Dr.WEB®
с 1992 года

Защити созданное

Курс DWCERT-070-3 Антивирусная система защиты (АСЗ) предприятия

Специальность:
сертифицированный специалист по антивирусной системе защиты предприятия

План

Дата актуализации 11.02.2014 г

I. Современные вирусные угрозы

ЗАБЛУЖДЕНИЕ

Вирусы пишут хакеры-одиночки.

Уже давно прошло то время, когда создателями вредоносного ПО были программисты-одиночки. Современные вредоносные программы разрабатываются не просто вирусописателями-профессионалами — 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 распределены следующим образом:

1. **Организаторы** — лица, которые организуют 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
   - 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

Такая «организация труда» позволила криминальным группировкам организовать тестирование разрабатываемых ими вредоносных программ на необнаружение всеми актуальными антивирусными решениями. Тестирование создаваемого вредоносного ПО на актуальных версиях антивирусов позволяет злоумышленникам внедрять жертвам вирусы и троянцев в обход антивирусной защиты. Ни одна антивирусная программа, как бы хороша она ни была в тестах на эвристики, не сможет ничего в этом случае сделать.

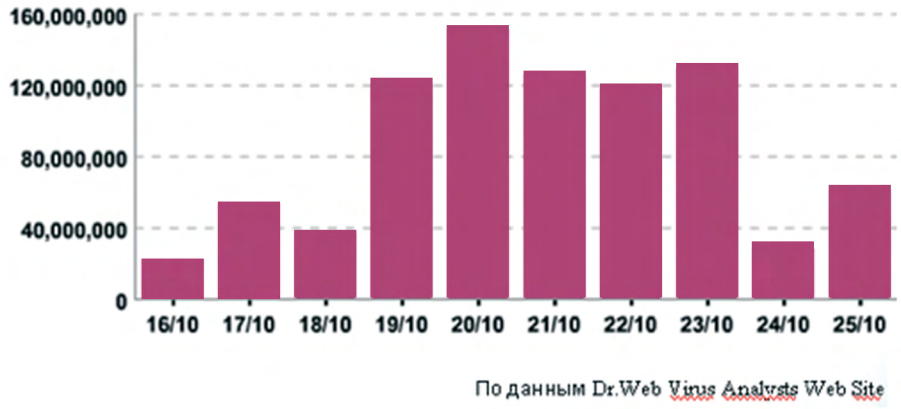
Также все чаще криминальные группировки создают так называемые таргетированные угрозы — вредоносные программы, разработанные для заражения конкретных групп пользователей (например, пользователей одного банка). Как правило, это качественно написанные вредоносные программы, не оказывающие существенного влияния на работу зараженных машин и в момент заражения не опознаваемые средствами защиты, что позволяет им оставаться необнаруженными в течение длительного времени.

В результате перехода к «промышленным» методам выпуска вредоносных программ в «дикую природу» выпускаются только те вредоносные программы, которые не обнаруживаются (до получения обновлений) антивирусами — даже с помощью эвристических механизмов. Это привело **к резкому росту количества необнаруживаемых на момент проникновения вредоносных программ.**

Переход вирусописательства в руки криминала обесценил тесты антивирусных программ как критерии выбора средства антивирусной защиты.

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

Дата актуализации 11.02.2014 г



Факты

- Служба вирусного мониторинга «Доктор Веб» производит сбор образцов вирусов по всему миру.
- Ежесуточно в антивирусную лабораторию «Доктор Веб» поступает в среднем более 100 000 образцов вредоносных программ.

Подробнее: http://live.drweb.com.

Вирусные аналитики — не волшебники, и мгновенно обработать многие тысячи ежедневно поступающих подозрительных файлов они не могут. Важнейшим элементом противодействия вредоносным программам являются автоматизированные системы обработки входящего потока подозрительных файлов, которые имеются у антивирусных компаний. Качество работы этих систем имеет не меньшее значение, чем качество работы коммерческих продуктов, работающих на компьютерах пользователей.

ЗАБЛУЖДЕНИЕ

Антивирус должен обнаруживать 100% вирусов.

Предыстория возникновения заблуждения

В антивирусной отрасли давно существуют так называемые 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, нужно 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, находящимися в неактивированном виде;
- такие тесты не показывают, насколько хорошо ведет себя антивирус в реальных условиях заражения компьютера вирусом, как он умеет лечить тот или иной вирус, 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 (так называемые 0day exploits — уязвимости, о которых пока известно только вирусописателю или для исправления которых производитель ПО пока еще не выпустил «заплатки»), либо с использованием методов социальной инженерии — т. е. будет запущен самим пользователем, который в том числе может отключить самозащиту антивируса.

ЗАБЛУЖДЕНИЕ

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.

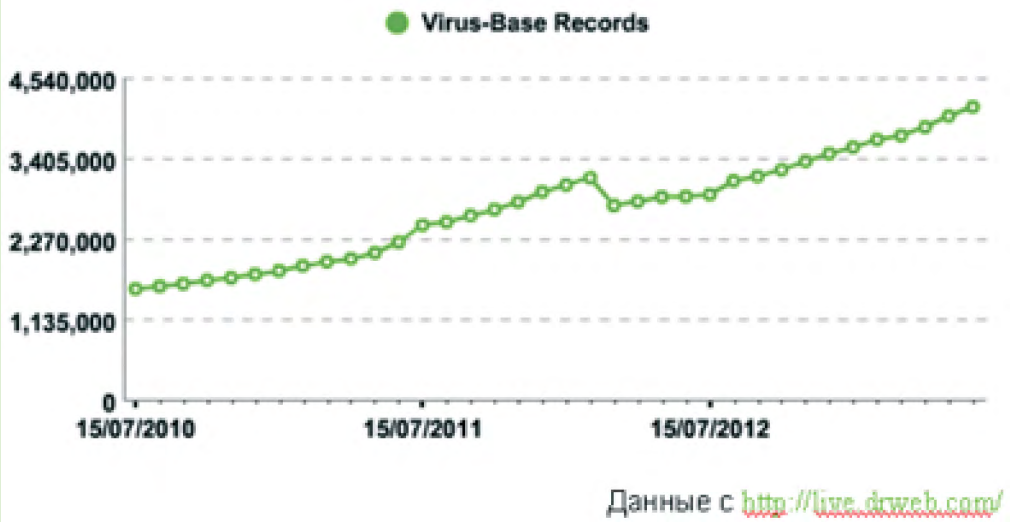
- **Технология FLY-CODE** — обеспечивает качественную проверку упакованных исполняемых объектов, распаковывает любые (даже нестандартные) упаковщики методом виртуализации исполнения файла, что позволяет обнаружить вирусы, упакованные даже неизвестными антивирусному ПО Dr.Web упаковщиками.
- **Технология 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.

Дата актуализации 11.02.2014 г

- **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.
- Компания «Доктор Веб» постоянно развивает технологии обнаружения вредоносных программ и выпускает новые версии антивирусного ядра. Но выпуск антивирусного ядра – это не только новые технологии, это оптимизация кода и снижение количества вирусных записей, что тоже положительно сказывается на скорости работы.



Снижение темпов роста количества записей – это итог внедрения новых технологий обнаружения: Dr.Web умеет обнаружить большее количество вредоносных программ меньшим количеством записей!

- 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 вирусных 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?

- Высокая скорость поиска вредоносных программ
- Снижение системных требований
- Экономия места на диске
- Экономия трафика при обновлении баз
- Возможность определять вирусы, которые появятся в будущем путем модификации уже существующих версий

Дата актуализации 11.02.2014 г

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.

ЗАБЛУЖДЕНИЕ

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

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.

ВНИМАНИЕ!

Антивирус действительно не всегда может обнаружить новейшую вредоносную программу, рассчитанную на скрытое проникновение, — но никакое другое программное обеспечение, кроме антивируса, не способно вылечить систему от уже проникшего троянца.

ЗАБЛУЖДЕНИЕ

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

Факты

- Современные вредоносные программы зачастую рассчитаны на долговременное присутствие на компьютере жертвы. Поэтому они не просто действуют незаметно для пользователя и не определяются на момент их создания многими антивирусными программами — существуют вредоносные программы, борющиеся с конкурентами и удаляющие иные вредоносные программы. Есть даже вредоносные программы, закрывающие уязвимости на компьютере!

- 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.

ЗАБЛУЖДЕНИЕ

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 меньше времени, 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.

Информационные ресурсы о современных вирусных угрозах

- Антивирусная лаборатория «Доктор Веб»: http://live.drweb.com
- Описания вирусов и вредоносных программ: http://vms.drweb.com/search
- Обзоры о вирусах и спаме: http://news.drweb.com/list/?c=10
- Горячая лента угроз: http://news.drweb.com/list/?c=23
- Подписка на рассылку новостей о вирусах и обзоры: https://news.drweb.com/news/subscribe
- Отправка подозрительного файла на анализ: https://vms.drweb.com/sendvirus
- Онлайн-сканер Dr.Web: http://vms.drweb.com/online

Дата актуализации 11.02.2014 г

II. Пути проникновения вирусных угроз в корпоративные сети

Большинство компаний совершают грубейшие ошибки при построении системы антивирусной защиты, руководствуясь устаревшими сведениями о путях проникновения вредоносных программ и их возможностях.

Для организации эффективной антивирусной системы защиты локальной сети ИБ-специалистам компании важно знать **актуальные** пути проникновения вредоносных программ в локальную сеть. Наиболее распространенными на сегодняшний день путями являются:

1. Уязвимости

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).

Вирус может проникнуть на компьютер через уязвимости нулевого дня, либо с использованием методов социальной инженерии — т. е. будет запущен самим пользователем, который в том числе может отключить самозащиту антивируса.

ВНИМАНИЕ!

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

ВНИМАНИЕ!

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

Автоматическое обновление антивируса категорически нельзя отключать!

2. Веб-сайты

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

- выходит в Интернет с рабочего компьютера, на котором стоит ПО, имеющее уязвимости;
- работает под Windows с правами администратора;
- работает, используя простые пароли, взлом которых не составляет труда;
- не производит обновления безопасности всего программного обеспечения, установленного на ПК.

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

*Троянцы семейства Carberp проникают на компьютеры пользователей **во время просмотра взломанных сайтов**. Не нужно предпринимать вообще никаких действий для того, чтобы «получить троянца»: **заражение происходит автоматически**.*

Дата актуализации 11.02.2014 г

Сайты, которые чаще всего являются источниками вредоносного ПО (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

3. Съемные устройства

Даже в серьезно 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.

4. Личные, в том числе мобильные устройства сотрудников

Сегодня более 60% работников имеют удаленный доступ к корпоративной информации с личных устройств, включая мобильные.

Увлеченные сотрудники работают не только в рабочее время и не только в офисе компании, 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.

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

- Мишенями атак преступных киберсообществ давно перестали быть только офисные ПК — атакам подвергаются и личные устройства сотрудников, включая мобильные устройства.
- Почти две трети работников (63,3%) имеют удаленный доступ к корпоративной информации с личных устройств, включая мобильные.
- До 70% случаев заражений локальных сетей происходит 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 пользователи никак не защищены от атак хакеров, используемые ими приложения могут иметь уязвимости, на компьютерах могут быть вирусы и троянцы. При этом эти люди регулярно заходят в локальную сеть компании.
- Это создает возможность утечки, подмены или компрометации важных для компании данных.

Дата актуализации 11.02.2014 г

Факты

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

5. Электронная почта

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 коллег, но и адреса клиентов и партнеров — т. е. распространение заражения начнется не только по локальной сети компании, но и за ее пределы.

Небрежность, халатность и простое незнание основ компьютерной безопасности сотрудников компании зачастую являются причинами того, что компьютеры компании становятся частью бот-сетей и источником спама, что вредит имиджу компании, может привести к внесению компании в черные списки и отключению от сети Интернет за рассылку спама.

6. Социальная инженерия

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 от администраций 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.

III. Задачи компании. Связь задач со структурой локальной сети

Как правило, в ходе работы сотрудники типичной компании:

- создают текстовые и графические файлы на компьютерах и мобильных устройствах;
- получают и отправляют почтовые сообщения — как внутри самой компании, так и внешним адресатам;
- получают, отправляют, дают возможность получить извне те или иные данные — обычно в виде файлов;
- помещают в файловое хранилище компании или скачивают из него хранящуюся там информацию — в том числе в виде файлов.

