Рекомендации для родителей по предупреждению контентных рисков.
Как избежать материалов с нежелательной информацией?

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.

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 информации. 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.

Как помочь ребенку, если он уже столкнулся с Интернет-угрозой

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

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 по предупреждению встречи с незнакомцами в сети

1. 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.

2. 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.

3. Объясните ребенку, что нельзя ставить на аватарку или размещать в сети фотографии, по которым можно судить о материальном благополучии семьи, а также фотографии других людей без их разрешения.

4. 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.

5. 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.