# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ (ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ) О ВОЗМОЖНОСТЯХ ОРГАНИЗАЦИИ РОДИТЕЛЬСКОГО КОНТРОЛЯ ЗА ДОСТУПОМ ДЕТЕЙ В СЕТЬ ИНТЕРНЕТ

*Методические рекомендации*

## Введение

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.

Данные методические рекомендации разработаны в соответствии с Федеральным законом от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию".

Цель данных методических рекомендаций - ознакомить родителей (законных представителей) с возможностью и необходимостью организации родительского контроля за доступом детей в сеть Интернет. Методические рекомендации предназначены для родителей (законных представителей), т.к. обеспечение безопасности детей в сети Интернет 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 ответственности родителей.

## Общий анализ проблемы и необходимость защиты детей в сети Интернет

XXI век стал периодом фундаментального роста и развития различных видов массовой информации, информационных и коммуникационных технологий, глобальной сети Интернет и информационного общества. Все это оказывает самое прямое воздействие на эмоциональное и физическое развитие подрастающего поколения. Сегодня многие ученые обеспокоены негативным влиянием информационного насилия на детскую психику.

Последние годы были ознаменованы большим количеством громких инцидентов, связанных с негативными последствиями нарушений информационной безопасности детей. В России проживает почти 21 миллион детей в возрасте до 14 лет. Из них 10 миллионов активно пользуется Интернетом, что составляет 18% интернет-аудитории нашей страны.

В социальном пространстве информация распространяется быстро, благодаря техническим возможностям. Сама информация часто носит противоречивый, агрессивный и негативный характер и влияет на социально-нравственные ориентиры общественной жизни. В связи с этим, возникает проблема информационной безопасности, без решения которой не представляется возможным полноценное развитие не только личности, но и общества. Современный школьник, включенный в процесс познания, оказывается незащищенным от потоков информации. Пропаганда жестокости средствами массовой информации, возрастающая роль Интернета, отсутствие цензуры является не только социальной, но и педагогической проблемой.

Современный подросток все меньше общается в реальной жизни со сверстниками, друзьями, одноклассниками. В среднестатистической семье телевизор включен до 7-8 часов в день, а центром внимания детей является компьютер - по статистике, на школьников приходится около 3-4 часа в день, что равнозначно пяти урокам в школе. Современные гаджеты и Интернет заменили детям прогулки на улице, общение со

сверстниками и родителями. Сегодня в обществе актуальна следующая проблема – неограниченный доступ ребенка к сети Интернет.

В России 1 сентября 2012 года вступил в силу Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию".

Данный закон регулирует отношения, связанные с защитой детей от травмирующего их психику информационного воздействия, жестокости и насилия в общедоступных СМИ. К информации, запрещенной для оборота среди детей, относится информация:

- ✓ побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- ✓ способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- ✓ обосновывающая или оправдывающая допустимость насилия и (или) жестокости, либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
- ✓ отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- ✓ оправдывающая противоправное поведение;
- ✓ содержащая нецензурную брань;
- ✓ содержащая информацию порнографического характера.

Оборот такой информации не допускается среди детей в местах, доступных для детей, без применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от такой информации.

Детей и подростков, без всякого сомнения, нужно защищать от разрушающего информационного воздействия на их несформировавшуюся личность. Кроме этого, информационная продукция, запрещенная для детей, не может распространяться в предназначенных для детей образовательных организациях, детских медицинских, санаторно-курортных, физкультурно-спортивных организациях, организациях культуры, организациях отдыха и оздоровления детей или на расстоянии менее чем сто метров от границ территории этих организаций.

В Законе определяются виды информации, распространение которой среди детей определенных возрастных категорий ограничено, к ней относится информация:

- ✓ представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
- ✓ вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
- ✓ представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
- ✓ содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Распространение такой информационной продукции допускается среди детей определенных возрастных групп при соблюдении обладателем информации установленного законом порядка доступа детей к информации (в частности, при условии, что в информационной продукции содержится идея торжества добра над злом, сострадание к жертве насилия, осуждение насилия, а изображение и описание насилия,

жестокости, антиобщественных действий носит ненатуралистический, кратковременный или эпизодический характер и т.п.).

