Информационно-методические материалы по теме «Безопасность детей в интернете»

1. Опасности, с которыми дети могут столкнуться в сети

Существует немало серьезных рисков, с которыми дети сталкиваются онлайн. Получая доступ к неподходящей информации на сайтах, посвященных преступной деятельности, или заходя на сайтах, подвергающие риску их конфиденциальность. Большую озабоченность вызывает порнографический и иной контент сексуальной направленности, распространены и другие виды неприемлемой доступной информации, которая может быть столь же вредной для детей.

Риск получения ребенком доступа к неподходящей информации включает в себя:

- Доступ к информации, которая может быть не подходящей для детей вообще;
- Сайты, посвященные продаже контрабандных товаров или другой незаконной деятельности;
- Сайты, подвергающие риску конфиденциальности посетителей;
- Сайты, размещающие изображения порнографического или иного сексуального контента, к которым дети могут легко получить доступ;
- Сайты с рекламой табака и алкоголя;
- Сайты, посвященные изготовлению взрывчатых веществ;
- Сайты, пропагандирующие наркотики;
- Сайты, пропагандирующие насилие;
- Сайты, публикующие дезинформацию;
- Сайты, позволяющие детям принимать детям участие в азартных играх онлайн.

Для детей эти риски могут оказаться очень опасными, ведь они могут выдать информацию о кредитной карте родителей и её пароль (а также любые другие пароли), выдать личную информацию о семье, купить вещи без ведома родителей, нарушить авторские права, совершить компьютерные преступления и многое другое. В некоторых случаях они даже не знают, что совершают это. Наконец, существует риск атаки личного компьютера вирусами или хакерами.

2. Безопасное общение детей в интернете

Если ребенок только начал общение с Интернетом, необходимо познакомить его с практическими способами безопасной работы в Интернете. Противостояние угрозам Интернета включает два основных момента:

- Находясь в Интернете, не нужно терять бдительности и поддаваться ухищрениям злоумышленников, реализующих атаку на локальный компьютер;
- Необходимо построить защиту компьютера, которая будет включать в себя надежное приложение-антивирус, а также новейшую версию браузера для работы в Интернете с предварительно настроенными параметрами безопасности.

Приведем некоторые рекомендации, которым необходимо следовать:

1. Работу с электронной почтой лучше всего осуществлять с помощью почтовых сервисов Web-сайтов, которые выполняют антивирусную проверку почтовых сообщений.

2. Можно использовать «временный» адрес электронной почты.

3. Запомните, что если вы используете почтовый клиент, никогда не конфигурируйте его на автоматическое открытие почтовых вложений. Любое послание от любого лица может содержать вложение самого опасного характера, поскольку его может послать кто угодно, в том числе вирус, заразивший компьютер отправителя.

4. Предпочтительно выступать на форумах с модераторами - такими, которые следят за поведением участников, и реагирует на плохое поведение и появление плохих личностей.

5. Знайте, что специфика общения в Интернете такова, что она имеет тенденцию притягивать негатив. Будьте очень рассудительны в том, как вы описываете вещи, следите за языком, который преднамеренно может передавать враждебность.

6. Используйте в письмах шаблонные приветствия и благодарности, которые вставляют в начало или конец каждого послания.

7. Непосредственно перед отправкой специалисты советуют всегда производить контрольное прочтение. Таким образом, можно убедиться, что приложены все файлы, а в сообщении написано то, что запланировано.

8. Следите за поведением своего компьютера, когда посещаете Web-сайты. Если компьютер начинает проявлять подозрительную активность или процессор по непонятным причинам начнет перезагружаться, проверьте с помощью диспетчера задач, что у вас запущено. Настораживать должны непонятные сообщения, некорректное и нелогичное поведение браузер и т.п. в крайнем случае, прервите соединение.

3. Инструкция по безопасному общению в чатах.

В Интернете также широко распространены службы для мгновенного обмена сообщениями и онлайн-общения (Windows Live Messenger, ICQ, IRC, чаты). Эти службы также могут таить в себе опасности при их использовании детьми, поэтому придерживаться некоторых правил.

1. Не доверяйте никому вашу личную информацию.
2. Сообщайте администратору чата о проявлениях оскорбительного поведения участников.
3. Если вам неприятно находится в чате, покиньте его.
4. Если вам что-то не понравилось, обязательно расскажите об этом родителям.
5. Будьте тактичны по отношению к другим людям в чате.

4. Интернет-этика

Если вы хотите, чтобы дети стали ответственными пользователями, объясните им фундаментальные правила поведения в сети:

- Узнайте правила прежде, чем что-нибудь сказать или сделать. Некоторые чаты и форумы имеют специальные правила, поясняющие, что Вы можете или не имеете права говорить или кто нарушает правила, знание правил может избавить вас и вашего ребенка от ненужного дискомфорта.
- Думайте прежде, чем что-либо напечатать. Удостоверьтесь, что вы говорите приемлемые вещи, которые не приведут к разгоревшемуся конфликту. Единственное,

в чем вы можете не сомневаться, - это в том, что всё, сказанное вами в Интернете, может вернуться и неотступно преследовать вас.

