

Памятка для родителей

Информационная безопасность детей

Определение термина «информационная безопасность детей» содержится в **Законе № 436 – ФЗ**, регулирующем 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.

Согласно Закону № 436 – ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

- информация, запрещенная для распространения среди детей;
- информация, распространение которой ограничено среди детей определенных возрастных категорий.

К информации запрещенной для распространения среди детей, относится:

- 1) информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;
- 2) 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;
- 3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
- 4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- 5) оправдывающая противоправное поведение;
- 6) содержащая нецензурную брань;
- 7) 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.

Обозначение категории информационной продукции знаком информационной продукции и (или) текстовым предупреждением об ограничении распространения информационной продукции среди детей осуществляется с соблюдением требований настоящего Федерального закона ее производителем и (или) распространителем следующим образом:

- 1) применительно к категории информационной продукции для детей, не достигших возраста шести лет, - в виде цифры "0" и знака "плюс";
- 2) применительно к категории информационной продукции для детей, достигших возраста шести лет, - в виде цифры "6" и знака "плюс" и (или) текстового предупреждения в виде словосочетания "для детей старше шести лет";
- 3) применительно к категории информационной продукции для детей, достигших возраста двенадцати лет, - в виде цифры "12" и знака "плюс" и (или) текстового предупреждения в виде словосочетания "для детей старше 12 лет";
- 4) применительно к категории информационной продукции для детей, достигших возраста шестнадцати лет, - в виде цифры "16" и знака "плюс" и (или) текстового предупреждения в виде словосочетания "для детей старше 16 лет";
- 5) применительно к категории информационной продукции, запрещенной для детей, - в виде цифры "18" и знака "плюс" и (или) текстового предупреждения в виде словосочетания "запрещено для детей".;

Правила работы в сети Интернет

1. Не входите на незнакомые сайты.
2. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
3. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.
4. Никогда не посылайте никому свой пароль.
5. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.
6. При общении в Интернет не указывайте свои личные данные, а используйте псевдоним (ник)
7. Без контроля взрослых ни в коем случае не встречайтесь с людьми, с которыми познакомились в сети Интернет.
8. Если в сети необходимо пройти регистрацию, то должны сделать ее так, чтобы в ней не было указано никакой личной информации.
9. Не всей информации, которая размещена в Интернете, можно верить.
10. Не оставляйте без присмотра компьютер с важными сведениям на экране
11. Не сохраняйте важные сведения на общедоступном компьютере.

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 (законным представителям) 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 Интерне. 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 Интернет, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

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

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
- 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.
- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
- Используйте специальные детские поисковые машины.
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
- Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
- Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего ПО.
- Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
- Научите детей не загружать файлы, программы или музыку без вашего согласия.
- Не разрешайте детям использовать службы мгновенного обмена сообщениями.
- В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
- Не забывайте беседовать с детьми об их друзьях в Интернет, как если бы речь шла о друзьях в реальной жизни.
- Не делайте «табу» из вопросов половой жизни, так как в Интернет дети могут легко наткнуться на порнографию или сайты «для взрослых».
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и 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.

Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в Интернет. 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

- Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
- 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.
- Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
- Не забывайте беседовать с детьми об их друзьях в Интернет.
- Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернет.
- Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
- 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 Интернет.
- Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
- Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
- Расскажите детям о порнографии в Интернет.
- Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
- 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 Интернет. 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 в этом возрасте от 13 до 17 лет

- Создайте список домашних правил посещения Интернет при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов («черный список»), часы работы в Интернет, руководство по общению в Интернет (в том числе в чатах).
- Компьютер с подключением к сети Интернет должен находиться в общей комнате.
- Не забывайте беседовать с детьми об их друзьях в Интернет, 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.
- Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
- Необходимо знать, какими чатами пользуются ваши дети. Поощряйте использование модулируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
- Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
- 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 Интернет.
- Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

- Расскажите детям о порнографии в Интернет. Помогите им защититься от спама. Научите подростков не выдавать в Интернет своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
- Приучите себя знакомиться с сайтами, которые посещают подростки.
- Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
- Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Ты учишься в 5-8 классах?



В этом разделе ты найдешь практические советы и рекомендации, которые помогут тебе быть осторожным при использовании Интернета.

Мы подскажем тебе, что делать, если кто-то проявляет к тебе агрессию.

