Работа по защите детей от нежелательной информации
МОУ СШ №67 в 2017-2018 учебном году

В целях оказания помощи классным руководителям при проведении классных часов и родительских собраний в течение 2017-2018 учебного года в средней школе № 67 продолжается работа по профилактике поведения детей в сети Интернет.

Цель: познакомить классных руководителей, родителей с правилами ответственного и безопасного поведения в современной информационной среде, с рисками и способами защиты от противоправных посягательств в сети Интернет..

Задачи:

- Дифференцированно и целенаправленно планировать просветительскую работу на основе выявленных потенциальных угроз.
- Повышать профессиональный уровень педагога с учетом развития ИКТ-технологий.
- Провести анкетирование учащихся, родителей по теме «Дети и интернет»; сделать анализ данных;
- Подготовка выступлений психолога, учителя информатики;
- Побудить родителей к полноценному общению со своими детьми.

Направления деятельности администрации по организации работы с молодыми специалистами:

- школьная документация;
- организация учебно-воспитательного процесса;
- методическое сопровождение классных руководителей;
- организация воспитательной работы в классе;
- психологические основы,
- разработка страницы на сайте школы.

Направления деятельности классных руководителей по организации работы по медиабезопасности:

- Анкетирование родителей, учащихся, педагогов.
- Работа с учителем информатики, психологом
- Подбор видеоматериалов, создание презентаций; буклетов для родителей.
- Проведение единого классного часа.
- Проведение родительского собрания:

При разработке рекомендаций для проведения собрания использованы материалы сети «Интернет», в приложении даются ссылки на источники информации. В сценарии собрания имеются гиперссылки на интернет-ресурсы (YouTube) и документы (при наведении курсора на гиперссылку и нажатии кнопки Ctrl на клавиатуре вашего компьютера, данная ссылка откроет видео и другие материалы).

Для организаторов собрания в помощь приводятся:
- анкеты для учащихся и родителей;
- выступления заместителя директора по воспитательной работе об актуальности темы, о том, что такое медиабезопасность;
- выступление учителя информатики, который рассказывает о рисках в сети «Интернет» и дает советы о их предотвращении;
- выступление психолога школы, дающего советы о том, как избежать интернет-угрозы;
- имеются социальные ролики и фильмы о детях в интернете, о рисках и угрозах сети;
- для родителей – буклеты-памятки от компании Microsoft.

На основании анализа анкет учащихся и родителей составляется план проведения собрания. Учитывая специфику темы, к разработке приглашаются:
- учитель информатики, который должен подготовить выступление по теме «Риски сети «Интернет», создать буклеты-памятки для родителей по материалам выступления психолога;
- психолог школы, который должен подготовить выступление по теме «Предотвращение рисков в интернете».

Тезисы:

1. Интернет – полезен и опасен одновременно. Нужен для работы, учебы, досуга, покупок и пр. Однако приносит немало бед. Декабрь 2010 – принятие Закона о защите детей от нежелательной информации. Виды запрещенной информации. Просмотр ролика «А вы знаете, чем занимаются ваши дети в интернете?».
2. Риски интернета: контентные, коммуникативные (кибербуллинг, груминг, киберпреследования), кибермошенничество, игровая зависимость (просмотр ролика про Сашу Фокина), вредоносные программы, установление контента.
3. Общие рекомендации для родителей по обеспечению безопасности детей в Интернете. Просмотр фильма «Дети в интернете»

Интернет постепенно проникает в каждую организацию, общественное учреждение, учебное заведение, в наши дома. Число пользователей Интернета в России стремительно растет, причем доля молодежи и совсем юной аудитории среди пользователей Всемирной паутины очень велика. Для многих, особенно молодых людей, он становится информационной средой, без которой они не представляют себе жизнь. И это не удивительно: ведь в Интернете можно найти информацию для реферата или курсовой, послушать любимую мелодию, купить понравившуюся книгу или обсудить горячую тему на многочисленных форумах. Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна: в ней появилась своя преступность, хулиганство, вредительство и прочие малоприятные явления. 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.

Иногда именно средства массовой информации, печатные и электронные, оказываются источником угрозы жизни и здоровью людей, в первую очередь детей и подростков. Наверное, вы слышали многочисленные истории о том, как дети становились жертвами преступлений, если вступали в виртуальное общение с незнакомыми людьми, а потом соглашались на встречу с ними. К сожалению, есть случаи, когда старшеклассники оказывались на скамье подсудимых и были осуждены за то, что, уверенные в своей безнаказанности, оставляли в социальных сетях посты, которые позже судом были квалифицированы как экстремистские высказывания. Наверное, если бы ребята были вовремя проинформированы о том, что их может ждать за эти высказывания, они бы не стали этого делать. Самоубийства …

Учитывая подобные факты и угрозы, Государственная Дума Российской Федерации в декабре 2010 года приняла закон «О защите детей от информации, причиняющей вред их здоровью и развитию». Он вступил в силу с 1 сентября 2012 года.

К информации, запрещенной для распространения среди детей, относится информация:

4. побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
5. 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;
6. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к лю-

дям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
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.

Что же такое «Медиабезопасность»?

Медиа – среда.

Безопасность – это состояние защищённости. Защищённости от последствий воздействия на Ваше тело, психику, Ваших близких, Ваше имущество, Ваши отношения.

БЕЗОПАСНОСТЬ, -и, ас. 1. см. безопасный. 2. Состояние, при котором не угрожает опасность, есть защита от опасности

Таким образом, мы с вами говорим об окружающей среде без опасностей для ребенка, то есть о безопасной среде. Сегодня на собрании мы хотим поговорить об информационной среде, точнее о сети «Интернет» и мобильной сети. Давайте посмотрим небольшой социальный ролик и обсудим нашу тему.

