

Рекомендации обеспечения безопасности учащихся в Интернете.

Поговорите с учащимся о безопасности в Интернете. Объясните основные правила, возможности различных технологий и последствия нарушений. Самое главное: убедите, что в любой непонятной или пугающей ситуации ему следует обращаться к педагогам, чтобы найти безопасное решение.

1. **Используйте компьютер и смартфон вместе с детьми.** Это хороший способ научить их правилам безопасности в Интернете. При этом дети поймут, что решать возможные проблемы лучше всего вместе.
2. **Расскажите детям больше о сайтах и сервисах в Интернете.** Поговорите о том, что их интересует в Интернете и какие страницы им можно посещать.
3. **Безопасные пароли.** Помогите своей семье приобрести правильные привычки в отношении паролей. Расскажите об их использовании. Напомните, что пароли никому нельзя передавать, за исключением лиц, которым можно доверять, например, родителям. Убедитесь, что у детей вошло в привычку выходить из своих аккаунтов, когда они используют общественные компьютеры в школе, кафе или библиотеке.
4. **Используйте настройки конфиденциальности и управления доступом.** В Интернете немало сайтов, на которых можно публиковать свои комментарии, фото и видео, рассказывать о том, что с вами произошло, как вы живете и т. д. Обычно такие сервисы позволяют определить уровень доступа к вашей информации ещё до ее публикации. Поговорите с членами своей семьи и определите, о чем не следует рассказывать всем. Научите детей уважать конфиденциальность друзей и родных.
5. **Проверьте возрастные ограничения.** Многие онлайн-сервисы, в том числе Google, предоставляют доступ ко всем функциям только совершеннолетним. А создавать аккаунты Google могут только пользователи не моложе 13 лет. Прежде чем ваш ребенок регистрируется на том или ином сайте, самостоятельно проверяйте условия его использования и соответствие материалов правилам, принятым в вашей семье.
6. **Научите детей ответственному поведению в Интернете.** Помните золотое правило: то, что вы не сказали бы человеку в личном общении, не стоит отправлять ему по SMS, электронной почте, в чате или комментариях на его странице. Поговорите с детьми о том, как другие могут воспринимать их слова, и разработайте для своей семьи правила общения.
7. **Посоветуйтесь с другими взрослыми.** Привлеките к обсуждению этой темы друзей, родственников и коллег. Другие родители и специалисты по работе с детьми могут оказать вам неоценимую помощь

в том, как научить детей и родственников правильному использованию самых разных информационных технологий.

8. **Защитите свой компьютер и личные данные.** Используйте антивирусное программное обеспечение и регулярно его обновляйте. Поговорите со своей семьей о типах личной информации – например, номер социального страхования, номер телефона или домашний адрес – эти данные не должны быть размещены в Интернете. Научите свою семью не принимать файлы или открывать вложения в электронной почте от неизвестных людей.
9. **Не останавливайтесь на достигнутом.** Безопасность в Интернете требует постоянного внимания, поскольку технологии непрерывно совершенствуются. Старайтесь всё время держать руку на пульсе. Пересматривайте правила пользования Интернетом в семье, следите за тем, как ваши близкие осваивают новые технологии, и время от времени давайте им советы.

Вредоносные программы (вирусы, черви, «тройные кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными и даже использовать ваш компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

- Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
- Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.
- Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелегальный контент.
- Периодически старайтесь полностью проверять свои домашние компьютеры.
- Делайте резервную копию важных данных.
- Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

Как настроить родительский контроль в Google Play

Чтобы ограничить покупку и скачивание контента в приложении "Play Маркет", вы можете включить родительский контроль.



Чем полезен родительский контроль

По умолчанию все, кто пользуется устройством, могут скачивать и покупать контент с любым возрастным ограничением. Включив родительский контроль, вы запретите доступ к определенному контенту.

Примечание. Запрещенный контент будет по-прежнему доступен по прямой ссылке.

Как настроить родительский контроль

Настроив родительский контроль, вы можете отключать и включать его. Все выбранные параметры сохраняются, поэтому их не нужно настраивать заново при повторном включении функции или смене PIN-кода. Благодаря этому вы сможете быстро включить родительский контроль и отдать устройство ребенку, а затем отключить фильтры, когда он вернет его.