Также мы поможем тебе сделать общение с людьми в Интернете, использование онлайн-игр и твоего мобильного телефона безопаснее.

Вы должны это знать:

-  Регистрируясь на сайтах, не указывайте личную информацию, которую могут все увидеть. Не нужно, чтобы незнакомые люди знали, как вы выглядите и где учитесь,.
-  Не рассказывайте незнакомым как где вы живете, можете сказать название города, но не адрес, по которому Вас могут найти.
-  Общайтесь по веб-камере только с друзьями. Следите, чтобы ваш разговор видели только вы, потому что чужие люди могут записать видео, которое видно через веб-камеру и использовать.
-  Нежелательные письма от незнакомых людей называются «Спам», на них нельзя отвечать, а лучше вообще не открывать потому, что в них могут быть вирусы.
Если вы ответите, люди отправившие письмо будут знать, что ваш почтовый ящик работает и дальше посылать вам спам.
-  Не забудьте сохранить все неприятные сообщения, которые вы получили, чтобы потом показать их взрослым. Взрослые помогут вам и скажут, как правильно поступить. Не расстраивайтесь, если Вы получили плохое сообщение.
-  Если вас кто-то расстроил или обидел, расскажите все взрослому.

Ты учишься в 1, 2 или 3-м классе или только собираешься пойти в школу?



В этом разделе ты можешь прочитать подсказки, которые помогут тебе быть осторожнее, когда ты пользуешься Интернетом.

Мы расскажем тебе что делать, если кто-то к тебе плохо относится в Интернете. Также мы поможем

тебе научиться безопасно пользоваться мобильным телефоном, общаться и играть в Интернете.

Ниже ты увидишь советы, которые помогут тебе и твоим друзьям пользоваться Интернетом безопасно. Прочитав их, ты узнаешь, что делать, если в Интернете тебе угрожают или кто-то с тобой нечестен.

Ты должен это знать:

-  Всегда спрашивай родителей о незнакомых вещах, о которых узнаешь в Интернете. Они расскажут, что безопасно делать, а что нет.
-  Прежде чем начать дружить с кем-то в Интернете спроси у родителей, как безопасно общаться.
-  Никогда не рассказывай о себе незнакомым людям. Где ты живешь, в какой школе учишься и номер твоего телефона должны знать только родители и друзья.
-  Никогда не отправляй свои фотографии людям, которых не знаешь лично. Компьютерный друг мог говорить о себе неправду. Ты ведь не хочешь, чтобы у незнакомого человека была твоя фотография, с которой он сможет сделать все, что захочет.
-  Не встречайся с людьми, с которыми познакомился в Интернете, без родителей. Многие люди выдают себя не за тех, кем являются на самом деле.
-  Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов - читать грубости так же неприятно, как и слышать. Ты можешь нечаянно обидеть человека.
-  Если тебя кто-то расстроил или обидел, обязательно расскажи об этом родителям.

Ты учишься в 9-11 классах?



В этом разделе ты найдешь практические советы и рекомендации, которые помогут тебе быть осторожным при использовании Интернета.

Мы подскажем тебе, что делать, если кто-то проявляет к тебе агрессию. Также мы поможем тебе безопасно общаться, учиться и играть в Интернете.

Ваш личный Интернет рекомендует ...

-  Не публикуй свои личные данные и личные данные своих друзей.



К личным данным относятся номера мобильного и домашнего телефонов, адрес электронной почты и любые фотографии, на которых изображены ты, твоя семья или друзья.



Если ты публикуешь фото- или видеоматериалы в Интернете – любой желающий может скопировать их и потом воспользоваться в своих целях.



Не верь спаму (нежелательной электронной рассылке) и не отвечай на него.



Не открывай файлы, полученные от людей, которых ты не знаешь. Неизвестно, что они могут содержать: это может быть как вирус, так и незаконный материал.



Следи за тем, что пишешь. Не пиши людям то, что никогда бы не сказал им в лицо.



Не забывай, что люди в Интернете могут говорить неправду.



Лучше не встречайся со своими виртуальными друзьями в реальной жизни без присутствия взрослых, которым ты доверяешь. Поверь, лучше не быть «клевым», чем быть в опасности!



Никогда не поздно рассказать, если что-то тебя смущает или настораживает.



