Внеурочное занятие для обучающихся 2-6 классов по теме:

ВРЕДОНОСНЫЕ ПРОГРАММЫ

Цель занятия:

Знакомство обучающихся с различными видами компьютерных вирусов, способами их распространения, профилактикой и методами борьбы с ними.

Задачи занятия:

- Определить, что такое вредоносные программы и как они работают. Ученики узнают, что такое вирусы, трояны и другие виды вредоносного ПО.
- Научиться распознавать потенциальные угрозы в интернете. Дети получат знания о том, как вредоносные программы могут попасть на компьютер или мобильное устройство.
- Изучить способы защиты от вредоносных программ. Обучение базовым методам защиты, таким как использование антивирусного программного обеспечения и обновление операционной системы.
- Развить ответственное отношение к использованию интернета. Подчеркнуть важность соблюдения правил безопасного поведения онлайн.

Формирующиеся ценности:

Осведомлённость Развитие понимания угроз в интернете и способов их предотвращения.

Ответственность Воспитание ответственного отношения к использованию технологий и защите личной информации.

Бдительность Поощрение активного и внимательного отношения к собственной безопасности в интернете.

Основные смыслы:

Что такое вредоносные программы: вредоносные программы — это программы, созданные чтобы нанести вред, украсть информацию или нарушить нормальную работу устройств.

Как вредоносные программы попадают на устройства: обсуждение методов распространения вредоносного ПО, включая заражённые вложения в электронной почте, загрузки из ненадёжных источников и фишинговые атаки.

Методы защиты: изучение способов защиты устройств, таких как регулярные обновления ПО, использование антивирусов и обучение тому, как избегать подозрительных ссылок и загрузок.

Продолжительность занятия:
35 (для 2-3 кл.) - 45 минут

Рекомендуемая форма проведения занятия:
беседа с элементами групповой работы.

Структура занятия

Часть 1. Введение в тему «Вредоносные программы»

Учитель: Сегодня мы начнём обсуждение очень важной темы, которая касается всех, кто использует компьютеры и интернет. Это тема вредоносных программ. Вредоносные программы — это специальные виды программ, которые могут причинить вред вашим устройствам или украсть вашу личную информацию.

Вредоносные программы

Учитель: Вредоносные программы могут быть разными. Некоторые из них называются вирусами, другие — шпионскими программами или троянами. Они могут делать разные вещи: от кражи паролей до удаления файлов.

Игра «Узнай вредоносную программу»

Учитель: Я буду описывать различные действия, а вам нужно определить, делает ли это вредоносная программа.

Ученики: отвечают на вопросы, различая типы вредоносных программ, такие как рекламное ПО, вирусы, трояны.

Обсуждение способов заражения

Учитель: Теперь, когда мы знаем, что такое вредоносные программы, давайте поговорим о том, как они могут попасть на наши компьютеры. Один из способов — это когда мы скачиваем что-то из интернета. Важно всегда быть уверенным в том, что вы скачиваете и откуда.

Ученики: обсуждают примеры, как вредоносные программы могут попасть на устройства через небезопасные загрузки, электронную почту и другие пути.

Эта часть занятия знакомит обучающихся с базовыми концепциями вредоносных программ и их потенциальным воздействием на цифровую жизнь, создавая основу для дальнейшего изучения методов защиты.

Часть 2. Как защититься от вредоносных программ

Учитель: Мы узнали, что такое вредоносные программы и как они могут попасть на наши устройства. Сегодня мы сосредоточимся на том, как мы можем защитить себя от этих угроз. Есть много способов, как мы можем это делать, даже будучи детьми!

Обучение использованию антивирусного программного обеспечения

Учитель: Первый и самый важный способ защиты — использование антивирусного ПО. Антивирусы помогают обнаруживать и удалять вредоносные программы с вашего компьютера.
Можете ли вы привести пример антивирусной программы?

Ученики: обсуждают различные антивирусные программы, которые они знают или слышали от родителей.

Роль обновлений программного обеспечения

Учитель: Ещё один важный аспект защиты — это обновления программного обеспечения. Когда компании обнаруживают ошибки или уязвимости в своих программах, они выпускают обновления, чтобы исправить их. Почему, по вашему мнению, важно регулярно обновлять программное обеспечение?

Ученики: обсуждают, как обновления помогают защитить их устройства от новых угроз и улучшить безопасность.

Изучение безопасного поведения в интернете

Учитель: Кроме использования антивирусов и обновлений, важно также знать, как безопасно вести себя в интернете. Например, не следует нажимать на подозрительные ссылки или скачивать файлы из ненадёжных источников.

Игра «Безопасный клик»

Учитель: Я покажу вам несколько примеров ссылок или сообщений, которые вы можете получить по электронной почте или в социальных сетях. Вы должны решить, безопасно ли нажимать на эту ссылку или лучше избегать её.

Ученики: участвуют в интерактивной игре, в ходе которой решают, какие действия безопасны, а какие могут привести к заражению их устройства вредоносным ПО.

Учитель: Мы многое узнали о том, как защитить свои устройства и данные. Помните, что безопасность в интернете начинается с вас и ваших действий. Главное — быть внимательным и осторожным. Поделитесь своими знаниями с родителями и расскажите им о том, как они могут защитить свои устройства.

Эта часть занятия акцентирует внимание на практических действиях, которые обучающиеся могут предпринять для защиты себя в цифровом мире, а также осознавать свою роль в поддержании личной и семейной кибербезопасности.