1. Откройте приложение "Play Маркет"  на устройстве Android.
2. В левом верхнем углу экрана нажмите на значок меню  и выберите **Настройки > Родительский контроль**.
3. **Включите** функцию.
4. Ограничьте доступ к настройкам родительского контроля, установив PIN-код. Желательно, чтобы другие пользователи устройства его не знали.
5. Установите фильтры.
 - **Приложения, игры, фильмы и сериалы.** Выберите максимально допустимое возрастное ограничение для скачиваемого и покупаемого контента.
 - **Музыка и книги.** Запретите или разрешите скачивание и покупку контента для взрослых.
6. Родительский контроль действует только на том устройстве, где вы его настроили. При необходимости включите его на другом устройстве, снова выполнив приведенные выше инструкции. Также учтите, что если на устройство добавлено несколько пользователей, для них можно установить разные фильтры.

Примечание. Родительский контроль с фильтрами для отдельных типов контента доступен не во всех странах. Например, если вы путешествуете в регионе, где функция не поддерживается, она начнет работать, только когда вы вернетесь домой.

Как работает родительский контроль

Родительский контроль по-разному фильтрует приложения, игры, музыку, фильмы, сериалы и книги. Чтобы узнать подробную информацию, прочитайте разделы ниже.

При настройке родительского контроля для приложений и игр вы можете установить максимально допустимое возрастное ограничение. Покупать и скачивать контент с более высоким ограничением будет нельзя.

Однако при поиске приложений и игр или при переходе по прямым ссылкам вы все равно сможете увидеть запрещенный контент.

Примечание. Вам по-прежнему будут доступны приложения и игры, скачанные до настройки родительского контроля, даже если их возрастное ограничение выше максимального.

Как работает родительский контроль в Play Играх

Родительский контроль не распространяется на контент в Play Играх, в том числе на купленный и рекомендованный.

Если вы попытаетесь установить игру в этом приложении, откроется ее страница в Play Маркете.

На ней родительский контроль может запретить доступ.

При настройке родительского контроля для фильмов вы можете установить максимально допустимое возрастное ограничение. Покупать, брать напрокат и воспроизводить контент с более высоким ограничением будет нельзя.

Однако при поиске фильмов или при переходе по прямым ссылкам вы все равно сможете увидеть запрещенный контент.

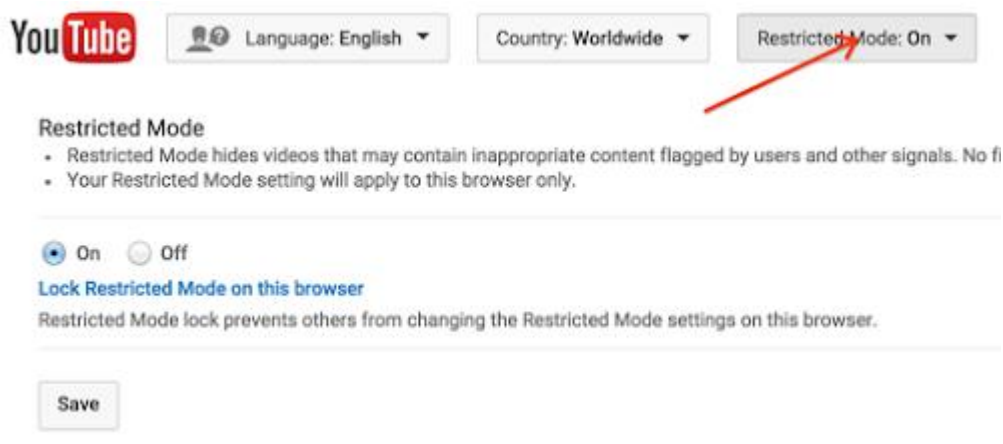
Если возрастное ограничение фильмов, в том числе купленных или взятых напрокат, превышает максимально допустимое, они будут скрыты в Play Маркете и Play Фильмах.

Чтобы этот контент снова стал виден, отключите родительский контроль.

