МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по организации и проведению в общеобразовательных организациях урока, посвященного Интернет безопасности детей

Данные методические рекомендации ориентированы на оказание методической помощи педагогам начального, основного общего, полного (среднего) общего образования по организации и проведению тематического урока, посвященного Интернет безопасности детей. В методических рекомендациях предлагаются концептуальные, содержательные, методические и технологические подходы к проведению урока в соответствии с возрастными особенностями детей.

Материалы методических рекомендаций также могут быть использованы для проведения по данной тематике: классного часа, урока- экскурсии или иного внеклассного занятия во внеурочной деятельности школьного педагога или в форме занятия в системе дополнительного образования.

Проблема обеспечения информационной безопасности детей в сети Интернет становится все более актуальной в связи с постоянным ростом несовершеннолетних пользователей. Число пользователей Интернета в России стремительно растет и молодеет, доля детской аудитории среди них очень велика. Для многих российских школьников Интернет становится информационной средой, без которой они не представляют себе жизнь. Вместе с тем, в Интернете содержатся огромные массивы информации, которая является запрещенной для детей, так как может нанести вред их физическому и психическому здоровью, духовному и нравственному развитию.

Согласно российскому законодательству информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

Развитие и обеспечение информационной грамотности признаны эффективной мерой противодействия посягательствам на детей с использованием сети Интернет. Формирование навыков информационной безопасности должно осуществляться на уроках информатики, обществознания, права, ОБЖ и т.д. и во внеурочной деятельности. Этому вопросу должно быть уделено достаточное внимание в программе по воспитанию и социализации обучающихся, которая является частью основной образовательной программы в соответствии с Федеральным государственным образовательным стандартом. Знания об Интернет угрозах, умения различать и предотвращать их последствия, защитить от них себя и своих близких - способствуют социализации детей.

Достичь действенных результатов в обеспечении информационной грамотности и, как следствие, - безопасности детей невозможно без привлечения родителей. Часто родители не понимают и недооценивают угрозы, которым подвергается их ребенок, находясь в сети Интернет. С родителями необходимо вести постоянную разъяснительную работу, т.к. без понимания родителями данной проблемы невозможно ее устранить силами только образовательной организации, и тем более отдельного педагога. На родительских собраниях, лекториях, встречах со специалистами нужно знакомить их с видами существующих интернет угроз, рекомендациями по обеспечению безопасности ребенка в сети Интернет дома (в зоне ответственности родителей).

Поэтому эффективное обеспечение безопасности детей при работе в сети Интернет является задачей, которую могут и должны решать вместе школа и семья, причем школа инициирует и организует это сотрудничество, просвещая родителей и обучая своих учеников.

Цель данных рекомендаций – обеспечение методический поддержки педагогов, организующих и проводящих занятия по интернет безопасности детей путем привития им навыков ответственного и безопасного поведения в среде Интернет.

# Пояснительная записка

30 октября 2014 во всех школах страны состоялся первый Единый урок безопасности в сети Интернет. Инициатором проведения урока стала временная комиссии Совета Федерации по развитию информационного общества. Данные методические рекомендации ориентированы на продолжение этой образовательной акции.

**Цель проведения занятий** - обеспечение информационной безопасности несовершеннолетних обучающихся и воспитанников путем привития им навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

# Задачи:

1. информирование обучающихся о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;
2. информирование обучающихся о способах незаконного распространения такой информации в информационно- телекоммуникационных сетях, в частности, в сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);
3. ознакомление обучающихся с международными принципами и нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;
4. обучение детей и подростков правилам ответственного и безопасного пользования услугами Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде, то есть намеренное и регулярное причинение вреда: запугивание, унижение, травля, физический и психологический террор - одним человеком или группой людей другому человеку с использованием электронных форм контакта) и буллицид (доведение до самоубийства путем психологического насилия);
5. предупреждение совершения обучающимися правонарушений с использованием информационно-телекоммуникационных технологий.

# Методические рекомендации

Формы работы с учащимися при проведении урока интернет безопасности могут быть самыми разнообразными, главное, чтобы они были увлекательными и эффективными, способствовали формированию навыков информационной безопасности, соответствовали возрасту учеников.

