KASPERSKY lab

Введение в основы цифровой грамотности и гигиены для учащихся младших классов

Материал для учителя

KASPERSKY lab

Введение в основы цифровой грамотности и гигиены для учащихся младших классов

Интернет – это технология, которая опутывает целый мир. Не осталось ни одного уголка, где бы нельзя было выйти в интернет. Благодаря интернету мы можем обмениваться самой разной информацией с любым человеком.

Разные технологии, использующие интернет, сейчас развиваются очень быстро. К сети сегодня подключают даже холодильники, чайники, автомобили и целые дома, а не только то, что привычно ассоциировать с интернетом: компьютеры и смартфоны.

Сколько таких вещей пока сосчитать трудно: данные разных аналитиков сильно различаются, но все они сходятся на том, что таких устройств в мире не менее 5 миллиардов.

Вещи подключаются к интернету с разными целями:

- Можно получать от хозяев указания по интернету, например, согреть еду к их приходу.
- Можно получать информацию из интернета, например, что впереди на дороге пробка.
- Можно передавать информацию через интернет хозяевам, например, изображение с камеры безопасности можно посмотреть, находясь вдали от дома.

Если говорить о безопасности подключенных вещей, то на сегодняшний день это все еще является проблемой. Большинство производителей не являются компаниями, специализирующимися на безопасности, и не всегда вспоминают о том, что следует нанимать соответствующих сотрудников. В итоге умные вещи часто бывают не вполне безопасны с точки зрения хранения ваших данных (например, тех же видеозаписей с камер видеонаблюдения или введенных в их память персональных данных), а также получения команд из интернета.

Внимание к безопасности в отношении подключенных предметов особенно важно для подрастающего поколения, ведь в их жизни такие устройства займут еще больше места и, вероятно, со временем будет легче найти подключаемый предмет, чем неподключаемый. Надеемся, правда, со временем проблем с безопасностью таких вещей станет меньше, но таких гарантий нам пока, к сожалению, никто не дает.

Сами люди с помощью интернета делают огромное количество разных вещей: общаются с друзьями, развлекаются, учатся, совершают покупки, оплачивают счета и многое другое.

Один из способов использования возможностей сети интернет – «хождение» по разным сайтам, на которые пользователь попадает с помощью специальных программ – браузеров.

Браузер не только позволяет переходить на разные сайты, но и умеет сохранять некоторую информацию для удобства использования, например:

- пароли, которые вводит пользователь;
- самые часто посещаемые сайты;
- последние сайты, на которых ты бывал.

С точки зрения удобства может казаться замечательным, что браузер хранит логины и пароли, а также то, что поисковики подсказывают интересные вам запросы, а контекстная реклама всегда в курсе ваших интересов.

С точки зрения безопасности, тем не менее, все не так радужно, ведь пароли, которые вы сохраняете в браузере, могут «утечь», особенно если вы не используете антивирус.

В интернете отправной точкой для любого поиска являются п**оисковики, или поисковые машины** – это страницы, которые находят все, что запрашивает пользователь. Ими можно пользоваться, чтобы прямо сразу, не переходя на другие страницы, посмотреть найденные фильмы и мультфильмы или послушать музыку.

Второй способ повседневного использования интернета – это программы и приложения, которые для нормальной работы должны выходить в интернет.

Интернет является огромным хранилищем самых разных данных. Он поможет сделать уроки, с его помощью можно смотреть мультфильмы и играть в игры, слушать музыку и читать книги.

Большую часть этой информации можно сохранить к себе на компьютер или другое устройство (скачать), чтобы иметь к ней доступ офлайн.

Можно также смотреть фильмы, читать или слушать музыку онлайн, не скачивая. Вся информация, которую мы находим в интернете, называется одним словом – контент.

Существует множество сайтов и специальных приложений, дающих доступ к тому или иному **контенту**: библиотеки, энциклопедии, видеосервисы, музыкальные сервисы, мультимедийные магазины, торрент-трекеры, файловые хранилища, поисковики.

Некоторые из этих ресурсов дают доступ только к одному виду информации, например, к книгам. В других собраны сразу все или, по крайней мере, несколько разных видов **контента**. Назначение некоторых ресурсов понятно из названия, другие же могут озадачить.

Если не соблюдать при использовании интернета осторожность, можно «поймать» компьютерный вирус, или, вернее, вредоносную программу.

Вредоносные программы (еще их называют вирусы) – это программы и приложения, которые используют преступники в своих целях, чтобы вредить пользователю.

Вирусы и прочие вредоносные программы сегодня существуют не только на компьютерах, но и на планшетах и смартфонах, и приносят в этом случае не меньше вреда.

Что делают вредоносные программы?