Просмотр ролика «А вы знаете, что ваш ребенок делает в интернете?»

Скажите, пожалуйста, какие проблемы вы увидели в этом ролике? (Мы не всегда знаем, чем наши дети занимаются в интернете, чем грозит интернет?)

На основании данных проведенного анкетирования, мы сделали выводы. Сейчас я кратко доведу до вас результаты (показ диаграмм).

Действительно, интернет может быть и полезным, и опасным. Давайте послушаем выступление учителя информатики с рассказом о том, какие же риски таит в себе интернет.

б) выступление учителя информатики «Риски сети «Интернет»

Контентные риски — это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

Как помочь ребенку избежать столкновения с нежелательным контентом:

• Приучите ребенка советоваться со взрослыми и немедленно сообщать о появлении нежелательной информации подобного рода;

• 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;

• Старайтесь спрашивать ребенка об увиденном в Интернете. Зачастую, открыв один сайт, ребенок захочет познакомиться и с другими подобными ресурсами.

Коммуникационные риски, такие как незаконные контакты (например, груминг), киберпреследования, 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 хотят 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. Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Предупреждение груминга:

• Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются;

• Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также пересылать интернет-знакомым свои фотографии;

• Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу;

• 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 сопровождении ребенка на эту встречу;

• Интересуйтесь тем, куда и с кем ходит ваш ребенок.

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

Предупреждение кибербуллинга:

• Объясните детям, 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;

• Научите детей 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.

Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и, тем более, не всегда знают, как ее предотвратить.

Вот на что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

• Беспокойное поведение

Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

• Неприязнь к Интернету

Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В очень 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 письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб

Предупреждение кибермошенничества:

• Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;

• Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных;

• Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если Ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности: ознакомьтесь с отзывами покупателей:

1. Проверьте реквизиты и название юридического лица – владельца магазина
2. Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs)
3. Поинтересуйтесь, выдает ли магазин кассовый чек
4. Сравните цены в разных интернет-магазинах.
5. Позвоните в справочную магазина
6. Обратите внимание на правила интернет-магазина
7. Выясните, сколько точно вам придется заплатить

Как распознать интернет- и игровую зависимость

Сегодня в России все более актуальны проблемы так называемой «интернет-зависимости» (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае, если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Согласно исследованиям Кимберли Янг, предвестниками интернет-зависимости являются:

• навязчивое стремление постоянно проверять электронную почту;
• предвкушение следующего сеанса онлайн;
• увеличение времени, проводимого онлайн;
• увеличение количества денег, расходуемых онлайн.

Не так давно по телевидению прошла передача, в которой рассказывали о мальчике Саше Фокине, страдающего геймерством. Давайте посмотрим видеоролик об этом ребенке. (Показ видеоролика «Саша Фокин»)

Я думаю, что обсуждать этот ролик бессмысленно, и так всё понятно. Надеюсь, что вы не хотите, чтобы ваш ребенок превратился в геймера, и сделаете все возможное, чтобы избежать подобное.

Но если Вы считаете, что Ваши близкие, в том числе дети, страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь. Помощь может быть оказана как в специальных терапевтических группах, так и стационарно, с использованием специальных медицинских процедур.

Как научить ребенка не загружать на компьютер вредоносные программы

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными и даже использовать Ваш компьютер для распространения вируса, рассылать от Вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

• Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери

данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

• Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.

• Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.

• Периодически старайтесь полностью проверять свои домашние компьютеры.

• Делайте резервную копию важных данных.

• Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

Контент-фильтры:

- iProtectYou Pro (http://soft.mail.ru/program_page.php?grp=5382)
- KidsControl (http://soft.mail.ru/program_page.php?grp=47967)
- CYBERsitter (http://www.securitylab.ru/software/240522.php)
- КиберМама 1.0b (http://www.securitylab.ru/software/273998.php)

Общие рекомендации для родителей по обеспечению безопасности детей и подростков в Интернете.

1. Расположите компьютер вашего ребенка в месте общей доступности: столовой или гостиной. Так вам будет проще уследить за тем, что делают дети в Интернете.
2. Следите, какие сайты посещают ваши дети. Если у вас маленькие дети, знакомьтесь с Интернетом вместе. Если у вас дети постарше, поговорите с ними о сайтах, которые они посещают, и обсудите, что допустимо, а что недопустимо в вашей семье. Список сайтов, которые посещает ваш ребенок, можно найти в истории браузера. Кроме того, вы можете воспользоваться инструментами блокировки нежелательного контента, такими как, например, безопасный поиск Google или безопасный режим на YouTube.
3. Расскажите детям о безопасности в Интернете. Вы не сможете все время следить за тем, что ваши дети делают в Сети. Им необходимо научиться самостоятельно пользоваться Интернетом безопасным и ответственным образом.
4. Установите защиту от вирусов. Используйте и регулярно обновляйте антивирусное ПО. Научите детей не загружать файлы с файлообменных сайтов, а также не принимать файлы и не загружать вложения, содержащиеся в электронных письмах от незнакомых людей.
5. Научите детей ответственному поведению в Интернете. Помните золотое правило: то, что вы не сказали бы человеку в лицо, не стоит отправлять ему по MS, электронной почте, чате или размещать в комментариях на его странице в Сети.
6. Оценивайте интернет-контент критически. То, что содержится в Интернете, не всегда правда. Дети должны научиться отличать надежные источники информации от ненадежных и проверять информацию, которую они находят в Интернете. Также объясните детям, что копирование и вставка содержания с чужих веб-сайтов могут быть признаны плагиатом.

Учитель информатики Дроздов С.А.
Педагог-психолог Чурсин С.В.