# Первый раздел: начальная школа - 1 - 4 классы.

В рамках урока «Интернет-безопасность» в начальных классах целесообразно ознакомить обучающихся:

* + с правилами ответственного и безопасного поведения в современной информационной среде, способах защиты от противоправных посягательств в сети Интернет и мобильной (сотовой) связи;
	+ как критически относиться к сообщениям в СМИ (в т.ч. электронных), мобильной (сотовой) связи, как отличить достоверные сведения от недостоверных, как избежать вредной и опасной для них информации, как распознать признаки злоупотребления их доверчивостью и сделать более безопасным свое общение в сети Интернет;
	+ как общаться в социальных сетях (сетевой этикет), не обижая своих виртуальных друзей, и избегать выкладывания в сеть компрометирующую информацию или оскорбительные комментарии и т.д.

Рекомендуется продемонстрировать возможности детских поисковых систем <http://kids.quintura.ru>, [http://agakids.ru](http://agakids.ru/) и детского браузера [http://www.gogul.tv](http://www.gogul.tv/), а также познакомить с детскими социальными сетями:

* <http://cyberpapa.ru/>,
* <http://interneshka.net/>,
* <http://kinderonline.ru/detskiy_portal.html>,
* <http://1dnevnik.ru/>,
* [http://www.detkino.ru](http://www.detkino.ru/).

Для отбора содержания урока могут быть использованы материалы сайта [www.detionline.com](http://www.detionline.com/) (видеоматериалы, материалы электронного журнала «Дети в информационном обществе», материалы Линии помощи), а также материалы других сайтов, содержащих информацию по безопасному использованию сети Интернет. Большое значение для эффективности урока Интернет-безопасности имеет не только содержание, но и форма его проведения.

Целесообразно использовать для 1-4 классов – урок-путешествие, урок- викторину, урок- соревнование, урок-игру, беседу.

# Полезные ссылки:

1. [http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/loputon\_ metsa.html](http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/loputon_%20metsa.html) – о правилах безопасного поведения в сети Интернет с элементами интерактива;
2. <http://www.nachalka.com/node/948>- учебное видео «Как обнаружить ложь и остаться правдивым в Интернете»;
3. <http://content-filtering.ru/aboutus/> - информационно-аналитический ресурс

«Ваш личный Интернет».

# Второй раздел: основная школа (5 - 7 и 8 - 9 классы)

В ходе урока «Интернет-безопасность» в среднем звене целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве:

* Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищѐнности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.);
* № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», (направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации,способной развить в ребѐнке порочные наклонности, сформировать у ребѐнка искажѐнную картину мира и неправильные жизненные установки.)

Важно ознакомить обучающихся с адресами помощи в случае интернет- угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Возможны следующие формы проведения урока: урок - пресс- конференция, урок-викторина, урок-соревнование, урок-презентация проектов, урок-практикум, урок-встреча с системными администраторами и т.д.

# Полезные ссылки:

1. [http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma\_ro oma.html](http://www.microsoft.com/eesti/haridus/veebivend/koomiksid/rus/ryhma_ro%20oma.html) - молодѐжная история с элементами интерактива;
2. <http://content-filtering.ru/aboutus> - информационно-аналитический ресурс

«Ваш личный Интернет»;

1. [www.icensor.ru](http://www.icensor.ru/) – Интернет-фильтр.

В качестве примера для учащихся 5-7 классов предлагается **урок - беседа «**10 правил безопасности в интернете».

В начале урока учащимся рекомендуется показать видео, где объясняются основные правила безопасности в интернете -

<http://www.youtube.com/watch?v=wVDsCpYSpeo>

Каждый современный человек, ежедневно проводит время в интернете. Но интернет — это не только источник информации и возможность общаться на расстояние, но и угроза компьютерной безопасности. Вы можете скачать из сети компьютерный вирус, Вашу учетную запись или адрес электронной почты, могут взломает злоумышленник.

Правила безопасности в интернете.

* 1. Используйте надежный пароль. Первое и главное правило сохранности Ваших данных, учетных записей, почтовой пересылки это надежный пароль! Много раз хакеры взламывали страницы в социальных сетях или почтовые адреса из-за того, что пользователь ставил простой пароль. Вы ведь не хотите, чтобы Ваши личную переписку узнал кто-то чужой? Используйте генератор паролей, чтобы получить надежный пароль.

**Генератор паролей** создается, чтобы помочь вам с придумыванием устойчивых к взлому и легко запоминающихся паролей.

Часто бывает: вы зарегистрировались где-нибудь, а там просят:

«введите пароль». В спешке приходится вводить что-нибудь типа qwerty или

12345. Последствия могут быть фатальными для вашего аккаунта: при попытке взлома такие пароли проверяются в первую очередь. Чтобы этого не происходило, надо создавать сложный пароль, желательно состоящий из букв разного регистра и содержащий цифры и другие символы.

Для создания таких паролей существуют специальные программы. Но, на наш взгляд, гораздо легче набрать наш адрес и просто выбрать понравившийся пароль.

# Советы:

* Выбирайте пароль посложнее, состоящий из символов разного регистра, с цифрами и для абсолютной надёжности - знаками препинания.
* Не используйте пароль, связанный с теми данными, которые могут быть о вас известны, например, ваше имя или дату рождения.
* Пароли, которые вы видите на экране создаются в реальном времени на вашем компьютере, поэтому исключена возможность перехвата пароля по сети. Разные посетители сайта видят разные пароли. Если вы зайдете на сайт второй раз, пароли будут другими.
* Вы можете выбрать пункт меню браузера "Файл|Сохранить как...", чтобы пользоваться генератором паролей в оффлайне.
* Генератор паролей полностью прозрачен: скачайте файл passwd.js, чтобы увидеть, как создается пароль, и убедиться в абсолютной надежности. Источник- <http://genpas.narod.ru/>
	1. Заходите в интернет с компьютера, на котором установлен фаервол или антивирус с фаерволом. Это в разы уменьшит вероятность поймать вирус или зайти на вредоносный сайт.
	2. Заведите один основной почтовый адрес и придумайте к нему сложный пароль. При регистрации на форумах, в соц. сетях и прочих сервисах Вы будете указывать его. Это необходимо если Вы забудете пароль или имя пользователя. Ни в коем случае не говорите, никому свой пароль к почте, иначе злоумышленник сможет через вашу почту получить доступ ко всем сервисам и сайтам, на которых указан Ваш почтовый адрес.
	3. Если Вы хотите скачать какой-то материал из интернета, на сайте где не нужна регистрация, но от Вас требуют ввести адрес своей электронной почты, то, скорее всего, на Ваш адрес будут высылать рекламу или спам. В таких случаях пользуйтесь одноразовыми почтовыми ящиками.
	4. Скачивайте программы либо с официальных сайтов разработчиков. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так Вы уменьшите риск скачать вирус вместо программы.
	5. Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были. В лучшем случае, Вы поможете автору сайта получить деньги, а в худшем — получите вирус. Используйте плагины для браузеров, которые отключают рекламу на сайтах.
	6. Если Вы работаете за компьютером, к которому имеют доступ другие люди (на роботе или в интернет кафе), не сохраняйте пароли в браузере. В противном случае, любой, кто имеет доступ к этому компьютеру, сможет зайти на сайт, используя Ваш пароль.
	7. Не открывайте письма от неизвестных Вам пользователей (адресов). Или письма с оповещением о выигрыше в лотереи, в которой Вы просто не участвовали.
	8. Не нажимайте на вплывающие окна, в которых написано, что Ваша учетная запись в социальной сети заблокирована. Это проделки злоумышленников! Если Вас вдруг заблокируют, Вы узнаете об этом, зайдя в эту социальную сеть, или администрация отправит Вам электронное письмо.
	9. Периодическим меняйте пароли на самых важных сайтах. Так Вы уменьшите риск взлома вашего пароля.

Пользуясь этими правилами безопасности в интернете, Вы существенно уменьшите риск получить вирус на свой компьютер или потерять учетную запись на любимом сайте

# Варианты работы с этой информацией.

1. **Обсуждение и дополнение основных 10 правил.**

Учащимся предлагается обсудить и дополнить эти основные правила с учетом уже имеющегося у них опыта работы в интернете.

# Рисуем инфографику

Учащимся предлагается нарисовать плакат в стиле современной инфографики, где размещаются основные правила безопасной работы в интернет.

<http://www.ligainternet.ru/encyclopedia-of-security/article.php?id=464>

# Третий раздел: старшая школа (10 - 11 классы).

В рамках урока «Интернет-безопасность» в старших классах целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве (см. рекомендации для проведения урока Интернет–безопасности в среднем звене).

Необходимо обратить внимание обучающихся на классификацию вредоносных информационных ресурсов:

* информация, причиняющая вред здоровью и (или) развитию детей;
* информация, запрещенная для распространения среди детей;
* информация, ограниченная для распространения среди детей определенных возрастных категорий.

На уроке необходимо затронуть следующие аспекты:

* перечень рисков, подстерегающих ребенка в сети Интернет;
* рекомендации по грамотному использованию электронной почты;
* технологии безопасного общения в средах мгновенного обмена сообщениями.

