

Сетевые средства «Родительского контроля»

Для дополнения существующих программных решений «родительского контроля» или в случае, если использование их затруднено, можно использовать сетевые средства, такие как «защищённые» сервера системы сетевых имён (DNS) и услуги операторов связи по предоставлению доступа к уже отфильтрованному сегменту сети Интернет.

Защищённые DNS работают на этапе преобразования имени сервера, вводимого пользователем в адресной строке Интернет-браузера, при переходе по ссылке, размещённой на уже открытой WEB-странице в ip-адрес, понятный сетевому оборудованию. При этом, если указанный адрес числится в списке «плохих» ресурсов, то происходит перенаправление пользователя на страницу с уведомлением о попытке посещения заблокированного ресурса.

Существует большое количество как платных, так и бесплатных сервисов «Защищённых» DNS. Для «русскоговорящего» сегмента сети Интернет наиболее оптимально использование сервисов, предоставляемых отечественными компаниями, такими как:

Яндекс.DNS - <http://dns.yandex.ru/>

Sky DNS - <https://www.skydns.ru/>

Rejector - <http://rejector.ru/>

Подробная информация о возможностях сервисов и о том, как их использовать приведена на официальных страницах. Первый и третий сервисы предоставляется бесплатно (Яндекс.DNS в режиме тестирования). Второй сервис отличаются тем, что наравне с бесплатным режимом работы предоставляет расширенные варианты сервиса за плату.

Операторы связи начали обеспечивать спрос на предоставление услуг «родительского контроля» предоставляя подключение к сегменту Интернет с применением контентной фильтрации. Функциональность решений и их стоимость сильно различается в зависимости от оператора и наличия технической возможности сетей в конкретном регионе. На территории Ямало-Ненецкого автономного округа средства родительского контроля доступны у операторов ОАО «Мобильные Телесистемы» (МТС), ОАО «Мегафон», ОАО «Вымпелком» (Билайн) при использовании услуг передачи данных посредством сетей мобильной связи. Актуальная информация о средствах родительского контроля имеется на сайтах операторов:

http://yanao.megafon.ru/tariffs/options/spetsialne/detskiy_internet.html,

http://yanao.megafon.ru/tariffs/options/spetsialne/optsiya_tineydzher.html

http://www.yamal.mts.ru/mobil_inet_and_tv/internet_phone/additionally_services/parent_control/

<http://safe.beeline.ru/>

Антивирусное программное обеспечение

BitDefender Internet Security



BitDefender Internet Security защищает интернет-соединения с использованием семейного фильтра, без

ощутимого замедления работы персонального компьютера. Он блокирует вирусы, атаки хакеров и спам, обеспечивая родительский контроль и защиту с помощью межсетевого экрана.

Возможности родительского контроля представлены следующим набором функций:

- ■ Применение политики разделения учетных записей по доступу к ресурсам компьютера и Интернет;
- ■ Блокирование доступа к несоответствующим вебсайтам и электронной почте;
- ■ Ограничение доступа детей к Интернету и отдельным приложениям (например, играм) по расписанию.

Основным приемом блокирования доступа к нежелательному контенту являются пять фильтров, обеспечивающих анализ электронной почты. Эвристический фильтр проверяет почту на наличие характеристик спама. Фильтр Whitelist/Blacklist отклоняет почту от известных адресов спаммеров и пропускает желательную почту. Фильтр URL блокирует почту, содержащую злонамеренные ссылки (список блокируемых сайтов регулярно пополняется вместе с обновлениями BitDefender). Фильтр символьных наборов (charset) блокирует почту, написанную в «странных» символах. Фильтр изображений решает, предназначены ли внедренные в электронную почту изображения для рассылки спама.

Защита пользователя при работе в пиринговых (P2P) сетях и при использовании сервисов обмена мгновенными сообщениями (ICQ, Skype и пр.) осуществляется, как и положено данной категории продуктов, не на уровне ограничения доступа к ним, а лишь защитой от проникновения вирусов. Это, несомненно, достойный функционал продукта. Однако он не учитывает социального влияния (доступа к нежелательным ресурсам) и правового использования контента (загрузки нелегального нелицензионного контента) данных сервисов пользователями Интернет, в частности, детьми.

Dr.Web Security Space

Dr.Web Security Space – это новейшее средство комплексной защиты компьютера, включающее в себя антивирус, веб-антивирус, антируткит, антишпион, антиспам. В состав Dr.Web Security Space также входит средство родительского контроля.



