

## Безопасный интернет.

### 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 так же 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.

## **Классификация 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 анорексии 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.

- 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 большого 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.

Весь материал - смотрите документ.

#### **Рекламные программы.**

Рекламные программы - нежелательное программное обеспечение, содержащее рекламу. Рекламные программы поставляются 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.

#### **Вредоносные 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 несанкционированно 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
- Депрессивные молодежные течения
- Наркотики
- Социальные сети, Знакомства, блоги чаты, секты.
- 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.

**Способы защиты сети Интернет.**

#### **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 ;

**Рекомендации для детей и родителей по безопасному использованию Интернета.**

По результатам тестирования и анкетирования мы решили найти возможные способы защиты для детей и родителей при работе с интернетом. Один из способов это установка программ фильтров. Но оказалось, что таких программ в интернете много. Нам захотелось

узнать какая программа более эффективна и провести анализ программ. Оказалось, что такой анализ уже сделан профессионалами, и мы хотим ознакомить вас с результатами, которые вы видите на слайде. Интернет фильтры работают во всех браузерах почти с равной эффективностью. Но по итогам сравнительных анализов самым доступным и качественным является программа «Интернет - Цензор» и «Интернет – Цензор Лайт».

Мы разработали рекомендации и инструкции для родителей. А также провели родительское собрание, на котором познакомили родителей со способами защиты в сети Интернет. А учащимся напомнили правила пользования сетью Интернет и сделали памятки для безопасного использования сетью.

### **Правила пользования Интернет для родителей.**

#### **Не разрешайте ребенку предоставлять личную информацию через Интернет.**

Ребенку нужно знать, что нельзя через Интернет давать сведения о своем имени, возрасте, номере телефона, номере школы или домашнем адресе, и т.д. Убедитесь, что у него нет доступа к номеру кредитной карты или банковским данным. Научите ребенка использовать прозвища (ники) при общении через Интернет: анонимность - отличный способ защиты. Не выкладывайте фотографии ребенка на веб-страницах или публичных форумах.

#### **Оградите ребенка от ненадлежащего веб-содержимого.**

Научите его, как следует поступать при столкновении с подозрительным материалом, расскажите, что не нужно нажимать на ссылки в электронных сообщениях от неизвестных источников, открывать различные вложения. Такие ссылки могут вести на нежелательные сайты, или содержать вирусы, которые заражат Ваш компьютер. Удаляйте с Вашего компьютера следы информации, которую нежелательно обнаружить Вашему ребенку.

#### **Ребенок должен понять, что его виртуальный собеседник может выдавать себя за другого.**

Отсутствием возможности видеть и слышать других пользователей легко воспользоваться. И 10-летний друг Вашего ребенка по чату в реальности может оказаться злоумышленником. Поэтому запретите ребенку назначать встречи с виртуальными знакомыми.

### **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 он-лайн 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.
  6. Объясните своему ребенку, что как и в реальной жизни и в Интернете нет разницы между неправильными и правильными поступками;
  7. Научите ваших детей уважать собеседников в Интернете. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернете и в реальной жизни;
  8. Скажите им, что никогда не стоит встречаться с друзьями из Интернета. Ведь люди могут оказаться совсем не теми, за кого себя выдают;
  9. 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.
- Разработав рекомендации для родителей, мы провели общешкольное родительское собрание для родителей 1-4 классов для ознакомления с результатами анкетирования.

### **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 своевременно обновляйте их, для того что бы защитить компьютер от вирусов и вредоносных программ. Обновление необходимо для пресечения проникновения новых вредоносных программ на Ваш компьютер.

Интернет может быть очень опасным, но в тоже время, нельзя не упомянуть о том, что Интернет сегодня является необходимостью. И здесь, как и в реальной жизни, всё зависит от самого человека. Если у него есть чувство меры в «отношениях с Интернетом» и не возникает нездоровая Интернет-зависимость, то такое достижение человечества, как Интернет вполне достойно всяческого уважения.

Нами достигнута цель нашей работы: определили осведомленность учащихся и родителей о безопасном использовании ресурсов в сети Интернет, разработали рекомендации по соблюдению правил безопасной работы в Интернете дома.

Так же достигнуты все задачи, которые мы ставили перед собой:

- изучили скрытые и открытые угрозы интернета;
- проанализировали классификацию интернет - угроз
- выделили способы защиты от интернет угроз;
- подготовили материал о том, что должны знать дети, родители, чтобы интернет стал безопасным;
- подготовили и провели анкетирование учащихся нашей школы по данному вопросу;

Мы провели актуальное исследование по нашей теме. Сделали важные выводы, определили, что эта тема очень важная и нужная и актуальная, особенно для молодежи. Как выяснилось, многие обучающиеся и их родители не знают, не подозревают об опасностях. Иногда попадают в неприятные истории. Благодаря нашим практическим действиям (выступление с презентацией, беседами, раздачей «Памятки о безопасности в интернете»), мы надеемся, что наша работа улучшила ситуацию в этом вопросе и обратила внимание на его важность.