Дети в Интернете: угрозы и способы защиты

[Елена Кунсэль](http://letidor.ru/profile/23725)



 Моя трехлетняя племяшка смело берет со стола телефон, проводит по нему пальчиком и изумленно застывает: у ее мамы iPhone, а тут – Samsung на Android. Она хитро улыбается и через пять минут уже рассматривает фотографии, а через десять – добирается до игр. Подходя к телевизору, тем же движением проводит по экрану пальчиком и озадаченно вздыхает: тут техника еще не дошла до маминого смартфона.

 Иногда мне кажется, что эти дети скоро будут проводить пальцами по лицам друг друга – чтобы понять, в какую сторону смайлик, разговаривать смс-ками, стоя рядом друг с другом, и продолжать потомство на facebook.

 Домашнее задание – на компьютере: найти в Википедии, вставить в Word и распечатать. Любой пятиклассник знает как, в отличие от его бабушки. А откуда знаем мы, куда этот пятиклассник «ходит», кроме Википедии? Почему мы так уверены, что на «Одноклассниках» сидят только «одноклассники»? И если не уверены, то, как уберечь, как научить «не брать конфетку у чужого дяди» - не отвечать на сообщения от неизвестного пользователя, будь там хоть десять радостных смайлов и хоть сто общих «друзей»?

Статистика посещений Интернета детьми

 Согласно [исследованию McAfee](http://letidor.ru/go.php?url=http://www.mcafee.com/sg/about/news/2012/q2/20120625-01.aspx), в 2011-ом году 70% подростков находили способы обходить «родительский контроль», так что их родители были не в курсе, чем именно занимались дети. Для сравнения, по данным исследования той же компании, в 2010 году своих родителей обманывали лишь 45% подростков в возрасте от 13 до 17 лет. Чем же занимаются эти милые дети в Интернете?

 По [данным исследований «Лаборатории Касперского»](http://letidor.ru/go.php?url=http://www.securelist.com/ru/blog?print_mode=1&weblogid=207768864) в 2013 году дети из России посещали следующие сайты:

- Социальные сети (59,6%)

- Интернет – магазины (9,1%)

- Порнография, эротика (8,8%)

- Почта (5,7%)

- Нелегальное ПО (3,4%)

- Остальное: игры, чаты и форумы, оружие, жестокость и насилие, нецензурная лексика, азартные игры, платежные системы, анонимные прокси-сервера, наркотики.

 Эксперты «Лаборатории» отметили, что среди остальных стран Россия лидирует по количеству детей, посещающих социальные сети. Исследователи так же отмечают, что по сравнению с предыдущими годами сильно возросла популярность Интернет-магазинов, а такая категория как «Наркотики» успешно реализуется в «Соцсетях», которые являются универсальной платформой для общения на эту тему.

 По [данным](http://letidor.ru/go.php?url=http://digit.ru/internet/20130530/401947153.html#ixzz2sFQQ1dUu) той же компании, каждый третий родитель РФ интересуется тем, как именно дети проводят время в Сети, какие посещает сайты и с кем общается, и это при том, что на одну семью приходится в среднем 3,6 различных электронных устройств с доступом в сеть и возможностью хранения больших объемов информации.

 Что же касается Европы, то по данным исследования, проведенного EU Kids Online II совместно с Фондом Развития Интернет и факультетом психологии МГУ имени М.В. Ломоносова, большая половина детей выходит в Интернет под контролем взрослых: 60% европейских школьников пользуются интернетом в школе и столько же детей выходит в Интернет из дома, из общей комнаты, то есть под присмотром родителей.

 В России по данным того же исследования 70% детей 9-10 лет и свыше 90% школьников старше 13 лет пользуются Интернетом без надзора старших. По данным «Лаборатории Касперского», дети изучают «запрещенные ресурсы» в часы, когда уроки уже закончились, а родители еще не пришли с работы, то есть с 15 до 17 часов.

Угрозы детям в Интернете

 Помимо всем известных положительных моментов, Интернет несет в себе опасность, которая может затронуть даже пользователей младшего дошкольного возраста. Неосторожный клик по яркой картинке на открытом родителем Youtube приводит к появлению на экране перед малышом клипа с сомнительным содержанием. Реклама на смартфоне или вдруг появившийся значок приложения с картинкой раздетой девушки – и ребенок уже задается вопросом, как это у него получилось.

 Поиск игр в сети, желание посмотреть научный фильм или мультик (в котором вдруг звучат бранные слова вместо привычных диалогов) могут привести к попаданию младших детей на сайты с нелицеприятным контентом «18+»,

а то и откровенной порнографией. Для родителей детей младшего возраста проблема стоит не «как ограничить», а «как оградить», потому что в том нежном возрасте еще нет мыслей о чём-то скверном, и ребенок по незнанию, а то и благодаря навязчивой рекламе становится свидетелем нежелательной информации.