Ключевыми функциями модуля Родительского контроля Dr.Web, заявленными разработчиком, являются:

- ■ Блокировка сайтов по категориям (порнография/эротика, наркотики, жестокость, нецензурная лексика, оружие, азартные игры, чаты, интернет-почта, социальные сети, экстремизм/терроризм);
- ■ Защита от киберпреступности, направленной против детей;
- ■ Блокировка доступа к переносным хранилищам информации, сетевым устройствам, дисководам, а также отдельным файлам и каталогам, что

делает невозможным удаление или похищение конфиденциальной информации.

Управление доступом к сайтам осуществляется с использованием белых и чёрных списков. Модуль Родительского Контроля позволяет ограничивать доступ как к конкретным сайтам или страничкам на сайтах, так и ко всем известным сайтам, содержащим информацию определенной тематики. Блокировка сайтов по тематике осуществляется автоматически с помощью списков, регулярно обновляемых компанией «Доктор Веб».

С помощью модуля Родительского контроля также осуществляется ограничение доступа пользователя к ресурсам, содержащимся как локально, на самом ПК, так и в сети. Пользователь может обезопасить свои данные от удаления или похищения злоумышленниками, запретив использование переносных хранилищ информации, сетевых устройств, а также отдельных файлов и каталогов. Ограничение доступа к ресурсам локальной файловой системы позволяет сохранить целостность важных файлов и защитить их от заражения вирусами, а также сохранит необходимую конфиденциальность данных.

Родительский контроль Dr.Web обладает высокой эффективностью и не мешает обычной работе пользователя за компьютером.

F-Secure Internet Security



F-Secure Internet Security обеспечивает полноценную и простую в использовании защиту от всех интернет-угроз, как известных, так и только что появившихся.

Родительский Контроль - часть пакета программ F-Secure Internet Security. Под управлением Родительского Контроля блокируется доступ к сайтам с несоответствующим информационным наполнением, что позволяет фильтровать контент web-страниц.

Разработчик декларирует возможность родительского контроля времени, проводимого ребёнком в сети Интернет. Еще одной отличительной особенностью продукта является возможность восстановления административного управления программой в случае утраты родительского пароля.

В то же время, стоит отметить некоторые нюансы функционирования модуля Родительский Контроль. Пользователь должен указывать точные доменные имена сайтов при занесении их в чёрный или белый список. Если пользователь добавит только, например example.com в белый список, то сайт с адресом www.example.com не будет расценен как разрешённый домен, и программа не гарантирует доступ к этому сайту. Чтобы иметь доступ к сайту, пользователь должен ввести домен в белый список в формате www.example.com.

В целом, F-Secure Internet Security обеспечивает минимальный набор функций родительского контроля, присущий всем антивирусным продуктам.

Kaspersky Internet Security

Kaspersky Internet Security обеспечивает защиту компьютера от известных и новых угроз, хакерских и мошеннических атак, спама и



других нежелательных данных. Родительский контроль - специальный компонент в составе Kaspersky Internet Security, выполняющий функции контроля доступа пользователей компьютера к интернет-ресурсам. Основной задачей является ограничение доступа, в первую очередь, к следующим ресурсам:

- ■Веб-сайтам, предназначенным для взрослой аудитории, либо содержание которых затрагивает темы порнографии, оружия, наркотиков, провоцирует жестокость, насилие и т.д.
- ■Веб-сайтам, которые являются потенциальной причиной потери времени (чаты, игровые ресурсы) или денег (интернет-магазины, аукционы).

Блокировка веб-сайтов производится по восьми категориям: порнография/эротика, наркотики, жестокость, нецензурная лексика, оружие, азартные игры, чаты и интернет-почта. Управление временем доступа к сети Интернет, как и у прочих разработчиков антивирусного программного обеспечения, основано на задании суточного расписания, в течение которого интернет-соединение разрешено. Кроме того, возможна установка суммарного суточного лимита времени использования интернет-соединения. Разработчик также декларирует возможности своего программного продукта по исключению доступа не только к нежелательному текстовому содержанию сайтов, но также и к иллюстративным, фото- и видео- материалам.

Тем не менее, если пользователь хочет ознакомиться с содержанием конкретного сайта, он имеет право приостановить работу компонента Родительский Контроль, и тем самым принимает все риски, которые связаны с просмотром конкретного контента. Таким образом, забота о полноте доступа либо ограничении доступа к Интернет-сайтам и сервисам полностью ложится на плечи родителей. Родители могут изменить правила фильтрации и просмотреть отчеты, формируемые программой.

McAfee Parental Controls



Продукты McAfee Internet Security и McAfee Total Protection содержат в своём составе программу родительского контроля McAfee Parental Controls. Программа Родительского Контроля обеспечивает надежную защиту для пользователей, их семей, их личных файлов и компьютеров. Это решение помогает защититься от хищения личных данных, блокировать передачу личной информации, а также запретить доступ к потенциально оскорбительным материалам в Интернете, включая изображения, поскольку в состав пакета входит McAfee ImageAnalyzer, защищающий детей от просмотра изображений непристойного содержания.

