиденциальной информации, блокировка провайдером доступа в Интернет в случае попадания компьютера в ботнет, используемый для рассылки спама.

На данный момент наиболее популярным путем распространения вредоносных программ является Интернет. Обычные пользователи могут заразиться при посещении вредоносных ресурсов, в частности фишинговых сайтов или сайтов, предлагающих «антивирусную защиту». Неверным является мнение, что данные проблемы нехарактерны для Рунета — в связи с большим количеством поддельных сайтов Банк России был вынужден разместить на своем сайте список реальных адресов российских кредитных организаций, а с сайтами, радостно сообщающими о найденном на вашем компьютере вирусе и предлагающими срочно загрузить некий «антивирус», наверное, сталкивались все.

Нельзя также сбрасывать со счетов и угрозу заражения через уязвимости установленного на компьютере программного обеспечения — операционной системы, браузера, офисных продуктов. В качестве примера такого уязвимого ПО можно привести продукты Adobe — Acrobat Reader и плагины для браузеров для отображения flash. Найденные в них уязвимости, оставшиеся открытыми в течение длительного времени, вывели эти продукты в одну из основных проблем для систем антивирусной безопасности.

Основные причины потери данных

Ontrack Data Recovery

При выборе антивирусного решения специалисты ИТ-отдела московского филиала «Мобилбанка» руководствовались, главным образом, потребительскими свойствами программного продукта, такими как надежность, простота в работе, нетребовательность к системным ресурсам и централизованное управление. Теперь под защитой Dr.Web находятся как рабочие станции, так и файловые серверы банка, а также почтовый и интернет-трафик. Компания «Мобилбанк» очень довольна уровнем защиты, предоставленной компанией «Доктор Веб».

Сергей Капитонов,
руководитель отдела по работе с партнерами «Системы информационной безопасности»

На данный момент не существует ни одной полностью неуязвимой операционной системы — уязвимости и вирусы существуют не только для всех них, но даже для многих широко распространенных программ. Даже если система не имеет известных уязвимостей и число вирусов для нее крайне мало, использование методов социальной инженерии позволяет заразить и «неуязвимую систему». В качестве примера можно привести появление вируса под Mac OS X, попадавшего в систему под видом нового видеокодека.

По мере убывания основными путями заражения компьютеров являются сменные диски, почта, веб-браузинг, уязвимости. Более того, во многих случаях именно пользователи, нарушая политики безопасности, способствуют (используя флеш-устройства, путешествуя по сайтам в рабочее время, открывая почту от неизвестных отправителей и пр.) проникновению вирусов в сеть компании.

Компания «Доктор Веб» рекомендует: основные принципы защиты компьютера при работе в сети Интернет

На компьютере, подключенном к сети Интернет, должны быть установлены все исправления безопасности, причем не только для операционной системы, но и для всех используемых программ — современной тенденцией является использование для проникновения на локальный компьютер уязвимостей именно в программах, а не в операционной системе.

Все используемые пароли должны быть достаточной длины. В паролях не должны использоваться простые сочетания букв. Использование простых паролей делает возможным злонамеренное проникновение через перебор паролей.

На компьютере должна быть установлена эффективная антивирусная программа, дающая возможность как постоянной защиты, так и периодических проверок. Антивирусная программа должна контролировать все протоколы, используемые для доступа в Интернет, сменные диски, локальную почту пользователя. Не стоит устанавливать неизвестные антивирусные программы — тенденцией последних лет стало создание «антивирусов», основной целью которых является заражение машины пользователя.

Более того, нельзя ограничиваться установкой только одного антивируса, не устанавливая систем контроля доступа и всех обновлений безопасности к ранее установленным программам. Установив защиту по минимуму, пользователь уподобляет свой компьютер неуязвимой крепости, у которой имеется только одна стена, — и противник всегда сможет ее обойти.

Пользователи данного компьютера должны иметь доступ только к тем локальным и сетевым ресурсам, которые им необходимы для выполнения рабочих обязанностей.

Поддельные антивирусные программы в последнее время распространились настолько, что стали представлять собой по-настоящему опасный тренд.

Эксперты отмечают, что хакеры снабжают данные разработки различными средствами шифрации данных, обхода настоящих антивирусов и другими разработками, способствующими проникновению заразы на компьютеры пользователей. Впервые поддельные антивирусы, как говорится в отчете, появились в начале 2008 года, и с тех пор специалистами APWG было обнаружено более 485 000 разнообразных фейк-антивирусов, поддельных «лечащих» утилит, разнообразных тюнеров системы. Все эти решения представляют собой в подавляющем большинстве случаев ядовитую смесь из троянов, шпионских программ и банковских разработок, ворующих данные.

Эксперты из группы APWGB (Anti-Phishing Working Group)

Вместе с продуктами Dr.Web мы получили не только надежные, но и удобные в использовании средства антивирусной и антиспам-защиты. Эти продукты, прошедшие сертификацию в Украине, полностью соответствуют требованиям, которые мы предъявляем к уровню информационной безопасности.

Виталий Микитенко,
заместитель начальника управления Генеральной прокуратуры Украины

Массовые перебои с энергоснабжением в Бразилии были делом рук хакеров, которые манипулировали системами управления.

Речь идет о случаях отключения электричества, в том числе о двухдневном блэкауте 26–27 сентября 2007 года, когда без света остались более 3 млн жителей в нескольких десятках городов.

Канал CBS

Windows-серверы всю жизнь были источниками всякой заразы в наших сетях. Эти вечно долго закрывающиеся уязвимости, зависания... Сравнив средства антивирусной защиты, разработанные различными вендорами, мы остановили свой выбор на продуктах компании «Доктор Веб». Уровень безопасности корпоративных данных, хранящихся на компьютерах и серверах банка, стал существенно выше, а намного более удобное администрирование сэкономило нам много времени. Как хорошо с антивирусом Dr.Web — теперь есть время на работе кофе попить.

Специалист ИТ-отдела
филиала «Хох» Банка Развития Региона

Основные принципы защиты локального компьютера, не подключенного к сети Интернет

Как это ни парадоксально, но практически все вышеперечисленное, за исключением контроля протоколов выхода в Интернет, актуально и для локальных компьютеров, включая установку патчей безопасности, ведь занесенные на компьютер вирусы могут использовать для своего распространения именно уязвимости в программах и операционных системах.

Компания «Доктор Веб» рекомендует: принципы обеспечения антивирусной безопасности

Достаточно часто в компаниях используются только продукты для защиты рабочих станций. При этом предполагается, что:

- вирусы могут проникнуть только через рабочие станции, и смысла в защите серверов нет;
- на серверах никто не работает и никто их не заразит;
- защита серверов стоит дорого.

Однако:

- Пользователь может заразить сервер неизвестным на момент заражения вирусом (принеся его или запустив из хранилища). Если бы был установлен антивирус, то он бы при очередном обновлении пролечил его или поймал сразу, основываясь на эвристических механизмах.
- Сервер может быть взломан хакерами. Если бы на сервере был установлен антивирус, то он бы отследил и уничтожил вредоносные программы. Более того, если бы сервер находился под контролем централизованной системы управления, то администратор мгновенно получил бы уведомление об изменении состояния станции (например, о попытке остановить систему защиты).

В связи с этим установка системы защиты непосредственно на почтовых серверах и интернет-шлюзах позволяет:

- Перенести защиту на уровень серверов и исключить ситуации, когда пользователь сам может отключить антивирус или снизить уровень защиты — руководство компании и системный администратор могут быть уверены в защищенности сети.
- Увеличить актуальность защиты. В отличие от рабочей станции, которая может не обновляться длительное время (например, во время отсутствия сотрудника), антивирусные базы сервера всегда поддерживаются в актуальном состоянии.
- Уменьшить вероятность возникновения конфликтов антивирусного ПО с другим программным обеспечением. Например, с самостоятельно установленным пользователем ПО.
- Проверять трафик до его поступления клиенту — в браузер или почтовый клиент. Вирусы не смогут воспользоваться уязвимостями операционных систем и соответствующих программ — не секрет, что уже достаточно давно для проникновения на компьютер в большей степени используются уязвимости программного обеспечения (в первую очередь Adobe), а не уязвимости операционных систем.
- Уменьшить нагрузку на рабочую станцию — работа пользователей становится более комфортной.
- Уменьшить долю спама в почтовом трафике до минимума, что существенно повысит производительность труда, так как:
- пользователи значительно меньше отвлекаются от основной работы на проверку приходящей почты;
- уменьшается вероятность пропуска или удаления важного сообщения.

