

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ

«БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ: ВОЗРАСТ И ЭТАПЫ РАЗВИТИЯ»

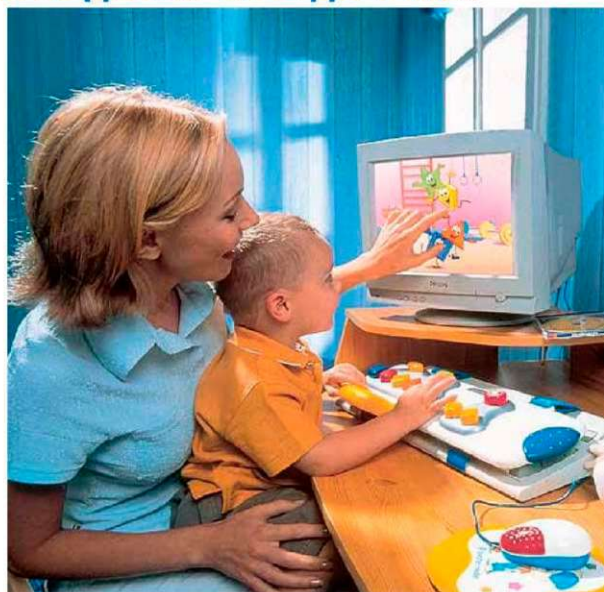
В нашем современном мире пользователи Сети становятся все моложе. Благодаря Интернету дети открывают для себя новый мир, получают огромное количество информации, знакомятся и общаются, занимаются творчеством.

Безопасность в Интернете детей от 2 до 5 лет

В этом возрасте дети уделяют собственно Интернету мало внимания. Однако онлайн-изображения и звуки могут стимулировать воображение и развивать фантазию ребенка.

ЧТО РЕБЕНОК МОЖЕТ ДЕЛАТЬ В ИНТЕРНЕТЕ:

Родители, а также старшие братья и сестры, могут выходить в Интернет вместе с дошкольниками для посещения детских сайтов и игр, общения по скайпу с родными и близкими.



Советы по безопасности

- ✚ Дети этого возраста должны выходить в Интернет только под присмотром родителей.
- ✚ Добавьте сайты, которые вы часто посещаете, в список Избранное, чтобы создать для детей личную интернет-среду.
- ✚ Используйте рассчитанные на детей поисковые машины (наподобие MSN Kids Search) или поисковые машины с фильтрами информации.
- ✚ Используйте средства блокирования нежелательного материала (например, MSN Premium's Parental Controls) как дополнение (не замену) к родительскому контролю.
- ✚ Помогите защитить детей от назойливых всплывающих окон с помощью специальных программ. Это функция также встроена в Windows XP с последним обновлением и в панель инструментов MSN.
- ✚ Когда маленькие дети начинают осваивать Сеть, остальные члены семьи должны служить для них примером.

Безопасность в Интернете детей от 5 до 7 лет

У детей этого возраста обычно открытая натура и положительный взгляд на мир.

Они доверяют авторитету взрослых, хотят вести себя хорошо, гордятся приобретенным умением читать и считать, готовы к новым познаниям и творчеству.



ЧТО РЕБЕНОК МОЖЕТ ДЕЛАТЬ В ИНТЕРНЕТЕ:

Играть, готовиться к школе, участвовать в конкурсах, общаться.

Однако дети этого возраста сильно зависят от взрослых при поиске сайтов, интерпретации информации из Интернета или отправке электронной почты.

