Данилова Зинаида Феликсовна

МБУ ДО "Центр внешкольной работы

 Промышленного района г. Ставрополя»

Педагог-организатор

**Методическая разработка по теме**

**«Усиление родительского контроля деятельности несовершеннолетних в сети ИНТЕРНЕТ»**



*В рамках мероприятий по обеспечению антитеррористической безопасности, противодействию религиозному и национальному экстремизму, проводимых в муниципальном бюджетном учреждении дополнительного образования «Центр внешкольной работы Промышленного района города Ставрополя» в 2020-2021 учебном году, был подготовлен материал и проведена беседа с родительской общественность по проблеме «Усиление родительского контроля деятельности несовершеннолетних в сети Интернет».*

# *Информационная безопасность детей* - это состояние защищённости от вреда, который может причинить информационная продукция. Страдает физическое, психическое, духовное, нравственное развитие детей.

# Информационную продукцию классифицируют по категориям: для детей, которые не достигли шести лет; для детей от шести лет; от двенадцати лет; от шестнадцати лет и информационная продукция, которая запрещена для детей.

В соответствии со ст. 5 Федерального Закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», к информации, запрещенной для распространения среди детей, относится информация:

1. - побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
2. - 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;
3. - 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;
4. - отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
5. - оправдывающая противоправное поведение;
6. - содержащая нецензурную брань;
7. - содержащая информацию порнографического характера.

Современный мир - высокотехнологичный, высокоразвитый мир. В современном мире очень большой процент детей остается без ежечасного родительского внимания. Окружающая «компьютеризированная» среда таит в себе опасность возникновения интернет-зависимости, вовлечения несовершеннолетних через социальные сети в преступную деятельность и т.д.

В такой ситуации важно вовремя «заметить», обратить внимание на таких детей. Чтобы такие дети не оставались вне поля зрения близких им людей, родные должны быть готовы оказать соответствующую помощь таким детям. А для этого сами родители должны иметь соответствующую подготовку. И в этом вопросе образовательные учреждения могут оказать помощь родителям в форме проведения родительских собраний, лекториев по вопросам обеспечения безопасности детей в интернет-пространстве, недопущения вовлечения несовершеннолетних через социальные сети в преступную деятельность.

Такой опасности подвержены люди любой возрастной и социальной категории, вследствие того, что интернетная сеть, на сегодняшний день, является кладезью информации и плохой, и хорошей, той информационной средой из которой дети черпают и полезную информацию в образовательных целях, но одновременно получают и информацию, которая является запрещенной для детей, так как может нанести вред их физическому и психическому здоровью, духовному и нравственному развитию.

В целях защиты детей особо важную роль имеет активная позиция, в первую очередь, родителей. Точно также как могут обучающиеся использовать возможности интернет-сети в учебных целях так же они могут быть вовлечены в интернет-преступность, хулиганство, вредительство и т.д. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям. В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания.

Исходя из вышеизложенного, и педагогам и родителям нужно уделять повышенное внимание вопросу обеспечения безопасности детей в Интернете.

Для защиты детей можно использовать некоторые ***правила*:**

1. Установить вместе с детьми четкие правила посещения сайтов. Определить, какие сайты они могут посещать, какие – нельзя посещать. Объяснить детям, что такое расизм, фашизм, межнациональная и религиозная вражда. Несмотря на то, что некоторые подобные материалы можно заблокировать с помощью специальных программных фильтров, не стоит надеяться на то, что удастся отфильтровать все подобные сайты. Выберите сайты, которые можно посещать вашему ребенку, и заблокируйте доступ к неподходящим материалам. Настройте параметры безопасности вашего компьютера.
2. Хорошей может стать идея разработки «семейного совместного документа» - соглашения по использованию сети Интернет, в котором можно описать права и обязанности каждого члена семьи в сфере пользования Интернет-пространством.
3. Помощь детям в выборе правильного регистрационного имени и пароля, не содержащей никакой личной информации.
4. Объяснение детям о необходимости защиты собственной конфиденциальности в сети Интернет. Т.е. о том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки, а также пересылать интернет-знакомым свои фотографии.
5. Старайтесь регулярно проверять список контактов своих детей, чтобы знать с кем контактирует в Интернете ваш ребенок, чтобы убедиться, что они лично знают всех, с кем они общаются. Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу.
6. Не позволяйте вашему ребенку встречаться с онлайн-знакомыми без вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на том, чтобы сопроводить ребенка на эту встречу. Всегда интересуйтесь тем, куда и с кем ходит ваш ребенок.

