

# БЕЗОПАСНЫЙ ИНТЕРНЕТ - ДЕТЯМ!

Нормативно-правовая база



- ФЗ от 29.12.2010 №436 «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- ФЗ от 25.07.2002 №114 «О противодействии экстремистской деятельности»;
- ФЗ от 02.07.2013 №187 «О внесении изменений в отдельные законодательные акты РФ по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях»;
- ФЗ от 03.07.1998 № 124 «Об основных гарантиях прав ребенка в РФ»;
- Методические рекомендации по ограничению в ОО доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования» (Письмо о направлении от 28.04.2014 № ДЛ-115/03);
- Перечень видов информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;
- Перечень видов информации, к которой может быть предоставлен доступ согласно определенной возрастной категории;
- Рекомендации по организации системы ограничения в ОО доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования;
- Постановление Правительства РФ от 26.10.2012 №1101 «О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в РФ запрещено».

## Практические советы для учителей

Учителя также играют важную роль в воспитании детей и могут показать им, как правильно и безопасно использовать новые технологии и, прежде всего, компьютеры, которые есть в большинстве школ и домов.

Именно поэтому мы предлагаем учителям серию следующих рекомендаций:

### **1. Узнайте подробнее.**

Найдите и изучите информацию об Интернет-угрозах. Узнайте, что они собой представляют, и какие от них последствия могут быть. Подумайте, как Вы сможете донести эту информацию до своих учеников и студентов.

### **2. Разработайте образовательный план по ИТ-безопасности.**

Т.к. молодые люди изучают, как обращаться с компьютерами и работать в Интернете, им следует также знать и о потенциальных опасностях. Таким образом, Вы должны быть уверены, что они способны соблюдать свою безопасность при работе с ПК и Интернетом. Составьте план обучения, определитесь с тем, что Вы им будете рассказывать, найдите требуемую информацию и документацию.

### **3. Сделайте Ваши рассказы интересными и практичными.**

Лучший способ донести эту информацию – это использовать практические примеры. Вы можете продемонстрировать некоторые опасности в Интернете, показав Вашим ученикам, какие негативные последствия они имеют. Расскажите новости и истории, которые связаны с подобными инцидентами.

#### **4. Научите их защищать себя.**

Во время практических занятий расскажите о том, как настроить антивирусные программы, создавать сложные пароли, объясните им, как можно безопасно совершать интернет-покупки, и пр.

#### **5. Практикуйте то, что Вы преподаете.**

Чтобы помочь детям избежать рисков, важно, чтобы Вы сами были осведомлены об этих рисках и избегали их. Используйте надежное решение безопасности, которое позволяет не только защититься от вирусов, спама, хакеров, мошенников и других угроз, но и содержит в себе функцию Родительского контроля, обеспечивающую безопасное использование Интернета детьми.

### **Практические советы для родителей**

#### **1. Поговорите с Вашими детьми.**

Начальной точкой для защиты Ваших детей должен стать разговор с ними. Вы должны знать, какие сайты они посещают, с кем они общаются, что они любят смотреть и т.д. Вы не должны позволять им уходить из дома и не предупреждать Вас, куда и с кем они пошли. Соответственно, Вы не должны разрешать им пользоваться Интернетом, если они не знают, как с ним обращаться.

#### **2. Обучите себя и поделитесь этими знаниями с Вашими детьми.**

Для многих родителей Интернет является все еще неизвестным миром. Кто-то использует его для поиска информации, чтения газет или скачивания музыки, фильмов и других файлов, но для большинства родителей те сервисы и сайты, которыми пользуются их дети, остаются для них неизвестными. По этой причине очень важно знать о тех утилитах, которые Интернет предлагает детям, о рисках, которые они могут в себе нести, а также о том, как их можно избежать. Узнав, Вы сможете затем советовать Вашим детям, как безопасно использовать Интернет.

#### **3. Установите правила для использования Интернета.**

Вы должны установить четкие и понятные правила, которые описывают расписание выхода в Интернет, максимальную продолжительность работы в Интернете, а также способ его использования. Убедитесь, что Ваши дети следуют этим правилам, особенно при использовании Интернета ночью. Также следует обратить внимание на расположение компьютера дома: если у Вас только один ПК на всю семью, то он должен располагаться в общей комнате, а не в спальне Вашего ребенка.