Как включить и отключить безопасный режим

1. Войдите в аккаунт YouTube.
2. В нижней части любой страницы нажмите кнопку с надписью **Безопасный режим**.
3. Выберите **Вкл.** или **Откл.**

Нажмите **Сохранить**.



Признаки компьютерной зависимости:

- когда родители просят отвлечься от игры на компьютере, ребенок демонстрирует острый эмоциональный протест;
- ребенок раздражается при вынужденном отвлечении;
- ребенок не может спланировать окончание игры на компьютере;
- ребенок постоянно просит деньги для обновления программного обеспечения компьютера и приобретения новых игр;
- ребенок забывает о домашних делах и приготовлении уроков;
- у ребенка сбивается режим дня, режим питания и сна, он перестает заботиться о собственном здоровье;
- чтобы постоянно поддерживать себя в бодрствующем состоянии, ребенок начинает злоупотреблять кофе и другими энергетическими напитками;
- прием пищи происходит без отрыва от игры на компьютере;
- ощущение эмоционального подъема во время игры на компьютере;
- ограничение общения постоянным обсуждением компьютерной тематики с окружающими;
- нетерпение, предвкушение и продумывание заранее своего возвращения к компьютеру.
- нередко развивается бессонница и нервное истощение.

Общая безопасность в интернете.

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Мошенники могут быть хорошо оснащены и использовать самые разные инструменты и методы — например, вирусное программное обеспечение (далее — вирусы), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и почтовых сервисах.

Вирусы.

Вирусы могут распространяться с помощью вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, на съемных носителях, через зараженные сайты. При этом сообщение с вирусом может быть получено как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки. Зараженными могут быть сайты, как специально созданные в целях мошенничества, так и обычные, но имеющие уязвимости информационной безопасности.

Рекомендации:

Использовать антивирусное программное обеспечение с обновленными базами вирусных сигнатур.

Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства

коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус.

Внимательно проверять доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).

Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

Не подключать к своему компьютеру непроверенные съемные носители.

Не поддаваться на провокации злоумышленников, например, с требованием перевести деньги или отправить SMS, чтобы снять блокировку компьютера.

Мошеннические письма.

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги. В таких случаях они пишут письма определенного сценария. Один из примеров — так называемые «нигерийские письма», в которых автор обещает жертве огромную прибыль взамен на небольшие накладные расходы.

Рекомендации:

Внимательно изучить информацию из письма. Проверить достоверность описанных фактов. Если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое.

Игнорировать такие письма.

Получение доступа к аккаунтам в социальных сетях и других сервисах.

Злоумышленники часто стремятся получить доступ к аккаунтам жертвы, например, в социальных сетях, почтовых и других сервисах. Украденные аккаунты они используют, например, для распространения спам-писем и вирусов.

Мошенники могут получить доступ к учётной записи следующими способами:

Заставить ввести свои данные на поддельном сайте.

Подобрать пароль, если он не является сложным.

Восстановить пароль с использованием “секретного вопроса” или введенного ящика электронной почты.

Перехватить пароль при передаче по незащищенным каналам связи.

Как правило, для кражи данных об аккаунтах используются фишинговые сайты. **Фишинг** (англ. phishing, от fishing— рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Злоумышленники создают фишинговые сайты, копирующие интерфейс известных ресурсов, а жертвы вводят на них свои логины и пароли, не понимая, что сайты поддельные.

Рекомендации:

Использовать сложные пароли (сложные пароли состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).

Никому не сообщать свой пароль.

Для восстановления пароля использовать привязанный к аккаунту мобильный номер, а не секретный вопрос или почтовый ящик.

Не передавать учетные данные — логины и пароли — по незащищенным каналам связи (незащищенными, как правило, являются открытые и общедоступные wi-fi сети).

Внимательно проверять доменные имена сайтов, на которых вводятся учетные данные.

Правило 1. Установите вместе с детьми четкие правила посещения сайтов. Определите, какие сайты они могут посещать, какие – посещать нельзя. Выберите сайты, которые можно посещать вашему ребенку, и заблокируйте доступ к неподходящим материалам. Настройте параметры безопасности вашего компьютера.

Правило 2. Помогите детям выбрать правильное регистрационное имя и пароль. Убедитесь в том, что они не содержат никакой личной информации.

Правило 3. Объясните детям необходимость защиты их конфиденциальности в сети Интернет. Настаивайте на том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки.

Правило 4. Не позволяйте ребенку встречаться с онлайн-знакомыми без разрешения. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу.

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг, кибербуллинг и др.). Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы. Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство, социальное бойкотирование с помощью различных интернет-сервисов. Предупреждение кибербуллинга: Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать. Научите детей правильно реагировать на обидные слова или действия других пользователей. Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз. Старайтесь следить за тем, что ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Правило 5. Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

Правило 6. Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.

Информация об организации безопасного доступа к сети «Интернет» для детей дома и в образовательном учреждении (программах «родительского контроля»)

Инструментарий, который можно использовать в различных операционных системах (Windows, Linux) для безопасного доступа к сети «Интернет» для детей дома и в образовательном учреждении, это:

1. специализированное программное обеспечение для контентной фильтрации,
2. программы «Родительский контроль» или «Семейная безопасность»,
3. специализированные детские браузеры.

Использование специализированных программ для осуществления контентной фильтрации от нежелательного содержимого в сети Интернет:

Child Protect <http://cp.s-soft.org/> - это социальный проект, цель которого оградить детей от нежелательного содержимого в Интернет. Работа программы незаметна для ребёнка. При попытке осуществить доступ на нежелательный сайт, который имеется в базе, браузер будет выдавать ошибку «Сервер не найден», создавая впечатление, что такого сайта не существует. Также существует возможность опционально блокировать доступ к социальным сетям: ВКонтакте, Одноклассники, МойМир@mail.ru, FaceBook. Программа работает скрытно от диспетчера задач Windows.

Программа **K-9** <http://www1.k9webprotection.com/> предназначена для эффективной защиты компьютеров, на которых работают дети, от нежелательного контента. Программа использует систему фильтрации содержимого сайтов по 55 категориям. Также в программе имеются опции «черного» и «белого» списка. Можно дополнительно заблокировать любой сайт из разрешённой категории. Кроме всего прочего, в настройках программы можно указать временной промежуток, в течение которого пользователь будет иметь возможность пользоваться Интернетом. Также имеется опция аудита активности пользователя с возможностью просмотра списка заблокированных адресов. Программа имеет защиту от удаления.

Naomi Internet Filter <http://www.newestsoft.com/Windows/Web-Development/Wizards-Components/Naomi-3290.html> предназначается для организации ограничения доступа к нежелательным Интернет-ресурсам. При своей работе утилита контролирует содержимое, загружаемое из Интернета, и запрещает доступ к нежелательным сайтам. Такая фильтрация осуществляется по ссылкам и ключевым словам (поддерживается 10 языков).

Программа не нуждается в настройках, нужно только задать пароль, чтобы было невозможно отключить фильтрацию без его ввода.

Дополнение **Adblocks Plus** к браузеру Mozilla FireFox позволяет настроить контент-фильтрацию и дополнительно избавиться от рекламы и всплывающих окон на сайтах. Для других браузеров также есть техническое решение этого дополнения <http://adblockplus.org/en/installation>. Список всех подписок доступен по ссылке <http://adblockplus.org/en/subscriptions>. Официальный сайт дополнения - <http://adblockplus.org/m/>.

NetPolice Lite <http://netpolice.ru/filters/lite/> - упрощенная версия платной программы NetPolice. К основным возможностям упрощенной версии относятся регулярные информационные отчеты, 5 категорий фильтрации, доступ к настройкам по единому паролю, перенаправление на безопасный поисковик (<http://search.netpolice.ru>), возможность самостоятельного формирования списка сайтов для блокировки (до 5 URL), блокировка загрузки исполняемых файлов, предупреждение о переходе на небезопасные сайты.

HandyCache <http://handycache.ru/> — это программа, которая экономит трафик, ускоряет загрузку страниц, блокирует рекламу и иное нежелательное содержимое и позволяет в автономном режиме (без подключения к Интернет) просмотреть любые посещенные ранее сайты. HandyCache сокращает трафик до 3-4 раз за счет кэша. Любой из установленных на компьютере браузеров может использовать возможности программы, а значит, нет необходимости загружать одни и те же страницы несколько раз для просмотра в разных браузерах.

