Dr.WEB®
Антивирус

Информационный бюллетень

Мобильные устройства как угроза безопасности сетей компаний и домашних компьютеров пользователей

Дата составления	9.10.12
Текущий уровень опасности	Высокий

Наиболее актуальные угрозы безопасности компаний*	Типы угроз
Вредоносные программы, предназначенные для мобильных устройств. Опасность проникновения вредоносных программ с личных компьютеров и устройств пользователей.	Android.SpyEye.1 Android.SpyEye.2.origin Коммерческие продукты для кибершпионажа

* Актуальность угроз определяется не только количеством и разнообразием вредоносных программ, но и уровнем защиты от них в компаниях и организациях различного типа.

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.freedrweb.com
www.av-desk.com

Тема выпуска: Мобильные устройства как угроза безопасности сетей компаний и домашних компьютеров пользователей

Причина выпуска бюллетеня

Развитие вредоносных программ для популярных мобильных платформ представляет серьезную опасность для корпоративных сред, в которых применяются личные мобильные устройства сотрудников.

Типичные представители вредоносных программ

К категории наиболее опасных угроз данного типа можно отнести:

1. Троянские программы семейства **Android.SpyEye**
2. Коммерческие продукты, предназначенные для кибершпионажа
3. Вредоносные приложения, способные перехватывать СМС и сообщения электронной почты, которые могут содержать конфиденциальную информацию

Кроме специализированных под конкретные ОС вредоносных программ, существуют троянцы, способные работать на любой мобильной платформе с поддержкой Java (например, Symbian OS, а также большинство сотовых телефонов).

Причина актуальности угрозы

На данный момент недостаточная защищенность мобильных устройств представляет серьезную угрозу как для их владельцев, так и для компаний, сотрудники которых так или иначе используют мобильные устройства.

Внедренная в мобильное устройство вредоносная программа может:

- получить доступ к почтовой переписке, паролям используемых программ, системам работы с денежными средствами;
- получить доступ к конфиденциальным данным, сохраненным в виде файлов, фотографиям;
- отправлять СМС и звонить на платные номера;
- включать микрофон без ведома жертвы — и тем самым получать информацию «из первых уст»;
- получать данные от GPS-навигатора о местонахождении жертвы — ее присутствии или отсутствии в определенных местах;
- получать доступ к конфиденциальным данным, сохраненным в виде фотографий и звуковых записей, а также СМС-переписке и истории совершенных звонков.

Владелец зараженного устройства может отказаться под полным круглосуточным контролем!

Для компаний заражение мобильных устройств сотрудников представляет особо опасную угрозу безопасности, поскольку:

- некоторое количество сотрудников работает с корпоративной почтой и конфиденциальными данными на своих устройствах; более семидесяти процентов для работы используют только личные устройства;
- троянские программы способны отсылать СМС-сообщения на платные номера и подключать жертву к так называемым подпискам с регулярной абонентской платой, что может привести к потере денежных средств пользователями корпоративных тарифов и, соответственно, компанией;
- доступ злоумышленников к сообщениям электронной почты и СМС может привести к разглашению важной конфиденциальной информации, включая пароли от различных учетных записей;
- вредоносные программы, способные получить доступ к операционной системе мобильного устройства с полномочиями администратора, могут устанавливать на инфицированное устройство другие приложения, в том числе программы-шпионы.

Отсутствие защиты не просто снижает эффективность работы — это создает возможность утечки, подмены или компрометации важных для компании материалов. Нередко сотрудники работают не только на своем рабочем месте, но и дома, в дороге, на отдыхе — распространение мобильных устройств и доступность Интернета в любой момент и в любом месте дают эту возможность. Как следствие, отсутствует гарантия получения только безопасного контента, вне офиса люди никак не защищены от атак злоумышленников. Не ограничиваемые корпоративной политикой безопасности, пользователи устройств самостоятельно скачивают и устанавливают различные приложения (в том числе для работы с документами, для работы в социальных сетях и т. д.). При этом эти приложения могут как иметь уязвимости, так и содержать в своем составе специально разработанные вредоносные программы.

