

**Приволжский межрегиональный центр
повышения квалификации и профессиональной
переподготовки работников образования К(П)ФУ**

***Современные подходы к обеспечению безопасной
работы детей в сети Интернет***

Сафин Алексей Алексеевич,
кандидат педагогических наук

Одна из важнейших проблем современного общества – особенности **социализации** современных детей и подростков в условиях стремительно нарастающих информационных потоков, прежде всего в электронном пространстве.

Сеть Интернет уже стала естественной коммуникационной средой для подрастающего поколения и оказывает безусловное влияние на мировоззрение и поведение школьников.

Основные тенденции развития современного информационного общества:

1. **Виртуализация** социальных практик, перемещении определяющих личность сфер из реальной формы бытия в цифровую.

Характеризуется как **особый вызов и экзистенциальный риск**, поскольку современный человек удовлетворяет многие свои потребности, связанные с коммуникацией, образованием, творчеством, семьей, благодаря виртуальной среде.

Перенос ценностей в виртуальную среду приводит к **зависимости** от нее и одновременному **ослаблению** реальных социальных связей.

2. Параллельно с виртуализацией социальной среды происходит **виртуализация социальных угроз и рисков**, которые практически беспрепятственно существуют в Интернете и активно воздействуют на различные категории его пользователей.

Исследователями установлено, что более высокие уровни **онлайн-активности** напрямую коррелируют с более высокими **онлайн-рисками**.

Дети и подростки – представители «цифрового поколения» – являются активными пользователями Интернет и крайне часто проявляют при этом беспечность, будучи убеждены в безопасности своих личных компьютеров и мобильных устройств.

Установлено, что **дети младшего школьного возраста** весьма чувствительны к негативному интернет-контенту, в **подростковом возрасте** доступность негативной интернет-информации (виртуальные развлечения, контакты в интернет-сообществах и т. п.) могут послужить причинами **девиантного поведения**.

Информационные риски в сети Интернет проявляются в трех основных категориях :

- в **контенте** (например, сайты сексуального, экстремистского, деструктивного, террористического характера)
- в **контактах** (например, буллинг на веб-сайтах и в онлайн-чатах, социальных сетях, с мгновенными сообщениями, онлайн-игровыми сайтами, использованием мобильных телефонов, цифровых медиа- и игровых консолей, встречи с онлайн-контактами в реальном мире и др.)
- в сфере **коммерции** (например, промышленный шпионаж, кража финансовых средств с электронных финансовых инструментов, нарушение авторских прав, вирусы, спам нежелательных коммерческих предложений и др.)

Среди **проблем безопасности детей** в информационном пространстве необходимо выделить факторы:

- влияния технологий современной мобильной связи;
- воздействия рекламы на юную аудиторию, а также восприятие содержания рекламных сообщений детско-юношеской аудиторией;
- определения так называемых «групп риска» с повышенной вероятностью негативного воздействия со стороны недобросовестных масс-медиа;

- реакции детей на новые жанры медиа и медиатекстов, например, реалити-шоу;
- характер интерактивного взаимодействия юных пользователей в сети Интернет, их реакция на определенные информационные ресурсы, оценка надежности найденной информации и т.д.

С точки зрения наиболее опасных для школьника **информационных угроз** попробуем составить следующую классификацию:

- угрозы обмана с целью наживы и/или физического воздействия;
- угрозы физического, нравственного и психологического воздействия;
- угрозы утечки конфиденциальной информации.

Отметим, что на сегодняшний день нет ни одной школьной дисциплины, дающей необходимые знания и умения, подготавливающие учащихся к снижению опасностей динамично изменяющейся информационной образовательной среды.

А между тем, актуализация проблем информационной безопасности учащихся от года к году возрастает, особенно при рассмотрении этой проблемы с позиций информационной социализации.

В соответствии с российским законодательством информационной безопасностью детей считается состояние защищенности детей, где отсутствует риск, который связан с причинением информацией, в т.ч. распространяемой в Интернете, вреда их здоровью, психическому, физическому, нравственному и духовному развитию.

Такую защищенность для ребенка должны обеспечить, в первую очередь, **родители и школа!**

Меры по снижению угроз информационного воздействия на детей:

- 1) ознакомление учащихся с видами информации, которая способна навредить здоровью и развитию несовершеннолетних, запрещена или ограничена для распространения по территории РФ, а также с негативными последствиями распространения подобной информации;
- 2) информирование школьников о методах незаконного распространения данной информации в сети Интернет и мобильной (сотовой) связи (включая рассылку SMS-сообщений с незаконным содержанием);
- 3) обучение учеников аспектам международных норм, нормативных правовых актов РФ, которые регулируют вопросы, касающиеся информационной безопасности несовершеннолетних

4) обучение учащихся правилам безопасного и ответственного пользования услугами сети и сотовой связи, иными электронными средствами связи и коммуникации, в т.ч. способам защиты от противоправных и других опасных посягательств в сети, конкретно, от способов разрушительного действия на психику детей, таких как кибербуллинг, означающий жестокое обращение с детьми в виртуальной среде и буллицид, подразумевающий доведение ребенка до суицида посредством психологического насилия;

5) профилактика у школьников игровой зависимости (игромании, гэмблинга) и интернетзависимости;

6) снижение риска совершения школьниками противоправных действий с применением информационно-телекоммуникационных технологий.

В процессе обучения правилам информационной безопасности дети должны приобрести компетенции:

- уметь с критикой относиться к различным сообщениям и другой информации, которую распространяю в сетях Интернет, мобильной (сотовой) связи, с помощью других электронных средств массовой коммуникации;
- уметь отличать достоверную информацию от недостоверной, вредную от безопасной;
- уходить от навязывания учащимся сведений, способных навредить их здоровью, психическому и нравственному развитию, репутации, чести и достоинству

- разоблачать признаки злоупотребления доверчивостью и неопытностью подростков, попытки их вовлечения в противоправную антиобщественную деятельность;
- распознавать манипулятивные техники, которые используются при подаче рекламной информации;
- с критикой относиться к информационной продукции, которая распространяется в информационно-телекоммуникационных сетях;
- уметь анализировать уровень достоверности данных и подлинность их источников;
- применять меры самозащиты от нежелательных для них сведений и контактов в сетях.

Применение разнообразных форм проведения профилактической работы, которые будут способствовать эффективному формированию информационной безопасности у всех участников образовательного пространства, так как формирование информационной культуры и безопасности – **процесс длительный и сложный, но важный и необходимый.**

Меры по обеспечению информационной безопасности учащихся должны обуславливаться, **возрастными, физиологическими и психологическими особенностями детей как формирующейся личности** и тем фактором, что они, по сравнению с другими представителями общества, гораздо более подвержены негативному воздействию информации, которая может нанести вред их **здоровью, психическому и нравственному развитию.**

Использованная литература

- 1.Федеральный закон Российской Федерации от 28 июля 2012 г. N 139-ФЗ "О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации»
- 2.Письмо МИНОБРНАУКИ РОССИИ от 28.04.2014 № ДЛ-115/03 «О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет»
- 3.Федеральный закон от 29 декабря 2010 года г. № 436-ФЗ (в ред. Федеральных законов от 28.07.2012 N 139-ФЗ, от 05.04.2013 N 50-ФЗ, от 29.06.2013 N 135-ФЗ,от 02.07.2013 N 185-ФЗ, от 14.10.2014) "О защите детей от информации, причиняющей вред их здоровью и развитию»
- 4.Письмо Минкомсвязи России от 14.08.2012 № 52-165/ВА "О применении норм Федерального закона от 29 декабря 2010 г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию»

Использованная литература

5.Письмо Минобрнауки России от 28.04.2014 № ДЛ-115/03 "О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет»

6.Приказ Минкомсвязи России от 16.06.2014 № 161"Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию" (Зарегистрировано в Минюсте России 12.08.2014 №33555)

7.Рекомендации по применению Федерального закона от 29 декабря 2010г. № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" в отношении печатной (книжной) продукции" (утв. Минкомсвязи России 22.01.2013 № АВ-П17-53)

8.Статья 13 Федерального закона от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» (пунктом 7 Положения о Министерстве юстиции Российской Федерации, утвержденного Указом Президента Российской Федерации от 13.10.2004 № 1313, на Минюст России возложены функции по ведению, опубликованию и размещению в сети Интернет федерального списка экстремистских материалов.
<http://www.minjust.ru/nko/fedspisok> - Федеральный список экстремистских материалов