- Воруют пароли от популярных сервисов и страниц, где можно что-либо оплачивать.
- Воруют данные карточек и пароли от сервисов банков.
- Шифруют (делают недоступными для пользователя) данные на его компьютере, чтобы требовать деньги за расшифровку.
- Рассылают сообщения, в том числе содержащие вредоносный код, с использованием страниц, к которым нашли пароли на компьютере.
- Включают веб-камеру, чтобы подсмотреть и подслушать, что происходит дома у жертвы.
- Могут сломать компьютер (впрочем, это бывает в последнее время редко, злоумышленникам гораздо интереснее создавать вредоносный код, который принесет им наживу, чем такой, который просто навредит пользователю).

«Подцепить» вредоносную программу можно, если скачивать что-либо из ненадежных источников. К ненадежным источникам любого контента относятся торрент-трекеры, файлообменники и другие нелицензионные ресурсы.

Торрент-трекер – это система, внутри которой пользователи могут передавать абсолютно любой контент друг другу совершенно бесплатно. Любой файл, который скачивается с торрент-трекера приходит прямо с компьютеров других пользователей, которые уже скачали его до вас.

Файловые хранилища – это такие специальные места, где пользователи хранят свои файлы прямо в интернете, и любой, кому они разрешат, может получить доступ к этому контенту и сохранить его себе на компьютер.

Кроме того, вредоносные программы часто распространяются в спаме – массовых рассылках по электронной почте или соцсетям, которые присылаются без разрешения пользователя.

Самое опасное, что вирус может поджидать вас на любой, даже самой хорошей странице в интернете.

Для безопасности устройств важно помнить, что любые мобильные приложения должны устанавливаться только из специальных магазинов приложений. Это касается не только самих программ, но и содержимого для них, такого как книги, музыка или какие-то покупки внутри игр.

Программы для компьютера должны скачиваться только с официальных страниц разработчика

Даже если вести себя в интернете максимально осторожно и соблюдать все меры осторожности, этого далеко не всегда бывает достаточно. Вредоносный код может попасть на ваш компьютер с популярного веб-сайта или в письме от знакомого, переписку с которым вы действительно ведете.

Чтобы избежать таких непредсказуемых ситуаций, нужен антивирус. Он охраняет ваш компьютер от заражения всегда.

Если вы попытаетесь перейти на зараженный сайт, антивирус заблокирует его; если вредоносная программа попытается пробраться на ваше устройство, антивирус не пропустит ее; если же вы сами по невнимательности установили вредоносную программу и теперь она пытается действовать – антивирус остановит ее и удалит.

Не используйте слишком простой пароль. Если пароль состоит из простого слова, злоумышленник может его легко подобрать. То же касается пароля, состоящего из вашего имени или, например, имени и даты рождения. Не подходят для пароля любые слова, связанные с вашей жизнью, которые легко найти в интернете: клички домашних животных, прозвище лучшего друга, фамилия директора школы. Все эти пароли легко подбираются, даже если вы добавите в начале и в конце цифры – это слишком популярный метод, злоумышленники уже умеют справляться и с ним.

Пароль должен состоять из 8, а лучше из 12 знаков, содержать буквы, как большие, так и маленькие, цифры и специальные символы. Самый идеальный вариант – выбрать фразу, которую вы легко запомните, написать ее латиницей, разбив слова специальными символами, и заменить 2-3 буквы на подходящие цифры.

При этом пароль должен быть таким, чтобы вы его запомнили.

[Плохие пароли: 1 и 5, поскольку содержат личные данные, 3, поскольку слишком легко подбирается, 2, поскольку является случайным набором букв, который сложно запомнить. Хорошие пароли: 4 (по инструкции выше), 6 – содержит более 12 символов, латинские буквы разного регистра, цифры и специальные знаки – и 7 – на самом деле это слово «сингулярность», написанное на латинской раскладке, каждая вторая буква большая, после каждой третьей буквы последовательно вставлены цифра 4, 3, 4 и !]

Информационные технологии облегчают нашу жизнь, делают ее разнообразнее и интереснее, но при их использовании, как и в любых других ситуациях, нужно соблюдать определенные правила, чтобы от такого полезного изобретения не было вреда. Вы наверняка знаете, что проводить много времени с устройством вредно для зрения и осанки.

Так сколько же времени безопасно проводить с устройством? Самый простой ответ на этот вопрос: столько, чтобы это не мешало другим активностям. Например, если тебе необходимо 10 часов в сутки на сон, 6 часов на посещение школы (с дорогой), 1,5 часа на завтрак, обед и ужин, 1-2 часа на домашние задания, 2 часа на посещение дополнительных занятий и еще 1-2 часа на прогулку, домашние дела и общение с родителями, то получается, что на сидение в интернете или видеоигры остается не более 1-2 часов в день.

KASPERSKY lab

kids.kaspersky.ru