Найти компании и организации, в которых не выполняются эти задачи, достаточно сложно. Поэтому в подавляющем числе случаев при решении вопроса об организации антивирусной системы защиты вопрос стоит не в том, выполняются или нет эти задачи, а в том, сколько сотрудников выполняет те или иные задачи.

Для выполнения задач компании в состав ее локальной сети должны входить:

- **рабочие станции и/или терминальные клиенты** — места, на которых работают сотрудники компании или ее посетители;
- **файловые серверы** — для хранения информации, в том числе файлов и документов, и обмена информацией между сотрудниками компании;
- **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 и т. д.;
- **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).

Естественно, не все эти компоненты встречаются всегда — а кроме перечисленных выше встречаются и иные компоненты локальной сети, но в подавляющем большинстве случаев в любой организации есть рабочие станции и как минимум один почтовый сервер, и один интернет-шлюз (он же может быть компьютером, к которому приходит кабель от провайдера услуг сети Интернет).

Исключений совсем немного:

- **Все или часть сотрудников выходят в Интернет по своему каналу связи.** В этом случае и сервер, и интернет-шлюз отсутствуют. Данный вариант достаточно затратен для компании и поэтому редок. Может встречаться либо в компаниях крайне небольшого размера (например, нотариальных конторах), либо в случае использования в компании большого количества внешних сотрудников. Такие сотрудники для обмена информацией используют общедоступные сервисы.
- **Компания использует внешние серверы.** Как правило, арендуются почтовые адреса или почтовые домены на внешнем сервере (например, на gmail.com).

Дата актуализации 11.02.2014 г

Таким образом, вопрос о том, есть ли в компании серверы, практически никогда не стоит. Вопрос заключается в том,

- сколько в компании серверов — в том числе и тех, защита которых клиентом на данный момент не предполагается;
- насколько совмещены их роли;
- где они размещены (локально или удаленно);
- как к ним получают доступ пользователи (по локальной сети или удаленно через сеть Интернет) и т. д.

Локальные сети провайдеров услуг

Особенностью сетей провайдеров услуг, и в первую очередь провайдеров услуг Интернет, является то, что эти компании имеют две как бы независимые локальные сети. Первая — это внутренняя сеть компании — со своим почтовым сервером, шлюзом сети Интернет и рабочими станциями сотрудников компании. И вторая — обслуживающая клиентов компании. Таким образом, для провайдера сети Интернет общая сеть может содержать следующее.

- Шлюз доступа клиентов компании в сеть Интернет. Через шлюз пользователи имеют доступ к сайтам сети Интернет, внешним почтовым серверам, удаленным рабочим местам и т. д.
- Почтовый сервер, на котором клиенты компании могут создавать свои почтовые ящики или арендовать домены.
- Внутреннюю сеть провайдера, в которой клиенты компании могут размещать свои сайты, файлы, документы и т. д. Обычно трафик внутренней сети бесплатен для клиентов.
- Виртуальные серверы, на которых клиенты компании могут создавать свои серверы.
- Рабочие станции и/или терминальные клиенты сотрудников самого провайдера.
- Внутренний почтовый сервер провайдера, возможно (но не обязательно) совмещенный с сервером, услуги которого предлагаются клиентам.

У крупных провайдеров количество серверов может быть достаточно значительным. Это делается как для распределения (балансировки) нагрузки в часы пик, так и для резервирования на случай отказа одного или нескольких серверов. Наличие или отсутствие каких-либо компонентов, количество серверов зависит от размера провайдера и списка услуг, предоставляемых им клиентам.

Провайдеры сети Интернет могут осуществлять защиту пользователей от поступления вирусов и спама:

- путем установки на компьютеры клиентов агентов антивирусной и антиспам-защиты;
- путем проверки почтового и интернет-трафика клиентов.

Рекомендуется совместное применение этих двух методов, так как этот подход имеет больше преимуществ по сравнению с применением только одного метода. Благодаря ему:

- за счет проверки трафика на уровне провайдера снижается нагрузка на компьютер пользователя — нет необходимости обрабатывать большое количества спама;
- использование антивирусной защиты на уровне пользователя позволяет перекрыть поступление вирусов через флеш-устройства.

Специальные системы

Существует ряд компаний и организаций, использующих системы, антивирусная защита которых должна осуществляться особым образом.

К числу таких систем относятся:

Высоконагруженные системы

Особенностью высоконагруженных систем является полное или почти полное использование программами, работающими на этих компьютерах, ресурсов системы. Примером таких систем в обыч-

ном офисе являются машины, на которых проводятся дизайнерские или конструкторские расчеты.

На такую машину можно установить все компоненты антивируса, кроме файлового монитора.

Поскольку данная конфигурация не обеспечивает **постоянной защиты**, то рекомендуется разрешить проверку архивов при получении и проводить частое (не реже одного раза в неделю, например в нерабочие дни) антивирусное сканирование.

Антивирусное ядро, используемое в решениях компании «Доктор Веб», потребляет крайне малое количество ресурсов и может автоматически снижать приоритет в случае высокой загрузки.

Системы реального времени

Особенностью систем реального времени является:

1. Требование гарантированного времени исполнения каждой операции в ходе их последовательности — циклограммы. К таким системам относятся системы, обслуживающие техпроцессы (налив топлива на АЗС или нефтебазе), военные системы (процедура запуска ракеты).

   Как известно, работа антивируса не предполагает гарантированного времени проверки файла — она может изменяться как минимум после каждого обновления.

   Таким образом, установка полноценной антивирусной системы на системы реального времени невозможна.

2. Для систем реального времени используют не только модификации обычных ОС — Windows NT4, Windows Embedded, но и специальные ОС, например Neitrino.

   Специализированные ОС антивирусными системами не поддерживаются.

Для защиты систем реального времени (ОСРВ) на основе обычных ОС (не ОСРВ) можно установить только антивирусный сканер, настроенный на проверку всей системы при старте. Кроме того, данная операционная система реального времени должна использоваться в составе сегмента локальной сети, обеспечивающей проверку сетевого трафика до его поступления на защищаемую машину.

Дата актуализации 11.02.2014 г

IV. Общая структура локальной сети

В зависимости от задач компании варианты структуры локальной сети могут выглядеть следующим образом:

- **Отдельно стоящие компьютеры, не связанные между собой и не имеющие выхода в Интернет.** Данный вариант обычно встречается, когда в числе других задач организации необходимо выполнять какие-либо работы повышенной секретности. В этом случае из сети выделяются отдельные компьютеры или серверы, а перенос данных между этими компьютерами и остальной сетью осуществляется на специальных (зачастую учтенных) носителях. В частности, выделение компьютеров может быть оправданно в случае необходимости снижения класса защиты, а значит, и уровня затрат на ее обеспечение согласно Федеральному закону № 152-ФЗ.
- **Отдельно стоящие компьютеры, не связанные между собой, но имеющие выход в Интернет.** Достаточно редко встречающийся случай. Наиболее распространенная его версия — работа отдельных сотрудников из дома или работа аутсорсеров. Каждый из таких сотрудников самостоятельно подключается к сети Интернет, и обмен данными ведется также через нее.
- **Связанные в локальную сеть компьютеры, не имеющие выхода в Интернет.** Данный вариант обычно используется в сетях, требующих повышенного уровня безопасности. В таких организациях есть обычная сеть или компьютеры, подключенные к сети Интернет, и изолированная от Интернета внутренняя сеть. Перенос данных между внутренней и внешней сетями осуществляется на специальных (зачастую учтенных) носителях.
- **Связанные в локальную сеть компьютеры, имеющие выход в Интернет.** Наиболее часто встречающийся в практике случай, не требующий комментариев.

В случае наличия доступа в сеть Интернет информация может находиться на рабочих станциях, локально расположенных серверах и удаленных серверах, в том числе размещенных в ЦОДах (облачные сервисы).

При выборе средств защиты, кроме топологии самой сети необходимо учитывать и тип доступа пользователей к компьютерам. Таких типов существует два — **однопользовательский и многопользовательский**. В первом случае на компьютере может работать только один пользователь, во втором — более одного. Как правило, кроме пользователя к компьютеру имеет доступ еще и администратор сети, поэтому все сети по умолчанию можно считать многопользовательскими.

На данный момент многопользовательские сети строятся либо на основе рабочих групп, либо на доменной основе. Другие варианты (одноранговые сети, сети на основе Novell Netware) достаточно редки. Разница между рабочими группами и доменами по большому счету заключается в том, что в последнем случае в сети имеется сервер домена (как минимум один или два — основной и резервный), на котором в структуре Active Directory хранится информация обо всех пользователях и компьютерах сети, групповых политиках данной сети, паролях и т. д.

Информация о том, на какой основе строится сеть, достаточно важна: в случае отсутствия доменной структуры нет гарантии того, что на всех компьютерах имеется один и тот же пароль администратора, что существенно усложняет процедуру развертывания антивирусной защиты за счет увеличения времени на подготовку сети к развертыванию.

Влияние законодательства

На организацию локальной сети, а значит, и на антивирусную систему ее защиты сильно влияет род деятельности компании, в связи с чем она может подпадать под те или иные требования законодательных актов. Так, в организации могут использоваться секретные документы, она может сотрудничать с определенными учреждениями (наиболее частый случай — институты и НИИ, работающие с Министерством обороны Российской Федерации).

Кроме того организация может обслуживать критически важные инфраструктуры (железные дороги, атомные станции и т.д.) — и тем самым подпадать под требования законов о защите критически

Дата актуализации 11.02.2014 г

важных инфраструктур. Как правило, в локальных сетях таких компаний **внутренняя локальная сеть отделена от внешней**, и большая часть сотрудников компании не должна иметь доступа в сеть Интернет или имеет доступ только к определенным сервисам.

Облака и локальные сети

Как правило, под переходом в облако подразумевается перенос рабочих станций и серверов в дата-центр (ЦОД) или использование внешних сервисов вместо собственных.

Это позволяет оптимизировать стоимость инфраструктуры и повысить отказоустойчивость серверных подсистем, но одновременно **повышает риски, связанные с информационной безопасностью:**

- доступ злоумышленников и вредоносных программ к корпоративным данным на удаленных серверах (со стороны сотрудников подрядчика, (в том числе проникших через виртуальные машины, не имеющие адекватной защиты),
- перехват и модификация информации во время ее передачи с и на удаленные серверы,
- возможность отказа удаленной инфраструктуры или потеря доступа к ней.

Переход на внешние сервисы означает для компании и возникновение новых рисков безопасности:

- Растут затраты на обеспечение безопасной передачи – требуется организация защищенного канала данных, а это означает и возросшие требования к ширине канала, и деньги на закупку соответствующих продуктов, и необходимость получения лицензий на работу со средствами шифрования.
- Отсутствует гарантия недоступности данных для сотрудников провайдера услуги.
- Возникает проблема с удалением данных, переданных в облако.

И это далеко не исчерпывающий список.

Похожие проблемы возникают и в случае использования сотрудниками сторонних облачных сервисов, т. к. данные из облака передаются по защищенному каналу в обход систем безопасности, а значит, передать пользователю можно все, что угодно.

По сути при передаче сервисов компании в облако компания переходит от ситуации контроля безопасности к ситуации доверия безопасности поставщику услуги.

