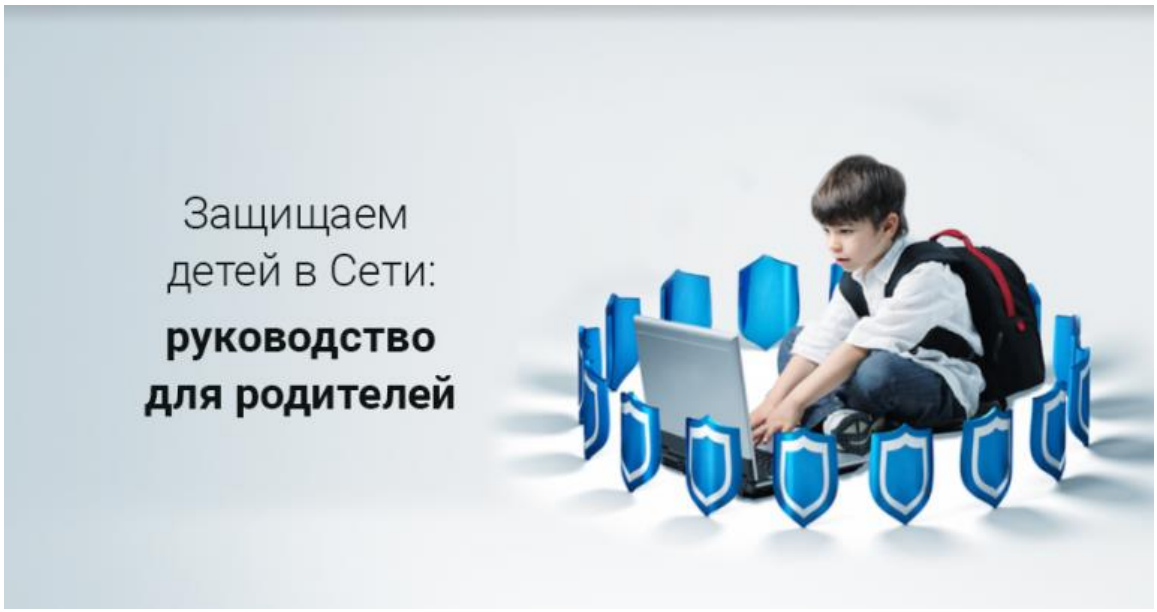
Полное руководство
по онлайн-защите детей — 2020

Обновлено 13.10.2020, использован материал https://ru.vpnmentor.com/blog/защищаем-детей-в-сети-руководство-для



Мы постоянно слышим истории о том, как очередная технология изменила нашу повседневную жизнь. Многие из нас уже давно размышляют над тем, как именно технологии изменили лично нас. Но подумал ли кто-нибудь о влиянии технологий на наших детей?

85% матерей заявили, что используют телефоны, планшеты и компьютеры, чтобы занять детей.

Возраст, в котором дети получают свое первое устройство с выходом в Сеть, постоянно снижается. Исследования показали, что у **83% американских домохозяек есть планшеты, а смартфоны есть у 77%.**

Скрыться от достижений прогресса нельзя даже в школе. Учителя задают домашнюю работу, для выполнения которой нужно искать информацию в Интернете и использовать различные программы.

Технологии адаптируются и не собираются исчезать из нашей жизни. Увы, многие из нас даже не задумываются о кибер-безопасности: исследования показали, что **68% родителей вообще не следят за тем, что делают в Интернете их дети.** А ведь с каждым годом дети все глубже и глубже уходят в Сеть!

Для многих детей Интернет стал чем-то даже более реальным, чем реальный мир. **Ради благополучия детей родителям необходимо знать, чем те заняты в Сети (и хорошим, и плохим), и понимать, как это влияет на эмоциональное и физическое состояние детей.**

Но есть одна проблема, которую с готовностью признают многие из нас: мы не совсем понимаем, если можно так выразиться, онлайн-мир. Instagram, Snapchat, Twitter? Уже сложно! А если вспомнить еще и про 2ch и TOR, то и вовсе дело плохо! Более того, многие из нас просто не умеют работать с Интернетом или компьютером.

