Внеурочное занятие для обучающихся 7-11 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:
45 минут

Рекомендуемая форма проведения занятия:
беседа с элементами групповой работы.

Структура занятия

Часть 1. Введение в тему «Вредоносные программы»

Учитель: Сегодня мы обсудим вредоносные программы. Это важная и актуальная тема, так как вредоносное ПО может серьезно угрожать как личной, так и общественной безопасности.

Вредоносные программы

Учитель: Вредоносное программное обеспечение или малварь (англ. Malware) включает различные типы программ, созданных с целью нанести вред пользователю, украсть данные или получить несанкционированный доступ к системам. Существует несколько основных типов вредоносных программ, включая вирусы, трояны, шпионское ПО и рансомвар (англ. Ransomware).

Ученики: обсуждают различия между различными типами вредоносных программ и примеры угроз, которые они представляют.

Исследование методов распространения

Учитель: Вредоносные программы могут распространяться различными способами, включая фишинговые атаки, заражённые вложения в электронной почте и незащищённые сетевые подключения. Подумайте, какие меры предосторожности могут помочь защититься от таких атак?

Ученики: предлагают идеи по предотвращению заражения, такие как не открывать подозрительные письма, использовать надежное антивирусное программное обеспечение и регулярно обновлять свои системы.

Разбор реальных кейсов

Учитель: Давайте рассмотрим несколько реальных примеров атак вредоносных программ, которые произошли в последние годы. Это поможет нам лучше понять, как вредоносное ПО может влиять на индивидуальных пользователей и организации.

Ученики: анализируют кейсы **(Приложение 1)**, обсуждая, какие ошибки были допущены и как можно было предотвратить атаки.

Учитель: Вредоносные программы представляют серьёзную угрозу в современном мире. Наша цель — научиться распознавать и защищаться от таких угроз.

Эта часть занятия устанавливает основу для глубокого понимания темы вредоносных программ и настраивает обучающихся к более активной работе по обеспечению своей кибербезопасности.

Часть 2. Методы защиты от вредоносных программ

Учитель: Мы обсудили, что такое вредоносные программы и как они могут попасть на ваши устройства. Сейчас сосредоточимся на том, как вы можете защитить себя от этих угроз. Давайте начнем с антивирусного программного обеспечения.

Использование антивирусного программного обеспечения

Учитель: Антивирусное программное обеспечение — это один из самых важных инструментов в борьбе против вредоносных программ. Как вы думаете, как работает антивирус?

Ученики: обсуждают, как антивирусное ПО может обнаруживать, блокировать и удалять вредоносные программы, используя базы данных известных вирусов и поведенческие методы для обнаружения новых угроз.

Обновление программного обеспечения и операционных систем

Учитель: Ещё один критически важный аспект защиты — это регулярное обновление вашего программного обеспечения и операционных систем. Почему это так важно?

Ученики: обсуждают, как обновления помогают исправлять уязвимости, которые могут быть использованы вредоносными программами для заражения устройств.

Практическое задание: настройка антивируса и проверка обновлений

Учитель: Теперь давайте попрактикуемся. Я хочу, чтобы каждый из вас проверил, установлены ли последние обновления на вашем устройстве и если нет, то обновил его. Затем мы проверим, как настроен ваш антивирус.

Ученики: выполняют задание, проверяя и обновляя свои устройства, а также проверяют и настраивают антивирусные программы под руководством учителя.

Изучение безопасного поведения в интернете

Учитель: Помимо использования технических инструментов, безопасное поведение в интернете также крайне важно. Давайте обсудим, какие поведенческие привычки помогут вам избежать вредоносных программ.

Ученики: разрабатывают список правил для безопасного поведения в интернете, в том числе не открывать подозрительные электронные письма, избегать сомнительных загрузок и не использовать публичные Wi-Fi сети для важных транзакций.

Учитель: Сейчас мы многое узнали о защите от вредоносных программ. Важно помнить, что кибербезопасность — это не только о защите технических устройств, но и о разумном поведении в интернете. Держите ваше программное обеспечение обновленным, используйте надежное антивирусное ПО и будьте внимательны в интернете.

Эта часть занятия помогает ученикам применять теоретические знания на практике и развивать навыки, необходимые для поддержания безопасности в цифровом мире.