 Известный антивирусный вендор Kaspersky Lab приводит полный список угроз, которым могут подвергаться дети разного возраста в Интернете, и которым эти дети могут подвергать родительский компьютер (а так же смартфон, планшет и другие устройства, подключенные к сети):

• «Попутные» заражения (т.е. вредоносные программы, загружаемые автоматически при просмотре зараженных сайтов).
• Заражение при использовании файлообменных (P2P) сетей, дающих другим пользователям доступ к вашему компьютеру.
• Нежелательная реклама, в том числе всплывающие окна и рекламные программы, которые часто устанавливаются автоматически вместе с бесплатным ПО, загружаемым из интернета.
• Получение ребенком информации сексуального характера (или иной неприемлемой информации).
• Загрузка ребенком из интернета пиратских материалов (например, музыкальных или видеофайлов).
• Ребенка могут обманным путем убедить предоставить личные данные (его собственные или ваши).
• Ребенок может стать жертвой запугивания через интернет (кибербуллинг).
• Ребенок может стать жертвой домогательств педофила (например, в онлайн-чатах).

К этому списку можно добавить следующее:

- Социальные сети, в которых может произойти практически всё вышеперечисленное.

- «Встречи в реале». По результатам [исследования Detionline.com](http://letidor.ru/go.php?url=http://detionline.com/assets/files/research/DigitalLiteracy.pdf), половина российских подростков встречаются с незнакомцами из интернета в «реале», в то время как европейские подростки более осторожны и лишь 10% идут на личную встречу после знакомства в интернете.

Если опасность, подстерегающая ребенка в интернете, носит всё-таки виртуальный характер (за исключением «недетского видео», которое может травмировать психику), то встречи с незнакомцами имеют непредсказуемые и сразу же очень «реальные» последствия: «подружка» из аськи в жизни оказывается 50-летним мужчиной со скверными намерениями, а онлайн приятель вдруг предлагает попробовать наркотики. И все, что родителям известно о «новом знакомом» – это его ник и ненастоящее имя в скайпе.

- Получение ребенком вредоносной информации – специально или случайно (например, всплывающая строка в поиске) – о наркотиках, суициде, причинении себе вреда (сюда же входят рекомендации по похудению) и сексуальных извращениях. Часто подростки даже не задумываются о том, чтобы попробовать нечто подобное, но попадая в новую компанию, стесняются отказать.

- И последняя «угроза», с которой сталкиваются дети в Интернете и которая не представляет опасности для вашего компьютера, но опасна для вашего ребенка - это Интернет-зависимость. К сожалению, она не лечится анитвирусами и «Родительским контролем», и посоветовать можно только одно надежное и проверенное средство – родительскую любовь и заранее выстроенные, хорошие отношения в семье.

Обзор технических средств защиты ребенка в Интернете

 По [данным исследования «Института семейной безопасности в Интернете»](http://letidor.ru/go.php?url=http://i-deti.org/upload/files/google_fosi_hart_survey-report_executive-summary_111206_rus.pdf)об осведомленности, отношении и использовании функции «Родительского контроля», проблема безопасности в Интернете не является предметом повышенного внимания родителей.

 Подавляющее большинство (86%) сообщили, что считают нахождение ребенка в интернете абсолютно (42%) и достаточно (44%) безопасным. И только 13% родителей признались, что сетевая активность детей очень (3%) и несколько (10%) небезопасна. Из опрошенных родителей 53% сообщили, что они использовали настройки или программное обеспечение для контроля или ограничения деятельности детей в Интернете.

 По результатам исследования "Цифровая компетентность подростков и родителей: результаты всероссийского исследования" (2013 г.) родители положительно относятся к Интернету, как к источнику интересной, развивающей информации (70 % опрошенных), как к возможности получать быстрый доступ к нужной информации (34 %), как к возможности использовать образовательные ресурсы (34 %), к разнообразию выбора (15 %) и возможностям для общения с друзьями (14 %).

 Негативную сторону интернета для своего ребенка родители видят в том, что он затягивает и отвлекает детей от учебы (55 %), переполнен ложной и психологически вредной информацией (43 %), мешает живому общению (8,5 %). Родители на данный момент испытывают некоторое замешательство в том, чтобы однозначно ответить на вопрос «полезен ли Интернет детям».

 При, казалось бы, высоком показателе осведомленности родителей об опасностях в Интернете, а так же о технических способах защиты детей, тем не менее, использует эти способы лишь половина родителей.

