**Использование интернета является безопасным, если выполняются три основных правила:**

1.Защитите свой компьютер

Регулярно обновляйте операционную систему.

Используйте антивирусную программу.

Применяйте брандмауэр.

Создавайте резервные копии важных файлов.

Будьте осторожны при загрузке содержимого.

2. Защитите себя в Интернете

С осторожностью разглашайте личную информацию.

Думайте о том, с кем разговариваете.

Помните, что в Интернете не вся информация надежна и не все

пользователи откровенны.

3. Соблюдайте правила

Закону необходимо подчиняться даже в Интернете.

При работе в Интернете не забывайте заботиться об остальных так же, как

о себе.

* ***Брандмауэр***

Программное обеспечение или устройство, предназначенное для контроля над обменом данными между сетями или сетью и отдельной компьютерной системой. Например, брандмауэр позволяет ограничивать трафик на основе предварительно заданных правил, которые разрешают обмен данными только между указанными адресами.

**Вирусы, черви и трояны**

Вирусы и черви представляют собой опасные программы, которые могут распространяться через электронную почту или веб-страницы. Вирусы могут повредить файлы или программное обеспечение, хранящиеся на компьютере.

Черви распространяются быстрее вирусов — напрямую с одного компьютера на другой. Например, червь электронной почты может осуществлять самостоятельную рассылку по адресам электронной почты из адресной книги пользователя. Интернет-червями осуществляется поиск компьютеров, которые подключены к Интернету и не содержат последние обновления системы безопасности.

«Троянские кони» (трояны) являются опасными программами, которые выглядят безопасными, например, играми, но после активации могут повредить файлы; при этом пользователь не будет об этом знать.

Хакеры и взломщики

Хакерами и взломщиками называют людей, которые взламывают защиту систем данных. Они могут вторгнуться на незащищенный компьютер через Интернет и воспользоваться им со злым умыслом, а также украсть или скопировать файлы и использовать их в противозаконной деятельности.

Лучшим способом защиты компьютера от вторжения является применение брандмауэра и регулярное обновление операционной системы.

Хакерами называют людей, которые знают о компьютерах и вычислительных системах больше, чем средний пользователь. Они имеют обширные знания о технологии, но они не используют эти знания для совершения преступления. Хакеры, как правило, не преследуют в своей деятельности корыстных целей, а желают углубиться в суть системы для собственного образования.

Взломщики также являются компьютерными специалистами высокого уровня, но, в отличие от хакеров, они используют свои знания для запрещенной деятельности: они вламываются в чужие компьютеры с корыстными намерениями и используют их в преступных целях. Наилучшей защитой от взлома компьютера является защита с помощью использования сервиса безопасности и противовирусной защиты (например, Live OneCare) и надлежащее поддержание операционной системы в порядке.

Спам в Интернете

Массовая рассылка нежелательных сообщений электронной почты известна как спам. Он приводит к перегрузке систем электронной почты и может заблокировать почтовые ящики. В качестве средства для рассылки спама его отправители иногда используют червей электронной почты.

**Пять правил относительно электронной почты:**

Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их, выбрав команду в меню сообщений.

Никогда не отвечайте на спам.

Применяйте фильтр спама поставщика услуг Интернета или программы работы с электронной почтой (при наличии подключения к Интернету).

Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.

Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их.

Дополнительные правила

Закрывайте сомнительные всплывающие окна

Всплывающие окна — это небольшие окна с содержимым, побуждающим к переходу по ссылке. При отображении такого окна самым безопасным способом его закрытия является нажатие значка X (обычно располагается в правом верхнем углу). Невозможно знать наверняка, какое действие последует после нажатия кнопки «Нет».

Остерегайтесь мошенничества

В Интернете легко скрыть свою личность. Рекомендуется проверять личность человека, с которым происходит общение (например, в дискуссионных группах). Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете. При запросе предоставления личной информации на веб-сайте всегда просматривайте разделы «Условия использования» или «Политика защиты конфиденциальной информации», чтобы убедиться в предоставлении оператором веб-сайта сведений о целях использования получаемой информации и ее передаче другим лицам.