Также существенно влияет на уровень информационной безопасности наличие централизованного управления антивирусной защитой сети. Внедрение системы централизованного управления позволяет:

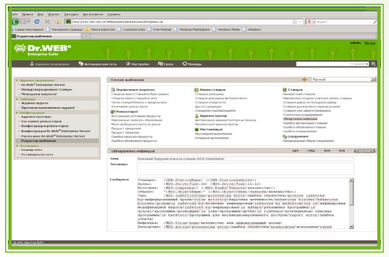
- создавать различные настройки для различных групп пользователей без необходимости настройки защиты на каждой конкретной рабочей станции;
- гарантировать, что антивирус на каждой рабочей станции не отключен и работает именно с теми настройками, которые задал администратор сети.

Продавцы фальшивого антивируса снабдили программу службой онлайновой технической поддержки, чтобы увеличить продажи продукта, причем на вопросы пользователей отвечает человек, а не программа-робот. Во время общения с техподдержкой, в задачи которой входит нагнетание страха, у пользователя возникает желание незамедлительно приобрести Live PC Care за 30–100 долларов.

Схема работы фальшивого антивируса Live PC Care работает следующим образом. После того как пользователь с помощью бесплатной пробной версии якобы мощного антивируса загрузит, установит и проведет сканирование системы, Live PC Care обязательно выдаст целый список обнаруженных вредоносных программ — вирусов, троянов, спам-ботов... Для излечения зараженного опаснейшими вредоносами компьютера предлагается приобрести полнофункциональную версию «антивируса».

http://soft.compulenta.ru

Dr.Web Enterprise Security Suite



Только централизованно управляемая защита всех узлов локальной сети дает гарантии того, что вирус не проникнет в сеть компании.

Варианты построения системы информационой безопасности. Оптимизация систем защиты

Как правило, система информационной безопасности должна обеспечивать для используемых бизнес-процедур:

- систему получения и отправки только чистых от вирусов и спама почтовых сообщений по всем используемым протоколам — как внутри самой компании, так и в ходе общения с внешними адресатами;
- систему ограничения доступа к различной информации, включая систему защиты от инсайдеров;
- систему получения и отправки тех или иных данных, обычно в виде файлов — как внутри самой компании, так и в ходе общения с внешними адресатами.

Также, как правило, для выполнения задач компании в состав ее локальной сети могут входить:

- рабочие станции и/или терминальные клиенты — собственно места, на которых работают сотрудники компании или ее посетители;
- файловые серверы — для хранения и обмена информацией между сотрудниками компании, в том числе файлами и документами;
- почтовые серверы — для обработки внутренней и внешней почты;
- интернет-шлюзы — для организации выхода из внутренней сети компании во внешнюю сеть (обычно, но не всегда в сеть Интернет);
- серверы баз данных, серверы приложений (например, сервер 1С), серверы DNS / DHCP / Active Directory — для выполнения повседневной работы, бизнес-процедур, организации связи отдельных компьютеров в единую сеть.

На сегодняшний день вирусы и другие вредоносные программы являются одной из основных причин утери данных. По различным оценкам, от 7 до 22% случаев утери данных происходит 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.

В связи с этим наличие современной антивирусной системы защиты является обязательным для локальной сети любой компании и, более того, для каждого компьютера этой компании, в не зависимости от того, какие задачи выполняет это компьютер.

Защита должна надежно перекрывать все пути проникновения вирусов в систему и все пути их распространения — совершенно недостаточно защищать отдельные участки сети, например только рабочие станции. Такая защита будет аналогична знаменитой линии Мажино — неуязвимой по ожиданиям ее строителей.

Так, если в компании отсутствует внутренний почтовый сервер, то должны защищаться каналы связи с внешним почтовым сервером, а также обеспечиваться внутренняя защита почты на случай взлома или атаки внешнего сервера.

В ходе конференции Black Hat, проходившей в Барселоне, была продемонстрирована возможность незаметного встраивания кода червя Conficker, а также иных скрытых данных в архивные файлы типа RAR и ZIP.

Исследователи обнаружили восемь уязвимостей в ZIP и семь «дыр» в 7ZIP, RAR, GZIP и CAB. Злоумышленники могут использовать найденные бреши для обхода корпоративных систем защиты, проверяющих почтовые вложения на присутствие в них вредоносного кода.

http://soft.compulenta.ru

Основной бизнес-продукт компании «Доктор Веб» был развернут во всех филиалах «МРСК Северо-Запада», охватив несколько тысяч рабочих станций и адресов электронной почты, а также несколько сотен файловых серверов и интернет-шлюзов. Столь крупное внедрение наглядно иллюстрирует возможность исключительной масштабируемости и удобство централизованного управления Dr.Web Enterprise Security Suite. Теперь каждый из нескольких тысяч компьютеров, входящих в разветвленную сеть ОАО «МРСК Северо-Запада», надежно защищен при помощи новейших антивирусных технологий, позволяющих противостоять вредоносным программам любого типа. Среди объектов защиты — персональные машины, работающие как под управлением Windows, так и UNIX-систем. Спасибо Dr.Web за наше спокойное настоящее!

Михаил Челушкин,
начальник отдела АСУ ОАО «МРСК Северо-Запада»

Пользователей ICQ атаковал очередной вирус под названием Snatch. В отличие от обычных тупых спам-ботов, он ведет себя более изобретательно и успешно маскируется под живого человека.

http://www.utro.ru/articles/2010/08/16/915087.shtml

Компания «Доктор Веб» рекомендует

Необходимо использовать продукты, обеспечивающие максимальную автоматизацию работ по защите сети, мгновенное распространение обновлений, получение централизованных отчетов, имеющие минимальные затраты на сопровождение, — только это обеспечит бесперебойную работу компании и минимизацию затрат на бизнес-процедуры.

Защита рабочих станций и файловых серверов локальной сети

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 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, они могут использовать их в качестве источника заражения, например, через открытые для общего доступа сетевые ресурсы.

Исследования, проведенные по заказу Cisco компанией InsightExpress, показали, что более половины сотрудников компаний используют на компьютерах запрещенные приложения.

Центр управления Dr.Web Enterprise Security Suite

Компания «Доктор Веб» рекомендует

Если рабочая станция не имеет доступа в Интернет и для нее перекрыты все возможные пути проникновения вирусов (в том числе пользователи не имеют возможности самостоятельно добавлять на нее новые файлы), то в том случае, если локальная сеть компании включает менее пяти компьютеров и защищаемые компьютеры не имеют доступа в Интернет, рекомендуется использовать для их защиты программные продукты Антивирус Dr.Web для рабочих станций Windows, Linux или Mac OS X — в зависимости от используемых операционных систем. Если же число рабочих станций больше, то рекомендуется использовать Dr.Web Enterprise Security Suite.

В том случае, если рабочая станция имеет выход в Интернет, то необходимым условием ее безопасной работы является наличие антиспама, средства ограничения доступа к ресурсам сети Интернет и средства проверки всего интернет-трафика.
В том случае, если есть вероятность атаки рабочей станции, в том числе и по локальной сети — изнутри компании, на рабочей станции должен быть установлен файервол. В этом случае в соответствии с размером сети для компьютеров, имеющих доступ в Интернет и требующих повышенной защиты, рекомендуется использовать Dr.Web Security Space или Dr.Web Enterprise Security Suite Комплексная защита.

Использование данных продуктов позволяет:

- Полностью исключить как возможность проникновения вирусов на рабочие станции (в том числе на мобильные устройства и ноутбуки) и серверы локальной сети, так и их распространение с незащищенных компьютеров.
- Защитить пользователей от поступления спама.
- Реализовать сервис защиты как от намеренных, так и непреднамеренных действий пользователей посредством ограничения доступа к используемым информационным ресурсам.
- Обеспечить надежную защиту как от атак, проводимых из локальной сети, так и от действий инсайдеров — сотрудников компании, стремящихся получить доступ к внутренней информации.

Российская экономика в 2008 году потеряла из-за спама от 1,3 до 1,9 миллиарда долларов, говорится в исследовании компании ФБК.

Аналитики получили свою оценку, подсчитав двумя способами, сколько рабочего времени уходит на спам. Первый заключался в оценке числа работников, пользующихся электронной почтой, по видам экономической деятельности и данных Росстата о средней заработной плате.

http://citcity.ru/20537

Для предприятий с многофилиальной структурой возможность централизованной информационной защиты представляет особую ценность.

