

ЛЕКЦИЯ-БЕСЕДА ПРЕДУПРЕЖДЕНИЕ НЕГАТИВНОГО ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ В СЕТИ «ИНТЕРНЕТ»

Целевая аудитория: родители (законные представители), педагогические работники.

Развитие коммуникативных навыков, в том числе навыков использования сети «Интернет», у современных детей происходит все более интенсивно с каждым годом. Они быстрее и легче осваивают основы работы с новыми техническими средствами (гаджетами) и сервисами, зачастую не понимая свойственных для «Интернет»-среды опасностей и угроз. В рамках настоящей беседы мы изучим материалы и сведения, необходимые для обеспечения информационной безопасности несовершеннолетних в сети Интернет.

Общая характеристика информационных угроз ребенку в сети «Интернет»

Итак, во всемирной сети существуют следующие виды опасности для несовершеннолетних пользователей:

1) Социальные сети, сайты знакомств. Виртуальное общение деформирует коммуникативные способности и навыки ребенка, усложняя процесс реального общения. Практика показывает, что в онлайн-переписке несовершеннолетний позволяет себе более конфликтные высказывания, использование нецензурной брани и т.д., даже если в реальной жизни подобной риторики он себе не позволял. Вседозволенность и псевдоанонимность сети порождает заблуждение, что в кругу сверстников можно вести себя так же, что, в свою очередь, ведет к социальной изоляции ребенка. Последняя же провоцирует проведение все большего времени в сети Интернет. Круг замкнулся. Помимо того, существуют прямая угроза жизни и здоровью несовершеннолетних от незнакомцев, предлагающих личные встречи, а также различных видов мошенничества. Вывод: Вам следует интересоваться кругом общения ребенка в сети, «мягко» контролируя коммуникацию со сверстниками, уделив особое внимание фактам общения со взрослыми и со сверстниками, с которыми ребенок в реальной жизни не знаком;

2) Суицид-сайты, сайты-форумы потенциальных самоубийц, Интернет-площадки, распространяющие различные молодежные субкультуры, подверженные самодеструктивному поведению, риску самоубийства. Обычно помимо непосредственного общения на подобных ресурсах предлагается к прочтению особого рода литература, ознакомление с которой порой приводит к самоубийству или причинению себе телесных повреждений. Таковыми, например, являются издания: Джей Эшер «13 причин почему», С. Крамер «50 дней до моего самоубийства», Джеффри Евгенис «Девственницы-самоубийцы», Э.Я. Володарского «Дневник самоубийцы» и др. Далеко не все из этих книг писались для целенаправленного деструктивного воздействия на несовершеннолетнего читателя, а некоторые даже считаются классикой психологического романа, однако рассчитаны на читателя, имеющего определенный жизненный опыт. Вывод: следует обращать особое внимание на контент, с которым знакомится Ваш ребенок;

3) Интернет-сайты, веб-сайты порнографической направленности крайне часто встречаются на просторах всемирной сети. По данным различных исследователей доля порнографических материалов от общего объема циркулирующей в сети информации составляет от 4 % до 37 %. Методология этих исследований не позволяет нам однозначно утверждать о подлинности этих сведений, однако дает представление об общей тенденции информационного оборота в сети Интернет. Даже если взять за основу наиболее оптимистичный (4 %) итог исследования, с учетом практически неизмеримого объема циркулирующей информации, это достаточно устрашающие цифры. Кроме того, следует помнить, что оборот порнографии – это бизнес, и заинтересованные в распространении подобной информации лица проводят активную и агрессивную политику по вовлечению в

просмотр этого контента максимального числа людей независимо от пола и возраста, в том числе с использованием вредоносного программного обеспечения.

