М Е Т О Д И Ч Е С К И Е Р Е К О М Е Н Д А Ц И И для родителей (законных представителей) по контролю за использованием несовершеннолетними сети Интернет во внеучебное время

1. Введение

Во всем мире придается большое значение защите несовершеннолетних от вредной для них информации в целях обеспечения нормального физического и психического развития.

Стремительное развитие информационных технологий заставило современное поколение детей и подростков столкнуться с принципиально новыми вызовами. Взросление, обучение и социализация детей проходят в условиях гиперинформационного общества. Процесс социализации через традиционные институты (семьи, школы) все активнее дополняется средствами массовой информации и массовых коммуникаций, особенно информационнотелекоммуникационной сетью «Интернет», которые становятся важнейшими институтами социализации, образования и просвещения нового поколения, в определенной мере замещая традиционно сложившиеся формы.

Современный подросток все меньше общается в реальной жизни со сверстниками, друзьями, одноклассниками. В среднестатистической семье телевизор включен до 7-8 часов в день, а центром внимания детей является компьютер – по статистике, на школьников приходится около 3-4 часа в день, что равнозначно пяти урокам в школе. Современные гаджеты и Интернет заменили детям прогулки на улице, общение со сверстниками и родителями. Сегодня в обществе актуальна следующая проблема – неограниченный доступ ребенка к сети Интернет.

Несмотря на прорыв в последние пять лет в развитии информационного права в России, новые риски и угрозы информационной и нравственно-психологической безопасности детей, связанные с развитием сети Интернет и мобильной связи требуют объединения усилий государства, профессионального сообщества, родительской общественности и иных институтов гражданского общества. Вызывает тревогу, что сегодня через информационные каналы продолжаются попытки навязывания деструктивных норм, ценностных ориентаций, образа жизни криминальной и маргинальной субкультур, явной и скрытой пропаганды потребления алкоголя, наркотиков, других психоактивных веществ, а также половой распущенности, пропаганды насилия и жестокости, агрессивного и суицидального поведения, воздействия на сознание и поведение несовершеннолетних религиозных и псевдорелигиозных тоталитарных сект, ориентированных в своей идеологии на разрушение традиций семейного воспитания, разрыв родственных связей своих членов, на сексуальное растление детей. Негативное воздействие указанной информации усугубляется реализацией игрушек и компьютерных игр, отрицательно влияющих на психическое здоровье и развитие детей, провоцирующих их на безнравственные действия, вызывающих проявления жестокости и агрессии.

Зачастую дети и подростки в полной мере не осознают все возможные проблемы, с которыми они могут столкнуться в сети. Сделать их пребывание в Интернете более безопасным, научить их ориентироваться в киберпространстве – важная задача для родителей и педагогов.

2. Онлайн-риски: что это такое

Риск – неотъемлемая часть человеческого существования и необходимое условие развития личности. Сегодня и в отечественной, и зарубежной науке все больше внимания уделяется проблеме онлайн-рисков, возникающих в процессе деятельности и общения в Интернете. Спектр проблем, с которыми дети и подростки имеют дело в сети, довольно широкий: от поломок программ и устройств до преследований и сексуальных домогательств.

4 категории онлайн-рисков

Все онлайн риски разделяются на четыре категории: коммуникационные, технические, контентные и потребительские риски, соответствующие четырем основным сферам деятельности в Интернете. В отдельную категорию выделяются обращения, связанные с интернет-зависимостью.

1. Коммуникационные риски (зона повышенной опасности).

Основное место, где дети и подростки сталкиваются с коммуникационными рисками, – это социальные сети.

Столкновение с коммуникационными рисками – наиболее серьезная проблема для детей и подростков и, по сравнению с другими типами онлайн-рисков, чаще причиняет ощутимый вред. Отчасти это обусловлено тем, что проблемы, связанные с онлайн-общением, не имеют простых и надежных технических решений. Антивирусы и программы фильтрации не могут защитить ребенка от травли или сексуальных домогательств. Кроме того, с коммуникационными рисками сложнее справиться самостоятельно.

Наиболее распространенные виды коммуникационных рисков — это кибертравля или кибербуллинг и различные формы сексуальных домогательств: секстинг, грумминг, онлайн-знакомства.

Коммуникационные риски – один из наиболее быстро эволюционирующих типов онлайн-рисков.

2. Технические риски (зона относительно контролируемых рисков).

Понятие технических рисков подразумевает повреждение устройств, имеющихся на них информации и программного обеспечения, а также кражу персональных данных в результате действия вредоносных программ.

К наиболее распространенным техническим рискам, с которыми могут столкнуться подростки, относятся: столкновение с вредоносными программами, взлом аккаунтов и потеря персональной информации.

Знание простых правил безопасности в большинстве случаев позволило бы избежать кражи личных данных, однако далеко не все российские подростки осознают необходимость защиты персональных данных и ведут себя в сети достаточно легкомысленно.

Школьники активнее, чем их родители, осваивают новые устройства и приложения, чувствуют себя в Интернете более уверенными и самостоятельными, поэтому они оказываются в состоянии сами позаботиться о своей безопасности. Все вместе это позволяет охарактеризовать техническую сферу как зону относительно контролируемых рисков.

3. Контентные риски (зона повышенного внимания родителей)

Контентные риски возникают в результате использования размещенных в сети материалов, содержащих незаконную или потенциально опасную информацию.

Столкновение с негативным контентом – самый распространенный тип онлайн-рисков.

К противозаконной, неэтичной и вредоносной информации относятся:

– пропаганда насилия, жестокости и агрессии;

– разжигание расовой ненависти, нетерпимости по отношению к другим людям по национальным, социальным, групповым признакам;

– пропаганда суицида;

– пропаганда азартных игр;

– пропаганда и распространение наркотических и отравляющих веществ;

– пропаганда деятельности различных сект, неформальных молодежных движений;

– эротика и порнография;

– нецензурная лексика и т.д.

Для школьников характерен упрощенно положительный образ Интернета, поэтому они склонны недооценивать негативное влияние информации, размещенной в Интернете. Взрослые, напротив, склонны переценивать угрозы, исходящие от онлайн-контента.

Хотя школьники примерно с одинаковой частотой сталкиваются в сети как с порнографией, так и с информацией, содержащей жестокость, насилие и агрессию, материалы сексуального характера вызывают негативную реакцию родителей чаще, чем информация про жестокость и насилие. Почему одни виды контента беспокоят родителей больше, чем другие?

Возможно, это связано с тем, что представления родителей о негативном контенте основываются на стереотипах общественного сознания. Взрослых, прежде всего, беспокоит контент, затрагивающий темы, о которых они не готовы говорить со своими детьми. Родителям проще незаметно следить за ребенком, используя программы контроля, чем поговорить с ребенком на «запретные темы».

Неэтичная и вредоносная информация может быть направлена на манипулирование сознанием и действиями различных групп людей. Такая информация часто бывает заманчивой и оказывает сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл происходящего и отказаться от просмотра и изучения сайтов с негативным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков – непредсказуемо; под воздействием таких сайтов может пострадать не только психика, но и физическое здоровье ребенка.

4. Потребительские риски (зона потенциальных угроз).

Понятие потребительских рисков включает приобретение некачественной или контрафактной продукции, потерю денежных средств и хищение персональной информации в процессе интернет-шопинга.

5. Интернет-зависимость (зона свободы от реальности).

Интернет-зависимость – это самостоятельный тип рисков, с которым сталкивается достаточно большое количество пользователей Интернета. Интернет, как насыщенное информационно-коммуникационное пространство, способствует формированию тенденции к бегству от реальности в иллюзорные виртуальные миры, характерной для подросткового возраста.

Наиболее распространенные симптомы чрезмерной увлеченности Интернетом – это потеря контроля в сети и синдром отмены.

Наиболее серьезный симптом интернет зависимости – это «замена реальности». По данным опросов, он встречается у четверти российских подростков. Его основные проявления — пренебрежение учебой или работой, семьей и домашними обязанностями, личной гигиеной, сном и питанием, а также сокращение социальных контактов.

Подростки с интернет-зависимостью, как правило, используют любую возможность, чтобы выйти в сеть: врут родителям, воруют деньги. Практически любой онлайн-ресурс может способствовать развитию своей специфической формы интернет-зависимости, даже Википедия.

К причинам формирования чрезмерной увлеченности Интернетом относятся проблемы в отношениях со сверстниками, отсутствие друзей, дефицит общения. Однако трудно сделать однозначный вывод, является ли социальная изоляция причиной или результатом чрезмерной увлеченности Интернетом.

3. Рекомендации для родителей по предупреждению онлайн-рисков

Находясь в Интернете, ребенок так же уязвим, как и в реальном мире: очень важно, чтобы родители знали об этом и понимали, как и от чего необходимо ребенка защитить. Онлайн-безопасность детей могут обеспечить только их родители. Дети до 10 лет должны выходить в Интернет только под присмотром (гласным или негласным) родителей. Родители обязательно должны объяснить детям правила поведения в Интернете, рассказать о пользе и вреде встречающейся там информации, обеспечить им необходимый контроль.

Чтобы свести к минимуму риски, необходимо принять следующие меры.

1. Компьютер лучше размещать в общем зале, а не в комнате ребенка.
2. Компьютер должен использоваться в том числе для обучения.
3. Следите за тем, как ваш ребенок использует компьютер.
4. Расспрашивайте ребенка о его интернет-друзьях.
5. Используйте специальные программные инструменты, которые позволяют блокировать доступ к сайтам «для взрослых».
6. Объясните ребенку, как опасно сообщать любую персональную информацию при виртуальном общении с посторонними.
7. Убедитесь, что ваш ребенок непременно рассказывает вам обо всем необычном, что он встретил в Интернете. Не забывайте останавливать его, если он позволяет себе отвечать собеседнику грубо или оскорбительно при виртуальном общении.
8. Убедитесь, что ваш ребенок знает, насколько опасно переносить в реальность общение с теми людьми, с которыми они разговаривают через Интернет.
9. Объясните ребенку, насколько опасно посылать или получать фото- и видеоматериалы по Интернету от тех людей, с которым нет личных контактов.
10. Убедитесь, что ваш ребенок не выходит в Интернет поздно ночью.

Средства обеспечения безопасности

Для обеспечения комплексной защиты наряду с организационными мерами защиты ребенка при посещении Интернета необходимо использовать доступные технические средства интернет-безопасности.

Необходимо помнить, что универсального средства, которое смогло бы удержать ребенка от поиска способов для обхода созданного ограничения, не существу-

ет. Поэтому всецело полагаться на программы родительского контроля нельзя: они не заменят беседы с родителями о правилах поведения в Интернете, о назначении компьютера. Тем не менее специальные программы и сервисы могут стать помощниками в воспитании ребенка.

