

Беляева Ольга Семеновна

учитель информатики

Муниципальное автономное образовательное учреждение

«Средняя общеобразовательная школа №1»

город Нурлат, Республика Татарстан

ТЕХНОЛОГИИ СОВРЕМЕННОГО УРОКА

МАСТЕР-КЛАСС «БЕЗОПАСНАЯ WEB-СТРАНА»

Интернет – прекрасное средство для обучения, отдыха и общения с друзьями.

http://www.youtube.com/watch?feature=player_embedded&v=9uvNVZMdeIk

Какие угрозы подстерегают ребенка в Интернете?

- Даже случайный клик по всплывшему баннеру или переход по ссылке может привести на сайт с опасным содержанием!
- А украденный пароль поможет злоумышленникам вести переписку от вашего имени. Последствия непредсказуемы.

Это очень серьезно!

Но не все так страшно, как может показаться на первый взгляд. Благодаря современным технологиям защиты, можно обезопасить себя и защитить наших детей от негативных последствий Интернета.

И вы сможете превратить Интернет в эффективный инструмент для образования ребенка!

Во время мастер-класса Вы получите ответы на следующие вопросы:

- Как обезопасить ребенка от злоумышленников в Интернете?
- Как заблокировать доступ к вредоносным сайтам?
- Как ограничить время, проведенное за компьютером?

Для доступа к различным Интернет-ресурсам и сервисам (e-mail, социальные сети, личный кабинет в электронном образовании) часто используются учетные записи с уникальным именем пользователя и паролем.

➤ Сколько символов в вашем пароле e-mail?

Но у каждого замка есть свой ключик.

Время «рассекречивания» паролей:

Пароль «09071985» (дата рождения) будет подобран за 1-2 секунды;

Пароль «андрей» будет подобран за 4 секунды

Пароль «Андрей» будет подобран за 3-4 минуты;

Пароль «1n2f4g8y0» будет подобран за 4 дня;

Пароль «ЕС3+gHFBI» будет подбираться 12 лет;

А пароль «kKC%5426hMIN» будет подбираться несколько миллионов лет.

➤ **Какие выводы можно сделать на данном этапе?**

Вывод 1. Пароль не должен быть коротким.

Иметь пароль менее 8 символов вообще нежелательно, а ещё лучше, чтобы пароль содержал 10-12 символов или больше.

Вывод 2. Пароль не должен содержать только цифры или только буквы (особенно повторяющиеся). Лучше всего, когда буквы и цифры чередуются, а ещё лучше, если в пароль добавляются специальные символы или знаки препинания.

Вывод 3. Важно использовать в одном пароле символы в верхнем и в нижнем регистре (и большие и маленькие). Делается это с помощью клавиши *Shift*.

Надежность пароля можно проверить на сайте [Microsoft](https://www.microsoft.com/en-us/security/default).

Современные школьники с легкостью и энтузиазмом пользуются самыми различными сервисами и приложениями, размещают личные данные и фотографии, используют сервисы навигации. Очень важно юных пользователей научить внимательно относиться ко всему, что они размещают о себе в Интернете. В различных Интернет сервисах можно включить специальные настройки приватности и делиться информацией только с ограниченным кругом лиц.

Интернет-риски, с которыми сталкиваются наши дети:

- Контентные (противозаконная информация)

- Электронные (хищение информации)
- Коммуникационные (межличностные отношения)
- Потребительские (злоупотребление в интернете правами потребителя)

Контентные риски связаны с нахождением в сети различных материалов, содержащих противозаконную, неэтичную и вредоносную информацию (насилие, агрессию, порнографию, пропаганду анорексии, суицида, азартных игр, наркотических веществ и т. д.).

Электронные риски – возможность столкнуться с хищением персональной информации или подвергнуться атаке вредоносных программ.

Коммуникационные риски связаны с общением и межличностными отношениями интернет-пользователей. Примерами таких рисков могут быть: кибербуллинг, незаконные контакты (например, груминг, сексуальные домогательства), знакомства в сети и встречи с интернет-знакомыми.

Подробнее остановимся, на коммуникационных рисках.