Сергей Кузнецов, руководитель отдела ИТО Группы компаний «ГЕМА»

Использование Dr.Web Security Space или Dr.Web Enterprise Security Suite Комплексная защита позволяет полностью исключить возможность проникновения вирусов и спама в локальную сеть и поднять производительность труда сотрудников, одновременно высвободив время системных администраторов для решения актуальных задач развития компании.

Внимание! Dr.Web Enterprise Security Suite Антивирусная защита обеспечивает только обнаружение и лечение вирусов любого типа, но не обеспечивает защиты от спама, возможности ограничения доступа к различным интернет-ресурсам, отдельным дискам, папкам или файлам, проверки всего интернет-трафика до поступления его в различные программы. Данные возможности доступны только в Dr.Web Enterprise Security Suite Комплексная защита.

Внимание! Подходы к обеспечению безопасности данных сервисов различаются для операционных систем Windows и UNIX. Для операционных систем Windows использование файлового антивируса подразумевает защиту серверов приложений и терминальных серверов, а для операционных систем UNIX для защиты каждого сервиса необходимо использовать собственные решения.

В связи с этим важно знать, какие дополнительные сервисы работают на файловом сервере и какие из этих сервисов необходимо защищать отдельно, к чему приведет использование совместно нескольких сервисов на одном защищаемом сервисе и насколько защищен будет тот или иной сервис. Так, например, использование на защищенном файловом сервере сервера баз данных не подразумевает лечения содержимого баз данных — для этого нужно использовать специальные решения.

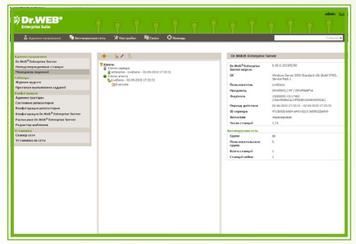
Внимание! Для построения системы защиты данных необходимо понимать пути получения данных, используемые сотрудниками и клиентами компании. Так, достаточно часто сотрудники компании используют не только собственный файловый сервис, но и внешние хранилища. При использовании таких хранилищ нет гарантии того, что пользователь получит файлы, чистые от вирусов, — методы, которые используют злоумышленники, достаточно разнообразны, и многие из них позволяют перехватывать канал связи с Интернетом и подменять передаваемую информацию. В связи с этим наряду и защитой файлового сервера компании и всех общедоступных ресурсов сети (например, расшаренных пользователями папок) в компании должен использоваться антивирусный шлюз, который не позволит получить внутрь компании или передать наружу зараженный файл.

Индекс проникновения вредоносного кода в России во второй половине 2008 года вырос на 58% по сравнению с первым полугодием и составил 21,1.

Общее количество сетевых угроз в России увеличилось на 6,8%, что связано более чем с 50-процентным ростом числа вирусов-червей.

Отчет Microsoft Security Intelligence Report (SIR)

Центр управления Dr.Web Enterprise Security Suite



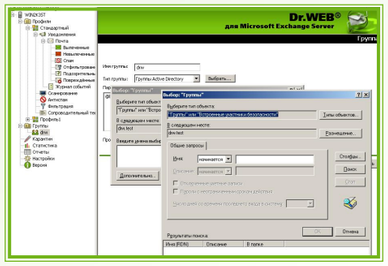
Для обеспечения надежной защиты данных, размещаемых на рабочих станциях и файловых серверах, необходимо ответить на следующие вопросы:

- Какое количество рабочих станций и файловых серверов используется в компании?
- На какой платформе работают рабочие станции и файловые серверы (Windows, UNIX)?
- Где располагаются рабочие станции и файловые серверы — внутри помещений компании или вне ее, например в арендуемом дата-центре?
- Кроме файлового сервера, имеются ли в компании общедоступные ресурсы?
- Используются ли для хранения файлов внешние, не принадлежащие компании файловые серверы?
- Имеется ли доступ извне компании к защищаемым ресурсам?

Аэрофлот подал иск в Арбитражный суд Москвы к банку ВТБ 24 на 194,2 млн рублей в связи с недостаточной защищенностью процессинговой системы, выявившейся в ходе хакерской атаки.

http://www.securitylab.ru/news/397362.php

Dr.Web для MS Exchange 2007/2010



Компания «Доктор Веб» рекомендует

Внимание! С точки зрения безопасности выставлять почтовый сервер в Интернет или внутреннюю сеть компании небезопасно.
В связи с этим компаниям рекомендуется размещать на границе сети или в специально организованной демилитаризованной зоне (DMZ) транзитные (или Frontend) почтовые серверы, основной функцией которых является прием и передача почты на размещенный внутри сети основной почтовый сервер компании и которые располагаются в зоне или во внешней сети, принимают почту и переправляют ее на основной почтовый сервер внутри сети организации. Одной из задач таких серверов как раз является фильтрация спама и вирусов. Управляться такие серверы могут как специалистами самой компании, так и сторонней компанией.

Следствием использования транзитных почтовых серверов служит не только возросшая безопасность почтовых сервисов компании, но и улучшение работы самого почтового сервера — за счет уменьшения его нагрузки. Что в свою очередь приводит к увеличению комфортности работы пользователей за счет уменьшения времени ожидания ответа сервера.

Важно помнить, что почтовый сервер — это по сути просто сервис, размещающийся на обычном файловом сервере. Поэтому, если используемой файловой системой является Windows, кроме защиты почтового сервиса необходимо осуществлять антивирусную защиту самого сервера.

Защита почтовых серверов

Почтовые серверы предназначены для обработки почты до ее поступления клиенту, а также перед отправкой. Кроме этого, почтовые серверы могут служить основой для систем массовой рассылки, обмена данными между сотрудниками компании, а также для построения систем документооборота.

В повседневной работе большинство пользователей компаний используют для отправки и получения или почтовый сервер компании, или удаленные почтовые сервисы, такие как gmail.com, mail.ru.

Бесперебойная работа почтовой системы, безусловно, является одним из ключевых условий работы компании. Несмотря на появление новых технологий, электронная почта в современном мире является одним из основных методов связи с партнерами и клиентами. Но почта — это не только удобный способ связи, это еще и один их основных путей проникновения вирусов в локальную сеть.
Как вирусописатели, так и спамеры активно используют недостатки почтовых протоколов и уязвимости почтовых серверов и клиентов. Иногда достаточно самого факта получения письма для заражения всей системы, даже если пользователь, его получивший, его не открывал.

Не менее важной проблемой является проблема спама. На данный момент спам является вторым по частоте использования хакерами путем проникновения вирусов в защищаемую сеть. Кроме этого, наличие спама отрицательно влияет на производительность работы сотрудников компании и служит косвенной причиной потери данных и уменьшения эффективности деятельности компаний.

Принципы защиты почтовых сервисов и почтовых серверов

- Необходимо защищать как внешнюю (входящую и исходящую), так и внутреннюю почту компании. В случае заражения сети компании именно почта может стать источником вирусов и путем проникновения их на все машины сети, так как на зараженной машине вредоносные программы имеют доступ к адресной книге сотрудника.
- Должны быть защищены все пути приема и отправки почты — зачастую недостаточно защитить только почтовый сервер, так как пользователи, как уже говорилось, могут пользоваться внешними сервисами. Здесь важно знать, что для получения и отправки почты пользователями используются протоколы POP3 и IMAP4, либо их защищенные версии POP3S и IMAP3S. Почтовые серверы сообщаются между собой по протоколу SMTP. В связи с этим необходимо либо ставить защиту на почтовый сервер (для обработки и фильтрации корпоративной почты) и дополнительно обрабатывать протоколы POP3 и IMAP4 на шлюзе сети Интернет, либо фильтровать всю внешнюю почту (протоколы POP3 и IMAP4, SMTP) на шлюзе, а на почтовом сервере сосредоточить только обработку внутренней почты. Последний вариант предпочтительней, так как в этом случае:
  - нагрузка на почтовый сервер значительно снижается (количество спама в почтовом трафике составляет до 98% и, естественно, его отсутствие благоприятно сказывается на работе почтового сервера);
  - отсутствие прямого доступа к почтовому серверу из сети Интернет не позволяет хакерам воспользоваться уязвимостями (ранее известными и уязвимостями нулевого дня), в том числе за счет специально сформированных писем.

