Родительское собрание «Безопасный интернет»

Цели и задачи:

1.Актуализировать проблему безопасности детей в сети Интернет;

2.Побудить родителей задуматься о собственной роли и ответственности о безопасности детей в сети Интернет;

3.Познакомить родителей с правилами безопасности при работе с Интернетом и детскими браузерами.

Ход собрания.

Виртуальная реальность, как и любое пространство, обладает своими плюсами и минусами. Существование кибер-опасностей так же неоспоримо, как польза и удовольствие от использования Интернет-ресурсов. За безопасностью пользователей следят как государственные структуры, так и сотрудники Интернет сервисов. Тем не менее, ежедневно появляются новые жертвы, чаще всего пострадавшие от собственной неосведомленности.

**Виртуальне риски:**

1. **Контентные риски**

Порнография, детская порнография, нарушение авторского права, пропаганда экстремизма и наркотиков, нецензурные тексты.

1. **Нарушения безопасности**

Вирусы, трояны, нежелательная почта (Спам), онлайн мошенничества.

1. **Коммуникационные риски**

Незаконный контакт, киберпреследование (угрозы, сексуальные домогательства с использованием информационных технологий).

**Блокировщики браузеров и Windows**

 Множество опасностей поджидает неопытного пользователя при работе в Интернете. Один из них – популярный блокировщик операционной системы Windows под общеизвестным названием Winlock. Этот вредоносный код можно легко получить, если открывать подозрительные ссылки и забывать регулярно обновлять базы своего антивируса. Winlock при старте Windows выводит поверх всех окон сообщение о том, что доступ в систему заблокирован, и для того, чтобы данное окно исчезло, необходимо отправить платное смс-сообщение.

Программа ориентирована на наивных пользователей, которые верят тому, что написано. Окно, возникающее поверх всех окон, предлагает ввести регистрационный код якобы для регистрации нелицензионной копии Windows. Для получения регистрационного кода требуется отправить смс-сообщение, цена которого составляет от 200 до 300 рублей. Само собой, мошенники не имеют никакого отношения к официальным дилерам операционной системы Windows. Злоумышленники пользуются тем, что большинство пользователей используют на домашних компьютерах пиратские версии ОС. К слову, регистрационный код для Windows покупается на сайте компании Microsoft и у официальных дилеров, и делается это вовсе не с помощью смс.

 Вирус не всегда прикидываются регистратором Windows, некоторые просят продлить доступ к эротическим материалам (привет посетителям порно-сайтов) или обвиняют пользователя в хранении незаконной информации. Ряд троянов пугает тем, что в течение суток система будет уничтожена, если не будет отправлено смс-сообщение.

 Существуют также «братья» вируса-вымогателя, копирующие интерфейс популярных программ. Они блокируют определенные приложения, а не всю систему сразу. Например, один из троянов убеждает пользователя в том, что он нарушил лицензионное соглашение беслпатной (!) программы Download Master и не дает пользоваться ею. Особо наглый вид вируса маскируется под антивирус Касперского и требует смс за продление лицензии. По такому же принципу блокируются браузеры, не позволяя пользователю загружать Интернет-страницы.

 Само собой, отправлять сообщение не надо, разве что если Вы хотите поделиться с вымогателями своими деньгами. Вирус легко удаляется специалистом по компьютерной безопасности или даже опытным пользователем. Кроме того, специалисты компании «Доктор Веб» и «Антивирус Касперского» разработали специальную форму, в которую можно ввести текст предполагаемого sms-сообщения и получить код разблокировки.

Любители онлайн-лотерей рискуют расстаться с $30, отправляя «СМС счастья», но еще хуже придется тем, кто поверит в эффективность лжеантивирусов — плата за это составляет в среднем $50. Впрочем, и это далеко не предел: за услуги по восстановлению данных, зашифрованных троянцем GpCode, его жертве придется отдать злоумышленникам в среднем $100.

 Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ предусмотрена в Статье 273 УК РФ. Добавим к этому мошенничество (Статья 159) и вымогательство (Статья 163), и получим состав преступления, за которое злоумышленникам светит лишение свободы на срок от семи до пятнадцати лет с конфискацией имущества.

Заработать свое на беззаботном пользователе можно и множеством других способов. Например, похитив отсканированное изображение его паспорта. Продажа этих данных принесет злоумышленникам около $25. Дешевле — в районе $10 — будет стоить информация о его кредитной карте, по $5 — пароль и логин от одной из многочисленных социальных сетей, пользователем которых он является. По данным «Лаборатории Касперского», доступ к электронной почте сегодня можно продать за $20, чуть меньше — $10 — стоит доступ к аккаунту хостинга-сервиса типа RapidShare. Меньшим спросом пользуются пароли от IM-мессенджеров (ICQ, и т.д.): прибыль от продажи этих данных составит около $3. Наибольшую же рентабельность показывают, как это ни удивительно, персонажи онлайн-игр: аккаунты серьезного уровня в популярной игре World Of Warcraft в среднем продаются по $150-160.