#### **4. Запретите детям предоставлять конфиденциальную информацию.**

Вы должны проинструктировать Ваших детей о том, что им нельзя предоставлять кому-либо в Интернете такие данные, как их имя, адрес или свои фотографии. Посоветуйте им использовать псевдоним или ник и покажите им, как можно создать сложные безопасные пароли (сочетание букв с нижним и верхним регистром, цифр, символов и т.д.), которые помогут предотвратить кражу регистрационных данных детей для доступа к почте, системам обмена сообщениями, форумам и пр.

#### **5. Научите своих детей быть осторожными.**

Информация в Интернете может быть обманчивой. Выше мы рассматривали с Вами, каким образом вредоносный код может маскироваться в виде различных кодеков и видеофайлов, как педофилы представляются другими людьми, чтобы установить контакт с детьми, и как сообщения, которые пришли от знакомого человека, могут оказаться зараженными. Зачастую в Интернете многие вещи выглядят не так, как они нам представляются. Научите Ваших детей быть осторожными и приучить их не делать ничего такого, что могло бы поставить под угрозу их безопасность и конфиденциальность.

#### **6. Установите эффективное решение безопасности.**

Чтобы защитить Ваших детей от вредоносных программ, лучший способ – это использовать обновляемое и эффективное решение безопасности. Такие решения для домашних пользователей, которые уничтожают вредоносные программы, блокируют доступ к тем веб-сайтам, которые могли бы заразить компьютер, фильтруют спам и, содержат функцию Родительского контроля, позволяющую Вам решить, какие сайты будут доступны для Ваших детей.

### **Практические советы для детей**

#### **1. Не нажимайте на ссылки.**

Когда Вы общаетесь в чате с помощью систем обмена мгновенными сообщениями или если Вы получили письмо, никогда не нажимайте непосредственно на ссылку. Если сообщение или письмо пришло к Вам от известного человека, то скопируйте адрес ссылки и поставьте его в адресной строке Вашего браузера. Если сообщение или письмо пришло к Вам от неизвестного человека, то лучше не открывать эту ссылку. Даже если Вы поставите ее в адресную строку браузера, то может открыться сайт с вредоносными программами, которые загрузятся на Ваш компьютер.

#### **2. Не скачивайте и не открывайте файлы из подозрительных источников.**

Несомненно, Вы получаете много сообщений, которые приглашают Вас скачать фото, песню или видео. Иногда такие сообщения могут отправляться без ведома человека, от которого они пришли к Вам, потому что его компьютер был заражен вредоносными программами, которые стали автоматически себя распространять среди других пользователей. В этом случае, лучше спросить знакомого Вам отправителя, действительно ли он отправил Вам это сообщение или файл. Если он не делал этого, то сообщите ему, что возможно его ПК заражен, и пусть он сообщит всем, чтобы не смотрели и удалили это сообщение или файл, которое якобы пришло от него другим пользователям.

#### **3. Не общайтесь с незнакомцами.**

Пользуясь чатами и системами обмена мгновенными сообщениями, Вы никогда не знаете, с кем Вы общаетесь на самом деле. Особенно это касается онлайн-сообществ, где люди никогда не видели друг друга в реальной жизни. Никогда не дружите с незнакомцами, и ни под какими предлогами не соглашайтесь на встречу с ними в реальной жизни.

#### **4. Не распространяйте через Интернет свою конфиденциальную информацию.**

Никогда не отправляйте личную информацию (Ваши данные, фотографии, адрес и пр.) по электронной почте и через системы обмена мгновенными сообщениями, а также никогда не публикуйте такого рода информацию в блогах и форумах. Кроме того, будьте внимательны при создании профилей в таких сервисах, как Facebook или MySpace. Вы никогда не должны размещать такую конфиденциальную информацию, как Ваш возраст и Ваш адрес. Также рекомендуем Вам не использовать свое настоящее имя, а пользоваться псевдонимом или ником.

#### **5. Будьте бдительны.**

Как правило, никто ничего не дает просто так. В Интернете если что-то выглядит очень привлекательно, то вряд ли оно есть таким на самом деле. Поэтому если Вы получили фантастическое предложение работы от неизвестных пользователей, то не обращайтесь на него внимания.

#### **6. Не запускайте подозрительные файлы.**

Если Ваше решение безопасности скажет Вам, что файл может содержать (или содержит) вредоносную программу, не открывайте этот файл. Просто удалите его.