- Не относитесь критически к другим, особенно новичкам, даже если они нарушают правила. Если вы должны помочь кому-то или исправить кого-то, сделайте это по электронной почте, а не на общественном форуме. Помните, что и вы когда-то были новичком.
- Не тратьте время других пользователей впустую. Не посылайте цепочку электронных писем, не передавайте киберслухи, не разыгрывайте других, не рассылайте снам.
- Защищайте личную жизнь и личную информацию других пользователей. Не публикуйте в онлайне чей-либо адрес электронной почты без разрешения владельца. Не используйте без разрешения чужой пароль.
- Не присваивайте вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).

5. Как не следует вести себя в сети

- Печатать ЗАГЛАВНЫМИ БУКВАМИ, что может рассматриваться как крик, провоцирующий спор или конфликт.
- Размещать ложную информацию или грубые высказывания о другом человеке.
- Отправлять большие вложенные файлы, не спросив разрешения у получателя.
- Общаться к другим в чате по их настоящему имени.
- Рассылать электронную почту рекламного содержания людям, которых Вы не знаете.
- Отклоняться о темы разговора на форуме.
- Не дожидаться своей очереди или не следовать правилам чата или форума.

6. Феномен «Интернет-зависимости». Профилактика интернет-зависимости у учащихся.

Интернет-зависимость можно сравнить с любой другой формой зависимости интернет-зависимость предлагает способ убежать от реальности, приятные чувства и альтернативную реальность, которая маскирует депрессию и беспокойство.

Социальные контакты в Интернете представляют большую опасность, чем телевидение, так как предполагают общение с другими людьми. Притворяясь новыми личностями, люди могут начать верить, что их любят и заботятся о них за их новые обличия. Интернет захватывает ребенка целиком, не оставляя ему ни времени, ни сил на другие виды деятельности, на упорядочивание жизни собственной становящейся личности. Феномен зависимости от Интернета постоянно изменяется, поэтому необходимо проводить профилактические меры по предупреждению Интернет-зависимости. Существует «группа риска» среди детей, которые могут быть подвержены Интернет-зависимости. Они необщительны или не имеют

коммуникативных навыков, они погружены в себя, много фантазируют, держаться в стороне от сверстников. Такие дети, чаще всего, не обладают способностью преодолевать стрессовые ситуации, трансформировать их в различного рода поисковую активность.

Психиатр Иван Голдберг, предложил 5 советов для преодоления этой зависимости:

1. Признайте свою зависимость.
2. Определите проблемы, лежащие в основе зависимости.
3. Решайте реальные проблемы. Старайтесь избежать стрессовых ситуаций.
4. Контролируйте работу на компьютере. Совсем не обязательно полностью выключать его - можно просто ограничить время нахождения в Интернете.
5. Проводите различие между интерактивной фантазией и полезным пользованием Интернета.

Список рекомендуемой литературы

1. Центр безопасного интернета в России: портал [Электронный ресурс]. - Режим доступа: http://www.saferunet.ru/. Дата обращения: 29.03.2013.
2. Защита детей от вредной информации в сети интернет: портал [Электронный ресурс]. - Режим доступа: http://www.internet-kontrol.ru/. Дата обращения: 29.03.2013.
3. Безопасность детей в Интернете [Электронный ресурс] / Российский офис Microsoft в рамках глобальных инициатив Microsoft. - Режим доступа: http://www.ifap.ru/library/book099.pdf Дата обращения: 29.03.2013.
4. Азбука безопасности: портал [Электронный ресурс]. - Режим доступа: http://azbez.com/safety/internet. Дата обращения: 29.03.2013.
5. On-Ляндия. Безопасная WEB-страна: портал [Электронный ресурс]. - Режим доступа: http://www.onlandia.by/html/etusivu.htm. Дата обращения: 29.03.2013.
6. Дети России Он-лайн: портал [Электронный ресурс]. - Режим доступа: http://detionline.com/. Дата обращения: 29.03.2013.
7. Фонд развития Интернет: портал [Электронный ресурс]. - Режим доступа: http**://www.fid.su/**. Дата обращения: 29.03.2013.
8. Лига безопасного интернета: портал [Электронный ресурс]. - Режим доступа: http://www.ligainternet.ru/inform-about-illegal-content Дата обращения: 29.03.2013.
9. Безопасный Интернет в России: портал [Электронный ресурс]. - Режим доступа: http://www.saferinternet.ru/. Дата обращения: 29.03.2013.
10. Правила безопасного пользования Интернетом: из специального документа американских епископов «Твоя семья и кибернетическое пространство», принятого 16 июня 2000 г. // Классное руководство и воспитание школьников. Приложение к газете «Первое сентября». - 2007. - № 9. - С. 15.
11. Здоровье и безопасность детей в мире компьютерных технологий и Интернет. Учебно-методический комплект. - М.: СОЛОН-ПРЕСС, 2010. - 176 е.: ил.

Составитель информационно-методических материалов - А.Ю. Муратов, директор Центра развития основного и среднего общего образования КГБОУ «Алтайский краевой институт повышения квалификации работников образования»

При составлении методических рекомендаций был использован следующий источник: Здоровье и безопасность детей в мире компьютерных технологий и Интернет. Учебно-методический комплект. - М.: СОЛОН- ПРЕСС, 2010.- 176 с.: ил.