Впрочем, есть и хорошие новости. **Чтобы защитить детей при работе в Сети, не нужно быть компьютерным гением — система родительского контроля устанавливается достаточно просто.** Что еще важнее, **простой разговор с ребенком станет лучшей мерой защиты!** Просто обозначьте четкие границы, чем можно и чем нельзя заниматься в Сети, и будьте готовы прийти на помощь ребенку, когда тот ошибется или зайдет слишком далеко. Собственно, именно этим и должны заниматься родители, разве нет?

В этом руководстве мы рассмотрим 8 областей, на которые вам следует обратить внимание при взаимодействии с миром Интернета. Многое зависит и от возраста вашего ребенка. Считайте это руководство чем-то вроде сборника советов о том, на что следует обращать внимание, пока ваш ребенок растет.

1. Смартфоны и приложения

Как гласит статистика, первый смартфон среднестатистический ребенок получает в 10 лет. Конечно, очень удобно, когда у ребенка есть такая штука, телефон в принципе делает жизнь

безопаснее и спокойнее — например, ребенок может позвонить и сказать, что безопасно добрался до дома, или попросить вас встретить его, или позвать на помощь. Включив в смартфоне ребенка GPS, вы сможете отследить его местоположение. Действительно, мечта любого родителя — знать, где сейчас находится твой ребенок!

Но смартфоны могут также стать и источником опасности для ребенка. Это личные устройства, поэтому мы не можем точно знать, для чего именно и как часто пользуются ими дети.

Если вы собираетесь подарить ребенку смартфон, то не помешает заранее составить четкий список правил. Но даже если у вашего ребенка смартфон уже есть, заняться правилами никогда не поздно. Нужно показать детям, что смартфон — это еще и большая ответственность.

Установите правила использования смартфона вашим ребенком. Если ваши дети будут привлекать вас к использованию ими телефона, это поможет обеспечить их безопасность.

Вот некоторые из уместных мер предосторожности:

- Прежде чем давать ребенку смартфон, пусть тот подпишет с вами специальный договор, где будут собраны все соответствующие правила. Повесьте этот договор у себя дома на видном месте.
- Скачайте приложения родительского контроля. С их помощью вы сможете ограничить использование смартфона, определить его местонахождение и отслеживать звонки и СМС ребенка. Такие приложения также могут блокировать определенные функции смартфона в определенное время.
- Договоритесь с ребенком о том, сколько времени тот может использовать смартфоном ежедневно.
- Подавайте ребенку личный пример. Не ужинайте, глядя в телефон, не набирайте СМС за рулем и так далее.
- Примите за правило зарядку мобильных устройств в комнате, где никто не спит — так ваши дети не будут засиживаться за телефоном допоздна.

2. Потоковые трансляции и Smart-TB

Было время, когда перед экраном телевизора собиралась вся семья… Конечно, у нас с вами наверняка были собственные телевизоры в собственных комнатах, и мы наверняка провели долгие часы перед ними, причем совершенно без нравоучений родителей.

Но это все лирика. Реальность же такова, что потоковые трансляции стали весьма популярными, и количество доступного контента выросло чуть ли не по экспоненте. Разумеется, далеко не все из этого разнообразия стоит смотреть детям.

Конечно, **у сервисов потокового вещания есть немало плюсов.** Например, там есть отличные образовательные передачи для детей и интересные документальные фильмы. Многие такие сервисы не показывают рекламу, что само по себе огромный плюс на фоне каналов обычного телевидения. С помощью потоковых трансляций вы сможете открыть перед ребенком целый новый мир! В общем, главное то, как вы все будете использовать.

У большинства крупнейших сервисов потокового вещания есть системы родительского контроля, некоторые из которых более совершенны, чем другие. Так, Netflix позволит вам создать отдельные профили для себя и ваших детей.

С их помощью вы сможете **гарантировать, что ваши дети смотрят лишь то, что подходит для их возраста.** Так как детское меню Netflix отличается по цвету от обычного, вы всегда сможете с легкостью определить, разрешенный ли контент смотрят ваши дети или нет. Разумеется, это не будет мешать вашим детям снова и снова пытаться получить доступ к именно вашему профилю, так что будьте бдительны!

iTunes и Apple TV позволяют родителям задать определенные рейтинги для контента, который смотрят их дети. А вот у Amazon Prime никакого родительского контроля нет, так что единственное, что вы можете сделать, это постоянно выходить из своей учетной записи и никому не говорить свой пароль.