Средства родительского контроля можно найти в приложениях, обеспечивающих безопасность работы в Интернете. Эти инструменты можно разделить на следующие группы:

1. Средства, ограничивающие время пользования Интернетом

1.1. «КиберМама».

Позволяет контролировать время, которое ребенок проводит за компьютером, но при этом не использует дополнительных средств для фильтрации информационного наполнения.

Можно установить ограничение на работу с компьютером, а также запретить запуск некоторых приложений. При помощи «КиберМамы» можно задать периодичность принудительного прерывания работы с Интернетом (например, каждые 45 минут) и продолжительность перерывов (компьютер будет временно заблокирован).

Для запуска приложений предусмотрены два режима работы: 1) ребенок может запускать все программы, кроме тех, которые внесены в «черный список», и 2) ребенок может запускать только те приложения, которые внесены в «белый список». Все попытки ребенка запустить ту или иную программу отражаются в отчете.

2. Средства, блокирующие доступ к опасным или нежелательным сайтам

2.1. Фильтр «Семейная безопасность» – встроенное средство контроля (download.ru.msn.com).

С помощью фильтра родители всегда могут посмотреть, что делал их ребенок: какие сайты посещал, какие программы или игры запускал. Предусмотрена блокировка переписки с любыми людьми из Интернета, кроме тех, контакты с которыми разрешены. Однако это правило затрагивает работу лишь только некоторых, не самых популярных программ — Windows Live Hotmail и Windows Live Messenger. Контроль общения в социальных сетях в этом решении отсутствует.

2.2. StaffCop Home Edition (www.staffcop.ru/home/).

Это приложение ничего не блокирует и не запрещает, но работает в фоновом режиме и незаметно для пользователя сохраняет разнообразную информацию: данные о сайтах, посещаемых пользователями, о контактах, запросах к поисковым системам и многое другое. Программа сохраняет всю переписку, которую ведут дети в системах мгновенного обмена сообщениями и социальных сетях. Дополнительно в программе реализована система периодического сохранения «снимков экрана». Также имеется «клавиатурный шпион», позволяющий родителям узнавать все пароли, вводимые детьми. Программа помогает организовать полный контроль за работой ребенка.

2.3. «Один дома».

Данная программа предназначена специально для защиты детей от просмотра нежелательного контента. В программе реализованы:

– интернет-фильтр, блокирующий загрузку любых потенциально опасных данных;

– возможность принудительного отключения целых разделов интернет-активности: социальных сетей, онлайн-игр, чатов;

– личный кабинет с веб-интерфейсом;

– диаграмма, информирующая о сайтах, на которые ребенок пытался зайти;

– бесплатные онлайн-консультации детских психологов;

– специальный детский поисковик и каталог рекомендованных интернет-ресурсов;

– большой сетевой портал для родителей и детей, где размещены новости, статьи профильных специалистов, блоги родителей и форум;

Контент-фильтр «Один дома» работает по технологии эвристической двухступенчатой фильтрации, то есть помимо имеющейся базы «белых» и «черных» сайтов используется моментальный лексический и контентный анализ интернет-страниц.

Фильтр для детей «Один дома» легко устанавливается на компьютер и имеет удобные настройки. Программа не влияет на объем передаваемого трафика и работает незаметно для пользователя, потому что для ее работы необходимы минимальные ресурсы компьютера. Пакет совместим с версиями Windows XP, Vista и 7.

2.4. «Интернет Цензор» (www.icensor.ru)

Главная задача этого пакета – сделать пребывание детей и подростков в Интернете безопасным, оградив их от посещения вредных ресурсов.

2.5. Avira Premium Security Suite (www.avira.com)

Этот пакет программных инструментов, применяемых комплексно. Он позволяет защитить компьютер от большинства современных угроз, реализует не только фильтрацию опасного контента, но и отражение хакерских атак. Если ребенок пользуется какой-либо социальной сетью, то его персональные данные не попадут вовне ни при каких обстоятельствах.

2.6. BitDefender Internet Security 2011 (www.bitdefender.ru)

Защищает ПК от вирусов, хакеров, взлома и попытки кражи персональных данных. Программа подходит для современных семей, привыкших активно пользоваться Интернетом. Среди ее возможностей: родительский контроль, удобно работающий в том числе и через iPhone, что позволяет 24 часа в сутки контролировать веб-сайты, которые посещают дети, а также их переписку; брэндмауэр, предотвращающий вторжение через сети Wi-Fi; кодирование переписки через сервисы мгновенного обмена сообщениями.

2.7. Dr.Web Security Space (www.drweb.com)

Это комплексное решение проблемы защиты ПК, позволяющее максимально надежно защитить компьютер от угроз разных типов. При этом модуль родительского контроля не только не позволяет заходить на нежелательные сайты, но и эффективно контролирует получаемые через мессенджеры сообщения.

2.8. F-Secure Internet Security 2009 (www.f-secure.com)

Комплексное решение для защиты от всех видов интернет-угроз. Программа обладает гибкой настройкой списка нежелательных для посещения сайтов, что позволит надежно перекрыть доступ к основным распространителям вредоносного контента. Содержит основные инструменты для информационной безопасности.