Законом устанавливается классификация информационной продукции по пяти возрастным категориям:

1. информационная продукция для детей, не достигших возраста шести лет;
2. информационная продукция для детей, достигших возраста шести лет;
3. информационная продукция для детей, достигших возраста двенадцати лет;
4. информационная продукция для детей, достигших возраста шестнадцати лет;
5. информационная продукция, запрещенная для детей.

**Контентные риски. Что это такое и как их избежать?**

Контент – это наполнение или содержание какого-либо информационного ресурса: текст, графика, музыка, видео, звуки и т.д. (например, контент интернетсайта); мобильный контент – мультимедийное наполнение, адаптированное для использования в мобильных устройствах (телефоны, смартфоны, коммуникаторы и т.д.): текст, графика, музыка, видео, игры, дополнительное программное обеспечение.

Информация нежелательного характера, которая несет в себе контентные риски, – это различные информационные ресурсы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию.

К противозаконной, неэтичной и вредоносной информации относятся:

- ✓ пропаганда насилия, жестокости и агрессии;
- ✓ разжигание расовой ненависти, нетерпимости по отношению к другим людям по национальным, социальным, групповым признакам;
- ✓ пропаганда суицида;
- ✓ пропаганда азартных игр;
- ✓ пропаганда и распространение наркотических и отравляющих веществ;
- ✓ пропаганда деятельности различных сект, неформальных молодежных движений;
- ✓ эротика и порнография;
- ✓ нецензурная лексика и т.д.

В сети Интернет такую информацию можно встретить практически везде: в социальных сетях, блогах, персональных сайтах, видеохостингах и др. Не являются исключением и мобильные сервисы.

Размещение противозаконной информации в сети Интернет преследуется по закону. Это относится в первую очередь к распространению наркотических веществ, порнографических материалов, особенно с участием несовершеннолетних, призывам к разжиганию национальной розни и экстремистским действиям. В российском законодательстве есть возможность в соответствии со статьями уголовного кодекса привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов электронных текстов и видеопродукции.

Неэтичный, противоречащий принятым в обществе нормам морали и социальным нормам, контент не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей и оказать вредоносное воздействие. Подобная информация не попадает под действие уголовного кодекса, но может оказать негативное влияние на психику человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, порнография, агрессивные онлайн-игры, азартные игры, информация о нездоровом образе жизни, принесении вреда здоровью и жизни, нецензурная брань, оскорбления и др.

Неэтичная и вредоносная информация может быть направлена на манипулирование сознанием и действиями различных групп людей. Такая информация часто бывает заманчивой и оказывает сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл происходящего и отказаться от просмотра и изучения сайтов с негативным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков – непредсказуемо; под воздействием таких сайтов может пострадать не только психика, но и физическое здоровье ребенка.
Вредоносный контент может привести к заражению компьютера вирусами и потере важных данных. Особенно опасными с этой точки зрения является просмотр через сеть Интернет тех или иных видеоматериалов. Очень многие распространители негативного контента преследуют определенную цель – заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера, получить деньги незаконным способом. Такие действия преследуются по закону в соответствии со ст. 272, 273, 274 Уголовного кодекса РФ.

**Контентная фильтрация домашнего интернета родителями.**

Для ограничения доступа детей к нежелательному, опасному контенту в настоящее время имеется возможность выбрать как коммерческое, так и свободно распространяемое программное обеспечение, сервисы, тарифные опции Интернетпровайдеров, специальные возможности антивирусных программ.
Принцип работы этих систем обычно строится на черных (запрещенных) и белых (разрешенных) списках, либо на основе фильтрации. Наиболее широкое распространение получили три алгоритма фильтрации:

1. фильтрация по ключевым словам (конкретные слова и словосочетания используются для включения блокировки веб-сайта);
2. динамическая фильтрация (содержимое запрашиваемого веб-ресурса анализируется в момент обращения, загрузка страниц ресурса в браузер блокируется, если содержимое определяется как нежелательное);
3. URL-фильтрация (запрашиваемая страница или целый домен, например, dosug.nu, могут быть определены или категорированы как нежелательный ресурс, вследствие чего доступ к таким страницам блокируется).

Лучшие в мире системы контентной фильтрации используют URLфильтрацию, основанную на анализе и категоризации Интернет-ресурсов. Такой механизм признан наиболее эффективным методом фильтрации контента.
Для ограничения доступа несовершеннолетних лиц к нежелательному или опасному контенту с настольных компьютеров и мобильных устройств можно использовать **дополнительные опции, предлагаемые большинством Интернетпровайдеров**. Для этого необходимо обратиться в службу технической поддержки провайдера (телефон данной службы обычно указан в договоре) и высказать пожелание подключения данной услуги. Далее необходимо следовать инструкциям оператора.
Можно также использовать **специализированное программное обеспечение и сервисы**. Наиболее популярные, некоммерческие версии: SkyDNS, NetPolice Child, Eyes Relax, Parental Control Bar, Norton Online Family, NetPolice Lite. Помимо этого существует возможность введения ограничения доступа к нежелательным сайтам путем установки дополнений (расширений) в Интернет-браузерах, таких как:
Internet Explorer, Mozilla FireFox, Chrome, Opera и других.
Обращаем внимание, что на домашних компьютерах также можно задействовать **антивирусные программы** с функцией «Родительский контроль», которые могут защитить ребенка от нежелательного контента. В основном это коммерческие продукты: Kaspersky Internet Security 2012, Kaspersky Crystal,

Kaspersky Internet Security 7.0, KinderGate Родительский контроль, ChildWebGuardian, Spector Pro 6.0, КиберМама, Eset Nod32 и других.
Однако существуют и бесплатные продукты, например, Avira Free Antivirus 2013 с веб-приложением Avira Free SocialShield.
Использование функции родительского контроля подробно описано в инструкциях пользователя для антивируса.
Стоит обратить особое внимание на наличие функции родительского контроля при приобретении антивирусной программы или продлении лицензии на следующий год, сообщить о вашем желании распространителю программного обеспечения. Практически все современные разработчики антивирусных пакетов имеют в своём арсенале продукты для обеспечения безопасности ребенка в сети, блокировки нежелательного и опасного контента.

**Возможности родительского контроля.**

*1. Фильтры web-сайтов*.
Слова-запреты (фильтры). Вы задаете набор ключевых слов, и если что-либо из их списка обнаруживается на web-странице, то она не открывается.
Создание белого списка. Более жесткий способ контроля, когда вы самостоятельно составляете белый список сайтов, которые может посещать ребенок.
Создание черного списка. В черном списке указываются сайты, на которые ребенку заходить запрещено. Приложение работает с базой данных, где содержатся сайты для взрослых. Крайне желательно, чтобы список регулярно обновлялся через Интернет, иначе появление новых ресурсов быстро сделает защиту неактуальной. Родители могут расширять черный список сайтов на свое усмотрение, при желании, используя автоматизированную информационную систему ведения и использования базы данных о сайтах, содержащих запрещённую к распространению в России информацию, утвержденную Постановлением Правительства Российской Федерации от 26 октября 2012 года № 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 информационнотелекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»»
(https://reestr.rublacklist.net).
*2. Ограничение времени, проводимого ребенком за компьютером*. Определяйте расписание пользования компьютером и Интернетом: выбирайте допустимое время суток и продолжительность работы. Так вам не придется прогонять ребенка от компьютера и вступать в конфликт - сеанс закончится сам собой.
*3. Установка запретов на использование детьми отдельных программ.*
Во избежание различных недоразумений родители могут ограничить список используемых ребенком программных продуктов. Большинство современных операционных систем имеют в своем составе инструмент доступа пользователей к программным продуктам, что дает возможность ограничения доступа ребенка к нежелательным программным продуктам.
*3. Управление доступом к игровым приложениям*.
Возможности родительского контроля позволяют помочь детям играть в безопасные, дружелюбные, занимательные и обучающие игры, соответствующие их возрасту. В частности, родители могут блокировать как все игры, так и только некоторые из них. Дополнительно родители могут устанавливать разрешение или запрет на доступ к отдельным играм, исходя из допустимой возрастной оценки и выбора типа содержимого.
*4. Журнал отчетов о работе ребенка за компьютером*.

С целью анализа того, чем занимался ребенок за компьютером в отсутствие взрослых, какие программы запускал, какие сайты просматривал в Интернете, с кем общался и т.д., родительский контроль ведет аудит всех действий подрастающего пользователя. В журнал записываются адреса посещенных детьми страниц Интернета. В некоторых программах журнал с отчетом можно получать по электронной почте, что очень удобно, если родитель находится вне дома, и хочет просмотреть, какие сайты посещал ребенок.

**Как помочь ребенку, если он уже столкнулся с Интернет-угрозой.**

✓ Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ним происходит. Ребенок должен Вам доверять и знать, что Вы хотите разобраться в ситуации и помочь ему, а не наказать.
✓ Постарайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка;
✓ Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети), или он попал в неприятную ситуацию (потратил Ваши или свои деньги в результате интернет-мошенничества и пр.) — постарайтесь его успокоить и вместе с ним разберитесь в ситуации — что привело к данному результату, какие неверные действия совершил сам ребенок, а где Вы не рассказали ему о правилах безопасности в Интернете;
✓ Если ситуация связана с насилием в Интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.), жестко настаивайте на избегании встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время;
✓ Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и с помощью технических средств — зайдите на страницы сайта, где был Ваш ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию — в дальнейшем это может Вам пригодиться (например, для обращения в правоохранительные органы);
✓ Если Вы не уверены в оценке серьезности произошедшего с Вашим ребенком, или ребенок недостаточно откровенен с Вами или вообще не готов идти на контакт, или Вы не знаете как поступить в той или иной ситуации — обратитесь к специалисту (телефон доверия, горячая линия и др.), где Вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организаций (МВД, МЧС, Сестры и др.)

**Сервисы, позволяющие родителям контролировать использование Интернета детьми**

✓ **КиберМама™** http://www.cybermama.ru - программа для ограничения времени работы на компьютере детей и подростков. Позволяет создавать расписание работы ребенка за компьютером и автоматически контролировать нежелательных игр и программ, блокировать доступ в Интернет. Программа проста и понятна в использовании и не требует от родителей специальных компьютерных навыков и знаний.
✓ **NetKids** - сервис, который позволяет родителям контролировать использование интернета детьми. NetKids это: Блокировка доступа к опасным сайтам; Отчеты о посещенных сайтах; Мониторинг общения в социальных сетях; Контроль загрузки фотографий и личной информации; Отчеты о поисковых запросах; Мониторинг

почтовых сообщений и записей в блогах. Вся работа осуществляется через удобный и понятный web-интерфейс.

✓ **KinderGate Родительский Контроль 1.0.** Эта программа-фильтр (www.usergate.ru) предлагает 82 категории фильтрации веб-сайтов в 5 основных уровнях доступа (по умолчанию запрещен доступ к фишинговым ресурсам, сайтам с порнографическим контентам, а также к сайтам, содержащим вредоносный код). Самый высокий уровень фильтрации подразумевает, в числе прочего, запрет прокси-серверов, сайтов знакомств. Доступно создание расширенных правил, «черных» и «белых» списков для сайтов. Можно установить ограничение скачивания видео, звуковых файлов, изображений, архивов и EXE-файлов, документов. В программе реализован модуль морфологического анализа, позволяющий блокировать веб-страницы с нецензурной лексикой. Для ограничения времени, проводимого ребенком за компьютером, предусмотрен специальный инструмент «Расписание работы». Кроме этого, доступна статистика посещенных веб-ресурсов с указанием значений входящего и исходящего трафика, а также просмотр сообщений в сетях odnoklassniki.ru и vkontakte.ru.

✓ **Интернет Цензор** – интернет-фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов. В основе работы программы лежит технология «белых списков», гарантирующая 100%-ную защиту от опасных и нежелательных материалов. Фильтр «Интернет Цензор» можно скачать бесплатно на официальном сайте. Программа содержит уникальные вручную проверенные «белые списки», включающие все безопасные сайты Рунета и основные иностранные ресурсы. Программа надежно защищена от взлома и обхода фильтрации. «Интернет Цензор» может использоваться как в домашних условиях, так и в образовательных учреждениях, библиотеках, музеях, интернет-кафе и иных местах, где возможно предоставление несовершеннолетним доступа в Интернет.

## Полезные сайты для родителей

✓ http://www.nachalka.com/bezopasnost – Безопасность детей в Интернете
✓ http://detionline.com – Дети России Онлайн. Сделаем Интернет безопаснее вместе
✓ http://www.ifap.ru/library/book099.pdf – Безопасность детей в Интернете
✓ http://www.microsoft.com/ru-ru/security/default.aspx – Центр безопасности Microsoft
✓ http://stopfraud.megafon.ru/parents – Безопасный Интернет от Мегафон
✓ http://www.fid.su/projects/journal – Фонд развития Интернет. Журнал «Дети в информационном обществе»
✓ http://www.mts.ru/help/useful_data/safety – Безопасный Интернет от МТС
✓ http://safe.beeline.ru/index.wbp – Безопасный Интернет от Билайн
✓ http://www.saferunet.ru – Центр безопасного Интернета в России
✓ http://www.friendlyrunet.ru/safety/74/index.phtml – Фонд «Дружественный Рунет»
✓ http://netpolice.ru/filters – Фильтры NetPolice
✓ http://www.socobraz.ru/index.php/Сообщество_родителей - Сообщество родителей СОЦОБРАЗ
✓ http://www.microsoft.com/ru-ru/security/family-safety/kids-social.aspx – Как помочь вашим детям более безопасно пользоваться сайтами социальных сетей?
✓ http://windows.microsoft.com/ru-RU/windows7/products/features/parental-controls – Родительский контроль в Windows 7
✓ http://play.mirchar.ru/sovety-roditelyam-po-obespecheniyu-bezopasnosti-detey.html – Консультации для родителей по обеспечению безопасности детей в Интернет
✓ http://www.internet-kontrol.ru/ –Защита детей от вредной информации в сети Интернет
✓ http://www.oszone.net/6213/ – Обеспечение безопасности детей при работе в Интернет
✓ http://wiki.saripkro.ru/index.php/Интернет-безопасность_для_родителей – Интернет-безопасность для родителей

✓ http://www.sch169.ru/doc/pam.pdf – Как защититься от интернет-угроз

## Информационная безопасность

Экспертами и членами Временной комиссии Совета Федерации по развитию информационного общества в рамках выполнения рекомендаций парламентских слушаний "Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве", которые прошли в Совете Федерации 17 апреля 2017 г., были разработаны методические рекомендации о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети "Интернет" (далее - методические рекомендации). В данных методических рекомендациях содержится памятка для родителей об информационной безопасности детей и памятка для обучающихся об информационной безопасности:

### Памятка для родителей об информационной безопасности детей

Определение термина "информационная безопасность детей" содержится в Федеральном законе N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию", регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону "информационная безопасность детей" - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. В силу Федерального закона N 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;
2. информация, распространение которой ограничено среди детей определенных возрастных категорий.
3. К информации, запрещенной для распространения среди детей, относится:
4. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;
5. способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
6. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
7. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
8. оправдывающая противоправное поведение;
9. содержащая нецензурную брань;
10. содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;

2. вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
4. содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

**Общие правила для родителей**

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.
2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)
4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).
5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

**Возраст от 7 до 8 лет**

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т.е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

*Советы по безопасности в сети Интернет для детей 7 - 8 лет*

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.
3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
4. Используйте специальные детские поисковые машины.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
9. Научите детей не загружать файлы, программы или музыку без вашего согласия.
10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
11. В "белый" список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
13. Не делайте "табу" из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты "для взрослых".
14. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

**Возраст детей от 9 до 12 лет**

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

*Советы по безопасности для детей от 9 до 12 лет*

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.
3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.
4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.
7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
8. Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними.
9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.
12. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.
13. Расскажите детям о порнографии в Интернете.

14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

**Возраст детей от 13 до 17 лет**

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок "для взрослых". Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в "свободное плавание" по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности - соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

*Советы по безопасности в этом возрасте от 13 до 17 лет*

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов ("черный список"), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).
2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.
3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование моделируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
11. Приучите себя знакомиться с сайтами, которые посещают подростки.
12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.

13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.
Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.

**Памятка для обучающихся об информационной безопасности**

**НЕЛЬЗЯ**

1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей);
2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;
3. Грубить, придираться, оказывать давление - вести себя невежливо и агрессивно;
4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;
5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

**ОСТОРОЖНО**

1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам;
2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;
3. Незаконное копирование файлов в Интернете - воровство;
4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;
5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

**МОЖНО**

1. Уважай других пользователей;
2. Пользуешься Интернет-источником - делай ссылку на него;
3. Открывай только те ссылки, в которых уверен;
4. Общаться за помощью взрослым - родители, опекуны и администрация сайтов всегда помогут;
5. Пройди обучение на сайте "Сетевичок" и получи паспорт цифрового гражданина!