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг, кибербуллинг и др.). Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они могут обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы.

В тех случаях, когда знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка, с целью войти в доверие к ребенку, узнать личную информацию и договориться о встрече, для установления дружеских отношений с ребенком с целью вступления в сексуальный контакт, специалисты используют специальный термин *«груминг».*

Используется также и другой термин **-** *кибербуллинг* **-** преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство, социальное бойкотирование с помощью различных интернет-сервисов.

Для того чтобы предупредить кибербуллинг нужно научить детей, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов - читать грубости также неприятно, как и слышать, правильно реагировать на обидные слова или действия других пользователей. Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз. Старайтесь следить за тем, что ваш ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Родителям важно вовремя заметить, что ребенок стал жертвой кибербуллинга, для того чтобы обезопасить:

* Беспокойное поведение. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии. Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением.
* Неприязнь к Интернету. Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.
* Нервозность при получении новых сообщений. Негативная реакция ребенка на звук электронного письма должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Объясняйте, чтобы дети уважали собственность других в Интернете, что незаконное копирование и использование чужой работы - текста, музыки, компьютерных игр и других программ - является кражей чужой интеллектуальной собственности.

Обращайте внимание, сколько времени проводят ваши дети в Интернете, чтобы вовремя заметить признаки возникающей интернет-зависимости.

Предвестниками «интернет-зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство») являются: навязчивое стремление постоянно проверять электронную почту; предвкушение следующего сеанса онлайн; увеличение времени, проводимого онлайн; увеличение количества денег, расходуемых онлайн. Если Вы считаете, что ваши дети, страдают от чрезмерной увлеченности компьютером, что наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой (например, педагогам-психологам, психологам). Они помогут построить диалог и убедить вашего ребенка признать существование проблемы и согласиться получить помощь.

Например, на сайте **«Дети онлайн»** [**www.detionline.com**](http://www.detionline.com/) открыта линия телефонного онлайн-консультирования, которая оказывает психологическую и информационную поддержку детям и подросткам, столкнувшимся с различными проблемами в Интернете.

На линии помощи «Дети Онлайн» работают психологи Фонда Развития Интернет и выпускники факультета психологии МГУ имени М.В. Ломоносова, которые оказывают психологическую и информационную помощь по проблемам безопасного использования Интернета. Целевая аудитория - дети, подростки, родители и работники образовательных и воспитательных учреждений. Служба Линия помощи «Дети Онлайн» включена в базу единого федерального номера телефона доверия для детей, подростков и их родителей. Обратиться на Линию помощи можно по телефону **8-800-25-000-15**, бесплатно позвонив из любой точки страны, либо по электронной почте: [**helpline@detionline.com.**](mailto:helpline@detionline.com) Звонки принимаются в рабочие дни с 9.00 до 18.00 по московскому времени.

* Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете - правда. Приучите их спрашивать о том, в чем они не уверены.
* Следует объяснить детям, что нужно относиться к полученным из Интернет материалам осторожно и критически, так как опубликовать информацию в Интернет может абсолютно любой человек.
* Родители могут контролировать деятельность детей в Интернете с помощью современных программ, которые могут фильтровать вредное содержимое, выяснить, какие сайты посещает ребенок, и с какой целью. Однако открытое, честное общение всегда предпочтительнее вторжения в личную жизнь.
* Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми. Если ваш ребенок ведет интернет-дневник, регулярно посещайте его. Помните, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются дети за компьютером. Будьте внимательны к вашим детям!