Необходимо обеспечить обучающихся:

* + инструкциями по безопасному общению в чатах;
	+ советами по профилактике и преодолению Интернет- зависимости;
	+ общими правилами по безопасности детей в сети Интернет.

Также рекомендуется рассмотреть следующие объекты, являющиеся опасными в Интернете:

* + нежелательные программы;
	+ защита личных данных;
	+ мошенничество;
	+ виртуальные «друзья»;
	+ пиратство;
	+ on-line-игры;
	+ этика;
	+ критический подход к информации.

Важно обеспечить обучающихся информацией о программном обеспечении, позволяющим осуществлять безопасную работу в сети Интернет, контентной фильтрации, а также ознакомить с адресами помощи в случае интернет- угрозы и интернет-насилия, номером всероссийского детского телефона доверия (8-800-2500015).

Возможные формы проведения урока в 9-11 классах – лекция, деловая игра, урок-презентация проектов, мозговой штурм «Интернет-безопасность», дискуссия, дебаты, встреча со специалистами медиа-сферы, системными администраторами и т.д.

# Полезные ссылки:

1. [http://www.kaspersky.ru](http://www.kaspersky.ru/) – антивирус «Лаборатория Касперского»;
2. <http://www.onlandia.org.ua/rus/>- безопасная web-зона;
3. [http://www.interneshka.net](http://www.interneshka.net/) – международный онлайн-конкурс по безопасному использованию Интернета;
4. [http://www.saferinternet.ru](http://www.saferinternet.ru/) – портал Российского Оргкомитета по безопасному использованию Интернета;
5. [http://content-filtering.ru](http://content-filtering.ru/) – Интернет СМИ «Ваш личный Интернет»;
6. [http://www.rgdb.ru](http://www.rgdb.ru/) – Российская государственная детская библиотека.

При подготовке урока, посвященного интернет безопасности школьников, можно использовать следующие материалы:

# 1. Электронные ресурсы по теме «Безопасный Интернет»

1. <http://www.saferinternet.ru/> - Безопасный Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы;
2. <http://www.saferunet.ru/> - Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействием им в отношении пользователей;
3. <http://www.fid.su/> - Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета;
4. <http://www.microsoft.com/Rus/athome/security/kids/etusivu.html> - Безопасность в Интернете. "Основы безопасности детей и молодежи вИнтернете" — интерактивный курс по Интерент-безопасности, предлагаемый российским офисом Microsoft в рамках глобальных инициатив Microsoft "Безопасность детей в Интернете" и "Партнерство в образовании". В разделе для учащихся (7-16 лет) предлагается изучить проблемы информационной безопасности посредством рассказов в картинках. В разделе для родителей и учителей содержится обновленная информация о том, как сделать Интернет для детей более безопасным, а также изложены проблемы компьютерной безопасности;
5. [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) – Club Symantec единый источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля;
6. <http://www.nachalka.com/bezopasnost> - Nachalka.com предназначен для учителей, родителей, детей, имеющих отношение к начальной школе. Статья

«Безопасность детей в Интернете». Советы учителям и родителям;

1. <http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html> - Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным;
2. <http://www.ifap.ru/library/book099.pdf> - «Безопасность детей в Интернете», компания Microsoft. Информация для родителей: памятки, советы, рекомендации;
3. <http://www.interneshka.net/children/index.phtml> - «Интернешка» - детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет;
4. <http://www.oszone.net/6213/> - OS.zone.net - Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль»;
5. <http://www.rgdb.ru/innocuous-internet>- Российская государственная детская библиотека. Ресурс для детей и родителей. Правила безопасного Интернета. Обзор программных продуктов для безопасного Интернета. Как защититься от Интернет-угроз. Ссылки на электронные ресурсы, информирующие об опасностях и защите в Сети;
6. <https://www.google.ru/safetycenter/families/start/basics/> - Центр безопасности. Краткие рекомендации помогут обеспечить безопасность членов семьи в Интернете, даже если вечно не хватает времени;
7. <https://ege.yandex.ru/security/>- Тесты по безопасности;
8. <http://www.slideshare.net/shperk/ss-47136465>- Безопасность в Интернете. Анатолий Шперх;
9. <http://shperk.ru/v-seti/prokrustovo-lozhe.html> - Прокрустово ложе для информационной картины. Как мы читаем тексты в интернете;
10. <http://shperk.ru/sovety/avtoritet.html> - Как отличить фейк от настоящего материала? Дело о летающем дьяке Крякутном;
11. <http://habrahabr.ru/company/mailru/blog/252091/> - Советы по безопасности.