3. Средства, обеспечивающие комплексную безопасность

3.1. Программа «Kaspersky Internet Security 7» (www.kav.ru)

Эта программа позволяет настраивать права доступа к определенным сайтам, почте и другим интернет-сервисам. Родители могут выбрать категории сайтов, на которые ребенок не сможет зайти, запретить его общение по электронной почте и в чатах. Кроме этого, можно составить «черный» и «белый» списки ресурсов.

Существует возможность для ограничения времени пользования Интернетом (однако нет ограничения времени пользования компьютером).

Все страницы, которые посещаются ребенком при включении родительского контроля, отслеживаются в отчете.

3.2. KidsControl 1.6

Программа контролирует время, которое ребенок проводит в Интернете. Ее особенность состоит в том, что при обнаружении запрещенного сайта или попытке выйти в Интернет в неположенное время ребенок не сможет загрузить веб-страницу: в браузере выдается пустая страница с надписью «Сервер не найден».

Специально для детей в KidsControl предусмотрены следующие ограничения: веб-фильтр по категориям, «черный» и «белый» списки сайтов, ограничение работы в Интернете по времени и запрет на скачивание файлов определенных типов.

3.3. Time Boss 2.34

Дает возможность ограничивать время пользования компьютером, время, проведенное в Интернете, а также составить список запрещенных программ и папок.

3.4. «KinderGate Родительский контроль» (www.usergate.ru)

Предоставляет возможность блокировки доступа к опасным или нежелательным сайтам. Дополнительную защиту от попадания на нежелательные сайты обеспечивают включенные в программу «KinderGate Родительский контроль» функция «Безопасный поиск» и система блокировки рекламы. Первая позволяет предотвратить вывод результатов по сомнительным запросам в различных поисковых системах, а вторая запрещает вывод рекламных сообщений.

Существует возможность отслеживания переписки с различными людьми, предусмотрена возможность ограничения времени, которое ребенок сможет проводить в Интернете.

Программа ведет подробную статистику посещения пользователями разных сайтов и выполнения ими других действий. Родители могут отслеживать работу детей в глобальной сети.

Несмотря на многообразие подходов к обеспечению функции родительского контроля, предлагаемые программные средства все же не лишены недостатков и далеко не всегда справляются с возложенными на них функциями. С недавнего времени существует еще один действенный способ сделать пребывание детей в Интернете более безопасным – установка детского браузера.

4. Первый российский детский браузер — «Гогуль»

Принцип проекта «Гогуль»: «Все, что не разрешено, – запрещено». Другими словами, ссылки для поисковой системы отбираются вручную специальной командой, которая занимается разработкой этого программного инструмента. В результате мы имеем своего рода сокращенный вариант Интернета, куда вошли лишь те ресурсы, которые составители проекта посчитали безопасными для детей. Сервис «Гогуль» можно условно разделить на две части – безопасную поисковую систему и детский браузер.

После установки браузера «Гогуль» он начинает работать по принципу брандмауэра, блокируя в детском режиме доступ ко всем другим браузерам. При каждой новой попытке запустить Chrome, Opera, Firefox, Internet Explorer или любой другой браузер на экране будет появляться окно с предложением ввести родительские логин и пароль. Если данные не введены, запустить любой другой браузер, кроме детского, не получится.

База данных поисковой системы может быть расширена родителями вручную. Если необходимо разрешить доступ ребенку к какому-нибудь сайту, это можно сделать, добавив адрес разрешенного ресурса в одну из категорий каталога «Гогуль» – «Образовательные», «Искусство и культура», «Природа и животные», «Развлекательные сайты» и т. д. Родительский контроль «Гогуль» позволяет не только вести статистику просмотренных интернет-страниц и ограничивать доступ к сайтам, но и управлять тем, сколько времени ребенок проводит в Интернете.

Специализированные ресурсы

О безопасности Интернета и детей в Интернете создано несколько специализированных ресурсов.

1. http://www.saferunet.ru – центр безопасного интернета в России посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Центр является уполномоченным российским членом европейской сети Центров безопасного Интернета (Insafe), действующей в рамках Safer Internet Programme Европейской Комиссии и объединяющей национальные центры безопасного Интернета стран ЕС и России

2. http://www.ligainternet.ru – лига безопасного Интернета – крупнейшая в России координационная площадка для борьбы с опасным контентом в Сети. Лига ставит перед собой следующие задачи:

– борьба с опасным контентом в Сети, которую обязуются вести все члены лиги всеми доступными способами и средствами;

– объединение профессионального сообщества участников интернет-рынка для выработки механизмов саморегуляции сообщества во избежание регулирования сверху и создания цензуры в Интернете;

– оказание реальной помощи детям и подросткам, которые прямым или косвенным образом стали жертвами распространения опасного контента в Интернете;

– оказание содействия государственным структурам в борьбе с владельцами интернет-ресурсов, занимающимися созданием и распространением опасного контента (детская порнография, пропаганда наркомании, насилия, фашизма и экстремизма);

– участие в разработке законодательных инициатив, направленных на ликвидацию опасного контента в Интернете.

3. http://i-deti.org

4. http://www.friendlyrunet.ru – фонд «Дружественный Рунет» реализует в России комплексную стратегию в области безопасного использования интернета. Главной целью фонда является содействие развитию сети Интернет как благоприятной среды, дружественной ко всем пользователям. Фонд поддерживает проекты, связанные с безопасным использованием интернета, содействует российским пользователям, общественным организациям, коммерческим компаниям и государственным ведомствам в противодействии обороту противоправного контента, а также в противодействии иным антиобщественным действиям в Сети.