Модным трендом при переходе в облако является использование так называемых облачных антивирусов. Как правило, ЦОДы построены на основе продуктов VmWare. В этом случае для обеспечения антивирусной безопасности на каждый сервер ЦОДа устанавливается специальная виртуальная машина, через которую проходит весь трафик и на которой проверяются все файловые операции, происходящие на виртуальных машинах ЦОДа – на всех остальных виртуальных машинах антивируса нет. Данная система организации безопасности основана на ложном предположении о том, что антивирус должен обнаруживать все пытающиеся проникнуть вредоносные программы и не учитывает требование к способности антивируса активно противодействовать обнаружению ранее неизвестных вредоносных программ. Кроме того, данная схема защиты противоречит готовящемуся стандарту в области безопасности – ГОСТу «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации». В частности, согласно данному документу требуется:

- проверка наличия вредоносных программ в загрузочных областях машинных носителей информации, подключенных к ИС;
- проверка наличия вредоносных программ в микропрограммном обеспечении, физическом и виртуальном аппаратном обеспечении;
- проверка оперативной памяти и файловой системы гипервизора и (или) виртуальных машин на наличие вредоносных программ;
- проверка наличия вредоносных программ в файлах-образах виртуализированного ПО и виртуальных машин, а также файлах-образах, используемых для обеспечения работы виртуальных файловых систем;

- проверка наличия вредоносных программ в файлах конфигурации гипервизора и (или) виртуальных машин;
- фильтрация сетевого трафика в виртуальных сетях гипервизора;
- фильтрация сетевого трафика для каждой виртуальной машины;
- фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, между внутренними и внешними сетевыми узлами хостовой операционной системы (гипервизора), а также при организации сетевого обмена с сетями пользования типа Интернет;
- проверка наличия вредоносных программ в операционной среде гипервизора системы хранения данных.

Все это возможно реализовать только при условии установки антивирусной защиты, в том числе и на каждую защищаемую виртуальную машину.

В связи со всем вышесказанным при использовании облачных сервисов необходимо предусматривать меры, противодействующие:

- получению доступа данных к удаленным серверам, хищению и/или модификации данных, в том числе во время передачи данных между удаленными серверами и серверами и рабочими станциями, находящимися в локальной сети компании;
- внедрению вредоносных программ на удаленные серверы и во время передачи данных;
- простоям на время отсутствия доступа к удаленным серверам.

В качестве таких мер могут быть использованы:

- системы шифрования, а также системы создания каналов VPN;
- почтовые шлюзы на стороне ЦОД и на стороне локальной сети или локальные почтовые серверы, проверяющие входящую почту и накапливающие почтовые сообщения во время отсутствия доступа к ЦОД;
- файловые серверы и сервисы, синхронизирующие содержание с содержанием удаленных серверов.

В качестве примера использования внешних сервисов можно назвать использование услуги «Антивирус Dr.Web» для бизнеса. Компания вместо организации собственной антивирусной инфраструктуры использует возможности провайдера услуг, у которого развернут интернет-сервис Dr.Web AV-Desk. Немаловажно, что данный сервис спроектирован таким образом, что для его клиентов не является критичным требование постоянного наличия доступа к серверу антивирусной защиты — антивирусная защита надежно работает даже в таких условиях.

Использование внешних сервисов

Сотрудники компаний и организаций нередко используют платные и бесплатные облачные сервисы – почтовые, сервисы хранения документов и т.д. (google.docs, google.mail, google.disk и аналогичные), доступ к которым не контролируется системами безопасности компании.

Использование данных сервисов также несет определенные риски. Внешние сервисы являются удобным путем проникновения, поскольку их использование не гарантирует, что хранящиеся там документы будут оставаться неизменными. В свою очередь измененные файлы, получаемые с облачных сервисов, попадают внутрь локальной сети минуя средства безопасности компании (например, антивирусы на интернет-шлюзе), так как передаются по защищенному каналу, не контролируемому средствами защиты.

В связи с этим любой компании требуется обеспечить защиту всех узлов сети, где так или иначе могут оказаться вредоносные файлы — или через которое они могут передаваться. Это включает, как минимум 1) рабочие станции, 2) почтовые серверы и интернет-шлюзы.

V. Требования законодательства Российской Федерации в области антивирусной защиты

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

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

И 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, но 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.

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 отдельных компьютерах 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 России и ФСТЭК России) и постановлениях правительства.

Согласно закону операторами персональных данных являются все физические и юридические лица, вне зависимости от формы собственности, размера и рода деятельности.

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 нужным 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 (**Центр управления Dr.Web + Dr.Web Desktop Security Suite Комплексная защита + Dr.Web Server Security Suite**);
- централизованно управляемую антивирусную защиту почтовых серверов и интернет-шлюзов (**Центр управления Dr.Web + Dr.Web Mail Security Suite + Dr.Web Gateway Security Suite**).

Стандарт ИБ Банка России СТО БР ИББС-1.0-2010

Банковская сфера является жестко регламентируемой областью деятельности.

В частности, системы информационной безопасности банков должны соответствовать требованиям стандарта ИБ Банка России 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 картами. 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.

На данный момент стандарт Банка России СТО БР ИББС-1.0-2010:

- 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 к 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 (Офисный контроль входит только в лицензию **Dr.Web Desktop Security Suite Комплексная защита**);
- 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 функций Офисного контроля (**Центр управления Dr.Web + Офисный контроль**, который входит только в лицензию **Dr.Web Desktop Security Suite Комплексная защита**).

Дата актуализации 11.02.2014 г

Антивирусная защита должна быть эшелонированной, а средства защиты должны устанавливаться как на рабочие станции, так и на серверы (**Центр управления Dr.Web + Dr.Web Desktop Security Suite Комплексная защита + Dr.Web Server Security Suite**).

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 (антиспам входит только в лицензию **Dr.Web Desktop Security Suite Комплексная защита**). 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 (**Центр управления Dr.Web + Dr.Web Mail Security Suite + Dr.Web Gateway Security Suite**).

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 (**Офисный контроль** входит в состав лицензии **Dr.Web Desktop Security Suite Комплексная защита**), так и средств проверки трафика для предотвращения проникновения вирусов с доступных, но взломанных ресурсов (HHTP-монитор **SpIDer Gate** входит в состав лицензии **Dr.Web Desktop Security Suite Комплексная защита**). Дополнительным требованием является наличие системы защиты от хакеров, то есть как минимум качественного брандмауэра (Брандмауэр Dr.Web является одним из компонентов продукта **Dr.Web Desktop Security Suite**).

Все используемые в организации средства защиты должны быть приобретены легально.

Резюмируя, 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 вредоносных объектов;
- наличие наряду с функцией защиты от вирусов системы защиты от спама, офисного контроля, брандмауэра, системы контроля трафика;
- 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.

Исполнение положений данного и других стандартов является рекомендательным, однако де-факто именно на основании этих стандартов проводится аттестация подразделений банков.

Более подробная информация о требованиях стандарта доступна по адресу:

http://www.abiss.ru/doc.

VI. Ошибки при построении антивирусной системы защиты локальной сети

Незнание актуальных путей проникновения вирусозависмых угроз в корпоративную сеть, возможностей современных антивирусных комплексов, требований законодательства в отношении защиты локальных сетей и бытующие заблуждения в среде ИТ-специалистов ИБ приводят к следующим типичным ошибкам при построении антивирусной системы защиты локальных сетей.

1. «Достаточно защиты только рабочих станций. Защита сервера не нужна».

Типичной для большинства компаний является ситуация, когда функции системы защиты от вредоносных программ возлагаются только и исключительно на антивирусы, установленные на рабочих станциях. При этом считается, что:

- вирусы могут проникнуть только через рабочие станции и смысла в защите серверов нет;
- все входящие файлы проходят через рабочие станции, и вполне достаточно защитить только их — установленный на рабочих станциях антивирус должен обеспечить обнаружение и удаление всех так или иначе поступающих в компанию вредоносных программ;
- на серверах никто не работает, и никто их не заразит;
- защита серверов стоит дорого.

В итоге реализованная таким образом антивирусная система защиты **не обеспечивает даже минимально необходимого уровня безопасности**.

Причины, по которым необходимо защищать сами серверы (файловые, терминальные, серверы приложений (баз данных)):

- Сервер может быть заражен **неизвестным** на момент заражения вирусом, который сначала проник на компьютер пользователя, а затем распространился по сети. Установленный на сервере антивирус сразу поймает его, основываясь на эвристических механизмах. В крайнем случае пролечит вирус при очередном обновлении. Отсутствие антивируса на сервере сделает сервер постоянным источником заражения.
- Сервер может быть взломан хакерами. Установленный на сервере антивирус отследит и уничтожит вредоносные программы. Если сервер находится под контролем централизованной системы управления, администратор мгновенно получит уведомление об изменении состояния станции (например, о попытке остановить систему защиты).
- 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 — или полученные от знакомых и коллег. На этих носителях могут быть вирусы. Современные сотовые телефоны по своим возможностям и количеству уязвимостей могут сравниться с компьютерами — в них используются операционные системы и приложения, которые тоже могут быть заражены. Вирусы с них могут попасть в корпоративную сеть и добраться до сервера.

2. «Компания обязана защищать только принадлежащие ей устройства».

Сегодня никто не отрицает безусловную необходимость защиты рабочих станций предприятия. Но наиболее частой ошибкой при построении защиты локальной сети является решение об организа-

ции защиты только офисных компьютеров сотрудников.

При старом, уходящем в прошлое методе организации работы компания могла в любой момент гарантировать соблюдение заданного уровня безопасности — ведь системные администраторы контролировали все до одного устройства в компании.

Теперь это невозможно, т. к. сегодня большая часть компьютеров, находящихся в пределах помещений компании, ей не принадлежит — это собственность сотрудников — их ноутбуки и смартфоны.

До 60% личных устройств сотрудников и их домашние компьютеры не имеют средств антивирусной защиты.

А ведь с них производятся заходы в локальную сеть, именно они являются источниками вредоносных файлов и отличным плацдармом для проникновения хакеров в локальную сеть в обход всех средств защиты периметра.

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.

ВАЖНО!

Центр управления Dr.Web Enterprise Security Suite позволяет управлять защитой как офисных компьютеров, так и домашних устройств сотрудников, включая мобильные устройства под управлением Android и Windows Mobile.

3. «Хватит одного антивируса. Комплексная защита — излишество».

Большинство компаний покупает для защиты рабочих станций только антивирус, а не комплексную защиту. Считается, что этого достаточно — даже если вирус попадет на машину, антивирус его уничтожит, а «спама у нас немного».

При этом ошибочно считается, что **единственной задачей антивируса является недопущение в локальную сеть вредоносных программ** — иными словами, качественный антивирус должен знать на момент проникновения все или практически все вредоносные программы. Задача ликвидации уже проникших и активных вредоносных программ возлагается на утилиту Dr.Web CureIt! **(к сожалению, в большинстве компаний эта лицензия используется незаконно на безоплатной основе)**, а антивирус, пропускающий вредоносные программы, считается некачественным и подлежащим замене.

ВНИМАНИЕ!

Сегодняшняя антивирусная система защиты не равна вчерашнему файловому антивирусу.

Функцией антивируса является обнаружение и уничтожение вредоносных файлов, но ликвидировать он может только **известные** вирусной базе угрозы или угрозы, которые могут быть обнаружены эвристическими механизмами. До получения обновлений антивирус не может ни обнаружить, ни уничтожить **новую неизвестную** угрозу.

Комплексная защита обеспечивает блокирование большинства путей поступления вирусов за счет возможности запрета использования сменных устройств и ограничения доступа к локальным и сетевым устройствам (в том числе каталогам на локальном компьютере и сайтам сети Интернет) — новый, еще не попавший на анализ в антивирусную лабораторию и поэтому не определяемый ни одним антивирусом вирус просто не сможет попасть на защищенный сервер или рабочую станцию.

Преимущества комплексной защиты

- Проверка интернет-трафика до его поступления в браузер и проверка почтового трафика до его поступления в почтовый клиент. То есть вирусы не смогут воспользоваться уязвимостями соответствующих программ — уже достаточно давно для проникновения на компьютер в большей степени используются уязвимости программного обеспечения (в первую очередь Adobe), а не уязвимости операционных систем;
- уменьшение доли спама в почтовом трафике до минимума, что существенно повышает производительность труда, так как:
- пользователи значительно меньше отвлекаются от основной работы на проверку приходящей почты,
- уменьшается вероятность пропуска или удаления важного сообщения.

4 «Все угрозы только из Интернета. Тогда зачем защищать компьютер без доступа к Интернету?»

Распространено мнение, что если компьютер не подключен к сети Интернет или изолирован от локальной сети, ему не нужна антивирусная система защиты. Такие незащищенные машины являются брешами в системе защиты предприятия и причинами инфицирования локальных сетей.

