«Безопасность в киберпространстве».

Проникновение глобальной сети во все сферы жизнедеятельности современного общества привело к вовлечению в информационное пространство и подрастающего поколения. Если ещё десять лет назад не все взрослые применяли возможности Интернета, то сегодня уже дети 5-6 лет активно пользуются Интернет-сервисами. Просмотр видеоконтента (мультипликационные фильмы, фильмы о природе и т.д.), развивающие игры, элементарный поиск необходимой информации, общение в социальных сетях - вот далеко неполный перечень функций Интернета для школьников.

Сегодня для обозначения этого глобального информационного пространства, состоящего из множества компьютеров, устройств, их соединяющих, спутников и позволяющего организовать общение через социальные сети, чаты, телефонные разговоры, передачу больших объемов данных на очень высокой скорости, используют термин - киберпространство.

В киберпространстве действуют законы и правила, которые мы и наши дети должны соблюдать. Поэтому, говоря о безопасности в нем, используют специальный термин – кибербезопасность. Это набор методов и способов, предназначенных для защиты компьютеров, компьютерных сетей, программ и данных от несанкционированного доступа к информации, от её копирования, изменения или уничтожения.

Всё ли безопасно и прозрачно? Почему 21 декабря 2010 года Государственная Дума приняла Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»? Именно в нем было введено понятие информационной безопасности детей как «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию». Зачем на всех уровнях школьного образования вводится новый курс «Основы кибербезопасности»? Почему во всех школах Российской Федерации компьютеры оснащены программами-фильтрами?

Рассмотрим причины столь внимательного отношения к использованию сети Интернет учащимися школ.

В возрасте 6-7 лет, когда дети приходят в школу меняется не только их социальный статус (они становятся учениками), но и взаимоотношения с окружающим миром. У младших школьников появляются новые обязанности, связанные, прежде всего, с выполнением домашних заданий и дополнительных поручений классного руководителя, новая информационная среда для активного участия в школьной жизни. Речь идет о Дневник.ру. Школьники и их родители подключаются к данной системе и применяют все её возможности. Дети узнают оценки, домашние задания, обсуждают мероприятия и новости школы, превращают личную страницу в портфолио, где рассказывают всем о своих достижениях. В этот же период младшие

школьники начинают осваивать и другие социальные информационные среды: ВКонтакте, Одноклассники.ru, Instagram, которые в отличие от Дневник.ру не являются закрытыми и безопасными. Именно эти новые сферы общения таят для детей множество опасностей.

Дети любят смеяться и шутить. Однако будучи достаточно сильно удаленными друг от друга и не имея возможности воочию увидеть реакцию других на свои действия и шутки, некоторые школьники переступают моральные границы в отношениях со своими сверстниками. Незначащие шутки в социальных сетях иногда достигают размеров серьезной травли, последствия которой могут быть самыми трагическими. Психологи выделили виды агрессии в Интернете: троллинг, флейм, нападки, клевета, самозванство.

Для описания таких моральных атак на детей был введен термин «кибер-хулиганство». Отличительной особенностью кибер-хулиганства является возможность стать жертвой в своем собственном доме, на глазах близких людей. Сегодня выделены виды кибер-хулиганства. Прежде всего, речь идет о кибер-буллинге, по-другому, интернет-травле. Кибер-буллинг страшен тем, что травля в сети проходит более жёстко, чем в обычной жизни, а её последствия могут быть совершенно незаметны для взрослых. Порочащие честь и достоинство комментарии к фотографиям знакомых и незнакомых ребят, сообщения, лживые новости о том или ином человеке – вот далеко неполный перечень противоправных действий, которые может совершить человек в сети, ощущая себя при этом абсолютно безнаказанным. Особенностью кибер-буллинга является то, что один и тот же ребёнок может одновременно быть и участником одной травли и жертвой другой. Согласно данным проведённого IT-компанией «Лаборатория Касперского» исследования, 13% сетевых конфликтов переросли в реальные, 7% оставили у детей тяжелейшие психологические травмы, при этом 26% родителей узнали о них позже, чем они начались.

Ещё одним видом кибер-хулиганства является кибер-груминг, который предполагает вхождение в доверие к ребёнку любого возраста c целью использования его в сексуальных целях. Преступники, опираясь на знание психологических особенностей развития детей разных возрастных периодов, начинают общение с ними, втираются в доверие, стремятся стать другом и из виртуального общения пытаются перейти в реальное. Детям самостоятельно очень сложно справиться с такими «доброжелателями», так как они прилагают максимум усилий для того, чтобы полностью подчинить себе жертву.

Выделяют ещё один вид кибер-груминга - настойчивое цепляние в сети c сексуальными предложениями, разговоры на темы секса, насилия и (или) изготовления, распространения и использования материалов со сценами насилия над детьми (в большинстве случаев - сексуального).

Желание иметь много друзей, общаться, чувствовать себя в центре событий особенно характерно для школьников подросткового возраста. Но этим детям присуща и растущая неуверенность в себе, стремление понять, кем стать в будущем, чем заниматься, в чем смысл жизни и где грани этой

жизни. Некоторые подростки впадают в депрессию. Они перестают нормально спать, общаться с родителями, у них теряется интерес ко всем своим прежним увлечениям и к учебе в школе, возникает ощущение постоянной усталости. Всё это заставляет подростков в Интернете искать ответы на то, что с ними происходит, погружаясь в него всё глубже и глубже. И здесь для детей появляются новые опасности и риски: сообщества, секты, группы смерти и т.д. Обычно их создатели – это люди с хорошим знанием психологии и медицины. Они знают, как поддержать ребенка, приободрить, стать другом, заставить сделать то, что им надо.

Особое беспокойство в последнее время вызывают так называемые «необычные» on-line игры и «группы смерти».

В марте 2017 года на Первом канале шел выпуск программы «Осторожно «Синий кит»». Впервые на центральном канале официально было сказано о существовании «групп смерти». Ведущие пригласили родителей погибших детей. Они рассказали о том, как ушли из жизни их дети, объяснили, что ничего необычного не происходило, единственное общее состояло в том, что дети в последние несколько дней стали более печальные и грустные. Эта передача вызвала большой общественный резонанс. 12 сентября 2017 на Первом канале выпуск программы «Время покажет», названный «Жнецы смерти», был посвящен обсуждению вопроса, кто же на самом деле стоит за детскими суицидами и «группами смерти» в социальных сетях. Тема выпуска – задержание кураторов «групп смерти». К удивлению зрителей, кураторами оказались школьники 14-15 лет - юноша и две девушки из Владимирской, Самарской и Нижегородской областей. Они использовали социальную сеть для рассылки опасных для жизни других детей заданий и для угроз в адрес тех школьников, которые отказывались выполнять их.

В августе 2017 года на Первом канале появилась информация о задержании в разных частях страны двух администраторов «групп смерти». Как показало следствие, подозреваемые изучали научные труды по психологии Фрейда и Роджерса, они вели записи, в которых отражали имена своих жертв, описывали их психологические проблемы, статистику совершенных злодеяний.

Кроме описанных выше рисков использования сети Интернет, к ним можно отнести и посещение учащимися сайтов, распространяющие вредоносные программы. В основном это происходит при подготовке домашних заданий, например, в форме доклада. Ребёнок ищет информацию, его вниманию предлагается книга с обещанием того, что в ней он найдёт всё необходимое. О том, что этот файл может быть потенциально опасным, школьник и не задумается. Речь идёт об исполняемых файлах, которые инициируют запуск вредоносного программного обеспечения. Особенностью данных файлов является то, что их расширение может быть двойным, например, \*.pdf.exe или \*.jpg.exe. Школьники видят главным образом первую часть названия, скачивают файл и, не вдумываясь, соглашаются с запуском программы. В результате, вредоносный код внедряется в программное обеспечение компьютера, и злоумышленники достигают своей цели:

скачивают данные, нарушают корректную работу компьютера, приобретают контроль над всеми его ресурсами.

Если в описанной ситуации школьники являются жертвами, то при скачивании контента, защищенного авторским правом, они фактически становятся преступниками. Большинство детей считают, что всё выложенное в сети является абсолютно доступным для копирования и использования. Некоторые допускают мысль о необходимости указания автора и адреса, по которому была найдена информация. Однако если обратиться к статье 1229 «Исключительное право» Гражданского кодекса РФ, то в ней указано, что «правообладатель может по своему усмотрению разрешать или запрещать другим лицам использование результата интеллектуальной деятельности или средства индивидуализации. Отсутствие запрета не считается согласием (разрешением)». Таким образом, если автор явно не дал согласие на копирование своего материала, то применение его будет незаконным и повлечёт за собой ответственность. Именно этого и не понимают большинство школьников, скачивая художественные и мультипликационные фильмы, музыку, игры. Ситуация обостряется при распространении такого контента. Поделиться с другом в социальной сети новой игрой, выложить в группу для всеобщего просмотра интересный фильм, отправить по электронной почте, понравившийся музыкальный хит - вот неполный список противоправных действий, совершаемых школьниками ежедневно.

Риск попасть в неприятную ситуацию возникает у детей и при работе с сайтами, предлагающими пользователям разбогатеть. Текст рекламы может быть различный, но основной мотив заключается в обещании большой финансовой прибыли и отсутствии какой-либо работы. При этом приводятся лжепримеры людей, якобы выигравших крупные суммы денег. Дети попадаются на такие призывы, и смело начинают действовать, тратя деньги своих родителей. Указание ребенком в социальной сети своего номера телефона позволяет мошенникам в дальнейшем отправлять ложные SMS сообщения о розыгрыше велосипеда, автомобиля и т.д. с просьбой отправить в ответ сообщение с некоторым текстом, например, «я счастливчик». Итогом такой операции будет снятие денег со счета мобильного телефона.

К последнему может привести и покупка каких-либо товаров в Интернет-магазинах. Некоторые из них предлагают скидки в обмен на предоставление информации о себе, например, номер мобильного телефона, адрес местожительства, паспортные данные родителей и т.д. Желание сэкономить движет школьниками при передаче посторонним лицам своих персональных данных. Дети просто не задумываются о серьёзности последствий своих поступков.

Рассмотрим средства и методы снижения рисков использования киберпространства школьниками.

Прежде всего, речь идёт об установке программ-фильтров. Они позволяют блокировать рекламу опасного характера, сайты экстремистской и «взрослой» направленности, защищают от вирусов и т.д. В основу разработки таких программ положена одна из технологий фильтрации либо их комбинация:

1) фильтрация по ключевым словам (конкретные слова и словосочетания используются для включения блокировки веб-сайта),

2) динамическая фильтрация (содержимое запрашиваемого веб-ресурса анализируется в момент обращения. Загрузка страниц ресурса в браузер блокируется, если содержимое определяется как нежелательное),

3) URL фильтрация (запрашиваемая страница или целый домен могут быть определены или категоризированы как нежелательный ресурс, вследствие чего доступ к таким страницам блокируется).

Примерами контент-фильтров, обеспечивающих соблюдение российского законодательств, касающегося защиты школьников от опасных Интернет-ресурсов, являются SkyDNS.Школа, ContentWasher, NetPoliceChild, KasperskyInternetSecurity, Интернет цензор.

Применение облачного контент-фильтра SkyDNS, блокирующего доступ к опасным сайтам еще до передачи информации с таких ресурсов, предполагает отсутствие необходимости ставить какое-либо программное обеспечение на компьютеры. Система родительского контроля SkyDNS защищает как отдельные компьютеры и мобильные устройства, так и всю домашнюю сеть через подключение к системе домашнего Wi-Fi роутера.

Особенностью SkyDNS является действие поисковой системы poisk.skydns.ru, дополнительно фильтрующей все поисковые запросы на предмет запрещенного контента. Разработчики обеспечивают корректную работу поисковой системы путем регулярного отслеживания запрещенных сайтов.

В течение 15 дней можно использовать данную систему бесплатно.

Ещё одной российской разработкой является KasperskySafeKids, который не только защищает детей от поиска неподходящих сайтов и информации, но и регулирует применение программ на компьютере, осуществляет контроль времени использования устройств, позволяет следить за публикациями ребенка в Facebook и ВКонтакте с помощью портала MyKaspersky.

Программа ContentWasher характеризуется большой функциональностью: позволяет создавать белый и черный список сайтов, блокировать социальные сети, ограничивает использование компьютера ребенком по времени. Кроме того, ContentWasher блокирует сайты, содержащие запрещенные слова, проверяет ICQ сообщения и сообщения электронной почты, блокирует рекламу, поддерживает режим безопасного поиска картинок, ограничивает запуск игр и программ.