Причина роста количества угроз для Android — открытость основных исходных кодов этой операционной системы. Любые обнаруженные в ней уязвимости мгновенно становятся достоянием широкой общественности. ОС Android доступна большому числу производителей, выпускающих смартфоны с различными техническими характеристиками и версиями операционной системы. Несмотря на попытки Google оперативно выпускать обновления системы, закрывающие обнаруживаемые уязвимости, обилие различных модификаций платформы часто мешает пользователям своевременно получать эти обновления, так как каждый производитель имеет свою стратегию по их выпуску. Случается и так, что производитель вообще отказывается от дальнейших обновлений некоторых моделей мобильных устройств по причине их устаревания, экономическим или техническим соображениям или же по каким-либо другим причинам, и пользователи становятся беззащитными перед угрозой проникновения в систему вредоносного ПО.

Доступный исходный код Android также может использоваться различными энтузиастами, создающими свои сборки операционной системы. Вирусописатели освоили и эту нишу. Они могут распространять троянские программы **(Android.SmsHider)**, имеющие цифровую подпись одного из образов такой сборки.

Среди типов данных, которые подвергаются опасности хищения при проникновении на мобильное устройство вредоносных программ, можно перечислить СМС-сообщения и почтовую переписку, документы, фотографии, посещенные веб-страницы, журнал браузера, данные GPS-приемника. Отдельную опасность представляет возможность подмены злоумышленниками просматриваемых пользователем веб-страниц, внедрение в них посторонних форм и объектов. Нельзя забывать и о том, что некоторые троянские программы способны записывать и передавать злоумышленникам голос во время телефонных разговоров с использованием инфицированного смартфона. Чем выше положение владельца такого устройства в компании, тем более ценными могут оказаться похищенные злоумышленниками сведения.

Пути и методы проникновения

Распространение вредоносных программ для мобильных устройств происходит следующими путями:

1. Использование известных уязвимостей, эксплуатирующихся для повышения привилегий вредоносного приложения в системе **(Android.Gongfu, Android.DreamExploid, Android.Wukong)**.
2. Использование методов социальной инженерии. Наиболее часто используются следующие методы:
   1) предложение установить обновления (в том числе с «официального веб-сайта Opera Mini») **(Android.Crusewind, Java.SMSSend, Android.SmsSend)**;
   2) предложение бесплатно загрузить платное коммерческое приложение;
   3) предложение в демонстрируемой рекламе срочной проверки мобильного устройства на вирусы. Нажав на рекламное сообщение, пользователь попадает на сайт, якобы сканирующий мобильное устройство. При этом сайт может заимствовать внешний вид известных антивирусных ресурсов и программ, например, внешнее оформление Dr.Web Security Space версии 7.0 **(Android.SmsSend)**.

При этом зачастую вредоносная программа даже не использует для установки никаких уязвимостей — ее инсталляция возлагается на жертву. Иногда в комплекте с инфицированным приложением жертве предлагается специальная пошаговая инструкция, позволяющая запустить ОС с полномочиями администратора. В инструкции утверждается, что это необходимо для корректной работы запускаемой программы или ее обновления **(Android.Gongfu)**.

3. Оптимизация поисковых запросов. В ключевых словах, которые разработчики добавляют в описания программ, помещаются популярные словосочетания, не относящиеся к данному продукту, например, названия популярных игр. В результате ссылки на подобные программы часто демонстрируются в первых строках результатов поиска по каталогу программ.
4. Использование методов фишинга. Например, далеко не все пользователи Android в курсе, что ресурса под названием Android Market больше не существует. Пользователи обращаются с соответствующими запросами к поисковым системам и получают в выдаче ссылки на веб-сайты, подражающие своим оформлением оригинальному порталу Android Market. Как вариант, злоумышленники могут создавать правдоподобные копии официального сайта Google Play и размещать их на интернет-ресурсах с адресами, похожими на истинный адрес данного каталога программ.

   Существуют специально разработанные партнерские программы, позволяющие создавать сайты-подделки, с которых посетителям раздаются различные вредоносные приложения, в том числе троянцы семейства Android.SmsSend.
5. Размещение вредоносных программ в официальном каталоге приложений (Google Play, ранее известный как Android Market) **(Android.SmsSend, Android.DreamExploid, Android.DDLight)**.
6. Распространение в составе легитимных программ на популярных сайтах-сборниках приложений **(Android.Spy, Android.Gongfu, Android.GoldDream, Android.Anzhu)**.
7. Маскировка под обычные приложения (в том числе приложения, позволяющие изменять фоновый рисунок Рабочего стола Android, программы составления гороскопов, диет, программа-фонарик, «живые обои» и т. д.).
8. Взлом веб-ресурсов (в том числе автоматический с использованием специализированного ПО). При открытии веб-страниц происходит автоматическое перенаправление пользователя на принадлежащий злоумышленникам интернет-ресурс или начинается непосредственно загрузка троянца.
9. Установка вредоносной программы в систему с использованием приложений-посредников (дропперов), способных загружать с сайтов злоумышленников вредоносное ПО.