Основные пути попадания вредоносных программ на такие машины и с них в локальную сеть или на компьютеры клиентов компании — съемные устройства, которые бесконтрольно используются сотрудниками в случае отсутствия на компьютере Офисного контроля, имеющего средства разграничения доступа.

5. «Под Маками и Линуксами вирусов нет».

Еще одним заблуждением является то, что в силу относительно малого количества вредоносных программ для операционных систем типа Mac, Linux и Unix необходимо защищать только рабочие станции и серверы, работающие с использованием операционных систем типа Windows. В результате такого подхода 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.

ВНИМАНИЕ!

Тенденцией 2013 года стал резкий рост количества атак на операционные системы Linux. Если ранее новости о заражении Linux-машин были крайне редки, то к середине 2013 года практически еженедельно появляется информация о новом массовом заражении или взломе.

6. «Письма на сервере не открываются, поэтому и сервер не заразится. А админ у нас толковый — сам вирусов не занесет».

Да, это так, но в случае хранения почты на сервере ТОЛЬКО антивирус для почтовых серверов способен удалить вредоносные программы из почтовых ящиков.

Кроме этого, нужно помнить: хотя антивирусные системы защиты шлюзов и почтовых систем выполняют задачу перехвата вирусов на стадии распространения (проникновения) и никак не участвуют в защите от вредоносных программ на этапе их активации (запуска) — это происходит на рабочих станциях — кроме установленной защиты сервисов, работающих на сервере (почтовых в том числе), необходимо **дополнительно использовать** антивирус для защиты файловой системы.

7. «Центр управления антивирусной системой защиты — только для удобства системного администратора».

Это в корне ошибочное мнение. Наличие средства централизованного управления антивирусной системой защиты существенно влияет на уровень информационной безопасности предприятия. Именно Центр управления является **гарантом соблюдения политик информационной безопасности** на каждом защищаемом объекте. Он 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;
- производить регулярные обновления системы и сканирования компьютеров.

ВНИМАНИЕ!

Центр управления Dr.Web лицензируется бесплатно.

Дата актуализации 11.02.2014 г

VII. Общие требования к организации антивирусной системы защиты локальной сети

1. Используемая антивирусная система защиты должна:

- **иметь стойкую систему самозащиты**, которая не позволит неизвестной вредоносной программе нарушить нормальную работу антивируса и сделает возможным функционирование АСЗ до поступления обновления, позволяющего пролечить заражение;
- **иметь систему обновлений**, находящуюся под контролем системы самозащиты антивирусной системы и **не использующую компоненты операционной системы**, которые могут быть скомпрометированы; систему обновления, позволяющую мгновенно, по сигналу системы централизованного управления доставить на защищаемый антивирусом объект обновления для лечения активного заражения;
- **иметь систему сбора информации о новых угрозах**, позволяющую максимально быстро передавать в антивирусную лабораторию материал для вирусного анализа и выпуска обновлений;
- **уметь лечить** не только поступающие (неактивные) вредоносные программы, но и уже запущенные, но ранее неизвестные вирусной базе;
- обладать дополнительными (кроме сигнатурных и эвристических) механизмами для обнаружения **новых неизвестных** вредоносных программ;
- проверять все поступающие из локальной сети файлы **до момента получения их используемыми приложениями**, что исключает использование вредоносными приложениями неизвестных уязвимостей данных приложений;
- иметь систему **централизованного сбора информации** с удаленных рабочих станций и серверов, позволяющую максимально быстро передавать в антивирусную лабораторию всю необходимую для решения проблемы информацию;
- иметь **локальную службу поддержки** на русском языке.

2. Необходимо использовать **систему централизованного управления** антивирусной защитой, которая должна:

- **Обеспечивать максимально быструю доставку обновлений** вирусных баз на все защищаемые рабочие станции и серверы – в том числе по решению администратора в ущерб общей производительности защищаемой локальной сети. Минимизация времени получения обновления должна в том числе обеспечиваться минимизацией размера самих обновлений, а также постоянным соединением защищаемых рабочих станций и серверов с сервером обновлений.
- Обеспечивать **невозможность отключения пользователями обновлений**. Мнение сотрудников любой должности о частоте проведения обновлений должно **ИГНОРИРОВАТЬСЯ**.

ВНИМАНИЕ!

Ни один программный продукт не требует столь частой актуализации, как антивирус. Новые вирусы пишутся постоянно, и вирусные базы обновляются с очень высокой частотой (не реже 1–2 раз в час). ***Автоматическое обновление антивируса отключать НЕЛЬЗЯ!***

Возможности централизованного управления антивирусной системой защиты Dr.Web позволяют:

- исключить возможность отмены обновления рабочей станции сотрудником;
- отключать от сети необновленного агента, а значит, предотвращать распространение эпидемий внутри локальной сети и за ее пределы;
- задать нужный режим обновлений компонентов Dr.Web на защищаемых станциях, распределив нагрузку на разные промежутки времени;
- проводить мониторинг вирусных баз и состояния станций.

- Обеспечивать невозможность отключения регулярных сканирований пользователями, запускать сканирования без вмешательства оператора рабочей станции, задавать графики сканирований с любой необходимой частотой. Мнение сотрудников любой должности о частоте сканирований должно ИГНОРИРОВАТЬСЯ.

ПОЧЕМУ важно регулярно сканировать систему?

- *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 неизвестных 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 – **это нормальное явление**.

Защита локальной сети при использовании облачных сервисов

Особое внимание необходимо уделить защите локальной сети при использовании облачных сервисов. В число рисков, связанных с использованием облачных сервисов, входят:

1. Возможность перехвата и модификации информации при передаче. В связи с этим рекомендуется использовать антивирусные прокси-серверы как на стороне облака, так и на стороне компании. Также хорошей практикой является использование защищенных каналов связи, однако необходимо учитывать риск внедрения вредоносных программ в разрыв между защищенным каналом и клиентской программой.
2. Возможность внедрения вредоносных программ на виртуальные машины. В связи с этим рекомендуется использовать антивирусные средства для защиты всех виртуальных машин вне зависимости от места их расположения.

Дополнительные требования

Использование антивирусных решений должно дополняться:

1. Изоляцией внутренней сети компании от сети Интернет — разделением сети на внешнюю и внутреннюю.
2. Журналированием действий пользователя и администратора.
3. Резервным копированием важной информации.

Должны быть разработаны следующие процедуры:

1. Периодического контроля всех реализованных программно-техническими средствами функций обеспечения информационной безопасности.
2. Восстановления всех реализованных программно-техническими средствами функций обеспечения информационной безопасности.
3. Реагирования на инциденты информационной безопасности.
4. Оповещения сотрудников и клиентов в случае инцидентов информационной безопасности.

Дата актуализации 11.02.2014 г

VIII. Характеристики элементов сети и принципы их защиты

1. Рабочие станции и мобильные устройства

Как показывает практика, именно рабочие станции (включая мобильные устройства) и серверы являются наиболее уязвимыми узлами локальной сети. Именно с них распространяются вирусы, а зачастую и спам. При этом на сами компьютеры вирусы могут попадать самыми разными путями — за подробной информацией обратитесь к разделу «Пути проникновения вредоносных программ».

Защита рабочих станций, принадлежащих компании

1. Теоретически абсолютно любую ошибку (уязвимость) в программе можно использовать для причинения вреда системе в целом. Причем это может быть и кратковременный сбой, и серьезная порча данных. Чтобы этого избежать, необходимо соблюдать несложные правила.
   - Своевременно скачивать и устанавливать все обновления и новые версии всего установленного на компьютерах программного обеспечения — не только операционной системы. Для этого все используемое ПО должно быть лицензионным.
   - Использовать **систему централизованной установки обновлений** всего установленного на ПК программного обеспечения — это позволит системному администратору в режиме реального времени контролировать отсутствие известных уязвимостей на защищаемых объектах.

   Только квалифицированный системный администратор может принимать решения о необходимости обновлений антивируса, установки той или иной программы или перезагрузки в связи с обновлением безопасности любой установленной на ПК программы. Мнение об этом других пользователей, независимо от их должности, должно ИГНОРИРОВАТЬСЯ.
2. Нужно обеспечить **централизованное управление** всеми компонентами антивирусной системы защиты всех рабочих станций локальной сети.
3. Необходимо использовать актуальную версию антивирусной системы защиты.
4. Вне зависимости от должности любой пользователь должен работать только под учетной записью с ограниченными правами. Учетная запись Гость должна быть отключена.
5. Состав установленного на компьютерах программного обеспечения должен быть известен системному администратору.
6. Должна быть запрещена самостоятельная установка пользователем любых программ - это не позволит вирусу, обошедшему защиту средств безопасности, установиться на компьютере.
7. Доступ пользователей должен быть ограничен только необходимыми для работы ресурсами локальной сети. Для этого требуется использовать настроенную систему контроля и ограничения доступа.

   Офисный контроль Dr.Web блокирует большинство путей поступления вирусов за счет возможности запрета использования сменных устройств (в том числе флешек) и ограничения доступа к локальным и сетевым устройствам (в том числе каталогам на локальном компьютере и интернет-сайтам).
8. Проверка почтового трафика должна производиться до попадания письма в почтовую программу, чтобы исключить возможность проникновения вредоносных программ через ее уязвимости

Дата актуализации 11.02.2014 г

9. Проверка интернет-трафика должна осуществляться до его попадания в клиентские приложения. Антивирусная система должна проверять все ссылки, по которым предлагается загрузка каких-либо ресурсов из Сети, и весь трафик до его попадания на компьютер.

HTTP-монитор Dr.Web производит проверку трафика до его поступления в браузер или почтовый клиент. В этом случае вирусы не смогут воспользоваться уязвимостями установленных на рабочей станции программ.

10. Персонал должен иметь доступ только к нужным для работы интернет-ресурсам. Мнение сотрудников, независимо от должности, о том, какой веб-ресурс является безопасным, а следовательно – возможным для посещения, должно ИГНОРИРОВАТЬСЯ. Возможность доступа персонала к ненужным интернет-ресурсам должна быть централизованно запрещена.

Офисный контроль Dr.Web позволяет:

- ограничить доступ к сети Интернет;
- вести черные и белые списки адресов, чтобы обеспечить доступ сотрудника к тем интернет-ресурсам, которые ему необходимы для выполнения служебных обязанностей;
- полностью запретить доступ к сети Интернет там, где это жизненно необходимо (например, на компьютерах с бухгалтерскими системами);
- сделать невозможной отмену ограничений сотрудником на станции.

ВНИМАНИЕ!

Этот компонент должен быть установлен также и на компьютерах, не подключенных к сети Интернет или изолированных от локальной сети.

11. Пользователь (а значит – и вредоносная программа, действующая от его имени) не должен иметь доступ ни к каким локальным и сетевым ресурсам, кроме необходимых для выполнения рабочих обязанностей. Убеждать персонал в том, что флешки опасны – бесполезно.

Система ограничения доступа Офисного контроля Dr.Web:

- позволяет определить файлы и папки в локальной сети, к которым сотрудник может иметь доступ, запретив те, которые должны быть ему недоступны, – т. е. обеспечивает защиту данных и важной информации 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.

Лучший опыт

Возможность подключения съемных устройств к рабочей станции надо **централизованно** запретить.

12. Дополнительно для предотвращения проникновений вредоносных объектов внутрь корпоративной сети на рабочих станциях помимо антивируса должны использоваться следующие компоненты защиты:

- **Антиспам** — для сокращения доли спама в почтовом трафике, что снижает риск заражения через спам-сообщения и повышает производительность труда.
- **Брандмауэр** — для обеспечения невозможности сканирования локальной сети извне, а также для защиты от внутрисетевых атак.

13. Антивирусная система защиты должна быть установлена на все рабочие станции под управлением любой ОС, включая Mac OS X, Linux и UNIX.

Защита компьютеров, на которых ведется работа с критически важными данными и/или денежными средствами

Для таких компьютеров в дополнение к вышесказанному есть еще ряд требований.

