Следственное управление
Следственного комитета Российской
Федерации по Мурманской области

Уполномоченный по правам ребенка
в Мурманской области

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Практическое руководство для родителей

Мурманск
2016

Уважаемые родители!

В наш стремительно развивающийся информационный век главным помощником не только для взрослых, но и для детей становится Интернет. Здесь можно найти нужную информацию, общаться, играть, читать книги. Но не следует думать, что Интернет – это всего лишь виртуальный ресурс и мощный помощник вашим детям для школы и получения знаний. В силу возраста и отсутствия жизненного опыта они могут столкнуться с реальной угрозой. Интернет – бесконтрольное и ничем не ограниченное средство передачи информации. Негативное влияние на психику вашего ребенка могут оказать порнографические сайты, бесплатные веб-страницы, пропагандирующие насилие и праворадикальные идеи. Опасность таится также в популярных социальных сетях, ведь по другую сторону монитора сидят люди, а не персонажи компьютерных игр. Нередко преступники находят контакт с детьми, напрашиваются к ним в виртуальные друзья, назначают встречи, совращают, склоняют к свершению суицида, затягивают в секты и т. д.

Наша памятка создана, в первую очередь, для родителей, которые смогут уберечь своих детей от негативных последствий и предотвратить совершение преступлений.

При подготовке брошюры были использованы материалы памятки для родителей «Безопасный Интернет», разработанной по инициативе Уполномоченного по правам ребенка в Ненецком автономном округе, и практического пособия «Как сделать Интернет безопасным для вашего ребенка», разработанного по инициативе Уполномоченного по правам ребенка в Санкт-Петербурге.

Опасности, с которыми могут столкнуться дети в сети Интернет

Явные опасности

Порнография, пропаганда насилия, экстремизм, агрессия, кибербуллинг (нападения с целью нанесения психологического вреда через электронную почту, в социальных сетях и т. д.), кидднеппинг (противоправные умышленные действия, направленные на тайный или открытый, либо с помощью обмана захват человека с последующим удержанием помимо его воли в другом месте; как правило совершается с целью получения выкупа от родственников или близких к похищенному лиц, а также принуждения этих лиц к выполнению необходимых для похитителей действий). Социальные сети, форумы, чаты – все это позволяет свободно вливать в детские умы подобную информацию, нанося непоправимый ущерб психике.

Опасные молодежные течения

Подросший ребенок, как правило, общается в сфере его возрастной группы, которая часто так и называется – сложный возраст. Сайты всевозможных фанатов, социальные сети, объединяющие людей с неуравновешенной психикой в разного рода группы депрессивных течений и группы суицидальной направленности, толкают порой детей к суициду (буллициду). Также опасение вызывает тот факт, что ряд экстремистских групп используют Интернет для распространения своих идей, пропаганды насилия в отношении национальных меньшинств и иммигрантов.

Секты

Следите за тем, с кем и на каких сайтах общается ребенок в Сети. Проверяйте сообщества, форумы, чаты и сразу блокируйте подозрительные из них. Сектанты-вербовщики всегда принимают облик друзей и обещают что-то хорошее. Не позволяйте встречаться с незнакомыми виртуальными собеседниками.

Вирусы, трояны, обманщики

Помимо опасностей человеческих, есть еще опасности чисто технические. Заблудившись в Сети, очень легко заразить компьютер вредоносными программами, которые могут добавить вам головной боли: кража паролей и прочей конфиденциальной информации, спам от вашего имени, хулиганство, вымогательство, угрозы – все это может быть плодами вирусов.

Правила медиабезопасности

Правило № 1

Как можно больше общайтесь со своим ребенком, чтобы избежать возникновения интернет-зависимости. Приобщайте ребенка к культуре и спорту, чтобы он не стремился заполнить свободное время компьютерными играми. Запомните! Не существует детей, которых бы не интересовало ничего, кроме компьютера. Помните, «ребенку для полного и гармоничного развития его личности необходимо расти в семейном окружении, в атмосфере счастья, любви и понимания».

Правило № 2

Прежде чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети (вредоносные программы, небезопасные сайты, интернет-мошенники и др.) и их последствиях.

Правило № 3

Существуют определенные механизмы контроля пользования Интернетом, например, совместное с ребенком пользование Интернетом или установка специальных систем фильтрации данных, самостоятельно закрывающих доступ к определенной информации. Критерии фильтрации при этом задает взрослый, что позволяет устанавливать определенное расписание пользования Интернетом.

Правило № 4

Возможные соцсети, которые могут посещать ваши дети, – это ВКонтакте, Одноклассники, Facebook, Фотострана, MySpace. Также обратите внимание на ресурс «Мой Мир» на почтовом сайте Mail. Станьте «другом» вашего ребенка в соцсетях. Это поможет вам контролировать виртуальные отношения ребенка с новыми «знакомыми» и «друзьями».

Правило № 5

Научите детей не оставлять в публичном доступе личную информацию: контакты, фото, видео. Запомните принцип Интернета: «Все, что вы выложили, может быть использовано против вас». Желательно оставлять только электронные способы связи. Например, специально выделенный для подобного общения e-mail или номер icq.

Правило № 6

Контролируйте время, которое ваш ребенок проводит в Интернете. Длительное времяпрепровождение в Сети может быть связано с «заигрываниями» со стороны педофилов, особенно в блогах, социальных сетях.

Правило № 7

Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием.

Правило № 8

Несмотря на моральный аспект, периодически читайте электронную почту ребенка, если вы видите, что после прочтения почты ваш ребенок расстроен, растерян, запуган.

Правило № 9

Главное средство защиты от мошенника, педофила – ребенок должен твердо усвоить, что виртуальные знакомые должны оставаться виртуальными. То есть – никаких встреч в реальном мире с теми друзьями, которых он обрел в Интернете. По крайней мере, без родительского присмотра.

