**Содержание:**


# Введение

Дети каждый день смотрят телевизор часами, но все больше и больше времени они проводят в Интернете, используя навыки, которым они быстро обучаются у своих сверстников. Дети используют интерактивные средства для игры, общения, написания блогов в Интернете, прослушивания музыки, размещения собственных фотографий и поиска других людей для общения в интерактивном режиме. Поскольку существует реальное несоответствие между грамотностью в отношении информационных средств между детьми и взрослыми, большинство взрослых мало знают о том, что делают их дети в Интернете или как они это делают. Виртуальный мир может как предложить детям возможности, так и расставить ловушки. Использование электронных, цифровых и интерактивных информационных средств оказывает значительное положительное воздействие на развитие детей: это увлекательно, это обучает и социализирует. Однако это также несет потенциальную возможность вреда для детей и сообществ, в зависимости от того, как осуществляется использование.

# Проблема безопасности сети Интернет для детей.

Сегодня трудно представить себе жизнь без компьютера. В настоящее время Интернет стал неотъемлемой частью повседневной жизни, бизнеса, политики, науки и образования. Стремительное развитие и распространение информационных технологий приводит к тому, что постоянно увеличивается число детей, которые используют компьютер в школе, на уроках информатики и для подготовки домашних заданий, а также проводят за ним часть своего свободного времени.

Использование Интернета дома и в образовательных учреждениях позволяет повысить эффективность обучения, а также получать свежие новости в интересующей области не только родителям и педагогам, но и учащимся, в том

числе школьникам.

Однако бурное развитие Интернета несет также существенные издержки. Современная научно - образовательная информационная среда характеризуется большим количеством образовательных ресурсов с неструктурированной и мало того, еще и не всегда достоверной информацией. Объем подобных ресурсов растет в геометрической прогрессии. Таким образом, неуклонно возрастает потребность в обеспечении эффективного использования информационных научно - образовательных ресурсов. Кроме того, наряду с полезной и необходимой информацией пользователи сталкиваются с ресурсами, содержащими неэтичный и агрессивный материал. Терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры материала, с которым могут соприкоснуться дети и подростки.

1 сентября 2012 года вступил в силу ФЕДЕРАЛЬНЫЙ ЗАКОН N 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию".

Он направлен на защиту детей от разрушительного, травмирующего их психику информационного воздействия, а также от информации, способной развить в ребенке порочные наклонности.

Как ожидалось, закон должен был способствовать формированию гармоничной и психологически устойчивой личности каждого ребенка, бережному и грамотному воспитанию детей на идеях добра и справедливости.

Бесконтрольное распространение нежелательной информации противоречит целям образования и воспитания молодежи. Однако, полностью отказываться от благ информационных технологий бессмысленно.

## 1.2 Классификация интернет – угроз

Попробуем разобраться, какие проблемы интерне-угрозы возникают у детей при использовании интернета (таб.1).

**Таблица №1. Классификация интернет-угроз.**

| *Классификация интернет – угроз* | *Описание классификации интернет-угроз* |
|---|---|

| | |
|---|---|
| Контентные риски. | Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент. |
| Неподобающий контент | В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анарексии и булимии, суицида, азартных игр и наркотических веществ. |
| Незаконный контент | В зависимости от законодательства страны разные материалы могут считаться нелегальными. В большинстве стран запрещены: материалы сексуального характера с участием детей и подростков, порнографический контент, описания насилия, в том числе сексуального, экстремизм и разжигание расовой ненависти. |
| Электронная безопасность | Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн - мошенничество и спам. |
| Вредоносные программы | Вредоносные программы - это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы - шпионы, нежелательное рекламное ПО и различные формы вредоносных кодов.<br><br>- Вредоносное ПО - Рекламное ПО - Шпионское ПО - Браузерный эксплойт |

| | |
|---|---|
| Спам | Спам - это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет - трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы. |
| Кибермошенничество | Кибермошенничество - это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким - либо образом использует личную информацию пользователя, с целью получить материальную прибыль. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг. |
| Коммуникационные риски | Коммуникационные риски связаны с межличностными отношениями интернет - пользователей и включают в себя контакты педофилов с детьми и киберпреследования. |

| | |
|---|---|
| Рекламные программы | Рекламные программы - нежелательное программное обеспечение, содержащее рекламу. Рекламные программы поставляется в сочетании с программными продуктами, как правило, бесплатными или условно-бесплатными. В дальнейшем, при использовании программного продукта пользователю принудительно показывается реклама, которая может содержать нежелательную информацию. Кроме того, бесконтрольно всплывающие рекламные окна раздражают и, в некоторых случаях, снижают производительность системы. Также, рекламные системы могут собирать конфиденциальную информацию о компьютере и пользователе, такую как IP-адрес компьютера, список часто посещаемых пользователем сайтов, поисковые запросы, прочие данные, которые можно использовать при проведении последующих рекламных кампаний. |
| Вредоносное программы | Вредоносные программы (вирусы) - любое программное обеспечение, специально созданное для причинения ущерба отдельному компьютеру или компьютерной сети. Вредоносные программы устанавливаются без Вашего разрешения и влияют на работу Вашего компьютера. Наиболее распространенными видами вредоносных программ являются компьютерные вирусы, которые чаще всего, проникают на компьютер через Интернет или по электронной почте. |
| Шпионские программы | Шпионская программа – это не санкционированно установленный программный продукт, целью которого является скрытое отслеживание поведения пользователя в сети. Также, подобные программы используются для сбора различных типов личной информации, например, привычка пользования Интернетом и посещаемые сайты. |

| | |
|---|---|
| Мошенничество | • Спам<br>• Депрессивные молодежные течения<br>• Наркотики<br>• Социальные сети, Знакомства, блоги чаты, секты.<br>• Экстремизм, нацизм, фашизм. |

Еще одна опасность, подстерегающая в Интернете - это ***интернет-зависимость***.

*Признаки Интернет- зависимости:*

- Навязчивые бесконечные путешествия по Всемирной паутине.
- Пристрастие к виртуальному общению и виртуальным знакомствам — большие объёмы переписки.
- Избыточность знакомых и друзей в Сети.
- Игровая зависимость — навязчивое увлечение компьютерными играми.
- Пристрастие к просмотру фильмов через интернет, когда «больной» может провести перед экраном весь день, не отрываясь из-за того, что в сети можно посмотреть практически любой фильм или передачу.

# Информационная безопасность детей

*Программы фильтры:*

**KinderGate Родительский Контроль** - это интернет-фильтр для дома, школы и других образовательных учреждений, который обеспечивает полный контроль интернета и надежную защиту от нежелательного контента.

**Детский интернет-браузер Гогуль** - это программа для ограничения доступа в интернет и фильтрации содержимого веб-ресурсов, для обеспечения безопасности ребёнка и родительского контроля детского сёрфинга по сети. Безопасность ребёнка в интернете обеспечивается за счёт каталога детских сайтов, проверенных педагогами и психологами, и насчитывающего тысячи детских интернет-сайтов. Гогуль ведёт статистику посещённых сайтов для родительского контроля интернет-сёрфинга ребёнка, а также может ограничивать время пребывания детей в интернет

**КиберМама** проследит за временем работы, предупредит ребенка о том, что скоро ему нужно будет отдохнуть и приостановит работу компьютера, когда заданное вами время истечет. КиберМама поддерживает следующие возможности:

- ограничение по суммарному времени работы;

- поддержка перерывов в работе;

- поддержка разрешенных интервалов работы;

- возможность запрета интернета

- возможность запрета игр/программ.

## Что делать, если ребенок столкнулся с какими-либо рисками в интернет сети

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 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 и др.)

## Рекомендации для родителей.

1. Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет;

2. Объясните детям, что если в Интернете что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством;

3. Составьте список правил работы детей в Интернет и помните, что лучше твердое «нет», чем неуверенное «да». Пусть ограничения будут минимальны, но зато действовать всегда и без оговорок.

4. Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), использовании онлайн игр и других ситуациях, требующих регистрации, нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации.

5. Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.