# Рекомендации по безопасному использованию сети Интернет с учетом возрастных и физиологических особенностей несовершеннолетних

Как показали исследования, проводимые в сети Интернет, наиболее растущим сегментом пользователей Интернет являются дошкольники. В этом возрасте взрослые будут играть определяющую роль в обучении детей безопасному использованию Интернет.

# Возраст от 5 до 6 лет.

Для детей такого возраста характерен положительный взгляд на мир. Они гордятся своим умением читать и считать, а также любят делиться своими идеями. Несмотря на то, что дети в этом возрасте очень способны в использовании игр и работе с мышью, все же они сильно зависят от вас при поиске детских сайтов.

# *Советы по безопасности в этом возрасте:*

* В таком возрасте желательно работать в Интернет только в присутствии родителей.
* Обязательно объясните вашему ребенку, что общение в Интернет - это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира.
* Добавьте детские сайты в раздел Избранное. Создайте там папку для сайтов, которые посещают ваши дети.
* Используйте средства блокирования нежелательного контента как дополнение к стандартной функции «Родительский контроль».
* Научите вашего ребенка никогда не выдавать в Интернет информацию о себе и своей семье.
* Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с работой в сети Интернет.

# Возраст от 7 до 8 лет.

Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате, находясь в Интернете, ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому в данном возрасте особенно полезны будут те отчеты, которые вам предоставит функция «Родительский контроль» или то, что вы сможете увидеть во временных файлах по использованию Интернета (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системеWindows).

В результате, у вашего ребенка не будет ощущения, что вы глядите ему через плечо на экран, однако, вы будете по-прежнему знать, какие сайты посещает ваш ребенок. Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернет. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты следует заметить, что в данном возрасте рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку. Помочь вам запретить ребенку использовать внешние бесплатные ящики сможет такое программное обеспечение, как Kaspersky Internet Security версии 7.0 со встроенным родительским контролем.

# *Советы по безопасности в этом возрасте:*

* Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
* 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.
* Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый «белый» список Интернета с помощью средства «Родительский контроль». В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
* Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
* Используйте средства блокирования нежелательного контента как дополнение к стандартной функции «Родительский контроль».
* Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
* Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
* Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
* Научите детей не загружать файлы, программы или музыку без вашего согласия.
* Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы. Подробнее о таких фильтрах вы можете узнать, например, по адресу: [http://www.microsoft.com/rus/athome/security/email/fightspam.mspx.](http://www.microsoft.com/rus/athome/security/email/fightspam.mspx)
* Не разрешайте детям использовать службы мгновенного обмена сообщениями;
* Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.
* Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых».
* Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и 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.

# Возраст 9-12 лет.

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

# *Советы по безопасности в этом возрасте:*

* Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
* 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.
* Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
* Используйте средства блокирования нежелательного контента как дополнение к стандартной функции «Родительский контроль».
* Не забывайте беседовать с детьми об их друзьях в Интернете.
* Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
* Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
* 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 сети Интернет.
* Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
* Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.
* Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с пользованием Интернетом. Оставайтесь спокойными и 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.
* Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
* Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

# Возраст 13-17 лет.

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, особенно важно 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. 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 Интернет.

# *Советы по безопасности в этом возрасте:*

* Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернете. Часы работы в Интернет могут быть легко настроены при помощи средств «Родительский контроль» Kaspersky Internet Security 7.0.
* Компьютер с подключением к Интернет должен находиться в общей комнате.
* 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.
* Используйте средства блокирования нежелательного контента как дополнение к стандартной функции «Родительский контроль».
* Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование моделируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
* Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из Интернета. - 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 Интернет.
* Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
* Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
* 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.
* Приучите себя знакомиться с сайтами, которые посещают подростки.
* Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
* Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что по закону дети не могут играть в эти игры. Обеспечивать родительский контроль в Интернете можно с помощью различного программного обеспечения.