#### **7. Поговорите с Вашими родителями или учителями.**

Если у Вас возникли вопросы обо всем этом, если Вы столкнулись с чем-то подозрительным, если Вы получили оскорбительные или опасные письма, то обсудите это с взрослыми. Они смогут Вам помочь.

### **Полезная информация о технологиях детской безопасности в сети Интернет**

1. «Безопасность детей в Интернете» <http://www.microsoft.com/rus/childsafety>
2. «Безопасность дома» <http://www.microsoft.com/rus/athome/security>

3. Брошюра «Отцы и дети. Угрозы в интернете» - <http://academy.kaspersky.com/?id=429>
4. Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным <http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html>
5. Онлайн игра «Изучи Интернет – управляй им» [www.igra-internet.ru](http://www.igra-internet.ru)
6. «Основы безопасности детей и молодежи в Интернете» — интерактивный курс по Интернет-безопасности <https://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu.htm>
7. «Сетевой экстрим» - тренинг – безопасность в сети интернет - <http://wiki.pskovedu.ru/index.php>
8. Памятка «Как защититься от интернет-угроз» - [pam.pdf](#)
9. Понятный Интернет [www.zaprosto-internet.ru](http://www.zaprosto-internet.ru)
10. Смешарики [www.smeshariki.ru](http://www.smeshariki.ru)
11. Справочник по детской безопасности в Интернете [www.google.ru/goodtoknow](http://www.google.ru/goodtoknow)
12. Специализированный сайт <http://detionline.com> – основной сайт, на котором можно получить информацию:
  - Линия помощи «Дети онлайн» - телефонное и онлайн консультирование для детей и взрослых по проблемам безопасного использования интернета и мобильной связи;
  - Журнал «Дети в информационном обществе» - посвящен актуальным вопросам влияния современных инфокоммуникационных технологий на образ жизни, воспитание и личностное становление подрастающих поколений;
  - Статистика и Исследования - посвящены изучению психологии цифрового поколения России. Особое внимание уделяется проблемам безопасности детей и подростков в интернете;
  - Образовательные проекты - повышение цифровой компетентности, культуры информационной безопасности, профилактика интернет-рисков среди пользователей Рунета: детей, подростков, родителей, учителей, старшего поколения.
13. Фонд развития Интернет [www.fid.su](http://www.fid.su)
14. Центр безопасного Интернета в России [www.saferunet.ru](http://www.saferunet.ru)
15. ЮНИСЕФ (международная организация представлена более чем в 150 странах мира). Защита прав детей и другие направления <http://www.unicef.org/ceecis/ru/>
16. Club Symantec единый источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». [http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs\\_teach\\_kids](http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs_teach_kids)
17. Nachalka.com предназначен для учителей, родителей, детей, имеющих отношение к начальной школе. Статья «Безопасность детей в Интернете». Советы учителям и родителям <http://www.nachalka.com/bezopasnost>
18. OS.zone.net - Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль» <http://www.oszone.net/6213/>

Если ты считаешь, что существует on-line-угроза для твоей безопасности, позвони на линию помощи «Дети онлайн» по телефону: **8-800-25-000-15** (по России звонок бесплатный) или напиши письмо - e-mail: [helpline@online.org](mailto:helpline@online.org)

Получить консультацию о том, как с помощью программного обеспечения Microsoft повысить безопасность детей и всей семьи при пользовании сети Интернет, можно по телефону **8-800-200-800-1** (бесплатный номер для территории России).

## Безопасный Интернет

**ТВОЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ**

В Европе свыше 13 миллионов детей, как ты, регулярно пользуются Интернетом. Если ты ищешь информацию по своему домашнему заданию или только хочешь повеселиться, то Интернет – замечательное место, но ты должен знать об опасностях и следовать советам:

**НЕ НАЖИМАЙ НЕИЗВЕСТНЫЕ ССЫЛКИ**

Когда ты общаешься в чатах и интернет-пейджерах или получаешь письмо, никогда не нажимай непосредственно на ссылку. ЕСЛИ ОНА ПРИШЛА ОТ НЕЗНАКОМОГО ЧЕЛОВЕКА, ЛУЧШЕ НЕ ОБРАЩАТЬ НА НЕЕ ВНИМАНИЯ.