4) Наркосайты. В сети «Интернет» распространены рецепты и советы изготовления наркотических средств, психотропных веществ, информация о «пользе» либо безопасности употребления таковых, завуалированные предложения и места приобретения таких средств и веществ. Для выявления таковых взрослому человеку понадобится знания не только официальных наименований наркотических средств и психотропных веществ, которые определены в утвержденном Постановлением Правительства РФ от 30 июня 1998 г. № 681 «Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации», но и арго-наименований, используемых в среде наркоманов. Для примера приведем лишь сленговые названия марихуаны: анаша, башатумнай, бошки, гандж, гарик, драч, дурь, дым, жареха, конопа, конопель, маняга, марго, маруся, маруха, молоко, план, пласт, пластилин, табакерка, трава, травка, шала, шан, шишки, шмаль. Вывод: предлагаем родителям и педагогам ознакомиться со сленговыми наименованиями наркотических средств и психотропных веществ на сайте «Нет наркотикам»¹, внимательно следить за употреблением таких слов ребенком, своевременно реагируя на попытку вовлечения его в «нарко-культуру».

5) Сайты, разжигающие расовую, национальную, религиозную рознь и вражду, а также иные формы экстремизма. Данный вид контента хотя и является объектом пристального внимания со стороны правоохранителей, его оборот пресекается в достаточно короткие сроки, однако сама по себе идеология экстремизма характерна для молодых людей в силу малого жизненного опыта, идеальности и максимализма во взглядах. Порой, достаточно одного факта несправедливого обращения или оскорбления и ребенок становится сторонником дискриминации какой-либо социальной группы. Молодежный экстремизм нередко представляет из себя лишь протест и браваду, обусловленные психологическим стремлением обозначить свой статус в социуме посредством дискриминации «чужой» группы людей. Такой группой могут быть как учащиеся соседней школы или болельщики спортивной команды-противника, так и иностранцы или иноверцы. Криминологические исследования говорят о том, что свидетелями или участниками конфликтных ситуаций на почве разной национальной или религиозной принадлежности становятся более трети школьников¹. Вывод: следует следить за высказываниями ребенка, осуждающими или превозносящими одну социальную группу над другой, своевременно проводя профилактико-корректирующие беседы о равенстве всех людей в правах и исторических последствиях главенства идей нацизма и фашизма.

6) Интернет-порталы, пропагандирующие насилие и девиантные формы поведения встречаются несколько реже, так как с самой криминальной идеологией ребенок зачастую знакомится «на улице». Вместе с тем, заинтересовавшись, он может свободно найти в Интернете интересующую его информацию и даже смоделировать преступное поведение с использованием игр типа «Тюряга», «Мафия», «GTA» и др. Некоторые из таких игр свободно доступны в качестве приложений в социальных сетях. Вывод: Обращайте внимание на видео-контент, игры и приложения в социальных сетях, которыми заинтересован Ваш ребенок (ученик). Помните, что запрет на просмотр или игру не является однозначным способом профилактики девиантного поведения ребенка. Целесообразно предпринять попытку «заменить» интерес к преступной идеологии другой информацией или занятием.

7) Религиозные секты, повсеместно имеющие веб-представительство наиболее опасны для детей, надлежащий надзор за которыми со стороны родителей, государства и общества не осуществляется. «Виртуальный собеседник» на подобных сайтах может существенно повлиять на мировоззрение подростка, склонить его к совершению преступления «во имя веры», саморазрушению или вовлечь в экстремистскую организацию.

8) Должный уровень защиты ребенка от вредоносной информации в сети «Интернет» может быть обеспечен, если сам родитель является уверенным пользователем современных информационно-коммуникационных систем и технологий. Для полноценного развития в этой сфере рекомендуем родителям освоить Интернет-лексикон, представленный в приложении к настоящим методическим рекомендациям.

Рекомендации родителям по обеспечению информационной безопасности ребенка 7-8 лет

Поведенческая характеристика несовершеннолетних в возрасте от 7 до 8 лет в сети «Интернет». Для несовершеннолетних в указанном возрасте характерна конкретность мышления, большая впечатлительность, любознательность, и вместе с тем неумение долго концентрировать свое внимание на чем-либо. Несмотря на то, что в данном возрасте авторитет взрослого еще высок, в сети Интернет несовершеннолетние преимущественно стараются посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых они не получили бы от родителей. Поэтому родителям (законным представителям) особенно полезны будут:

- изучение вкладки «История» в установленных на компьютере Интернет-браузерах;
- изучение отчетов программ по ограничению использования Интернета (так называемый «Родительский контроль»);
- изучение временных файлов Интернет (по общему правилу папка C:\Users\User\AppData\Local\Temp в операционной системе Windows 10);

Желательно, чтобы ребенок не видел и не знал о подобном контроле со стороны родителей, ведь тогда у него не будет ощущение, что за ним постоянно следят. В свою очередь, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по сети Интернет, используют электронную почту, заходят на сайты и чаты, не рекомендованные для несовершеннолетних. Следует помнить, что лучшим способом профилактики девиации несовершеннолетних под воздействием Интернет-среды остается совместное использование компьютера. Это особенно актуально для детей в раннем возрасте.