Впрочем, все это не сможет заменить регулярных обсуждений просмотренных фильмов и передач вместе с ребенком.

Контролируйте просмотр детьми телевизора посредством ограничения количества часов просмотра в день, применения настроек родительского контроля, разъяснения ребенку содержания просматриваемых им телепередач и организации совместного семейного просмотра телепередач.

3. Игровые приставки и онлайн-игры

Согласно статистке, 91% детей от 2 до 17 лет, играют в видеоигры. **Игровые приставки уже очень долгое время вызывают у родителей… озабоченность, не сказать — страх.** Очень

много игр эксплуатируют темы жестокости или сексуальности, **поэтому важно тщательно следить за тем, во что играют ваши дети.**

Кроме того, есть еще и многопользовательские игры (они же «онлайн-игры»), и там **дети могут стать жертвами травли со стороны других игроков.** Многие игры дают игрокам из всех уголков земного шара возможность общаться друг с другом в чатах, что может угрожать благополучию детей: **они могут стать жертвами кибер-хулиганов или извращенцев.** Кроме того, дети могут подружиться с другими игроками и рассказать им про себя что-нибудь излишне личное.

В то же время, компьютерные игры — это отличный способ развития самых разных навыков ребенка. Играя, дети учатся решать различные проблемы, преследовать долгосрочные цели, работать в команде. А еще в игры очень весело играть всей семьей! К счастью, в большинстве игровых консолей поддерживаются весьма продвинутые системы родительского контроля, позволяющие **родителям следить за тем, как и во что играют их дети.**

Обсуждайте с детьми игры, в которые они играют. Убедитесь, что профиль ребенка переведен в приватный режим. Подумайте над установкой приставки в месте, которым пользуются все члены семьи. Изучайте возрастные рейтинги игр. При создании профилей используйте родительский контроль. Объясните ребенку, что разговаривать онлайн можно далеко не со всеми.

4. Социальные сети

Формат изменился, но родители все равно продолжают переживать про телешоу и компьютерные игры, за которыми проводят время их дети. Теперь же к списку поводов для беспокойства надо добавить еще и социальные сети.

Подростки в США пользуются социальными сетями едва ли не поголовно! Более того, 71% сидят сразу в нескольких социальных сетях. Дети в наши дни проводят на этих сайтах слишком много времени. Исследование, проведенное некоммерческой организацией Common Sense Media, показало, что **дети в возрасте от 8 до 12 лет проводят онлайн по 6 часов в день,** и большая часть этого времени проходит именно в социальных сетях. Для подростков **от 13 до 18 лет это значение доходит до целых 9 часов!**

Как выяснили недавно ученые из Гарварда, большинство социальных сетей требуют, чтобы пользователям было не меньше 13 лет, однако это не помешало 68% опрошенных родителей помочь с регистрацией своим детям.

Для малолетних детей и подростков пристраститься к социальным сетям особенно просто. А это открывает дверь самым разным проблемам — например, кибербуллингу, разглашению личной информации и разговорам с незнакомыми людьми (подробнее о чем читайте далее).

Доступ к социальным сетям также является одним из центральных элементов развивающейся социальной идентичности подростков: так они заводят новых друзей, так они могут безопасно развлекаться. Главное здесь — обозначить границы и не допускать инцидентов.

Обеспечьте безопасную среду. Не позволяйте детям проводить время в социальных сетях, пока те не достигнут приемлемого возраста. Компьютер должен находиться в месте, которым пользуются все члены семьи. Ограничьте время, которое можно проводить в социальных сетях. Заблокируйте приложениям доступ к местоположению. Измените настройки конфиденциальности. Отслеживайте онлайн-активность ваших детей.

5. Кибербуллинг

Наши дети теперь живут на два мира, реальный и виртуальный. Увы, в виртуальном мире тоже есть хулиганы.

Кибербуллинг часто становится темой новостных выпусков — как правило, в связи с подростковыми самоубийствами, вызванными онлайн-травлей.