Особенностью методик заражения мобильных устройств является учет возможности использования жертвами различных платформ. Так, в зависимости от типа клиентской ОС жертвы могут получать либо приложения для Android (.apk), либо кросс-платформенные файлы типа .jar.

Цель проникновения

1. Хищение приватной и конфиденциальной информации с инфицированного устройства: СМС-сообщений, почтовой переписки, контактов, документов, фотографий.

   Так, **Android.Gone.1** за 60 секунд «угоняет» всю хранящуюся на работающем под управлением Android мобильном телефоне информацию, включая идентификационную информацию о зараженном устройстве (в том числе версию операционной системы, модель телефона, наименование мобильного оператора, номер IMEI и телефонный номер пользователя), контакты, сообщения, последние звонки, историю браузера и т. д.
2. Осуществление слежки за пользователем инфицированного устройства: перехват его телефонных переговоров, СМС, электронной почты, слежение за его перемещениями по данным GPS-навигатора.
3. Рассылка СМС. Зараженные устройства могут использоваться для рассылки спама или иных тестовых сообщений **(Android.NoWay)**, политических **(Android.Arspam)** и религиозных сообщений. Список рассылки может задаваться извне или браться из списка абонентов адресной книги. При этом вредоносная программа старается скрыть следы своей деятельности, удаляя из памяти смартфона отосланные ею сообщения и входящие СМС с информацией о приеме платежа оператором **(Android.SmsSend)**.

   Отправка платного СМС может производиться уже на этапе установки вредоносной программы — при запуске пользователю демонстрируется текст о том, что владелец мобильного устройства соглашается с неким условиями, причем само соглашение с перечнем этих условий, как правило, отсутствует. В случае если соглашение присутствует, оно может быть скрыто от пользователя или иметь нейтральный, незаметный вид. Например, последнее слово в тексте может представлять собой гиперссылку на страницу с лицензионным соглашением и никак не выделяться на фоне окружающих слов. При подтверждении согласия нажатием на соответствующую кнопку приложение немедленно попытается отправить платное СМС-сообщение. Также возможен вариант, когда после запуска на экране устройства появляется вступительный текст и две кнопки: подтверждение согласия с условиями лицензии, и вторая, при нажатии на которую должен открываться тест соглашения, при этом соглашение располагается на стороннем веб-сайте, который в данный момент не функционирует, поэтому ознакомиться с предлагаемыми условиями пользователь не может.
4. Осуществление звонков на платные номера (**Android.Fakevoice**), кража денег со счетов владельцев мобильных телефонов путем подписки их на различные платные сервисы.
5. Добавление сайтов, указанных в конфигурационном файле вредоносной программы, в закладки браузера (**Android.Anzhu** не просто устанавливает закладки из переданного вирусописателями списка, но также меняет их атрибуты, помечая как посещенные, что придает таким закладкам больший вес в глазах пользователя).
6. Кража конфиденциальной информации **(Android.Gongfu, Android.SpyEye, Android.DreamExploid, Android.Gone)**. Украденные данные загружаются на специально созданный вирусописателями сайт. Данные могут быть проданы для использования в спам-рассылках, целевом вымогательстве, осуществляемом с учетом знания данных жертвы. К числу платных шпионских программ относятся **Flexispy, Mobile Spy, Mobistealth**.
7. Вымогательство денег за похищенную информацию **(Android.Gone)**.
8. Запуск и удаление различных программ на инфицированном устройстве, загрузка других вредоносных приложений **(Android.Gongfu, Android.Anzhu)**.
9. Выполнение на инфицированном устройстве получаемых от управляющего центра команд (функции бэкдора имеют **Android.Plankton**, **Android.Gongfu**, **Android.GoldDream**, **Android.Anzhu**). Расширяемая архитектура вредоносных программ дает возможность владельцам криминальной сети загружать специальные дополнения (плагины) для выполнения дополнительных деструктивных действий — в том числе для проведения атаки на целевую компанию.
10. Кража паролей доступа к различным программам и интернет-сервисам, например к FTP-ресурсам компании.
11. Кража денежных средств через системы ДБО **(Android.SpyEye)**.
12. Включение зараженных машин в управляемые ботнеты, координируемые из одного (или нескольких) командных центров.