1. Компьютер для работы с денежными средствами (системами дистанционного банковского обслуживания) не должен использоваться для работы с критически важными данными, и наоборот. Никакие другие операции на таком выделенном компьютере производиться не должны.
2. На выделенном компьютере требуется:

- исключить возможность запуска иных программ, тем более неизвестного назначения и полученных от неизвестных отправителей;
- удалить системы и сервисы удаленного управления и заблокировать возможность удаленных подключений на время работы критичных для бизнеса систем — всех, кроме ресурса, к которому подключается система ДБО;
- заблокировать возможность посещения внешних интернет-ресурсов средствами компонента Офисный контроль Dr.Web;
- протоколировать все события, в том числе все действия администраторов и пользователей компьютера;
- отключить возможность запуска программ из папок с документами и каталогов для временных файлов, таких как Temp;
- использовать только устойчивые к взлому пароли доступа. Стойкость паролей должна контролироваться средствами централизованной системы, обеспечивающей соответствие используемых паролей требованиям безопасности, и их периодическую замену.

3. Перед началом работы с системой ДБО и/или важными данными требуется проводить обновление антивируса и быстрое сканирование системы.
4. После завершения работы с системой ДБО и/или важными данными необходимо корректно завершить работу с данными системами (совершить выход из системы).

Защита личных компьютерных устройств, с которых сотрудникам компании открыт доступ в корпоративную сеть

Сегодня многие офисные сотрудники используют собственные устройства для доступа к корпоративным ресурсам и/или работают удаленно. Сложился широкий круг профессий, представители которых всегда находятся на связи: на работе, в дороге, дома. В интересах компании сделать так, чтобы в любом месте работа была безопасной, а корпоративные данные – защищены.

Чаще всего на домашних компьютерах установлена операционная система Windows. Она хорошо известная хакерам именно в силу ее распространенности — для нее и создается большая часть вре-

доносных программ. Способы защиты данной операционной системы также хорошо известны, но для домашних компьютеров сотрудников, с которых осуществляется вход в корпоративную сеть, необходимо совместить требование по соблюдению корпоративных ограничений с одной стороны, и свободного использования личного компьютера/устройства, с другой. Например, необходимо совместить запрет на посещение социальных сетей в рабочее время и потребность в таком общении в свободное время. Необходимо также учесть возможность работы на компьютере не только самого сотрудника, но и членов его семьи.

Возможны два варианта защиты.

- **Первый** – добавить учетную запись еще одного пользователя на домашний компьютер (благо Windows это позволяет) и для этого пользователя реализовать все необходимые настройки безопасности. К сожалению, этот способ позволяет выполнить требования по безопасности только частично. Так, если при работе под учетной записью «защищенного» пользователя вирус и не пройдет, то ничто не помешает ему проникнуть на компьютер во время работы под другими учетными записями и получить доступ к сохраненной, но беззащитной информации. Также ничто не помешает ему, находясь в незащищенной учетной записи, изменить настройки безопасности. Так что для защищенного пользователя необходимо дополнительно устанавливать хранилище файлов и систему контроля целостности. Но самая главная проблема – необходимость настройки всего этого администратором для каждого пользователя, причем в большинстве случаев удаленно.
- **Второй вариант (более правильный)** – использовать загрузочный диск или USB, на котором находятся все необходимые для защищенной работы компоненты. Обойти защиту смогут лишь вирусы на уровне BIOS, но это все же пока редкость.

ВНИМАНИЕ!

Только обеспечив защищенность всех устройств, включая мобильные, на которых работают сотрудники компании, можно гарантировать, что с личных компьютеров и мобильных устройств сотрудников в корпоративную сеть не попадет ничего вредоносного, а данные и пароли, используемые сотрудниками для доступа в сеть компании, не будут похищены.

1. Мнение сотрудника, независимо от должности, 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.
2. Соблюдение политики информационной безопасности предприятия и на личных устройствах сотрудников, включая невозможность отключения ими обновлений и регулярных сканирований, а также удаления отдельных компонентов защиты, должно быть обеспечено с помощью централизованных средств управления антивирусной системы защиты.

В остальном для обеспечения защиты личных компьютеров сотрудников необходима система, аналогичная применяемой для защиты рабочих станций, принадлежащих компании.

Возможности антивирусной системы Dr.Web позволяют

централизованно администрировать защиту как корпоративных, так и личных компьютеров сотрудников, включая мобильные устройства.

Защита мобильных устройств, с которых открыт доступ в корпоративную сеть, включая не принадлежащие компании личные мобильные устройства сотрудников

Современные сотовые телефоны и мобильные устройства по своим возможностям и количеству уязвимостей могут сравниться с рабочими станциями. На современных мобильных устройствах используются достаточно мощные операционные системы и приложения, которые могут быть заражены, — причем теми же методами, что и приложения для рабочих станций. При этом основной проблемой использования собственных мобильных устройств сотрудниками компании является возможность распространения с них вредоносных программ и заражения локальной сети — или получение доступа к ее ресурсам в обход защиты.

Операционные системы мобильных устройств построены, как правило, на базе iOS от Apple или вариантов Android. При этом сами системы обычно гораздо более слабые по ресурсам, чем на обычных компьютерах. На данных устройствах, как правило, нет возможности использовать несколько учетных записей, что позволило бы ограничить права пользователей и уменьшить риск заражений. Поэтому защита может быть только частичной. Плюс существует огромный риск потери или кражи устройства и попадания всей информации (включая пароли и имена доступа к корпоративным ресурсам) к третьим лицам.

На мобильном устройстве в целях обеспечения защиты от проникновения вредоносных файлов должны использоваться:

1. **Антивирус** — это позволит не допустить на устройство вредоносные файлы, в том числе предназначенные для контроля за перемещением владельца устройства, а также его контактами и переговорами.
2. **Система защиты от утери мобильного устройства**, что позволит найти устройство в случае его утери и не дать доступа злоумышленнику к данным, хранящимся на нем.
3. **Система хранения конфиденциальной информации** в защищенном хранилище, что не даст возможности злоумышленнику воспользоваться данными, попавшими на мобильное устройство.

Защита мобильных устройств является обязательной, если данные устройства используются для получения СМС-сообщений, подтверждающих банковские операции, — в связи с наличием вредоносного ПО, модифицирующего такие сообщения.

2. Серверы

Как уже упоминалось, в состав сети, выполняющей типичные «офисные» задачи, с большой степенью вероятности могут входить:

- файловые серверы;
- почтовые серверы;
- интернет-шлюзы;
- серверы баз данных, серверы приложений, серверы DNS/DHCP/Active Directory...

2.1. Совмещение ролей серверов

Функции серверов могут быть как совмещены на одном сервере, так и разнесены по отдельным серверам (а в этом случае серверы могут размещаться либо на территории компании (и тем самым за их безопасность отвечают подразделения самой компании), либо удаленно (в том числе в ЦОДах)).

В первом случае один и тот же сервер может выполнять функции как почтового сервера, так и интернет-шлюза и файлового сервера. Поэтому в случае совмещения на одном сервере функций не-

скольких (если речь не идет о виртуализации серверов — о чем поговорим далее) говорят о ролях сервера — роли почтового сервера, роли шлюза и т. д. Необходимо отличать случай совмещения ролей сервера от запуска различных серверов с помощью систем виртуализации. В последнем случае каждый сервер запускается на отдельной, изолированной от других виртуальной машине и не влияет на работу иных серверов (если не учитывать использование ресурсов сервера виртуализации).

Функции разных типов серверов могут быть совмещены на одном сервере — и, если речь не идет о виртуализации серверов, говорят о ролях сервера.

Необходимо отличать случай совмещения ролей сервера от запуска различных серверов с помощью систем виртуализации. В последнем случае каждый сервер запускается на отдельной, изолированной от других виртуальной машине и не влияет на работу иных серверов (если не учитывать использование ресурсов сервера виртуализации).

Достаточно часто один сервер совмещает в себе роли интернет-шлюза и почтового сервера. Файловый сервер, помимо выполнения своей основной функции (хранения файлов и обеспечения к ним доступа), может использоваться и для организации других сервисов, обслуживающих сеть. Например:

- сервера DNS/DHCP, предназначенного для раздачи пользователям компании адресов локальной сети;
- сервера Active Directory, предназначенного для хранения данных о пользователях сети;
- сервера баз данных и сервера приложений (например, сервер 1С);
- терминального сервера;
- почтового сервера;
- шлюза сети Интернет.

ВНИМАНИЕ!

- *Совмещение ролей позволяет компании уменьшить количество серверов (сэкономить на покупке серверного оборудования), но одновременно существенно снижает общий уровень безопасности — взлом одного сервера дает доступ ко всем сервисам сети компании.*
- С точки зрения безопасности и надежности сети не рекомендуется на шлюзе в Интернете поднимать другие сервисы, кроме брандмауэра.
- Контроллер AD рекомендуется устанавливать на выделенном сервере.

Если совмещение ролей нежелательно (в связи с требованиями безопасности, несовместимостью программ и пр.), на одном физическом сервере могут быть развернуты несколько виртуальных серверов, каждый из которых обеспечивает какой-либо сетевой сервис: DNS, DHCP, AD, файловый сервер и т. д. В этом случае при проектировании системы защиты необходимо учитывать риск заражения виртуальной машины с машины, выполняющей роль гипервизора, а также риск распространения вредоносных программ между виртуальными машинами.

Функции разных типов серверов могут быть разнесены по отдельным серверам. Такие серверы территориально могут размещаться либо на территории компании (и тем самым за их безопасность отвечают подразделения самой компании), либо удаленно (в том числе в ЦОДах).

2.2. Резервирование нагрузки и ее распределение

Для увеличения общей надежности сервисов на серверах используются средства резервирования — как на уровне одного сервера (использование отказоустойчивых компонентов, райд-массивов и т. д.), так и на уровне самого сервиса — используется больше серверов, чем это необходимо для обеспечения бесперебойной работы компании, и отказ одного сервера не приводит к отказу всего сервиса. Наиболее часто реализуются две схемы:

- **горячее резервирование** — нагрузка (например, входящие почтовые сообщения) равномерно распределяется с помощью программного или аппаратного балансировщика между всеми серверами. В случае отказа одного из серверов нагрузка просто перестает поступать на него;
- **холодное резервирование** — работает только часть серверов, остальные находятся в ожидании. В случае отказа работающего сервера нагрузка с него перебрасывается на автоматически вводимый в действие сервер.

Число серверов, отвечающих за тот или иной сервис, может быть больше одного, когда один сервер заведомо не может справляться с заданной нагрузкой. Наиболее часто в случае недостаточной мощности одного сервера используется либо распределение нагрузки с помощью балансировщика, либо организация серверов в единый кластер. В последнем случае сервер является одним из узлов кластера.

2.3. Файловые серверы (они же серверы баз данных и серверы приложений)

Назначение и типы файловых серверов

Файловый сервер — это компьютер, где размещаются/хранятся те или иные файлы, доступные для пользователей.

Важно понимать различие между файловыми серверами, создаваемыми на платформах Windows и Unix.

Функция файлового сервера встроена в операционную систему Windows, и пользователям могут быть открыты для доступа (расшарены) любые папки (директории). Файловый сервер — это одна из ролей сервера, такая же, как и сервер DNS/DHCP, AD, сервер БД, терминальный сервис, почтовый сервер, шлюз в Интернет и т. д. Но файловый сервер не обязан быть сервером баз данных или предоставлять терминальный сервис — ни одна роль не может быть основной или дополнительной для другой. Выбор ролей сервера осуществляет его администратор.

ВНИМАНИЕ!

В операционной системе Windows файловый антивирус проверяет файлы всей системы, а не только те, которые доступны для пользователей.

- Функции файлового сервера для операционных систем Unix в большинстве случаев реализуются через дополнительно устанавливаемую подсистему Samba, эмулирующую соответствующие сервисы Windows.

ВНИМАНИЕ!

В операционной системе Unix файловый антивирус проверяет только открытые для пользователей области, все остальные файлы не проверяются. Это связано с тем, что файловый антивирус для операционных систем Unix представляет собой плагин (дополнительный модуль) для подсистемы Samba.

Количество файловых серверов компании

Можно считать, что в каждой компании есть как минимум один сервер Active Directory или DNS/DHCP. А то и два — основной и резервный, так как работа данного сервиса критична для компании. Случаи, когда адреса прописываются вручную, можно не учитывать — это удобно только для очень маленьких компаний.