Попадали ли вы в такие ситуации?

 Куда проще позаботиться о безопасности компьютера заранее. Для этого нужно соблюдать банальные правила безопасности:

 1) Всегда держать включенным антивирус и регулярно обновлять его базы

 2) Не переходить по сомнительным ссылкам и не устанавливать на компьютер неизвестные приложения

 Источник: <http://www.saferunet.ru/adult/news/799/>

Знаете ли вы, какие существуют законы, связанные с сетью Интернет?)

**Нормативно-правовые акты РФ, направленные на борьбу с преступлениями в сети Интернет**

 Международное и российское законодательства содержат нормативные акты, направленные на борьбу с преступлениями в сети Интернет.

 Вашему вниманию представлены выдержки из нормативно-правовой базы по видам контента:

Постановление Правительства РФ от 10 сентября 2007 г. №575

«Об утверждении Правил оказания телематических услуг связи» (с изменениями от 16 февраля 2008 г.)

Постановление Правительства РФ от 23 января 2006 г. №32

«Об утверждении Правил оказания услуг связи по передаче данных» (с изменениями от 16 февраля 2008 г.)

Обзор международного законодательства по вопросам противодействия распространению детской порнографии Обзор российского законодательства по вопросам противодействия распространению детской порнографии

Законодательство РФ о детской порнографии

 Источник:http://www.friendlyrunet.ru/

Большинство родителей не запрещают своим детям пользоваться Интернетом. И это естественно, ибо Сеть – не только познавательный, но и развлекательный инструмент. Следует понимать, что подключаясь к Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет.

К сожалению, это не всегда помогает уберечь ребенка от опасного контента.

 Начать с того, что, как показывает практика, родители понятия не имеют, какие сайты посещает их любимое чадо. А, между прочим, самый популярный объект детского интереса в Интернете - это игры. Большинство детей выходит во всемирную паутину именно ради онлайн-игр или поиска информации о них. Спорить о целесообразности подобного увлечения можно долго (что и происходит на сетевых страницах и в научных кабинетах), но если игра не культивирует жестокость и насилие, ничего опасного в ней нет. Кроме игрозависимости, но это отдельная тема.

 Довольно часто дети обращаются к Сети в поиске информации по учебе. Это могут быть научные статьи, электронные варианты учебников и многое другое. Интернет значительно упрощает учебный процесс, позволяет ребенку экономить свое время. Ему не нужно идти в библиотеку, ждать своей очереди, искать нужную книгу, а затем проводить над ней несколько часов, выписывая необходимый материал. Другая сторона медали – с помощью Интернета дети научились отлынивать от настоящей учебы, скачивая уже готовые рефераты, выдавая их за свои.

Дети любят общаться в чатах и заводить виртуальных друзей. Поскольку Интернет в общем-то анонимен, собеседником ребенка может оказаться абсолютно любой человек, не обязательно с хорошими намерениями. Юный пользователь имеет все шансы познакомиться с мошенниками, сектантами, педофилами и прочими колоритными личностями, которые умело войдут в доверие, а зачем назначат встречу в реальной жизни. На которой или похитят, или совратят, или «промоют мозги» для вовлечения в свои ряды себе на пользу. Многие дети и не догадываются о том, что о таких подозрительных знакомых надо непременно сообщать родителям, а об отдельных экземплярах - даже в милицию.

 Прочие детские увлечения в Интернете с трудом поддаются классификации и мало чем отличаются от запросов среднестатистического пользователя. Дети просматривают картинки, читают анекдоты и забавные истории, смотрят клипы, скачивают музыку. Что примечательно – редкий ребенок специально пойдет на опасный сектантский или экстремистский ресурс. Если он и окажется на нем, то либо по случайной ссылке, либо из-за всплывающего окна. Аналогично дети попадают на ресурсы с порнографией. Конечно, часть детей заходит на порноресурсы вполне осознанно и столь же осознанно ищет их в Сети, но этой темой одержимы в основном подростки в период бурного сексуального созревания. Дети помладше не уделяют ей много внимания, хотя, по данным ученых, средний возраст первого контакта с порноконтентом – 11 лет (в отдельных случаях опускающийся до восьми и даже шести). К сожалению, непреднамеренные посещения не делают подобные сайты менее опасными для детской психики. Также не зря на многих безопасных ресурсах вроде форумов и социальных сетей установлено ограничение «с 13 лет». Детям, младше обозначенного возраста, на таких страницах делать нечего – просто в силу уровня их психики и знаний.

 Так есть ли в Сети места, где ребенок может чувствовать себя безопасно и получить всю необходимую информацию?

 Ссылки на «вредные» сайты дети чаще всего получают из поисковиков, которые индексируют всю информацию. Достаточно набрать вполне безобидный и даже детский запрос – «девочки» или «кукла Барби» - и посмотреть результаты поиска. Понимая эту проблему, ряд разработчиков попытался предложить специальные детские поисковики без индексации вредного для развития детей контента. Существует специальный детский поисковик Agakids.ru, фильтрующий негативный контент в результатах поиска. Он работает на основе каталога сайтов для детей. Кроме поисковика на Agakids есть почтовый сервис, клуб знакомств, форум, радио, игры, новости и ролики с мультфильмами.

 Детская социальная сеть Твиди.ру предлагает общение в чате, ленту новостей, адаптированную специально для юных читателей, место для создания собственного файлового архива и множество игр.

 Сеть Бибигон является детским вариантом онлайн-дневника с электронным школьным журналом. Ребенок получает собственную страничку, на которой может делать записи и загружать свои фотографии.

 Портал Детский Мир собрал в себе несколько сервисов сразу: блоги, знакомства, чаты, игры, чтение и даже уроки английского языка. Остается только ввести автоматическое обновление аккаунта до «одноклассников» или «вконтанте» в день совершеннолетия.

 Есть в Интернете и более узко-ориентированные ресурсы. Например, детский развлекательный сайт Ребзики содержит раскраски и паззлы, а Теремок.ру полон самых разных развивающих игр. Почитать стихи, рассказы, песенки, загадки и прочий фольклорный материал ребенок сможет на сайте Кошки-мышки.ру.

 В любом случае, нет стопроцентного способа оградить детей от нежелательного контента. Нужно быть готовым к тому, что во время путешествия по Интернету ребенок может оказаться на ресурсах с нелицеприятным содержанием и защитить его смогут только воспитание и моральная устойчивость. А задача общества – предоставить необходимую информацию и помощь, чтобы вхождение ребенка в «полный» Интернет было гармоничным и безвредным – и для ребенка, и для общества.

 Источник: <http://www.saferunet.ru/children/news/562/>

 **Попались в Сеть**

 Согласно статистике, в США от Интернета зависимы 3-5% взрослого населения. Боюсь, что это неточные данные. В Южной Корее считают, что злоупотребляют Сетью 40% школьников, а от 10 до 15% — зависимы. Примерно такие же цифры в Китае. В России эта проблема станет очень актуальной в течение ближайших 10 лет.

 Сегодня значительная часть общения проходит в Интернете. И мы не знаем, какие изменения это повлечёт для будущего поколения: насколько важным будет для них живое индивидуальное общение, обмен эмоциями? Но уже очевидно, что злоупотребление виртуальной реальностью приводит к настоящей инвалидности. Есть молодые люди 30-35 лет, которые не могут работать, содержать и обслуживать себя. Родные кормят их с ложечки прямо возле компьютера.

**Первые признаки интернет-зависимости:**

• долгое нахождение в Сети,

 • бесцельное её использование,

 • вытеснение других интересов,

 • снижение настроения, проявление агрессии при невозможности войти в Интернет.

 Источник: Аргументы и факты

** Несколько**

 **шокирующих фактов**

 **о социальных сетях**

1. Приблизительно пятнадцатью процентами пользователей социальные сети применяются для организации слежки.
2. Широкий выбор в социальных сетях и вседозволенность приводят к всплеску желаний. После знакомств в социальных сетях втрое выросло количество измен.
3. Исследованиями установлено, что нахождение в соцсетях ведет к увеличению риска самоубийства, так как человек до минимума сводит свое общение с окружающими и отрешается от действительности.
4. В соответствии со статистикой количество преступлений на сексуальной почве, направленных на несовершеннолетних, выросло из-за соцсетей в 26 раз.
5. Ежегодно около 100 человек лишаются жизни из-за сообщения, оставленного в соцсетях, и эта цифра возрастает.
6. Социальные службы используют для вербовки своих агентов не только спецслужбы, но и различные группировки, в том числе террористической направленности.
7. В 2011 году в Великобритании каждые четверо из пяти грабителей пользовались при подготовке грабежа социальной сетью.
8. Социальные сети сужают кругозор человека: он становится зависим от пустых и ненужных сообщений.
9. Чрезмерная увлеченность соцсетями, по данным исследований, ведет к снижению иммунитета, сердечно-сосудистым болезням и душевной дисгармонии. Активные, но не дающие развития мыслительные процессы наряду с малой подвижностью способствуют развитию заболеваний эндокринной системы.