С каждым годом молодежи в интернете становиться больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

**Компьютерные вирусы**

*Компьютерный вирус* - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.
*Методы защиты от вредоносных программ:*

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;
2. Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;
6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

**Сети WI-FI**

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд "WECA", что обозначало словосочетание "Wireless Fidelity", который переводится как "беспроводная точность".
До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура "Wi-Fi". Такое название было дано с намеком на стандарт высшей звуковой техники Hi-Fi, что в переводе означает "высокая точность".
Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.
*Советы по безопасности работы в общедоступных сетях Wi-fi:*
1. Не передавай свою личную информацию через общедоступные Wi-Fi сети.
Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
3. При использовании Wi-Fi отключи функцию "Общий доступ к файлам и принтерам". Данная функция закрыта по умолчанию, однако некоторые
пользователи активируют ее для удобства использования в работе или учебе;
4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно "https://";
6. В мобильном телефоне отключи функцию "Подключение к Wi-Fi
автоматически". Не допускай автоматического подключения устройства к сетям WiFi без твоего согласия.

**Социальные сети**

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.
*Основные советы по безопасности в социальных сетях:*
1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

**Электронные деньги**

*Электронные деньги* - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.
Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.
В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.
Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).
*Основные советы по безопасной работе с электронными деньгами:*
1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли - это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;; 4. Не вводи свои личные данные на сайтах, которым не доверяешь.

**Электронная почта**

Электронная почта - это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.
*Основные советы по безопасной работе с электронной почтой:*
1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать "музыкальный_фанат@" или "рок2013" вместо "тема13";

3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на "Выйти".

**Кибербуллинг или виртуальное издевательство**

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

*Основные советы по борьбе с кибербуллингом:*

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
2. Управляй своей киберрепутацией;
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
5. Соблюдай свою виртуальную честь смолоду;
6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

**Мобильный телефон**

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

*Основные советы для безопасности мобильного телефона:*

✓ Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;

✓ Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
✓ Необходимо обновлять операционную систему твоего смартфона;
✓ Используй антивирусные программы для мобильных телефонов;
✓ Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
✓ После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
✓ Периодически проверяй, какие платные услуги активированы на твоем номере;
✓ Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
✓ Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

## Online игры

Современные онлайн-игры - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.
Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.
В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.
*Основные советы по безопасности твоего игрового аккаунта:*
1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
3. Не указывай личную информацию в профайле игры;
4. Уважай других участников по игре;
5. Не устанавливай неофициальные патчи и моды;
6. Используй сложные и разные пароли;
7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

## Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься "любимым" делом.
Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей. На английском языке phishing читается как фишинг (от fishing - рыбная ловля, password - пароль).
*Основные советы по борьбе с фишингом:*
1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;

2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;
7. Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

## Цифровая репутация

*Цифровая репутация* - это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. "Цифровая репутация" - это твой имидж, который формируется из информации о тебе в интернете.
Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.
Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.
Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.
*Основные советы по защите цифровой репутации:*
1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только "для друзей";
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

## Авторское право

Современные школьники - активные пользователи цифрового пространства.
Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин "интеллектуальная собственность" относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему

справедливые возможности заработать на результатах своего труда, получить известность и признание.

Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование "пиратского" программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.

**Список использованной литературы:**


1. О защите детей от информации, причиняющей вред их здоровью и развитию: федеральный закон от 29.12.2010 N 436-ФЗ [Электронный ресурс] // СПС Консультант Плюс (дата обращения: 13.07.2018).
2. Гендина Н. И. Основы информационной культуры школьника: учебнометодический комплекс для учащихся 5-7-х классов общеобразовательных организаций / Н. И. Гендина, Е. В. Косолапова. – М.: РШБА, 2017. – 432 с.
3. Безопасный интернет – детям! Полезные советы для тебя и твоих друзей [Электронный ресурс]: сайт // Министерство внутренних дел Российской Федерации.
4. Линия помощи «Дети онлайн» [Электронный ресурс]: сайт. – Режим доступа: http://detionline.com/.
5. Методические рекомендации по контролю за использованием несовершеннолетними сети Интернет во внеучебное время.Методические рекомендации / Сост. О.В. Пикулик, С.В. Синаторов. – Саратов: ГАОУ ДПО «СарИПКиПРО». – 2012. – 39 с.
6. Правила поведения учащихся в современной информационной среде [Электронный ресурс]: сайт. Режим доступа: http://5319sc5.edusite.ru/DswMedia/ravila_povedenija_v_inv_srede.pdf
7. Сайт «Безопасность детей» Онлайн Энциклопедия
8. Журнал «Дети в информационном обществе» - Режим доступа: http://detionline.com/journal/numbers/28