Киберхулиганы есть на всех перечисленных нами платформах. Они распространяют слухи и отправляют сообщения с угрозами в социальных сетях, по СМС или на электронные адреса, притворяются другими детьми и выкладывают от их имени провокационные материалы, делают частные фото достоянием общественности, не имея на то разрешения, а также пишут про других детей унизительные или оскорбительные сообщения.

Публичность киберхулиганов — вот что делает их столь опасными. Если раньше ребенка задирали на игровой площадке, то свидетелями тому было лишь несколько сверстников. Сейчас же самые сокровенные тайны вашего ребенка могут быть опубликованы на потеху Интернету! Более того, пока вы не примете меры, этот контент никто не будет удалять!

Кибербуллинг оказывает негативное влияние не только на репутацию жертвы, но и на репутацию самих хулиганов. Он также может серьезно повлиять на будущее ребенка, в том числе на учебу в университете и работу.

А еще от киберхулиганов нельзя укрыться. Если вашего ребенка достают обычные хулиганы, то он может скрыться от них дома. Но цифровые платформы доступны постоянно, и поэтому от киберхулиганов укрыться просто негде.

Зачастую очень сложно понять, столкнулся ли ваш ребенок с онлайн-травлей или нет. В конце концов, все происходит в Сети, так что родителям и учителям сложнее узнать про это. По данным организации i-SAFE, **менее половины всех детей, столкнувшихся с киберхулиганами, рассказывают об этом родителям или другим взрослым.** Исследование, заказанное правительством США, показало, что **21% подростков от 12 до 18 лет становились жертвами хулиганов, причем 16% столкнулись именно с кибербуллингом.**

Проще всего предотвратить кибербуллинг или остановить его, если хорошо знать особенности поведения вашего ребенка и знать, на какие тревожные признаки следует обращать внимание.

Если ребенок стал жертвой кибербуллинга, то он может закрыть одну учетную запись в социальных сетях и завести себе новую. Ребенок может начать избегать общения, даже в том случае, если раньше это доставляло ему удовольствие. Жертвы и зачинщики травли часто прячут экраны или мобильные устройства, когда рядом с ними находятся другие люди, они перестают рассказывать о том, чем занимаются в сети. Также ребенок может начать испытывать стресс. Поговорите с ребенком про кибербуллинг.

6. Конфиденциальность и защита информации

Будучи родителями, мы не можем не волноваться о том, какое влияние окажет Интернет на эмоциональное и физическое благополучие наших детей. Дети легко могут пасть жертвами различных угроз, связанных с нарушением конфиденциальности данных, и некоторые из них могут нанести еще и серьезный финансовый урон. Взрослые, впрочем, сталкиваются с теми же проблемами — это **вредоносное ПО и компьютерные вирусы, фишинг и кража личности.**

Проблема в том, что у детей мало жизненного опыта. Проблема в том, что они куда более склонны доверять незнакомцам, чем мы, циники-взрослые. Ребенок может назвать свое полное имя и домашний адрес и даже не задуматься о том, что это может стать причиной больших проблем. **Детей можно с легкостью обмануть и заставить, к примеру, выдать данные вашей банковской карты вредоносному стороннему приложению.**

Хакеры и воры могут выудить информацию из детей самыми разными способами. Бесплатные игры, фильмы и даже рингтоны «для детей» могут оказаться настоящими троянскими конями и заразить ваш компьютер вирусами, которые украдут ваши данные.

Хакеры могут притвориться, что они представляют, к примеру, Google, отправив ребенку письмо с требованием сообщить пароль, а могут притвориться и одним из его или ее друзей.

Что необходимо обсудить с ребенком?

- **Поговорите с ребенком про самые серьезные онлайн-угрозы современности.** Дети должны знать, что такое фишинговая атака, они должны уметь отличать надежный сайт с играми от опасного.
- Убедитесь, что дети хранят свою личную информацию в тайне от посторонних и никогда не выкладывают в Сеть свое полное имя, номер телефона, адрес или номер школы.
- Поговорите с детьми о паролях. Надежный пароль — это самый лучший способ защиты от хакеров и кражи личности. Используйте безопасный генератор паролей (например, созданный нами) для того, чтобы создать вашему ребенку максимально надежный пароль.
- Скажите детям, что не стоит пользоваться публичными точками доступа wi-fi — с помощью таких сетей хакерам не составит труда взломать их устройства.