Советы по безопасности

- ✚ Добавьте сайты, которые вы часто посещаете, в список Избранное, чтобы создать для детей личную интернет-среду.
- ✚ Используйте рассчитанные на детей поисковые машины (наподобие MSN Kids Search) или поисковые машины с фильтрами информации.
- ✚ Используйте средства блокирования нежелательного материала (например, MSN Premium's Parental Controls) как дополнение (не замену) к родительскому контролю.
- ✚ Помогите защитить детей от назойливых всплывающих окон с помощью специальных программ. Это функция также встроена в Windows XP с последним обновлением и в панель инструментов MSN.
- ✚ Расскажите детям о конфиденциальности. Научите их никогда не выдавать в Интернете информацию о себе и своей семье. Если на сайте необходимо, чтобы ребенок ввел имя, помогите ему придумать псевдоним, не раскрывающий никакой личной информации, объясните, для чего это нужно.
- ✚ Не разрешайте детям этого возраста пользоваться службами мгновенного обмена сообщениями, чатами или досками объявлений, самостоятельно отправлять письма по электронной почте.
- ✚ Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится. Получите дополнительную информацию об обращении с интернет-преступниками и хулиганами. Сообщите о негативном контенте в компетентные органы (*подробнее: на стр. 9*)

Безопасность в Интернете детей от 7 до 9 лет

Детей этой возрастной группы (как правило, ученики 1-3 классов) только начинают развивать чувство своей моральной и половой индивидуальности.

Они доверчивы и не сомневаются в авторитетах, часто интересуются жизнью старших детей.

Однако в этом возрасте у детей появляется желание выяснить границы свободы: что они могут себе позволить делать без разрешения родителей.



ЧТО РЕБЕНОК МОЖЕТ ДЕЛАТЬ В ИНТЕРНЕТЕ:

Дети этого возраста любят путешествовать по Интернету и играть в сетевые игры. Возможно, они используют электронную почту и могут также заходить на сайты и чаты, посещать которые родители не разрешали.

Советы по безопасности

- ✚ Создайте список домашних правил Интернета при участии детей.
- ✚ Приучите детей посещать строго те сайты, которые вы разрешили.
- ✚ Держите компьютеры с подключением к Интернету в общих комнатах.
- ✚ Используйте рассчитанные на детей поисковые машины (наподобие MSN Kids Search) или поисковые машины с фильтрами информации.
- ✚ Используйте средства блокирования нежелательного материала (например, MSN Premium's Parental Controls) как дополнение (не замену) к родительскому контролю.
- ✚ Создайте семейный электронный ящик вместо того, чтобы позволять детям иметь собственные адреса.
- ✚ Научите детей советоваться с вами перед раскрытием информации через электронную почту, чаты, доски объявлений, регистрационные формы и личные профили.
- ✚ Научите детей не загружать программы, музыку или файлы без вашего разрешения.
- ✚ Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.
- ✚ Не разрешайте детям этого возраста пользоваться службами мгновенного обмена сообщениями.
- ✚ Позволяйте детям заходить на детские сайты только с хорошей репутацией и контролируемым общением.
- ✚ Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.
- ✚ Говорите с детьми о традиционных семейных ценностях, взаимоотношениях между полами, так как в Интернете дети могут легко натолкнуться на порнографию или сайты «для взрослых».
- ✚ Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повто-

рится. Получите дополнительную информацию об обращении с интернет-преступниками и хулиганами. Сообщите о негативном контенте в компетентные органы (*подробнее: на стр. 9*)

Безопасность в Интернете детей от 9 до 13 лет

Этот возраст – время быстрых изменений в жизни.

Хотя дети все еще сильно зависят от своих родителей, они уже хотят некоторой свободы.

Ребята начинают интересоваться окружающим миром, и отношения с друзьями становятся для них по-настоящему важными.



ЧТО РЕБЕНОК ДЕЛАЕТ В ИНТЕРНЕТЕ:

Дети этого возраста используют интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в игры онлайн, заходят на фанатские сайты своих кумиров. Их любимый способ общения – мгновенный обмен сообщениями.