Обсуждайте использование Интернета

Большая часть материалов, доступных в Интернете, является непригодной для несовершеннолетних. Обсудите с детьми, как правильно и безопасно использовать Интернет.

***Законы также применяются к Интернету***

Что разрешено и что запрещено в Интернете?

Интернет является общественным ресурсом. В Интернете необходимо следовать основным правилам так же, как правилам дорожного движения при вождении.

Законы также применяются к Интернету

Несмотря на то, что большая часть законов была создана до широкого распространения Интернета, закон также распространяется и на него. Все, что незаконно в обычной жизни, незаконно и в Интернете.

Интернет предоставляет беспрецедентные возможности свободного общения, но они также подразумевают ответственность. Например, владелец веб-сайта всегда несет ответственность за его содержимое и законность самого сайта и места его публикации.

**Авторское право**

Авторским правом защищается способ реализации идеи, но не сама идея. Разрешается копирование материала из Интернета для личного использования, но присвоение авторства этого материала запрещено. Например, при использовании материала в собственной презентации необходимо указать источник.

Передача и использование незаконных материалов (например, пиратские копии фильмов или музыкальных произведений, программное обеспечение с надорванными защитными кодами и т.д.) является противозаконным.

Копирование программного обеспечения или баз данных, для которых требуется лицензия, запрещено даже в целях личного использования.

Неразрешенное использование материала может привести к административному взысканию в судебном порядке, а также иметь прочие правовые последствия.

Дополнительная информация об авторском праве

Интернет является общественным ресурсом. В Интернете необходимо следовать основным правилам так же, как правилам дорожного движения при вождении.

***Дополнительная информация об авторском праве:***

http://www.author.ee

**Об информационной безопасности**

**Помните**

После публикации информации в Интернете ее больше невозможно будет контролировать и удалять каждую ее копию.

**Проверяйте**

Всегда удостоверяйтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.

**Думайте**

Благоразумно ли размещать личную информацию на собственном веб-сайте, если невозможно быть уверенным в целях ее использования?

**Обращайте внимание**

Имена учеников, их фотографии и другая личная информация из школьного журнала может публиковаться на веб-сайте школы только с согласия учеников и их родителей.

**Глоссарий**

Антивирусная программа

Программа, предназначенная для предотвращения доступа к персональному компьютеру для вредоносных программ — она обнаруживает инфицированные файлы и удаляет их.

Сетевой дневник

Общественный интерактивный дневник.

Чат

Дискуссионный форум, работающий в режиме реального времени. В нем пользователи поочередно пишут сообщения, сразу отображающиеся на экране. Сообщения заменяются по мере написания новых, поэтому отображаются только самые последние сообщения.

Защита данных

Набор правил, которые обеспечивают сохранение конфиденциальности информации. Безопасность данных распространяется на конфиденциальную информацию, например, личную информацию, и поддерживается политикой информационной безопасности или заявлением о конфиденциальной информации.

Дискуссионный форум

Место обсуждения в Интернете, часто посвященное определенной теме. Здесь люди могут оставлять сообщения в интерактивном режиме, используя форматы, указанные поставщиком данной услуги. Для некоторых дискуссионных форумов требуется регистрация.

В некоторых форумах имеется архив, который можно использовать для поиска определенной темы. Некоторые форумы контролируются администратором, который имеет право удалять и редактировать любые размещенные сообщения или запрещать доступ для пользователей, которые оскорбляют своих собеседников.

Загрузка

Сохранение файлов из Интернета на собственном компьютере.

Брандмауэр

Программное обеспечение или устройство, предназначенное для контроля над обменом данными между сетями или сетью и отдельной компьютерной системой. Например, брандмауэр позволяет ограничивать трафик на основе предварительно заданных правил, которые разрешают обмен данными только между указанными адресами.

Хакер, взломщик

Человек, взламывающий информационные сети или системы организации, либо использующий их без разрешения. Примечание: термин «хакер» имеет два значения — он может также означать опытного компьютерного пользователя. (см. Хакеры и взломщики)

Опасные программы: вирусы, черви и трояны

Программа или часть программы, которая предназначена для распространения нежелательных событий в компьютерной или информационной системе, например, вирусов, червей или троянов.