Методы перехвата информации

1. Контроль за всеми СМС-сообщениями, а также входящими и исходящими телефонными звонками, запись сведений об этих событиях (в том числе телефонных номеров, с которых или на которые выполнялся звонок или отправлялось сообщение), сохранение содержания звонка и содержимого СМС **(Android.GoldDream)**.
2. Запись нажатий пользователем клавиш — в том числе на виртуальной клавиатуре **(Android.AntaresSpy.1)**.
3. Перехват информации, вводимой пользователем в браузере (в том числе во время работы с банком).
4. Подмена страниц банковских сайтов — в просматриваемую пользователем веб-страницу осуществляется инъекция постороннего содержимого, которое может включать различный текст или веб-формы. Таким образом, ничего не подозревающая жертва загружает в браузере настольного компьютера или ноутбука веб-страницу банка, в котором у нее открыт счет, и обнаруживает сообщение о том, что банком введены в действие новые меры безопасности, без соблюдения которых пользователь не сможет получить доступ к системе «Банк-Клиент», а также предложение загрузить на мобильный телефон специальное приложение, содержащее троянскую программу **(Android.SpyEye.1)**.
5. Анализатор трафика и вклинивание в интернет-трафик в поисках учетных данных и передаваемых значений.
6. Перехват функций, которые могут участвовать в передаче данных.
7. Запись голоса во время телефонных разговоров.
8. Копирование и передача файлов, хранящихся во внутренней памяти устройства или на подключаемом накопителе.

Методы маскировки от средств контроля и наблюдения

1. Маскировка под легитимное ПО: игры, живые обои, «полезные» программы и т. д.
2. Маскировка под компонент операционной системы или системную утилиту.
3. Запуск процесса с привилегиями администратора, блокировка попыток удалить вредоносное приложение **(Android.SmsSend.186.origin)**.
4. Скрытие требуемых для работы вредоносной программы разрешений **(Android.MulDrop.5.origin)**.

Обязательные средства защиты

Средство защиты	Необходимость применения
Система проверки ссылок	Система Cloud Checker позволяет исключить возможность перехода на зараженные и мошеннические ресурсы.
Проверка всех поступающих на устройство файлов (через GPRS/Infrared/Bluetooth/Wi-Fi/USB-соединения или во время синхронизации с ПК)	Позволяет уменьшить риск внедрения вредоносных программ из недоверенных источников, а также избежать скрытой загрузки незапрошенных компонентов приложений, содержащих вредоносный функционал.
Формирование списка разрешенных приложений	Позволяет уменьшить риск запуска неизвестных приложений без их предварительной проверки на безопасность.
Система ограничения доступа	Позволяет ограничить количество посещаемых ресурсов до необходимого минимума, что минимизирует риск заражения с сайтов, содержащих вредоносные объекты.
Антивирусный монитор	Позволяет исключить заражение с помощью вредоносных объектов, проникших на машину пользователя без проверки — в том числе в запароленных архивах или с помощью специальных протоколов передачи данных.
Антивирусный сканер	Периодическая глубокая проверка дает возможность обнаружения вредоносных программ, каким-либо образом сумевших проникнуть на устройство (в том числе в тот период, когда сигнатура данной вредоносной программы еще не была добавлена в вирусные базы).

Кроме установки и настройки программных средств защиты, рекомендуется:

1) ограничить права пользователей и запретить для них запуск операционной системы с правами администратора;
2) пользователям корпоративных тарифов мобильной связи запретить отправку СМС на короткие номера;
3) своевременно устанавливать все обновления системы безопасности и использовать стойкие пароли.

Внимание! Перечисленные меры защиты должны быть приняты на всех мобильных устройствах, вне зависимости от используемой операционной системы.