Советы по безопасности

- ✚ Создайте список домашних правил Интернета при участии детей.
- ✚ Держите компьютеры с подключением к Сети в общих комнатах, а не в спальнях детей.
- ✚ Используйте средства фильтрации нежелательного материала (наподобие MSN Premium's Parental Controls) как дополнение (не замену) к родительскому контролю.
- ✚ Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.
- ✚ Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
- ✚ Позволяйте детям заходить на детские сайты только с хорошей репутацией и контролируемым общением.
- ✚ Научите детей никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Познакомьте их с информационно-развлекательный сайтом, для детей и подростков открытым Роскомнадзором <http://персональныеданные.дети/>.
- ✚ Научите детей не загружать программы без вашего разрешения – они могут ненароком загрузить вирус или шпионскую программу. Кроме того, объясните ребятам, что, делая файлы общими или загружая из Интернета тексты, фотографии или рисунки, они могут нарушать чьи-то авторские права.
- ✚ Чтобы ребенок не мог заниматься чем-то посторонним без вашего ведома, создайте ему учетную запись с ограниченными правами.
- ✚ Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит их или угрожает. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам об этом. Похвалите их и побуждайте подойти еще раз, если случай по-

вторится. Получите дополнительную информацию об обращении с интернет-преступниками и хулиганами. Сообщите о негативном контенте в компетентные органы (*подробнее: на стр. 9*).

- ✚ Говорите с детьми о традиционных семейных ценностях, взаимоотношениях между полами, так как в Интернете дети могут легко натолкнуться на порнографию или сайты «для взрослых».
- ✚ По-прежнему пользуйтесь семейным электронным ящиком вместо того, чтобы позволять детям иметь собственные адреса, либо настаивайте на том, чтобы дети предоставили вам доступ к своей электронной почте, чтобы вы могли убедиться, что они не общаются с незнакомцами.
- ✚ Расскажите детям об ответственном, достойном поведении в Интернете. Ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

Безопасность в Интернете детей от 13 до 17 лет

Младшие подростки, как правило, проходят через период низкой самооценки; ищут поддержку у друзей и неохотно слушают родителей.

Те, кто постарше – ищут свое место в мире и пытаются обрести собственную независимость. В этом возрасте подростки уже полноценно общаются с окружающим миром. Они бурлят новыми мыслями и идеями, но испытывают недостаток жизненного опыта.

Родителям важно продолжать следить, как в этом возрасте их дети используют Интернет.



ЧТО ПОДРОСТКИ ДЕЛАЕТ В ИНТЕРНЕТЕ:

Они скачивают музыку, пользуются электронной почтой, службами мгновенного обмена сообщениями и играют. Большинство пользуются чатами, общаются в приватном режиме.

Мальчики в этом возрасте склонны сметать все ограничения и жаждут грубого юмора, крови, азартных игр и картинок для взрослых.

Девочкам больше нравится общаться в чатах; и юные дамы более чувствительны к сексуальным домогательствам в Интернете.

В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей.

Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности

- ✚ Создайте список домашних правил Интернета при участии подростков. Следует указать список запрещенных сайтов, часы нахождения в Сети и руководство по общению в Интернете (в том числе и в чатах).
- ✚ Держите компьютеры с подключением к Интернету в общих комнатах.
- ✚ Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются, так, как если бы речь шла о друзьях в реальной жизни. Спрашивайте о людях, с которыми подростки общаются, используя мгновенный обмен сообщениями, и убедитесь, что эти люди им знакомы.
- ✚ Используйте средства блокирования нежелательного материала (например, MSN Premium's Parental Controls) как дополнение (не замену) к родительскому контролю.
- ✚ Знайте, какими чатами и досками объявлений пользуются дети и с кем они общаются. Поощряйте использование модерлируемых чатов и настаивайте, чтобы подростки не общались с кем-то в приватном режиме.
- ✚ Настаивайте, чтобы они никогда не соглашались на личные встречи с друзьями из Интернета без вашего сопровождения на первой встрече (или сопровождения другого взрослого, которому вы доверяете). Объясните, что если виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к заботе подростка о собственной безопасности.
- ✚ Научите детей никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Познакомьте их с информационно-развлекательный сайтом, для детей и подростков открытым Роскомнадзором <http://персональныеданные.дети/>.
- ✚ Научите детей не загружать программы, музыку или файлы без вашего разрешения. Объясните, что иначе подростки могут нарушить авторские права и тем самым закон.
- ✚ Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит их или угрожает. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам об этом. Похвалите их и побуждайте подойти еще раз, если случай повторится. Получите дополнительную информацию об обращении с интернет-преступниками и интернет-преступниками и хулиганами. Сообщите о негативном контенте в компетентные органы (*подробнее: на стр. 9*).
- ✚ Говорите с детьми о традиционных семейных ценностях, взаимоотношениях между полами, расскажите детям о порнографии в интернете и противоправности ее распространения, направьте их на хорошие сайты о здоровье, вреде ранних половых контактов, предупреждении подростковой беременности.
- ✚ Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
- ✚ Возьмите за правило знакомиться с сайтами, которые посещают подростки. Убедитесь, что дети не посещают сайты с оскорбительным содержанием, не публикуют личную информацию или свои фотографии.
- ✚ Напоминайте детям об ответственном, достойном поведении в Интернете. Ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
- ✚ Убедитесь, что подростки советуются с вами перед покупкой или продажей чего-либо в Интернете.
- ✚ Обсудите с подростками азартные сетевые игры и их возможный риск. Напомните, что для детей это незаконно.

Зачастую наши дети более «продвинутые» интернет-пользователи, чем мы, их родители. Обсуждать с детьми их путешествия в Сети поможет приведенная ниже информация.



Список терминов

- **Аккаунт** (англ.- account) – учетная запись, регистрационная запись.
- **Антивирус** – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.
- **Администраторы, модераторы сайта** – специальные сотрудники сайта, которые следят за исполнением установленных на сайте правил.
- **Базы данных (БД)** – специальное программное обеспечение, предназначенное для организации хранения и доступа к данным (информации). Используются при создании программных решений для автоматизации сайта.
- **Браузер** – программа, позволяющая просматривать страницы в сети Интернет. Самые популярные Opera, Mozilla Firefox, Google Chrome, Internet Explorer.
- **Веб-сайт** (англ. Website, от web – паутина и site – «место») в компьютерной сети. Когда говорят «своя страничка в Интернет», то подразумевается целый веб-сайт или личная страница в составе чужого сайта. Кроме веб-сайтов в сети Интернет так же доступны WAP-сайты для мобильных телефонов.
- **Виртуальный собеседник** (англ. chatterbot) – это компьютерная программа, которая создана для имитации речевого поведения человека при общении с одним или несколькими пользователями.
- **Всемирная паутина** – это все веб-сайты Интернета.
- **Домен** (англ. domain), Доменный адрес (англ. domain name) – область пространства иерархических имен сети Интернет, которая обозначается уникальным именем. Это более практичный аналог IP-адреса, обозначаемого цифрами. Доменная адресация возникла в Интернет для удобства пользователей: легче запомнить доменный адрес (например, www.microsoft.com), чем числа IP-адреса. Доменный адрес может содержать латинские буквы, цифры, точки и некоторые другие знаки.
- **Доменный почтовый ящик**, в который поступает почта, приходящая на любые возможные адреса домена (все-что-угодно@ваш-домен).
- **Интернет** – всемирная система объединённых компьютерных сетей для хранения и передачи информации.
- **Игнор** – игнорирование, занесение в черный список.
- **Кибербуллинг** – травля через Интернет, электронную почту, СМС и т. д., агрессивное преследование одного из членов коллектива (школьников или студентов) со стороны остальных членов коллектива или его части.
- **Логин** (от английского log in — «входить в») – это имя, которое вы выбираете для регистрации в системе или имя, которое система вам сама присваивает. Каждый пользователь в системе имеет свой уникальный логин. Он помогает системе и другим пользователям отличить одного пользователя от другого.
- **Он-лайн игры** – игровой процесс основан на взаимодействии с другими игроками и игровым миром, требующий постоянного подключения к Интернету.
- **Интернет-магазин**. Действующим Законодательством РФ не определено понятие «Интернет-магазин». В классическом понимании "Интернет-магазин" ("Электронный магазин", "Сетевой магазин"; и т.д.), – это интерактивный сайт, в котором: рекламируются