В качестве дополнительных средств контентной фильтрации я предлагаю использовать следующий программный продукт:***Интернет Цензор.*** Программа «Интернет Цензор» предназначена для предотвращения посещения сайтов, противоречащих законодательству РФ, а также любых сайтов деструктивной направленности лицами моложе 18 лет. Программа обеспечивает родителям полный контроль за деятельностью в сети их детей. Основной функцией «Интернет Цензора» является блокирование доступа к интернет- сайтам, которые не входят в разрешенную белую базу сайтов, составленную и предложенную компанией-разработчиком, а также в список, составленный самими родителями. База сайтов, разрешённых компанией к посещению, постоянно обновляется. Обновления скачиваются программой с сервера компании автоматически раз в день. В дополнение к этому пользователь может воспользоваться кнопкой «Проверить обновления» в интерфейсе программы.

Белый список в интерфейсе программы родители заполняют самостоятельно после скачивания и установки программы на домашний компьютер. Этот список для программы важнее, чем база компании-разработчика. При работе «Интернет Цензор» сначала обращается к «родительскому» списку разрешённых адресов. Кроме того, владелец программы может создать чёрный список ресурсов и запретить посещение сайтов, доступ к которым разрешён компанией-разработчиком. Таким образом, ваши запреты или разрешения будут приниматься во внимание в первую очередь.

При включении режима фильтрации вместо запрещенных к просмотру ресурсов ваш браузер будет показывать страницу-заменитель. В случае, если на разрешенном ресурсе есть нежелательные элементы, замене подвергнется лишь часть страницы – та, что содержит части, не допущенные к просмотру.

Уважаемые родители, помните, что контроль за поведением детей в интернете - это важная обязанность. Если вам необходима для этого техническая помощь, обратитесь за ней к более информационно грамотным друзьям, или к сотрудникам Ростелекома, или по многочисленным объявлениям услуг компьютерных мастеров.

**ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ**

Родитель, помни, что несовершеннолетние наиболее подвержены опасностям сети Интернет, а родители несут ответственность за своих детей.

**ЧЕМ ОПАСЕН ИНТЕРНЕТ ДЛЯ ДЕТЕЙ?**

В интернете можно найти информацию и иллюстрации практически на любую тему. Необходимо обеспечить защиту детей от контактов в интернете с нежелательными людьми, от знакомства с материалами недетской тематики или просто опасными для детской психики, от вредоносных программ и интернет-атак.

Так как дети по своей наивности, открытости и неопытности, не способны распознать опасность, а любознательность детей делает их крайне уязвимыми в интернет-пространстве, об их безопасности, в первую очередь, должны беспокоиться родители.

**ОПАСНОСТЬ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ МОЖНО РАЗДЕЛИТЬ НА ТРИ ВИДА:**

1. Доступная для детей негативная информация.
2. Противоправные и социально-опасные действия самого ребенка.
3. Целенаправленные действия третьих лиц в отношении ребенка.

*Наиболее опасные* в сервисах интернет-общения:

1. Педофилы, для которых дети становятся объектами развратных действий и преступлений против половой неприкосновенности.
2. Сектанты, навязывающие нетрадиционные, асоциальные отношения и ценности.
3. Интернет-аферисты (мошенники, онлайн-игроки и пр.), прививающие детям склонность к азартным играм, выманивающие у детей конфиденциальную информацию о родителях и уровне материальной обеспеченности семьи, а также ставящие ребенка в материальную и иную зависимость.

Кибербуллеры унижают и «травят детей». Кибербуллинг набирает обороты как со стороны злоумышленников, так и среди подростковых социальных групп.

Среди детей приобрели моду суицид и игры со смертью, селфхарм (самоповреждение), анорексия, экстремальные селфи, а также различные радикальные движения: против родителей и семьи, школ и педагогов и прочее.

Более половины детей сталкивается с интернет-угрозами, не ставя в известность родителей, в ряде случаев, боясь их, в ряде случаев, не доверяя.

Как правило, родители не уделяют большого значения интернет-безопасности и интернет-воспитанию детей.