McAfee Parental Controls также позволяет получить подробный отчет об использовании ресурсов Интернета любым пользователем домашнего компьютера, вести журнал участия ребенка в службах мгновенного обмена сообщениями, устанавливая временные квоты для работы в Сети. Кроме того, программа позволяет отслеживать, контролировать и фиксировать случаи несанкционированного пользования Интернетом и предоставляет надежное хранилище для личных паролей.

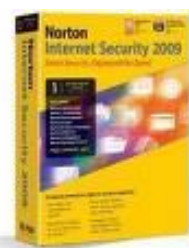
Программа McAfee Parental Controls обеспечивает выполнение следующих функций родительского контроля:

- ■Фильтрация веб-узлов по ключевым словам;
- ■Фильтрация веб-сайтов;
- ■Настройка ограничений по времени для просмотра веб-узлов;
- ■Настройка группы рейтинга содержимого с учётом возраста пользователя;
- ■Фильтрация потенциально неприемлемых изображений в Интернете;
- ■Включение функции поиска с учётом возрастных ограничений;
- ■Настройка учётных записей пользователей.

Несмотря на внушительный функционал Родительского Контроля, аналитики отмечают сложность процедуры установки программы. Кроме того, наличие многочисленных опций и буквенных сокращений в обозначениях вызывают значительные трудности в понимании настройки функций программы для обычного пользователя.

Norton Parental Controls

Продукты Norton 360 и Norton Internet Security позиционируются разработчиком как комплексные средства обеспечения безопасности компьютеров. Модуль родительского контроля Norton Parental Controls предлагается в составе дополнительного модуля Norton Add-on Pack к данным продуктам.



По данным разработчика, дополнительный модуль Norton Add-on Pack расширяет функциональность продуктов, а именно:

- ■Добавляет средства родительского контроля и блокирования конфиденциальной информации к продукту Norton Internet Security или Norton 360.
- ■Предоставляет защищенные паролем стандартные профили управления для взрослых, подростков и детей, которые можно адаптировать в соответствии с потребностями конкретного пользователя.
- ■Блокирует нежелательные веб-сайты в соответствии с параметрами профиля пользователя и регистрирует в журнале все попытки обращения к таким веб-сайтам.
- ■Предотвращает случайную передачу секретной информации (указанной как конфиденциальная) с компьютера.

Функция родительского контроля позволяет ограничить список типов веб-сайтов, к которым разрешен доступ, а также разрешить просмотр только веб-сайтов определенных типов. С помощью параметров настройки родители могут указать, какие типы веб-сайтов следует разрешить, а какие заблокировать. В модуле родительского контроля предусмотрено более 40 тематических категорий, таких как «Контент для взрослых», «Порнография», «Сексуальная ориентация», «Оружие», «Насилие» и др.

В то же время, как отмечают исследователи, продукт не обеспечивает блокирования портов пиринговых сетей, позволяющих ребёнку без ведома родителей скачивать и передавать информацию в виде файлов, видео- и фото-изображений и архивов.

В заключение необходимо отметить, что все продукты, представленные в настоящем обзоре, являются лидирующими на российском рынке средств

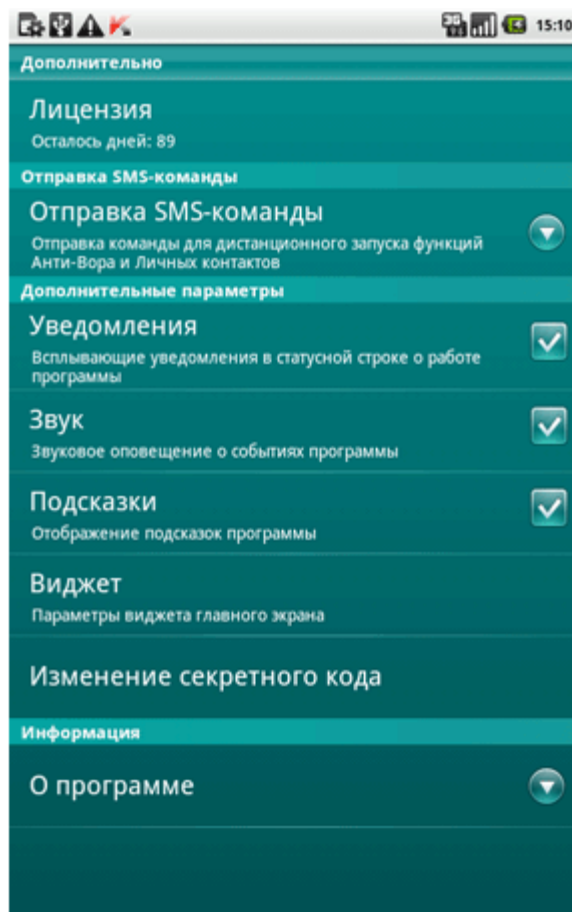
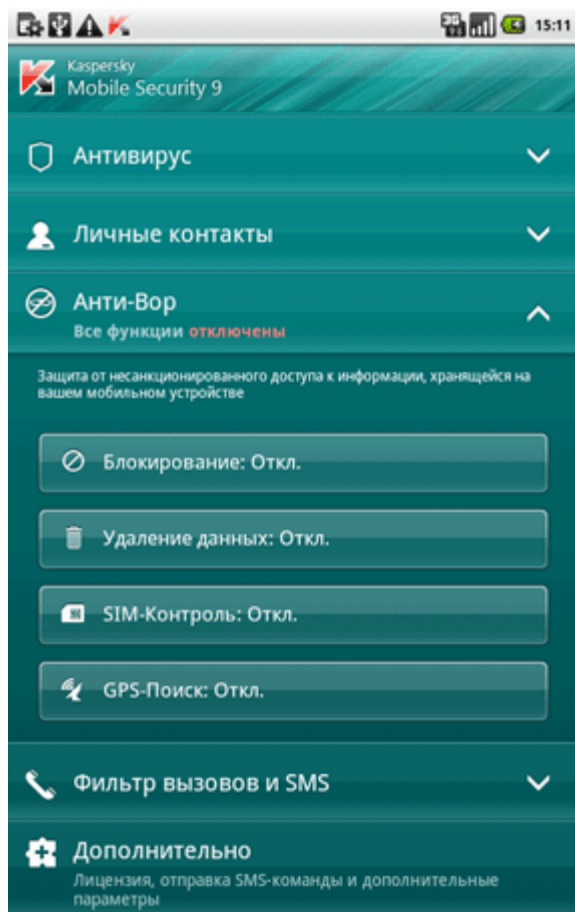
антивирусной защиты. В то же время, их возможности по части управления доступом в сеть Интернет и функциям родительского контроля весьма скромные, поскольку данный функционал не является определяющим для данных продуктов.

Для полнофункциональной защиты детей и семьи от негативного влияния Интернета лучше пользоваться специализированными средствами родительского контроля в сочетании с программными средствами антивирусной защиты.

Мобильные версии антивирусного программного обеспечения

[↑#Kaspersky Mobile Security 9](#)

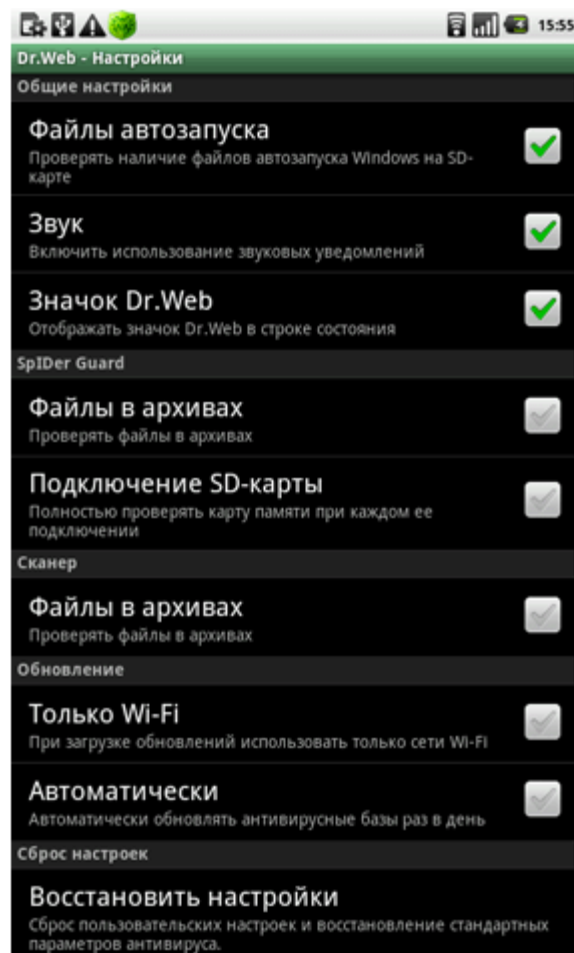
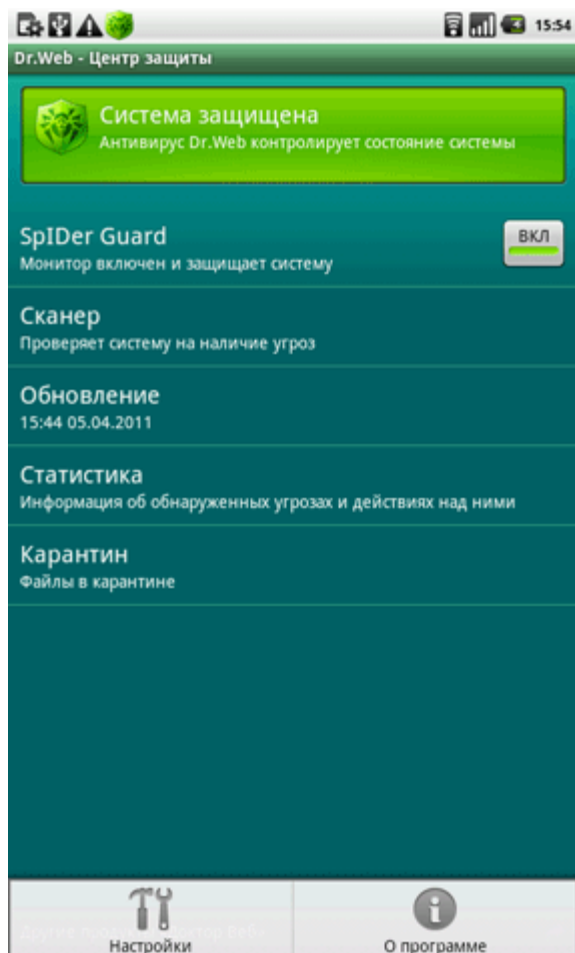
Мультиплатформенный инструментарий "Лабораторией Касперского" продукт который обеспечивает комплексную защиту как от вредоносного ПО, так и от нежелательных коротких текстовых сообщений и звонков. Реализованные в программе [функции](#) помогают вернуть устройство владельцу в случае его утери или кражи, а также позволяют скрывать от любопытных глаз контакты, историю звонков и SMS-переписку. В частности, отправив посредством SMS специальные инструкции на собственный номер, пользователь может определить координаты телефона, его местоположение на карте Google Maps, произвести дистанционную блокировку и при необходимости удалить всю хранящуюся в памяти аппарата конфиденциальную информацию. Не менее интересной возможностью Kaspersky Mobile Security 9 является контроль замены SIM-карты: в случае обнаружения чужой "симки" устройство автоматически блокируется и незаметно сообщает законному владельцу новый номер телефона. Наконец, еще одной отличительной особенностью решения является внушительного объема русскоязычная документация, доступная на сайте разработчика в формате PDF и разъясняющая все тонкости работы с приложением.



В отличие от редакций для [Windows](#) Mobile и Symbian OS, в сборку Kaspersky Mobile Security 9 для "Андроида" включены не все компоненты, поэтому при изучении упомянутого выше [ресурса](#) стоит помнить об отсутствии модуля шифрования с функцией создания секретных директорий для особо важных документов и файлов, родительского контроля и брандмауэра, ограничивающего сетевые соединения в соответствии с установленным пользователем уровнем безопасности. По словам представителей "Лаборатории Касперского", реализация перечисленных функций — дело ближайшего будущего, и работа в этом направлении уже ведется.