Рекомендуемые средства защиты

Средство защиты	Необходимость применения
Загрузка приложений только из известных и проверенных источников	Разработчики вредоносных программ зачастую предлагают загрузить известную программу «удобно и бесплатно». Однако в большинстве случаев сайты разработчиков этих программ позволяют сделать то же самое!*
Использование системы удаленного управления мобильным устройством в случае его утери или кражи	Система Антивор позволяет исключить риск утечки конфиденциальной информации в результате кражи устройства.
Система централизованного управления	▪ Позволяет исключить возможность отключения пользователями систем защиты. ▪ Позволяет устанавливать единые для всей компании или групп пользователей правила информационной безопасности. ▪ Позволяет в случае возникновения той или иной угрозы мгновенно менять настройки системы безопасности.
Система сбора и анализа статистики	Дает возможность контролировать уровень защищенности компании в режиме реального времени, определять источники заражения.
Система сбора информации для служб технической поддержки	Позволяет минимизировать время решения тех или иных проблем.

* Для компаний, использующих решения Dr.Web для защиты рабочих станций, предоставляется бесплатная лицензия на Dr.Web Mobile Security Suite на тот же срок и на такое же количество защищаемых объектов, что и купленная лицензия.

Скомпрометированные средства защиты

Средство защиты	Методы обхода системы защиты
Установка приложений только с официального сайта Google Play* (ранее Android Market)	Схема работы Google Play позволяет загружать на него вредоносные программы, тем более что в момент загрузки на Google Play они могут не детектироваться ни одним антивирусом.
Использование программ, работающих в защищенном окружении (в том числе Java)	Подмена программных компонентов

* Плюсом использования Google Play является возможность централизованного удаления установленных приложений. Компания Google, как и Apple, может задействовать эту функцию, например, в случае если какое-либо приложение представляет угрозу для пользователей.

С момента выпуска предыдущего бюллетеня появились сведения о возможности обхода вредоносными программами двухшаговых систем аутентификации (например, включающих использование карты с чипом и пинкода). Кроме этого, был зафиксирован факт перехвата одноразовых паролей, высылаемых банком в виде СМС-сообщений.

Пример настройки средств защиты

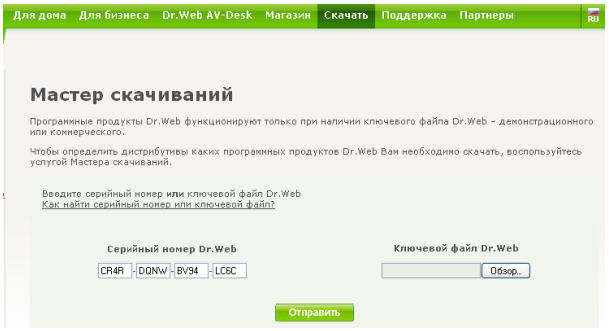
В качестве примера рассмотрим настройку системы защиты для операционной системы Android.

Установку версии антивируса Dr.Web, поддерживающей возможность централизованного управления, можно осуществить путем запуска установочного файла на мобильном устройстве или с помощью программы синхронизации с ПК. Версию без централизованного управления можно установить также с Google Play — для этого нужно только найти в списке приложений Dr.Web для Android и нажать Install (Установить).

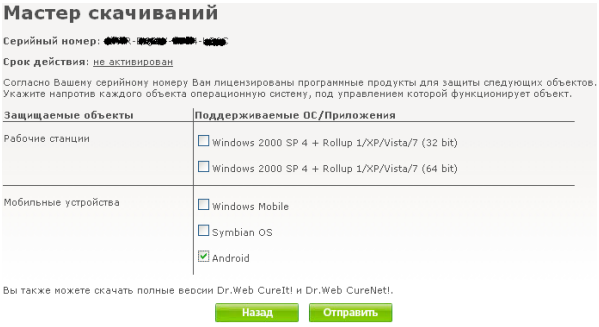
Чтобы установить приложение без использования Google Play, необходимо разрешить такой вид установки. Для этого откройте экран **Настройки → Приложения** и установите флажок **Неизвестные источники**.