Основные проекты фонда:

– горячая линия по приему сообщений о противоправном контенте;

– специализированная линия помощи детям «Дети онлайн»;

– просветительские проекты.

Советы по безопасности детей
разных возрастных категорий в сети Интернет

5-6 лет

1. В таком возрасте желательно работать в Интернет только в присутствии родителей.

2. Обязательно объясните вашему ребенку, что общение в Интернет – это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира.

3. Добавьте детские сайты в раздел Избранное. Создайте там папку для сайтов, которые посещают ваши дети.

4. Используйте специальные детские поисковые машины, типа MSN Kids Search.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Научите вашего ребенка никогда не выдавать в Интернет информацию о себе и своей семье;

7. Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

7-8 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

2. Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

3. 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.

4. Приучите детей, что они должны посещать только те сайты, которые вы разрешили, т.е. создайте им так называемый «белый» список Интернет с помощью средств Родительского контроля. Как это сделать, мы поговорим позднее.

5. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

6. Используйте специальные детские поисковые машины, типа MSN Kids Search.

7. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

8. Создайте семейный электронный ящик чтобы не позволить детям иметь собственные адреса.

9. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.

10. Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

11. Научите детей не загружать файлы, программы или музыку без вашего согласия.

12. Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.

13. Не разрешайте детям использовать службы мгновенного обмена сообщениями;

14. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией;

15. Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни;

16. Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых»;

17. 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.

9-12 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

2. Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

3. 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.

4. Компьютер с подключением в Интернет должен находиться в общей комнате 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.

8. Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.

9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.

10. Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

11. Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.

12. 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.

13. Расскажите детям о порнографии в Интернет.

14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электрон-ной почте, чтобы вы убедились, что они не общаются с незнакомцами.

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

13-17 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 Интернет, руководство по общению в Интернет (в том числе в чатах).

2. Компьютер с подключением к Интернет должен находиться в общей комнате.

3. Не забывайте беседовать с детьми об их друзьях в 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 чатами пользуются ваши дети. Поощряйте использование модерируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из Интернет.

7. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернет.

8. Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. 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.

10. Расскажите детям о порнографии в Интернет.

11. Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

12. Приучите себя знакомиться с сайтами, которые посещают подростки.

13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закона.

Предотвращение
коммуникационных рисков

1. Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не надо писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать.

2. Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором и тем более пытаться ответить ему тем же. Лучше вообще покинуть данный ресурс и удалить оттуда личную информацию, если не получается решить проблему мирным путем. Лучший способ испортить хулигану его выходку – полностью его игнорировать.

3. Обратите внимание на психологические особенности вашего ребенка. Признаки того, что ребѐнок подвергается кибербуллингу, – различны, но есть несколько общих моментов: видимый эмоциональный стресс во время и после использования Интернета, прекращение общения с друзьями, прогулы учебных занятий, не-

стабильные оценки, резкие перемены в настроении, поведении, склонность к депрессии.

4. Если у вас есть информация, что кто-то из друзей или знакомых вашего ребенка подвергается буллингу или кибербуллингу, то сообщите об этом классному руководителю или школьному психологу – необходимо принять меры по защите ребенка.

5. Объясните детям, что личная информация, которую они выкладывают в Интернете (домашний адрес, номер мобильного или домашнего телефона, адрес электронной почты, личные фотографии) может быть использована агрессорами против них.

6. Помогите ребенку найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаления странички. Большинство социальных сетей и сервисов электронной почты имеют в настройках опцию «заблокировать пользователя» или «занести в черный список».

7. Поддерживайте доверительные отношения с ребенком, чтобы вовремя заметить, если в его адрес начнут поступать угрозы. Наблюдайте за его настроением во время и после общения с кем-либо в Интернете.

8. Убедитесь, что оскорбления (буллинг) из сети не перешли в реальную жизнь. Если поступающие угрозы являются достаточно серьезными, касаются жизни или здоровья ребенка, а также членов вашей семьи, то вы имеете право на защиту со стороны правоохранительных органов, а действия обидчиков могут подпадать под статьи Уголовного и Административного кодексов о правонарушениях.

К а к п о м о ч ь р е б е н к у ,
е с л и о н у ж е с т о л к н у л с я с И н т е р н е т - у г р о з о й

1. Установите положительный эмоциональный контакт с ребенком, постарайтесь расположить его к разговору о том, что произошло. Расскажите о своей обеспокоенности его состоянием. Ребенок должен вам доверять и понимать, что вы хотите разобраться в ситуации и помочь ему, но ни в коем случае не наказать.

2. Если ребенок расстроен увиденным (например, кто-то взломал его профиль в социальной сети) или попал в неприятную ситуацию (потратил деньги в результате интернет-мошенничества и пр.), постарайтесь его успокоить и вместе разберитесь в ситуации. Выясните, что привело к данному результату – действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в Интернете.

3. Если ситуация связана с насилием в Интернете в отношении ребенка, то необходимо узнать информацию об обидчике, историю их взаимоотношений, выяснить, существует ли договоренность о встрече в реальной жизни и случались ли подобные встречи раньше, узнать о том, что известно обидчику о ребенке (реальное имя, фамилия, адрес, телефон, номер школы и т.п.). Объясните и обсудите, какой опасности может подвергнуться ребенок при встрече с незнакомцами, особенно без свидетелей.

4. Соберите полную информацию о происшествии – как со слов ребенка, так и с помощью технических средств. Зайдите на страницы сайта, где был ребенок, посмотрите список его друзей, прочтите сообщения. При необходимости скопируйте и сохраните эту информацию – в дальнейшем это может вам пригодиться для обращения в правоохранительные органы.

5. В случае, если вы не уверены в своей оценке того, насколько серьезно произошедшее с ребенком, или ребенок недостаточно откровенен с вами и не готов идти на контакт, обратитесь к специалисту (телефон доверия, горячая линия и др.), где вам дадут рекомендации и подскажут, куда и в какой форме обратиться по данной проблеме.

Рекомендации приработев социальных сетях

1. Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях от других пользователей или друзей. Не следует бездумно открывать все ссылки подряд – сначала необходимо убедиться в том, что присланная вам ссылка ведет на безопасный или знакомый вам ресурс.

2. Контролируйте информацию о себе, которую вы размещаете. Обычно злоумышленники взламывают учетные записи на сайтах следующим образом: они нажимают на ссылку "Забыли пароль?" на странице входа в учетную запись. При этом для восстановления или установки нового пароля система может предложить ответить на секретный вопрос. Это может быть дата рождения, родной город, девичья фамилия матери и т.п. Ответы на подобные вопросы можно легко найти в сведениях, которые вы опубликовали на своей странице в какой-либо популярной социальной сети. Поэтому при установке секретных вопросов необходимо придумывать их самостоятельно (если сайт, на котором вы регистрируетесь, это позволяет) или по возможности не использовать личные сведения, которые легко найти в сети.

3. Не думайте, что сообщение, которое вы получили, было отправлено тем, кого вы знаете, только потому, что так написано. Помните, что хакеры могут взламывать учетные записи и рассылать электронные сообщения, которые будут выглядеть так, как будто они были отправлены вашими друзьями. Если у вас возникло такое подозрение, будет лучше связаться с отправителем альтернативным способом, например, по телефону, чтобы убедиться в том, что именно этот человек отправил вам данное сообщение. Точно так же необходимо относиться и к приглашениям зарегистрироваться в той или иной социальной сети.

4. Чтобы не раскрыть адреса электронной почты своих друзей, не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты. При подключении к новой социальной сети вы можете получить предложение ввести адрес электронной почты и пароль, чтобы узнать, есть ли в этой сети пользователи, с которыми вы уже поддерживаете отношения при помощи электронной переписки. Используя эти данные, сайт может рассылать электронные сообщения (например, приглашения присоединиться к этой сети от вашего лица) всем пользователям из вашего списка контактов. Социальные сети должны предупреждать об этом, но зачастую этого не делают.

5. Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки. Нажав на ссылку, которую вы получили в электронном сообщении или нашли на каком-либо сайте, вы можете попасть на поддельный сайт, где оставленные вами личные сведения будут украдены мошенниками.

6. Не добавляйте в друзья в социальных сетях всех подряд. Мошенники могут создавать фальшивые профили, чтобы получить от вас информацию, которая доступна только вашим друзьям.

7. Не регистрируйтесь во всех социальных сетях без разбора. Оцените сайт, который вы планируете использовать, и убедитесь, что вы правильно понимаете его политику конфиденциальности. Узнайте, существует ли на сайте контроль контента, который публикуется его пользователями. К сайтам, на которых вы оставляете свои персональные данные, необходимо относиться с той же серьезностью, которую требуют сайты, где вы совершаете какие-либо покупки при помощи кредитной карты.

8. Учитывайте тот факт, что все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены. На большинстве сервисов вы можете в любой момент удалить свою учетную запись, но, несмотря на это, не забывайте, что практически любой пользователь может распечатать или сохранить на своем компьютере фотографии, видео, контактные данные и другие оставленные вами сведения.

9. Проявляйте осторожность при установке приложений или дополнений для социальных сетей. Многие социальные сети позволяют загружать сторонние приложения, которые расширяют возможности личной страницы. Довольно часто такие приложения используются для кражи личных данных, поэтому к их использованию необходимо относиться так же серьѐзно, как и к установке на свой компьютер программ, которые вы можете найти в Интернете.

10. Расскажите вашим детям об опасностях, которые могут подстерегать их в социальных сетях. Если ваши дети посещают социальные сети, расскажите им о правилах безопасного пользования этими ресурсами.

Предотвращение
технических рисков

1. Установите на все домашние компьютеры антивирусные программы и специальные почтовые фильтры для предотвращения заражения компьютера и потери ваших данных. Подобные программы наблюдают за трафиком и могут остановить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

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

3. Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.

4. Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.

5. Регулярно делайте резервную копию важных данных, а также научите этому ваших детей.

6. Старайтесь периодически менять пароли (например, от электронной почты, от профилей в социальных сетях), но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т.п.).

7. Расскажите ребенку, что нельзя сообщать пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.

8. Расскажите ребенку, что если он пользуется Интернетом с помощью чужого устройства, он не должен забывать выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы. Никогда не следует сохранять на чужом компьютере свои пароли, личные файлы, историю переписки – по этой информации злоумышленники могут многое узнать о вашем ребенке.

Предотвращение
контентных рисков

1. Установите на компьютер специальные программные фильтры, которые могут блокировать всплывающие окна и сайты с определенной тематикой. Почти каждый интернет-браузер обладает настройками безопасности: какой контент должен быть заблокирован, а какой можно загружать на компьютер. Настройки браузера устанавливаются бесплатно. На сайте каждого разработчика интернет-браузеров можно найти нужную информацию в разделе «Безопасность». Специальные программы, называемые системами родительского контроля, позволяют родителям самим решать, что их дети могут просматривать в Интернете, отсекать «плохие» сайты, содержащие нежелательную информацию, в соответствии с введенными настройками. Такие программы позволяют смотреть отчеты о том, какие сайты посещал ребенок, сколько времени пользовался Интернетом, устанавливать ограничения пользования компьютером и Интернетом по времени. Родительский контроль можно также устанавливать непосредственно с помощью операционной системы, антивирусных программ, специальных программ.

2. Знайте, что у популярных поисковых систем и почтовых служб существуют специальные защитные функции, которые легко можно настроить самостоятельно. В большинстве популярных поисковых систем есть опция так называемого безопасного поиска, которая предполагает фильтрацию сайтов сомнительного содержания в поисковой выдаче. При активации этой функции поисковые машины производят фильтрацию не только по выдаче сайтов, но и по выдаче картинок на любой запрос. У почтовых сервисов можно настроить специальные фильтры, чтобы блокировались все сообщения с определенными параметрами или словами.

3. Создайте на компьютере несколько учетных записей, чтобы каждый пользователь мог входить в компьютер (систему) независимо и иметь собственный уникальный профиль. В таком случае ребенок будет входить в систему только под своим логином и паролем, не имея административных прав на контроль системных настроек, установку программ. Учетная запись администратора должна быть у родителя. Тогда только родитель сможет контролировать системные настройки и устанавливать новое программное обеспечение, ограничивая в таких правах других пользователей компьютера. Для работы в Интернете необходимо создавать надежные пароли. Пароль защищает компьютер и блокирует возможность его использования без разрешения владельца. Напомните вашему ребенку, что нельзя сообщать этот пароль друзьям, в противном случае пароль должен быть изменен.

4. Поддерживайте доверительные отношения с ребенком, чтобы всегда быть в курсе, с какой информацией он сталкивается в сети. Попав случайно на опасный, но интересный сайт, ребенок с большой вероятностью из любопытства захочет познакомиться и с другими подобными ресурсами. Важно заметить это как можно раньше и объяснить ребенку, чем именно ему грозит просмотр подобных сайтов, а также обновить настройки безопасности браузера или программного фильтра. Младшим детям нужно подробно объяснить, что это за материалы, для чего их публикуют, какие опасности они несут, в чем состоит вред такой информации. Старших детей необходимо научить критически относиться к содержанию онлайновых материалов и не доверять им без совета с вами.

5. Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете, – правда. Необходимо проверять информацию, увиденную в Интернете. Для этого существуют определенные правила проверки достоверности информа-

ции. Признаки надежного сайта, информации которого можно доверять, включают: авторство сайта, контактные данные авторов, источники информации, аккуратность в оформлении информации, актуальность данных.

6. Помните, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог – гораздо конструктивнее, чем постоянное отслеживание посещаемых сайтов и блокировка контента.

Предотвращение
потребительских рисков

1. Проинформируйте ребенка о самых распространенных методах мошенничества в сети. Всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в Интернете.

2. Не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать интернет-покупки.

3. Не отправляйте о себе слишком много информации при совершении интернет-покупок: данные счетов, пароли, домашние адреса и телефоны. Помните, что никогда администратор или модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.

4. Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.

5. Убедитесь в безопасности сайта, на котором вы или ваш ребенок планируете совершить покупку.

6. Посещая веб-сайты, самостоятельно набирайте в браузере адрес веб-сайта или пользуйтесь ссылкой из «Избранного» (Favorites); никогда не щелкайте на ссылку, содержащуюся в подозрительном электронном письме.

7. Контролируйте списание средств с ваших кредитных или лицевых счетов. Для этого можно использовать, например, услугу информирования об операциях со счетов по SMS, которые предоставляют в том числе и многие банки в России.

8. Нужно как можно быстрее обратиться к настоящим сотрудникам организации, если получилось так, что конфиденциальная информация была предоставлена вами или вашими детьми неизвестным лицам, выдающим себя за сотрудников той или иной компании либо организации. При немедленном обращении компания может уменьшить ущерб, нанесенный вашей семье и другим лицам.

Предупреждение
Интернет-зависимости

В первую очередь необходимо обратить внимание на возможные признаки Интернет-зависимости у вашего ребенка.

1. Оцените, сколько времени ваш ребенок проводит в сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.

2. Поговорите с ребенком о том, чем он занимается в Интернете.

Социальные сети создают иллюзию полной занятости – чем больше ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно

охватить – ответить на все сообщения, проследить за всеми событиями, показать себя. Выясните, поддерживается ли интерес вашего ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в сети и не заменяет ли оно реальное общение с друзьями.

3. Понаблюдайте за сменой настроения и поведения вашего ребенка после выхода из Интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться. Из числа физических симптомов можно выделить: головные боли, боли в спине, расстройства сна, снижение физической активности, потеря аппетита и другие.

