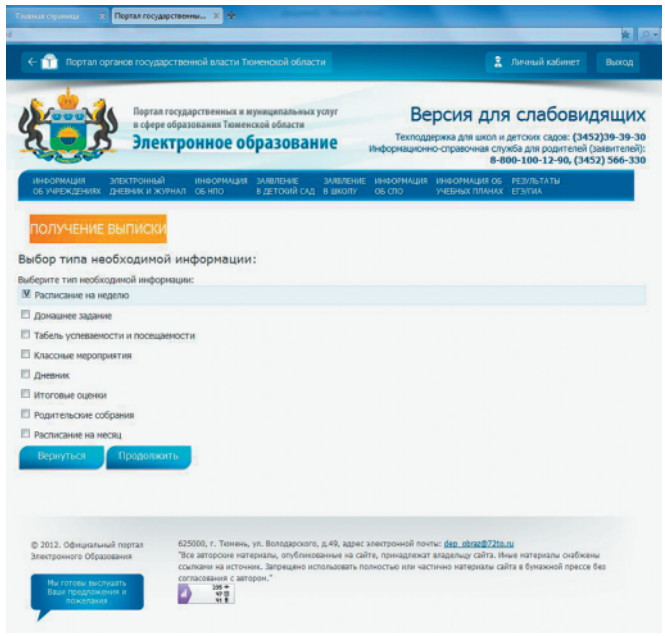
Шаг 3. Выбрать интересующую информацию и нажать кнопку «Продолжить».



Шаг 4. Указать период и нажать кнопку «Продолжить», после чего Вы сможете просмотреть нужную информацию.

4. БЕЗОПАСНОСТЬ ДЕТЕЙ В СОЦИАЛЬНЫХ СЕТЯХ. РОДИТЕЛЬСКИЙ КОНТРОЛЬ.

Нынешние дети начинают учиться считать, писать и читать практически одновременно с работой за компьютером. Хорошо это или плохо — вопрос спорный. Но, несомненно, освоение компьютера с юных лет открывает широкие возможности в плане развития и образования, которые чаще всего реализуются при активном подключении родителей в качестве направляющей и контролирующей стороны.

В России около 8 миллионов пользователей глобальной сети — дети. Они могут играть, знакомиться, познавать мир... Но, в отличие от взрослых, в виртуальном мире они не чувствуют опасности. Наша обязанность — защитить их от негативного контента.

Основные риски в Интернете:

— Сегодня не нужно работать в ФСБ, чтобы узнать о человеке все, достаточно залезть в Интернет, и Вы найдете фамилию, возраст, адрес, место учебы, материальное положение. Практика показывает, что дети в поисках друзей размещают о себе в Сетях только голую правду. А опытным мошенникам не остается ничего кроме как воспользоваться их наивностью и недостатком родительского контроля. Только контролируя Интернет, отслеживая переписку ребенка, родители могут обнаружить тех, кто отправляет подозрительные сообщения их детям, пытается втереться к ним в доверие, договориться о встрече, задает наводящие вопросы и забрасывает просьбами выслать откровенные фотографии.

— Глобальная Сеть содержит большое количество информации взрослого содержания. Интернет насчитывает сотни миллионов порнографических страниц.

— Другая серьезная проблема — распространение наркотиков через Глобальную Сеть. Достаточно набрать в поисковике название наркотического средства, чтобы узнать все, начиная от того, как его приготовить до того, где взять.

— В Интернете легко найти информацию суицидального характера, видеоматериалы по дракам, вскрытиям. Здесь же дети, оставшись без надлежащего контроля родителей, могут свободно познакомиться с любыми формами экстремизма.

— Интернет — реальный пожиратель времени. В поисках развлечений, играя или просто зависая в чате, можно проводить часы драгоценной жизни. В последние годы набирает обороты болезнь под названием «Интернет-зависимость». Дети начинают пропускать уроки, хуже учиться, становятся раздражительными. По мнению врачей, родителям следует контролировать, чтобы младший школьник проводил за компьютером не больше четверти часа.

— Кроме того, через Интернет легко проникают вредоносные программы в виде вложенных файлов электронных писем, троянских коней, HTML и Java-вирусов и могут привести к поломке компьютера.

С 1 ноября 2012 года вступили в силу изменения в федеральный закон «Об информации, информационных технологиях и о защите информации». Их суть — создание и ведение в режиме онлайн Единого общероссийского автоматизированного реестра сетевых адресов, позволяющего идентифицировать сайты с информацией, распространение которой в Российской Федерации запрещено. Информацию пользователи могут отправлять на всероссийский сайт **www.zapret-info.gov.ru** и тюменский **www.blacklist72.ru**.

