Информационная безопасность

Нормативное регулирование:

- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Педагогам:

Решение задачи по обеспечению безопасности при использовании компьютера и интернета детьми требует комплексного подхода, решения множества психолого-педагогических вопросов. Школа должна играть одну из ключевых ролей в обучении детей безопасному использованию интернет-технологий. Помимо выполнения очевидных мер безопасности (установка антивирусных программ, брандмауэров, фильтров, ограничений по времени) необходима разработка и реализация правил электронной безопасности, которые требуют привлечения широкого спектра заинтересованных лиц: директора школы, классных руководителей, преподавателей информационных технологий, самих учащихся и их родителей, поставщиков услуг интернета. Среди них могут быть следующие:

Разработать четкие правила и процедуры использования интернета в школе, включая правили против агрессии по интернету и через мобильные телефоны, и регулярно оценивать и пересматривать их эффективность.
Обеспечить осведомленность о правилах допустимого пользования ИКТ и их применении. Очень важно, чтобы эти правила соответствовали возрасту.
Ввести действенные санкции к нарушителям правил пользования интернетом.
Назначить координатора действий по электронной безопасности.
Использовать лицензированного поставщика услуг интернета.
Использовать программные продукты фильтрации/мониторинга.
Обеспечить обучение всех детей навыкам электронной безопасности.
Обеспечить обучение и повышение квалификации коллектива в области электронной безопасности.
Организовать в школе пункт приема обращений, чтобы иметь возможность собирать и регистрировать происшествия в области нарушений электронной безопасности.
Проводить регулярную проверку принимаемых мер в области электронной безопасности.

Общие рекомендации по обеспечению безопасной работы детей в интернете для родителей и педагогов:

Установите компьютер в местах, где к нему будет общий доступ (в общей комнате, компьютерном классе), чтобы ребенок не мог долго оставаться наедине с компьютером
Будьте осведомлены об интернет-сайтах, которые используют дети и о том, как они проводят время онлайн
Установите брандмауэр и антивирусное программное обеспечение, объясните

детям как программы фильтрации и блокировки или мониторинга могут им помочь безопасно использовать интернет. Объясните им принципы работы этих программ, а также причины, из-за которых вы их используете. Храните в секрете любые пароли, связанные с этими программами.
Получайте новые знания о том, как безопасно использовать интернет (через интернет-сайты, от интернет-провайдеров, из публикаций по данной теме в прессе и в специальной литературе, на обучающих семинарах)
Установите правила использования компьютера и интернета (дома, в школе)
Однако недостаточно просто иметь эти правила, взрослые должны активно использовать методы, которые помогают детям определить, каким должно быть безопасное поведение, и самим вести себя соответствующим образом.

Информационная безопасность в Интернете может обсуждаться во время уроков информатики, социологии, ОБЖ, гражданского права и др. На уроках информатики для младших школьников стоит обратиться к онлайновой игре «Wild Web Wood», содержащей основные понятия об устройстве Интернета, правилах работы в нем, в том числе — о сетевом этикете. Дети с помощью выбранных героев игры и мудрого Паучка найдут в ней много полезных советов о безопасном использовании Интернета, которые интересно также будет узнать родителям и педагогам. Игра создана на основе справочника Совета Европы «Интернет-грамотность», переведена на русский язык и будет интересна детям младшего и среднего школьного возраста. Ее можно найти по адресу: http://www.wildwebwoods.org

На сайте Роскомнадзора представлены презентации и видеоуроки, в которых рассказывается, что такое персональные данные, какие существуют виды киберугроз, как обратиться в Роскомнадзор за защитой своих прав. Материалы доступны по ссылке.»

Ученикам:

Вредоносные программы — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с интернетом и даже использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Как не подцепить вирус:

Не открывай материал, присланный незнакомцами.
Не открывай сомнительный файл с вложениями, даже если ты получил его от своего знакомого. Свяжись с другом, от которого ты получил сообщение, и уточни у него, действительно ли он является автором послания
Не запускай и не скачивай файлы (например, музыку, фильмы, игры) из сомнительных источников.
Старайся не нажимать на рекламные баннеры, даже если они кажутся тебе очень заманчивыми.