10.Более 90% пользователей с доверием относятся к советам ровесников на сайтах, тогда как рекламе верят только 14%. Маркетинговые службы активно этим пользуются.

11.У среднего пользователя друзьями числится 195 человек.

12.Наиболее активна Интернет-аудитория в России: средний пользователь проводит в нем 6,6 часов в неделю, просматривая 1307 Интернет-страниц.

13.80% людей больше верят собственным онлайн-друзьям, чем реальным.

14.Еженедельно в социальных сетях дети проводят: от 7 до 14 часов – 23%, 14-21 час – 57% и больше 21 часа – 20%.

15.80% родителей считают, что им известно, что их дети делают в Интернете, но 31% детей убеждены, что их родители об этом не знают.

 Источник: smonews

**Игромания.**

 Через злоупотребление Интернетом — когда с ним забавляются, как с новой игрушкой, — проходят все. Но не все остаются в виртуальном пространстве.

 В зависимости от свойств характера люди обращаются к разным ресурсам Интернета. Тот, кто вспыльчив, эмоционально неустойчив, агрессивен, скорее подсядет на различного рода «стрелялки» — игры, которые часто связывают с совершением преступлений в реальной жизни. Мы изучали поведение таких людей и обнаружили у них повышенный уровень агрессивности и тревожности. Можно предположить, что у некоторых из них игра агрессию снижает, у других, наоборот, ещё больше повышает. И хотя нельзя сказать, что деструктивные игры напрямую провоцируют преступления, в любом случае они не обучают человека нормальному поведению. Поэтому их, прежде чем допускать к продаже, необходимо подвергать психологической экспертизе, как в большинстве стран.

 К многоуровневым онлайн-играм, общению в чатах чаще обращаются робкие, тревожные, погруженные в себя подростки. Им сложно решать частые в этом возрасте межличностные конфликты, а в Интернете общение спокойно, безопасно. Чаще всего за помощью обращаются родители студентов. Пока ребёнок учится в школе, возможности пользования Всемирной паутиной у него всё же ограниченны. Да и конфликты со сверстниками пока ещё не воспринимаются слишком серьёзно. Но на первом-втором курсе начинаются проблемы. С высокой долей вероятности они возникают у детей, которые рано пошли в школу, досрочно поступили в вуз. Они всегда находятся среди старших, которые их отвергают, и скрываются от обидчиков за волшебным монитором. Опасность — не в пребывании в Интернете, а в том, что зависимость от виртуального пространства вызывает задержку социального и эмоционального развития — неспособность работать и достигать результата, иметь друзей, создать семью.

 Основная проблема формирования интернет-зависимости зачастую не в этих детях, а в их родителях. Ведь умение понимать людей, общаться закладывается в семье. Чувства развиваются через их переживания, через разговоры, которые ведутся дома во время ужина. Часто оказывается, что в семьях интернет-зависимых люди никогда в жизни не ели за одним столом. Никогда!

 Так как же вернуть человека в реальную жизнь из виртуальной? Механические ограничения — программы по контролю доступа и даже попытки обрезать провода — не помогут. Один мой пациент — студент — просто сбежал из дома, где родители пытались его контролировать, в интернет-кафе и жил там неделю. Это довольно распространённый случай. Кроме того, я категорически против помещения таких людей в больницы или в специальные лагеря, как это делается в Китае. Временные ограничения ничего не дают, если человека не научить дружить, если не изменить его ценности. Первым делом нужно обратиться к психотерапевту — именно врачу, чтобы исключить наличие других заболеваний. Ребёнок с вами наверняка не пойдёт. Но, возможно, в этом и нет необходимости. Главное — изменить своё отношение к детям должны сами родители.

Заключение

 Не стоит думать, что Интернет – это безопасное место, в котором ваши дети могут чувствовать себя защищенными. Надеюсь, что вы понимаете, что использование только средств воспитательной работы без организации действенного контроля – это практически бесполезное занятие. Точно так же как и использование репрессивных средств контроля без организации воспитательной работы. Только в единстве данных средств вы сможете помочь вашим детям чувствовать себя в безопасности и оградить их от влияния злоумышленников.

 Вывод: Только от нас зависит будут подвергаться лишней опасности в сети Интернет наши дети или нет.