Рекомендуемые для родителей правила безопасного поведения в Интернет для детей в возрасте 7-8 лет:

- 1) создайте список домашних правил посещения сети «Интернет» при участии детей и требуйте его выполнения;
- 2) требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;
- 3) персональный компьютер с подключением в сеть «Интернет» должен находиться в общей комнате под присмотром родителей. Ноутбуком, планшетным компьютером или мобильным телефоном с подключением к сети Интернет ребенок должен пользоваться также под присмотром родителей;
- 4) используйте предназначенные для детей поисковые системы (например, <http://www.kinder.ru>, <http://kids.quintura.ru> и другие). Перед тем, как рекомендовать ребенку пользоваться конкретной поисковой системой, попробуйте самостоятельно ввести в нее несколько поисковых запросов, так как не все подобные системы фильтруют негативный контент эффективно;
- 5) используйте средства блокирования нежелательного контента как дополнение к стандартному «Родительскому контролю»;
- 6) создайте общий для всей семьи электронный ящик и аккаунт в социальной сети, чтобы у ребенка не возникала необходимость создавать собственные;
- 7) приучите детей советоваться с вами перед распространением какой-либо информации посредством сети Интернет (через электронную почту, в чате или форме, на странице аккаунта);

- 8) научите детей не загружать файлы, программы или музыку без вашего согласия;
- 9) в «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией;
- 10) беседуйте с детьми об их друзьях в «Интернет», как если бы речь шла о друзьях в реальной жизни;
- 11) приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Рекомендации родителям по обеспечению информационной безопасности ребенка 9-12 лет

Поведенческая характеристика несовершеннолетних в возрасте от 9 до 12 лет в сети «Интернет».

Несовершеннолетние в этом возрасте отличаются внутренней уравновешенностью, большой жизнерадостностью, постоянным стремлением к активной практической деятельности, их увлекает совместная коллективная деятельность. Эмоции занимают важное место в психике этого возраста, им подчинено поведение несовершеннолетних. Дети этого возраста весьма дружелюбны, контактны, их захватывают игры, приключения, поиск, они весьма расположены к эмоционально окрашенным обычаям жизни, ритуалам и символам.

В данном возрасте дети, как правило, уже слышаны о том, какая информация существует в сети «Интернет». Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств «Родительского контроля».

Правила безопасного поведения за компьютером для детей в возрасте от 9 до 12 лет:

- 1) совместно с ребенком создайте список домашних правил посещения «Интернет» и контролируйте их выполнения;
- 2) требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером;
- 3) объясните ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь;
- 4) персональный компьютер с подключением в сеть «Интернет» должен находиться в общей комнате под присмотром родителей. Ноутбуком, планшетным компьютером или мобильным телефоном с подключением к сети Интернет ребенок должен пользоваться также под присмотром родителей;
- 5) используйте средства блокирования нежелательного контента как дополнение к стандартному «Родительскому контролю»;
- 6) не забывайте беседовать с детьми об их друзьях в «Интернет»;
- 7) настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по «Интернет». Объясните, почему подобные встречи для него опасны;
- 8) позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними;
- 9) приучите детей никогда не передавать персональные данные и иную личную информацию через «Интернет» без вашего разрешения;
- 10) приучите детей не загружать и не устанавливать программное обеспечение без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы и уничтожить важную для них и для вас информацию;
- 11) создайте вашему ребенку ограниченную учетную запись для работы на компьютере;
- 12) проследите, что при регистрации аккаунтов в социальных сетях ребенок указал свой реальный возраст, имя и фотографию. С одной стороны это обеспечит внутреннюю фильтрацию доступного ему контента, а с другой повысит социальную ответственность ребенка за размещаемую в сети информацию;

13) приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с «Интернет». Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях;

14) настаивайте на предоставлении вам доступа к аккаунтам электронной почты и социальных сетей для осуществления контроля за их коммуникацией;

15) объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Рекомендации родителям по обеспечению информационной безопасности подростка 13-17 лет

Поведенческая характеристика несовершеннолетних в возрасте детей от 13 до 17 лет в сети «Интернет». В этом возрасте подростки активно используют поисковые системы, пользуются социальными сетями, электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Юношам в этом возрасте свойственен социальный протест и нигилизм, максимализм в высказываниях и действиях. Они могут стремиться к получению сведений об азартных играх, насилии и жестокости, экстремистской и порнографической информации. Девушки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в «Интернет». В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как последние уже знают о возможностях сети Интернет значительно больше своих родителей. Тем не менее, на этом этапе особенно важно строго соблюдать правила Интернет-безопасности, как можно чаще просматривать отчеты о деятельности детей в «Интернет». Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете.

Правила безопасного поведения за компьютером для несовершеннолетнего в возрасте от 13 до 17 лет:

1) создайте список домашних правил посещения «Интернет» при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в сети «Интернет», руководство по общению в сети «Интернет» (в том числе в чатах);

2) персональный компьютер с подключением в сеть «Интернет» должен находиться в общей комнате под присмотром родителей. Ноутбуком, планшетным компьютером или мобильным телефоном с подключением к сети «Интернет» ребенок должен пользоваться также под присмотром родителей;

3) не забывайте беседовать с детьми об их друзьях в сети «Интернет», о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы;

4) используйте средства блокирования нежелательного контента как дополнение к стандартному «Родительскому контролю»;

5) необходимо знать, какими социальными сетями и чатами пользуются ваши дети. Не забывайте, что современный мобильный телефон – это полноценный компьютер, обладающий равными с ноутбуком или персональным компьютером возможностями;

6) настаивайте на том, чтобы дети без вашего разрешения не встречались лично с друзьями из сети «Интернет». Ненавязчиво контролируйте эти встречи;

7) приучите детей никогда не передавать персональные данные и иную личную информацию через «Интернет» без вашего разрешения;

8) приучите детей не загружать и не устанавливать программы без вашего разрешения;

9) приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с «Интернет». Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях;

- 10) помогите ребенку защититься от спама. Научите не выдавать в «Интернет» своего реального электронного адреса, не отвечать на нежелательные письма и правильно использовать специальные почтовые фильтры;
- 11) просматривайте сайты, которые посещает ваш ребенок;
- 12) объясните ребенку, что «Интернет» – реальное социальное пространство. Также как и в реальной жизни здесь нельзя хулиганить, распространять сплетни или угрозы;
- 13) обсудите с ребенком проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Перечень Интернет–терминов, знание которых необходимо родителям для обеспечения информационной безопасности ребенка

Администраторы, модераторы сайта – специальные сотрудники соответствующей организации или физические лица, которые следят за исполнением установленных на сайте правил.

Аккаунт – учетная запись, регистрационная запись.

Антивирус – комплекс компьютерных программ, предотвращающий проникновение вирусов на компьютер, осматривающий содержимое компьютера на предмет наличия вирусов. Антивирус также «лечит» или удаляет зараженные файлы.

Браузер – специальная программа, предназначенная для просмотра страниц сайтов в сети «Интернет». Например, Google Chrome, Opera, Mozilla Firefox и другие.

Веб-сайт – страница или группа страниц, объединённых единой тематикой, автором, организацией и т.п. Имеет определенный адрес в сети «Интернет».

Виртуальный собеседник – компьютерная программа, которая создана для имитации речевого поведения человека при общении с одним или несколькими пользователями.

