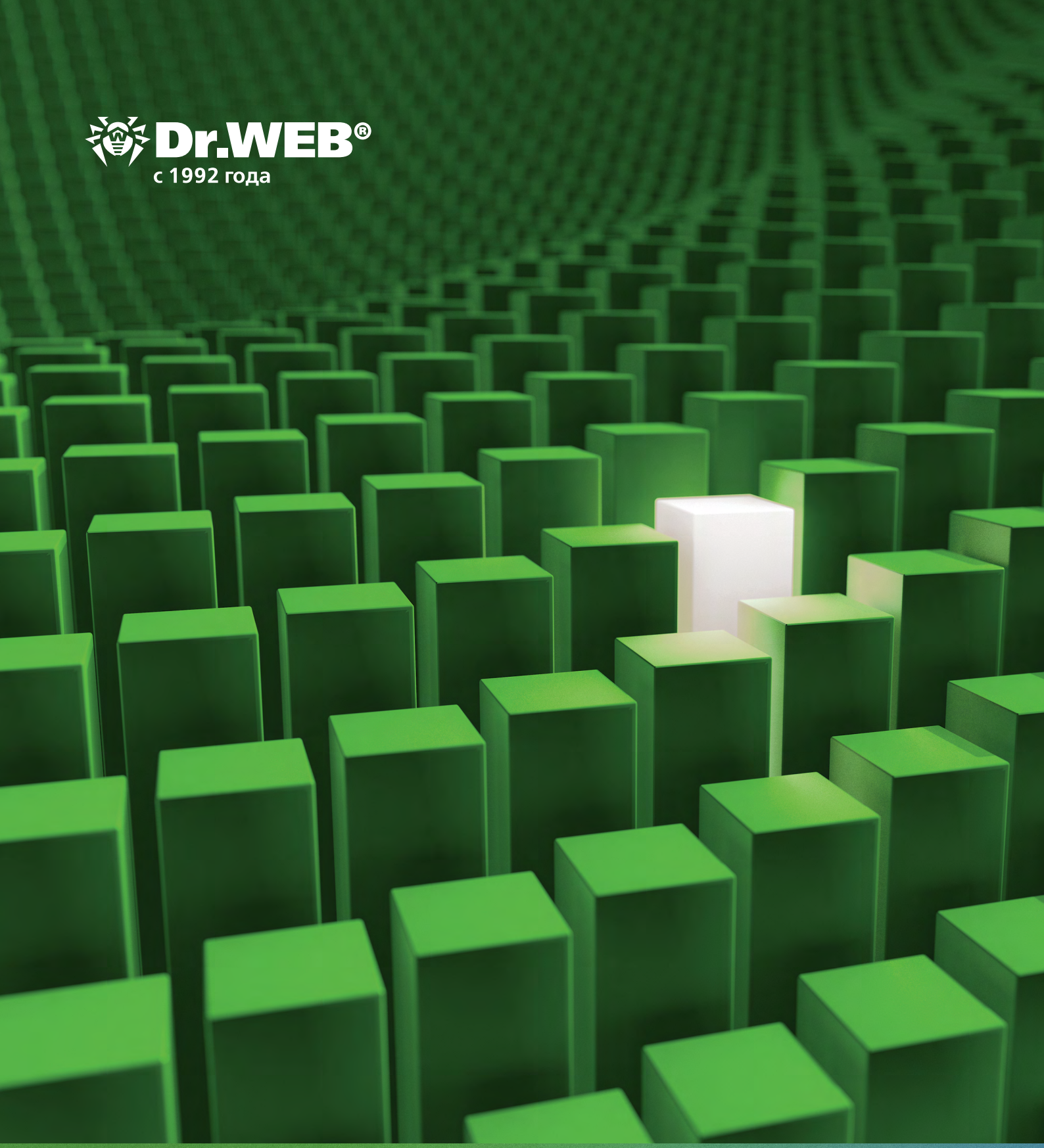
Dr.WEB®
с 1992 года



# АНТИВИРУСНАЯ СИСТЕМА ЗАЩИТЫ ПРЕДПРИЯТИЯ

# Содержание

# 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

Увеличению количества вредоносных файлов способствует распространение услуги по разработке вредоносных программ — для «получения» работающего вредоносного кода теперь не обязательно иметь навыки программиста.

## Основные векторы коммерческого кибермошенничества

- Компрометация компьютерных систем — с целью присоединения их к бот-сетям различного назначения, хищения хранящейся в системе информации, организации (D)DoS-атак.
- Вымогательство и/или порча информации.
- 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 количества преступлений, 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.

