

Внеурочное занятие для обучающихся 7-11 классов по теме

КОНФИДЕНЦИАЛЬНОСТЬ ДАННЫХ

Цель занятия:

Формирование теоретических знаний и практических навыков безопасного поведения в сети Интернет, ответственного отношения к персональным данным и личной информации.

Задачи занятия:

- Познакомить учащихся с понятием конфиденциальности данных.
- Объяснить, почему важно защищать личную информацию.
- Научить базовым правилам защиты личной информации в интернете.
- Развить осознанное отношение к информации, которой дети делятся онлайн.

Формирующиеся ценности:

Уважение к личной и чужой приватности Ученики учатся ценить личную информацию — как свою, так и других. Понимание того, что некоторые данные не предназначены для публичного доступа и должны быть защищены.

Ответственность за распространение и защиту личной информации Развитие ответственного отношения к управлению личной информацией. Понимание, что распространение чужой информации без разрешения может иметь серьезные последствия.

Осведомлённость о последствиях деления информацией в интернете Осознание того, что информация, размещенная в интернете, может сохраняться там навсегда, и что неосторожное обращение с данными может привести к нежелательным или вредным последствиям.

Основные смыслы:

Что такое личные данные и конфиденциальность: занятие начинается с определения личных данных: это информация, которая может идентифицировать индивидуума, например, имя, адрес, телефонный номер или дата рождения. Конфиденциальность данных включает правила и методы, которые помогают защитить эту информацию от несанкционированного доступа и использования.

Риски, связанные с незащищённой личной информацией: школьники изучают, что происходит, когда личная информация не защищена. Обсуждаются риски (кража идентичности, потеря конфиденциальности, мошенничество). Занятие направлено на то, чтобы показать, как неправильное обращение с данными может навредить не только ученику, но и его семье.

Простые способы защиты личной информации для детей: школьники учатся основным методам защиты личных данных, включая использование сложных паролей, осторожность при общении в интернете, избегание передачи личной информации незнакомцам и важность общения с родителями или учителями при возникновении подозрительных ситуаций.



Продолжительность занятия:
45 минут



Рекомендуемая форма проведения занятия:
беседа с элементами групповой работы.

Структура занятия

Часть 1. Осознание важности конфиденциальности данных

Учитель: Сегодня мы обсудим тему, которая затрагивает каждого из нас каждый день — конфиденциальность данных. Мы живём в мире, где наша личная информация постоянно циркулирует в интернете, но как мы можем убедиться, что она защищена? Давайте начнем с понимания, что такое личные данные.

Введение в понятие личных данных

Учитель: Что такое личные данные? Это любая информация, которая может быть использована для идентификации вас как личности. Это может быть ваше имя, адрес, номер телефона, а также более чувствительная информация, например, номер социального страхования или данные банковских счетов. Почему, по вашему мнению, важно защищать такую информацию?

Ученики: обсуждают значимость защиты личной информации, включая риски кражи идентичности, мошенничества и потери конфиденциальности.

Значение конфиденциальности в современном мире

Учитель: Почему конфиденциальность данных стала такой важной в обществе? Как это связано с вашими ежедневными действиями в интернете?

Ученики: делают выводы о связи между конфиденциальностью данных и современными технологиями, обсуждают, как технологии влияют на их личную жизнь и свободу.

Учитель: На основе сегодняшнего обсуждения мы видим, что конфиденциальность данных играет критическую роль в защите нашей личности и финансового благополучия.

Эта часть занятия направлена на создание основы для глубокого понимания конфиденциальности данных, акцентируя внимание на её значении и связанных с ней рисках в современном цифровом мире, что помогает подготовить обучающихся к ответственному обращению с личной информацией.

Часть 2. Методы защиты личных данных

Учитель: Мы обсудили важность защиты личной информации. Сейчас углубимся в специфические способы, как можно защитить ваши данные от нежелательного доступа и злоупотребления. Давайте начнем с обзора некоторых технологических инструментов.

Технические инструменты для защиты данных

Учитель: Первый инструмент, о котором поговорим, — это VPN или виртуальная частная сеть. Кто-нибудь может объяснить, что это такое и как это помогает защищать ваши данные?

Ученики: обсуждают, что такое VPN и как он шифрует интернет-трафик, обеспечивая более безопасное подключение.

Учитель: Отлично! Кроме VPN ключевыми стратегиями защиты также являются использование антивирусного программного обеспечения и настройка сильных паролей. Поговорим о том, как создать сильный пароль. Каким критериям должен соответствовать сильный пароль?

Ученики: перечисляют критерии (длина пароля, использование символов, цифр и букв разного регистра).

Поведенческие стратегии защиты данных

Учитель: Технические инструменты важны, но также критически важно вести себя безопасно в интернете. Давайте обсудим, какие поведенческие стратегии можно применять каждый день для защиты ваших данных.

Ученики: обсуждают стратегии (не делиться личной информацией в социальных сетях, проверка источников перед загрузкой файлов и осторожность при общении в интернете).

Интерактивное упражнение «Реальный сценарий»

Учитель: Для закрепления этих идей давайте проведем интерактивное упражнение. Я раздам вам карточки с различными сценариями (**Приложение 1**), где вам нужно будет определить, какие действия следует предпринять для защиты ваших данных.

Ученики: работают в группах, анализируя сценарии и предлагая решения на основе обсужденных стратегий.

Учитель: Сегодня мы узнали много нового о том, как защитить наши данные. Важно помнить, что конфиденциальность данных — это не только технический вопрос, но и вопрос вашего поведения в интернете. В качестве домашнего задания попросите у родителей помочь проверить настройки безопасности ваших устройств и аккаунтов.