Также можно считать, что в каждой более-менее крупной компании есть сервер 1С — случаи, когда используется другая бухгалтерская программа или когда используется несерверная версия, также относительно редки.

Защита файловых серверов

1. Требования к обеспечению безопасности файловых серверов 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.
2. Решая вопрос организации защиты сервера, важно:

- знать, какие дополнительные сервисы работают на файловом сервере;
- осознавать, к чему приведет совместное использование нескольких сервисов на одном защищаемом сервисе и насколько надежно будет защищен тот или иной сервис.

> ***ВНИМАНИЕ!***
> *Использование на защищенном файловом сервере сервера баз данных не подразумевает лечения содержимого баз данных — для этого нужно использовать специальные решения.*

3. 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, не зараженные вирусами, — возможен перехват канала связи с Интернетом и подмена передаваемой информации. В связи с этим наряду с защитой файлового сервера компании и всех общедоступных ресурсов сети (например, расшаренных пользователями папок) в компании должен использоваться антивирусный шлюз, который не позволит получить или передать наружу зараженный файл.

2.4. Серверы печати

Достаточно часто файловые серверы используются в качестве серверов печати — то есть они имеют сервисы, позволяющие принимать и отправлять по специальному протоколу на печать документы. Такие серверы также подлежат защите, так как:

- имеется достаточное число вредоносных программ, заражающих серверы печати;
- злоумышленник может как перехватывать информацию, отправляемую на печать, так и отправлять на печать документы, запрещенные к распространению за пределами компании.

ВАЖНО!

Если в качестве платформы для сервера используется Linux, рекомендуется защищать не только функции файлового сервиса данного сервера (сервис Samba), но и сам сервер. То есть нужно использовать два программных продукта Dr.Web:

1. Антивирус Dr.Web для Linux
2. Dr.Web для файловых серверов Unix

Необходимо учитывать риск заражения не только файловых серверов, но и непосредственно самих принтеров, особенно доступных из сети Интернет. В связи с недостатком ресурсов на таких устройствах антивирусные средства на них использованы быть не могут. Поэтому в качестве мер защиты должны использоваться средства ограничения доступа.

2.5. Терминальные серверы

Назначение и краткое описание принципов работы

При наличии терминального сервера пользователи работают не на рабочих станциях, а непосредственно на сервере — как будто клавиатура, мышь и монитор подсоединяются к самому серверу.

Существуют два варианта подключения к терминальному серверу:

- со специального устройства — тонкого клиента, не имеющего жесткого диска, единственной функцией которого является подключение к терминальному клиенту;
- с помощью специальной программы из обычной операционной системы.

Терминальные серверы могут быть созданы как на основе операционной системы Windows, так и на основе Unix.

Защита терминальных серверов

Обеспечение безопасности терминальных серверов осуществляется продуктами, предназначенными для защиты файловых систем компьютеров, так как единственное отличие между файловыми и терминальными серверами с точки зрения обеспечения защиты — это необходимость проверки терминальных сессий клиентов — их открытия и закрытия.

- Если вход на терминальные серверы осуществляется с тонких клиентов, защита тонких клиентов **не требуется** (на тонкие клиенты не устанавливается никакое антивирусное ПО), однако для защиты терминальных сессий необходимо приобретение лицензий **Dr.Web Desktop Security Suite Комплексная защита**, равное количеству подключений — в дополнение к лицензии на защиту самого терминального сервера **Dr.Web Server Security Suite**.
- Если вход на терминальные серверы осуществляется не с тонких клиентов, требуется защита клиентов, подключающихся к терминальному серверу (**Dr.Web Desktop Security Suite Комплексная защита + Dr.Web Server Security Suite**). При этом система защиты рабочих станций при использовании входа на терминальный сервер и без его использования не отличается. Единственное, что нужно учитывать в данном случае, — при использовании рабочих станций их количество не учитывается в количестве лицензий на подключения к терминальному серверу.

2.6. Виртуальные (в том числе облачные) серверы и рабочие станции

Назначение и краткое описание принципов работы

В связи с ростом мощности серверов, казалось бы, выгодно использовать один и тот же сервер для организации работы нескольких сервисов. Однако совмещение сервисов зачастую или невозможно, или небезопасно. Выходом является использование виртуальных серверов — серверов, единственным сервисом которых является так называемый гипервизор — сервис, обслуживающий запускаемые в виртуальном окружении операционные системы. При этом операционные системы и приложения, на них запускаемые, работают не на физическом сервере, а в его эмуляции.

3. Почтовые серверы

Почтовый сервер — это просто сервис, размещающийся на обычном файловом сервере.

Назначение почтовых серверов

- обработка входящей и исходящей почты,
- массовая рассылка почтовых сообщений,
- обмен данных между сотрудниками компании,
- основа для построения систем документооборота.

Наиболее распространенные почтовые серверы

- Microsoft Exchange, Kerio MailServer, Lotus Domino и Communigate Pro являются коммерческими решениями.
- Sendmail, Postfix, Exim (только под Unix), как правило, используются только в бесплатном варианте реализации. Если компания небольшая, такого клиента труднее уговорить на платную защиту от вирусов.

Количество почтовых серверов в компании

От бесперебойного функционирования почты компании, а также ее «чистоты» от вирусов и спама зависят **все** бизнес-процессы компании. Практически в любой компании есть почтовый сервер.

Случаи, когда компании используют внешние почтовые серверы, не принадлежащие компании, достаточно редки — даже если компания использует облачные сервисы, обычно почтовые серверы администрируются сотрудниками компании или (в случае передачи услуг на аутсорсинг) сотрудники компании имеют к ним доступ. Однако встречаются случаи, когда компании (обычно небольшого размера) вместо развертывания собственного почтового сервера арендуют почтовые ящики на внешнем сервисе (таком как gmail).

В зависимости от организации компании в ней может быть больше одного почтового сервера. Например, в многофилиальной сети в каждом филиале может быть свой почтовый сервер, почтовый сервер может быть вынесен за пределы внутренней сети компании (в демилитаризованную зону) и т. д.

Облака и почтовые серверы

Перенос в ЦОД почтового сервера, с одной стороны, повышает надежность работы почтового сервера — она теперь равна надежности самого ЦОДа. Однако, с другой стороны, любое прекращение связи с ЦОДом (падение ЦОДа, обрыв линии) приводит к приостановке работы всей компании. В результате для обеспечения отказа нужно использовать как минимум два канала до двух провайдеров услуг, вводить внутри локальной сети компании транзитные серверы, способные принимать почту на время недоступности основного сервера. Не помешают и серверы, обеспечивающие гарантию неизменности почты от момента ее передачи и до приема.

Организация фильтрации почты

Почтовый трафик является основным переносчиком вирусов и спама. 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 — в ней могут быть как адреса ваших сотрудников, так и адреса ваших клиентов.

Наличие значительной доли вредоносных файлов в почтовом трафике, а также «изобретательность» сотрудников приводят к:

- потерям и утечкам данных в результате деятельности вирусов и хакерских утилит;
- захвату локальной сети в результате вирусной атаки и превращению ее в элемент бот-сети;
- внесению компании в черные списки и отключению от сети Интернет за рассылку спама;
- снижению времени отклика почтового сервера, занятого обработкой паразитного трафика;
- снижению производительности почтового сервера или его полной неработоспособности;
- повышению нагрузки на внутреннюю сеть, снижению производительности сетевых ресурсов и пропускной способности каналов;
- выходу сервера из строя в результате получения «почтовой бомбы»;
- простоям оборудования;
- повышению затрат на хранение почты, в том числе и спама;
- повышению требований к аппаратной части почтовых серверов, а значит, к необходимости апгрейда или покупки новых машин.

При этом компания несет следующие **репутационные убытки**:

- нарушение бесперебойности бизнес-процессов;
- задержки в выполнении сотрудниками должностных обязанностей или невозможность исполнения служебных обязанностей (простои);

- вероятности пропуска важной информации;
- потери рабочего времени на устранение вирусных инцидентов;
- задержки в выполнении обязательств компании перед клиентами;
- увеличение размеров почтовых ящиков пользователей и их резервных копий, что в свою очередь приводит к проблемам поиска нужной информации;
- ухудшение репутации в глазах потребителей и партнеров;
- формирование мнения о компании как о технологически отсталой;
- уход клиентов или отказ от услуг компании.

1. Необходимо фильтровать как внешнюю (входящую и исходящую), так и внутреннюю почту компании — т. е. должны фильтроваться все пути приема и отправки почты.

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.

2. Почту необходимо фильтровать на сервере, а затем дополнительно на рабочих станциях.

Такая организация защиты приводит к значительному снижению нагрузки и на почтовый сервер, и на рабочие станции:

- Только почтовый антивирус может удалять в ходе периодических проверок почтовых ящиков вредоносные программы, ранее в них попавшие, — никакой иной антивирус сделать это не в состоянии.
- Фильтрация на уровне почтового сервера позволит не только более эффективно фильтровать почтовые сообщения, но и очищать почтовые базы от вирусов, неизвестных на момент попадания, что в свою очередь исключает их случайную отправку получателю. Также серверные решения для фильтрации почты на серверах и шлюзах позволяют реализовать фильтрацию по используемым форматам данных, предельным размерам файлов и другим критериям, чего нет в решениях для защиты рабочих станций.
- Проверка трафика производится до его поступления в почтовый клиент. То есть вирусы не смогут воспользоваться уязвимостями операционных систем и соответствующих программ.
- Фильтрация почты на уровне серверов исключает ситуации, когда пользователь сам может отключить антивирус или снизить уровень защиты — руководство компании и системный администратор могут быть уверены в защищенности сети.
- Увеличивается актуальность защиты. В отличие от рабочей станции, которая может не обновляться длительное время (например, во время отсутствия сотрудника), вирусные базы сервера всегда поддерживаются в актуальном состоянии.
- Уменьшается вероятность возникновения конфликтов антивирусного ПО с другим программным обеспечением. Например, с самостоятельно установленным пользователем ПО.
- Почта, включая спам, будет отфильтрована один раз на сервере, а не несколько раз на каждой станции — это улучшит их быстродействие, и сотрудники станут значительно реже жаловаться на «тормоза» на их рабочих ПК и отвлекать вас на их устранение.
- Благодаря антиспам-фильтрации непродуктивная паразитная нагрузка на почтовый сервер снижается (количество спама в почтовом трафике составляет до 98%, и его отсев благоприятно скажется на работе почтового сервера). Это сократит количество жалоб сотрудников на задержки в доставке почты и на потерянные письма.
- Существенно уменьшится внутрисетевой трафик за счет применяемых в серверных продуктах для антивирусной фильтрации почты алгоритмов шифрования и сжатия — этого функционала нет в продуктах для защиты рабочих станций ни у одного производителя.

3. Должна быть обеспечена защита самого почтового сервера

Защита самих почтовых серверов (например, средствами Dr.Web Server Security Suite) является обязательной мерой защиты от вирусов, неизвестных системе антивирусной защиты на момент заражения. Проникновение неизвестной вредоносной программы на сам почтовый сервер и/или в почтовые ящики превращает почтовый сервер в постоянный источник вредоносных программ.

4. Должны быть защищены все пути приема и отправки почты, а не только сам почтовый сервер.

Особенностью работы современного офиса является использование сотрудниками компании не только внутренних, но и внешних сервисов, в том числе почтовых. Зачастую сотрудники, ответственные за обеспечение безопасности компании, не информируются о случаях использования таких сервисов.

Возможные почтовые потоки компании

- Пользователь (либо программы, на установку которых он согласился, не зная их возможностей) может отправлять и получать письма:
- напрямую на почтовые серверы сети Интернет (по протоколу SMTP), если в сети открыт 25-й порт;
- на почтовые службы сервисов типа mail.ru/gmail.com — по протоколам pop3/imap4.
- Пользователь (либо программы, на установку которых он согласился, не зная их возможностей) может отправлять письма по закрытым каналам, и сервер не сможет их проверить.
- Сервер (либо программы, установленные на нем) может создавать почтовые рассылки и самостоятельно уведомлять получателей и отправителей о различных событиях.