В интерактивном мире дети могут быть так же беззащитны, как и в реальном. Поэтому важно сделать все возможное, чтобы защитить их.

**РЕКОМЕНДАЦИИ:**

1. Расположить ребенка к доверительному диалогу по вопросам интернет-безопасности. Объяснить, что Интернет является не только надежным источником информации, но и опасным собеседником а доверять следует родителям, педагогам и лучшим друзьям.

2. Установить с ребенком «правила» работы с компьютером и гаджетами, временные ограничения, определить ресурсы, которые можно и нужно посещать. Объяснить, что Интернет, в первую очередь, является средством развития и обучения, и только второстепенно — развлечений и общения. Желательно договориться, что новые игры и программы будут устанавливаться совместно с родителями.

3. Ввести ограничения по использованию гаджетов. Дошкольникам, а также ученикам младших классов мобильный Интернет не нужен в повседневной жизни.

4. Запретить общение с незнакомыми людьми. Эта мера должна восприниматься так же, как и запрет общения с незнакомыми на улице!

5. Привить культуру поведения в IT-пространстве, постоянно осуществляя интернет-воспитание ребенка.

6. Надлежащим образом настроить компьютерную технику ребенка. Использовать контент-фильтры, затрудняющие посещение определенных видов ресурсов на уровне оператора связи и на уровне операционной системы. Контент-фильтрация не всегда эффективна, в частности, из-за того, что не ко всем сайтам закрыт доступ, а соцсети, онлайн-игры, переписка и иная активность ребенка остаются в стороне!

7. Контролировать деятельность ребенка с компьютером и гаджетами, в частности, при помощи средств родительского контроля. При этом, ребенку нужно объяснить, что Вы это делаете для того, чтобы предотвратить опасность, и что на это имеете полное право. Знайте, что дети способны удалять историю переписки и посещения сайтов, существует множество средств родительского контроля, которые необходимо использовать для того, чтобы обезопасить своего ребенка.

**НЕСКОЛЬКО СОВЕТОВ ПО ОБЕСПЕЧЕНИЮ ИНТЕРНЕТ-БЕЗОПАСНОСТИ:**

Расскажите своим детям о потенциальных угрозах, с которыми они могут столкнуться в интернете.

Если возможно, поставьте компьютер в общей комнате.

Постарайтесь проводить время за компьютером всей семьей.

Попросите детей рассказывать обо всем, что вызывает у них неприятные чувства или дискомфорт при посещении интернета.

Ограничьте материалы, доступные детям через компьютер.

Вам помогут сделать это антивирусные программы и сами браузеры.

Так например, Internet Explorer включает компонент Content Advisor, а **Kaspersky Internet Security** компонент «Родительский контроль».

Объясните детям, что им разрешено, а что запрещено делать в интернете:

* регистрироваться в социальных сетях и на других сайтах;
* совершать покупки в интернете;
* скачивать музыку, игры и другой контент в интернете;
* использовать программы мгновенного обмена сообщениями;
* посещать чаты.

Если детям разрешено использовать программы мгновенного обмена сообщениями или посещать интернет-чаты, расскажите им об опасностях общения или отправки сообщений людям, которых они не знают и которым не доверяют.

Установите надежную антивирусную программу, способную защитить компьютер от вредоносных программ и хакерских атак. Многие продукты для обеспечения безопасности в интернете сочетают в себе возможности антивирусной защиты и расширенные функции родительского контроля, которые помогают защитить детей, когда те находятся в интернете.

Контроль переписки через социальные сети с помощью функции «Родительский контроль» позволяет:

* сформировать списки контактов, переписка с которыми будет разрешена или запрещена.
* задать ключевые слова, наличие которых будет проверяться в сообщениях.
* указать личную информацию, пересылка которой будет запрещена.

Если переписка с контактом запрещена, то все сообщения, адресованные этому контакту или полученные от него, будут блокироваться. Информация о заблокированных сообщениях, а также о наличии ключевых слов в сообщениях выводится в отчет. Для каждой учетной записи пользователя компьютера можно посмотреть краткую статистику переписки через социальные сети, а также подробный отчет о событиях.