Правило № 10

Средство защиты от оскорблений в Сети – игнорирование пользователя. Объясните ребенку, как пользоваться настройками приватности; как блокировать нежелательного «гостя»: добавить пользователя в «черный список», пожаловаться модератору сайта.

Практические рекомендации по установке защиты от вредоносной информации для наиболее используемых устройств и операционных систем

- **Не пугайтесь большого объема текста, вы можете использовать только один из описанных ниже способов защиты – это в любом случае гораздо лучше, чем ничего.**
- **Настройки каждого способа защиты мы приводим для наиболее используемых устройств и операционных систем (это тоже пугающе увеличивает объем брошюры).**
- **Каждый из приведенных ниже способов может работать как самостоятельно, так и в сочетании с другими.**
- **Использование сочетания нескольких способов защиты повышает эффективность.**

Мы расскажем, как защитить ребенка от вредной информации в компьютере и Интернете с помощью:

- ✓ **DNS-сервиса,**
- ✓ **операционной системы компьютера,**
- ✓ **настроек поисковых систем,**
- ✓ **настроек браузера,**
- ✓ **провайдера и операторов сотовой связи,**
- ✓ **специального программного обеспечения.**

Помните, что нет способов защиты со стопроцентной гарантией, и никакие технические средства не заменят ваших доверительных отношений с ребенком. Взаимопонимание, искренность и готовность поделиться тревожными мыслями – самая универсальная «подушка безопасности», которая сбережет вашу семью от всех невзгод.

Защита с помощью DNS-сервиса

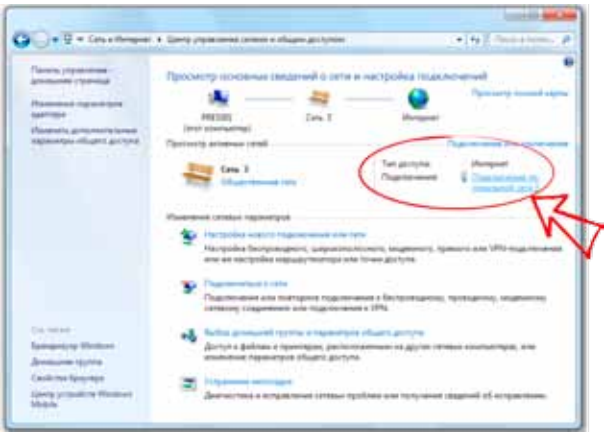
Эффективная система, которая отсекает компьютер (ноутбук, планшет, смартфон) от зараженных и мошеннических сайтов, эротического и порнографического контента на страницах.

От вас требуется только изменить два набора цифр в определенном месте настроек компьютера.

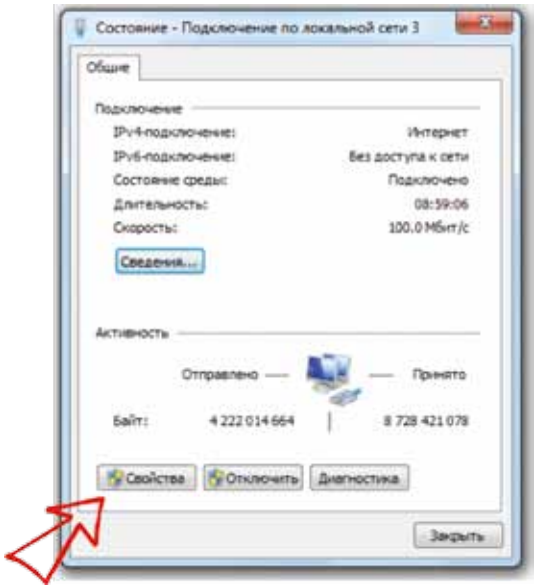
> DNS – это адресная книга Интернета, где указан цифровой адрес каждого сайта. Сервисы безопасных DNS попросту не пускают компьютер на опасные ресурсы. Например, когда вы пытаетесь зайти на зараженный сайт, на экран выводится сообщение, что затребованная страница блокирована по такой-то причине. Сервисов DNS немало, среди них есть и бесплатные, например, Яндекс.DNS, Norton DNS, MetaCert DNS (более подробную информацию вы можете прочитать на сайтах производителей).

DNS-сервис на компьютере с Windows 7 или Vista

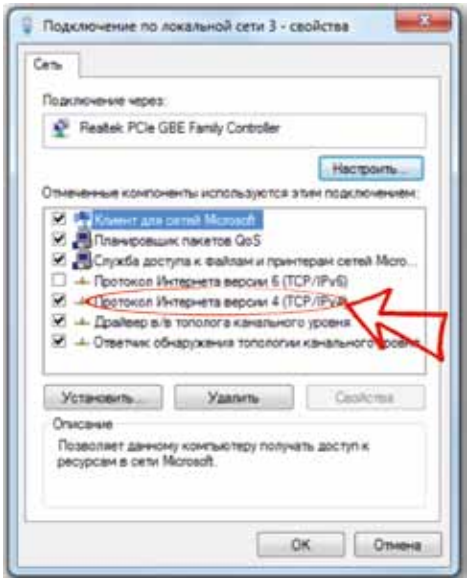
1. Откройте **Меню «Пуск»** и выберите **Панель управления.**
2. В разделе **Сеть и Интернет** откройте **Просмотр состояния сети и задач.**
3. В разделе **Просмотр активных сетей** нажмите напротив пункта **Подключения** ссылку **Беспроводное сетевое соединение** или **Подключение по локальной сети.**



4. Откройте меню **Свойства.**

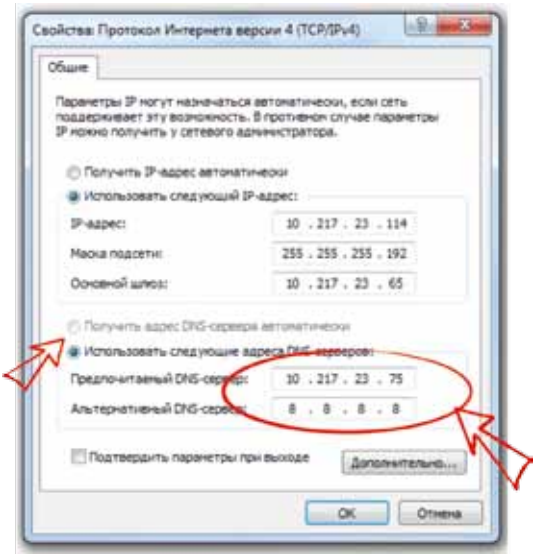


5. Выберете пункт **Протокол Интернета версии 4 (TCP/IPv4)** и нажмите на кнопку **Свойства**.



6. Во вкладке **Общие** выберите пункт **Использовать следующие адреса DNS-серверов**.

7. Введите адреса выбранного вами режима DNS-сервиса (см. стр. 6) в поля **Предпочитаемый DNS-сервер** и **Альтернативный DNS-сервер** и сохраните изменения.



Безопасные адреса DNS-серверов

Эти цифры нужно ввести в настройки вашего сетевого соединения.

Яндекс.DNS:

Безопасный – без мошеннических сайтов и вирусов:

DNS1: 77.88.8.2
DNS2: 77.88.8.88

Семейный – без мошеннических сайтов и вирусов, без сайтов для взрослых:

DNS1: 77.88.8.3
DNS2: 77.88.8.7

Norton DNS:

С блокировкой вредоносных сайтов:

DNS1: 199.85.126.10
DNS2: 199.85.127.10

С блокировкой вредоносных сайтов, сайтов для взрослых:

DNS1: 199.85.126.20
DNS2: 199.85.127.20

С блокировкой вредоносных сайтов, сайтов для взрослых, сайтов, распространяющих файлы:

DNS1: 199.85.126.30
DNS2: 199.85.127.30

MetaCert DNS:

С блокировкой взрослых сайтов, без ограничения доступа к остальным ресурсам в Интернете:

DNS: 184.169.223.35

DNS-сервис на компьютере с Windows XP

1. Откройте **Меню «Пуск»** и выберите **Панель управления.**
2. Откройте **Сетевые подключения.**
3. Выберите используемый вами тип сетевого подключения (проводное или беспроводное).
4. Откройте меню **Свойства.**
5. Выберите пункт **Протокол Интернета (TCP/IP)** и нажмите на кнопку **Свойства.**
6. Выберите пункт **Использовать следующие адреса DNS-серверов.**
7. Введите адреса выбранного вами режима DNS-сервиса (см. стр. 6) в поля **Предпочитаемый DNS-сервер** и **Альтернативный DNS-сервер** и сохраните изменения.

DNS-сервис на компьютере с MacOX X

1. Откройте **Системные настройки** – **Сеть.**
2. Выберите сеть, для которой вы хотите настроить DNS-сервиса, и нажмите на кнопку **Дополнительно.**
3. Перейдите на вкладку **DNS.**
4. Нажмите на «+» под списком **DNS-серверы.**
5. Введите адреса выбранного вами режима DNS-сервиса (см. стр. 6) в поле и нажмите **OK.**
6. Нажмите кнопку **Применить,** чтобы сохранить изменения.

DNS-сервис на компьютере с Windows 8

1. Откройте панель **Charms bar,** наведя мышку в правую часть экрана, и выберите **Параметры.**
2. Выберите **Панель управления.**
3. Откройте **Просмотр состояния сети и задач.**
4. Выберите **Изменение параметров адаптера.**
5. Выберите используемый вами тип подключения (проводное или беспроводное).
6. Откройте меню **Свойства.**
7. Выберите пункт **Протокол Интернета версии 4 (TCP/IPv4)** и нажмите на кнопку **Свойства.**

8. Выберите пункт **Использовать следующие адреса DNS-серверов.**
9. Введите адреса выбранного вами режима DNS-сервиса (см. стр. 6) в поля **Предпочитаемый DNS-сервер** и **Альтернативный DNS-сервер** и сохраните изменения.

DNS-сервис на компьютере с Linux (Ubuntu)

1. Щелкните на значке сетевого подключения в верхней панели.
2. Выберите **Изменить соединения.**
3. Выберите сеть, для которой вы хотите настроить DNS-сервис, и нажмите **Изменить.**
4. Перейдите на вкладку **Параметры IPv4.**
5. В пункте **Способ настройки** выберите **Автоматически (DHCP, только адрес).**
6. Введите адреса выбранного вами режима DNS-сервиса (см. стр. 6) в поле **Серверы DNS** и сохраните изменения.

Защита с помощью операционной системы

Операционная система – это комплекс программ, назначением которого является обеспечение взаимодействия пользователя с компьютером.

Говоря проще – это самая главная программа, контролирующая все устройство (компьютер, смартфон, планшет, ноутбук и т. д.) и помогающая вам им пользоваться.

Наиболее известные из них для стационарных компьютеров и ноутбуков: Windows, Linux, MacOS.

В планшетах и смартфонах, помимо мобильных версий уже названных ОС (Windows и Mac) Windows Phone и iOS, добавляется Android.

Все они имеют функции «Родительский контроль», включение которых обеспечивает наиболее комплексную защиту вашего ребенка от вредной информации.

В отличие от **DNS-сервиса** эти настройки будут блокировать ненужный контент не только в Интернете, но и в самом компьютере (планшете, смартфоне).

Включенный в операционной системе «Родительский контроль» позволяет, например, установить ограничение времени, проводимого ребенком за компьютером, ввести запрет на доступ детей к отдельным играм и на использование определенных программ. Также с его помощью можно ограничить круг общения ребенка (например, разрешить переписку в Mail и «говорилках» лишь с определенными пользователями) или закрыть доступ к указанным веб-сайтам.

MacOS X

На компьютерах Mac и ноутбуках MacBook уже предусмотрено стандартное средство – **Родительский контроль,** которое позволяет настроить компьютер так, чтобы дети использовали его не во вред.

Настроить параметры использования компьютера можно через меню **Системные настройки** в меню **Родительский контроль.**

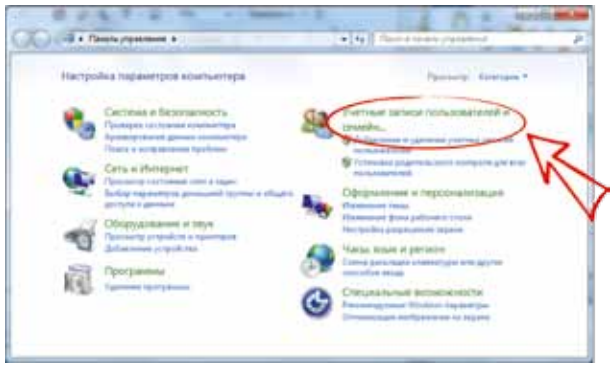
- **Программы** – ограничение доступа к приложениям, например, к играм с большим количеством насилия.
- **Веб** – ограничение на доступ к некоторым интернет-ресурсам.
- **Пользователи** – ограничение круга общения ребенка (например, разрешить переписку в Mail и «Сообщениях» лишь с определенными пользователями).
- **Время** – можно задать временные интервалы для использования компьютера.
- **Другие** – ограничение доступа детей к аппаратным возможностям Mac, таким как встроенная камера, принтеры и привод оптических дисков.

Windows 7

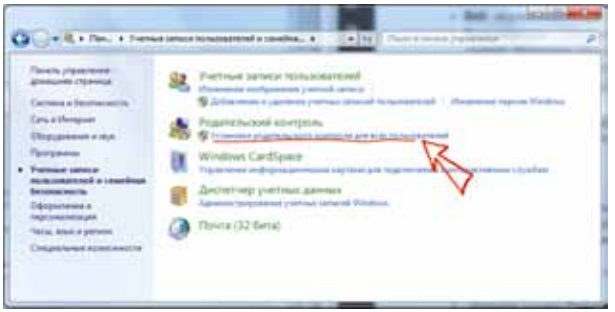
Для настройки ограничения доступа на компьютере с ОС Windows 7 требуется создать для ребенка отдельный аккаунт без администраторских прав (**Панель управления** → **Учетные записи пользователей**).

Включение родительского контроля для учетной записи обычного пользователя:

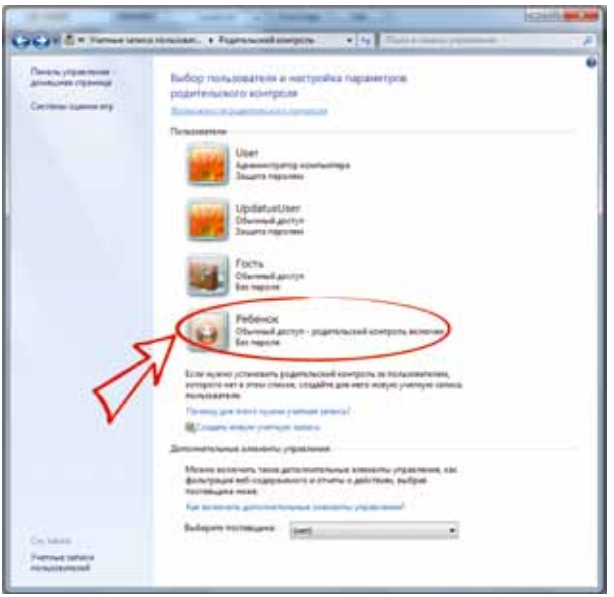
1. Зайдите в раздел **Учетные записи пользователей и семейная безопасность (Пуск** → **Панель управления)**.



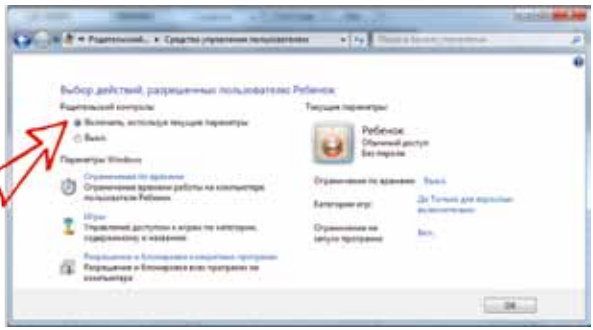
2. В разделе **Учетные записи пользователей и семейная безопасность** щелкните **Установить родительский контроль для всех пользователей.**



3. Выберите учетную запись обычного пользователя, для которой следует включить родительский контроль. Это делается кликом на иконке учетной записи (например, **Ребенок**), после чего вы попадете в окно настроек ограничений. (Если учетная запись обычного пользователя еще не настроена, выберите параметр **Создать новую учетную запись**).



4. Выберите пункт **Включить, используя текущие параметры.** Настройте параметры предлагаемых ограничений**.**



Если в процессе включения родительского контроля операционная система будет предлагать совершить еще какие-то действия (не указанные в этом порядке), следуйте ее подсказкам. Например, если на вашей учетной записи (с правом администратора) не установлен пароль, то ОС предложит это сделать, чтобы ребенок не смог в нее войти и поменять настройки своей учетной записи.

После включения родительского контроля для учетной записи обычного пользователя, которая назначена ребенку, можно настроить отдельные параметры контроля. В Windows 7 можно установить: ограничение времени, проводимого ребенком за компьютером, запрет на доступ детей к отдельным играм, запрет на использование определенных программ.

Средства родительского контроля Windows 7 можно существенно расширить, установив компонент **Семейная безопасность** из набора **Windows Live**. В этом случае открываются дополнительные возможности: веб-фильтр, создание отчетов о действиях, запросы на разрешение. Подключить компонент можно на вкладке **Родительский контроль.**

Windows Vista

Чтобы включить родительский контроль для стандартной учетной записи пользователя:

1. В разделе **Учетные записи** пользователей выберите **Задание родительских элементов управления.** Введите пароль администратора или подтверждение пароля, если появится соответствующий запрос.
2. Выберите стандартную учетную запись, для которой следует включить родительский контроль.
3. В группе **Родительский контроль** выберите **Вкл.**

После включения для учетной записи ребенка родительского контроля можно настроить индивидуальные параметры контроля. В Windows Vista можно установить ограничение времени, проводимого ребенком за компьютером, установить запрет на доступ детей к отдельным играм и на использование определенных программ.

Windows 8

Для настройки ограничения доступа на компьютере с ОС Windows 8 требуется создать для ребенка отдельный аккаунт без администраторских прав **(Панель управления → Учетные записи пользователей).**

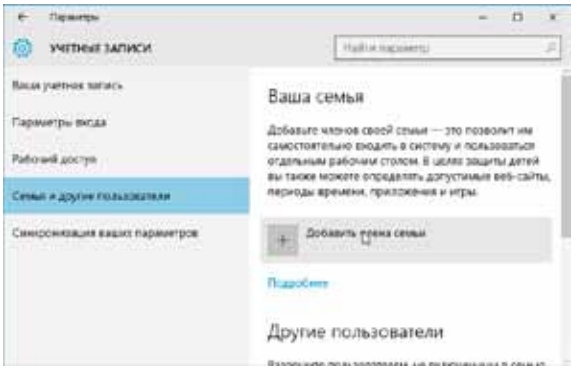
Включение родительского контроля для учетной записи обычного пользователя:

1. В окне **Учетные записи пользователей** перейти по ссылке **Семейная безопасность** на левой панели внизу.
2. В открывшемся окне выбрать учетную запись, для которой требуется изменить параметры семейной безопасности.
3. В нижней части окна вы увидите список доступных функций семейной безопасности. В настройках вы можете указать:
   - какие сайты может просматривать ребенок, установив уровень ограничения в зависимости от категории и типа содержимого сайтов (в разделе **Веб-фильтр**);
   - установить лимит времени пользования компьютером или определить, в какой промежуток времени ребенок может пользоваться компьютером (раздел **Ограничение времени**);
   - выбрать приложения, которые ребенку позволено запускать (раздел **Ограничение приложений**);
   - определить список игр, которые может скачивать и открывать ребенок (раздел **Ограничения для игр**).

Если в процессе настройки службы семейной безопасности операционная система будет предлагать совершить еще какие-то действия (не указанные в этом порядке), следуйте ее подсказкам. Например, если на вашей учетной записи (с правом администратора) не установлен пароль, то ОС предложит это сделать, чтобы ребенок не смог в нее войти и поменять настройки своей учетной записи.

Windows 10

1. Чтобы включить родительский контроль в Windows 10, перейдите из меню **Пуск** в раздел **Учетные записи пользователей.** В категории **Семья и другие пользователи** нажмите **Добавить члена семьи.**

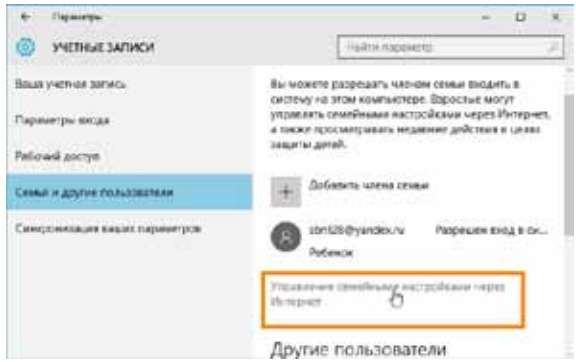


2. Система на выбор предложит создать профиль для ребенка или взрослого. Выбрав соответствующий пункт, введите адрес электронной почты. Подтвердите его, для чего зайдите в папку входящих сообщений электронной почты.

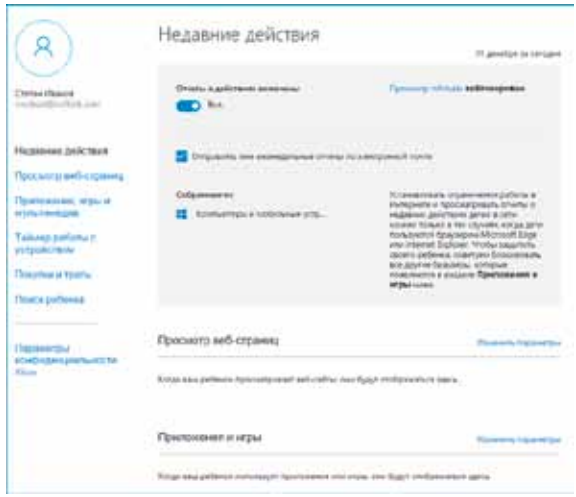
> ОС не позволит активировать родительский контроль для локальной учетной записи. Поэтому создайте новый профиль для каждого юзера, которого предстоит контролировать.

3. Включение функции родительского контроля закончено. Чтобы отключить этот режим, зайдите под именем администратора и выполните соответствующие настройки в разделе **Семья и другие пользователи.** Здесь кликните на учетную запись ребенка и нажмите кнопку **Удалить,** подтвердив выбранное действие, когда это запросит система.

Для выполнения настройки параметров родительского контроля перейдите в раздел **Семья и другие пользователи,** где откройте пункт **Управление семейными настройками через Интернет.**



После этого ОС откроет перед вами новое окно браузера. Здесь выберите пользователя, за которым ведете контроль, и настройте функцию мониторинга.



Навигация на странице осуществляется в левой части, где есть шесть пунктов:

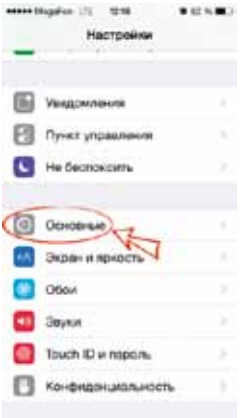
1. **Недавние действия.** Раздел позволит следить за действиями ребенка, адресами просмотренных страниц, а также мониторить общее время нахождения за устройством.
2. **Просмотр веб-страниц.** Здесь вы сможете контролировать просматриваемые ребенком сайты. Открыть или закрыть доступ к интернет-ресурсам на свое усмотрение.

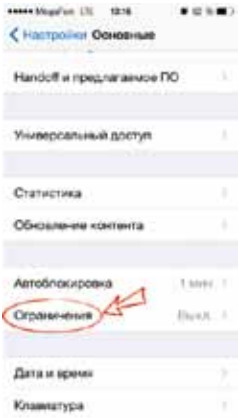
3. **Приложения, игры и мультимедиа.** Можно установить ограничения на скачиваемые в интернет-магазине Windows программы и игры. Оценка возрастной категории в этом случае выполняется автоматически.
4. **Таймер работы с устройством.** Здесь вы сможете указать суммарное время, которое ребенок проведет перед устройством.
5. **Покупки и траты.** Раздел позволит вам следить за тратами, которые делаются в онлайн-магазине Windows. Вы можете зачислить деньги на счет пользователя, не предоставляя данных своей кредитной карты.
6. **Поиск ребенка.** В этом разделе доступен поиск мобильного устройства ребенка, если оно поддерживает функцию определения местоположения, на карте.

Защита с помощью настроек смартфона

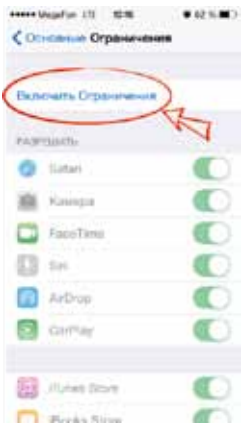
Мобильная операционная система iOS

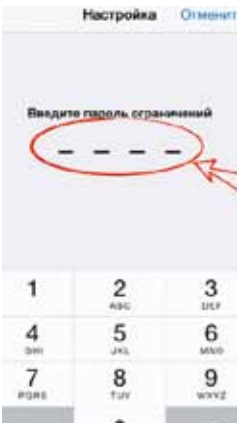
На устройстве iPhone и iPad можно включить функцию **Ограничения.**





1. Перейдите в меню **Настройки** → **Основные.**
2. Выберите пункт **Ограничения.**
3. Выберите пункт **Включить ограничения** и введите пароль.
4. В разделе **Разрешенный контент** в пункте **Возрастной ценз** указать **Россия.**

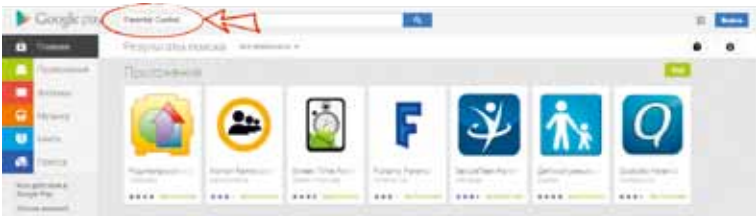




5. Установить возрастные ограничения можно и в отдельных программах.

Google Android

Родительский контроль не предусмотрен, но можно найти более 500 приложений, готовых защитить вашего ребенка – достаточно набрать **Parental Control** в поиске и выбрать по отзывам подходящее.



Microsoft Windows Phone 8

Функция **Nokia Kid's Corner** автоматически блокирует доступ к Интернету и делает невозможным совершение покупок. В настройках функции **Nokia Kid's Corner** можно выбрать контент (музыку, видео или игры) или приложения (камера, плеер и т. д.), которые будут доступны малышу, а также установить ПИН-код для защиты основных функций и информации на телефоне.

Защита с помощью настроек поисковых систем

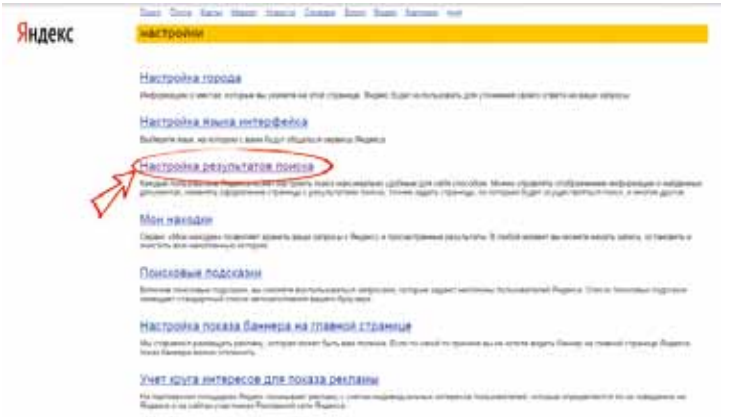
Тут, прежде всего, имеет смысл настроить родительский контроль в системах Яндекс и Google. Это менее глобальный барьер по сравнению с предыдущими, и лучше его использовать в сочетании с другими защитами. Преимущество этого способа в простоте, а недостаток в том, что выбор поисковых систем не ограничивается Яндекс и Google и можно воспользоваться другой, где настройки не установлены. Кроме того, так защищается только поиск.