Старайся не посещать сомнительные сайты или ресурсы.
Для защиты от спама:
Не выдавай в Интернет своего реального электронного адреса, есть риск использования твоего почтового ящика в качестве рассылки спама.
Старайся чаще менять пароли к электронной почте, к страничке в социальной сети и др.
Заведи себе два адреса — частный, для переписки (приватный и малоизвестный, который ты никогда не публикуешь в общедоступных источниках), и публичный — для публичной деятельности (форумов, чатов и так далее).
Если ты не пользуешься компьютером, старайся отключать его от соединения с Интернетом.

Борьба с вирусами:

Не сохраняй на своем компьютере неизвестные файлы. Подозрительные сообщения лучше немедленно удалять:
удали сообщение из папки Входящие;
удали сообщение из папки Удаленные (Корзина);
выполни над папками операцию "Сжать" (Файл/Папка/Сжать все папки).
Если твой компьютер заражен:

Отключи компьютер от интернета и локальной сети.
Не пытайся самостоятельно решить проблему, не жми на все кнопки подряд, посоветуйся со взрослым.
Или если необходимо, обратись за помощью в службу технической поддержки производителя установленного на твоем компьютере антивирусного ПО.
Если ты уверенный пользователь компьютера:

Загрузи компьютер в безопасном режиме (включи компьютер, нажми и, удерживая клавишу F8, выбери Безопасный режим (Safe Mode) в открывшемся меню).
Проведи полную антивирусную проверку компьютера.
Если в результате проверки обнаружен вирус, червь или троянская программа, следуйте указаниям производителя антивирусного ПО. Хорошие антивирусы предлагают лечение зараженных объектов, помещение подозрительных объектов в карантин и удаление троянских программ и червей.

Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: хакер незаконно получает доступ к личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб. Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.

Предупреждение кибермошенничества:

Ни под каким предлогом не выдавай незнакомым людям свои личные данные (домашний адрес, номер телефона и т.д.) и пароли.
Перед тем, как воспользоваться развлекательными услугами Интернета (скачать

музыку, фильм и т.д.), проверь, что после этого тебя не попросят заплатить деньги.
Не верь всему, что видишь в Интернет.
Старайся остерегаться новых предложений и услуг, все они требуют вложения крупной суммы денег (например, местонахождение человека по номеру его мобильного, повышение рейтинга в социальной сети и т.д.)
Советуйся со взрослыми перед тем, как загрузить, скачать или установить ту или иную услугу.
Очень внимательно выбирай сайты, на которых ты хочешь сделать покупки и удостоверься в их надежности. Собери как можно больше информации о сайте, спросив, например, название, адрес и номер телефона центрального офиса, описания общих положений контракта и, особенно о том, как отменить заказ; кроме того выясни о защите и управлении личными данными и безопасности оплаты; и сравни цены, отыскав такой же предмет на других сайтах.
Если ты получил неожиданное электронное письмо, в котором тебе предлагается невероятно выгодная сделка, вероятность того, что это мошенничество, очень велика.

Борьба с кибермошенничеством:

Если компьютер подцепил вирус, не отправляй смс сообщение, даже если тебе обещают таким образом очистить компьютер от вредоносных программ или разблокировать компьютер.
В случае взлома страницы в социальной сети — смени пароли.
Обратись за советом к взрослому.

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Предупреждение кибербуллинга:

Не сообщай свои данные агрессору (реальное имя, фамилию, адрес, телефон, номер школы и т.п.). Когда злоумышленнику становятся известны твои анкетные данные, происходит так называемый «троллинг» или травля.
Не открывай доступ к своей страничке незнакомым людям.
Следи за информацией, которую ты выкладываешь в Интернете
Придерживайся правил сетевой этики, не отвечай грубо на сообщения, этим ты можешь спровоцировать собеседника. Игнорируй сообщения от незнакомых, агрессивных и подозрительных личностей. Нужно понимать, что онлайн-общение не является приватным. Другие пользователи могут скопировать, распечатать или переслать твою личную переписку.
Если ты видишь или знаешь, что твоего друга запугивают, поддержи его и сообщи об этом.
Не посылай сообщения или изображения, которые могут огорчить кого-нибудь.