Что можно сделать для создания безопасной обстановки:

- Установите на ваш компьютер и мобильные устройства ваших домочадцев надежный антивирус.
- Рассмотрите вариант установки VPN-сервиса. VPN, виртуальная частная сеть, зашифрует ваше интернет-подключение и позвит анонимизировать все ваши действия в Сети. Таким образом, хакерам будет гораздо сложнее украсть вашу конфиденциальную информацию.
- Если вы и ваши дети используете дома сразу несколько устройств для выхода в Сеть, подумайте об установке VPN на роутер. Это позволит защитить весь трафик, проходящий через ваш роутер,

и избавит вас от необходимости настраивать VPN-приложение на каждом отдельно взятом устройстве.

- Установите блокировщик рекламы, чтобы вашим детям не пришлось бороться с искушениями лже-рекламы, за которыми, как правило, скрываются лишь опасные вирусы.
- Если ваши дети используют смартфоны, убедитесь, что выставлены максимальные настройки безопасности.

7. Контент, не предназначенный для детей

В Интернете нет ни границ, ни преград, а это значит, что ваши дети могут найти контент, предназначенный для взрослых. Эти материалы вполне могут лишить их душевного покоя. От сквернословия и до насилия и порнографии — у разных людей разные представления о недопустимом.

Это будет достаточно сложно, но все же однажды вам придется обсудить с детьми то, что может попасться им на глаза в Сети. **Многие дети не обращаются к родителям, когда сталкиваются с чем-то, что они не должны видеть** — например, потому что боятся, что родители рассердятся, или заберут их смартфоны, или ограничат доступ к Интернету.

Но если ваш ребенок решил обратиться к вам с такой проблемой, **то держите себя в руках и спокойно все обсудите.** Если речь идет о контенте сексуального характера, то, скорее всего, ребенок уже достаточно смущен и растерян, особенно из-за того, что все это ему приходится обсуждать с родителями. Дайте детям понять, что вы всегда готовы помочь им, и ответить на их вопросы без осуждения.

Подростки могут натолкнуться на контент сексуального характера в Сети по самым разным причинам. Может, по ошибке, или по присланной другом ссылке, или из-за природной любопытности.

Будет очень полезно честно и открыть поговорить с детьми о сексе, в частности — обсудить онлайн-порно. Это очень важный момент! Различные исследования показали, что порнография может оказать разрушительное действие на подростков, исказив в ошибочную, нездоровую сторону их представления о сексе. Из-за порнографии дети могут начать воспринимать окружающих как объекты, а не как людей мыслящих и чувствующих. Впрочем, испытывать интерес к теме секса и отношений — абсолютно нормально! **Такой разговор станет отличной возможностью направить детей на правильный путь познания сексуальности.**

Конечно, есть еще множество способов оградить своих детей от контента, к которому они пока что не готовы. Например, можно настроить родительский контроль на компьютере. Но помните, что ничто не в силах заменить откровенный и искренний разговор по душам с ребенком.

Поговорите с ребенком:

- Скажите детям, что они всегда могут обратиться к вам за помощью и ответами — в частности, о том, что они видели в сети.
- Скажите детям, что нет ничего дурного в том, чтобы интересоваться сексом. Дайте им ссылки на правильные ресурсы на эту тему (например, Brook и Thinkuknow). Thinkunow особенно хорошо подойдет для детей младшего возраста, также там вы найдете материалы и ссылки для детей самых разных возрастных групп. Возможно, не помешает почитать сайт вместе с ребенком и обсудить вопросы, которые у него могут возникнуть.

Чтобы можно сделать для блокировки нежелательного контента:

- **Установите фильтры для блокировки контента (например, порно).** Ваш интернет-провайдер, скорее всего, предоставляет доступ к функции родительского контроля, как и большинство игровых приставок. Настроить такую систему будет достаточно просто.
- Переведите Google в безопасный режим, чтобы дети не наткнулись случайно в результатах поисков на что-нибудь нежелательное.
- Установите блокировщик рекламы, чтобы защититься от вирусов, которые могут распространять нежелательный контент.