Программа **Kontrol Lite** <http://www.kontrol.info/> - бесплатная версия Интернет-фильтра семейства Kontrol, которая позволяет блокировать сайты для взрослых. Отключить ее могут только родители, знающие пароль. После загрузки и установки программы необходимо пройти регистрацию на сайте разработчика и получить login и пароль. Без них программа работать не будет.

ParentalControl <http://www.securitylab.ru/software/270756.ph> - дополнение к браузеру Internet Explorer, которое помогает предотвратить доступ детей к сайтам для взрослых. Программа поставляется с набором настроенных фильтров, основанных на анализе материалов, позволяющим взрослым выбирать различные параметры фильтрации для своего ребенка. Также можно самостоятельно заблокировать или разрешить для просмотра любой сайт. Текущая версия работает только с этим браузером.

Использование функции «родительского контроля» или «семейной безопасности»

Вкладка «Семейная безопасность» Windows Live 2011 для ОС Vista и 7 <http://explore.live.com/windows-live-family-safety?os=winxp>, для Windows XP - <http://explore.live.com/windows-live-family-safety-xp> позволяет выбирать, какое содержимое будет доступно детям в Интернете. Имеется возможность устанавливать ограничения на поисковые запросы, отслеживать посещаемые сайты, разрешать или блокировать доступ к ним. Фильтр «Семейной безопасности» должен быть установлен на каждом компьютере, который используют дети. Если фильтр не установлен, параметры безопасности не будут применены.

Если в образовательном учреждении или на домашнем компьютере используются антивирусная программа Kaspersky Internet Security версии 2010, то в этой программе есть вкладка «Родительский контроль», в которой можно заблокировать доступ к нежелательным сайтам.

Использование специализированного браузера, созданного для детской аудитории

Детский браузер **Гогуль** <http://www.gogul.tv/> специально разработан для детей, их родителей и педагогов. Эта программа мультиплатформенная, т.е. работает и в Linux и в Windows. Детский браузер Гогуль обеспечит контроль посещения ребёнком сайтов в сети Интернет.

Программа родительского контроля **Angry Duck** <http://www.gogul.tv/about/#5> является также бесплатным необязательным дополнением к детскому браузеру Гогуль. По желанию родителей может блокировать запуск всех иных браузеров до ввода родительского пароля, а также выполнять другие функции по ограничению доступа детей к компьютеру.

Использование виртуальных социальных сервисов по осуществлению контентной фильтрации с ведением «белых списков» сайтов, посещение которых одобрено, и специализированных поисковых машин в сети Интернет, которые специально организованы для работы с детьми <http://school.yandex.ru/> возможно в школьном Яндексe, который включает в себя фильтрацию контента. Можно использовать «по умолчанию» эту поисковую машину дома и в школе.

NetPolice DNS <http://netpolice.ru/filters/dns-filter/> поможет ограничить доступ к нежелательному содержимому, проводить мониторинг активности, снизить затраты на Интернет-трафик. DNS-фильтр предоставляется всем желающим бесплатно. Для подключения фильтра необходимо выполнить настройку на компьютере. После этого все запросы к Интернет-ресурсам будут автоматически проходить проверку на категорию запрашиваемого контента. Если запрашиваемый сайт будет относиться к нежелательной категории, то такой запрос будет заблокирован. Взамен заблокированного ресурса для просмотра будет предоставляться страница блокировки. DNS-фильтр - это дополнительная защита компьютера, так как Интернет-ресурсы с нежелательным содержанием очень часто заражают компьютер вирусами, «червями», шпионами и т.д. Таким образом, исключение доступа к небезопасным ресурсам значительно снижает риск нанесения ущерба компьютеру и данным, хранящимся на нем.

Рассмотренные выше версии являются бесплатными.

Программы, решения и сервисы данного перечня можно использовать для организации безопасного информационного пространства в каждом образовательном учреждении, на каждом домашнем компьютере.