4. Поговорите со школьным психологом и классным руководителем о поведении вашего ребенка, его успеваемости и отношениях с другими учениками. Настораживающими факторами являются замкнутость, скрытность, нежелание идти на контакт. Узнайте, нет ли у вашего ребенка навязчивого стремления выйти в Интернет с помощью телефона или иных мобильных устройств во время урока.

Если вы обнаружили возможные симптомы Интернет-зависимости у своего ребенка, необходимо придерживаться следующего алгоритма действий:

1. Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и т. д.

2. Не запрещайте ребенку пользоваться Интернетом, но постарайтесь установить регламент пользования (количество времени, которые ребенок может проводить онлайн, запрет на сеть до выполнения домашних уроков и пр.). Для этого можно использовать специальные программы родительского контроля, ограничивающие время в сети.

3. Ограничьте возможность доступа к Интернету только своим компьютером или компьютером, находящимся в общей комнате – это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает Ваш ребенок.

4. Попросите ребенка в течение недели подробно записывать, на что тратится время, проводимое в Интернете. Это поможет наглядно увидеть и осознать проблему, а также избавиться от некоторых навязчивых действий – например, от бездумного об-новления странички в ожидании новых сообщений.

5. Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь. Например, для многих компьютерных игр существуют аналогичные настольные игры, в которые можно играть всей семьей или с друзьями – при этом общаясь друг с другом «вживую». Важно, чтобы у ребенка были не связанные с Интернетом увлечения, которым он мог бы посвящать свое свободное время.

6. Дети с Интернет-зависимостью субъективно ощущают невозможность обходиться без сети. Постарайтесь тактично поговорить об этом с ребенком. При случае обсудите с ним ситуацию, когда в силу каких-то причин он был вынужден обходиться без Интернета. Важно, чтобы ребенок понял – ничего не произойдет, если он на некоторое время «выпадет» из жизни Интернет-сообщества.

7. В случае серьезных проблем обратитесь за помощью к специалисту.

Куда обращаться, чтобы защитить ребенка

1. Фонд поддержки детей, находящихся в трудной жизненной ситуации – общероссийский проект «телефон доверия». По телефону 8-800-2000-122 предостав-

ляются психологические консультации по проблемам насилия и принуждения к сексуальной эксплуатации, оказывается помощь жертвам подобных преступлений, а также консультации по всем психологическим проблемам детей и подростков. Все консультации, а также звонок на телефонный номер Линии помощи, бесплатны; консультации предоставляются круглосуточно.

На сайте Фонда http://www.fond-detyam.ru можно получить консультации, вступив в переписку со специалистами Фонда

2. На сайте http://www.ya-roditel.ru есть полезные материалы, адресованные родителям, обеспокоенным интернет-угрозами детям.

3. Центр безопасного Интернета в России

На сайте www.saferunet.ru необходимо кликнуть на красный баннер "горячая линия" и сообщить о противоправном контенте.

Там же: линия помощи - консультации по вопросам Интернет-угроз. Линия помощи работает в Интернет-варианте:

– по всем вопросам, связанным с безопасным использованием Интернета – посредством тематических веб-форм обращений на сайте, или через электронную почту helpline@saferunet.ru;

– по общим вопросам, в том числе по вопросам, связанным с безопасным использованием Интернета – посредством тематических веб-форм на специальном сайте www.psyhelpline.ru.

4. Линия помощи «Дети-онлайн».

Линия помощи «Дети-онлайн» – служба телефонного и онлайн-консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками интернета и мобильной связи.

Обратиться на линию помощи можно:

– телефон 8-800-250-00-15 (звонить с 9.00 до 18.00 по рабочим дням, время московское, звонки по России бесплатные);

– по электронной почте helpline@detionline.com;

– на сайте www.detionline.com.

4. Список используемых материалов

1. Распоряжение Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р (Концепция информационной безопасности детей).

2. Ковалева Т. Ф. О реализации прав детей на защиту от информации, причиняющей вред их здоровью и развитию // Научно-методический электронный жур-нал «Концепт». – 2016. – Т. 24. – С. 94–100. – URL: http://e-koncept.ru/2016/56420.htm.

3. Солдатова Г.У., Шляпников В. Н., Журина М.А. Эволюция онлайн-рисков: итоги пятилетней работы линии помощи «Дети онлайн» – Консультативная психология и психотерапия-2015. Том. 23, № 3. – URL: https://www.ya-roditel.ru/professionals/help/evolyutsiya-onlayn-riskov-itogi-pyatiletney-raboty-linii-pomoshchi-deti-onlayn/.

4. Ребенок в сети. Портал «Безопасность пользователей в сети Интернет. – URL: https://safe-surf.ru/users-of/article/99/#Контентныериски.

5. Методические рекомендации по контролю за использованием несовершеннолетними сети Интернет во внеучебное время. Методические рекомендации / Сост. О.В. Пикулик, С.В. Синаторов. – Саратов: ГАОУ ДПО «СарИПКиПРО». – 2012. – 39 с.

6. Рекомендации «Безопасность детей в Интернете». / Автор-сост.: Н.И. Баскакова, / Под общей ред. Н.К. Солоповой, к.п.н., доцента, проректора по учебно-методической работе и информатизации ТОИПКРО. – Тамбов: ТОИПКРО, 2011
7. Методические рекомендации для родителей (законных представителей) о возможностях организации родительского контроля за доступом детей в сеть Интернет: Методические рекомендации / Сост.: Шарипова Г.И., Тагиров И.Х. – Уфа: Издательство ИРО РБ, 2018.