8. Онлайн-маньяки

В последней главе этого руководства мы коснемся самой темной, самой жуткой угрозы: онлайн-маньяков, охотящихся на детей. По данным Министерства Юстиции США, порядка **13% детей, имевших доступ в Интернет, становились жертвами приставаний сексуального характера, а еще в среднем 1 ребенок из 25 сталкивается с настойчивыми просьбами перенести общение «в реальный мир».**

Такие маньяки стремятся «привязать» к себе детей, сформировать с ними доверительную связь в целях дальнейшей эксплуатации.

Интернет сделал жизнь маньяков-педофилов существенно проще. **Теперь они могут выслеживать жертв в Сети, используя для этого социальные сети, электронную почту, мессенджеры и так далее.** Однако чаще всего маньяки используют онлайн-чаты: **в 76% случаев общение с маньяками начиналось именно в чате.**

Эти хищники могут создать сразу несколько онлайн-личностей, притворяясь детьми и пытаясь заманить жертв в свою ловушку. Изучая аккаунты в социальных сетях и анализируя ответы ребенка, маньяки пытаются узнать про него как можно больше.

Преступники могут одновременно общаться сразу с несколькими детьми, однако усилия свои они сконцентрируют на самом уязвимом из всех. И поверьте, эти маньяки не удовлетворятся одним лишь онлайн-общением с ребенком. **Зачастую они заставляют детей перевести общение в видео-мессенджер и обмениваться интимными фотографиями.** Они даже могут попытаться договориться с ребенком о реальной встрече — с реальными последствиями!

Понять, не общается ли ваш ребенок с таким маньяком, довольно сложно, потому как практически всегда таких собеседников дети от родителей скрывают. **Но есть определенные тревожные признаки:** дети, попавшиеся на крючок маньяка, могут начать вести себя очень скрытно, так как маньяки часто требуют от ребенка ничего и никому не рассказывать. Дети могут грустить, чувствовать себя потерянно, сталкиваться с внезапными переменами настроения. Крайне важно дать ребенку понять, что вы всегда готовы помочь и выслушать его или ее, о чем бы ни зашла речь.

Что следует обсудить с ребенком?

- **Обсудите с ребенком тему онлайн-маньяков.** Убедитесь, что дети осознают всю необходимость соблюдения осторожности при общении в сети, что они не будут рассказывать незнакомым людям персональную информацию.
- Скажите вашим детям, что они всегда могут обратиться к вам за помощью, о чем бы ни шла речь.
- Есть смысл вместе с детьми почитать какие-нибудь обучающие материалы на эту тему. Так, замечательные видео есть на сайте Thinkuknow.
- Если вам кажется, что ваш ребенок попал в зону риска, **обратитесь за помощью к его или ее учителям, социальным работникам и полиции.**

Заключение

Защитить безопасность своих детей при работе в сети можно с помощью самых разных решений, от VPN-сервисов и антивирусов до фильтров интернет-контента и систем родительского контроля. **Увы, ничто из этого не гарантирует 100% защиты ребенка.**

Как мы уже неоднократно сказали в этом руководстве, главное — не научиться настраивать различные приложения (это самое простое, так что не надо бояться и жаловаться на неумение работать с компьютером), не отслеживать все новые тренды, появляющиеся в сети (поверьте, это никому не под силу).

Самое главное и самое сложное — **регулярно и честно обсуждать с ребенком его или ее жизнь.** Помните, что с помощью провайдера, социальных сетей, игровых сервисов и всего прочего мы можете ограничить ребенку доступ к тому или иному контенту, однако это еще не значит, что все вышеперечисленные будут заботиться о нем.

Кто же должен заботиться о ребенке вообще и его онлайн-безопасности в частности? Вы и только вы. Обсудив с ребенком способы безопасной работы в Сети, вы сможете построить с ним доверительные, позитивные отношения.

Интернет-безопасность ребенка должна стать приоритетом для родителей и опекунов. И если вам пригодилось это руководство, то обязательно поделитесь ими с вашими друзьями и близкими в социальных сетях.

Вы можете свободно делиться этим постом или его частями и копировать его на ваш сайт, в ваш блог или социальные сети. Все, чего мы просим, — это указание на наше авторство. Мы хотим, чтобы ваши дети оставались в безопасности, и поэтому важна ваша помощь в распространение этой информации.