**ОБРАТИТЕ ВНИМАНИЕ НА ПОДОЗРИТЕЛЬНЫЕ ХЕШ-ТЕГИ:**

#f53 #f57 #f58 #d28 #морекитов #тихийдом #хочувигру #млечныйпуть #хочувигру #хочу\_в\_игру #ждуинструкцию #млечныйпуть

**ЕСЛИ НА КОМПЮТЕРЕ И МОБИЛЬНОМ УСТРОЙСТВЕ ВАШЕГО РЕБЕНКА НЕ УСТАНОВЛЕН РОДИТЕЛЬСКИЙ КОНТРОЛЬ, НА ЧТО СТОИТ ОБРАТИТЬ ВНИМАНИЕ:**

1. Подросток не высыпается, даже если рано ложится спать - проследите, спит ли он в ранние утренние часы.

2. Рисует китов, бабочек, единорогов.

3. Состоит в группах, содержащих в названии следующее: «Киты плывут вверх», «Разбуди меня в 4.20», «f57», «f58», «Тихийдом», «Рина», «Няпока», «Море китов», «50 дней до моего...», «домкитов», «млечныйпуть», «150звёзд», «ff33», «d28», «хочувигру».

4. Закрыл в Контакте доступ к подробной информации, в переписке с друзьями (на личной стене) есть фразы "разбуди меня в 4.20", "я в игре". И совсем уж страшно, если на стене появляются цифры, начиная от 50 и меньше.

5. Переписывается в вайбере (и др. мессенджерах) с незнакомыми людьми, которые дают странные распоряжения.

**ПОМНИТЕ!**

**САМОЕ ДОРОГОЕ, ЧТО ЕСТЬ В НАШЕЙ ЖИЗНИ**

**– ЭТО НАШИ ДЕТИ!**



***Использованные документы:***

1. Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребёнка в Российской Федерации»
2. ст. 4 Закона РФ от 27.12.1991 № 2124-1 «О средствах массовой информации» (запрет использования СМИ для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости;
3. ст. 5 Федерального закона от 13.03.2006 № 38-ФЗ «О рекламе»
4. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
5. Федеральный закон № 139-ФЗ от 28 июля 2012 года «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет».
6. Постановление Государственной Думы Федерального собрания РФ от 24.11.2000 № 843-III ГД «О государственной политике в области телевизионного вещания и радиовещания» (с требованием о принятии мер по формированию условий развития телевизионного вещания и радиовещания с учётом интересов детей и молодёжи, защите их от информации, оказывающей негативное воздействие на нравственное, физическое, психическое здоровье детей и молодёжи);
7. Письмо Роспотребнадзора от 17.09.2008 № 01/10237-8-32 «О мерах, направленных на нераспространение информации, наносящей вред здоровью, нравственному и духовному развитию детей и подростков».

***Интернет-ресурсы:***

1. О линии помощи «Дети онлайн» - <http://www.fid.su/projects/detionline>
2. Памятка для родителей - <https://infourok.ru/pamyatka-roditelskiy-kontrol-v-seti-internet-3278891.html>
3. «Родительский контроль» Kaspersky Internet Security 7.0. – <https://www.kaspersky.ru/safe-kids?campaign=kl-ru_yadirectps-ksk_acq_ona_sem_bra_onl_b2c_ya_lnk_______&redef=1&referer1=kl-ru_yadirectps-ksk&referer2=kl-ru_yadirectps-ksk_acq_ona_sem_bra_onl_b2c_ya_lnk_______&ksid=747f42b4-d726-4a80-87fa-d06aa9d950e2&ksprof_id=426&ksaffcode=cr6301492598&ksdevice=desktop&kschadid=6301492598&kschname=yandex&kpid=Yandex%7c37250098%7c3488073853%7c6301492598%7ckwd-14378651225%7cdesktop&yclid=1299088063407620990>