Dr.Web

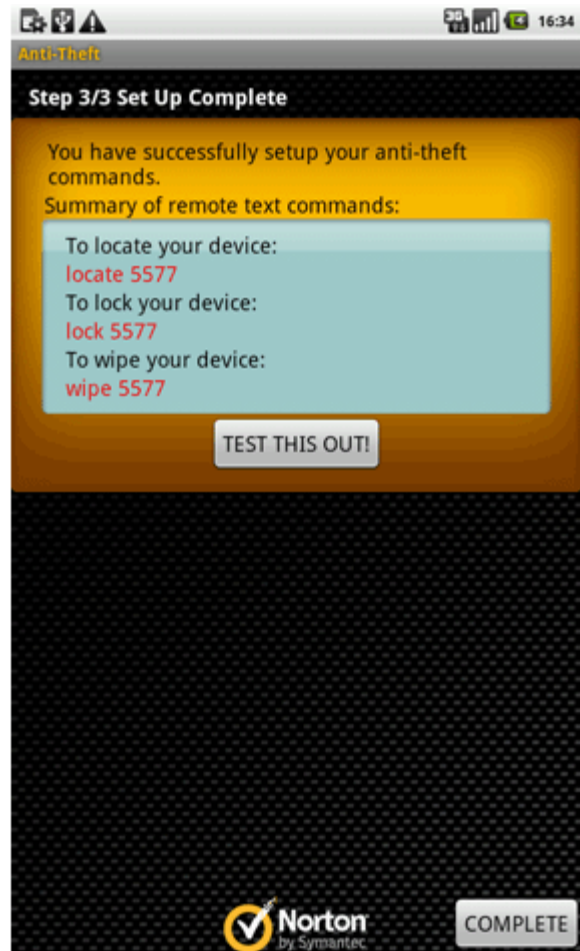
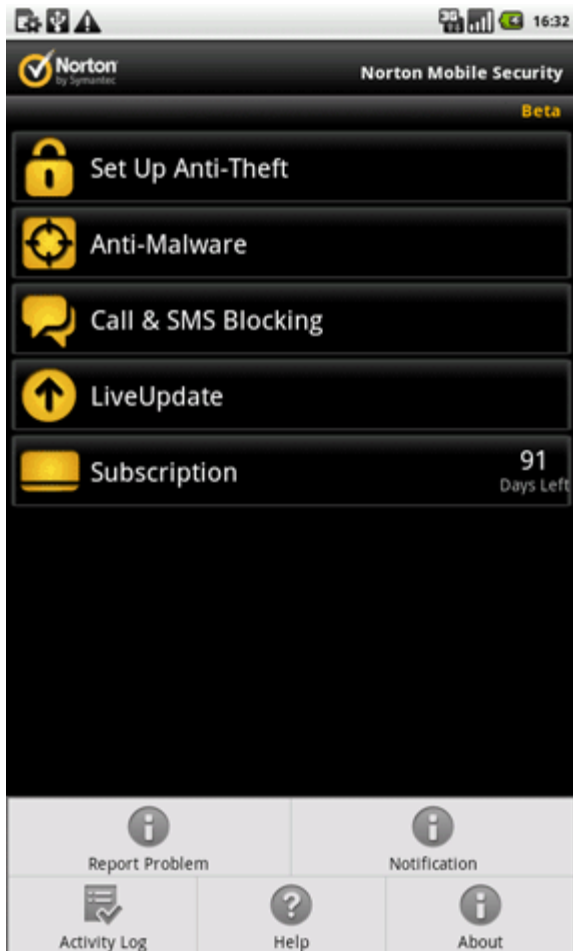
Dr.Web умеет выполнять проверку данных в режиме реального времени и вылавливать зловредов "на лету". При этом разработчики в документации к программе [открыто предупреждают](#), что постоянное функционирование сканирующего файлы монитора может повлечь увеличение расхода заряда батареи мобильного устройства.



Представители компании "Доктор Веб" подчеркивают, что, в отличие от других аналогичных продуктов, Dr.Web позволяет при необходимости прочитать заблокированное сообщение или перезвонить на занесенный в "черный" список телефонный номер. При этом в самой системе никаких следов нежелательных звонков или сообщений не остается, так как вся информация сохраняется исключительно в логе приложения. С помощью виджета рабочего стола пользователь может мгновенно определять текущий режим работы программы, переключаться между режимами, а также получать сведения о пропущенных вызовах или оставшихся без внимания коротких текстовых сообщениях.