Домен, доменный адрес – Область пространства иерархических имен сети «Интернет», которая обозначается уникальным доменным именем, обслуживается набором серверов доменных имен (DNS). Для каждого зарегистрированного доменного имени определен единственный Администратор. Это более практичный аналог IP-адреса. Доменная адресация возникла в «Интернет» для удобства пользователей: легче запомнить доменный адрес (например, www.microsoft.com), чем четыре числа IP-адреса. Доменный адрес может содержать латинские буквы, цифры, точки и некоторые другие знаки.

Интернет-магазин – интерактивный сайт, где рекламируются товары и услуги, принимаются заказы на товары и услуги, посетителю, предлагаются различные варианты оплаты заказанных товаров и услуг, возможна их мгновенная оплата через «Интернет».

Логин – имя, которое вы выбираете для регистрации в системе или имя, которое система вам сама присваивает. Каждый пользователь в системе имеет свой уникальный логин. Он помогает системе и другим пользователям отличить одного пользователя от другого.

Новые СМИ или новые медиа – интерактивные электронные издания и новые формы коммуникации производителей контента с потребителями. Существенно отличаются от традиционных медиа (газеты, радио, телевидение).

Онлайн игры – игровой процесс, основанный на взаимодействии с другими игроками и виртуальным игровым миром, требующий постоянного подключения к сети «Интернет».

Пароль – набор символов, известный только одному пользователю, необходимый для авторизации (входа) на сайт или получения полного доступа к его функционалу.

Персональная страница – совокупность веб-страниц, с содержанием, описывающим сферу интересов какого-либо человека (группы лиц), обычно созданная им самим.

Почтовый ящик – дисковое пространство на почтовом сервере, выделенное для отправки писем пользователя, их получения и хранения. Имеет определенный адрес, состоящий из логина, значка «@», наименования хоста и домена.

«Родительский контроль» – программы и службы, которые позволяют родителям (иным законным представителям) несовершеннолетнего отслеживать, как ребенок использует компьютер посредством фильтрации веб-содержимого, управления контактами

электронной почты, ограничения на общение через Интернет. Функционал «родительского контроля» постоянно расширяется и совершенствуется.

Сервер – компьютер или специализированное устройство в сети со специальным программным обеспечением, обеспечивающий доступ многих пользователей к расположенной на нем информации и функционирование любых необходимых сервисов «Интернет»; сайт, крупный информационный ресурс «Интернета».

Социальные сети – сайты в «Интернет», на которых пользователи создают личные аккаунт-страницы для коммуникации с другими пользователями. К наиболее характерным чертам социальных сетей следует отнести систему «друзей» и «групп», возможность обмена не только текстовыми сообщениями, но и музыкальными композициями, графическим и видео контентом. Самые популярные русскоязычные социальные сети: «ВКонтакте» и «Одноклассники».

Спам – рассылка не запрашиваемой коммерческой и иной нежелательной рекламы или иных видов сообщений лицам, не выразившим желания их получать.

Трафик – поток (объем) информации, проходящей через канал связи, приходящийся на сайт. Может быть исходящим и входящим.

Тролли, троллинг – размещение в «Интернете» провокационных сообщений с целью вызвать конфликты между субъектами, взаимные оскорбления и т. п.

Файл – форма хранения информации на компьютере. Они могут быть текстовые, музыкальные, видео, графические, мультимедийные и иные. Файлы можно создавать, копировать, пересылать (например, по электронной почте), выкладывать на сайт для скачивания, скачивать, то есть сохранять на свой компьютер.

Фишинг – вид мошенничества в «Интернет», когда у пользователя пытаются узнать логины и пароли, позволяющие, как правило, совершить хищение или открывающие доступ к ценной информации в сети.

Хостинг – услуга по предоставлению интернет-сервера и обеспечению его круглосуточной работоспособности. В большинстве случаев предоставляется виртуальный сервер (т.н. виртуальный хостинг), т.е. программное обеспечение, обеспечивающее работу необходимых Вам сервисов, но работающее на одной аппаратной платформе с другими подобными виртуальными серверами. Различают также платный (коммерческий) и бесплатный хостинг.

«Черный список» или «Спам лист» – список сайтов, проектов или людей, которые проводят мошеннические операции в сети, нарушают требования закона, моральные нормы социального общения или не выполняют взятые на себя обязательства в сети «Интернет».

Электронная почта – технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети.