



# Безопасный интернет для родителей



Выполнили учителя  
информатики  
МБОУ «Гимназии №1»:  
Бердникова В.В.  
Шабалин В.Л.

Город Ангарск

## Безопасный интернет- Что из этого следует?

Наивный вопрос, – скажут многие.

Что плохого, что плохого...

ну, взрослые сайты, ну гадости всякие.

Примерно, так многие взрослые и скажут. Вот тут то и проявляются главные проблемы взаимосвязи **взрослый-ребенок-интернет**. Первое, часто дети разбираются в IT технологиях лучше, чем родители и их интересы простираются много дальше пикантных сайтов, второе, родители часто не понимают, а в чем же состоят истинные опасности всемирной компьютерной сети Интернет для несовершеннолетних.

# Основные проблемы:

- Взрослый контент. Ресурсы так или иначе связанные с сексом и вопросами интимных отношений. Наибольшую опасность представляют ресурсы пропагандирующие нездоровый секс, а также различные порносайты, где секс представлен в наиболее brutальной форме;
- Запрещенная или крайне нежелательная информация. Наркотики, расовая нетерпимость, жестокость, деструктивные секты, финансовые аферы и так далее. Не всегда можно определить такие сайты с первого взгляда даже взрослому и в этом их опасность;

# Основные проблемы:

- Игры. Онлайн игры опасны слишком глубоким погружением ребенка в виртуальный мир, из которого выбираться будет не так уж и просто. Также вредят психике ребенка игры со слишком жестоким или сексуальным сюжетом. А многопользовательские миры еще и потенциально опасны игровыми партнерами, которыми могут оказаться криминальные элементы и разного рода извращенцы;
- Интернет-казино и другие подобные ресурсы. Зависимость от азартных игр, траты больших сумм денег, воровство;
- Социальные сети. Интернет-ресурсы знакомств. Опасны возможностью познакомиться со взрослым, который имеет криминальные намерения. Опасны слишком глубоким погружением ребенка в мир онлайн общения, которое в итоге заменит ему реальные увлечения, спорт, учебу и встречи с друзьями.

# Основные проблемы:

- Мошенничество. Аферисты всех мастей используют любую возможность для того, чтобы забрать ваши деньги и часто привлекают к этому детей, которые становятся слепым орудием в их руках;
- Реальные встречи. Взрослые с криминальными намерениями могут назначать встречи вашему ребенку в реальном мире, часто под видом друга или подружки из социальной сети или онлайн игры.

# Основные способы защиты детей в интернете

Теперь рассмотрим, как защитить от интернета детей. Вы, возможно, удивитесь, но **основным контролем было и остается личное участие родителя** в интернет-интересах ребенка. Конечно, не всегда это возможно реализовать по объективным причинам, но стремиться к этому надо.

Вы же интересуетесь школьной жизнью ребенка – да?

Давайте определим, как ребенок вообще может попасть в интернет, поскольку многие сужают этот круг до ноутбука, но это далеко не так.

# Устройства для выхода во всемирную паутину:

- Стационарный персональный компьютер;
- Ноутбук, нетбук;
- Планшетный компьютер, смартфон, мобильный телефон с браузером;
- Электронные книги, игровые приставки с выходом в интернет;
- Телевизионные устройства с функцией Smart TV.

# Устройства для выхода во всемирную паутину:

Далее надо понять, где ребенок может выйти в интернет:

- Дома;
- У друзей;
- В школе или каких-то специализированных кружках;
- В компьютерных клубах;
- С мобильных устройств, где угодно.



# Что из этого следует?

Что, по сути, ребенок имеет широкие возможности обойти родительские запреты, да хотя бы зайдя после школы к приятелю «поиграть в шахматы». И что одним вашим компьютером дома дело не ограничивается. И соответственно, **самое первая и лучшая защита ребенка – это в разумных пределах удовлетворить его любопытство.** Здраво осветить интересующие его моменты, объяснить, в чем опасность тех или иных сайтов, сделать акцент на множестве вирусов и мошенниках, которые постоянно пытаются получить всеми правдами и неправдами доступ к вашему личному ПК и так далее. Дело в том, что запретный плод всегда манит к себе значительно сильнее, и в итоге поиск подростком фотографии обнаженной женской груди приводит его на сайты каких-то сексуальных извращенцев.

# **Теперь рассмотрим технические аспекты защиты детей в интернете**

Только учтите, что идеальной защиты еще не придумали и что подавляющее большинство подростков тем или иным способом пытаются обойти родительские запреты с переменным успехом.

# Теперь рассмотрим технические аспекты защиты детей в интернете

1. Установка специализированного программного обеспечения для выхода в интернет, обычно называется «детский браузер». В русскоязычной среде популярен **Гугль** (работает на базе **Mozilla**) и дополнительный компонент **Angry Duck**, который запрещает запуск других браузеров. Содержит список доступных детских сайтов, запрещает доступ к ряду нежелательных ресурсов, контролирует и ограничивает время ребенка в сети. Также **Angry Duck** не разрешает вызов диспетчера задач, чтобы ребенок не мог выгрузить процесс из памяти. Из минусов можно выделить то, что это совсем детская программа и в глазах подростка она будет смотреться по-идиотски. Являясь нестандартным программным обеспечением для посещения интернета, **Гугль** может быть плохо совместим с рядом сайтов, иметь проблемы с надёжностью, безопасностью и так далее. Поэтому такие «игрушки» скорее стоит использовать в случае с совсем маленькими детьми для ознакомления их интернетом и защиты от нежелательного контента;

# Теперь рассмотрим технические аспекты защиты детей в интернете

2. Использование стандартных фильтров поисковых систем, например, Яндекса или Google. У Яндекса это называется «семейный поиск», а у Google «строгая фильтрация». Данную защиту нельзя рассматривать как основную, поскольку она не мешает сделать прямой переход на нежелательный сайт, минуя поиск. Да и никто не запрещает подростку воспользоваться альтернативными поисковиками. Но подобные защитные механизмы в любом случае не помешают. Тем более что иногда самая банальная защита оказывается самой эффективной. Только включая её, не забудьте защитить настройки паролем, а то ребенок скинет их простым движением мыши;

# Теперь рассмотрим технические аспекты защиты детей в интернете

3. Использование функций ограничения доступа в стандартных системах безопасности, например, в антивирусных пакетах. Большинство популярных антивирусов, например **Касперский** или **Dr.Web** имеют компоненты родительского контроля, которые запрещают ребенку доступ к указанным интернетовским или локальным ресурсам, в том числе и программам. Обычно в них можно указать фильтрацию по словам, например, по слову «секс», по именам сайтов, а также ограничить время нахождения ребенка в интернете и защитить его от вредного влияния;

# Теперь рассмотрим технические аспекты защиты детей в интернете

4. Популярными приложениями являются: **KinderGate**, **KidGid**, **Интернет Цензор**. Обычно такие программы не только закрывают доступ к ряду ресурсов по указанным параметрам, но и ограничивают время нахождения ребенка в сети (например, отключают доступ с 20:00 до 10:00), а также запоминают, сайты на которых ребенок был в процессе пользования интернетом. Кстати, дети регулярно ищут способы обойти их защиту, чтобы удостовериться в этом, достаточно набрать имя программы и что-то вроде «отключить». В случае каких-то неполадок или попыток сбоя взрослый может получить предупреждение на почту. Минус у всех этих программ один и тот же, они не всегда адекватно могут запретить или разрешить тот или иной ресурс. Поскольку вред сайта часто не ограничивается набором слов на странице и часто, казалось бы, безобидная **онлайн игра** может повредить психику подростка значительно сильнее, чем сайт с эротикой.

# Дополнительная информация

1. Можно обратиться к провайдеру(фирма, которая устанавливала интернет);
2. Приобрести роутер с функцией «безопасный интернет» примерная стоимость 2000 рублей;
3. Сервис:  
Yandex.dns – там даны адреса, которые можно прописать в настройках роутера.

## Итак:

Всё вышесказанное можно подытожить следующим образом – **универсальной защиты от интернета не существует**, и всегда хорошо, когда вы сможете сами принимать участие в «виртуальной» жизни вашего ребенка и мотивировать его к **самоцензуре**. Посидите рядом, когда он играет в игры, посетите его любимые сайты, поговорите про интересы, пусть он вас познакомит со своими виртуальными друзьями и т.д. Ведь многие сайты сами по себе не являются вредными, и лишь часть их контента можно признать нежелательным для ребенка.



## И так:

Еще стоит сказать, что программные продукты родительского контроля большей частью предназначены для установки на операционную систему Windows, а для защиты мобильных устройств используются другие решения.

# Основные правила безопасности для родителей

1. Прежде, чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети (вредоносные программы, небезопасные сайты, интернет-мошенники и др.) и их последствиях.
2. Четко определите время, которое Ваш ребенок может проводить в Интернете, и сайты, которые он может посещать.
3. Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений.
4. Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения.
5. Спрашивайте ребенка о том, что он видел и делал в Интернете.

# Основные правила безопасности для родителей

6. Объясните ребенку, что при общении в Интернете (чаты, форумы, сервисы мгновенного обмена сообщениями, онлайн-игры) и других ситуациях, требующих регистрации, нельзя использовать реальное имя. Помогите ему выбрать регистрационное имя, не содержащее никакой личной информации.
7. Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также "показывать" свои фотографии.
8. Помогите ребенку понять, что далеко не все, что он может прочесть или увидеть в Интернете — правда. Приучите его спрашивать то, в чём он не уверен.

# Основные правила безопасности для родителей

10. Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием.
11. Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации.
12. Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без вашего разрешения или в отсутствии взрослого человека.
13. Постарайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются.
14. Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов — читать грубости так же неприятно, как и слышать.

# Основные правила безопасности для родителей

15. Проверяйте актуальность уже установленных правил. Следите за тем, чтобы ваши правила соответствовали возрасту и развитию вашего ребенка.

# Что делать, если ребенок уже столкнулся с какой-либо интернет-угрозой

1. Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказывать.
2. Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он попал в неприятную ситуацию (потратил деньги в результате интернет-мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату – непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в Интернете.

# Что делать, если ребенок уже столкнулся с какой-либо интернет-угрозой

3. Если ситуация связана с насилием в Интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно обидчику о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т. п.). Объясните и обсудите, какой опасности может подвергнуться ребенок при встрече с незнакомцами, особенно без свидетелей.
4. Соберите наиболее полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств. Зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.

# Что делать, если ребенок уже столкнулся с какой-либо интернет-угрозой

5. В случае, если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации и подскажут, куда и в какой форме обратиться по данной проблеме.

*Линия помощи «Дети онлайн» (8 800 25 000 15) — бесплатная всероссийская служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования Интернета и мобильной связи. На Линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М.В.Ломоносова и Фонда Развития Интернет.*



# Литература:

1. В основе рекомендаций лежит разработанная Фондом Развития Интернет классификация интернет-рисков, результаты исследования «Дети России онлайн», которое было проведено Фондом Развития Интернет по методологии международного исследовательского проекта Еврокомиссии «EU Kids Online II» (2010—2011 годы), а также обращения пользователей, поступившие на Линию помощи «Дети онлайн».
2. <http://bezopasnost-detej.ru/kak-zashchitit-rebenka/71-kak-zashchitit-detej-ot-interneta>
3. <http://nsportal.ru/nachalnaya-shkola/>