Борьба с кибербуллингом:

Не предпринимай самостоятельных действий по наказанию агрессора
Немедленно обратись за советом к родителям или в специальные организации за

помощью
Сделай снимок экрана с оскорблениями (screen-shot) и перешлите его модераторам ресурса.
Или напиши письмо в техподдержку с просьбой удалить аккаунт хулигана. Важно помнить, что адекватно отреагировав на неприятное сообщение, оповестив администрацию ресурса о киберхулигане, можно обезопасить от него, не только себя, но и остальных пользователей.
Если же преследование происходит лично, с помощью электронной почты, сервисов мгновенных сообщений (ICQ, Google talk и т.д.) или IP телефонии (Skype) избавиться от неприятного собеседника можно нажав клавишу «игнорировать» (или «черный список»). У большинства программ, предназначенных для общения, существует такая или аналогичная функция.

Груминг — установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече.

Предупреждение груминга:

Следи за информацией, которую ты выкладываешь в Интернете. Не выкладывай свои личные данные в Интернете (домашний адрес, номер телефона, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.). Помни, любая информация может быть использована против тебя, в том числе в корыстных и преступных целях
Используй псевдоним при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), пользовании он-лайн играми и других ситуациях
Не размещай и не посылай свои фотографии незнакомцам
Будь осторожен при общении с незнакомыми людьми. Старайся рассказывать, как можно меньше информации о себе.

Борьба с грумингом:

Если новый знакомый пытается говорить с тобой на неприятные или пугающие тебя темы и говорит об этом как о секрете, который останется только между вами – немедленно сообщи об этом родителям или старшим
Сделай снимок с экрана (screen-shot)
Никогда не соглашайся на личные встречи с незнакомцами. Твои собеседники могут оказаться совсем не теми, за кого себя выдают. Или приходи на встречу только со взрослым.

На сайте Роскомнадзора представлены презентации и видеоуроки, в которых рассказывается, что такое персональные данные, какие существуют виды киберугроз, как обратиться в Роскомнадзор за защитой своих прав. Материалы доступны по ссылке.»

Родителям:

Дети и подростки — активные пользователи интернета. С каждым годом сообщество российских интернет-пользователей молодеет. Дети поколения Рунета растут в мире, сильно отличающемся от того, в котором росли их родители. Одной из важнейших координат их развития становятся инфо-коммуникационные технологии и, в первую очередь, интернет. Между тем, помимо огромного количества возможностей, интернет несет и множество рисков. 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 их родителей. Мы предлагаем Вам полезную информацию и серию рекомендаций. С их помощью Вы сможете помочь своему ребенку использовать интернет более грамотно и безопасно.

В основе рекомендаций лежит разработанная Фондом Развития Интернет классификация интернет-рисков, результаты исследования «Дети России онлайн», которое было проведено Фондом Развития Интернет по методологии международного исследовательского проекта Еврокомиссии «EU Kids Online II» (2010—2011 годы), а также обращения пользователей, поступившие на Линию помощи «Дети Онлайн».

Основные правила безопасности для родителей:

Прежде, чем позволить ребенку пользоваться Интернетом, расскажите ему о возможных опасностях Сети (вредоносные программы, небезопасные сайты, интернет-мошенники и др.) и их последствиях.
Четко определите время, которое Ваш ребенок может проводить в Интернете, и сайты, которые он может посещать.
Убедитесь, что на компьютерах установлены и правильно настроены антивирусные программы, средства фильтрации контента и нежелательных сообщений.
Контролируйте деятельность ребенка в Интернете с помощью специального программного обеспечения.
Спрашивайте ребенка о том, что он видел и делал в Интернтете
Объясните ребенку, что при общении в Интернете (чаты, форумы, сервисы мгновенного обмена сообщениями, онлайн-игры) и других ситуациях, требующих регистрации, нельзя использовать реальное имя. Помогите ему выбрать регистрационное имя, не содержащее никакой личной информации.
Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т.д.), а также "показывать" свои фотографии.
Помогите ребенку понять, что далеко не все, что он может прочесть или увидеть в Интернете — правда. Приучите его спрашивать то, в чем он не уверен.
Объясните ребенку, что нельзя открывать файлы, полученные от неизвестных пользователей, так как они могут содержать вирусы или фото/видео с негативным содержанием.
Приучите ребенка советоваться со взрослыми и немедленно сообщать о

появлении нежелательной информации.
Не позволяйте Вашему ребенку встречаться с онлайн-знакомыми без Вашего разрешения или в отсутствии взрослого человека.
Постараться регулярно проверять список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются;
Объясните детям, что при общении в Интернете, они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов — читать грубости также неприятно, как и слышать;
Проверяйте актуальность уже установленных правил. Следите за тем, чтобы Ваши правила соответствовали возрасту и развитию Вашего ребенка.

Что делать, если ребенок уже столкнулся с какой-либо интернет-угрозой?

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

Если ребенок расстроен чем-то увиденным (например, кто-то взломал его профиль в социальной сети) или он 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 – непосредственно действия самого ребенка, недостаточность вашего контроля или незнание ребенком правил безопасного поведения в интернете.
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.
Соберите наиболее 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.
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.

Профилактика основных интернет-рисков и борьба с ними:

Вредоносные программы — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с интернетом, а также могут использовать ваш компьютер для распространения

своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из интернета файлов.

Предупреждение столкновения с вредоносными программами:

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.
Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.
Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.
Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.
Регулярно делайте резервную копию важных данных, а также научите это делать ваших детей.
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). Расскажите ребенку, что нельзя рассказывать никакие пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.
Расскажите ребенку, что если он пользуется интернетом с помощью чужого устройства, он должен не 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.

Как избавиться от вредоносных программ:

Загрузите компьютер в безопасном режиме (включите компьютер, нажмите и, удерживая клавишу F8, выберите Безопасный режим (Safe Mode) в открывшемся меню).
Проведите полную антивирусную проверку компьютера.
Если в результате проверки обнаружен вирус, червь или троянская программа, следуйте указаниям производителя антивирусного ПО. Хорошие антивирусы предлагают лечение зараженных объектов, помещение подозрительных объектов в карантин и удаление троянских программ и червей.
При невозможности самостоятельно решить проблему обратитесь за помощью в службу технической поддержки производителя установленного на вашем компьютере антивирусного ПО или в технический сервис.

Кибермошенничество — один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.). Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.

Предупреждение кибермошенничества:

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.
Не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки.
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.
Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.
Убедитесь в безопасности сайта, на котором Вы или Ваш ребенок планируете совершить покупку:
Ознакомьтесь с отзывами покупателей.
Избегайте предоплаты.
Проверьте реквизиты и название юридического лица – владельца магазина.
Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис Whois).
Поинтересуйтесь возможностью получения кассового чека и других документов за покупку.
Сравните цены в различных интернет-магазинах.
Позвоните в справочную магазина.
Обратите внимание на правила интернет-магазина.
Выясните, сколько точно вам придется заплатить.
Как справляться с кибермошенничеством

Проговорите с ребенком всю ситуацию. Он должен рассказать, какой сайт он посещал, на какие баннеры нажимал, какими услугами сети пользовался, что видел и т.д. Сохраните все электронные свидетельства совершенных действий и операций, скриншоты экранов – они могут служить доказательствами в дальнейшем.
Фишинг и вишинг: В случае хищения данных, поставьте в известность свой банк или финансовую организацию, если необходимо, то закройте или временно заблокируйте ваши счета. Запросите отчет о финансовых операциях и проверьте их корректность, о выявленных расхождениях поставьте в известность вашу финансовую организацию.

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. Английское слово буллинг (bullying, от bully — драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Исследования буллинга начались еще в 70-х годов. прошлого века. Это поведение всегда присутствует в подростковой среде. В современном информационном обществе для буллинга все чаще используются инфокоммуникационные технологии. Буллинг, осуществляемый в виртуальной среде с помощью интернета и мобильного телефона, называют кибербуллингом. Многие исследования показывают, что кибербуллинг часто сопровождает традиционный буллинг.

Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент.

Предотвращение кибербуллинга:

Объясните детям, что при общении в интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не стоит писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать. Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором, и тем более пытаться ответить ему тем же. Возможно стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем. Лучший способ испортить хулигану его выходку – отвечать ему полным игнорированием.

Обратите внимание на психологические особенности вашего ребенка. Специалисты выделяют характерные черты, типичные для жертв буллинга, они часто бывают: пугливы, чувствительны, замкнуты и застенчивы; тревожны, неуверены в себе, несчастны; склонны к депрессии и чаще своих ровесников думают о самоубийстве; не имеют ни одного близкого друга и успешнее общаются с взрослыми, нежели со сверстниками; мальчики могут быть физически слабее своих ровесников.

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.

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. Помогите ребенку найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички. Поддерживайте доверительные отношения с вашим ребенком, чтобы вовремя заметить, если в его адрес начнет поступать агрессия или угрозы. Наблюдайте за его настроением во время и после общения с кем-либо в интернете. 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 попадать под статьи действия уголовного и административного кодексов о правонарушениях.

Как справляться с кибербуллингом:

Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию.
Сохраните все возможные свидетельства происходящего (скриншоты экрана, электронные письма, фотографии и т.п.).
Сохраняйте спокойствие — вы можете еще больше напугать ребенка своей бурной реакцией на то, что он вам рассказал и показал. Главной задачей является эмоциональная поддержка ребенка. Нужно дать ему уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.
Повторите ребенку простейшие правила безопасности при пользовании интернетом, дайте советы по дальнейшему предотвращению кибер-буллинга.

Встречи с незнакомцами и груминг

Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Также юный пользователь рискует подвергнуться оскорблениям, запугиванию и домогательствам. Особенно опасным может стать груминг – установление дружеских отношений с ребенком с целью личной встречи, вступления с ним в сексуальные отношения, шантажа и эксплуатации. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети. Общаясь лично («в привате»), злоумышленник, чаще всего представляясь сверстником, входит в доверие к ребенку, а затем пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече. Иногда такие люди выманивают у детей информацию, которой потом могут шантажировать ребенка, например, просят прислать личные фотографии или провоцируют на непристойные действия перед веб-камерой.

Предупреждение встреч с незнакомцами и груминга:

Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе, с кем ребенок общается в сети. Обратите внимание, кого ребенок добавляет к себе «в друзья», с кем предпочитает общаться в сети — с ровесниками или людьми старше себя.
Объясните ребенку, что нельзя разглашать в интернете информацию личного характера (номер телефона, домашний адрес, название/номер школы и т. д.), а также пересылать виртуальным знакомым свои фотографии или видео.
Объясните ребенку, что нельзя ставить на аватарку или размещать в сети фотографии, по которым можно судить о материальном благополучии семьи, а также нехорошо ставить на аватарку фотографии других людей без их разрешения.
Объясните ребенку, что при общении на ресурсах, требующих регистрации (в

чатах, на форумах, через сервисы мгновенного обмена сообщениями, в онлайн-играх), лучше не использовать реальное имя. Помогите ему выбрать ник, не содержащий никакой личной информации.
Объясните ребенку опасность встречи с незнакомыми людьми из интернета. В сети человек может представиться кем угодно, поэтому на реальную встречу с интернет-другом надо обязательно ходить в сопровождении взрослых.
Детский познавательный интерес к теме сексуальных отношений между мужчиной и женщиной может активно эксплуатироваться злоумышленниками в интернете. Постарайтесь сами поговорить с ребенком на эту тему. Объясните ему, что нормальные отношения между людьми связаны с доверием, ответственностью и заботой, но в интернете тема любви часто представляется в неправильной, вульгарной форме. Важно, чтобы ребенок был вовлечен в любимое дело, увлекался занятиями, соответствующими его возрасту, которым он может посвящать свободное время.

Как противостоять грумингу:

Если ребенок желает познакомиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу
Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию
Сохраняйте спокойствие — вы можете еще больше напугать ребенка своей бурной реакцией на то, что он рассказал или показал. Главной задачей является эмоциональная поддержка ребенка. Нужно дать ребенку уверенность в том, что проблему можно преодолеть. Никогда не наказывайте и не ограничивайте действия ребенка в ответ на его признание.
Сохраните все свидетельства переписки и контактов незнакомца с ребенком (скриншоты экрана, электронные письма, фотографии и т.п.).
При обнаружении признаков совращения следует немедленно сообщить об этом в правоохранительные органы.
Повторите ребенку простейшие правила безопасности при пользовании интернетом, дайте советы по дальнейшему предотвращению груминга.

Контентные риски:

К контентным рискам относятся материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию. В первую очередь, с таким контентом можно столкнуться на сайтах социальных сетей, в блогах, на торрентах. Но сегодня практически весь интернет - это виртуальное пространство риска.

Противозаконный контент - распространение наркотических веществ через интернет, порнографические материалы с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям.

Вредоносный (опасный) контент - контент, способный нанести прямой вред психическому и физическому здоровью детей и подростков. Неэтичный контент - контент, который не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей. Подобное содержимое может распространяться ограниченно (например, "только для взрослых").

Особо опасны сайты, на которых обсуждаются способы причинения боли и вреда, способы чрезмерного похудения, способы самоубийства, сайты, посвященные наркотикам, сайты, на которых размещены полные ненависти сообщения, направленные против отдельных групп или лиц. Столкновения с контентными рисками могут иметь негативные последствия для эмоциональной сферы, психологического развития, социализации, а также физического здоровья детей и подростков.

Рекомендации по предупреждению контентных рисков:

Используйте специальные технические средства, чтобы ограничивать доступ ребенка к негативной информации – программы родительского контроля и контентной фильтрации, настройки безопасного поиска. Часто пакет функций родительского контроля уже есть в вашей антивирусной программе. Программы родительского контроля позволяют: установить запрет на посещения сайтов различного негативного содержания, сайтов онлайн-знакомств, сайтов с вредоносным содержимым; ограничить время доступа ребенка к интернету; производить мониторинг переписки в социальных сетях и онлайн мессенджерах (чатах); блокировать сомнительные поисковые запросы в поисковых системах; блокировать баннеры; а также отслеживать все действия ребенка в сети.
Если ребенок пользуется общим компьютером, для каждого члена семьи создайте свою учетную запись на компьютере. Ваша учетная запись должна иметь надежный пароль и обладать правами администратора, чтобы ребенок не мог менять установленные вами настройки и программы.
Регулярно следите за активностью вашего ребенка в сети. Просматривайте историю посещений сайтов, чтобы быть уверенным, что среди них нет опасных. При необходимости обновляйте настройки технических средств безопасности.
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 информации. Признаки надежного сайта, информации которого можно доверять, включают: авторство сайта, контактные данные авторов, источники информации, аккуратность представления информации, цель создания сайта, актуальность данных. Расскажите об этих правилах вашим детям.
Поддерживайте доверительные отношения с вашим ребенком, чтобы всегда быть в курсе с какой информацией он сталкивается в сети. Попав случайно на какой-либо опасный, но интересный сайт, ребенок может продолжить поиск подобных ресурсов. Важно заметить это как можно раньше и объяснить, ребенку, чем именно ему грозит просмотр подобных сайтов.
Важно помнить, что невозможно всегда находиться рядом с детьми и постоянно их контролировать. Доверительные отношения с детьми, открытый и доброжелательный диалог зачастую могут выступать более эффективными средствами для обеспечения безопасности вашего ребенка, чем постоянное отслеживание посещаемых сайтов и блокировка всевозможного контента.

Интернет-зависимость — навязчивое желание войти в интернет, находясь офлайн и неспособность выйти из интернета, будучи онлайн. (Гриффит В., 1996). По своим проявлениям она схожа с уже известными формами аддиктивного поведения (например, в результате употребления алкоголя или наркотиков), но относится к типу нехимических зависимостей, то есть не приводящих

непосредственно к разрушению организма. По своим симптомам интернет-зависимость ближе к зависимости от азартных игр; для этого состояния характерны следующие признаки: потеря ощущения времени, невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в интернет. Исследователи отмечают, что большая часть Интернет-зависимых (91 %) пользуется сервисами Интернета, связанными с общением. Другую часть зависимых (9%) привлекают информационные сервисы сети.

Предупреждение интернет-зависимости:

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.
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.
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.
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.

Как справляться с интернет-зависимостью:

Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и т.д.
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.
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.
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 обновления странички в ожидании новых сообщений.

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. 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. В случае серьезных проблем обратитесь за помощью к специалисту. Информацию, куда обращаться вы можете найти в разделе Полезная информация.

На сайте Роскомнадзора представлены презентации и видеоуроки, в которых рассказывается, что такое персональные данные, какие существуют виды киберугроз, как обратиться в Роскомнадзор за защитой своих прав. Материалы доступны по ссылке.»