**НЕ СКАЧИВАЙ ФАЙЛЫ ИЗ НЕИЗВЕСТНЫХ ИСТОЧНИКОВ**

Без сомнения, ты часто получаешь сообщения, предлагающие тебе скачать фото, песню или видео. ИНОГДА ТАКИЕ ФАЙЛЫ МОГУТ ОТПРАВЛЯТЬСЯ НЕ ЧЕЛОВЕКОМ ИЗ ТВОИХ КОНТАКТОВ, А ВИРУСОМ, КОТОРЫЙ ЗАРАЗИЛ ЕГО КОМПЬЮТЕР И ПЫТАЕТСЯ РАСПРОСТРАНЯТЬСЯ СРЕДИ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ.

Именно по этой причине ты должен всегда спрашивать своего знакомого, действительно ли он отправил тебе сообщение или файл. Если он этого не делал, сообщи ему, что его компьютер заражен. Пусть он сообщит своим знакомым, которые получили от него подобное сообщение или файл, чтобы они не открывали их и

**НЕ ОТКРЫВАЙ ПОДОЗРИТЕЛЬНЫЕ ФАЙЛЫ**

Если твое решение безопасности говорит тебе, что файл содержит или может содержать угрозу, не открывай файл. ПРОСТО УДАЛИ ЕГО.

**НЕ ОБЩАЙСЯ С НЕЗНАКОМЦАМИ**

В чатах или системах обмена мгновенными сообщениями ТЫ НИКОГДА НЕ МОЖЕШЬ БЫТЬ УВЕРЕН В ТОМ, КТО С ТОБОЙ ОБЩАЕТСЯ. Никогда не заводи дружбу с незнакомцами, и ни под какими предлогами не соглашайся на встречу с ними в реальной жизни.

**НЕ РАСПРОСТРАНЯЙ В ИНТЕРНЕТЕ ЛИЧНУЮ ИНФОРМАЦИЮ**

Никогда не отрывай свою личную информацию (твои данные, фотографии, адрес и пр.) по электронной почте и через системы обмена мгновенными сообщениями, а также никогда не публикуй такого рода информацию в блогах и форумах. Кроме того, будь внимательным при создании профилей в таких сервисах, как Facebook или MySpace. Ты никогда не должен размещать такую конфиденциальную информацию, как твой возраст и твой адрес проживания. Также рекомендуем тебе не использовать свое настоящее имя, а пользоваться псевдонимом или ником.

**ОСТЕРЕГАЙТЕСЬ ЗАМАНЧИВЫХ ПРЕДЛОЖЕНИЙ РАБОТЫ**

Как правило, никто ничего не дает просто так. Если ты получил фантастическое предложение работы от неизвестных пользователей, то НЕ ОБРАЩАЙ НА НЕГО ВНИМАНИЯ.

### Список использованных ресурсов

1. «Безопасность детей в Интернете» <http://www.microsoft.com/rus/childsafety>
2. «Безопасность дома» <http://www.microsoft.com/rus/athome/security>
3. Онлайн игра «Изучи Интернет – управляй им» [www.igra-internet.ru](http://www.igra-internet.ru)
4. «Основы безопасности детей и молодежи в Интернете» — интерактивный курс по Интернет-безопасности <https://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu.htm>
5. Понятный Интернет [www.zaprosto-internet.ru](http://www.zaprosto-internet.ru)
6. Смешарики [www.smeshariki.ru](http://www.smeshariki.ru)
7. Специализированный сайт <http://detionline.com> – основной сайт, на котором можно получить информацию:
  - Линия помощи «Дети онлайн» - телефонное и онлайн консультирование для детей и взрослых по проблемам безопасного использования интернета и мобильной связи;
  - Журнал «Дети в информационном обществе» - посвящен актуальным вопросам влияния современных инфокоммуникационных технологий на образ жизни, воспитание и личностное становление подрастающих поколений;
  - Статистика и Исследования - посвящены изучению психологии цифрового поколения России. Особое внимание уделяется проблемам безопасности детей и подростков в интернете;
  - Образовательные проекты - повышение цифровой компетентности, культуры информационной безопасности, профилактика интернет-рисков среди пользователей Рунета: детей, подростков, родителей, учителей, старшего поколения.
8. Справочник по детской безопасности в Интернете [www.google.ru/goodtoknow](http://www.google.ru/goodtoknow)
9. Фонд развития Интернет [www.fid.ru](http://www.fid.ru)
10. Центр безопасного Интернета в России [www.saferunet.ru](http://www.saferunet.ru)
11. ЮНИСЕФ (международная организация представлена более чем в 150 странах мира). Защита прав детей и другие направления <http://www.unicef.org/ceecis/ru/>