Перед выпуском вредоносных программ в «живую природу» криминальные группировки тестируют их на необнаружение всеми актуальными антивирусными решениями, что 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 — если пользователь не использует возможности Превентивной защиты и Офисного контроля.

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.

## 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.

**ФАКТЫ**

Ежесуточно в антивирусную лабораторию «Доктор Веб» поступает до миллиона и более образцов вредоносных программ.

**ЗАБЛУЖДЕНИЕ**

### Антивирус должен обнаруживать 100% вирусов.

Иными словами, качественный антивирус должен знать на момент проникновения все или практически все вредоносные программы. Антивирус, пропускающий вредоносные программы, считается некачественным и подлежащим замене.

### 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.

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.

**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 образца 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.
- **Технология Dr.Web ShellGuard** — закрывает путь в компьютер для эксплойтов — вредоносных объектов, пытающихся использовать уязвимости, в том числе еще не известные никому, кроме вирусописателей (так называемые уязвимости «нулевого дня»), с целью получения контроля над атакуемыми приложениями или операционной системой в целом, контролируя запущенные процессы «изнутри».
- **Традиционный эвристический анализатор** — содержит механизмы обнаружения неизвестных вредоносных программ. Работа эвристического анализатора опирается на знания (эвристики) об определенных особенностях (признаках) вирусов — как характерных именно для вирусного кода, так и, наоборот, крайне редко встречающихся в вирусах. Каждый из таких признаков

характеризуется своим «весом» — числом, модуль которого определяет важность, серьезность данного признака, а знак, соответственно, указывает на то, подтверждает он или опровергает гипотезу о возможном наличии неизвестного вируса в анализируемом коде.

- **Модуль эмуляции исполнения** — технология эмуляции исполнения программного кода необходима для обнаружения полиморфных и сложношифрованных вирусов, когда непосредственное применение поиска по контрольным суммам невозможно либо крайне затруднено (из-за невозможности построения надежных сигнатур). Метод состоит в имитации исполнения анализируемого кода эмулятором — программной моделью процессора (и отчасти компьютера и ОС).

**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. Как и вирусы, они относятся к категории вредоносных программ и могут нанести серьезный ущерб владельцу инфицированного компьютера.

### Опасные троянцы:

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

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

**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 в момент проникновения, рассчитанную на скрытое проникновение, — но никакое другое программное обеспечение, кроме антивируса, не способно вылечить систему от уже проникшего и запущенного 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.

# 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

Образовательный проект «Антивирусная правДА!»:
https://www.drweb.ru/pravda

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

# Пути проникновения вирусных угроз в корпоративные сети

**Большинство компаний совершают грубейшие ошибки при построении антивирусной системы 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. Ошибки в настройках антивирусной защиты

Статистика службы технической поддержки компании «Доктор Веб» свидетельствует, что заражения зачастую происходят уже известными антивирусной защите вирусами и троянцами — вследствие того, что администраторы сети отключают антивирусную проверку отдельных каталогов и целых дисков, проверку трафика браузера и почтовых клиентов. Распространенной ошибкой является отказ от ограничения прав доступа к мошенническим и заведомо вредоносным сайтам.

Ни один антивирус не может знать все вредоносные программы — и это действительно так, если мы говорим о традиционном антивирусе, использующем только вирусные базы. Антивирус Dr.Web использует Превентивную защиту и облачный сервис Dr.Web Cloud, что позволяет предотвращать заражение неизвестными антивирусному ядру угрозами — но по-настоящему эффективной защита становится только в том случае, если администратор самостоятельно настроит ограничения на доступ к ресурсам системы и сети Интернет с помощью Dr.Web Process Heuristic и Брандмауэра Dr.Web.

## 2. 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).

Централизованное управление обновлениями с помощью Центра управления Dr.Web позволяет компании иметь актуальную систему защиты — отказ от проведения обновлений и перезагрузки является грубейшей ошибкой, так как каждое обновление — это информация о ранее неизвестных сотнях и тысячах вредоносных программ, которые именно в этот момент могут атаковать вашу систему.

**ВНИМАНИЕ!**

Никакое другое программное обеспечение, кроме антивируса, не способно вылечить систему от вредоносного ПО, проникшего через уязвимости.

## 3. 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.**

**ВНИМАНИЕ!**

По статистике, более 80% сайтов сети Интернет имеют уязвимости и могут быть взломаны. Для утечки личных данных или заражения системы зачастую достаточно просто зайти на зараженный сайт.

### 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.

## 4. 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.

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.

## 5. Личные, в том числе мобильные устройства сотрудников

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

### 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.

## 6. Электронная почта

Почтовый трафик является основным переносчиком вирусов и спама. В случае заражения компьютера вредоносные программы могут получить доступ к адресной книге сотрудника, где 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.