Киберугрозы – это устные преследования, которые могут произойти во время пользования Интернетом. Они могут принимать различные формы. Например, электронные письма с угрозами; угрожающие (неприличные) сеансы мгновенных сообщений; агрессивные сообщения по мобильной связи; вебсайты, созданные, чтобы осмеивать других; отправление сообщения от лица другого человека; пересылка личных сообщений, фотографий или видеосъемок другим пользователям.

Как избежать киберугроз? Подсказки для подростков

- Не разглашай свою личную информацию (пароль, имя, адрес, номер телефона, имена членов семьи или друзей). Вся информация может быть использована интернет-злоумышленниками против тебя. Не сообщай свои пароли даже друзьям. Они могут сообщить их кому-то еще. Не исключено, что они станут использовать полученную информацию против тебя.
- Не отправляй свои фотографии и не оставляй адрес электронной почты интернет-знакомым без разрешения родителей.

- Не отвечай на сообщения, будучи в плохом настроении: слово – не воробей, вылетит – не поймаешь.
- Удаляй сообщения от незнакомых, агрессивно настроенных или подозрительных пользователей.
- Если что-то в Интернете кажется тебе подозрительным, скорее всего, оно таким и является. Выходи с насторожившего тебя сайта, чата и т.д.
- Ты должен(а) понимать, что онлайн-общение не является приватным. Другие могут скопировать, распечатать или переслать твои сообщения и фотографии. Будь осторожен(а)!
- Прикрепленные к письмам или сообщениям файлы могут содержать обычные или саморазмножающиеся вирусы.
- Друзья по чату не всегда являются теми, за кого себя выдают.
- Всегда помни, что ответственный взрослый человек не ищет отношений с детьми и подростками.
- Защити себя – никогда не соглашайся встретиться с интернет-знакомыми.



Что делать, если ты уже стал(а) объектом киберугроз?

- Расскажи об этом родителям и продолжай напоминать, пока они не примут нужных мер.
- Никогда не принимай, не читай и не отвечай на сообщения от киберзлоумышленников.
- Не удаляй сообщения с угрозами. Они могут понадобиться при принятии соответствующих мер.
- Если ты получаешь угрозы через службу мгновенных сообщений или в чате, то помни, что обидчик всегда может быть занесен в черный список или заблокирован.
- Если злоумышленник угрожает нанести вред твоей жизни – обратись в правоохранительные органы.



Что должны делать родители?

- Никогда не ставьте компьютер в детскую спальню.
- Больше общайтесь с ребенком.
- Примите участие в процессе накопления опыта Вашим ребёнком для работы в Интернете.
- Регулярно просматривайте файлы на своем компьютере.
- Научите ребенка ответственно пользоваться интернет-ресурсами.
- Проведите с ребенком беседу об опасностях Интернета. Ребенок должен знать, что к Вам всегда можно обратиться за помощью.
- Узнайте больше о «плюсах» и «минусах» пользования Интернетом.

- Обсудите с другими родителями свой опыт работы в Интернете - это будет полезно не только Вам.
- Объясните Вашему ребенку, что ответственный взрослый человек не станет искать отношений с несовершеннолетними.



Блог – это интернет-пространство, где пользователь можешь записать свои мысли и чувства, свои тайные желания и надежды. Блог доступен для просмотра другими пользователями, которые тоже могут оставить в нем свои комментарии.

Блог – это дневник, размещенный в Интернете. В основном, организации бесплатно размещают онлайн-дневники – они получают прибыль, помещая ссылки на страницах блогов. Единственное, что отличает блог от других веб-страниц – его формат. Записи в дневнике вывешены в обратнo-хронологическом порядке, каждая из которых содержит область для комментариев читателей. Это позволяет обсуждать предложенные темы в непрерывном диалоге. Блог может быть составлен любым пользователем на любую тему: школьный обед, как убить паука и т.д. Часто блог содержит ссылки на другие блоги.

Привлекательность блогов для подростков естественна. Создание блогов стало событием общественного значения. Блог - это способ общаться, держать связь, делиться идеями личного характера в неформальном форуме. Показывая свой личный дневник миллионам незнакомцев, подростки стараются привлечь к себе внимание, прячась за экраном компьютера. Не удивительно, что они все больше и больше времени проводят за написанием блогов.