В связи с этим необходимо **проверять почтовый трафик, не только идущий на почтовые серверы компании, но и трафик на внешние серверы, неподконтрольные компании**, уровень защиты которых неизвестен. На практике это означает:

- фильтровать всю корпоративную почту на почтовом сервере (с помощью **Dr.Web Mail Security Suite Антивирус + Антиспам**) и дополнительно обрабатывать протоколы POP3 и IMAP4 на шлюзе сети Интернет (в зависимости от используемого на шлюзе продукта, обрабатывающего трафик — **Dr.Web Mail Security Suite Антивирус + Антиспам, Dr.Web Mail Security Suite Антивирус + Антиспам + SMTP proxy или Dr.Web Gateway Security Suite Антивирус**) — дополнительно к проверке почты на рабочей станции;
- фильтровать всю внешнюю почту (протоколы POP3 и IMAP4, SMTP) на шлюзе (с помощью **Dr.Web Mail Security Suite Антивирус + Антиспам + SMTP proxy**), а на почтовом сервере сосредоточить только обработку внутренней почты (**Dr.Web Mail Security Suite Антивирус + Антиспам**) — дополнительно к проверке почты на рабочей станции.

Второй вариант предпочтительнее, 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;
- качество фильтрации на почтовом шлюзе значительно выше за счет того, что решение для почтового шлюза не ограничивается по функционалу почтовым сервером.

Дата актуализации 11.02.2014 г

5. Фильтрация почты должна быть комплексной.

Только комплексные решения для электронной почты, сочетающие в себе антивирус и антиспам, могут обеспечить ее полноценную защиту и снижение расходов компании. Использование антивируса без антиспама:

- позволяет злоумышленникам проводить атаки на почтовые серверы компании и почтовые клиенты ее сотрудников;
- приводит к повышению платы за трафик;
- приводит к повышению непродуктивной паразитической нагрузки на почтовые серверы;
- снижает производительность труда всех сотрудников компании, получающих почту и вынужденных заниматься чисткой ящиков от спама.

6. Дополнительные меры защиты

- 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). Поскольку всегда имеется вероятность того, что **новый неизвестный** вирус проникнет в почту до того, как он попадет на исследование в антивирусную лабораторию, рекомендуется либо периодически проверять почтовые ящики пользователей на присутствие ранее необнаруженных вирусов, либо проверять почту при ее отправке сотруднику.
- 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 претензий по неверной фильтрации (например, в случае завышения уровня детекта выше рекомендуемого). Наличие карантина и функции архивации сообщений в **Dr.Web Mail Security Suite** позволяет восстанавливать сообщения, случайно удаленные сотрудниками из почтовых ящиков, а также проводить расследования, связанные с утечкой информации.

4. Почтовые шлюзы

Почтовый шлюз — в отличие от почтового сервера — не хранит почту — он обрабатывает ее «на лету» и передает по назначению. Почтовые шлюзы используются:

- **Провайдерами услуг доступа** — для фильтрации почты клиентов от вирусов и спама.
- **Компаниями** — как для снижения нагрузки на почтовый сервер компании, так и для изоляции его от сети Интернет (повышенный уровень защиты).

Применение почтовых шлюзов обусловлено их большей эффективностью фильтрации вредоносных программ и спама, что недоступно при организации фильтрации на почтовых серверах. Причиной этого служат ограничения, накладываемые на работу антивирусных программ почтовыми серверами. Так, например, в случае фильтрации почтового трафика для Microsoft Exchange ограничения API (программного интерфейса взаимодействия почтового сервера с антивирусным и антиспам-модулем фильтрации) позволяют реализовать только проверку частей писем (а не писем целиком) на наличие вредоносных программ и спама. В частности, это приводит к тому, что показываемая статистика не отражает правильного количества проверенных почтовых сообщений, так как плагин знает только количество проверенных частей писем, но не количество самих писем.

Имея собственные модули приема и передачи почты и выход в Интернет, почтовые шлюзы могут реализовывать механизмы фильтрации и проверки подлинности, недоступные в ином случае.

ВНИМАНИЕ!

В случае использования облачных почтовых сервисов использование почтовых шлюзов на стороне компании является обязательным — только данная мера гарантирует чистоту принимаемого почтового трафика.

Виды почтовых шлюзов

Как правило, почтовые шлюзы строятся на основе операционных систем Unix. При этом могут встречаться два варианта: использование обычного почтового сервера (зачастую бесплатного, типа Postfix или Sendmail) в роли транзитного сервера или использование специального антивирусного решения, имеющего модуль транзитной передачи почтовых сообщений.

Значительно реже в качестве шлюза используется одна из ролей сервера MS Exchange (Edge). Суть в том, что задачи (роли), выполняемые MS Exchange, могут как выполнятся на одном сервере, так и разноситься по нескольким серверам. Одна из ролей MS Exchange – почтовый шлюз. Однако в связи с особенностями лицензирования разделение по ролям требует покупки особых лицензий, поэтому использование **Dr.Web SMTP-proxy** вместо роли Edge ведет к экономии средств.

В качестве почтового шлюза могут использоваться как программные решения, так и программно-аппаратные комплексы, автоматически фильтрующие входящий и исходящий трафик по всем протоколам – решающие в том числе и задачу фильтрации почтовых сообщений в случае использования сотрудниками внешних почтовых сервисов.

ВНИМАНИЕ!

С точки зрения безопасности и надежности сети не рекомендуется на шлюзе в Интернет поднимать другие сервисы, кроме брандмауэра. Контроллер AD также рекомендуется устанавливать на выделенном сервере.

Принципы фильтрации почты на почтовом шлюзе

1. **Фильтрацию почты желательно производить через почтовый шлюз (Dr.Web Mail Security Suite Антивирус + (Антиспам) + SMTP proxy).**

   Выставлять почтовый сервер в Интернет или внутреннюю сеть компании **небезопасно**. Злоумышленник имеет большие возможности по доступу к серверу или подмене трафика, в том числе и за счет аппаратных закладок. Даже если помещения расположены в одном здании, всегда есть вероятность перехвата или подмены трафика.

   Наилучшим является вариант размещения почтового сервера на границе сети или в специальной организованной демилитаризованной зоне (DMZ) транзитных (или Frontend) почтовых серверов. Серверы принимают почту и переправляют ее на основной почтовый сервер внутрь сети организации, одновременно фильтруя трафик на спам и вирусы до его попадания во внутреннюю сеть компании. Управляться такие серверы могут как специалистами самой компании, так и сторонней компанией (например, специалистами дата-центра).

   Настоятельно рекомендуется использовать фильтрацию почтового трафика на шлюзе в таких случаях:

- компания – интернет-провайдер;
- почтовый сервер компании находится вне охраняемой территории компании (например, во внешнем дата-центре);
- компания арендует почтовые адреса на специальном сервисе;
- помещения компании не сосредоточены внутри одного охраняемого периметра, а размещаются в нескольких местах, и для связи между ними не используется выделенный канал (компания с многофилиальной структурой).

ВНИМАНИЕ!

Антивирусный прокси-сервер, используемый в шлюзовых антивирусных системах фильтрации почтового трафика, позволяет существенно увеличить качество фильтрации почтового потока за счет реализации механизмов, невозможных на почтовом сервере в связи с ограничениями предоставляемых антивирусным программам интерфейсов взаимодействия с сервером. Например, предоставляемый антивирусным системам интерфейс взаимодействия с почтовым сервером MS Exchange не позволяет получить письмо целиком, что существенно затрудняет его анализ на спам.

Преимущества фильтрации почты на шлюзе

- Отсутствие прямого доступа к почтовому серверу из сети Интернет не позволит злоумышленникам воспользоваться уязвимостями (как ранее известными, так и уязвимостями нулевого дня), в том числе за счет специально сформированных писем.
- Использование шлюзовых антивирусных решений (например, **Dr.Web Mail Security Suite Антивирус + Антиспам + SMTP proxy**):
  - существенно повышает общую безопасность сети;
  - значительно улучшает качество фильтрации за счет отсутствия ограничений, накладываемых почтовыми серверами;
  - снижает нагрузку на внутренние почтовые серверы и рабочие станции;
  - повышает стабильность работы системы проверки почты в целом.
- Обработка почты на шлюзе позволяет не допустить попадание спама на почтовый сервер, что кардинально снижает объем паразитного трафика, а значит, повышает его производительность и доступность для пользователей. Это в итоге сокращает затраты на ИТ-инфраструктуру за счет:
  - существенного сокращения расходов на оплату паразитного трафика;
  - отсутствия необходимости увеличивать количество серверов или проводить аппаратные апгрейды;
  - сокращения затрат на хранение почты, в том числе и спама.

2. Необходимо обеспечивать защиту самого сервера, на котором развернут почтовый шлюз

Как и почтовый сервер, шлюз это просто сервис, размещающийся на обычном сервере. Поэтому, если используемой файловой системой является Windows, кроме защиты шлюза необходимо использовать и защиту самого сервера, то есть не один, а два продукта – например, Dr.Web Server Security Suite и Dr.Web Mail Security Suite.

5. Интернет-шлюзы

Назначение и краткое описание принципов работы

Так как пользователей сети Интернет много, а кабель, ведущий наружу компании, чаще всего один, то необходим сервер, через который осуществляется выход пользователей наружу.

Использование шлюзовых антивирусных решений позволяет:

- исключить возможность использования вредоносными программами уязвимостей, в том числе еще неизвестных – и за этот счет уменьшить вероятность заражения локальной сети и/или выведения ее из строя;
- ускорить работу рабочих станций за счет переноса систем антивирусной проверки на шлюз компании.

Как правило, шлюзовые антивирусные решения позволяют осуществлять в рамках реализуемой корпоративной политики регулирование доступа к веб-ресурсам, а также политики доступа к определенным типам файлов.

В качестве шлюза могут использоваться как программные решения, так и программно-аппаратные комплексы, автоматически фильтрующие входящий и исходящий интернет-трафик по всем основным протоколам – в том числе и в случае наличия свободного доступа сотрудников к внешним ресурсам сети Интернет.

Шлюз сети Интернет есть в каждой компании, имеющей выход в Интернет. Для многофилиальной компании количество шлюзов не меньше количества филиалов/подразделений.

Наличие защиты шлюза необходимо, если:

- серверы компании размещаются вне ее охраняемой территории,
- компания имеет филиалы,
- подразделения компании разнесены по нескольким адресам или отдельным помещениям.

ВНИМАНИЕ! В случае использования облачных сервисов, а также при наличии филиалов использование шлюзов на стороне компании является обязательным — только данная мера гарантирует чистоту принимаемого интернет-трафика.

Принципы фильтрации интернет-трафика на шлюзах

1. Как правило, антивирусные решения для интернет-шлюзов не представляют собой самостоятельные программы – они являются дополнительными модулями к программам, которые должны быть установлены на серверы и которые обеспечивают доступ в Интернет.
2. Как и почтовый сервер, шлюз это просто сервис, размещающийся на обычном сервере. Поэтому, если используемой файловой системой является Windows, кроме защиты шлюза сети Интернет требуется обеспечить и защиту самого сервера, то есть приобрести два продукта:

- **Dr.Web Server Security Suite** (программный продукт Dr.Web для файловых серверов Windows);
- **Dr.Web Gateway Security Suite** (программный продукт Dr.Web для интернет-шлюзов Kerio или Dr.Web для Microsoft ISA Server и Forefront TMG).

ВНИМАНИЕ! Отсутствие такой защиты позволяет злоумышленникам скомпрометировать сеть компании.

IX. Экспертиза вирусозависимых инцидентов

1. Кибермошенничество и вирусозависимые компьютерные инциденты

Термин

Вирусозависимый компьютерный инцидент (далее — ВКИ) — компьютерный инцидент, для совершения которого использовалась вредоносная или потенциально опасная программа (-ы).

Среди разнообразных инцидентов информационной безопасности (ИБ) вирусозависимые инциденты преобладают. Для совершения ВКИ злоумышленниками используется вредоносное, потенциально опасное ПО или мошеннические технологии социальной инженерии, приводящие к запуску самой жертвой вредоносного или потенциально опасного ПО. Такие инциденты классифицируются УК РФ как мошенничество, что позволяет назвать этот сегмент рынка услуг обеспечения ИБ **сегментом менеджмента инцидентов кибермошенничества**.