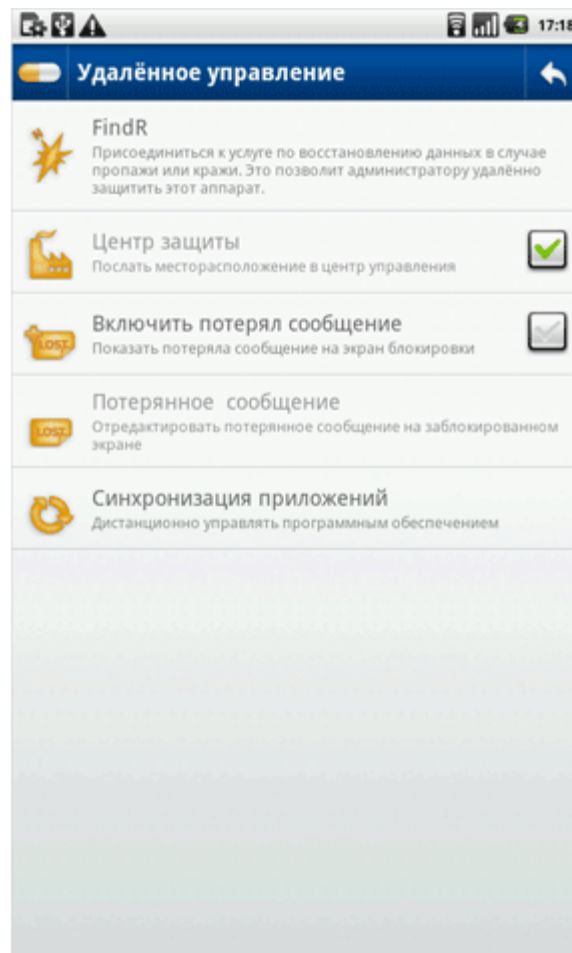
Norton Mobile Security

Разработанный "Симантеком" инструментарий также может похвастать "противоугонной" системой, позволяющей определить местоположение телефона и удаленно заблокировать его работу либо удалить важные данные, вылавливающим трояны и шпионские программы модулем, а также механизмом блокировки входящих звонков и SMS с определенных номеров. Norton Mobile Security, — опции сокрытия личных контактов и выборочной проверки файлов. В рамках бета-тестирования пакет распространяется бесплатно, однако есть все основания полагать, что после завершения отладки кода продукта Symantec переведет свой проект на коммерческие рельсы. Впрочем, не будем загадывать наперед.



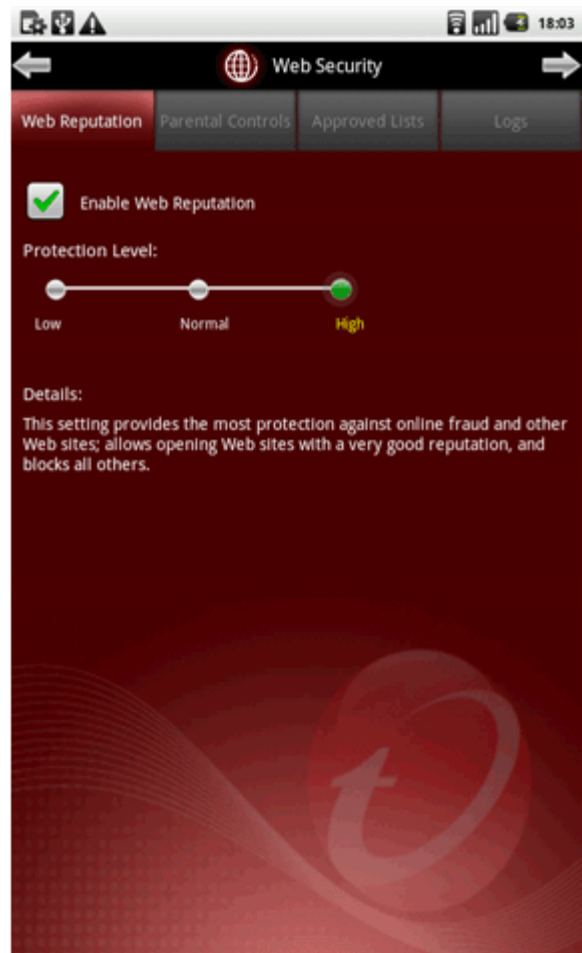
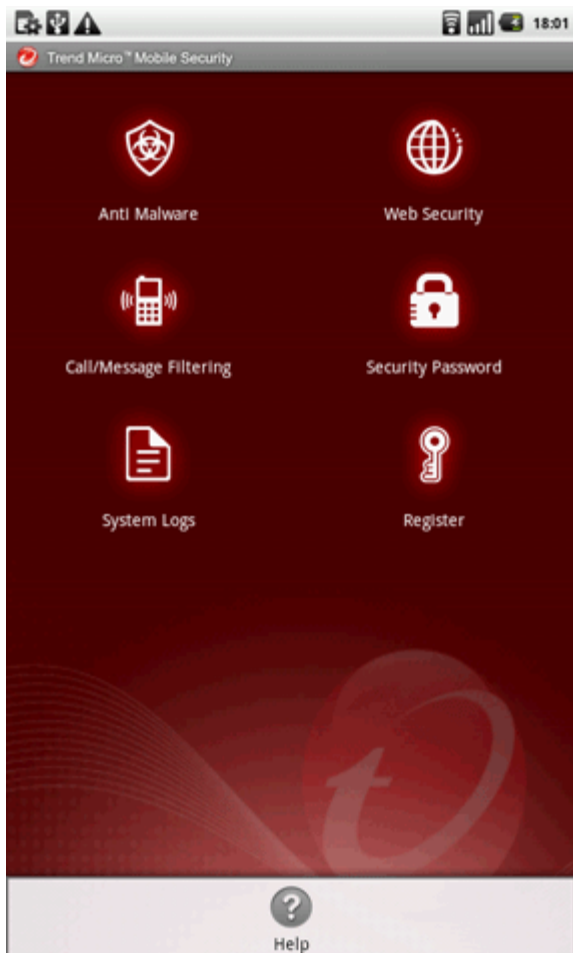
AVG Mobilation for Android

Характеризуется богатым функционалом. Из отличительных особенностей продукта стоит отметить работающий в режиме реального времени антивирус, встроенные средства резервного копирования приложений, записей адресной книги, сообщений, закладок [браузера](#) и прочих данных на SD-карту, механизм удаленного управления устройством посредством размещенного на сайте [droidsecurity.com](#) онлайн-инструментария FindR и дистанционной блокировки телефона, систему фильтрации SMS-сообщений, а также модуль защиты любых программ с помощью пароля от несанкционированного доступа. Отдельного упоминания заслуживают диспетчер задач и утилита удаления файлов без возможности их последующего восстановления.