Сексуальный киберманьяк (predator, англ. – «хищник») может получить достаточное количество информации из блога, чтобы составить свое представление (досье) об авторе. Номер школы, имена друзей и учителей, физический адрес, названия улиц, город – все это может быть использовано киберманьяком в корыстных целях. В то время, как ребенок размещает, по его мнению, совершенно безобидную информацию, он в действительности вырисовывает путь к своему дому. Подростку легко внушить ложное чувство безопасности тем, что он считает Интернет анонимным.

Эта ощущаемая анонимность увеличивает риск столкновения с другими опасностями: киберзапугиванием и распространением слухов через Интернет. Не видя своей аудитории, блоггеры не могут ясно представить и понять, какой вред наносят их слова. Школьные сплетни проникают в блоги, и объект сплетен страдает от рук неизвестного онлайн-противника.

Блоги могут быть использованы в качестве одного из способов киберзапугивания. Нельзя преувеличить вред, наносимый киберугрозами. Известен случай, когда в результате киберзапугивания тринадцатилетний подросток покончил жизнь самоубийством. Подростки, особенно в отношении блогов, иногда забывают, что любая информация, размещенная в Интернете, привлекает нежданную аудиторию, что может привести к непредсказуемым последствиям.

Подсказки по безопасности блогов для подростков



Очень важно знать, с какими опасностями ты можешь столкнуться, ведя онлайн-дневник. Помни, что Интернет – густо заселенное пространство, и всегда найдутся люди, киберзлоумышленники, которые захотят проникнуть в твою личную жизнь и получить информацию о тебе, что в дальнейшем может стать причиной проблемы.

Киберманьяки находятся в Интернете 24 часа в сутки, выискивая объект насмешек и пытаясь разработать план захвата жертвы. Если ты не будешь осторожен, то можешь оказаться в очень неудобной и возможно опасной ситуации.

Киберманьяки любят составлять головоломки. Каждая малейшая деталь личной информации для такого человека – это часть головоломки твоей жизни. Помни, что для киберманьяка нужно немного информации, чтобы дать развернутый ответ о твоей личной жизни. Получив достаточное число деталей, благодаря информации, которую ты бессознательно предоставил, он сможет составить всю историю твоей жизни.

Если хочешь создать свой блог, запомни следующие правила:

- **Пароль защитит твой блог. Убедись в том, что никто, кроме твоих родителей, не знает твой пароль.**
- **Не размещай детали личной жизни (места, где ты бываешь, магазины и другую информацию) в своем блоге.**
- **Не указывай в профиле пользователя блога свою личную информацию (имя, домашний адрес, номер телефона, номер школы, почтовый индекс, адрес электронной почты и экранное имя). Такого рода информацией интересуются киберманьяки.**
- **Не стоит размещать личную информацию о своих знакомых - ты можешь привлечь к ним внимание киберманьяка.**
- **Попробуй поставить себя на место киберзлоумышленника. Прочитай свои записи и посмотри, смог бы ты сам выбрать детали, которые приведут к разоблачению твоей личной информации. Если ты нашел какие-то очевидные факты, поменяй их на более обобщенную информацию.**

- **Не размещай свои фотографии и фотографии своих знакомых в блоге.**
- **Не оставляй страницу с блогом открытой на компьютере без присмотра. Любой может войти и написать все, что угодно от твоего имени.**
- **Не распространяй слухи и сплетни о своих знакомых.**

Тридцатое виртуальное царство» или «путешествия юного героя в Интернете»