- Объясните своему ребенку, что как и в реальной жизни и в Интернете нет разницы между неправильными и правильными поступками;
- Научите ваших детей уважать собеседников в Интернете. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернете и в реальной жизни;
- Скажите им, что никогда не стоит встречаться с друзьями из Интернета. Ведь люди могут оказаться совсем не теми, за кого себя выдают;
- Объясните, что далеко не все, что можно увидеть в Интернете – правда. При сомнениях, пусть лучше уточнит у вас.

10. Компьютер с подключением к Интернету должен находиться в общей комнате.

11. Приучите себя знакомиться с сайтами, которые посещают ваши дети.

12. Используйте современные программы, которые предоставляют возможность фильтрации содержимого сайтов, контролировать места посещения и деятельность там.

## Правила пользования Интернет

1. Всегда спрашивай родителей, взрослых о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.
2. Нежелательно размещать персональную информацию в интернете. Персональная информация — это ваше имя, фамилия, возраст, номер мобильного телефона, адрес электронной почты, домашний адрес и адрес школы, в которой Вы учитесь.
3. Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус!
4. Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari!
5. Контролируйте работу за компьютером. Неограниченное использование компьютера может привести к физическим (глазным, гиподинамия, остеохондроз) и психологическим заболеваниям (Интернет-зависимость). Через каждые 20 минут работы выполни зарядку для глаз.
6. Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми познакомились в Интернете.
7. Если хочешь скачать картинку или мелодию, но тебя просят отправить смс – не спеши! Сначала проверь этот номер в Интернете – безопасно ли отправлять на

него смс и не обманут ли тебя. Сделать это можно на специальном сайте.

8. Не используйте в качестве паролей набор цифр: 1234, дату вашего рождения и т.п. «Легкие» пароли быстро взламываются, и Вы можете стать жертвой злоумышленников. Не передавайте свой пароль посторонним лицам.
9. Используйте на компьютерах лицензионное программное обеспечение, антивирусные программы и своевременное обновляйте их, для того что бы защитить компьютер от вирусов и вредоносных программ. Обновление необходимо для пресечения проникновения новых вредоносных программ на Ваш компьютер.

## Вывод

Современный мир плотно насыщен разного рода технологиями, а также новыми открытиями в различных сферах жизнедеятельности. Мы являемся непосредственными участниками всего, что нас окружает, и соответственно каким-либо образом взаимодействуем, как между собой, так и между предметами и процессами, происходящими вокруг нас. Немалый вес имеет и информация, которая все больше и больше заполняет современный мир, а вместе с ним и общество. Мы ее получаем, накапливаем, обмениваемся ей, именно она источник наших знаний, на ее фоне формируются наше мнения на какие-либо процессы или события, именно она является одним из важнейших компонентов, формирующих современное общество. Для гармоничного развития личности ребенку необходимо освоение новых технологий, а соответственно и знакомство с Интернетом, как с глобальным источником информации. Но реальность такова, что дети реже используют Интернет как библиотеку знаний, а делают упор на игры и общение в сети. Интернет стал неотъемлемой частью нашей жизни. С помощью всемирной паутины мы находим нужную информацию, общаемся с друзьями, узнаем последние новости, совершаем покупки и еще очень много всего. Но, как известно, в Интернете есть не только полезное. Интернет для детей таит в себе множество опасностей. Существует множество сайтов, пропагандирующих порнографию, проституцию, насилие, войны, межнациональную и религиозную рознь, употребление наркотиков и алкоголя. Такого рода информация может травмировать психику ребенка, вызвать страх, панику и внушить им ужас. Большинство взрослых, которые знакомы с Интернетом, понимают и осознают эту проблему. Но лишь немногие из них знают, как правильно защитить детей от такого рода информации. Поэтому я считаю, что в школе на родительском собрании следует проводить беседу с родителями, возможно даже и обучение.

# Список используемых ресурсов


1. https://infourok.ru/doklad-bezopasnost-v-seti-internet-dlya-detey-i-roditeley-1706553.html
2. https://multiurok.ru/files/issledovatelskaia-rabota-bezopasnost-v-seti-intern.html
3. https://урок.рф/library/bezopasnost_podrostka_v_seti_internet_070928.html
4. https://findmykids.org/blog/ru/detskaya-bezopasnost-v-internete