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

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 это делать 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 рассказывать никакие 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 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

1. Загрузите компьютер в безопасном режиме (включите компьютер, нажмите и, удерживая клавишу F8, выберите Безопасный режим (Safe Mode) в открывшемся меню).
2. Проведите полную антивирусную проверку компьютера.
3. 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.
4. При невозможности самостоятельно решить проблему обратитесь за помощью в службу технической поддержки производителя установленного на вашем компьютере антивирусного ПО или в технический сервис.

Повысьте уровень безопасности вашего компьютера.

Если на вашем компьютере установлена операционная система Microsoft® Windows® XP Service Pack 2, то можно использовать Windows Security Center. Эта программа позволяет просматривать информацию о состоянии защиты компьютера и изменять настройки, а также получать дополнительные сведения по вопросам безопасности.

Security Center показывает состояние трех важных компонентов безопасности: брандмауэра

Интернета, антивирусных программ и службы автоматического обновления. Кроме того, он служит для перехода к другим разделам безопасности, а также поиска технической поддержки и ресурсов, имеющих отношение к защите компьютера.

Security Center работает в фоновом режиме, постоянно проверяя состояние трех наиболее важных компонентов.

Для того чтобы повысить уровень общей безопасности в Windows XP, нужно проделать следующее:

• нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel;

• в панели управления откройте Центр обеспечения безопасности/Security Center;

• убедитесь, что включены основные компоненты безопасности (брандмауэр, автоматическое обновление, защита от вирусов).

Включить или отключить брандмауэр и автоматическое обновление вы можете непосредственно в Центре обеспечения безопасности.

Для управления защитой от вирусов обратитесь к настройкам установленного антивирусного программного обеспечения.

Установите на вашем компьютере антишпионские настройки или дополнительное антишпионское программное обеспечение

Шпионскими называются программы, выполняющие определенные действия (например, сбор личной информации или изменение настроек) без согласия и контроля пользователя. Они могут существенно замедлить работу системы и привести к нежелательным изменениям в важных настройках.

Такие программы трудно удалить. Антишпионское программное обеспечение поможет избавиться от шпионских и других нежелательных программ. Проверка компьютера может выполняться по расписанию в удобное для вас время.

Для того чтобы предотвратить появление шпионского программного обеспечения на вашем компьютере, необходимо убедиться в том, что включены основные средства Центра обеспечения безопасности вашей операционной системы.

Рекомендуется также для повседневной работы использовать учетную запись с ограниченными правами.

Для удаления шпионского программного обеспечения, попавшего на ваш компьютер, следует воспользоваться специальным антишпионским программным обеспечением, в частности, следующими программами: Windows Defender; Malicious Software Removal Tool.

Эти бесплатные программы вы можете загрузить с сайта http://www.microsoft.com/downloads

Для этого в строке Search в выпадающем списке выберите All Downloads, в строке справа введите название одного из указанных выше продуктов и нажмите кнопку Go.

Блокируйте доступ к неподходящим материалам

Один из наилучших способов защиты от нежелательной информации - это блокирование доступа еще до того, как она может быть получена.

Microsoft предлагает несколько таких способов.

Для того чтобы блокировать доступ к нежелательной информации в Internet Explorer® и MSN Explorer, нужно выполнить следующее:

• нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/ Control Panel;

• в панели управления откройте Свойства обозревателя/internet Options;

• в появившемся окне перейдите на вкладку Содержание/Content;

• в разделе Ограничение доступа/Content Advisor нажмите кнопку Включить/Enable;

• в появившемся окне введите пароль, который будет защищать вводимые вами ограничения от изменения детьми;

• в окне Ограничение доступа/Content Advisor вы можете блокировать доступ к нежелательной информации.

Повысьте уровень безопасности ребенка с электронной почтой OUTLOOK® EXPRESS.

Для повышения уровня безопасности при работе ребенка с электронной почтой в меню программы Outlook® Express в разделе Сервис/Tools выберите команду Параметры/Options.

Перейдите на вкладку Безопасность/Security.

При помощи переключателя выберите зону безопасности для Internet Explorer/Select the Internet Explorer security zone to use вы можете уменьшить вероятность появления вирусов на вашем компьютере. Для этих же целей служит переключатель. Не разрешать сохранение или открытие вложений, которые могут содержать вирусы/Do not allow attachments to be saved or opened that could potentially be a virus). Если же вирус все же попал на ваш компьютер, ограничить его дальнейшее распространение вы можете, установив галочку. Предупреждать, если приложения пытаются отправить почту от моего имени/Wam me when other applications try to send mail as me.

Для защиты пересылаемых писем от подделки и от возможности перехвата и прочтения кем-либо, кроме указанного получателя, есть возможность Шифровать содержимое и вложения всех исходящих сообщений/Encrypt content and attachments for all outgoing messages и Подписывать все отправляемы* сообщения/Digitally sign all outgoing messages.

Заблокируйте поступление спама

Чтобы блокировать поступление спама (нежелательной почты), необходимо воспользоваться почтовым сервером, имеющим защиту от спама (например, hotmail.com), или почтовым клиентом, имеющим спам-фильтр (например, Microsoft Outlook).

Чтобы настроить спам-фильтр для почтового ящика, размещенного на сервере hotmail.com, необходимо зайти в этот почтовый ящик и перейти по ссылке Options и в вертикальном меню выбрать вкладку Mail. Перейдя по ссылке Junk E-mail Filter, вы можете изменить настройки фильтра нежелательной почты.