- Сказка – ложь, да в ней намек – добрым молодцам урок. Ты, конечно, помнишь, что именно так заканчиваются все сказки. А с чего они начинаются? С того, как добрый молодец или юная красавица отправляются на поиски лучшей доли. В нашем с тобой мире каждое утро на такие же поиски отправляются сотни тысяч ребят по всему земному шару. Только путешествуют они не в реальном, а в виртуальном пространстве.
- Это захватывающее приключение, полное неожиданных открытий, новых мест и опасностей. Да, да, ты все верно прочитал. Именно опасностей. А как же без них? Помнишь, сколько козней чинила Баба-Яга Аленушке, а как отважно бился с Кощеем Бессмертным Иванушка? Ни одна сказка не обходится без отрицательных героев. А реальность виртуальная? Тут все гораздо сложнее. Она тоже не обходится без отрицательных героев. Только догадаться, кто являет собой зло, а кто добро, здесь гораздо сложнее.
- Давай попробуем разобраться, как сделать наше путешествие максимально полезным и безопасным. Начнем с начала. Итак, если ты оказался в сети впервые, то тебе, конечно, понадобится помощь взрослых. Именно они станут твоим путеводным клубочком по всемирной паутине. Конечно, лучше заранее узнать о тех опасностях, которые тебя подстерегают, а уже потом отправляться в путь.
- Что ж, тут придется многому учиться. Никуда не денешься. И чем раньше ты начнешь осваивать эти премудрости, тем проще будет совершить твое путешествие. Давай мы с тобой договоримся о том, что твоими главными помощниками станут родители. В любой непонятной ситуации лучше советуйся с ними, чем на каком-то форуме с неизвестными людьми.
- Как ты понимаешь, любой мир, виртуальный или реальный – это прежде всего люди. А они бывают разными. Никогда не знаешь, кто здесь овца, а кто волк в овечьей шкуре. Поэтому будь осторожен. Не надо доверять всем и каждому. Интернет – это не монолог (речь одного), а полилог (речь многих). Ведь получить доступ в Интернет легко, и еще легче оставить там информацию, тем более ее никто не

проверяет. И у каждого на все есть свое мнение. У тебя же есть возможность узнать из множества этих мнений истинное. Поэтому ищи внимательно, не останавливаясь на одном источнике. Родители помогут тебе найти различные словари, энциклопедии и просто занимательные сайты, путешествуя по страницам которых, ты сможешь найти массу интересного, а главное достоверного материала. Лучше ориентироваться на известные ресурсы, чем на сомнительные форумы и чаты.

- **Если ты не уверен, правдива ли найденная тобой информация, обратись к родителям. Попроси их посмотреть, что ты нашел и где.**
- Кроме того, важно, чтобы родители показали тебе, как правильно искать информацию. Какие нужно ввести слова, чтобы поисковая система начала верный поиск. Ведь, чем правильней ты сформулируешь критерии отбора информации, тем успешнее окажется путешествие к новым знаниям.
- Будь начеку! Внимательно следи за тем, что ты скачиваешь из Интернета. Потому что подчас за ссылкой может скрываться вирус. Думаю, ты понимаешь, насколько это опасно. Поэтому лучше в очередной раз спросить разрешения у родителей. Также не следует открывать файлы и ссылки, приходящие от незнакомых людей.
- Каждое путешествие когда-нибудь заканчивается, и как ни грустно, но твое путешествие закончилось. Информацию ты нашел. Зло победил. И что же дальше? Вся прелесть Интернета в том, что твои приключения не ограничены во времени. Ты можешь каждый день становиться героем! И каждое твое приключение будет заканчиваться победой!
- Только будь внимателен и осторожен и все получится!

По секрету всему свету



«У тебя есть «аська»?» - этот вопрос тебе, наверняка, приходилось не раз слышать от своих сверстников и друзей. А уж какое неподдельное возмущение следовало за ответом «нет»! Но всё это в прошлом. Сейчас уже редко встретишь человека среди твоего брата, который бы не улыбался часами в монитор, отправляя килограмм сообщений в минуту. И это не единственная функция знакомой тебе ICQ и других подобных программ.

- Программы мгновенного обмена сообщениями (мессенджеры, от англ. instantmessengers) так же, как и чаты, позволяют общаться в режиме реального времени. Разница лишь в том, что ты можешь выбрать человека, с которым хочешь переписываться, и внести его в список

своих контактов. В этом случае ты избежишь нежелательного и порой опасного общения с незнакомыми людьми.

