Внеурочное занятие для обучающихся 7-11 классов

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Цель занятия:

Обеспечение информационной безопасности школьников посредством привития им навыков ответственного и безопасного поведения в современной информационно-коммуникационной среде.

Задачи занятия:

- Определить, что такое интернет-безопасность и почему она важна для детей.
- Научить детей распознавать безопасные и небезопасные онлайн-практики.
- Обсудить, какие действия следует предпринимать при столкновении с неприятными или небезопасными ситуациями в интернете.
- Развить у детей навыки безопасного общения в интернете и использования интернет-ресурсов.

Формирующиеся ценности:

Уважение Понимание важности уважительного общения в интернете и уважения чужой конфиденциальности и личных данных.

Ответственность Развитие ответственного подхода к использованию интернета, включая осознанное обращение с личной информацией и информацией других.

Самозащита Осознание важности защиты своей личности и личных данных в интернете.

Социальная ответственность Формирование чувства ответственности за свои действия в интернете и понимание последствий этих действий.

Основные смыслы:

Что такое интернет-безопасность: интернет является мощным инструментом, который требует осторожного и ответственного использования.

Распознавание угроз: обучение школьников способам распознавания потенциально опасных или нежелательных ситуаций в интернете, таких как фишинг, кибербуллинг или неприемлемый контент.

Правила безопасного поведения в интернете: ознакомление с основными правилами безопасности, включая неразглашение личной информации, использование сложных паролей и обращение за помощью к взрослым.

Последствия небезопасного поведения: обсуждение возможных последствий небрежного поведения в интернете, осознание важности соблюдения правил безопасности.

Продолжительность занятия:
45 минут

Рекомендуемая форма проведения занятия:
беседа

Структура занятия

Часть 1. Введение в тему «Интернет-безопасность»

Учитель: Сегодня мы обсудим очень важную тему — безопасность в интернете. Это особенно актуально для вас, так как большая часть вашей социальной активности и обучения происходит онлайн. Давайте начнём с основ: какие ассоциации у вас возникают, когда слышите «интернет-безопасность»? Какие аспекты этой темы кажутся вам наиболее важными?

Ученики: делятся своими мыслями о том, что такое интернет-безопасность и почему она важна.

Учитель: Отличные ответы! Интернет-безопасность включает в себя множество аспектов, от защиты личной информации до предотвращения киберпреступлений. Давайте сначала определим основные угрозы, с которыми вы можете столкнуться в интернете.

Обсуждение основных угроз

Учитель: Давайте определим основные угрозы, с которыми вы можете столкнуться в интернете, составим список и обсудим, как они могут повлиять на вас.

Ученики: перечисляют угрозы (фишинг, вирусы, кибербуллинг, утечки данных и пр).

Учитель: Очень важно, что вы осознаете эти угрозы. Теперь давайте подумаем, почему молодые люди особенно уязвимы в интернете и что это значит для вашей повседневной жизни в сети.

Понимание влияния угроз на молодёжь

Учитель: Почему, по вашему мнению, подростки и молодые люди могут быть особенно уязвимы в сети?

Ученики: обсуждают возможные причины, включая недостаток опыта, высокий уровень доверия к онлайн-информации, социальное давление использовать определенные платформы.

Эта часть занятия направлена на повышение осведомлённости обучающихся о рисках в интернете и мотивацию к изучению способов защиты собственной информации и личной безопасности онлайн.

Часть 2. Способы защиты в интернете и критическое мышление

Учитель: Мы обсудили основные угрозы интернета. Сейчас мы обсудим методы защиты, которые помогут вам сохранять безопасность онлайн. Начнем с основных инструментов и практик, которые каждый из вас может использовать.

Обсуждение инструментов защиты

Учитель: Какие инструменты или практики защиты вы знаете и уже используете для сохранения вашей безопасности в интернете?

Ученики: делятся примерами, такими как антивирусное программное обеспечение, двухфакторная аутентификация, сложные пароли, использование VPN.

Учитель: Отлично! Эти инструменты очень важны. Давайте теперь поговорим о том, как правильно использовать социальные сети и другие онлайн-платформы, чтобы минимизировать риски.

Разработка навыков безопасного использования социальных сетей

Учитель: Социальные сети могут быть минным полем в плане безопасности. Какие правила следует соблюдать, чтобы ваш профиль был защищён?

Ученики: обсуждают правила, такие как настройки приватности, осторожность с размещением личной информации, избегание общения с незнакомцами.

Учитель: Правильно. Также важно знать, как распознавать фишинговые атаки и мошеннические сообщения.
Давайте выполним упражнение на распознавание таких угроз.

Упражнение по распознаванию фишинга и мошенничества

Учитель: Я покажу вам несколько примеров сообщений, а вы должны будете определить, являются ли они безопасными или потенциально опасными.

Ученики: анализируют сообщения и обсуждают признаки фишинга и мошенничества. **(Приложение 1)**

Эта часть занятия помогает ученикам понять и освоить конкретные способы защиты в интернете, развивая при этом критическое мышление и ответственное поведение онлайн.

Часть 3. Ролевые игры и сценарное планирование

Учитель: Мы уже обсудили, какие угрозы существуют в интернете и какие инструменты защиты мы можем использовать. Теперь давайте попробуем применить эти знания на практике. Мы проведём несколько ролевых игр, чтобы вы смогли представить себя в различных ситуациях и попробовали принять безопасные решения.

Ролевая игра «Решение в реальном времени»

Учитель: Предлагаю разделиться на небольшие группы. Каждая группа получит карточку со сценарием, где описана потенциально опасная ситуация в интернете. Ваша задача — обсудить сценарий и предложить, как вы бы поступили в данной ситуации.

Ученики: работают в группах, каждая группа анализирует свой сценарий и разрабатывает план действий. По итогу работы проходит обсуждение различных подходов к решению проблем кибербезопасности. **(Приложение 2)**

Сценарное планирование

Учитель: Отлично справились! Приступаем к выполнению следующего задание. Представьте, что вам необходимо разработать план безопасности для мероприятия в вашей школе, которое будет полностью проводиться онлайн. Что вы бы предложили включить?

Ученики: обсуждают и разрабатывают комплексный план безопасности, используя знания, которые они получили.

Обсуждение и обратная связь

Учитель: Познакомимся с вашими планами. Какие идеи вы предложили? Как думаете, могли бы эти меры реально повысить безопасность онлайн-мероприятий?

Ученики: представляют свои планы и получают обратную связь от учителя и одноклассников.

Учитель: Вы проделали отличную работу, применяя теоретические знания на практике. Это позволит не только защитить себя, но и помочь обеспечить безопасность других в интернете. Надеюсь, вы используете эти навыки в жизни.

Эта часть занятия позволяет школьникам активно участвовать в процессе обучения, применяя теоретические знания в практических, реальных сценариях, что способствует лучшему усвоению материала и развитию критического мышления.

Часть 4. Заключительная

Учитель: Мы много сегодня говорили о том, как обезопасить себя в интернете. Теперь давайте подведём итоги и поговорим о том, что каждый из вас может делать, чтобы поддерживать свою безопасность в сети.

Обсуждение ключевых выводов

Учитель: Какие основные моменты вы вынесли для себя из сегодняшнего урока? Какие действия вы считаете наиболее важными для вашей безопасности в интернете?

Ученики: делятся своими мыслями и выводами, рассказывая о мерах, которые они планируют принять для улучшения своей интернет-безопасности.

Закрепление знаний

Учитель: Чтобы убедиться, что вы помните и готовы применять эти знания, я предлагаю вам выполнить небольшой проект, который мы обсудим сейчас.

Учитель: Вам необходимо подготовить презентацию, которую можно использовать для обучения правилам безопасности в интернете других учеников или членов вашей семьи. Выберите одну конкретную тему, которую мы обсуждали, и разработайте информационные материалы по ней.

Ученики: принимают задание и начинают планировать свои проекты.

Обещание безопасности

Учитель: Кроме того, я хочу, чтобы каждый из вас дал обещание безопасности — обещание, которое вы сами составите, о том, как вы будете поддерживать безопасность в интернете. Это может быть что-то вроде регулярной проверки настроек приватности или обещания не делиться личной информацией с незнакомцами.

Ученики: составляют и делятся своими обещаниями безопасности.

Поддержка и ресурсы

Учитель: Помните, что вы всегда можете обратиться за помощью или дополнительной информацией ко мне или любому другому учителю. В школе также есть ресурсы, такие как брошюры и книги о безопасности в интернете, которые вы можете использовать. Безопасность в интернете — это непрерывный процесс обучения и адаптации. Я горжусь вашим усердием и ответственным подходом к этой теме. Продолжайте быть бдительными и информированными. Благодарю вас за активную работу!

Эта часть занятия направлена на то, чтобы мотивировать обучающихся к активным действиям, способствующим их безопасности в интернете, и помочь им почувствовать ответственность за свои действия в сети.