товары и услуги, принимаются заказы на товары и услуги, посетителю, предлагаются различные варианты оплаты заказанных товаров и услуг, возможна их мгновенная оплата через Интернет.

- **Пароль** – набор символов, известный только одному пользователю, необходимый для авторизации (для «входа») на сайте.
- **Персональная страница** (персональный сайт) – совокупность Web-страниц, с содержанием, описывающим сферу интересов какого-либо человека (группы лиц), обычно созданная им самим.
- **Посетители** – количество уникальных посетителей побывавших на страницах вашего ресурса.
- **Почтовый ящик** - дисковое пространство на почтовом сервере, выделенное для хранения, отправки писем пользователя и т.д. (приходящих на его адрес и подлежащих отправке).
- **Родительский контроль** – это программы и службы, которые позволяют родителям и опекунам отслеживать, как ребенок использует компьютер: от фильтрации веб-содержимого и управления контактами электронной почты до ограничений на общение через Интернет. Цель таких средств — обеспечить безопасность ребенка в Интернете, и эти инструменты иногда называют семейными настройками и настройками семейной безопасности. Windows 7, Windows Vista, Xbox 360, Xbox Live, Bing и другие продукты Microsoft включают встроенные настройки семейной безопасности.
- **Сайт** (от англ. website: web — «паутина, сеть» и site — «место», буквально «место, сегмент, часть в сети») – совокупность электронных документов (файлов) частного лица или организации в компьютерной сети, объединённых под одним адресом (доменным именем или IP-адресом).
- **Сервер** (Web-сервер) -1) Компьютер или специализированное устройство в сети со специальным программным обеспечением, обеспечивающий доступ многих пользователей к расположенной на нем информации и функционирование любых необходимых сервисов Интернет: http (сайт), E-mail (электронная почта), конференции, ftp и т.п. Для размещения сайта в Интернет необходим веб-сервер с поддержкой как минимум сервиса http.
2) Сайт, крупный информационный ресурс Интернета.
- **Спам** (англ. spam) – рассылка коммерческой и иной рекламы или иных видов сообщений лицам, не выразившим желания их получать, незапрошенные или нежелательные письма.
- **Социальные сети** – сайты в Интернете, на которых рядовые пользователи заводят свои странички для общения с друзьями. Одна из обычных черт социальных сетей – система «друзей» и «групп». Самые популярные русскоязычные: ВКонтакте, Одноклассники.ш, Мой Мир, Мой Круг, ЖЖ и др.
- **Трафик** (traffic) – поток (объем) информации, проходящей через канал связи, приходящийся на сайт. Может быть исходящим и входящим.
- **Тролли, троллинг** – (от англ. trolling — «ловля на блесну») – размещение в Интернете провокационных сообщений с целью вызвать конфликты между субъектами, взаимные оскорбления и т. п.
- **Файлы, скачивание.** Вся информация в компьютере сохраняется в виде файлов. Это могут быть текстовые файлы, музыкальные, видео, графические, мультимедийные и проч. Файлы можно создавать, копировать, пересылать (например, по электронной почте), выкладывать на сайт для скачивания, скачивать, то есть сохранять на свой компьютер.
- **Фишинг** (от английского fish — «ловить рыбу») – вид мошенничества в интернете, когда у пользователя пытаются узнать логины и пароли.
- «Черный список сайтов» (black list), или как еще его называют "скам лист", представляет собой список сайтов, проектов или людей, которые проводят мошеннические операции в сети или не выполняют взятые на себя обязательства.