Из технических средств защиты детей в Интернете можно назвать следующие:

**1. «Родительский контроль» от антивирусных вендоров**

 У всех антивирусных вендоров – лидирующих производителей антивирусных программ – есть пакет услуг «Родительский контроль».

«Родительский контроль» включает в себя стандартный набор функций, а именно:

- Ограничение времени нахождения ребенка в сети;
- Ограничение времени пользования компьютером;
- Возможность создания графики с допустимыми часами работы в течение дня;

- Блокировка сайтов с запрещенным контентом – создание «чёрных» списков на основе баз данных антивирусного производителя по категориям (наркотики, социальные сети и т.д.) и создание «белых списков» родителем;
- Ограничение на запуск приложений (например, игр) и установку новых программ; - возможность следить за перепиской ребенка в соцсетях и чатах (ICQ, Skype) и контролировать пересылку личной информации (в основном, это платные пакеты услуг).

В первую пятерку заслуживающих доверия антивирусных вендоров входят:

- McAfee
- TrendMicro
- Kaspersky Lab
- Eset (Nod 32)
- Symantec (Norton)

 Каждая компания по-своему заботится о безопасности детей. Kasperskiy Lab предлагает [список советов по защите](http://letidor.ru/go.php?url=http://www.kaspersky.ru/keeping_children_safe) ребенка от угроз в сети. McAfee проводит регулярные [исследования](http://letidor.ru/go.php?url=http://www.mcafee.com/sg/about/news/2012/q2/20120625-01.aspx) среди американских подростков. Компания Trend Micro разработала отдельную программу, уделив безопасности детей особое внимание. Ежегодно TrendMicro проводит конкурс для подростков «What's your Story?», в рамках которого детям предлагается снять небольшой видеоролик, нарисовать рисунок, написать рассказ, песню или стихотворение на тему «Как сделать пребывание в интернете безопасным». В 2011 г. на конкурс попало более 100 работ, которые были просмотрены более 150 000 раз.

 Некоторые антивирусные компании ведут свои блоги по безопасности детей – например, [блог Trend Micro](http://letidor.ru/go.php?url=http://www.trendmicro.com.ru/home/internet-safety-for-kids/protection/) и не самый приятный [блог](http://letidor.ru/go.php?url=http://blog.netkidscontrol.ru/), содержание которого стоило бы пометить как «18+», интересное скорее подросткам, чем сознательным родителям.

Отличные советы для родителей [опубликовала](http://letidor.ru/go.php?url=http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx) компания Microsoft в разделе «Семейная безопасность». Многие статьи переводные из американских источников, тем не менее, несут в себе полезную информацию. В США родители активнее сталкиваются с последствиями преследований в Интернете, и нас, скорее всего, в будущем ожидает похожий сценарий развития отношений наших детей и Интернета.

**2. Отдельные программы «Родительского контроля»**

 В пример можно привести разработку российской компании Etensys программу KinderGate. Некоторые ресурсы [сравнивают](http://letidor.ru/go.php?url=http://www.dgl.ru/reviews/detki-v-setke-obzor-neskolkih-programm-roditelskogo-kontrolya_2205.html)функциональность этой недорогой программы с «Родительским контролем» известных вендоров. KinderGate неоднократно занимала первые места в списках рейтингов, так что если вы пользуетесь антивирусом без встроенного «Родительского контроля», то эта программа может стать для вас хорошим решением.

**3. Операционные системы**

 В операционных системах Microsoft Windows и Apple iOS автоматически встроены функции «Родительского контроля». Изучив настройки, можно назначить ребенка отдельным пользователем со своим паролем и задать ему ограничения – например, по времени использования компьютера, блокировку новых программ, а так же возможность отслеживать действия ребенка в Интернете после приобретения им дополнительных приложений. Дополнительные функции Windows7 позволяют родителю настроить «Безопасный поиск», который задействует механизмы фильтрации поисковых систем в Интернете, таких как google.ru и yandex.ru.

**4. «Родительский контроль» в Интернете**

 Крупные сервисы не менее озабочены проблемой, как обезопасить пребывание детей в Интернете. После очередных судебных разбирательств и изменений в системе защиты персональных данных, компания Google запустила проект [«Good to know»](http://letidor.ru/go.php?url=http://www.google.ru/intl/ru/goodtoknow/familysafety/), с разделом «Семейная безопасность» и рекомендациями по безопасности детей-онлайн.

 На YouTube, одном из сервисов Google, можно найти видео о правилах поведения на видеосервисе. Родитель имеет возможность настроить YouTube таким образом, чтобы сервис показывал только видеоматериалы, разрешенные к просмотру детей (правда, тогда придется каждый раз менять настройки для себя при желании посмотреть «недетское» видео). То же касается и поисковой системы Google (и остальных крупных поисковых систем).