Постразговор: Что делать после занятия

Обсуждение с семьей

Цель: закрепление полученных знаний через семейное обсуждение.

Задание: Поделитесь с родителями или опекунами основными моментами урока и обсудите с ними, какие меры безопасности применяются в вашем доме. Это может включать обсуждение настроек приватности на устройствах или просмотр установленных приложений.

Личный аудит безопасности

Цель: развитие навыков самооценки и самостоятельного управления безопасностью личных данных.

Задание: провести аудит своих онлайн-профилей и устройств, проверив настройки конфиденциальности и безопасности. Убедиться, что личная информация защищена.

Создание проекта по безопасности в интернете

Цель: развитие творческих и коммуникативных навыков.

Задание: разработать и провести мастер-класс о безопасности в интернете для младших школьников. Мастер-классы могут включать темы о фишинге, безопасном использовании соцсетей, важности сильных паролей и т.д.

Предлагаемые задания призваны помочь обучающимся закрепить полученные знания, развить навыки применения этих знаний в реальной жизни и способствовать безопасности в их широком социальном и семейном кругу.

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

Приложение 1 **5 опасных**

1. Сообщение от имени банка.
В сообщении говорится, что с вашего счёта была совершена подозрительная операция. Для её отмены вам нужно перейти по ссылке и ввести свои личные данные.

2. Сообщение с просьбой о помощи.
В сообщении говорится, что ваш знакомый или родственник попал в беду и ему срочно нужны деньги. Вас просят перевести определённую сумму на указанный счёт.

3. Сообщение о выигрыше.
В сообщении говорится, что вы выиграли крупную сумму денег в лотерее или конкурсе, и вам нужно оплатить комиссию или налог для получения приза.

4. Сообщение о продаже товара.
В сообщении предлагается купить товар по очень низкой цене. Вас просят оплатить полную стоимость товара, а затем обещают выслать его.

5. Сообщение о взломе.
В сообщении говорится, что ваша учётная запись была взломана, и нужно срочно изменить пароль. Вас просят перейти по ссылке и ввести текущий пароль.

Приложение 1 **5 безопасных**

1. Сообщение от государственного органа.
Сообщение содержит информацию о важном событии, мероприятии или изменении в законодательстве.
Оно подписано официальным лицом или организацией.

2. Сообщение от знакомого.
Сообщение отправлено человеком, которого вы знаете лично. В нём содержится информация, которая соответствует характеру вашего общения.

3. Сообщение от компании, с которой у вас есть деловые отношения.
Сообщение касается вопросов, связанных с вашими деловыми отношениями. Оно подписано представителем компании, с которой вы сотрудничаете.

4. Сообщение от благотворительной организации.
Сообщение содержит просьбу о пожертвовании на благотворительные цели. Оно подписано известной и уважаемой организацией.

5. Сообщение от образовательного учреждения.
Сообщение касается вопросов, связанных с вашим обучением или участием в мероприятии.
Оно подписано представителем образовательного учреждения, с которым вы связаны.

Приложение 2 **Примеры ситуаций**

1. Встреча с мошенниками.
Пользователь получает сообщение от неизвестного человека, который представляется сотрудником банка и просит предоставить личные данные для подтверждения личности. Пользователь не подозревает, что это мошенник, и предоставляет свои данные, после чего злоумышленник получает доступ к его банковскому счёту и переводит деньги на свой счёт.

2. Небезопасный сайт.
Пользователь посещает сайт, который выглядит как официальный, но на самом деле является мошенническим. Пользователь вводит свои личные данные на сайте, думая, что это необходимо для регистрации или покупки товара. Однако эти данные используются злоумышленниками для кражи личных данных пользователя.

3. Взлом аккаунта.
Пользователь забывает выйти из своего аккаунта на чужом устройстве и оставляет его без присмотра. Этим пользуется злоумышленник, который получает доступ к аккаунту пользователя и начинает рассылать спам или публиковать неприемлемый контент от имени пользователя.

4. Кибербуллинг.
Пользователь становится объектом кибербуллинга — травли и преследования в интернете. Злоумышленники публикуют оскорбительные комментарии и посты о пользователе, распространяют его личную информацию и создают поддельные аккаунты, чтобы навредить ему.

5. Небезопасная загрузка.
Пользователь загружает файл или программу из ненадёжного источника. Этот файл оказывается вредоносным и заражает устройство пользователя вирусом или другим вредоносным ПО. Это может привести к потере данных, сбоям в работе устройства или даже краже личных данных пользователя.