

Методические рекомендации родителям по информационной безопасности детей

В России около 8 миллионов пользователей глобальной сети — дети. Они могут играть, знакомиться, познавать мир... Но в отличие от взрослых, в виртуальном мире они не чувствуют опасности. Наша обязанность — защитить их от негативного контента.

Преступники и злоумышленники.

Преступники используют преимущества анонимности для завязывания доверительных и дружеских отношений с неопытными молодыми людьми. Преимущественно контакты с детьми устанавливают в чатах, по электронной почте или на форумах. Для решения своих проблем многие подростки обращаются за поддержкой на конференции, где незнакомые люди могут привлечь подростка своим вниманием, заботливостью, добротой и даже подарками. Злоумышленники выслушивают проблемы подростков и сочувствуют им, но постепенно вносят в свои беседы оттенок сексуальности или демонстрируют материалы эротического содержания. Преступники могут также обсуждать возможность встречи с детьми в реальной жизни.

Заражение вредоносными и нежелательными программами.

К вредоносным программам относятся вирусы, черви и «троянские кони» — это компьютерные программы, которые могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с Интернетом, использовать компьютер для распространения своих копий на компьютеры коллег, друзей, родственников пользователя и по всей остальной глобальной Сети.

Под «нежелательным программным обеспечением» понимаются программы, которые выполняют на компьютере некие задачи без согласия на то пользователя. Они могут показывать рекламные сообщения, объявления или собирать личные данные о человеке, его окружении.

Необходимо постоянно улучшать защиту компьютера. Более подробную информацию см. на веб-сайте Microsoft по адресу <http://www.microsoft.com/Rus/Security/Protect/Default.mspx>

Азартные игры в Интернете.

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. Сайты с азартными играми могут допускать, что люди выигрывают или проигрывают игровые деньги.

Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

Онлайновое пиратство.

Онлайновое пиратство – это незаконное копирование и распространение (как для деловых, так и для личных целей) материалов, защищенных авторским правом – например, музыки, фильмов, игр или программ – без разрешения правообладателя.

Раскрытие личных данных.

Последние исследования показывают, что сегодня примерно половина всех веб-журналов принадлежат подросткам. При этом двое из трех раскрывают свой возраст; трое из пяти публикуют сведения о месте проживания и контактную информацию, а каждый пятый сообщает свое полное имя. Подробное раскрытие личных данных потенциально опасно.

Интернет-мошенничество и хищение данных кредитной карты.

Интернет-мошенничество может осуществляться с помощью фальшивых электронных писем, в которые включается ссылка, ведущая на популярный узел, но в действительности она приводит пользователя на мошеннический узел, который выглядит точно так же, как официальный. Убедив пользователя в том, что он находится на официальном узле, хакеры пытаются склонить его к вводу паролей, номеров кредитных карт и другой секретной информации, которая потом будет использована с ущербом для пользователя. Поэтому, посещая веб-сайты, нужно самостоятельно набирать в обозревателе адрес веб-сайта и не пользоваться ссылкой, содержащейся в подозрительном электронном письме.

Неправильное формирование нравственных ценностей.

В Интернете можно встретить материалы нежелательного характера, к которым можно отнести материалы порнографического, ненавистнического содержания, материалы суицидальной направленности, сектантские материалы, включающие ненормативную лексику. Существуют средства фильтрации нежелательного материала, но фильтры могут только помочь в блокировании только некоторых нежелательных материалов и решить полностью проблему не могут. Поэтому взрослым важно поддерживать доверительные отношения с детьми, чтобы они без колебаний обращались за советом и помощью.

С более подробной информацией об опасностях и правилах безопасности в Интернете можно ознакомиться в буклете <http://www.ifap.ru/library/book099.pdf>

Советы родителям.

Опасности

Расскажите своим детям об опасностях, существующих в Интернете, и научите правильно выходить из неприятных ситуаций.

Компьютер

Повысьте уровень общей безопасности Вашего компьютера.