**5. «Родительский контроль» от провайдера**

 Провайдеры со своей стороны предоставляю схожие услуги. Например, МГТС [предлагает](http://letidor.ru/go.php?url=http://mgts.ru/home/internet/services/parental-control/) родителям вводить ограничения по времени пребывания в Интернете ребенка в их отсутствие, предоставляет отчеты о просмотренных сайтах. Из минусов этой системы – возможность ребенком при наличии данных, например, номера договора, получить пароль для изменения настроек в личном кабинете. При входе в личный кабинет интересующийся родитель сразу же увидит произошедшие изменения и сможет самостоятельно принять меры.

Безопасность в социальных сетях

 Это особо острый вопрос, так как с одной стороны, соцсетей не так много и в любом «Родительском контроле» их можно включить в «чёрные списки» или исключить из «белых». Но если десятилетний ребенок примет запрет спокойно, то подросток открыто воспротивится решению родителей. Да и не стоит забывать, что в окружении ребенка всегда есть друзья, родители которых могут не ограничивать чадо в пользовании компьютером.

 Владельцы соцсетей пытаются контролировать контент и общение посетителей. В 2012 году «Одноклассники» ввели функцию запрета получения сообщений детьми младше 14 от неизвестных людей, не принадлежащих к группе друзей или друзей родителей. Тогда же соцсеть запустила «Тревожную кнопку», благодаря которой можно пожаловаться на недопустимую информацию или сообщений от незнакомцев.

 Американская соцсеть Facebook постоянно усовершенствует систему родительского контроля на станицах Facebook. У родителя есть возможность «прикрепить» ребенка к себе и разрешать «дружбу», видеть, что делает ребенок, с кем он общается и о чем думает.

 Как уже говорилось ранее, некоторые «Родительские контроли» позволяют читать личную переписку ребенка в соцсетях (правда, возникает морально-нравственный вопрос – до какого возраста ребенка родитель имеет на это право и вопрос воспитательный - согласен ли с этим подросток, способный самостоятельно отключить ненужные ему компоненты в системе «Родительского контроля»).

**Детские порталы**

 Многие родители разрешают детям (обычно речь идет о детях младшего школьного возраста) посещать только определенные сайты, действуя по принципу создания «белых списков». В интернете уже давно появились сайты для детей младшего возраста – с песенками, мультфильмами, развивающими играми и раскрасками, а так же образовательные порталы для детей постарше. В связи с воплощением в жизнь идеи домашнего образования, таких ресурсов становится всё больше и больше. Появляются ресурсы для самостоятельного обучения, сайты, посвященные играм и творчеству – то есть не затягивающие в «Инетрнет-паутину», а лишь обогащающие реальную жизнь ребенка.

 Некоторые организации, как, например, «Центр анализа интернет-ресурсов», считают необходимым создание отдельной социальной сети для школьников. Идея неплоха, но есть свои «но»: подростки уже познали «взрослые» социальные сети и переход в соцсеть, которая будет ограничиваться школой, а то и классом, и контролироваться классным руководителем, может быть принят в штыки. Во-вторых, обязанность контролировать школьников ляжет на плечи классных руководителей, итак постоянно занятых заполнением бумажек для отчетности вместо более плотного общения с детьми.

 Многие преподаватели высших учебных заведений отмечают, что с появлением соцсетей стало гораздо удобнее информировать студентов о домашнем задании, переносе занятий и информационных ресурсах перед сдачей экзаменов. Но применимо ли это к школьникам, или мы всё-таки хотим больше и более «реального» общения для наших детей, в настоящем, не виртуальном мире?

**Детские браузеры**

 Детские браузеры, например [Гогуль](http://letidor.ru/go.php?url=http://gogul.tv/about/" \t "_blank), работают по принципу «белых списков». Правда, создавать списки будет не родитель, а разработчик в лице психологов и педагогов. В браузере «Гогуль» «безопасность ребёнка в Интернете обеспечивается за счёт наличия собственного каталога детских сайтов, проверенных педагогами и психологами и рекомендованных к просмотру». Браузер так же предоставляет родителям статистику посещений и помогает ограничить время пребывания ребенка в сети.

 Как мы видим, сейчас существует множество способов контролировать детей. Каждый родитель способен выбрать лучший способ для себя и своей семьи в зависимости от провайдера и антивирусного ПО, которыми родители уже пользуются, и конечно, в зависимости от возраста, характера и условий жизни ребенка. Любознательные родители без труда смогут найти подробные инструкции по использованию функций «Родительского контроля» или выбрать подходящее для себя средство и способ защиты, тем более, что при необходимости любое техническое средство защиты можно изменить или дополнить. Остается вопрос мотивации «защищать» ребенка в сети. Но это уже совсем другая история.