Кибер-буллинг, или травля в Интернете, представляет собой метод морального унижения человека, подавления его достоинства путем публикации различных текстов, размещения там фото- и видеоматериалов оскорбительного характера.

Способы Интернет-травли разнообразны:

В социальных сетях, на электронную почту, в системах Интернет-коммуникаций жертва получает запугивающие, уничижительные сообщения.

В социальных сетях создаются группы против «жертвы», где она высмеивается. Там размещаются ролики, тексты унижительного содержания, проводятся опросы из серии «Хотели бы вы, чтобы Петю выгнали из класса?»

На сайтах знакомств от имени «жертвы» размещаются анкеты непристойного содержания с указанием настоящей почты или телефона, а в социальных сетях создаются поддельные странички «жертвы», где размещается информация непристойного, унижительного характера.

Взламывается страничка «жертвы» в социальных сетях и там размещается неподобающая информация.

Поведение ребенка снимается на видео, а затем размещается в Интернете, порой в измененном виде.

Рекомендации по борьбе с кибербуллингом:

- При общении в Интернете оставайтесь дружелюбными с другими пользователями.
- Лучший способ испортить хулигану его выходку — отвечать ему полным игнорированием.
- Личная информация, которую пользователи выкладывают в Интернете, а также фотографии могут быть использованы агрессорами против них.

По данным исследований, особенно остро ситуацию буллинга переживают дети 11–12 лет — им гораздо тяжелее в подобных ситуациях, чем более старшим школьникам. Зачастую младшие ребята не знают, как поступить и куда обратиться за помощью. Существует достаточно большое количество организаций, специализирующихся на помощи подросткам, столкнувшимся с кибербуллингом. Одной из таких организаций является линия помощи «Дети онлайн». Сюда можно обратиться по телефону (8-800-25-000-15) или по электронной почте helpline@detionline.com), чтобы получить квалифицированную помощь и психологическую поддержку.

Как показывает опыт, еще одна форма профилактики и информирования учеников о проблеме буллинга и кибербуллинга - общешкольные просветительские мероприятия, которые ученики могут проводить как самостоятельно, так и при поддержке администрации и педагогического коллектива школы.

Защитить ребенка от неправомерного контента возможно, используя возможности самой операционной системы. В Windows 7 это можно сделать так:

1. В свойствах обозревателя браузера можно настроить зону опасных и надежных сайтов.

2. Настроить Родительский контроль: ограничение по времени, доступ к играм, разрешение и блокировка конкретных программ.

Возможно также, установить специальное программное обеспечение – программы-фильтры, способное блокировать вредоносное ПО.

Надо сказать, что в школьный Интернет в Республике Татарстан достаточно защищен, фильтрация доступа к Интернет-ресурсам осуществляется централизованно Центром Информационных технологий РТ.

И, конечно, необходима консультационная работа с родителями с тем, чтобы они в свою очередь разъясняли своим детям, как вести себя на просторах Интернета и всегда были рядом, когда детям нужна помощь. Вот такие памятки мы раздавали родителям на родительском собрании, посвященном безопасному поведению в сети Интернет.

Предлагаю разобраться в трудной ситуации, в которую попала девочка.

Письмо девочки.

Здравствуйте, меня зовут Мария, мне 14 лет. Недавно я была в гостях у двоюродных братьев и с их компьютера заходила на свою страничку в социальной сети, но не вышла перед тем, как уйти из гостей. Братья разослали всем моим друзьям неприличные картинки, а на моей стене написали оскорбительные сообщения про всех моих знакомых. Что же мне делать? Что подумают мои друзья? Удалять страницу очень не хочется. Хочу отомстить своим братьям, хотя и понимаю, что это неправильно.

Какие советы можно дать девочке. Что ей делать?

Использованные ресурсы:

1. <http://www.razbiraeminternet.ru/>
2. http://www.chaynikam.net/view_articles.php?id=19
3. <https://www.microsoft.com/ru-ru/security/pc-security/password-checker.aspx>
4. <http://www.youtube.com/watch?v=QvOlgob5njQ>
5. http://www.youtube.com/watch?feature=player_embedded&v=9uvNVZMd eIk