Занятие: **«Киберугрозы современности: главные правила их распознавания и предотвращения»**

Форма занятия: семинар

Цель: расширение знаний о киберугрозах, формирование навыков их распознавания и оценки рисков.

Возраст обучающихся: 6-9 класс.

План занятия:

1. Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете. Составление листовок «Правила защиты от киберугроз» (20 мин.)

2. Практикум «Опасность 419» (20 мин.)

3. Подведение итогов занятия. (5 мин.)

Ход занятия.

Занятие начинается показом социального видеоролика «Безопасный интернет - детям!». После просмотра ролика учитель объявляет тему занятия и предлагает ученикам самим сформулировать цель занятия.

 Доклад «Киберугрозы и информационная безопасность», сайт http://www.kaspersky.ru/downloads/pdf/kaspersky\_global\_it\_security\_risks\_survey.pdf )

1. Обсуждение правил предотвращения киберугроз, которые встречаются при работе в Интернете. Продолжительность 20 минут.

У каждого ученика на столе лежит чистый лист бумаги – заготовка листовки по безопасности в Интернете. Перед тем, как начать работать учитель объясняет, что по ходу обсуждения каждый ученик должен заполнять листовку правилами, которые ему кажутся необходимыми и важными. После того, завершения обсуждения, отдельные ученики зачитывают свои листовки, остальные могут добавлять правила. Листовки собираются после урока для того, чтобы их раздать ученикам других классов.

Учитель начинает обсуждение с вопроса к аудитории: «Что вы знаете об угрозах, которые исходят из Интернета?» Просит учеников перечислить опасности, которые могут угрожать человеку, его персональному компьютеру, мобильным устройствам. На доске фиксируются ответы учеников.

После короткого обсуждения учитель приводит данные «Лаборатории Касперского» За последний год 91% компаний, представители которых приняли участие в опросе, сталкивались с угрозами информационной безопасности. В России этот показатель еще выше – 96%. Более того, ситуация становится только хуже: почти половина участников исследования утверждает, что количество кибератак за этот период увеличилось. Перечисляя киберугрозы, которые представляются им самыми значительными, большинство участников исследования во всем мире ставят на первое место вирусы, шпионское ПО и другие вредоносные программы (61%). Спам назвали источником угрозы 56% респондентов. Третье место (36%) заняли фишинговые атаки, за ними идут сбои, вызванные проникновением в корпоративную сеть (24%), и DDoS-атаки (19%)3.

Таким образом, можно выделить 3 группы серьезных киберугроз:

1. Шпионское ПО и др. вредоносные программы,

2. Спамы,

3. Фишинговые атаки.

Обсуждение основных правил защиты от главных киберугроз. Все ответы детей записываются на доске.

При обсуждении внимание учеников обращается на то, откуда могут исходить опасность. На первом месте в этом списке стоят социальные сети. Хотя в последнее время стали распространенными атаки на компьютер через мобильные устройства памяти (флешки).

*«Сегодня большинство вредоносных программ создаются либо для того, чтобы рассылать спам, либо для того, чтобы красть у пользователя важные данные.*

*Если данные действительно важные и дорогостоящие, то для их похищения злоумышленники специально разрабатывают троян, который гарантированно будет работать на компьютерах в той организации, откуда нужно украсть данные. Осуществить внедрение такого вредоносного ПО обычно гораздо проще не через интернет, а с помощью записанных на флэшках «троянов». Флэшки могут подбрасываться как в здание, где располагается организация, так и размещаться, скажем, на парковке рядом с ним, где их с большой долей вероятности наверняка найдёт именно сотрудник нужной организации. Поэтому если вы нашли на улице или в здании флэшку, не торопитесь радостно вставлять её в свой компьютер – лучше сначала отдайте системному администратору, который просканирует её и при необходимости обезвредит.*

*Бывают и более банальные, но не менее эффективные способы заразить компьютер недостаточно осторожного пользователя. Например, от знакомого по Skype Вам может прийти сообщение в духе «Посмотри, на этой фотографии он так похож на нашего друга (одноклассника)!», ну и, конечно, ссылка на саму эту фотографию. При переходе по ссылке фотография почему-то не открывается в браузере, а сохраняется на жесткий диск, но мало кто на это обращает внимание. Хотя они-то как раз и должны насторожить! В общем, когда «фото» не открывается, пользователь «входит» в папку с ним, и видит, что это не просто abcd.jpg, а abcd.jpg.scr, то есть, исполняемый файл, а его компьютер уже заражен вирусом».*

После обсуждения листовок на доске должен быть записаны основные правила защиты от киберугроз.