Для установки версии с возможностью использования в корпоративной сети необходимо:

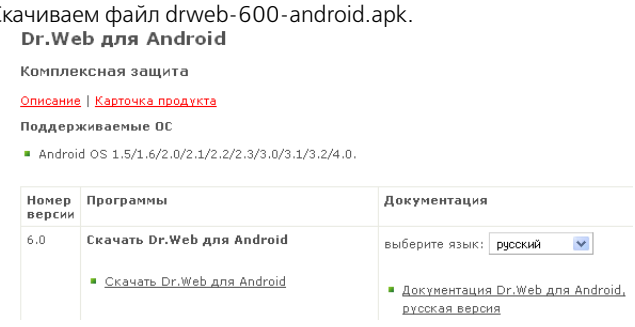
- Скачать файл установки Dr.Web для Android. Для этого на странице вводим серийный номер продукта, используемого для защиты рабочих станций.



Нажимаем **Отправить** и на странице **Мастера скачивания** выбираем, что мы хотим защищать.

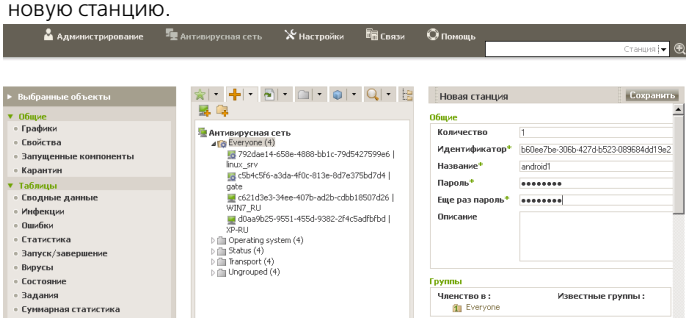


Скачиваем файл drweb-600-android.apk.

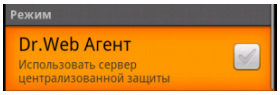


- Подключаем мобильное устройство к компьютеру при помощи USB-соединения и выбираем опцию распознавания мобильного устройства как диска.
- Копируем на SD-карту файл drweb-600-android.apk.
- Запускаем на мобильном устройстве любой файловый менеджер (например, ASTRO из Android Market), открываем папку /sdcard и запускаем drweb-600-android.apk.
- Антивирус Dr.Web установлен, однако для дальнейшей работы с приложением необходимо либо зарегистрировать лицензию и скопировать полученный ключевой файл на защищаемое устройство, либо подключить его к системе централизованного управления.

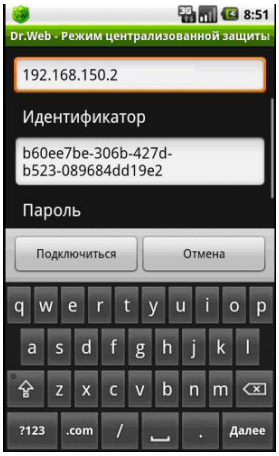
Для включения устройства в состав системы безопасности открываем Центр управления Enterprise Security Suite и создаем новую станцию.



Зайдя в меню Dr.Web для Android, переходим в раздел **Инструменты** или нажимаем кнопку **Меню** и выбираем пункт **Настройки**. В разделе Режим отмечаем флажок **Dr.Web Агент**.



В открывшемся окне указываем IP-адрес сервера централизованной антивирусной защиты и, при необходимости, через двоеточие после IP-адреса порт, использующийся для подключения к серверу, идентификатор, присвоенный вашему мобильному устройству при создании станции, и пароль.



Нажимаем **Подключиться**.

В режиме централизованной защиты блокируется возможность ручного запуска и настройки обновлений. Системный администратор может определять параметры постоянной защиты, определять список приложений, доступных пользователям антивирусной сети на их устройствах, и проводить проверку системы по требованию.

О компании «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности и лидер российского рынка интернет-сервисов безопасности. Антивирусные продукты Dr.Web разрабатываются с 1992 года и имеют сертификаты ФСТЭК России, ФСБ России и Министерства обороны РФ.

Наличие в нашем штате экспертов по различным вопросам, связанным с информационной безопасностью, позволяет нам максимально учитывать особенности работы компаний самого разного размера и профиля деятельности. Мы предлагаем нашим клиентам оптимальный выбор продуктов, имеющих минимальную совокупную стоимость, и, как разработчик этих продуктов, гарантируем их высокое качество. Проверить качество работы наших решений вы можете как с помощью бесплатных лечащих утилит Dr.Web CureNet! и Dr.Web CureIt!, так и с помощью сервиса тестирования наших решений — Dr.Web LiveDemo.