Время

Следите за достижением равновесия у вашего ребенка между временем, проводимым в Интернете и вне его.

Правила

Обсудите внутрисемейные правила пользования Интернетом.

Этикет

Научите детей уважать других в Интернете.

Внутрисемейные правила пользования Интернетом.

Перед тем как дети начнут осваивать Интернет необходимо обсудить и договориться о правилах поведения в сети. Соглашение о семейных правилах пользования сетью можно оформить с ребенком письменно, распечатать, подписать и прикрепить около компьютера. Ниже приведен образец такого соглашения, разработанный специалистами корпорации Microsoft.

Соглашение о кодексе поведения в Интернете.

Я обязуюсь:

- Обращаться к моим родителям, чтобы узнать правила пользования Интернетом: куда мне можно заходить, что можно делать и как долго позволяется находиться в Интернете (____ минут или ____ часов).
- Никогда не выдавать без разрешения родителей личную информацию: домашний адрес, номер телефона, рабочий адрес или номер телефона родителей, номера кредитных карточек или название и расположение моей школы.
- Всегда немедленно сообщать родителям, если я увижу или получу в Интернете что-либо тревожащее меня или угрожающее мне; сюда входят сообщения электронной почты, сайты или даже содержимое обычной почты от друзей в Интернете.
- Никогда не соглашаться лично встретиться с человеком, с которым я познакомился в Интернете, без разрешения родителей.
- Никогда не отправлять без разрешения родителей свои фотографии или фотографии членов семьи другим людям через Интернет или обычной почтой.
- Никогда никому, кроме своих родителей, не выдавать пароли Интернета (даже лучшим друзьям).
- Вести себя в Интернете правильно и не делать ничего, что может обидеть или разозлить других людей или противоречить

закону.

- Никогда не загружать, не устанавливать и не копировать ничего с дисков или из Интернета без должного разрешения.

- Никогда не делать без разрешения родителей в Интернете ничего, требующего оплаты.

- Сообщить моим родителям мое регистрационное имя в Интернете и имена в чате.

Имя (ребенок) Дата

Родитель или опекун Дата

Повышение уровня безопасности детей в Интернете при помощи технических и технологических средств

Вопросы информационной безопасности и совершенствования технологических решений в этой области находятся в поле внимания ведущих корпораций и компаний производителей программного обеспечения для компьютеров.

Инструменты безопасности от Microsoft.

Корпорация Microsoft предлагает использовать программу Windows Security Center, которая 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.

Для удаления шпионского программного обеспечения, попавшего на компьютер, предлагаются специальное антишпионское программное обеспечение, в частности, программы: Windows Defender, Malicious Software Removal Tool. Эти бесплатные программы можно загрузить с сайта <http://www.microsoft.com/downloads>.

Кроме того, для обеспечения безопасной работы в сети Интернет можно внести соответствующие изменения в настройки программ. Например, заблокировать доступ к нежелательной информации в Internet Explorer и MSN Explorer, повысить уровень безопасности при работе ребенка с электронной почтой в программе Outlook Express, повысить уровень конфиденциальности при общении вашего ребенка в Интернете.

Не следует забывать, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются дети за компьютером.

Более подробную информацию о защите своего домашнего компьютера можно найти на сайте <http://www.microsoft.com/rus/security>

Инструменты безопасности Google.

Компания Google создала Интернет ресурс «Справочник по детской безопасности в Интернете». Адрес ресурса: google.ru/familysafety

В разделе «Инструменты безопасности Google» говорится о специальных инструментах безопасного поиска с помощью которого родители могут оградить себя и своих детей от неприемлемого контента.

Раздел «Рекомендации партнеров» включает практические рекомендации о том, как помочь юным пользователям оставаться в безопасности в киберпространстве и избежать существующих рисков.

Здесь вы также узнаете, куда дети и взрослые могут обратиться по вопросам безопасного использования Интернета.

Видеоролики для детей о безопасности в Интернет
Сотрудниками Youtube создано несколько видеороликов, рассказывающих детям, как надо и как не надо вести себя в Интернете.