Проверка почтового трафика на шлюзе также рекомендуется в том случае, если почтовый сервер находится вне охраняемой территории компании (например, во внешнем дата-центре) или компания арендует почтовые адреса на специальном сервисе. В данном случае отсутствует гарантия поступления в компанию только проверенного (легитимного) трафика — даже в том случае, если защита почтового сервера осуществляется системными администраторами компании, злоумышленник имеет гораздо большие возможности по доступу к серверу или подмене трафика, в то числе и за счет аппаратных закладок.

Уязвимости веб-приложений, на долю которых приходится 55%, превосходят по численности все другие виды выявленных угроз ИТ-безопасности.

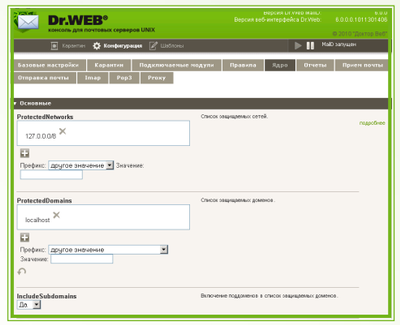
Отчет IBM X-Force

http://citforum.ru/news/24596

Когда мы заказывали демоверсию Dr.Web для защиты почтовых серверов UNIX, мы не были уверены, что этот продукт нам действительно необходим. Но первые же дни показали, что встроенный антиспам отсеивает около 95% спам-писем, в которых чаще всего и располагаются вирусы. Теперь канал поступления вирусов надежно заблокирован продуктами компании «Доктор Веб!»

Михаил Давлетбаев,
заместитель начальник отдела системных корпоративных ресурсов службы ИТ «Газпром Трансгаз»

Dr.Web для почтовых серверов UNIX



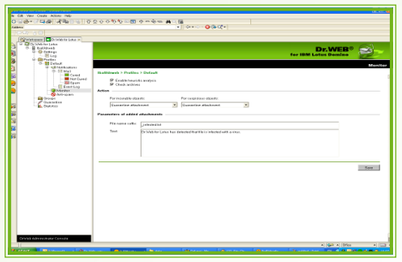
Обнаружен новый способ распространения троянцев, блокирующих Windows, — через комментарии в «Живом Журнале» (LiveJournal, LJ) — сервисе блогов, особо популярном у русскоязычных пользователей. Жертва, нажимая на полученный комментарий, попадает на сайт фотохостинга, откуда направляется на интернет-ресурс с порнографическим контентом, где ей предлагается загрузить exe-файл, за которым скрывается Trojan.Winlock.

http://news.drweb.com/show/?i=1455&c=9&lng=ru&p=0

Очень сложно найти оптимальный антивирус для проверки трафика, идущего через Exchange. Это само по себе нелегкое для сервера решение, и утяжелять его безмерно еще антивирусом — не самый лучший вариант. Мы перепробовали много разных решений, но Dr.Web меньше всего замедляет работу нашего Exchange-сервера. Что нам нравится в продуктах Dr.Web — так это то, что вы в первую очередь заботитесь о корпоративных пользователях.

Павел Глушков,
системный администратор «Федеральной службы по надзору в сфере транспорта»

Dr.Web для Lotus Domino



- Достаточно часто почтовые серверы хранят почту пользователей — либо постоянно (пользователи хранят всю почту на сервере компании и получают к ней доступ по протоколу IMAP4), либо временно (до момента выхода сотрудника на работу).
  В связи с тем, что всегда имеется вероятность того, что вирус попадет в почту до того, как он попадет на исследование в антивирусную лабораторию, рекомендуется либо периодически проверять почтовые ящики пользователей на присутствие ранее не обнаруженных вирусов, либо проверять почту при ее отправке сотруднику.
- В том случае, если помещения компании или организации не сосредоточены внутри одного охраняемого периметра, а размещаются в нескольких местах и для связи между ними не используется выделенный канал, то прием и передача почтовых сообщений между этим частями компании должны осуществляться через шлюз — даже если помещения расположены в одном здании, всегда есть вероятность перехвата или подмены трафика.
- Отфильтрованная почта должна помещаться в карантин и/или архивироваться на случай возникновения тех или иных претензий, а также проведения расследований по инцидентам информационной безопасности.

Для обеспечения надежной защиты почтовых сервисов необходимо ответить на следующие вопросы:

- Все помещения и подразделения вашей компании размещены внутри одного охраняемого периметра?
- Используется ли в случае наличия удаленных сотрудников или подразделений для организации передачи данных выделенный канал, поддерживающий шифрование?
- Какие используются почтовые серверы (Exchange, Sendmail...)? На какой платформе работает ваш почтовый сервис (Windows, UNIX)?
- Доступен ли используемый почтовый сервер непосредственно из сети Интернет или отделен от нее почтовым шлюзом?
- Имеют ли сотрудники компании доступ к внешним почтовым сервисам?

Шлюзы сети Интернет

Наличие защиты шлюза необходимо, если серверы компании размещаются вне ее охраняемой территории, компания имеет филиалы или помещения компании разнесены по нескольким адресам или отдельным помещениям.

Компания «Доктор Веб» рекомендует

Использование средств защиты интернет-шлюза обеспечивает не только защиту от проникновения вирусов в локальную сеть, но и экономию трафика, а также управление правами доступа к различным ресурсам сети Интернет. Данные возможности используются в современных решения для защиты интернет-шлюзов.

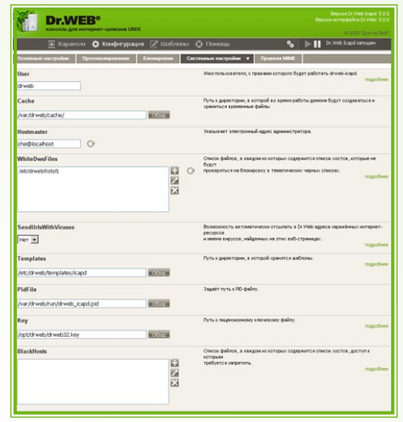
Внимание! Как и почтовый сервер, шлюз — это просто сервис, размещающийся на обычном сервере. Поэтому, если используемой файловой системой является Windows, кроме защиты почтового сервиса необходимо реализовать антивирусную защиту и самого сервера.

Согласно результатам исследования, начиная с февраля 2010 года российский интернет-домен (.ru) находится на первом месте по количеству зарегистрированного на нем нежелательного контента (спама), обогнав такие домены, как .com, .net, .cn (Китай) и .info.

При этом согласно исследованию типичное спам-сообщение рассылается с компьютера, физически расположенного в США, Индии или Бразилии, имеет URL-адрес на домене .ru, а его хостинг находится в Китае.

Отчет 2010 Mid-Year Trend and Risk Report, подготовленный группой исследований и разработок в области информационной защиты IBM X-Force

Dr.Web Gateway Security Suite



20,1% опрошенных участников сообщили, что сокращения затронули часть специалистов этой профессии.

Почти 7% респондентов ответили, что у них сократили всех сисадминов.

Индекс проникновения вредоносного кода в России во второй половине 2008 года вырос на 58% по сравнению с первым полугодием и составил 21,1.

Professionali.ru

Dr.Web Office Shield

Использование программно-аппаратных решений

Одними их основных проблем, с которыми сталкиваются компании в ходе внедрения и сопровождения антивирусных решений, являются:

- Недостаток времени на постоянный мониторинг антивирусной защиты.
- Отсутствие времени на изучение всех аспектов антивирусной безопасности и формирование собственной политики информационной безопасности.
- Проблемы с поиском необходимых специалистов, имеющих опыт работ, связанный с информационной безопасностью, и глубокие знания в области защиты от вирусов и спама.

Выходом является использование решений, готовых к работе с момента включения. Использование программно-аппаратных комплексов позволяет:

- снизить время развертывания системы защиты до минимума;
- упростить процедуры развертывания системы защиты и ее сопровождения за счет наличия удобного интерфейса управления, рассчитанного на неспециалистов;
- обеспечить защиту всей сети компании путем покупки одного интегрированного решения.

Компания «Доктор Веб» рекомендует

Использование программно-аппаратных средств обеспечивает не только минимальное время развертывания системы защиты и снижение расходов на обеспечение информационной безопасности, но и экономию трафика, а также выполнение требований законодательства в области антивирусной защиты и защиты от средств несанкционированного доступа.

Внимание! Dr.Web Office Shield обеспечивает не только защиту почтового и интернет-трафика, но и защиту компьютеров сети — использование Dr.Web Office Shield позволяет перекрыть все пути проникновения вирусов и спама в сеть компании.

Внимание! Dr.Web Office Shield может использоваться не только в уже существующей сети, но и для создания новых сетей — благодаря наличию соответствующих сервисов.

Внимание! Dr.Web Office Shield может использоваться для защиты как обычных, так и беспроводных сетей.

Централизованное управление антивирусной сетью компании

Только централизация всех аспектов защиты может дать реальную экономию средств.

Возможность единого «взгляда сверху» на антивирусную сеть предприятия любого масштаба с одного рабочего места, где бы оно ни находилось, минимальная трудоемкость развертывания сети и простота администрирования — все это сокращает необходимое для обслуживания системы время до минимума. Наличие удобного веб-интерфейса, возможность автоматизации работы за счет интеграции с системой Windows NAP и интерфейс для написания собственных обработчиков событий на скриптовом языке значительно снижают нагрузку на системных администраторов.

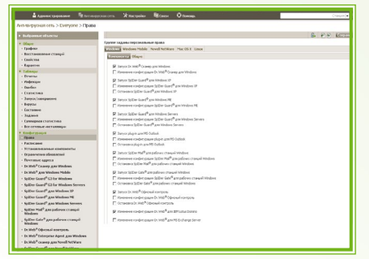
Использование функций централизованной защиты позволяет:

- благодаря наличию встроенных антивируса, антиспама, брандмауэра и офисного контроля обеспечить комплексную защиту всех узлов сети, в том числе:
  - рабочих станций и ноутбуков, работающих на платформах Windows и Mac OS X;
  - файловых серверов Windows и Novell NetWare;
  - почтовых серверов UNIX, Microsoft Exchange, IBM Lotus;
  - мобильных устройств на основе Windows Mobile;
- проводить централизованную установку, обновление и настройку программных средств антивирусной защиты, в том числе на недоступных с сервера компьютерах;
- оперативно управлять системой защиты локальной сети в любой момент времени, из любой точки мира, с любой операционной системы и без необходимости предварительной установки дополнительного программного обеспечения;
- реализовать необходимые для конкретного предприятия и отдельных групп сотрудников политики безопасности;
- назначать отдельных администраторов для различных групп;
- проводить антивирусную полную или выборочную проверку узла сети на наличие вирусных угроз как по команде пользователя или администратора, так и по расписанию;
- осуществлять сбор и анализ информации различного типа о состоянии системы защиты узлов локальной сети, а также создание отчетов за необходимый период времени;
- уведомлять администраторов и пользователей о состоянии системы защиты;

Как пишет The Wall Street Journal, за период с мая прошлого года по нынешний сентябрь криминальная сеть в США с помощью троянской программы Zeus похитила по меньшей мере 3 миллиона долларов, британская — не меньше 9,5 миллиона долларов.

http://www.rian.ru

Dr.Web Enterprise Security Suite



- проводить рассылку информационных сообщений пользователям в режиме реального времени.

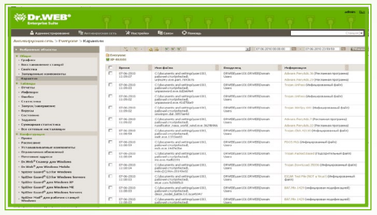
Возможность объединения серверов антивирусной защиты в иерархическую систему позволяет создать единую антивирусную сеть, состоящую из соединенных между собой рабочих станций, что, в свою очередь, позволяет не только наладить сбор консолидированной информации по всей сети на одном сервере, но и в целом повысить ее надежность. Даже в случае исключения из сети одного сервера обеспечивается необходимый уровень информационной безопасности компании! Возможность реализации иерархии серверов делает комплекс незаменимым для компаний, имеющих многофилиальную структуру, изолированную от сети Интернет.

Антивирусная сеть, основанная на Dr.Web Enterprise Security Suite, обладает высокой прозрачностью работы. Журнал аудита действий администраторов позволяет отслеживать все шаги по установке и настройке системы. Все компоненты антивирусной сети могут вести файлы отчетов с настраиваемым уровнем детализации. Любое действие над файлами, производимое компонентами антивирусной сети, отображается в статистике. Предусмотрена система оповещения администратора о проблемах, возникающих в антивирусной сети. Ее сообщения могут как отображаться в веб-интерфейсе администратора, так и приходить по электронной почте.

Продемонстрирован прототип руткита для смартфонов, способного выполнять функции прослушивающего устройства, скрыто от владельца аппарата включающего микрофон и инициирующего звонок по заданному телефонному номеру (прослушивание производится в рамках скрытого сеанса связи).

http://www.darkreading.com

Dr.Web Enterprise Security Suite



Дополнительный плюс Dr.Web Enterprise Security Suite — шифрование данных в процессе обмена информацией между его компонентами, что обеспечивает безопасное администрирование тысяч клиентов вне зависимости от того, в какой точке мира они находятся — невозможность перехвата трафика и его подмены дает дополнительную устойчивость системе защиты.

Индивидуализация информационной безопасности, внедрение плана активных мероприятий по предотвращению реализации различных угроз — все это позволяет создать ту среду, в которой будет невозможно существовать вирусам.

Почему Dr.Web?

С 1992 года развиваются и совершенствуются технологии антивирусных решений Dr.Web. Обширная география пользователей свидетельствует о степени исключительного доверия к продуктам компании.

Выгоды использования продуктов компании «Доктор Веб»

- Полная защита от существующих угроз. Использование продуктов компании «Доктор Веб» обеспечивает надежную защиту от большинства существующих угроз. Непревзойденное качество лечения и высокий уровень самозащиты не дают шанса вирусам и другим вредоносным объектам проникнуть в защищаемую сеть, а наличие встроенного брандмауэра и системы Офисного контроля не только преграждает путь вирусам через уязвимости операционных систем и программ, но и обеспечивает надежный контроль над работой установленных приложений.
- Увеличение производительности труда сотрудников. Внедрение комплексной защиты дает мгновенный положительный эффект. Снижение потока спама практически до нуля позволяет сотрудникам компании работать более эффективно — теперь важные сообщения не затеряются среди нежелательной корреспонденции. Исключение вероятности заражения компьютеров сети избавляет от простоев сотрудников во время восстановления информации, потерянной из-за вирусов.
- Сохранение репутации компании. Использование антивирусной системы не дает возможности злоумышленникам превратить сеть в источник вирусов и спама, которые могут попасть вашим клиентам. Использование антивируса от компании «Доктор Веб» — это надежная гарантия репутации компании как делового партнера.
- Снижение непрофильных затрат. Использование продуктов компании «Доктор Веб» позволяет не только снизить нагрузку на системных администраторов, с которых будет снята работа по устранению последствий вирусных эпидемий, но и:
  - уменьшить вынужденные простои сотрудников и предприятия в целом, связанные с необходимостью устранения последствий деятельности вирусов;
  - уменьшить стоимость закупаемых серверов и рабочих станций, на которые теперь не будет поступать поток вирусов и спама.
- Простота выбора нужной конфигурации. Для продуктов компании «Доктор Веб» используется гибкая система лицензирования — в отличие от многих решений клиент приобретает только те компоненты защиты, которые ему нужны, и не переплачивает за ненужные ему компоненты защиты или вообще целые продуктовые решения, которые никогда не будут им использоваться.
- Наличие сервиса Dr.Web LiveDemo позволяет системным администраторам протестировать выбранную конфигурацию комплекса еще до приобретения, непосредственно на серверах компании «Доктор Веб». Чтобы получить доступ к виртуальной локальной сети, необходимо лишь заполнить анкету, размещенную на соответствующей странице сайта, описав интересующую конфигурацию локальной сети.
- Установка в день приобретения. Клиенты компании «Доктор Веб» имеют возможность установки продукта в день платежа и даже ранее. Наличие сервиса мгновенной выписки лицензионных ключевых файлов сокращает время их получения до нескольких минут, в то время как на получение ключей от других производителей могут уходить дни и даже недели.
- Наличие сертификатов. В отличие от большинства конкурирующих решений, все продукты компании «Доктор Веб» имеют сертификаты соответствия ФСТЭК и ФСБ, что дает возможность использования комплекса в организациях, требующих повышенного уровня безопасности.
- Продукты компании «Доктор Веб» соответствует требованиям закона о защите персональных данных, предъявляемым к антивирусным продуктам, и могут применяться в сетях, соответствующих максимально возможному уровню защищенности.

Dr.Web — российские технологии для антивирусной защиты информации

Антивирусные продукты Dr.Web разрабатываются с 1992 года и созданы на основе собственной технологии. «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственной уникальной технологией детектирования и лечения вредоносных программ; имеет собственную службу вирусного мониторинга и аналитическую лабораторию. Это обуславливает высокую скорость реакции специалистов компании на новые вирусные угрозы, способность оказать помощь клиентам в решении проблем любой сложности в считанные часы.

Dr.Web имеет самый высокий в антивирусной индустрии процент эффективного лечения активного заражения.

Важным показателем качества работы антивирусной программы является не только ее способность находить вирусы, но и лечить их; не просто удалять инфицированные файлы вместе с важной для пользователя информацией, но и возвращать их в первоначальное «здоровое» состояние. Возможность работы на уже инфицированном компьютере и исключительная вирусоустойчивость выделяют Dr.Web среди всех других аналогичных программ.

Опыт крупных проектов

На основе продуктов компании «Доктор Веб» построены системы информационной безопасности практически всех крупных органов государственной власти России — Правительства РФ, Совета Федерации РФ, Администрации Президента РФ, Министерства обороны РФ, Министерства иностранных дел РФ, ФСБ, Министерства финансов РФ, Министерства образования и науки РФ и многих других госучреждений.

Система Dr.Web Enterprise Security Suite защищает сети многих крупных организаций с территориально распределенной структурой. Так, внедрение Dr.Web Enterprise Security Suite в системе ГАС «Правосудие», формирующей единую информационную среду для всех судов общей юрисдикции Судебного департамента при Верховном Суде РФ, позволило надежно защитить около 2000 тыс. судов, в числе которых находятся верховные суды республик РФ, областные и краевые суды, суды городов федерального значения и автономных округов, военные районные, гарнизонные суды, а также управления Судебного департамента в субъектах РФ, ресурсы Судебного Департамента при Верховном Суде РФ.

Приложение 1.

Термины и определения

ЛВС — локальная вычислительная сеть компании.

Антивирусная сеть — совокупность компьютеров и устройств, защищенных антивирусными средствами.

Администратор или системный администратор — сотрудник, обеспечивающий управление ЛВС.

ИТ-инфраструктура — комплекс аппаратного и программного обеспечения, позволяющего осуществлять деятельность компании или организации с использованием ЛВС, осуществлять в соответствии с политикой информационной безопасности использование сети Интернет, а также осуществлять защиту ЛВС от доступа вредоносных программ.

ИС — информационная система.

НСД — несанкционированный доступ (к информации).

СКС — структурированная кабельная система.

Опорная сеть — фрагмент СКС, состоящий из коммутационного оборудования и выполняющий функции организации VLAN, обеспечения отказоустойчивости, безопасности и маршрутизации сетевого трафика между VLAN.

VLAN — выделенный сегмент ЛВС, используемый для группирования пользователей СКС по какому-либо признаку, например по подразделению.

Сеть периметра — компьютерная сеть, логически находящаяся между ЛВС и сетью Интернет и предназначенная для концентрации средств защиты информации с целью защиты ИТ-инфраструктуры от ИТ-угроз.

DMZ (демилитаризованная зона) — часть сети периметра, доступная для взаимодействия из сети Интернет.

Ботнет — сеть зараженных компьютеров, управляемых из единого центра и предназначенных, как правило, для проведения распределенных атак или распространения спама.

Приложение 2.

Требования в области защиты информации

На данный момент существует два обязательных к исполнению на территории Российской Федерации документа, описывающих требования по защите информации:

- стандарт ИБ ЦБ РФ СТО БР ИББС-1.0-2010;
- Федеральный закон № 152-ФЗ «О персональных данных».

Если стандарт СТО БР является обязательным только для банковской сферы, то Федеральный закон № 152-ФЗ обязателен для всех компаний и организаций, вне зависимости от рода их деятельности, а также для физических лиц.

Кроме этого, существует «Доктрина информационной безопасности Российской Федерации» (http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm) и ряд других документов и стандартов (например, ГОСТ Р ИСО/МЭК 13569 «Финансовые услуги. Рекомендации по информационной безопасности»; ГОСТ Р (МС ИСО/МЭК 13335) «Информационные технологии»; ГОСТ Р (МС ИСО/МЭК ТО 18044) «Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности»; ГОСТ Р (МС ИСО/МЭК 15408) «Информационная технология. Методы и средства обеспечения безопасности»). Однако все они либо не являются обязательными, либо относятся только к определенным организациям.

В связи с этим более подробно ниже будут рассмотрены только требования СТО БР и Федерального закона № 152-ФЗ.

Стандарт ИБ ЦБ РФ СТО БР ИББС–1.0–2010

Банковская сфера является одной из немногих, если не единственной жестко регламентируемой областью деятельности. В частности, системы информационной безопасности банков должны соответствовать требованиям стандарта ИБ ЦБ РФ СТО БР ИББС-1.0-2010, закона о защите персональных данных, других стандартов, описывающих требования в области безопасности (например, ГОСТ Р ИСО/МЭК 13569). Жестко регламентируется работа с пластиковыми карточками. При этом локальные сети кредитных организаций достаточно сложно организованы — банки имеют филиалы в самых труднодоступных уголках страны и за ее пределами, поддерживаются внешние устройства (банкоматы), имеется возможность удаленного входа для сотрудников и клиентов банка.

Стандарт Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» является достаточно зрелым — на данный момент уже существует три его редакции, последняя введена в действие в июне 2010 года. На данный момент стандарт:

- определяет терминологию, основные модели угроз и задачи организаций по их выявлению;
- перечисляет основные типы объектов, подлежащих защите, прав доступа и соответствующих им ролей персонала;
- дает рекомендации по конфигурации сети;
- определяет требования по антивирусной защите, политике использования ресурсов Интернета на различных этапах жизненного цикла сети.

В части программного обеспечения, согласно требованиям стандарта, должна быть обеспечена защита от:

- умышленного либо неумышленного раскрытия, модификации или уничтожения защищаемых данных. В частности, это подразумевает необходимость использования средств ограничения доступа к различным ресурсам — офисного контроля;
- установки средств защиты кем-либо, кроме администратора, несанкционированного внесения изменений в порядок функционирования системы защиты, изменения ее возможностей. Данное требование приводит к необходимости разграничения прав доступа к настройкам системы, защите ее от несанкционированного воздействия. Это подразумевает использование в локальной сети только программных продуктов, поддерживающих ролевой принцип доступа, а также применение уже упомянутых функций офисного контроля.

Антивирусная защита должна быть эшелонированной, а средства защиты должны устанавливаться как на рабочие станции, так и на серверы.

В организации, соответствующей требованиям стандарта, должна использоваться только защищенная почта, что вместе с требованием о наличии защиты от вирусов и спама подразумевает установку средств антивирусной фильтрации почтовых сообщений. Причем в связи с тем, что в соответствии со стандартом все серверы (в том числе и почтовые) не должны иметь непосредственного выхода в Интернет, система антивирусной защиты может быть разделена на две части: антивирусный шлюз, имеющий выход в Интернет или вынесенный в демилитаризованную зону, и непосредственно почтовый сервис. Такая конфигурация позволяет снизить нагрузку на сервер благодаря возможности отсечения потока спама до его поступления внутрь сети. Дополнительным требованием к почтовому сервису является необходимость обеспечения архивации всех почтовых сообщений. Функция архивации может быть возложена как на сервис антивирусной защиты (в случае поддержки им данного функционала), так и на специализированное ПО.

В свою очередь доступ в сеть Интернет должен использоваться только для обеспечения банковской деятельности, что подразумевает использование как средств офисного контроля (для ограничения списка доступных ресурсов глобальной сети), так и средств проверки трафика (для предотвращения проникновения вирусов с доступных для доступа, но взломанных ресурсов). Дополнительным требованием является наличие системы защиты от хакеров, то есть как минимум качественного файервола.

Все используемые в организации средства защиты должны быть легально приобретены.

Суммируя вышеприведенные требования, можно сказать, что антивирусный продукт для банковской сферы должен отвечать следующим требованиям:

- Возможность обеспечения централизованной защиты сети.
- Поддержка ролей с различным уровнем доступных прав — как администраторов, так и простых пользователей.
- Возможность защиты всех узлов сети — рабочих станций и серверов, вне зависимости от используемой на них операционной системы. В стандарте не оговариваются требования по защите внешних и встроенных систем (в том числе) банкоматов. Однако логично, что в случае использования на них операционных систем, для которых существуют вирусы, они тоже должны быть защищены от проникновения вирусов.
- Наличие, кроме функции защиты от вирусов, системы защиты от спама, офисного контроля, файервола, системы контроля трафика.

- По возможности должна быть доступна функция архивации почтовых сообщений.
- Возможность обеспечения антивирусной защиты в локальной сети, не имеющей прямого доступа в Интернет, в том числе получения и распространения обновлений в такой сети, вынесения ряда сервисов в демилитаризованную зону.

Положения стандарта СТО БР ИББС-1.0-2010 развивают и уточняют:

- СТО БР ИББС-1.1-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит ИБ».
- СТО БР ИББС-1.2-2010 «Обеспечение ИБ организаций банковской системы РФ. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.0-2007 «Обеспечение ИБ организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения ИБ».
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.1-2007 «Обеспечение информационной безопасности организаций банковской системы РФ. Методические рекомендации по документации в области обеспечения ИБ».
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ».
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.3-2010 «Обеспечение ИБ организаций банковской системы РФ. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы РФ».
- Рекомендации в области стандартизации Банка России РС БР ИББС-2.4-2010 «Обеспечение ИБ организаций банковской системы РФ. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах ПД организаций банков банковской системы РФ».

В общем случае процедура приведения системы информационной безопасности в соответствие с требованиями стандарта Банка России включает в себя:

- выявление несоответствий требованиям стандарта, а также определение порядка действий по приведению системы информационной безопасности в соответствие с требованиями;
- разработку требуемой нормативной документации, закупку и настройку необходимых технических решений, обучение персонала;
- введение в практику необходимых управленческих процедур;
- проведение итоговой оценки и, при необходимости, повторение процедуры.

В результате выполнения данной процедуры в компании будет создана работающая эффективная и надежная система информационной безопасности, включающая в себя как технические средства, так и процедуры действий в тех или иных случаях.

Более подробно ознакомиться с требованиями стандарта можно по адресу: http://www.abiss.ru/doc.

Внимание! На данный момент стандарт ИБ ЦБ РФ СТО БР ИББС-1.0-2010 является наиболее проработанным документом, регламентирующим требования в области защиты от ИТ-угроз. В связи с этим данный стандарт рекомендуется для использования всем компаниям и организациям.

Федеральный закон № 152–ФЗ «О персональных данных»

Вопреки устоявшемуся мнению Федеральный закон № 152-ФЗ «О персональных данных» описывает защиту не всей локальной сети, а только персональных данных, обрабатываемых на компьютерах данной сети, — защита всех остальных компьютеров и каналов передачи данных в сферу действия данного закона не попадает. Именно в связи с этим возможно снижение стоимости системы защиты сети в целом — обезличивание данных или изоляция их обработки на отдельные компьютеры позволяют относить требования закона только к этим компьютерам, а не ко всей сети.

При этом сам Федеральный закон № 152-ФЗ «О персональных данных» практически не определяет никаких требований по защите — все требования содержатся в документах регуляторов (уполномоченных федеральных органов — Россвязькомнадзора, ФСБ и ФСТЭК) и постановлениях правительства. Список документов, содержащих требования, достаточно велик, но основными являются следующие:

- Постановление Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
- Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Постановление Правительства РФ от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
- Нормативно-методические документы регуляторов. В том числе:
  - Совместный приказ от 13.02.2008 № 55/86/20 ФСТЭК, ФСБ, Мининформсвязь, утверждающий «Порядок проведения классификации информационных систем персональных данных»;
  - «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная 15 февраля 2008 г.;
  - «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная 14 февраля 2008 г.;
  - «Положение о методах и способах защиты информации в информационных системах персональных данных».

В отдельных случаях кроме этих документов нужно учитывать положения других постановлений и законов. Так, в случае использования биометрических систем нужно использовать постановление Правительства РФ № 512 от 06.07.2008 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных». При защите персональных данных государственных служащих нужно учитывать требования федеральных законов «О муниципальной службе в РФ», «О системе государственной гражданской службы РФ», «О государственной гражданской службе РФ» и других.

Одним из распространенных мифов, окружающих Федеральный закон № 152-ФЗ, является миф, гласящий, что принятие закона отложено. Это не так. Выполнение закона отложено для локальных сетей, существовавших на момент принятия закона, — таким образом, все новые сети должны соответствовать его положениям уже сейчас.

Согласно закону операторами являются все физические и юридические лица, вне зависимости от формы собственности, размера и рода деятельности. Исключений немного: действие закона не распространяется на:

- обработку персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
- хранение и использование архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- обработку персональных данных, отнесенных к сведениям, составляющим государственную тайну.

Закон и документы регуляторов определяют:

- кто является оператором персональных данных;
- права и обязанности операторов персональных данных;
- список регуляторов;
- правила обработки персональных данных;
- порядок заполнения и подачи уведомления об обработке персональных данных;
- виды проверок и порядок их проведения регулятором;
- список документов, необходимых к созданию в процессе внедрения положений закона;
- виды угроз и порядок определения их важности;

- порядок классификации информационной системы;
- методы защиты персональных данных в зависимости от классификации системы и актуальных угроз.

В области антивирусной защиты внедрение Федерального закона № 152-ФЗ требует:

- внедрения антивирусной защиты на всех серверах и рабочих станциях, где осуществляется обработка персональных данных;
- обеспечения необходимого уровня доступа только к необходимым ресурсам;
- защиты каналов доступа в Интернет;
- использования централизованно управляемой защиты.

Все это подразумевает:

- использование на рабочих станциях и файловых серверах централизованно управляемой комплексной защиты, включающей средства защиты от вирусов, а также офисный контроль;
- централизованно управляемую антивирусную защиту почтовых серверов и интернет-шлюзов.

Приложение 3.

Основные возможности решений на основе Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite предназначен для обеспечения централизованной защиты локальных сетей любого типа от спама и вредоносных объектов любого типа.

Внедрение Dr.Web Enterprise Security Suite позволяет обеспечить:

- Защиту файловых серверов и рабочих станций (в том числе защиту мобильных устройств и ноутбуков). Так, для операционных систем типа Windows обеспечивается:
  - защита входящей и исходящей электронной корреспонденции по протоколам IMAP, SMTP, POP3 независимо от используемого почтового клиента, как от вредоносных программ, так и от спама;
  - проверка всех объектов, поступающих на компьютер пользователя по протоколу HTTP, до их поступления в локальный кэш браузера;
  - защита от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам, в том числе сменным дискам, каталогам и интернет-сайтам.
- Антивирусную полную или выборочную проверку узла сети на наличие вирусных угроз как по команде пользователя или администратора, так и по расписанию.
- Централизованную установку, обновление и настройку программных средств антивирусной защиты, в том числе на недоступных с сервера узлах сети.
- Настройку различных ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне.
- Сбор и анализ информации различного типа о состоянии системы защиты узлов локальной сети, а также создание отчетов за необходимый период времени.
- Уведомление администраторов и пользователей о состоянии системы защиты.
- Рассылку информационных сообщений пользователям в режиме реального времени.
- Автоматическое резервное копирование критически важных данных и конфигурации антивирусного сервера по заранее заданному расписанию, а также восстановление сервера из резервной копии.

Особенностями Dr.Web Enterprise Security Suite являются:

- Возможность управления системой защиты через веб-интерфейс — из любой точки сети Интернет и без необходимости установки какого-либо дополнительного ПО.
- Наличие технологий, позволяющих минимизировать время проверки и загрузку рабочей станции (в том числе за счет многопоточной проверки и отложенной проверки файлов, открываемых «на чтение»), что обеспечивает комфортную работу пользователей даже на компьютерах со слабой конфигурацией.
- Наличие технологий, позволяющих обнаруживать новейшие вирусы, в том числе скрытые под неизвестными упаковщиками.
- Проверка файлов и почтовых сообщений до попадания их в соответствующие приложения, что не дает возможности хакерам воспользоваться уязвимостями программного обеспечения.
- Отсутствие необходимости обучения системы антиспама, использующей современные эвристические механизмы.
- Возможность организации автоматической системы реагирования на вирусные атаки без дозакупки специализированных аппаратных комплексов.
- Наличие системы самозащиты, что не дает возможности вирусам вывести систему из строя.

