

Способы родительского контроля

Есть два основных пути обеспечения родительского контроля: данная услуга может быть обеспечена антивирусными программами, либо специально созданными под эту задачу утилитами (программами).

Среди антивирусных программ:

[Kaspersky Internet Security 2012 и Kaspersky CRYSTAL](#),

[Panda Internet Security](#)

[Avira Premium Security Suite](#)

[Dr.Web Security Space](#)

[Microsoft Windows Live Family Safety](#)

И другие.

С исследованием эффективности фильтров родительского контроля, обеспечиваемых антивирусными программами, можно познакомиться [здесь](#).

Программы родительского контроля предназначены, в первую очередь, для создания ограничений ребенку, они призваны обеспечить его безопасность, оградить от того, что, возможно, ему еще рано знать и видеть. Одна из основных задач приложений – создание фильтра web-сайтов. Все очень просто: на одни страницы заходить можно, на другие – нельзя. Как осуществляется подобный контроль? Обычно предлагается два варианта ограничений.

Приложение работает с базой данных, где содержатся сайты для взрослых. Крайне желательно, чтобы список регулярно обновлялся через интернет, иначе появление новых ресурсов быстро сделает защиту неактуальной. Администратор или, в данном случае, родители могут расширять черный список сайтов на свое усмотрение.

Довольно часто применяется более жесткий способ контроля – создание белого списка. Ребенок может посещать только те web-сайты, которые ему разрешили родители. Минус подобного контроля заключается в чрезмерной строгости, можно даже сказать, в жестокости. Пустили дочь за компьютер, а сайт с описаниями технических характеристик кукол не включили в белый список. Девочка в слезах. Подружки давно хвастаются новинками кукольного мира, а ребенок даже не в курсе, о чем вообще сверстники ведут разговор, интернета-то нормального нет. Зато не надо автоматически обновлять списки, актуальность со временем практически не теряется.

Еще один способ родительского контроля заключается в фильтрации сайтов по их содержанию. Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на web-странице, то она не открывается. Родителям, возможно, придется отбросить прочь страх и стыд, самостоятельно вписывая мат, пошлости, уголовщину и прочие вещи, запрещенные для ребенка.

Обеспечение безопасности ребенка за компьютером заключается не только в ограничении доступа к web-сайтам. Есть еще одна, если так можно выразиться, группа риска – это

программы обмена мгновенными сообщениями. Ребенок наивен, он может нечаянно рассказать незнакомцу ваши личные данные. Злоумышленники хитры, они прикидываются ровесниками, невзначай задают каверзные вопросы. Напрашивается и вторая опасность – собеседники ребенка могут научить его, в лучшем случае, мелким пакостям, а о примерах серьезных бед лучше даже не вспоминать. Некоторые программы родительского контроля способны производить анализ информации, отправляемой с компьютера. Если в ней встречаются некие ключевые слова, например, адрес, номер школы или телефона, то происходит блокировка отправки сообщения.