При помощи ссылки Block Senders, находящейся на вкладке Mail, вы можете добавить любого отправителя в список заблокированных, при этом почта от этого отправителя не будет поступать в ваш почтовый ящик.

В случае, если ваш почтовый сервер не имеет фильтра нежелательной почты, можно воспользоваться фильтром, встроенным в Microsoft Outlook.

Для настройки этого фильтра в меню Microsoft Outlook выберите Сервис/Tools, в открывшемся меню выберите команду Параметры/Options. В открывшемся диалоговом окне перейдите на вкладку Настройки/Preferences и нажмите кнопку Нежелательная почта/Junk E-mail.

В появившемся диалоговом окне вы можете внести изменения в настройки фильтра нежелательной почты. Кроме того, вы можете воспользоваться спам-фильтрами других разработчиков.

Создайте отдельные учетные записи для разных пользователей

Windows XP позволяет создать несколько учетных записей. Каждый пользователь сможет входить в систему независимо и иметь уникальный профиль с собственным рабочим столом и папкой «Мои документы». Родитель может создать себе учетную запись администратора, дающую полный контроль над компьютером, а детям - ограниченные учетные записи. Пользователи с ограниченными учетными записями не смогут изменить системные настройки или установить новое аппаратное или программное обеспечение, включая большинство игр, медиаплееров и программ поддержки чатов.

Для того чтобы создать отдельную учетную запись для ребенка с ограниченными правами доступа для работы в Интернете, необходимо выполнить следующие действия:

- нажмите кнопку Пуск/ Start, в открывшемся меню выберите Панель управления/Control Panel;
- в панели управления откройте Учетные записи пользователей/User Accounts;
- в открывшемся окне выберите Создание учетной записи/Create a new account, введите ее имя;
- на этапе выбора типа учетной записи установите переключатель в положение Ограниченная запись/Limited;
- после нажатия кнопки Создать учетную запись/Create Account процесс создания учетной записи с ограниченными правами будет завершени ваш ребенок сможет выбрать ее при

следующем входе в систему.

Повысьте уровень конфиденциальности при общении вашего ребенка в интернете с помощью INTERNET EXPLORER.

Сохранение конфиденциальности личной информации вашего ребенка при его работе в Интернете является важным механизмом безопасности.

Для того чтобы повысить уровень конфиденциальности при общении вашего ребенка в Интернете, выполните следующие действия:

• нажмите кнопку Пуск/Start, в открывшемся меню выберите Панель управления/Control Panel;

• в панели управления откройте Свойства обозревателя/internet Options;

• в появившемся окне перейдите на вкладку Конфиденциальность/Рпуасу;

• при помощи ползунка выберите необходимый уровень конфиденциальности.

Создавайте надежные пароли

Пароли - это ключи, которыми можно разблокировать компьютер и учетные записи в Интернете. Чем надежнее пароль, тем лучше защита от вторжения хакеров и мошенников, которые могут воспользоваться вашими личными данными в корыстных целях, например, открыть новые счета кредитных карт, обратиться за ипотекой или даже общаться через Интернет от вашего имени. Вы можете не подозревать о таких действиях до тех пор, пока не станет слишком поздно. Создавать надежные пароли несложно. Для укрепления безопасности компьютера достаточно приложить незначительные усилия, с которыми можно познакомиться на сайте Microsoft по адресу http://www.microsoft.com/rus/athome/securitv/privacv/password.ms Обычно подготовка к школе заключалась в укладывании в портфель карандашей, тетрадей и учебников. Сегодня в начале этого списка нередко находится компьютер. Ознакомьтесь с этими советами, чтобы защитить компьютеры, которыми вы пользуетесь в школе, от вирусов, хакеров, программ-шпионов и других возможных атак.

В настоящее время все большее распространение получают беспроводные сети. Это дает возможность путешествовать по Интернету, находясь в библиотеке, кафе или учебной аудитории. Возможно, вы уже пользовались беспроводными сетями дома, в аэропорту, кафетериях. Такие сети очень удобны, но их использование сопряжено со снижением уровня безопасности. Если вы устанавливаете беспроводную сеть дома или собираетесь активно использовать беспроводными сетями общего назначения, прочитайте соответствующие разделы брошюры и обратите особое внимание на информацию по безопасности. Принимайте необходимые меры предосторожности, пользуясь беспроводной связью!

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

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 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:

- 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

1. 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.

2. 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

1. 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.

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. 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.

3. 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.

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 удаление странички.

7. 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.

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 попадать под статьи действия уголовного и административного кодексов о правонарушениях.

Как справляться с кибербуллингом

1. Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию.

2. Сохраните все возможные свидетельства происходящего (скриншоты экрана, электронные письма, фотографии и т.п.).

3. 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.

4. 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

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 себя.

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 нехорошо ставить на аватарку 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.

6. 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

1. Если ребенок желает познакомиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу

2. Проговорите с ребенком ситуацию и внимательно его выслушайте. Выясните у ребенка всю возможную информацию

3. 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.

4. Сохраните все свидетельства переписки и контактов незнакомца с ребенком (скриншоты экрана, электронные письма, фотографии и т.п.).

5. При обнаружении признаков совращения следует немедленно сообщить об этом в правоохранительные органы.

6. 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

1. 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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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 проц.) пользуется сервисами Интернета, связанными с общением. Другую часть зависимых (9 проц.) привлекают информационные сервисы сети.

Предупреждение интернет-зависимости

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 заметает 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.

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 обновления 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.