Внимание! Dr.Web Enterprise Security Suite Антивирус обеспечивает только обнаружение и лечение вирусов любого типа, но не обеспечивает защиты от спама, возможность ограничения доступа к различным интернет-ресурсам, отдельным дискам, папкам или файлам, проверки интернет-трафика до поступления его в различные программы. Данные возможности доступны только в Dr.Web Enterprise Security Suite Комплексная защита.

Использование Dr.Web Enterprise Security Suite позволит не только исключить возможность проникновения вирусов и спама в локальную сеть, но и поднять производительность труда сотрудников, высвободить время системных администраторов для решения актуальных задач.

Сервер антивирусной защиты может быть установлен на операционные системы:

- Microsoft Windows 2000/XP/2003/Vista/2008/7 (32- и 64-битные системы);
- Linux (основанные на glibc версий 2.3 и выше) и FreeBSD (версий 6.4 и выше) (32- и 64-битные системы);
- Solaris (для платформ Intel и Sparc).

Dr.Web Enterprise Security Suite поставляется в конфигурации, обеспечивающей надежную защиту при работе в локальной сети и Интернет с веб-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также сетевыми ресурсами. Системный администратор может самостоятельно определить уровень защиты каждого компьютера сети в зависимости от уровня угроз и действующей политики информационной безопасности.

Dr.Web Enterprise Security Suite одинаково надежно работает в сетях любого размера и сложности. Комплекс может быть адаптирован для работы как в простых сетях, состоящих из нескольких компьютеров, так и в сложных распределенных интранет-сетях, насчитывающих десятки тысяч узлов. Масштабирование обеспечивается за счет возможности использования иерархии взаимодействующих серверов Dr.Web Enterprise Security Suite и отдельного SQL-сервера для хранения данных, наличия комплексной структуры взаимодействия между ними и защищаемыми узлами сети.

Dr.Web Enterprise Security Suite обладает минимальной совокупной стоимости по сравнению с конкурирующими программами благодаря возможности развертывания сети под Windows- и UNIX-серверами, простоте установки и надежности защиты, возможности установки на 32- и 64-битные операционные системы. С учетом традиционных для компании «Доктор Веб»:

- высокой эффективности обнаружения угроз, включая еще не известные вирусы,
- минимальной нагрузки на сеть благодаря компактности ядра и использованию в нем новейших технологий,
- возможности установки на уже зараженную систему,

использование Dr.Web Enterprise Security Suite является оптимальным выбором.

Dr.Web Enterprise Security Suite имеет в своем составе решения для защиты всех узлов сети — рабочих станций, терминальных клиентов, почтовых серверов, интернет-шлюзов и мобильных устройств.
В частности, Dr.Web для MS Exchange обеспечивает:

- проверку всех входящих и исходящих сообщений в реальном времени с учетом индивидуальных настроек групп и отдельных пользователей;
- фильтрацию и блокировку спама, в том числе по белым и черным спискам адресов;
- изоляцию инфицированных и подозрительных объектов в карантине;
- фильтрацию электронных писем по различным критериям;
- отправку уведомлений о вирусных событиях;
- ведение журнала вирусных событий;
- сбор статистики и рассылку отчетов о работе программы.

Особенностями Dr.Web для Microsoft Exchange Server являются:

- Возможность установки для любых ролей Microsoft Exchange Server.
- Наличие антиспама, что дает возможность существенно снизить нагрузку на сервер, увеличить производительность труда сотрудников компании.
- Отсутствие необходимости обучения антиспама — Dr.Web для Microsoft Exchange Server 2007 готов к фильтрации спама с момента установки.
- Наличие черных и белых списков адресов, что позволяет как исключать из проверки определенные адреса, так и увеличивать ее эффективность.
- Наличие возможности фильтрации по типам файлов, что позволяет снизить трафик компании.
- Наличие возможности группировки, что позволяет настроить продукт с учетом потребностей различных групп пользователей, а наличие системы наполнения состава групп из Active Directory существенно сокращает введение системы антивирусной защиты в строй и упрощает сопровождение продукта.
- Наличие механизма обнаружения вирусов, скрытых неизвестными упаковщиками.
- Наличие дополнительных механизмов обнаружения неизвестных угроз, что увеличивает вероятность обнаружения вирусов новейших типов.

Необходимо особо отметить возможность поставки Dr.Web Enterprise Security Suite в предустановленном виде — в виде компактного программно-аппаратного комплекса Dr.Web Office Shield, максимально готового к началу работы.

Dr.Web Office Shield включает в себя:

- средства защиты почтового и интернет-трафика;
- средства защиты рабочих станций и серверов от вирусов и спама;
- средства ограничения доступа как к локальным ресурсам, так и ресурсам сети Интернет;
- средства анализа и ограничения интернет-трафика;
- корпоративный и персональный брандмауэры.

Dr.Web Office Shield может использоваться как в уже существующей сети, так и для создания новых сетей.

Использование программно-аппаратных комплексов позволяет:

- обеспечить полную антивирусную защиту филиалов компании за счет использования одного продукта;
- снизить время развертывания системы защиты до минимума;
- упростить процедуры развертывания системы защиты и ее сопровождения за счет наличия удобного интерфейса управления, рассчитанного на неспециалистов;
- обеспечить защиту всей сети компании либо филиала путем покупки одного устройства.

Dr.Web Enterprise Security Suite сертифицирован ФСТЭК на соответствие:

- ТУ и НДВ 4 на применение в составе подсистемы антивирусной защиты 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 уровню контроля отсутствия недекларированных возможностей» и требованиям технических условий.

Приложение 4.

Что такое сертифицированное ПО?

Сертифицированным программным обеспечением является:

- ПО, прошедшее проверку соответствия в Системе сертификации средств защиты информации по требованиям государственных стандартов и нормативных документов по защите информации ФСТЭК России и ФСБ России, что подтверждается сертификатом соответствия. ПО сертифицируется на соответствие техническим документам (РД, ТУ или ЗБ) и с параметрами, указанными в этой документации.
- ПО, дистрибутив которого соответствует эталонному экземпляру, подвергавшемуся сертификационным испытаниям, что подтверждается соответствующими записями в сопроводительной документации на сертифицированное ПО (формуляре) и специальным голографическим знаком соответствия с уникальным номером, который идентифицирует данный экземпляр в системе государственного учета сертифицированных продуктов.
- ПО, механизмы защиты развернутой версии которого настроены в соответствии с сертифицированными параметрами.
- ПО, все доработки (обновления) которого, критичные для безопасности, подвергаются сертификационным испытаниям и доводятся до конечного пользователя. При выпуске обновлений и исправлений в системе безопасности сертифицированного продукта производитель обязан предоставить обновления на сертификацию и довести информацию до потребителя.
- ПО, контролируемое в процессе эксплуатации. ПО должно иметь средства контроля целостности, учета событий внедрения в ПО обновлений безопасности, контроля защищенности в процессе эксплуатации. У потребителя должны быть механизмы проверки целостности обновлений средств защиты с использованием контрольных сумм.
- ПО, каждый сертифицированный экземпляр которого учтен в реестре сертифицированных продуктов. Производитель обязан маркировать средства защиты и обеспечивать беспрепятственный доступ должностных лиц органов, осуществляющих контроль над сертифицированными средствами защиты, к учетной информации.

Комплект поставки сертифицированного ПО должен включать:

- копию сертификата соответствия (заверенную печатью заявителя);
- верифицированный дистрибутив ПО, формуляр с указанием контрольной суммы дистрибутива и специальный голографический знак соответствия;
- документацию и материалы для настройки ПО в соответствии с сертифицированными параметрами, приведенными в технической документации;
- все необходимые инструменты для получения потребителем обновлений безопасности;
- все необходимые программные средства (встроенные или наложенные), предназначенные для выполнения данных требований в области целостности, учета событий внедрения в ПО обновлений безопасности, контроля защищенности в процессе эксплуатации.

Каждый экземпляр сертифицированного ПО сопровождается уникальными номерами, идентифицирующими средство защиты в соответствии с порядками, установленными для данной системы сертификации.

Требования в области использования сертифицированного программного обеспечения к каждой конкретной компании формируются на основе положений, методических и нормативных документов в области технической защиты информации (включая «Доктрину информационной безопасности Российской Федерации», Федеральный закон от 20 февраля 1995 г. № 24-ФЗ и постановление № 781 от 17 ноября 2007).

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

Украина

Центр технической поддержки «Доктор Веб»
01001, Киев, пер. Михайловский, 17
Телефон/факс: +38 (044) 238-24-35, 279-20-38
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