Видеоролик «Развлечения и безопасность в Интернете».

Адрес видео ролика: <http://www.youtube.com/watch?v=HbVgg6-3EWo&feature=autoplay&list=PLD70B32DF5C50A1D7&playnext=1>

Как обнаружить ложь и остаться правдивым в Интернете?

В Сети ты можешь встретить все, что угодно – от уроков истории и фотографий звезд до скабрёзных шуток и нелепых картинок. Но не стоит думать, что, раз информация появилась в Интернете, она является достоверной. Чтобы разобраться, какой информации в Сети можно, а какой нельзя доверять, следуй простым советам:

- Относись к информации осторожно. То, что веб-сайт здорово сделан, это еще ни о чем не говорит. Спроси себя – за что этот сайт выступает? В чем меня хотят убедить его создатели? Чего этому сайту не достает? Узнай об авторах сайта: зайдя в раздел “О нас” или нажми на похожие ссылки на странице. Узнай, кто разместил информацию. Если источник надежный, например, университет, то, вполне возможно, что информации на сайте можно доверять.
- Следуй правилу трех источников. Проведи свое расследование и сравни три источника информации, прежде чем решить, каким источникам можно доверять. Не забывай, что факты, которые журналисты сообщают, нужно очень хорошо проверить, если ты хочешь использовать их в своей домашней работе.

Как предоставлять достоверную информацию?

Будь ответственным – и в реале, и в Сети. Простое правило: если ты не будешь делать что-то в реальной жизни, не стоит это делать в онлайн. Не занимайся плагиатом. То, что материал есть в Сети, не означает, что его можно взять без спроса. Если ты хочешь использовать его, спроси разрешения.

Сообщая о неприемлемом контенте, ты не становишься доносчиком. Наоборот, ты помогаешь делу безопасности Сети. Когда ты грубишь в Интернете, ты провоцируешь других на

такое же поведение. Попробуй оставаться вежливым или просто промолчать. Тебе станет приятнее.

Все, что ты размещаешь в Интернете навсегда остается с тобой – как татуировка. Только ты не сможешь эту информацию удалить или контролировать ее использование. Ты ведь не хочешь оправдываться за свои фотографии перед своим будущим работодателем?

Итак:

Проверь хотя бы три источника информации, прежде чем ты решишь, что информация достоверна. И в Интернете, и в реальной жизни соблюдай правила. Агрессия, кража, обман – запрещены. Сообщай о тех, кто ведет себя подобным образом.

Защищай себя – сейчас и в будущем. Подумай, прежде чем что-либо разместить в Интернете.

Видеоролик «Как оставаться в безопасности на YouTube»

Адрес видео ролика:

<http://www.youtube.com/watch?v=HbVgg6-3EWo&feature=autoplay&list=PLD70B32DF5C50A1D7&playnext=1>

YouTube – это сообщество, основанное на взаимном доверии. Мы надеемся, что ты ответственно пользуешься нашим сайтом. Чтобы оставаться в безопасности на YouTube, соблюдай несколько простых правил.

Правила

Будь сознательным.

YouTube не предназначен для детей до 13 лет. Если ты младше, ждем тебя на сайте, как только тебе исполнится 13. Изучи принципы сообщества – они о том, что можно и чего нельзя делать на сайте. Мы серьезно настроены. Если ты получишь три предупреждения о нарушении правил, мы закроем твой аккаунт. Если аккаунт закрыли, новый создавать нельзя. Отмечая видео, которые, по твоему мнению, нарушают наши правила, ты помогаешь нам поддерживать безопасность на сайте. Не груби в комментариях. Ты не должен соглашаться с другими, просто уважай чужое мнение. Соблюдай авторские права – если материал не твой, не размещай его.