Возможность получения сотрудниками компании исполняемых программ в виде вложений в почтовые сообщения стало одной из причин эпидемии троянцев-шифровальщиков.

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.

## 7. 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.

# Требования законодательства Российской Федерации в области антивирусной защиты

**На данный момент существует ряд обязательных для исполнения на территории Российской Федерации документов, описывающих требования к защите информации. В том числе это:**

- Федеральный закон № 152-ФЗ «О персональных данных»;
- Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- стандарт ИБ Банка России СТО БР ИББС 1.0.

Важно отметить, что Федеральный закон № 152 ФЗ – в отличие, например, от стандарта СТО БР – 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.

## Федеральный закон № 152-ФЗ «О персональных данных»

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

**В области антивирусной защиты исполнение требований Федерального закона № 152-ФЗ и подзаконных актов подразумевает:**

- 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

### В части программного обеспечения, согласно требованиям стандарта СТО БР ИББС-1.0-2010, 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**).

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**).

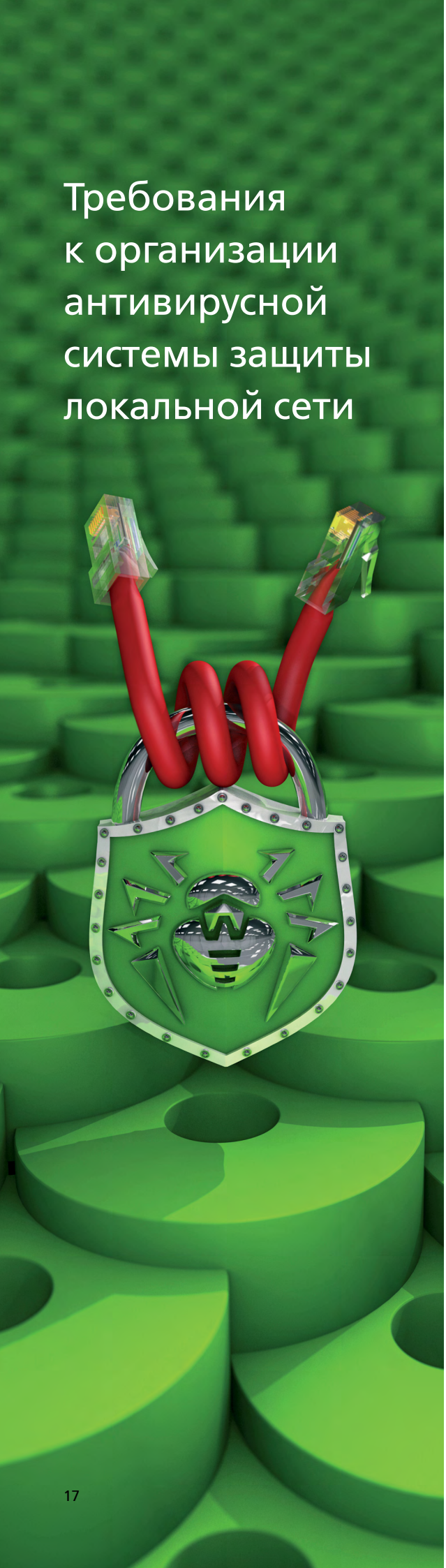
В организации, соответствующей требованиям стандарта, должна использоваться только защищенная почта, что вместе с требованием о наличии защиты от вирусов и спама подразумевает установку средств антивирусной фильтрации почтовых сообщений (антиспам входит только в лицензию **Dr.Web Desktop Security Suite 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

(HTTP-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.

# Требования к организации антивирусной системы защиты локальной сети



## Общие требования

### 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.

### Центр управления Dr.Web позволяет централизованно контролировать соблюдение политики безопасности в части проведения регулярных сканирований:

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

### Центр управления Dr.Web Enterprise Security Suite обеспечивает централизованное управление защитой всех узлов корпоративной сети:

- рабочих станций, клиентов терминальных серверов и клиентов встроенных систем на платформах Windows, Linux и macOS;
- файловых серверов и серверов приложений (включая терминальные серверы) Windows, Novell NetWare, macOS, Unix (Samba) и Novell Storage Services;
- почтовых серверов Unix, Microsoft Exchange, IBM Lotus, Kerio;
- интернет-шлюзов Unix и Kerio;
- мобильных устройств на основе Android и BlackBerry.