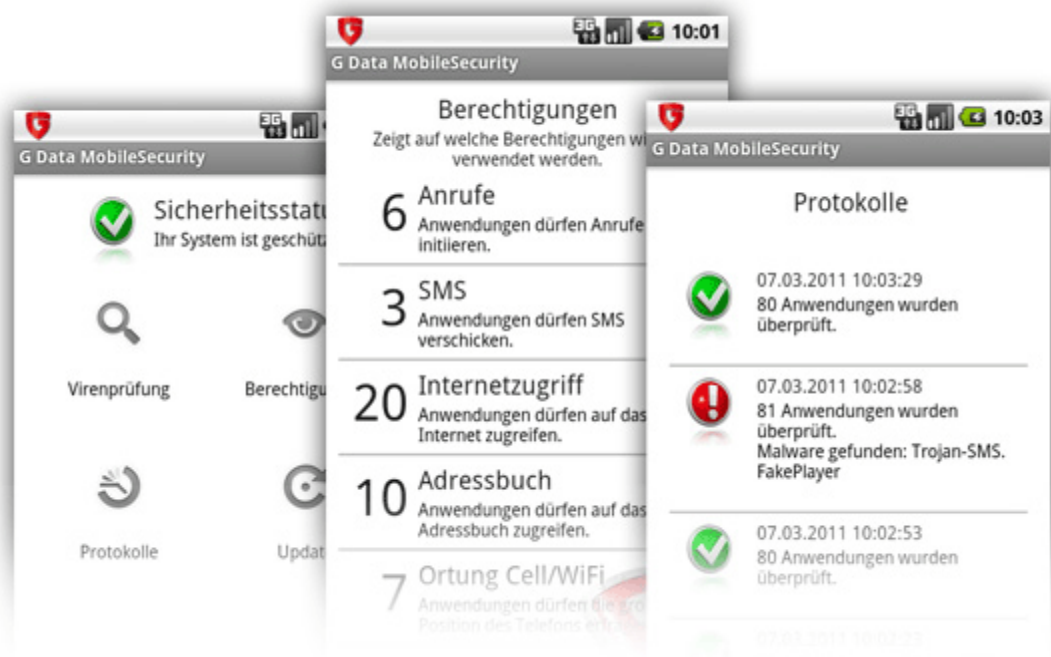
Trend Micro Mobile Security

В активе этого продукта — антивирус, система защиты от фишинговых и прочих вредоносных [веб-ресурсов](#), фильтр звонков и SMS, а также модуль родительского контроля, ограничивающий доступ детей к содержащим несоответствующий их возрасту контент сайтам. Начинка неплохая, но, увы, не лишенная одного досадного недостатка, выражающегося в излишней подозрительности компонента Web Reputation, норовящего заблокировать даже безобидные интернет-ресурсы. Безопасность, конечно, требует жертв, но чтобы настолько серьезных... В общем, вопрос полезности задействованной в Trend Micro Mobile Security технологии репутационных оценок для сайтов остался для нас открытым. К тому же следует учитывать ее бесполезность в случае использования клиент-серверных приложений, например браузера Opera Mini, обходящего защиту разработки Trend Micro на раз-два.



G Data MobileSecurity

Программный продукт, впервые анонсированный немецкой компанией G Data Software в ходе проходившей в начале марта выставки CeBIT 2011. Его продажи должны начаться в мае этого года (официальный релиз локализованной версии в России ожидается в августе). Поскольку данный материал готовился и верстался ранее упомянутой даты, опробовать в действии приложение нам не удалось и пришлось ограничиться информационными материалами, присланными пресс-службой разработчика. По сведениям последней, в G Data MobileSecurity будет задействован антивирус, модуль фильтрации звонков и сообщений, а также брандмауэр с функцией контроля активности установленного в "гуглофоне" ПО, позволяющей пресекать несанкционированную отправку SMS, передачу данных по сети и выполнение программами иных недозволённых действий.



Таков список продуктов, предлагаемых разработчиками средств информационной безопасности для защиты мобильных устройств под управлением операционной системы Android, и, чтобы читателю было проще разобраться в многообразии приложений, мы объединили все характеристики рассмотренных решений в одну таблицу. Вот она.