Уважай себя и других. Если ты считаешь, что тебе что-то угрожает на сайте – расскажи взрослому. Или посети центр безопасности YouTube, чтобы узнать, как решить проблему. Не поддавайся на провокации. Удаляй нежелательные комментарии к своим видео и используй инструменты YouTube для того, чтобы блокировать нежелательных юзеров. Ты можешь убрать нецензурные слова и комментарии на темы секса в любых видео. Кликни на параметр “скрыть оскорбительные слова” рядом с пунктом “текстовые комментарии”. Перед тем, как разместить видео, представь, что его увидит твоя бабушка. Если бы тебе этого не хотелось – подумай хорошенько, стоит ли вообще размещать материал. Откровенный сексуальный контент запрещен на YouTube.

Даже если на этих видео лично ты. Не размещай такие материалы, а если увидишь подобное – отмечай, как неприемлемое.

Личные данные.

Делай свои видео доступными только избранным и давай доступ к ним только тем, кому доверяешь. Сохраняй свои личные данные в тайне. Не разглашай такую информацию, как адрес или номер телефона. Помни: сотрудники YouTube никогда не просят твой пароль, e-mail или любую другую информацию об аккаунте. Не доверяй тому, кто требует от тебя такие сведения. Если чье-то видео использует твои данные без твоего согласия, обратись к тому, кто его разместил. Иногда люди не осознают, что нарушили правила. Если все же видео не убрали, сообщи администрации. Прежде чем разместить видео, получи разрешения от тех, кто на нем запечатлен. Если ты разместил личные данные человека без его разрешения, тебя могут исключить из сообщества.

Тебе может понравиться не все, что ты увидишь, что-то может показаться тебе оскорбительным. Если ты обнаружишь видео, нарушающее правила, отметь его как неприемлемое. Если нарушения нет – посмотри что-то другое, зачем тратить время на то, что тебе не интересно?

Помни, это сообщество – для тебя! Наслаждайся возможностями сайта. Есть много способов проявить себя на сайте. Главное – уважать при этом других.

Видеоролик «Остерегайся мошенничества в Интернете»

Адрес видео ролика: <http://www.youtube.com/watch?v=AMCvZXcd9w&feature=BFa&list=PLD70B32DF5C50A1D7&lf=autoplay>

Видеоролик «Как обнаружить ложь и остаться правдивым в

Интернете»

Адрес видео ролика:

<http://www.youtube.com/watch?v=5YhdS7rrxt8&feature=relmfu>

Линия помощи «Дети онлайн»

Линия помощи «Дети онлайн» — служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования интернета и мобильной связи. На Линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М.В. Ломоносова и Фонда Развития Интернет. Телефон доступа 8 800 25 000 15. Адрес ресурса: <http://detionline.com/video/professional> Раздел «Консультирование» содержатся ответы на следующие вопросы:

- Что происходит с психикой ребенка или подростка, когда он играет в компьютерные сетевые игры, в так называемые «стрелялки»? Опасна ли эта агрессивность, которая проявляется в подобных играх?
- Каковы первые признаки компьютерной зависимости у детей и

подростков? Что нужно родителям делать в том случае, если у ребенка проявляются симптомы такого рода зависимости?

- Как влияет на детей и подростков многочасовое сидение за компьютером?

В разделе «Правила безопасности» включены практические рекомендации для родителей, детей и педагогов.

Педагогический аспект обеспечения безопасности ребенка в Интернет

Решение задачи по обеспечению безопасности при использовании компьютера и Интернета детьми требует комплексного подхода, решения множества психолого-педагогических вопросов. 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. Информационная безопасность в Интернете может обсуждаться во время уроков информатики, социологии, ОБЖ, гражданского права и др.

Ограничение доступа к нежелательной информации нужно сочетать с демонстрацией качественных образовательных ресурсов. Поэтому, изучение разделов школьной программы необходимо снабдить ссылками как на традиционные бумажные, так и электронные учебники, учебные пособия, энциклопедии, справочники, словари, ресурсы электронных федеральных образовательных коллекций, цифровых хранилищ библиотек и музеев, образовательных сайтов, дидактические материалы учителя, работы других учащихся.