Часть 3. Практические упражнения и ролевые игры

Учитель: Мы уже узнали, как вредоносные программы могут повредить наши устройства и как мы можем защититься, используя антивирусное программное обеспечение и обновления. Сейчас мы сосредоточимся на практическом применении этих знаний.

Упражнение «Мой безопасный компьютер»

Учитель: Давайте начнем с упражнения «Мой безопасный компьютер». Я раздам вам листы бумаги, на которых нарисован компьютер. Ваша задача — добавить на рисунок элементы, которые помогут защитить компьютер от вредоносных программ. Например, вы можете нарисовать антивирусную программу, символ обновления или даже «щит» безопасности.

Ученики: рисуют и описывают, как каждый элемент помогает защитить компьютер.

Ролевая игра «Охотники за вирусами»

Учитель: Я буду описывать различные ситуации, а вы должны будете решить, как лучше всего защитить ваш компьютер в каждом конкретном случае.

Ученики: участвуют в ролевой игре, выбирая действия для защиты компьютера от вирусов, такие как не открывать подозрительные файлы, не посещать сомнительные сайты и не скачивать программы с непроверенных источников.

Обсуждение и обратная связь

Учитель: Отличная работа сегодня, ребята! Давайте поделимся нашими проектами и обсудим, что нового вы узнали и что считаете самым важным в защите от вредоносных программ.

Ученики: демонстрируют свои работы и обсуждают узнанное, делятся советами о том, как избегать угроз и что делать в случае заражения.

Эта часть занятия позволяет обучающимся применять теоретические знания на практике, развивает их креативное и критическое мышление и укрепляет понимание необходимости защиты личной информации и устройств в цифровом мире.

Часть 4: Заключительная

Учитель: Мы многое узнали сегодня о вредоносных программах и о том, как мы можем защитить себя и наши устройства. Давайте закрепим наши знания и обсудим, что каждый из вас может делать, чтобы оставаться в безопасности.

Обсуждение ключевых выводов

Учитель: Давайте вспомним основные моменты, которые мы сегодня обсуждали. Какие типы вредоносных программ мы изучили? И какие инструменты защиты вы теперь знаете?

Ученики: перечисляют виды вредоносных программ, такие как вирусы, трояны, и способы защиты, включая использование антивирусного программного обеспечения, обновления программ и осторожное поведение в интернете.

Викторина по безопасности

Учитель: Чтобы убедиться, что вы хорошо усвоили материал, давайте проведем небольшую викторину **(Приложение 1)**.
Я буду задавать вопросы, а вы будете отвечать. Готовы?

Ученики: участвуют в викторине, отвечая на вопросы по теме урока, что помогает им лучше запомнить и понять изученный материал.

Составление плана действий

Учитель: Теперь, когда вы знаете, как защитить свои устройства, давайте каждый из вас подумает и скажет, какое конкретное действие он собирается предпринять дома для улучшения собственной кибербезопасности.

Ученики: делятся своими планами о том, как они будут применять усвоенные знания дома, например, попросить родителей установить антивирусное программное обеспечение или регулярно обновлять свои устройства.

Учитель: Отличная работа сегодня, ребята! Помните, что соблюдать осторожность в интернете — это очень важно. Всегда используйте то, что вы узнали сегодня, чтобы защитить себя и свои устройства. Расскажите членам своей семьи и своим друзьям, что они смогут предпринять, чтобы оставаться в безопасности."

Эта часть занятия помогает обучающимся закрепить полученные знания и применить их в реальной жизни, почувствовать себя более компетентными и уверенными в вопросах кибербезопасности.

Постразговор: Что делать после занятия

Обсуждение с семьей

Цель: закрепление полученных знаний через семейное обсуждение, проверка настройки безопасности на домашних устройствах.

Задание: поделиться с родителями полученными знаниями о вредоносных программах, рассказать им о различных типах вредоносного ПО и способах защиты.

Ревизия безопасности устройств

Цель: развитие практических навыков управления безопасностью устройств в целях обеспечения их защиты от вредоносных программ.

Задание: проверить настройки безопасности и антивирусные программы на всех домашних устройствах. Убедиться, что программное обеспечение обновлено до последних версий.

Создание информационного плаката

Цель: развитие навыков визуальной коммуникации.

Задание: нарисовать плакат, который мог бы помочь вашим друзьям узнать о вредоносных программах и о том, как их можно предотвратить. Включить в плакат советы по безопасности, которые вы изучили.

Игра «Безопасный интернет»

Цель: закрепление знаний о безопасности в интернете через игровую форму, развитие навыков распознавания потенциальных угроз в различных интернет-ситуациях.

Задание: совместно с родителями (друзьями) разработать игру, в которой участникам необходимо определять безопасные и небезопасные действия в интернете. При разработке игры можно использовать примеры о том, как избежать вредоносных программ, которые рассматривались на занятии.

Кармазин Виталий Юрьевич.
Кандидат технических наук, доцент
кафедры цифровой экономики
ФГБОУ ВО Вавиловский университет

Приложение 1

Викторина «Вредоносные программы»

- Что такое вредоносная программа?
- Как можно заразиться вирусом?
- Какие действия может выполнять вирус?
- Какой антивирусный продукт защищает ваш компьютер?
- Что нужно делать, чтобы не заразить компьютер вирусом?
- Можно ли удалить вирус с компьютера самостоятельно?
- Что делать, если вы подозреваете, что ваш компьютер заражён вирусом?
- Может ли вирус повредить данные на вашем компьютере?
- Что такое троянская программа?
- Чем отличается вирус от червя?

Кармазин Виталий Юрьевич.
Кандидат технических наук, доцент
кафедры цифровой экономики
ФГБОУ ВО Вавиловский университет