Эта часть занятия способствует пониманию обучающимися необходимости защиты личной информации, обеспечивая им навыки, которые они могут использовать для повышения своей безопасности онлайн.

Часть 3. Применение знаний в проектах и исследованиях

Учитель: Теперь, когда мы знаем о технических и поведенческих способах защиты наших данных, давайте перейдем к практическому применению этих знаний. Каждый из вас сможет исследовать, как технологии могут помочь защитить личные данные в реальных сценариях.

Создание проектов по защите данных

Учитель: Ваша задача — выбрать одну тему, которая связана с защитой данных в интернете. Это может быть исследование, как работает VPN, создание руководства по созданию сильных паролей, или анализ мер безопасности в популярных социальных сетях.

Ученики: выбирают темы и начинают планирование своих проектов.

Работа в группах

Учитель: Вы будете работать в группах, чтобы поделиться идеями и ресурсами. Это также позволит вам учиться друг у друга и развивать коммуникативные навыки.

Ученики: организуются в группы по интересам и начинают совместную работу над проектами.

Использование цифровых инструментов

Учитель: Для выполнения этих проектов можно использовать различные цифровые инструменты. Например, для создания презентаций пригодится PowerPoint, а для сбора информации — цифровые библиотеки и научные базы данных.

Подготовка к презентациям

Учитель: Когда ваши проекты будут готовы, каждая группа сможет поделиться своими находками и рекомендациями по защите данных с классом.

Ученики: готовят презентации, практикуют выступления и готовят ответы на возможные вопросы.

Эта часть занятия помогает обучающимся не только расширить свои знания о защите данных, но и развить навыки исследования, коммуникации и использования цифровых инструментов, которые будут полезны им в будущем. Такой подход поддерживает активное и целенаправленное обучение, готовя школьников к реальным вызовам в области конфиденциальности данных.

Часть 4. Заключительная

Учитель: Мы приближаемся к концу нашего занятия о конфиденциальности данных. Сегодня вы все работали над проектами, исследуя различные аспекты защиты личной информации. Давайте обсудим, что вы узнали и как можно применить эти знания на практике.

Учитель: Теперь, когда мы обсудили ваши проекты, давайте подумаем, почему важно продолжать обращать внимание на конфиденциальность данных в вашей повседневной жизни?

Ученики: делятся своими мыслями о том, как они могут применять усвоенные знания в повседневной жизни, в школе и дома, чтобы защитить свои данные.

Планы на будущее

Учитель: Что вы планируете делать по-другому после этого занятия? Есть ли конкретные шаги или изменения, которые вы хотели бы внести в свои ежедневные привычки?

Ученики: описывают изменения, которые они планируют внедрить, например, использование более сложных паролей, осторожность при распространении информации в социальных сетях, регулярные проверки настроек приватности.

Учитель: Защита ваших личных данных — это непрерывный процесс, который требует внимания и осознанности. Вы все показали отличное понимание темы и усердие в работе над проектами.

Продолжайте оставаться информированными и обучайте других важности сохранения конфиденциальности данных. Спасибо за активное участие и творческий подход!

Эта часть занятия не только закрепляет знания обучающихся о конфиденциальности данных, но и стимулирует их к активному участию в защите своих данных в цифровом мире; подчеркивает значение непрерывного образования и самосовершенствования в области кибербезопасности.

Постразговор: Что делать после урока

Семейное обсуждение

Цель: способствовать осведомленности всей семьи о защите личных данных и обеспечить защиту домашних устройств.

Задание: проведите обсуждение с вашими родителями о важности конфиденциальности данных и расскажите им о том, что узнали на уроке. Можете также проверить настройки конфиденциальности на семейных устройствах вместе с родителями.

Персональный аудит безопасности

Цель: укрепить защиту персональных данных в интернете и развить привычку регулярно обновлять настройки безопасности.

Задание: проведите аудит безопасности своих онлайн-аккаунтов. Проверьте настройки конфиденциальности в социальных сетях, на почтовых сервисах и других онлайн-платформах, которые используете. Убедитесь, что используете сильные и уникальные пароли для каждого аккаунта.

Приложение 1

Вот несколько сценариев, в которых нужно определить, какие действия следует предпринять для защиты данных:

- **Потеря или кража устройства с конфиденциальной информацией.**
В этом случае необходимо немедленно заблокировать устройство и обратиться в службу поддержки для восстановления доступа к данным. Также стоит обратиться в правоохранительные органы, если есть подозрение на кражу.
- **Утечка данных в результате взлома системы безопасности.**
В такой ситуации необходимо провести аудит системы безопасности, выявить уязвимости и принять меры по их устранению. Также следует уведомить пользователей о возможной утечке данных и предложить им принять дополнительные меры предосторожности.
- **Фишинговая атака или мошенничество с использованием личных данных.** В таком случае необходимо проверить, не были ли украдены личные данные, и предпринять необходимые меры для их защиты. Например, сменить пароли, установить антивирусное ПО и т. д.
- **Неавторизованный доступ к данным.**
Если кто-то получил несанкционированный доступ к вашим данным, необходимо немедленно принять меры для блокировки устройства. Это может включать в себя изменение паролей, отключение учётных записей и обращение в службу безопасности.
- **Вирусная атака или вредоносное ПО.**
В случае обнаружения вирусной атаки или вредоносного ПО необходимо удалить программу, восстановить систему из резервной копии и установить антивирусное ПО. Также рекомендуется проверить все устройства, подключённые к сети, на наличие вирусов.

Кармазин Виталий Юрьевич.

Кандидат технических наук, доцент
кафедры цифровой экономики
ФГБОУ ВО Вавиловский университет