Для детей и их неравнодушных родителей существует бесплатная линия помощи «Дети онл@йн» http://detionline.com.

4.1. РОДИТЕЛЬСКИЙ КОНТРОЛЬ КОМПЬЮТЕРА

Как правило, родителям требуется организовать контроль за временем работы на компьютере (время приходится ограничивать), регулировать доступ к «вредным» программам (в частности, к играм), а также наблюдать за использованием Интернета и блокировать доступ к неподходящим для ребенка ресурсам.

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 веб-сайтов. Все очень просто: на одни страницы заходить можно, на другие — нельзя.

Как осуществляется родительский контроль?

Обычно предлагается два варианта ограничений.

1. 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 веб-сайты, которые ему разрешили родители.

2. Еще один способ родительского контроля заключается в фильтрации сайтов по их содержимому. Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на веб-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 веб-сайтам. Есть еще одна, если так можно выразиться, группа риска — это программы обмена мгновенными сообщениями. Ребенок наивен, он может нечаянно рассказать незна-комцу ваши личные данные. Злоумышленники хитры, они прикидываются ровесниками, невзначай задают каверзные вопросы. 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.

Как обезопасить младшее поколение от негативных последствий пребывания в Сети?

1. Компьютер не должен стоять в детской комнате. Лучше всего, если он будет в зале, где кто-нибудь из родителей сможет постоянно следить за тем, чем занимается ребенок.

2. Ребенку надо показать Интернет, заинтересовать полезными, с вашей точки зрения, сайтами, объяснить, что можно делать, а что нельзя.

Родительский контроль компьютера — это набор программ и действий, который направлен на организацию или запрет использования детьми компьютерного времени, доступа к играм или другим программам, и самое главное — для избежания просмотра сайтов с «недетским» содержимым.

В Windows 7 можно устанавливать ограничения на использование детьми компьютера и повысить их безопасность в Интернете, не контролируя каждое их действие лично.

Функция родительского контроля позволяет:

- *ограничивать часы работы детей на компьютере;*
- *устанавливать перечень доступных им программ и компьютерных игр (и время их использования);*
- *блокировать доступ к просмотру нежелательных телепередач и фильмов.*

Чтобы повысить безопасность детей в Интернете, загрузите Семейную безопасность WindowsLive. Эта бесплатная программа поможет вам управлять списком веб-сайтов, которые доступны вашим детям, и контактов, с которыми они могут общаться по сети. Она также предоставляет полезные и простые в изучении отчеты об их действиях в Интернете.

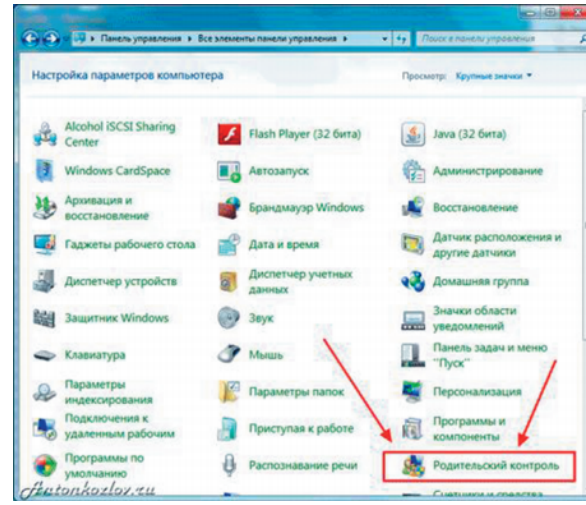
Несложно просмотреть, чем занимался ребенок в интернете в Ваше отсутствие. Простые примеры: после настройки родительского контроля компьютер сына или дочки будет включаться только после 6 вечера; игры будут доступны до 10 часов ночи; ни один сайт, содержащий в названии набор букв (s)*ex или por*(n), не будет открываться.

Идеального рецепта настройки родительского контроля не существует, поскольку тут все зависит от целого ряда факторов: уровня компьютерной подготовки ребенка и его родителей, компьютерных предпочтений и степени сознательности подрастающего поколения и, наконец, от отношения самих родителей к данной проблеме. Вариантов организации родительского контроля несколько.

Родительский контроль скачать бесплатно вполне возможно, существуют хорошие некоммерческие программы, но зачастую многим пользователям достаточно уже встроенных в Windows инструментов.