- **Хиты** – количество просмотров страниц, на которых побывали посетители ресурса.
- **Хостер (hoster)** - синоним слова хостинг-провайдер (см.)
- **Хостинг (hosting)** - Услуга по предоставлению интернет-сервера и обеспечению его круглосуточной работоспособности. В большинстве случаев предоставляется виртуальный сервер (т.н. виртуальный хостинг), т.е. программное обеспечение, обеспечивающее работу необходимых Вам сервисов, но работающее на одной аппаратной платформе с другими подобными виртуальными серверами. Различают также платный (коммерческий) и бесплатный хостинг.
- **Хостинг-провайдер (hosting provider)** - организация, профессионально занимающаяся предоставлением услуг Хостинга. Лучше выбирать услуги профессиональных Хостеров, т.е. Компаний, основной деятельностью которых является Хостинг, а не обычных Интернет-провайдеров, для которых Хостинг дополнительная услуга к основной.
- **Хосты** – количество посетителей с уникальным IP-адресом.
- **Электронная почта** (англ. email, e-mail, от англ. electronic mail) – технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети. Электронная почта по составу элементов и принципу работы практически повторяет систему обычной (бумажной) почты, заимствуя как термины (почта, письмо, вложение, ящик, доставка и другие), так и характерные особенности – простоту использования, задержки передачи сообщений, достаточную надёжность и в то же время отсутствие гарантии доставки.

При создании памятки использованы материалы:

Безмальный В. Обеспечение безопасности детей при работе в Интернете // КомпьютерПресс. – 2008. – N 10. – С. 62–69.

Сборник руководств и инструкций по обеспечению безопасности детей в сети // Исползуй.ру (<http://ispolzuy.ru/category/kategorii-problem/bezopasnost/roditelskii-kontrol>)

Обзор средств защиты детей от несоответствующей информации в сети // IXBT.com
<http://www.ixbt.com/soft/parentalcontrol.shtml>

Интернет // Википедия (<https://ru.wikipedia.org/wiki/Интернет>)

Словарь компьютерных терминов // Викизнание (http://www.wikiznanie.ru/ru-wz/index.php/Словарь_компьютерных_терминов)

Памятка для родителей об информационной безопасности детей

Определение термина «информационная безопасность детей» содержится в **Федеральном законе № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»**, регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону **«информационная безопасность детей» - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.**

В силу Федерального закона № 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;
2. информация, распространение которой ограничено среди детей определенных возрастных категорий.
3. К информации, запрещенной для распространения среди детей, относится:
 - информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;
 - способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
 - обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
 - отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
 - оправдывающая противоправное поведение;
 - содержащая нецензурную брань;
 - содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
2. вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
4. содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.

2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)
4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающим и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).
5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

■ Возраст от 7 до 8 лет

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7-8 лет

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.
3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
4. Используйте специальные детские поисковые машины.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
9. Научите детей не загружать файлы, программы или музыку без вашего согласия.
10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.

11. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.

12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.

13. Не делайте «табу» из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».

14. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

■ Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже слышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности для детей от 9 до 12 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.

2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.

3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.

4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

6. Не забывайте принимать непосредственное участие в жизни ребенка беседовать с детьми об их друзьях в Интернете.

7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.

8. Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.

9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.

12. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.

13. Расскажите детям о порнографии в Интернете.

14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

■ Возраст детей от 13 до 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности -соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте от 13 до 17 лет

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).

2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.

3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.

4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.

5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модулируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.

6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.

7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.

9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

11. Приучите себя знакомиться с сайтами, которые посещают подростки.

12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде — даже в виртуальном мире.

13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

**Постоянно контролируйте использование Интернета Вашим ребенком!
Это не нарушение его личного пространства, а мера предосторожности и проявление
Вашей родительской ответственности и заботы.**