Сайт «Спасение Детей от Киберпреступлений» представляет одноименную общественную организацию, созданную 19 января 2016 года родителями детей, погибших в результате киберпреступлений.

Основная цель деятельности организации состоит в выявлении противоправных действий в отношении детей в Интернете, в предотвращении преступлений, в организации помощи пострадавшим детям и их родителям. На сайте представлены статьи по рассматриваемой проблематике, приведены законы, которые определяют ответственность взрослых, представлены памятки для родителей и детей: «Безопасный интернет», «Смертельно опасное воздействие на ребенка в соцсетях», «Права, обязанности и ответственность родителей». Кроме того, родители могут посмотреть документальные фильмы, передачи, репортажи, интервью, повествующие о киберпреступлениях и способах борьбы с ними, ознакомиться с процессом настройки родительского контроля в операционной системе семейства Windows.

Аналогичную функцию выполняет сайт Синий кит. Для того чтобы бороться с врагом, необходимо знать его привычки, особенности поведения, слабости, страхи. Именно поэтому разработчики сайта представили всю актуальную информацию о так называемой игре «Синий кит». Прежде всего, на сайте родители могут найти описание игры, её специфики, предлагаемые задания, причины участия детей в этой игре. Речь идёт о самом сложном возрасте – переходном. Когда ребёнок пытается разобраться в том, что ему нужно, понять окружающий мир, чувствует дисгармонию внутри себя. Он ещё и не взрослый самостоятельный человек, но очень хочет таковым стать, при этом старших окружающих ему слушать уже не хочется. Они кажутся ему авторитарными, надменными. И здесь появляется человек («куратор»), который общается дружелюбно и располагающе: «Привет, кис. Что случилось?». Он втирается в доверие, и подросток начинает зависеть от этого общения. Родители становятся лишними, от них надо всё скрывать. Куратор постепенно внушает мысль о том, что «жить не зачем». Однако, если в процессе игры ребёнок приходит в себя, хочет выйти из нее, то на него начинается страшное давление и угрозы.

Подросток начинает бояться уже не за себя, а за родных людей. Он становится подавленным, у него возникает чувство страха, перемешанное с чувством безысходности, начинается депрессия. Для родителей разработчики сайта перечислили все основные признаки подростковой депрессии. Внимательный родитель всегда заметит соответствующие изменения в поведении ребёнка. В такой ситуации, как утверждает Бенджамин Шайн, «то, что родители должны сделать — это 90% времени слушать своего ребенка. Оставшиеся 10% следует потратить на то, чтобы помочь ему решить проблему».

Психологи рекомендуют говорить с детьми об Интернете:

«Регулярно разговаривайте об Интернете.

Расскажите ребенку об основных угрозах, с которыми он может столкнуться в Сети.

Будьте в курсе событий ребенка в реальной жизни и виртуальном пространстве.

Искренне интересуйтесь активностью ребенка в Интернете. Попросите его помочь вам завести аккаунт в социальной сети или игре, где он «обитает».

Расскажите о нормах онлайн-этикета.

Объясните необходимость защиты персональной информации. Любая личная информация, которую ребенок выкладывает в Сеть, может быть использована другими людьми против него. Расскажите ему про средства защиты персональных данных, помогите установить настройки приватности на всех посещаемых ресурсах.

Проинформируйте о том, где можно получить помощь.

Если ребёнок столкнётся с проблемой в Сети, он может обратиться к администрации сайта, в службу технической поддержки или к взрослому, которому он доверяет.

Станьте для ребенка примером ответственного онлайн-пользователя».

Кроме того, психологи советуют родителям вместе с детьми знакомиться с новинками компьютерных игр, обсуждать их, а порой и играть в онлайн-игры. Родители сами должны доверять детям и вызывать доверие у них. Именно такой подход позволит объяснить ребёнку, почему нельзя делиться в Интернете информацией личного характера, пересылать свои фотографии малознакомым людям, включать в состав друзей в социальных сетях всех, кто делает соответствующий запрос.

Если возникла неприятная ситуация, например, агрессия против ребенка с чьей-либо стороны, необходимо сохранять все полученные письма, файлы и изображения. С. Махринский и В. Тюменев рекомендуют записывать время и дату получения тех или иных сообщений, это поможет в дальнейшем при обращении в правоохранительные органы.