- И что бы ни говорили твои родители, у «аськи» есть масса преимуществ. Во-первых, больше не надо бежать на почту и клеить марки на конверты. Теперь послание другу долетает за секунду в любую точку планеты. И заметь, даже без почтового голубя. Во-вторых, что обязательно нужно сообщить родителям, с помощью таких программ ты можешь узнавать домашнее задание и другую полезную информацию. Если у тебя много друзей в других городах и странах, то без мессенджера тем более никак не обойтись. Ты не только можешь обмениваться с ними различными файлами – например, посылать новые фотографии, но и разговаривать с ними посредством «видеозвонка». Не забудь только обзавестись наушниками, микрофоном и web-камерой.
- Программ-мессенджеров существует великое множество – ICQ, QIP, MailAgent, Miranda, &RQ, Skype. Скорее всего, ты знаешь, что ICQ появилась первой. Она и сейчас остается популярной. Наверняка, у многих твоих друзей, а может, и у тебя стоит именно эта программа.
- Изначально мессенджеры создавались с одной целью – передавать информацию. Но некоторые из них свободно можно использовать для развлечения. Например, установив MailAgent на своем компьютере, ты сможешь играть в онлайн-игры: шашки, шахматы и морской бой. Также, эта программа позволит тебе радовать своих друзей не только традиционными смайликами - «колобками», но и отправлять им забавные мульты (flash-ролики). Разбудить же задумавшегося собеседника можно специальным «будильником».
- Думаешь, с друзьями можно только переписываться?! Нет, с ними можно еще и перерисовываться! Программа ArtyTalk, а в народе просто «рисоваська» как раз для этого. И даже если ты не умеешь рисовать – не беда. Большое количество клипартов и шаблонов помогут тебе создать настоящий шедевр.
- Общение через программы-мессенджеры, несомненно, принесет тебе много пользы. Но не стоит забывать и о безопасности. Обязательно включи опцию «анти-спам». Тогда в твоём компьютере вряд ли появятся незваные гости – вирусы. Также следи за тем, кого ты добавляешь в свой список контактов. Ведь основное преимущество «аськи» и состоит в общении только с друзьями, а не со всеми подряд, как в чатах.
- И помни, что общения вживую никто не отменял!
- Бегом на улицу лепить снеговика!

Термины информационно-коммуникационных технологий



Основные понятия

- **Интернет** - Internet
Иногда называемый просто "Сеть" или "Инет", "Нет". Это глобальная сеть с миллионами подключенных к ней компьютеров.
- **Всемирная сеть** - (WorldWideWeb)
Собрание онлайн-документов, хранимых на серверах всего мира, подключенных к Интернету. Всемирная сеть не является синонимом Интернета.
- **URL-адрес**
Унифицированный указатель информационного ресурса, глобальный адрес документов и других ресурсов в Интернете.
- **Веб-страница** - Webpage
Документ в Интернете. Каждая веб-страница имеет свой неповторимый URL-адрес.
- **Имя домена** - Domainname
Название, идентифицирующее один или несколько IP-адресов.
Например:
gov - Правительственные учреждения
edu - Образовательные учреждения
org - Некоммерческие организации
com - Коммерческие организации
net - Сетевые организации
- **IP**
Сокращение InternetProtocol (интернет-протокол). Способ обмена, отправки и получения всех видов информации. Может использоваться для телефонных звонков, онлайн-игр и просмотра видео.
Интернет-протокол процесс формирования информации в пакеты и передачи их из одной точки в другую. Может работать быстрее и посылать больше информации, потому что разбивает большое количество информации на малые пакеты, которые быстрее отправляются, тем самым, делая передачу информации более дешевой.
- **Провайдер интернет-услуг** - ISP
Коммерческая или некоммерческая организация, предоставляющая пользователям доступ к Интернету и сопутствующие услуги.
- **Локальная сеть (LAN)**
Компьютерная сеть, охватывающая небольшую площадь, например, дом, офис или небольшую группу помещений.
- **База данных** - Database
Часто сокращается до БД. Информация, упорядоченная таким образом, что компьютерная программа может быстро выбрать из нее необходимую часть данных. База данных, в принципе, подобна электронной картотеке.
- **HTML**
Сокращение HyperTextMarkupLanguage (язык гипертекстовой разметки). Это язык разработки документов в Интернете.

- **Bluetooth**

Промышленная спецификация для беспроводных локальных сетей с персональными компьютерами. Технология Bluetooth (также называемая «Голубой зуб») обеспечивает беспроводное подключение и обмен информацией между такими устройствами как карманные компьютеры, мобильные телефоны, ноутбуки, персональные компьютеры, принтеры и цифровые фотокамеры посредством надежной, дешевой и распространенной во всех странах радиочастоты с малым радиусом действия.

- **ADSL** или Асимметричная DSL (цифровая абонентская линия) - вид DSL

Технология передачи данных, позволяющая осуществлять более быструю передачу данных по телефонным линиям с медными проводами, чем у обычного модема.

- **Основные понятия WWW**

- **Браузер** - Browser

Программа, используемая для просмотра веб-страниц. Наиболее популярные браузеры для персональных компьютеров MicrosoftInternetExplorer, MozillaFirefox, Opera, Netscape и AppleSafari.