Часть 3. Заключительная

Учитель: Мы подошли к завершению нашего занятия о вредоносных программах. Сегодня мы поговорили о различных типах вредоносного ПО, о том, как они распространяются и какие меры защиты можно применять. Теперь давайте подведём итоги и обсудим, что вы можете сделать ещё, чтобы оставаться в безопасности."

Обсуждение ключевых выводов

Учитель: Какие основные типы вредоносных программ мы обсудили? Какие методы защиты вы считаете наиболее эффективными? Свой ответ аргументируйте.

Ученики: делятся своими ответами, обсуждая различные виды вредоносного ПО и их методы борьбы, такие как антивирусное программное обеспечение, регулярные обновления и безопасное поведение в интернете.

Рефлексия и личные планы

Учитель: На основе сегодняшних обсуждений, какие личные шаги вы планируете предпринять, чтобы защитить себя от вредоносных программ? Может быть, вы захотите изменить свои привычки или помочь членам семьи улучшить их кибербезопасность.

Ученики: описывают конкретные действия, которые они планируют предпринять, включая установку или обновление антивирусного программного обеспечения, изменение паролей на более сложные, проведение обучения безопасности для семьи и друзей.

Подведение итогов и домашнее задание

Учитель: Ваше домашнее задание будет состоять из двух частей: первая — проверить все ваши устройства на наличие антивирусного программного обеспечения и убедиться, что оно активно и обновлено. Вторая часть — подготовить презентацию о важности кибербезопасности для представления в вашем классе.

Ученики: принимают информацию и готовятся к выполнению задания.

Учитель: Помните, кибербезопасность — это непрерывный процесс. Чем более вы осведомлены о вредоносных программах и методах их предотвращения, тем безопаснее будет ваш опыт в интернете.

Эта часть занятия побуждает обучающихся к активному и продолжительному участию в своей кибербезопасности, мотивирует их к самообразованию и помощи другим в этой важной области.

Постразговор: Что делать после занятия

Создание и распространение информационных материалов

Цель: распространение знаний о кибербезопасности среди сверстников и младших школьников, повышение общей осведомленности о киберугрозах.

Задание: сверстать брошюры о вредоносном программном обеспечении и способах его предотвращения. Раздать брошюры ученикам школы.

Практикум по кибербезопасности

Цель: применение теоретических знаний на практике, улучшение кибербезопасности в своем непосредственном окружении.

Задание: разработать проект, который включает в себя создание защищенной сетевой среды в школе или дома, например, настройка сетевого фаервола или проведение аудита безопасности сети.

Предлагаемые задания направлены на то, чтобы обучающиеся не только расширили свои знания и развили навыки в области кибербезопасности, но и активно внесли свой вклад в безопасность своего окружения, став более ответственными и компетентными в вопросах кибербезопасности.

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

Приложение 1

Вот несколько примеров атак вредоносных программ, которые произошли в последние годы в России:

В 2023 году произошла крупная кибератака на российские информационные ресурсы. Злоумышленники использовали вредоносное программное обеспечение для внедрения в системы и сбора конфиденциальной информации. В результате атаки были скомпрометированы данные многих организаций и государственных структур.

В начале 2022 года была зафиксирована масштабная атака на российские компании с использованием вредоносного программного обеспечения. Целью злоумышленников было получение доступа к финансовым данным и платёжным системам. Атака привела к значительным финансовым потерям для пострадавших компаний.

В конце 2021 года произошла серия атак на государственные и частные организации в России с использованием вирусов-шифровальщиков. Эти вирусы блокировали доступ к данным на компьютерах и требовали выкуп за их расшифровку. Атаки привели к серьёзным проблемам для многих организаций.

В середине 2020 года были зафиксированы атаки на российские банки и финансовые учреждения с использованием троянских программ. Трояны позволяли злоумышленникам получать доступ к банковским счетам и переводить средства на свои счета. Это привело к крупным финансовым потерям для банков и их клиентов.

В течение 2019–2020 годов происходили атаки на сайты российских государственных органов и СМИ с использованием DDoS-атак. Эти атаки приводили к временному отключению сайтов и нарушению их работы. DDoS-атака — это попытка сделать сайт недоступным для пользователей, перегружая его запросами.