Основные векторы коммерческого кибермошенничества

- Компрометация компьютерных систем — с целью присоединения их к бот-сетям для слежения за жертвой, хищения хранящейся в системе информации, организации отказа в обслуживании и (d)DOS-атак.
- Хищения средств аутентификации к системам дистанционного банковского обслуживания и платежным онлайн-системам — с целью дальнейшего хищения денежных средств.
- Хищения данных банковских карт — с целью дальнейшего хищения денежных средств.
- Мошенничество, связанное с брендами — с целью наживы или реже дискредитации.
- Хищения проприетарного контента — с целью его незаконного использования.

Причины роста хищений, совершаемых с помощью вредоносных компьютерных программ:

- рост количества вредоносных программ,
- изобретение вирусописателями еще более успешных новых угроз,
- использование вирусами уязвимостей, еще не закрытых производителями ПО,
- использование жертвами нелицензионного ПО (в том числе антивируса),
- неправильное использование средств защиты (в том числе антивируса),
- несоблюдение правил безопасного поведения в Интернете (в том числе отключение некоторых компонентов антивируса),
- неправильные настройки безопасности (в том числе антивируса),
- несоблюдение основ информационной безопасности,
- человеческий фактор — халатность, невнимательность, попустительство и т. д.

Для атак на компьютерные системы предприятий кибермошенники успешно эксплуатируют:

- недостатки построения антивирусных систем защиты всех узлов корпоративной сети или полное отсутствие антивирусной системы защиты (речь не об использовании антивирусов, а именно о системах антивирусной защиты);
- недостатки или полное отсутствие на предприятиях политик ИБ;

- несоблюдение сотрудниками предприятий политик ИБ по причинам неграмотности в вопросах основ ИБ, неосознания проблемы, халатности;
- средства социальной инженерии.

ВНИМАНИЕ!

Антивирус есть основное средство противодействия кибермошенничеству. Компания «Доктор Веб» разрабатывает эффективные и многофункциональные средства защиты от программ, используемых для совершения компьютерных преступлений.

2. Служба реагирования на инциденты ИБ

В 2013 году границы компетенции «Доктор Веб» были расширены и компания стала игроком сегмента услуг обеспечения ИБ и менеджмента инцидентов кибермошенничества в частности.

Сегодня в компании «Доктор Веб» действует служба реагирования на инциденты ИБ. В составе службы функционируют лаборатория компьютерной экспертизы, которая занимается исследованиями артефактов, имеющих отношение к инциденту ИБ, и аналитическая группа, которая составляет аналитические отчеты и ведет статистическую деятельность.

3. Экспертиза ВКИ

Экспертиза ПО, использованного для совершения компьютерного мошенничества, является одним из процессуальных действий при расследовании киберпреступлений, одним из важнейших элементов доказательственной базы.

Компания «Доктор Веб» производит экспертизу компьютерных инцидентов против конфиденциальности, целостности и доступности компьютерных данных и систем, **для совершения которых использовались вредоносные программы и потенциально опасное ПО**.

Форма подачи заявки на экспертизу: https://support.drweb.com/expertise.

Перечень услуг экспертизы ВКИ «Доктор Веб»

- Предварительная оценка инцидента, объема экспертизы и мер, необходимых для устранения последствий произошедшего.
- Экспертные исследования компьютерных и других артефактов (накопителей на жестких магнитных дисках, текстовых, звуковых, фото-, видеоматериалов), предположительно имеющих отношение к ВКИ.
- **Не имеет аналогов!** Психологическая экспертиза личностей (персонала) с целью выявления фактов причастности к совершению / пособничеству / укрывательству / поощрению противоправных действий в отношении заказчика (комплексное определение рисков), а также фактов бездействия или халатного отношения к служебным обязанностям.
- Рекомендации по вопросам построения системы антивирусной защиты с целью недопущения ВКИ или сокращения их количества в будущем.
- Все исследования производятся с соблюдением требований ст. 79, 84, 85, 86 ГПК РФ и ст. 57, 195, 204 УПК РФ.

Преимущества экспертизы «Доктор Веб»

- Более чем двадцатилетний опыт вирусных исследований.
- Знание современных вирусных угроз, их постоянный мониторинг и изучение, наличие собственных методик их обнаружения (детектирования).

- Эффективное противостояние новым угрозам, непрерывная разработка технологий борьбы с новыми, еще неизвестными вредоносными программами и уловками злоумышленников.
- Высокая квалификация персонала.
- Собственная служба глобального вирусного мониторинга.
- Собственная антивирусная лаборатория.
- **Не имеет аналогов!** Уникальная экспертиза персонала заказчика.
- Наличие специального оборудования, позволяющего снимать информацию в соответствии с процедурами, исключающими неполное снятие информации и обеспечивающими неопровергаемую доказательную базу в суде.

Технические средства — объекты воздействия вредоносных программ, экспертизу работы которых проводит «Доктор Веб»

- Серверное оборудование
- Платежные терминалы и банкоматы
- Рабочие места, оборудованные стационарными или мобильными компьютерами
- Собственные компьютеры и мобильные устройства сотрудников, подключаемые к корпоративной сети
- Любые съемные носители информации

Перечень вопросов, ответы на которые даст экспертиза «Доктор Веб» в зависимости от объема услуг, оплаченных заказчиком по договору.

Вопросы	Ответы
Что было скомпрометировано (объект экспертизы)	▪ Была ли нарушена целостность компьютерной системы. ▪ Был ли КИ совершен с помощью вредоносного ПО (в этом случае он является ВКИ, а значит, лежит в пределах границ экспертизы «Доктор Веб»). ▪ Являлся ли ВКИ последствием умышленных действий.
Где произошел ВКИ (среда ВКИ)	▪ Описание технических характеристик и особенностей системы, в которой произошел ВКИ, а также ее окружения. Цели использования системы заказчиком (необходимо для правильной приоритизации ИИБ). ▪ Есть ли признаки несанкционированного доступа к компьютерной системе. ▪ Описание средств защиты системы, в которой произошел ВКИ, и были ли они скомпрометированы. Если да — что послужило причиной компрометации.
Что послужило причиной возникновения (совершения) ВКИ	▪ Какие нарушения правил эксплуатации компьютерной системы или политики безопасности со стороны персонала послужили причиной ВКИ.
Каким образом совершен ВКИ	▪ Перечень вирусов и вредоносного ПО, использованного для совершения ВКИ, с описанием их функциональных особенностей (как задействованных злоумышленником в данном ВКИ, так и несущих потенциальную угрозу). ▪ Действия, предпринятые сотрудниками заказчика для обнаружения ВКИ и после его обнаружения. Оценка правильности этих действий.
К каким результатам привел ВКИ	▪ Текущее состояние компьютерной системы. ▪ В чем состоит факт компрометации (что похищено). ▪ Последствия компрометации. ▪ Можно ли продолжать пользоваться скомпрометированной компьютерной системой.

Дата актуализации 11.02.2014 г

Кто причастен к ВКИ	▪ Круг лиц, причастных к ВКИ (умышленно или по халатности), и мера причастности каждого.
Какие собраны доказательства совершения ВКИ	▪ Находится ли ВКИ в области юрисдикции судебной компьютерно-технической экспертизы (СКТЭ). Возможно ли обращение в правоохранительные органы и затем в суд. Шансы на выигрыш дела. ▪ Перечень собранных доказательств.
Как не допустить подобных ВКИ в будущем	▪ Рекомендации по построению системы антивирусной защиты с целью недопущения ВКИ или сокращения их количества в будущем.

Дата актуализации 11.02.2014 г

X. Правила поведения в условиях произошедшего вирусозависимого инцидента

Похищены средства из системы дистанционного банковского обслуживания

К сожалению, 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.
   Образец заявления
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.
   Образец заявления
4. Напишите заявление в полицию и приложите к нему заявления в два банка (получателя и отправителя платежа). Для этого надо посетить ближайшее отделение.
   Образец заявления

ВНИМАНИЕ!

Против вас совершено противоправное действие — могут присутствовать признаки преступлений, предусмотренных ст. 159.6, 165, 272, 273 УК РФ (по состоянию на 10.12.2012).
Для возбуждения в отношении злоумышленников уголовного дела правоохранительным органам необходим процессуальный повод — ваше заявление о преступлении.
Образец заявления

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.
Образец заявления

ВНИМАНИЕ!

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

ВАЖНО!

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!!!

Файлы зашифрованы троянцем семейства Encoder

Троянцы семейства Encoder «прославились» тем, что шифруют данные на компьютере жертвы. Эти данные можно попытаться восстановить. Для этого как можно скорее обратитесь в службу технической поддержки «Доктор Веб» по телефону или с другого компьютера!

ВНИМАНИЕ!

- *Не пользуйтесь зараженным компьютером до получения инструкций от службы технической поддержки «Доктор Веб» — даже если в нем есть острая (производственная) необходимость!*
- *Не пытайтесь переустановить систему!*
- *Не пытайтесь удалить с диска какие-либо файлы или программы!*
- *Если вы запустили антивирусное сканирование, нельзя предпринимать никаких необратимых действий по лечению/удалению вредоносных объектов. Прежде чем что-то делать с найденными вирусами/троянцами, следует проконсультироваться со специалистом «Доктор Веб» или в крайнем случае сохранить копии всего найденного вредоносного — это может потребоваться для определения ключа для расшифровки данных.*

Как составить запрос в службу технической поддержки «Доктор Веб»

1. Заполните форму запроса поддержки.
2. Сообщите как можно больше информации о том, как произошло заражение, в том числе требования злоумышленников. Если есть хоть какие-то подозрения о том, запуск чего послужил причиной срабатывания троянца, приложите к запросу соответствующие файлы или ссылки.

3. Прикрепите к комментарию в запросе несколько зашифрованных файлов (по возможности разных типов и размеров: jpg, zip, doc, pdf и т. п.) и требования злоумышленников о перечислении денежных средств.
4. Если троянец был получен по электронной почте (часто письма с такими троянцами имитируют письмо из банка с уведомлением о каких-то проблемах) и вы не удалили это письмо — сохраните письмо в eml-файл и прикрепите этот файл к комментарию в запросе.

Отправить запрос на расшифровку

Настоятельно рекомендуем обратиться с заявлением в полицию.

Против вас совершено противоправное действие — могут присутствовать признаки преступлений, предусмотренных ст. 159.6, 163, 165, 272, 273 УК РФ.
Для возбуждения в отношении злоумышленников уголовного дела правоохранительным органам необходим процессуальный повод — ваше заявление о преступлении.

Образец заявления

Приготовьтесь к тому, что ваш компьютер будет изъят на какое-то время на экспертизу.
Если у вас откажутся принять заявление — получите письменный отказ и обращайтесь с жалобой в вышестоящий орган полиции (к начальнику полиции вашего города или области).

Троянец-блокировщик заблокировал Windows

ВНИМАНИЕ!

Ни в коем случае не следует платить выкуп — вы никогда не получите обещанный вымогателями код разблокировки!

Воспользуйтесь бесплатным сервисом компании «Доктор Веб» по разблокировке Windows от троянца.

Настоятельно рекомендуем обратиться с заявлением в полицию.

Действия автора (авторов) троянца содержат в себе признаки составов двух преступлений с единым умыслом. Это преступление, предусмотренное ст. 273 УК РФ («Создание, использование и распространение вредоносных программ для ЭВМ»), а также ст. 163 УК РФ («Вымогательство»). Кроме того, если в ответ не пришла «спасительная утилита» для разблокировки, к первым двум составам добавляется третий — ст. 165 УК РФ («Причинение имущественного ущерба путем обмана или злоупотребления доверием»).
Для возбуждения в отношении злоумышленников уголовного дела правоохранительным органам необходим процессуальный повод — ваше заявление о преступлении.

Образец заявления

Если у вас откажутся принять заявление, получите письменный отказ и обращайтесь с жалобой в вышестоящий орган полиции — к начальнику полиции вашего города (области).

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

Телефон: +7 (495) 789–45–87 (многоканальный);
Факс: +7 (495) 789–45–97

www.drweb.com | www.drweb.com | www.av-desk.com | http://freedrweb.com | http://mobi.drweb.com