4.1.1. ВСТРОЕННЫЙ В WINDOWS 7 РОДИТЕЛЬСКИЙ КОНТРОЛЬ

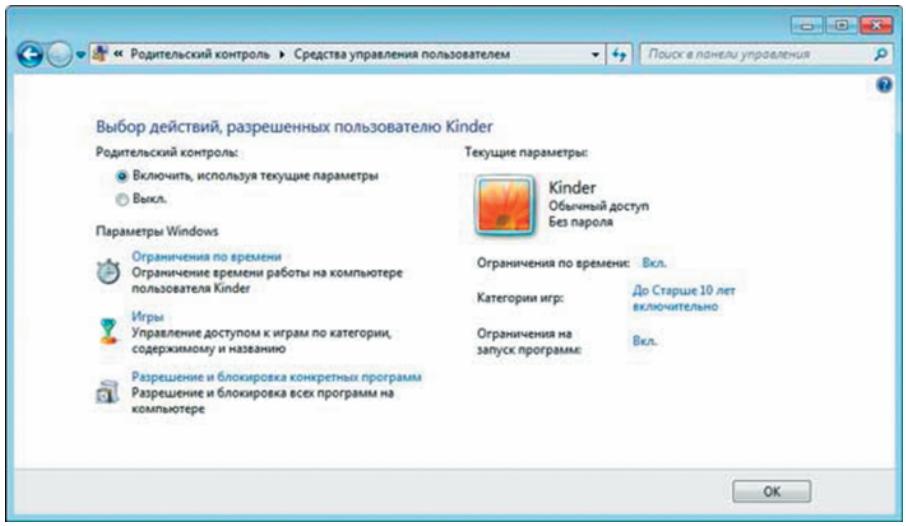
Встроенные средства Windows 7 позволяют вводить некоторые ограничения, касающиеся работы ребенка на компьютере, — устанавливать временной интервал, в течение которого дети могут пользоваться компьютером, а также определять перечень доступных игр и приложений.

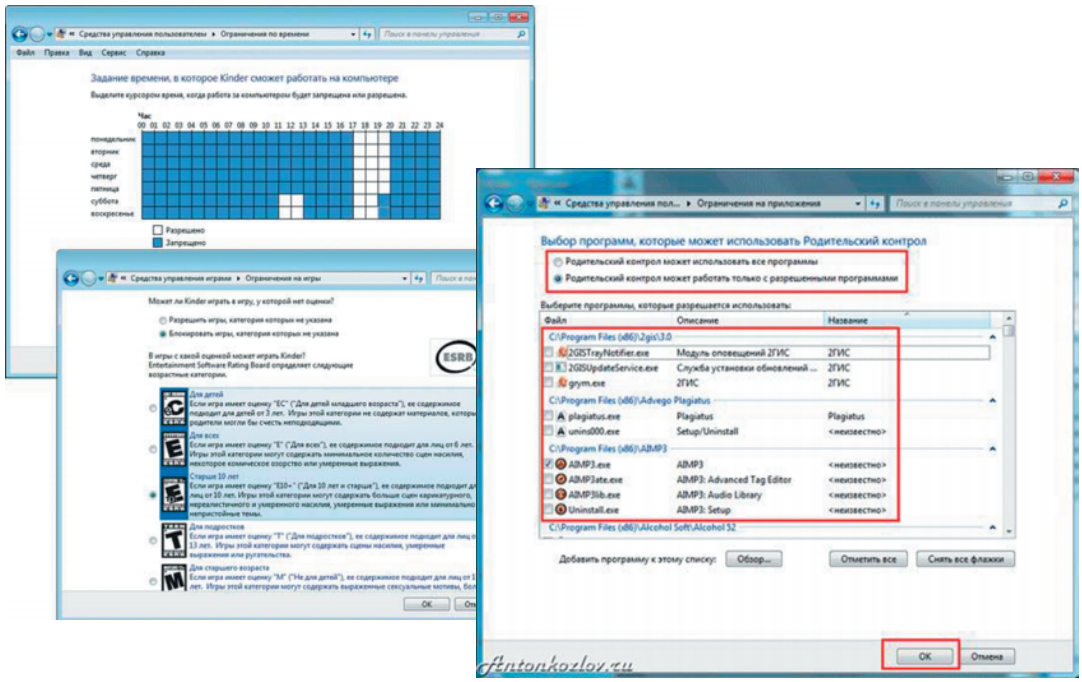


Для настройки родительского контроля встроенными средствами Windows необходимо иметь отдельную учетную запись с правами администратора, а также одну (или более, если детей несколько и требуется разграничение прав) учетную запись обычного пользователя, под которой ребенок будет заходить в систему.

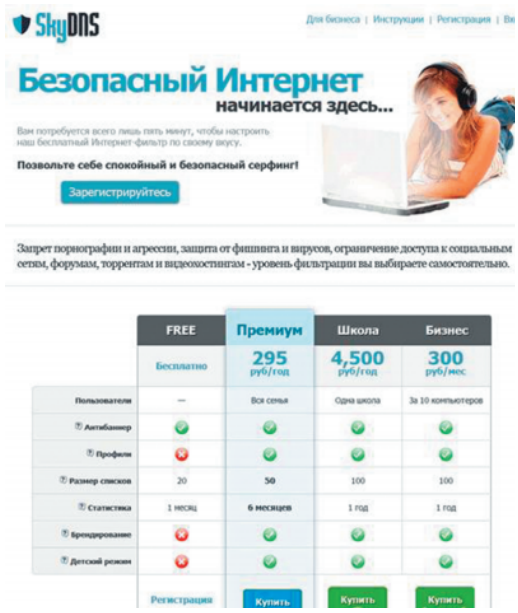
Разумеется, гостевой профиль должен быть отключен, а на профиль администратора установлен пароль — в противном случае ребенок рано или поздно отключит родительский контроль и будет использовать компьютер безо всяких ограничений.

Можно, например, настроить расписание работы по дням недели, что позволит ограничить общее время работы на компьютере, поскольку по окончании разрешенного периода времени будет происходить автоматический выход из системы. Не сложнее окажется отрегулировать доступ к играм, установив на них общий запрет, либо запретив доступ только к отдельным установленным на компьютере играм, указав их вручную либо путем выбора возрастной категории.





4.1.2. ДРУГИЕ ПРОГРАММЫ ДЛЯ РОДИТЕЛЬСКОГО КОНТРОЛЯ



Более продвинутые программы во многом имеют похожие функции с разными названиями. В них несложно разобраться за несколько минут, и почти в каждой из них на вопрос как установить родительский контроль отвечает пошаговый мастер настроек — он запускается при первом использовании программы.

В декабре 2012 года порталом Anti-Malware.ru было проведено тестирование модулей Родительского контроля в ведущих программных решениях производителей по обеспечению безопасной работы в сети Интернет. В результате тестов были определены 4 программных продукта, которые наиболее эффективно ограничивают просмотр детьми нежелательного контента — KinderGateParental Control 1.5, KasperskyInternetSecurity 2013, ContentKeeperExpress и AviraInternet Security.

1. Проект **SkyDNS** (www.skydns.ru) — это не программа, а целый щит, ограждающий ваш компьютер от потенциально опасных сайтов.

Сайт сервиса: https://www.skydns.ru/.
Работа под управлением: Windows, Mac OS X, Linux
Цена: «Премиум» — 295 руб. в год; «Школа» — 4500 руб. в год; «Бизнес» — 300 руб. в месяц.

Зарегистрировавшись на сайте проекта, вы получаете гораздо более безопасный серфинг интернета. Проект заносит в свой черный список сайты с сомнительным содержимым, предоставляя свободный доступ к остальным, «правильным» ресурсам. Определение блокируемых категорий через сервис SkyDNS:

2. Среди классических вариантов родительского контроля последнее время наибольшей популярностью на компьютерах российских пользователей пользуется продукт, поставляемый в составе продуктов Лаборатории Касперского — **KasperskyCrystal** и **KasperskyInternetSecurity**. Отдельно установить «Касперский родительский контроль», к сожалению, не получится.

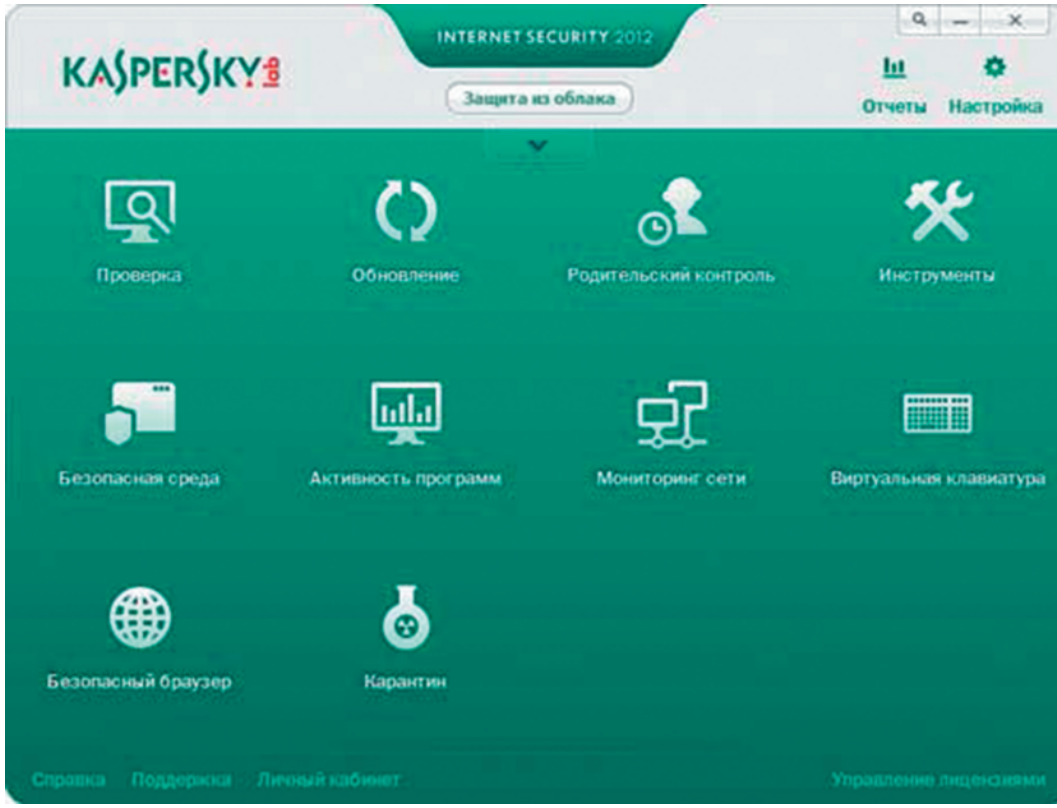
Сайт программы: http://www.kaspersky.ru/kaspersky_internet_security

Размер дистрибутива: 149 Мбайт

Работа под управлением: Windows XP/Vista/7

Цена: лицензия на два компьютера сроком на 1 год — 1600 руб.

KasperskyInternetSecurity 2012 — ориентированный на домашних пользователей инструмент для многоуровневой защиты от всех интернет-угроз: вирусов, хакерских атак и спама.



Входящий в состав продукта модуль «Родительский контроль» позволяет регулировать доступ детей к веб-сайтам и их общение в социальных сетях («ВКонтакте», «Одноклассники», Facebook, Twitter и др.) и через программы обмена сообщениями (ICQ и др.), а также ограничивать время доступа к компьютеру и отдельным приложениям.

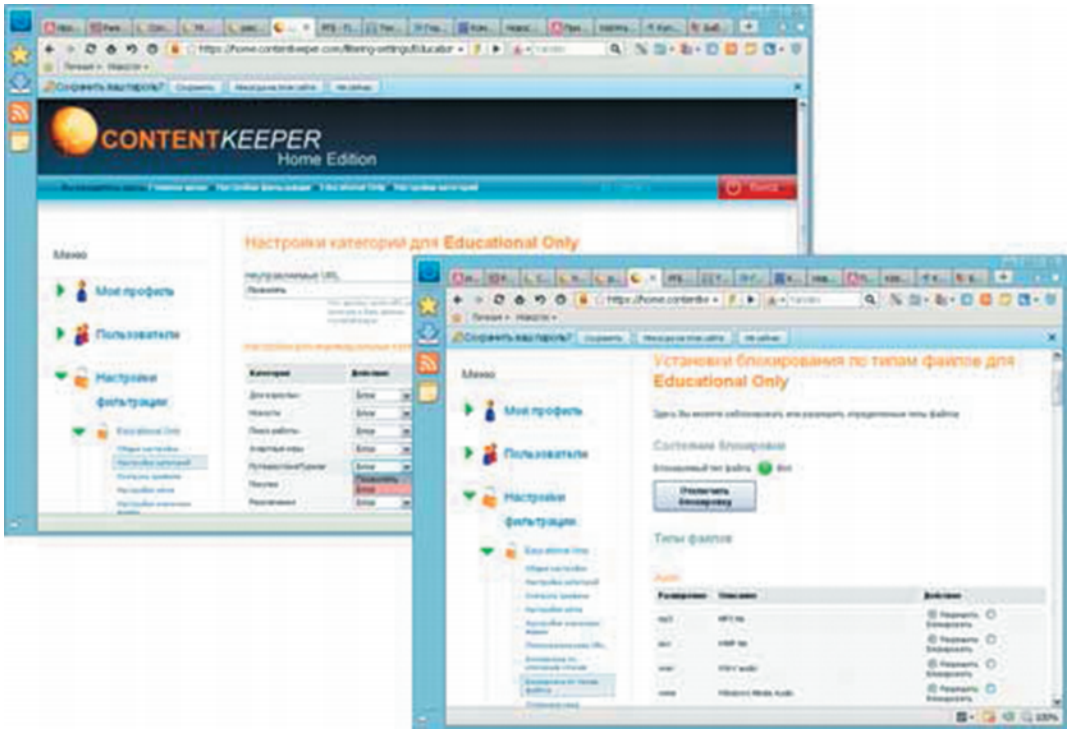
3. **ContentKeeperHome** — «облачная» система фильтрации веб-контента, которая ориентирована на домашних пользователей.

Сайт сервиса: https://home.contentkeeper.com/

Работа под управлением:Windows 2000/XP/Server 2003/Server 2008/Vista/7

Цена: 29,95 долл.

Система обеспечивает очень высокое качество фильтрации при минимальной нагрузке на ресурсы компьютера, что является результатом применения технологии SaaS (Softwareasa Service).Система фильтрации ContentKeeperHome предлагается на коммерческой основе, для ознакомления доступна бесплатная лицензия сроком на один месяц. Данное решение позволяет родителям легко отслеживать, управлять, контролировать и обеспечивать безопасность работы в Интернете для всех членов семьи. Контроль осуществляется путем блокирования доступа к неподходящему или вредному контенту и ресурсам.



4. **TimeBoss** — простая и удобная программа для организации родительского контроля. С ее помощью родители легко могут ограничивать время компьютерной деятельности ребенка (в том числе в играх и Интернете), определять перечень доступных приложений (включая игры), вводить ограничения на ряд системных операций, запрещать доступ к отдельным папкам, а также регулировать посещение сайтов при интернет-серфинге.

Разработчик: NicekitSoftware

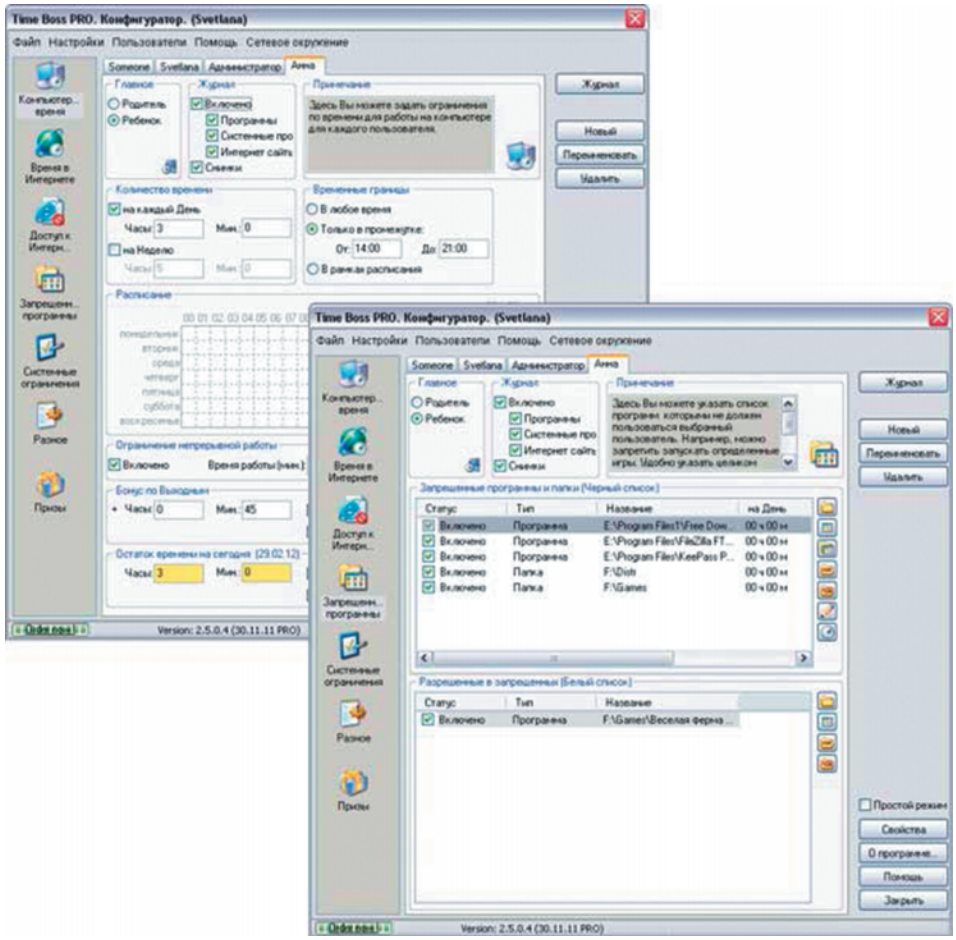
Сайт программы: http://nicekit.ru/parental-control/time-boss.php

Размер дистрибутива: 1,8 Мбайт

Работа под управлением: Windows XP/Vista/7

Цена: Time Boss — 600 руб.; Time Boss PRO — 800 руб.

Программа обеспечивает контроль для всех зарегистрированных в системе пользователей и потому при необходимости может быть использована для настройки разных вариантов ограничений по различным профилям.



5. Программа **«KinderGate Родительский Контроль»** — инструмент для организации контроля доступа детей в Интернет, рассчитанный на домашних пользователей и образовательные учреждения.

Разработчик: EntensysCorporation

Сайт программы: http://www.kindergate.ru/

Размер дистрибутива: 33,7 Мбайт

Работа под управлением: Windows XP/Vista/7

Цена: подписка на два месяца — 100 руб.; подписка на год — 490 руб.

Решение включает функционал для мониторинга действий ребенка в Сети: отслеживание посещаемых ресурсов при серфинге, мониторинг сообщений в сетевых мессенджерах (поддерживаются протоколы ICQ, Jabber, MSN, Mail.ru, YMSG) и наблюдение за перепиской ребенка в социальных сетях «ВКонтакте», «Одноклассники» и Facebook.

В дополнение можно посмотреть и другие программные продукты: КиберМама, KidsControl, SpectorPro, ParentalControlBar.

!!! Помните: ни одно программное обеспечение не идеально.

4.2. ОБУЧЕНИЕ ДЕТЕЙ ОСНОВАМ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ИНТЕРНЕТОМ

Скачать родительский контроль, установить и настроить его недостаточно: ни одна лучшая программа родительского контроля не даст гарантий от опасности. **В дополнение к программам нужен и визуальный доступ к компьютеру.** Возможно, лучший метод родительского контроля в том, чтобы совместно обсудить опасности сомнительных сайтов? В дружеской и равноправной беседе родителей с детьми можно достичь согласия и понимания гораздо проще и результативнее, чем используя отключаемые программы и другие электронные методы. Запретный плод сладок.

!!! Станьте друзьями для своих детей: старшими, мудрыми и опытными, с которыми хочется поговорить на любую тему с удовольствием. Это и есть самый лучший метод родительского контроля, который принесет множество позитива в общение с детьми.

1. Научите детей никому не сообщать пароли.

Согласно исследованиям 75 процентов детей в возрасте от 8 до 9 лет сообщают свои пароли другим лицам.

Правила, которые дети должны знать и соблюдать:

- ***Никогда не сообщать свои пароли другим,*** даже друзьям.
- ***Обеспечить защиту для записанных паролей.*** Будьте внимательны к тому, где вы храните или записываете пароли.
- ***Никогда не предоставлять свой пароль по электронной почте или в ответ на запрос по электронной почте.***

• ***Не вводить пароли на компьютерах, которые вы не контролируете.*** Не пользуйтесь общедоступными компьютерами в школе, библиотеке, в интернет-кафе или в компьютерных лабораториях, кроме как для анонимного просмотра страниц в Интернете. Не используйте эти компьютеры с учетными записями, где требуется вводить имя пользователя и пароль.

2. Помощь детям в безопасном использовании социальных сетей.

• ***Беседуйте с детьми по поводу их общения в социальных сетях.*** Просите детей рассказывать вам, если им встретится в Интернете то, что вызывает у них беспокойство, неудобство или страх.

• ***Определите правила работы в Интернете.*** Как только ваши дети станут самостоятельно пользоваться Интернетом, установите правила пользования Интернетом. В этих правилах должно быть определено, могут ли ваши дети использовать сайты социальных сетей и каким образом.

• ***Убедитесь в том, что ваши дети соблюдают возрастные ограничения.*** Рекомендуемый возраст для регистрации на сайтах социальных сетей обычно составляет 13 и более лет.

• ***Учитесь.*** Оцените сайты, которые планирует использовать ваш ребенок, и убедитесь, что вы и ваш ребенок понимают политику конфиденциальности и правила поведения. Узнайте, существует ли на сайте контроль над публикуемым содержимым. Кроме того, периодически просматривайте страницу вашего ребенка.

• ***Научите своих детей никогда лично не встречаться с теми, с кем они общались только по сети.*** Дети подвергаются реальной опасности во время личной встречи с незнакомыми людьми, с которыми они общались только по сети.

• ***Попросите детей общаться только с теми людьми, которых они уже знают.*** Вы можете помочь защитить ваших детей, попросив их использовать данные сайты для общения с друзьями и никогда не общаться с теми, с кем они лично не встречались.

• ***Убедитесь в том, что ваши дети не указывают свои полные имена.*** Научите своего ребенка указывать только свое имя или псевдоним и ни в коем случае не использовать псевдонимы, которые могли бы привлечь нежелательное внимание.

• ***Относитесь с осторожностью к идентифицирующей информации в профиле вашего ребенка.*** На многих сайтах социальных сетей дети могут присоединяться к общественным группам, включающих учеников определенной школы.

• ***Постарайтесь выбрать сайт, который не столь широко используется.*** Некоторые сайты позволяют защитить вашу страницу с помощью пароля или другими способами, чтобы ограничить круг посетителей, разрешив его только тем лицам, которых знает ваш ребенок.

• ***Следите за деталями на фотографиях.*** Объясните детям, что фотографии могут раскрывать много личной информации. Попросите детей не публиковать фотографии себя или своих друзей, на которых имеются четко идентифицируемые данные, такие как названия улиц, государственные номера автомобилей или название школы на одежде.

• ***Предостерегите своего ребенка относительно выражения своих эмоций перед незнакомцами.*** Объясните детям, что написанное ими сможет прочесть любой, кто имеет доступ в Интернет, и похитители часто ищут эмоционально уязвимых детей.

• ***Расскажите детям об интернет-угрозах.*** Как только ваши дети станут достаточно взрослыми для использования сайтов социальных сетей, расскажите им о кибер-угрозах. Расскажите детям, что если у них возникнет ощущение, что им угрожают через Интернет, то им сразу же следует сообщить об этом родителям, учителю или другому взрослому человеку, которому они доверяют.

• ***Удаление страницы вашего ребенка.*** Если ваши дети отказываются соблюдать установленные вами правила для защиты их безопасности, и вы безуспешно пытались помочь им изменить свое поведение, можно обратиться на веб-сайт социальной сети, которую использует ваш ребенок, с просьбой удалить его страницу.

3. Если ваши дети пишут блоги, убедитесь в том, что они не рассказывают слишком много о себе.

Практика написания блогов (сокращение от англ. «weblog» — дневник в сети) или личного интерактивного журнала очень быстро стала популярной среди подростков, многие из которых ведут свои блоги без ведома родителей или опекунов. Недавние исследования показали, что на сегодняшний день примерно половину всех блогов пишут подростки, при этом каждые двое из троих указывают свой возраст, каждые трое из пяти сообщают о месте своего проживания и дают контактную информацию, а каждый пятый указывает свое полное имя. Разглашение подробной личной информации сопряжено с риском.

4. Помните об интернет-мошенниках.

Согласно данным Федеральной торговой комиссии США, 31 процент жертв похищения личных данных составляют молодежь. Подростки становятся привлекательными объектами для мошенников, поскольку у них хорошие кредитные оценки и малый долг, по сравнению со взрослыми они меньше заботятся о безопасном хранении информации.

• ***Никогда не разглашайте личную информацию.***

• ***Обязательно завершайте сеанс с выходом из системы при работе на общедоступном компьютере.*** Если вы используете компьютер в библиотеке или в интернет-кафе, прежде чем покинуть компьютер, полностью завершите все сеансы с выходом из системы.

• ***Придумывайте безопасные пароли и держите их в секрете.***

• ***Используйте только безопасные сайты.*** Если ваши дети совершают покупки в Ин-тернете, то им следует каждый раз убеждаться в том, что URL-адрес сайта, на котором они вводят финансовую информацию, начинается с префикса https://, в правом нижнем углу имеется желтый значок замка или адресная строка отображается зеленым цветом. Они могут щелкнуть по значку замка или в адресной строке, чтобы проверить сертификат безопасности данного сайта.

• ***Распознавание мошенников и сообщение о фактах мошенничества.*** Расскажите своим детям о признаках подделки идентификационных данных: предложение утвержденных кредитных карт, звонки из агентств по сбору информации или незнакомые финансовые документы. Если у вашего ребенка возникнет подозрение на подделку личных данных, немедленно предпримите соответствующие действия, чтобы ограничить ущерб. Обратитесь в свою кредитную компанию, банки или все три организации по кредитной отчетности, а также в полицию. Закройте все счета, которые подвергались фальсификации, и попросите детей поменять пароли для всех своих учетных записей в Интернете. Ведите журнал всех выполняемых действий.