- **Закладка** - Bookmark

Прямая ссылка на часто посещаемый сайт, сохраненная в вашем браузере для обеспечения более удобного нахождения этого сайта. Закладки помогают переходить на сайты, которые вы часто посещаете.

- **Новичок** - Newbie

Пояснение

Новичок, тот, кто плохо знаком с Интернетом или с компьютерами вообще.

Вход в компьютерную систему - Login

Подключение или получение доступа к удаленной компьютерной системе, сети, серверу или веб-странице. Для входа необходимо указать имя пользователя и пароль.

- **Пароль** - Password

Комбинация букв и других символов, которые необходимо указать для вхождения в компьютерную систему или программу. Как правило, никто не должен догадаться о выборе пароля. Также целесообразно менять свой пароль минимум каждые шесть месяцев.

- **Скачать / Загрузить** (на компьютер пользователя) - Download

Передача файла или файлов с одного компьютера на другой, например, с сервера на настольный компьютер. Скачивание противоположно загрузке на сервер.

- **Загрузка на сервер («аплоад»)** - Upload

Копирование файла с вашего компьютера на сервер или главную компьютерную систему. Скачивание (загрузка на персональный компьютер) процесс противоположный загрузке на сервер

Баг - Bug

Ошибка или дефект в программном или аппаратном обеспечении, в результате чего программа работает со сбоями.

Кукисы - Cookie

Слово образовано от английского cookie (дословно «пирожок») и означает небольшой объем информации о вас (точнее, о вашем компьютере). Это небольшой файл, который сервер автоматически посылает вашему компьютеру, когда вы просматриваете определенные веб-страницы.

- **Коммуникационные сервисы**

- **Чат - Chat**

Общение пользователей в реальном времени посредством компьютеров.

- **Блог - Blog**

Страница или сайт в Интернете, обеспечивающая публичный доступ к личному дневнику/записям какого-либо человека.

- **ЧаВО- FAQ**

Является сокращением словосочетания «Часто задаваемые вопросы и ответы» (Frequently Asked Questions). Обозначает список вопросов, которые часто задают по какой-то теме, и ответы на эти вопросы.

E-mail

или электронная почта электронная передача сообщений, текста и документов с одного компьютера на другой

Знак @ - (@ sign)

В англоязычных странах знак читают как «эт» (от английского слова at), в русском же называют «собака» или "собачка". Он является частью адреса электронной почты, отделяющей имя пользователя от названия домена (обе эти части являются обязательными для работы с электронной почтой).

Электронная книга - E-book

Электронный (или цифровой) вариант книги.

- **Сетевой этикет**

- **Сетевой этикет - Netiquette**

Кодекс поведения и неофициальные правила, которыми следует руководствоваться в Интернете.

Смайл (смайлик) - Smiley

Схематичное изображение человеческого лица, используется в текстовых сообщениях для передачи с сообщением своих эмоций.

Смайлы используются в текстовых сообщениях таким же образом, как и изменение голоса и выражение лица при личном общении или в телефонном разговоре.

- **КРИК В ФОРУМАХ - SHOUTING**

Если кто-то ПЕЧАТАЕТ ВСЕ ПРЕДЛОЖЕНИЕ ЗАГЛАВНЫМИ БУКВАМИ, говорят, что он КРИЧИТ. Сетевой этикет не приветствует публикацию сообщений ЗАГЛАВНЫМИ БУКВАМИ, особенно в электронной почте.

- **Гейминг - Gaming**

Означает занятие какой-то игрой с помощью видеоприставки, в Интернете или на компьютере.

- **Интернет-опасности**

- **Хакер - Hacker**

Сленговый термин для компьютерного фанатика, который любит изучать языки программирования и компьютерные системы, и часто считается экспертом в этой области. Часто путают с взломщиками эти увлеченные своим хобби люди являются квалифицированными программистами с репутацией людей, склонных к взлому систем безопасности.

- **Вирус - Virus**

Программа или код, загружаемый на ваш компьютер без вашего ведома и выполняемый вопреки вашей воле. Вирусы могут копировать сами себя

- **Фишинг - Phishing**

Один из видов кибермошенничества, спам рассылка электронных писем от имени известных компаний, а на самом деле, указанная в письме ссылка ведет на поддельный сайт мошенников. Все введенные логины и пароли получают мошенники.