Семейный поиск Яндекс

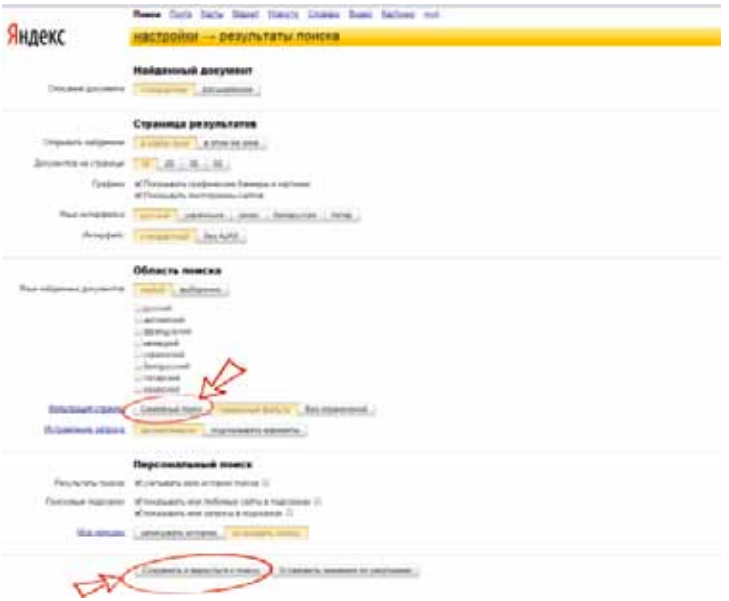
Поисковая система Яндекс позволяет настроить уровень фильтрации: семейный поиск, умеренный фильтр и без ограничений.

1. Перейти по ссылке **Настройка** (Шестеренка), расположенной в верхней части страницы.

2. Выбрать раздел **Настройка результатов поиска.**



3. В разделе **Область поиска** выделить в **Фильтрации страниц** кнопку **Семейный поиск.**
4. Отметить **Сохранить и вернуться к поиску.**



Безопасный поиск Google

Поисковая система Google позволяет не только установить настройки, но и защитить их таким образом, чтобы другие пользователи компьютера не могли их изменить.

1. В разделе **Настройки,** который находится на главной странице внизу, выбрать раздел **Настройки поиска.**

2. Отметить галочкой **Не показывать непристойные результаты.** Чтобы ребенок не мог изменить настройки поиска, можно включить защиту настроек **Безопасного поиска.**

3. Нажать кнопку **Сохранить** внизу страницы.

Защита с помощью настроек браузера

Браузер – этим мудреным словом называется программа, которая позволяет просматривать сайты и которой пользуется каждый, кто выходит в Интернет. Это известные всем пользователям Internet Explorer, Chrome, Opera, Mozilla и т. д.

Ниже приведены особенности и настройки безопасности для основных браузеров.

В этом способе защиты главное понимать, что браузеров на сегодняшний день достаточно много и на одном компьютере их, как правило, установлено несколько. Если вы настроили, например, Opera, а Chrome оставили без внимания, то с помощью второго браузера можно беспрепятственно попасть на вредные сайты.

Избежать этого можно, установив **детский интернет-браузер «Гогуль»** (http://www.gogul.tv/) – бесплатное расширение для браузера Mozilla Firefox. Он обеспечит родительский контроль и ограничения детей в Сети от нежелательного контента. Для того, чтобы дети не пользовались другим браузером, разработано дополнительное приложение – **Angry Duck**, которое блокирует во время своей работы все браузеры, за исключением «Гогуля». Его также можно скачать с сайта http://www.gogul.tv/.

Настройки для Google Chrome

1. Создать и войти в аккаунт Google.
2. Нажав в верхней части страницы кнопку **Настройка и управление Google Chrome,** в контекстном меню выбрать пункт **Настройки.**
3. В разделе **Пользователи** нужно нажать кнопку **Добавить пользователя.**
4. В окне **Создание аккаунта пользователя** выбрать изображение и имя для нового пользователя.
5. Активировать пункт **Контролируемый профиль, управляемый пользователем user@gmail.com,** а затем нажать на кнопку **Создать.** Для контролируемого профиля, находящегося под родительским контролем Хрома, по умолчанию включена функция **Безопасный поиск.** При вводе определенных запросов в браузере Google Chrome не будут показываться результаты поисковой выдачи.

6. Пользователь с контролируемого профиля может запросить доступ к конкретному сайту. В разделе **Запросы** вы можете одобрять или отклонять права доступа к конкретным сайтам.
7. В разделе **Статистика** содержатся данные о просмотре веб-страниц. Здесь вы увидите, какие сайты посещались ребенком, сколько раз посещались эти сайты, а также в какое время были эти посещения.

Настройки для Internet Explorer

1. **Сервис → Свойства обозревателя → Содержание → Ограничение доступа → Включить.**
2. В открывшемся окне можно выбрать ограничения доступа вашего компьютера к материалам Всемирной паутины.
3. Ввести пароль, с помощью которого можно устанавливать и снимать ограничения на просмотр, когда вам того захочется.
4. В Internet Explorer 8 на той же закладке есть кнопка **Родительский контроль.**

Настройки для Mozilla Firefox

1. Войдите в настройки браузера: **Правка → Настройки.**
2. Во вкладке **Основные** выберите **При запуске Firefox: Показать домашнюю страницу.**
3. В поле **Домашняя страница** наберите: **http://family.yandex.ru.**
4. Нажмите **ОК.**

Настройки для Opera

1. Войдите в настройки браузера: **Opera → Настройки → Общие настройки.**
2. Во вкладке **Основные** выберите **При запуске: Начать с домашней страницы.**
3. В поле **Домашняя** наберите: **http://family.yandex.ru.**
4. Нажмите **ОК.**

Защита с помощью провайдера и операторов сотовой связи

Интернет-провайдер – это та фирма, которая предоставляет вам возможность выходить в Интернет. Многие провайдеры предоставляют услугу «Безопасный интернет». Об условиях подключения можно узнать в офисах или на сайте конкретного провайдера. Если нет желания и возможности самому воспользоваться способами, описанными выше, можно обратиться за этой услугой к вашему провайдеру. Тогда Интернет на всех устройствах в доме будет защищен.

Аналогичные услуги предоставляют и операторы мобильной связи, которые по сути дела тоже являются провайдерами мобильного Интернета.

МТС

Антивирус с функцией родительского контроля позволит защитить ваш компьютер от всех основных видов сетевых угроз.

Услуга «Переключаемые профили» позволяет настроить на устройстве профили разного уровня доступа к сети: «Стандартный», «Расширенный» и «Максимальный». Система блокирует определенные порты и протоколы, что гарантирует высокую степень защиты от вредоносного интернет-трафика.

Мегафон

Услуга «Детский Интернет».

Билайн

«Родительский контроль» в «Домашнем Интернете» предлагает защиту домашнего ПК по трем параметрам: ограничение по возрасту (ограничение контента), отчет о посещении и ограничение по времени.

Более детальную информацию имеет смысл узнавать в офисах и на сайтах интернет-провайдеров и операторов мобильной связи, услугами которых пользуетесь вы и ваши дети.

Защита с помощью специального программного обеспечения

В заключении нашего обзора способов защиты от вредного контента в Интернете коротко скажем о специальных программах, которые помогут вам решить эту задачу. Эти продукты распространяются как бесплатно, так и на коммерческой основе или в пакете антивирусных программ.

Бесплатные программы

«Интернет Цензор» устанавливается на компьютер под управлением MS Windows и обеспечивает фильтрацию для всех веб-браузеров и программ (http://icensor.ru).

Программа **«Интернет Цензор Лайт»** устанавливается как дополнение к веб-браузеру Mozilla Firefox и обеспечивает фильтрацию только для данного браузера.

Сервис **NetKids** предназначен для настоящего родительского контроля над детьми в Интернете (http://netkidscontrol.ru). Сервис NetKids позволяет блокировать доступ к сайтам, содержащим сексуальный, агрессивный, мошеннический контент, делает недоступными сайты, пропагандирующие наркотики и нездоровый образ жизни.

Коммерческое программное обеспечение

KinderGate Родительский Контроль (Windows, Linux) – программный модуль с простым и удобным интерфейсом и гибкими настройками, не требующий создания отдельного детского аккаунта.

«Родительский контроль» в антивирусных программах: McAfee, TrendMicro, Kaspersky Lab, Eset (NOD32), Symantec (Norton), разработка российской компании Etensys – программа KinderGate.

Результаты тестов программ на эффективность можно посмотреть, например, здесь: http://www.anti-malware.ru/.

Куда можно обратиться?

Линия помощи «Дети Онлайн»

Если вы нуждаетесь в консультации специалиста по вопросам безопасного использования Интернета или если ваш ребенок уже столкнулся с рисками в Сети, обратитесь на линию помощи «Дети Онлайн» с 9 до 18 (по московскому времени) по рабочим дням по телефону: **8-800-25-000-15** (звонок по России бесплатный). Психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М. В. Ломоносова и Фонда Развития Интернет. Также свои вопросы можно задать, отправив письмо по электронной почте: **helpline@detionline.com.**

«Горячая линия» Центра безопасного Интернета в России

«Горячая линия» позволяет любому пользователю сообщить о противоправном контенте в Сети. Сервис является анонимным и бесплатным.

Если ребенок получил от интернет-собеседника угрозу, хамство, оскорбление, сообщите об этом в «Горячую линию» Центра безопасного Интернета в России: **www.saferunet.ru.**

Детский «Телефон доверия»

Телефоны единой кризисной службы для детей, подростков и их родителей: **8-800-2000-122** (звонок по России бесплатный)**.**

Реестр запрещенных сайтов

Здесь можно подать жалобу на опасный ресурс:
http://eais.rkn.gov.ru

Уполномоченный по правам ребенка в Мурманской области
183025, г. Мурманск, ул. К. Маркса, 25А
Тел.: (8152) 486-588, 486-596; e-mail: rebenok@gov-murman.ru

Следственное управление Следственного комитета Российской Федерации по Мурманской области
183038, г. Мурманск, ул. К. Либкнехта, д. 48.
Тел.: **(8152) 403-930, 403-918**; факс: **(8152) 423-828**
Дежурный по следственному управлению: **8-921-043-13-00**
«Телефон доверия» следственного управления СК России по Мурманской области (круглосуточный): **8-921-040-07-04**

Круглосуточная телефонная линия «Ребёнок в опасности»:
(8152) 420-132 и **123** (операторы Мегафон и МТС)

Следственное управление Следственного комитета
Российской Федерации по Мурманской области

183038, г. Мурманск, ул. К. Либкнехта, д. 48
Тел.: **(815-2) 403-930, 403-918**; факс: **(815-2) 423-828**
Дежурный по следственному управлению: **8-921-043-13-00**

«Телефон доверия» следственного управления СК России
по Мурманской области (круглосуточный): **8-921-040-07-04**

Круглосуточная телефонная линия «Ребёнок в опасности»:
(815-2) 420-132 и 123 (операторы Мегафон и МТС)