**Только централизованное управление защитой средствами Центра управления Dr.Web дает реальную экономию средств.**

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

### Использование функций Центра управления Dr.Web позволяет:

- проводить централизованную установку, обновление и настройку программных средств антивирусной защиты, в том числе на недоступных с сервера компьютерах;
- оперативно управлять системой защиты локальной сети в любой момент

времени, из любой точки мира, с любой операционной системы и без необходимости предварительной установки дополнительного программного обеспечения;

- реализовать необходимые для конкретного предприятия и отдельных групп сотрудников политики безопасности;
- назначать отдельных администраторов для различных групп;
- проводить антивирусную полную или выборочную проверку узла сети на наличие вирусных угроз как по команде пользователя или администратора, так и по расписанию;
- осуществлять сбор и анализ информации различного типа о состоянии системы защиты узлов локальной сети, а также создание отчетов за необходимый период времени;
- уведомлять администраторов и пользователей о состоянии системы защиты;
- проводить рассылку информационных сообщений пользователям в режиме реального времени.

**Центр управления Dr.Web лицензируется бесплатно.**
**Подробнее:** http://products.drweb.com/enterprise_security_suite/control_center

## Защита 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.

### В качестве мер защиты в случае использования облачных сервисов должны использоваться:

- 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.

### 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.

## Организация защиты рабочих станций

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.

### 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.

**ВНИМАНИЕ!**

Почтовые потоки, проходящие через рабочую станцию и сервер, не совпадают.

- 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.

Поэтому почтовый трафик надо фильтровать как на уровне почтового сервера, так и на уровне рабочих станций.

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.

**Уже достаточно давно для проникновения на компьютер в большей степени используются уязвимости программного обеспечения (в первую очередь Adobe), а не уязвимости операционных систем. Компоненты Dr.Web SpIDer Gate и SpIDer Mail производят 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;
- ограничить доступ к сменным носителям;
- 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, так как:
  - пользователи значительно меньше отвлекаются от основной работы на проверку приходящей почты,
  - уменьшается вероятность пропуска или удаления важного сообщения.
- **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 macOS, Linux и UNIX. Если обеспечивается защита только Windows, 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!**

Начиная с 2013 года тенденцией стал резкий рост количества атак на операционные системы Linux и иные системы, в силу различных причин не защищаемые антивирусом. Если ранее новости о заражении Linux-машин были крайне редки, то с середины 2013 года практически еженедельно появляется информация о новом массовом заражении или взломе.

## 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 критиче-

ски 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 вредоносных 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.

**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.

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.**

## Организация защиты файловых серверов

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

### Почему важно защищать серверы?

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

**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.**

**ВНИМАНИЕ!**

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

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, — возможны 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.

## 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:

- Антивирус Dr.Web для Linux
- 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.

## 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.

**Центр управления Dr.Web** позволяет централизованно контролировать антивирусную систему защиты любого количества файловых серверов под управлением Windows, macOS, Unix (Samba), Novell NetWare, Novell Storage Services.

## 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.

### 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 антивирусной системе 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.

## 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.

## 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 пери-

метра, 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**.

## Принципы фильтрации интернет-трафика на шлюзах

**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.

Использование антивирусной фильтрации на базе шлюзовых решений обеспечивает:

- защиту от заражения при наличии доступа к ресурсам компании со стороны сотрудников, работающих удаленно;
- защиту от проникновения вредоносных программ на компьютеры и устройства, не имеющие антивирусной защиты в связи с невозможностью ее установки, — в том числе принтеры, сетевое оборудование, систему управления технологическими процессами.

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 необходимо приобрести два антивирусных 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.

# Экспертиза вирусозависимых инцидентов

**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**.

## 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.

## 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 в соответствии с действующим законодательством РФ.

# 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.

**ВНИМАНИЕ!**

– Не пытайтесь обновить антивирус или запустить сканирование – так вы уничтожите следы злоумышленников в системе!

– Не пытайтесь переустановить операционную систему!

– Не пытайтесь удалить с диска какие-либо файлы или программы!

– Не пользуйтесь компьютером, с которого предположительно произошла утечка средств аутентификации к системе ДБО – даже если в нем есть острая (производственная) необходимость!

### Ваши действия должны быть быстрыми и решительными:

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

**ВНИМАНИЕ!**

Против вас совершено противоправное действие — могут присутствовать признаки преступлений, предусмотренных 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.

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

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

**ВНИМАНИЕ!**

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

**ВАЖНО!**

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!

**Образцы заявлений:** http://legal.drweb.com/templates

## 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»!

**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.

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.

**Образцы заявлений:** http://legal.drweb.com/templates



125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Телефон: +7 (495) 789–45–87 (многоканальный)
Факс: +7 (495) 789–45–97