Информационная безопасность

Политика, реализуемая для обеспечения контроля над рисками информационной безопасности.

Спам

Нежелательная электронная почта, которая, как правило, рассылается в целях прямого почтового маркетинга. Спам почти всегда единовременно рассылается большому кругу получателей.

Почта; электронная почта; сообщение электронной почты

Электронная передача текста или изображений между адресами компьютерного приложения.

Операционная система

Главная программа, которая работает «между» компьютером и прикладным программным обеспечением. С помощью операционной системы компьютер управляет установленным программным обеспечением, а также контролирует и использует его. К распространенным операционным системам относятся Microsoft® Windows®, Apple® Mac OS и Linux®.

Всплывающее окно

Новое окно, которое открывается поверх активного окна обозревателя Интернета. Как правило, такое окно не содержит собственного веб-адреса, однако в некоторых случаях может его содержать. Во всплывающих окнах, которые открываются без запроса пользователя, обычно содержится реклам

Сервер

Программа, которая распределяет файлы по компьютерам в сети на основе предварительно заданных правил. Например, в Интернете пользователи получают сообщения электронной почты от сервера электронной почты сети. Сервером часто называют компьютер, на котором установлена серверная программа.

Вирус

Вредоносная программа, которая распространяется, копируя себя в другие программы. Вирус может распространяться через файлы, сообщения электронной почты или веб-страницы. Компьютер может заразиться вирусом во время работы пользователя в Интернете или при открытии вложений электронной почты. Вирусы могут снизить работоспособность компьютера или системы.

Червь

Вредоносная программа, которая может независимо распространяться через информационные сети. Черви могут распространяться через электронную почту или бреши в системе защиты информации в обозревателе Интернета или операционной системе. Даже если пользователем не выполняются никакие действия, черви могут получить доступ к незащищенным компьютерам при их подключении к Интернету. Черви затрудняют работу системы или компьютера и могут распространять другие вредоносные программы.

**Основные правила для школьников младших классов**

Вы должны это знать:

Всегда спрашивайте родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

Прежде чем начать дружить с кем-то в Интернете, спросите у родителей как безопасно общаться.

Никогда не рассказывайте о себе незнакомым людям. Где вы живете, в какой школе учитесь, номер телефона должны знать только ваши друзья и семья.

Не отправляйте фотографии людям, которых вы не знаете. Не надо чтобы незнакомые люди видели фотографии Вас, Ваших друзей или Вашей семьи.

Не встречайтесь без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

Общаясь в Интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.

Если вас кто-то расстроил или обидел, обязательно расскажите родителям.

**Основные правила для школьников средних классов**

Вы должны это знать:

При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.

Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.

Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылась вам спам.

Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.

Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом

Если вас кто-то расстроил или обидел, расскажите все взрослому.

**Основные правила для родителей**

Чтобы помочь своим детям, Вы должны это знать:

* Будьте в курсе того, чем занимаются ваши дети в Интернете. Попросите их научить Вас пользоваться различными приложениями, которыми вы не пользовались ранее.
* Помогите своим детям понять, что они не должны предоставлять никому информацию о себе в Интернете — номер мобильно телефона, домашний адрес, название/номер школы, а также показывать фотографии свои и семьи. Ведь любой человек в Интернете может это увидеть.
* Если Ваш ребенок получает спам (нежелательную электронную почту), напомните ему, чтобы он не верил написанному в письмах и ни в коем случае не отвечал на них.
* Объясните детям, что нельзя открывайте файлы, присланные от неизвестных Вам людей. Эти файлы могут содержать вирусы или фото/видео с «агрессивным» содержанием.
* Помогите ребенку понять, что некоторые люди в Интернете могут говорить не правду и быть не теми, за кого себя выдают. Дети никогда не должны встречаться с сетевыми друзьями в реальной жизни самостоятельно без взрослых.

* Постоянно общайтесь со своими детьми. Никогда не поздно рассказать ребенку, как правильно поступать и реагировать на действия других людей в Интернете.
* Научите своих детей как реагировать, в случае, если их кто-то обидел или они получили/натолкнулись на агрессивный контент в Интернете, так же расскажите куда в подобном случае они могут обратится.
* Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации