V Городской конкурс методических разработок по информатике
«Вернисаж педагогических идей»

«Лучшая методическая разработка воспитательного мероприятия по информатике».

Тема: "Информационная безопасность: Мифы и реальность"

Автор: Жулина Анна Сергеевна, студент, Сургутский государственный педагогический университет

Пояснительная записка

В современном мире, пронизанном информационными технологиями, вопросы информационной безопасности приобретают особую актуальность. Подростки, активно использующие интернет и социальные сети, зачастую недооценивают риски, связанные с распространением личной информации, общением с незнакомцами в сети, скачиванием сомнительного контента и подвержены влиянию дезинформации. Данная методическая разработка направлена на повышение уровня информационной грамотности учащихся 7-9 классов, формирование у них осознанного и ответственного отношения к собственной безопасности в информационном пространстве.

Мероприятие проводится в интерактивной форме, предполагающей активное участие учащихся в обсуждении проблемных ситуаций, анализе мифов об информационной безопасности и выработке правил безопасного поведения в сети. Использование игровых элементов и групповой работы позволяет вовлечь каждого участника в процесс обучения, сделать его более интересным и запоминающимся.

Цель мероприятия: Формирование у учащихся осознанного и ответственного отношения к информационной безопасности, развитие навыков безопасного поведения в информационном пространстве.

Задачи:

1.Образовательные:

- Расширить знания учащихся об основных угрозах информационной безопасности в современном мире.
- Развеять распространенные мифы об информационной безопасности.
- Сформировать понимание важности защиты личной информации в сети.
- Познакомить с основными правилами безопасного поведения в интернете.

2.Развивающие:

- Развитие критического мышления, умения анализировать информацию и оценивать ее достоверность.
- Развитие коммуникативных навыков, умения работать в команде, аргументировать свою точку зрения.

- Развитие умения принимать осознанные решения в ситуациях, связанных с информационной безопасностью.

3.Воспитательные:

- Воспитание ответственности за свои действия в информационном пространстве.
- Формирование культуры общения в сети, уважительного отношения к другим пользователям.
- Формирование гражданской позиции в вопросах защиты информации.

Форма проведения: Интерактивная игра-дискуссия с элементами квеста.

Оборудование:

- Раздаточные материалы (карточки с мифами и фактами, сценарии для ролевых игр, памятки с правилами безопасного поведения).
- Листы бумаги, ручки, маркеры.

Участники: Учащиеся 7-9 классов (класс делится на 3-4 команды).

Место проведения: Класс информатики или актовый зал.

Продолжительность: 45-60 минут.

План мероприятия

1. Вступление (5 минут)

Приветствие участников.

Актуализация темы: краткое обсуждение роли информации в современном мире и связанных с этим угроз.

Определение целей и задач мероприятия.

Разделение на команды и выбор капитанов.

2. Разминка "Мифы и реальность" (10 минут)

Командам предлагаются карточки с утверждениями, касающимися информационной безопасности (см. Приложение 1).

Задача команд: определить, является ли утверждение мифом или фактом, и аргументировать свой ответ.

Ведущий организует обсуждение каждого утверждения, раскрывая истинную информацию.

3. Практическая часть "Квест информационной безопасности" (20 минут)

Командам предлагается пройти серию станций (заданий), посвященных различным аспектам информационной безопасности. Каждая станция содержит проблемную ситуацию или задачу, требующую анализа и принятия решения.

Станции квеста:

Станция 1: "Личная информация под прицелом". Задание: Анализ вымышленного профиля в социальной сети и выявление информации, представляющей угрозу для безопасности пользователя (см. Приложение 2).

Станция 2: "Фишинговая атака". Задание: Распознавание фишингового письма и определение действий, которые необходимо предпринять для защиты от мошенничества (см. Приложение 3).

Станция 3: "Парольная безопасность". Задание: Разработка надежного пароля и обсуждение правил хранения и использования паролей (см. Приложение 4).

Станция 4: "Кибербуллинг". Задание: Ролевая игра, в которой участники разыгрывают ситуацию кибербуллинга и предлагают способы ее решения (см. Приложение 5).

4. Подведение итогов и рефлексия (10 минут)

Обсуждение результатов квеста, анализ ошибок и успехов команд.

Обобщение основных правил безопасного поведения в информационном пространстве.

Вопросы к участникам:

- Что нового вы узнали на мероприятии?
- Какие правила информационной безопасности вы будете соблюдать в дальнейшем?
- Что вы расскажете своим друзьям и близким об информационной безопасности?

Вручение памяток с правилами безопасного поведения в интернете (см. Приложение 6).

5. Заключение (5 минут)

Благодарность участникам за активное участие.

Подчеркивание важности постоянного повышения уровня информационной грамотности.

Анонс дальнейших мероприятий по теме информационной безопасности.

Заключение

Данная методическая разработка предоставляет учителю информатики готовый сценарий для проведения воспитательного мероприятия, направленного на повышение уровня информационной грамотности учащихся. Использование интерактивных форм работы, игровых элементов и практических заданий позволяет сделать процесс обучения более интересным и эффективным. Важно отметить, что вопросы информационной безопасности требуют постоянного внимания и актуализации, поэтому рекомендуется регулярно проводить подобные мероприятия с учащимися, адаптируя их к изменяющимся реалиям информационного пространства.

Список использованной литературы

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ.

2. Концепция информационной безопасности детей (утверждена распоряжением Правительства Российской Федерации от 02.12.2015 N 2471-р).

3. https://родителям.дети.рф/ (информационный портал "Я родитель")

4. https://onlife.videomore.ru/ - проект "Безопасность детей в интернете"

Приложения

Приложение 1: Карточки "Мифы и реальность"

1. Утверждение: Антивирусная программа гарантирует полную защиту от всех угроз в интернете.

Ответ: Миф. Антивирусные программы являются важным инструментом защиты, но они не могут гарантировать 100% защиту. Важно также соблюдать правила безопасного поведения и регулярно обновлять антивирусные базы.

2. Утверждение: В интернете все анонимно, и никто не узнает, кто я на самом деле.

Ответ: Миф. В интернете практически невозможно оставаться полностью анонимным. Многие сайты и сервисы собирают информацию о пользователях, включая IP-адрес, данные о браузере и устройстве.

3. Утверждение: Если я ничего не публикую в интернете, то моя личная информация в безопасности.

Ответ: Миф. Даже если вы не публикуете информацию о себе в интернете, другие люди могут это делать (например, друзья, родственники). Кроме того, ваши данные могут быть собраны различными компаниями и организациями.

4. Утверждение: Все, что написано в интернете, - правда.

Ответ: Миф. В интернете много ложной и недостоверной информации. Важно критически оценивать информацию и проверять ее в надежных источниках.

5. Утверждение: Чем сложнее пароль, тем он надежнее.

Ответ: Факт. Сложные пароли труднее взломать. Рекомендуется использовать пароли, состоящие из букв разного регистра, цифр и специальных символов.

6. Утверждение: Установив блокировщик рекламы, я полностью обезопасил свой компьютер от вирусов.

Ответ: Миф. Блокировщик рекламы уменьшает риск заражения вредоносным ПО, распространяемого через рекламные баннеры, но не гарантирует полной защиты. Необходимо использовать антивирус и соблюдать правила безопасного серфинга.

Приложение 2: Станция "Личная информация под прицелом"

Задание: Проанализируйте вымышленный профиль в социальной сети и определите, какая информация может представлять угрозу для безопасности пользователя. Предложите способы защиты личной информации.

Вымышленный профиль:

Имя: Иван Иванов

Возраст: 14 лет

Место учебы: Школа №10, 8 класс

Фотографии: Фотографии дома, школы, друзей.

Информация о себе: Люблю играть в компьютерные игры, увлекаюсь футболом. Живу рядом со школой.

Друзья: 250 человек (многие незнакомые)

Публикации: Рассказы о покупках, планах на выходные, местоположении во время отдыха.

Вопросы для обсуждения:

- Какая информация в профиле может быть использована злоумышленниками?
- Какие действия можно предпринять для защиты личной информации?
- Стоит ли добавлять в друзья незнакомых людей?
- Как часто нужно обновлять настройки приватности в социальных сетях?

Приложение 3: Станция "Фишинговая атака"

Задание: Распознайте фишинговое письмо и определите действия, которые необходимо предпринять для защиты от мошенничества.

Фишинговое письмо (пример):

Тема: Важное уведомление от вашего банка!

Текст:

Уважаемый клиент!

В связи с недавними обновлениями системы безопасности, нам необходимо подтвердить ваши данные. Пожалуйста, перейдите по ссылке ниже и введите свой логин и пароль от интернет-банка.

https://apwg.org/

С уважением,

Служба поддержки вашего банка.

Вопросы для обсуждения:

- Какие признаки указывают на то, что письмо является фишинговым?
- Какие действия нельзя совершать в ответ на такое письмо?
- Как проверить подлинность письма от банка?
- Куда можно обратиться, если вы стали жертвой фишинговой атаки?

Приложение 4: Станция "Парольная безопасность"

Задание: Разработайте надежный пароль для своей учетной записи и обсудите правила хранения и использования паролей.

Правила создания надежного пароля:

- Длина пароля не менее 12 символов.
- Использование букв разного регистра, цифр и специальных символов.
- Отсутствие личной информации (имя, дата рождения и т.д.).
- Отсутствие распространенных слов и фраз.

Вопросы для обсуждения:

- Почему важно использовать разные пароли для разных учетных записей?
- Как часто нужно менять пароли?
- Где безопасно хранить пароли?
- Что делать, если вы забыли свой пароль?

Приложение 5: Станция "Кибербуллинг"

Задание: Разыграйте ситуацию кибербуллинга и предложите способы ее решения.

Сценарий:

Один из учеников класса становится жертвой кибербуллинга в социальной сети. Одноклассники публикуют о нем оскорбительные комментарии и фотографии.

Роли:

- Жертва кибербуллинга
- Агрессор (обидчик)
- Свидетели (одноклассники)

Вопросы для обсуждения:

- Как чувствует себя жертва кибербуллинга?
- Какие мотивы могут быть у агрессора?
- Как должны реагировать свидетели на кибербуллинг?
- Какие действия может предпринять жертва кибербуллинга?
- Куда можно обратиться за помощью в случае кибербуллинга?

Приложение 6: Памятка "Правила безопасного поведения в интернете"

1. Защищайте свою личную информацию: не сообщайте незнакомым людям свои имя, адрес, номер телефона, пароли и другую конфиденциальную информацию.

2. Будьте осторожны при общении с незнакомцами: не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в интернете, без сопровождения взрослых.

3. Не открывайте подозрительные ссылки и вложения: не переходите по ссылкам, которые приходят от незнакомых людей, и не скачивайте файлы из ненадежных источников.

4. Используйте надежные пароли: создавайте сложные пароли, состоящие из букв разного регистра, цифр и специальных символов, и не используйте один и тот же пароль для разных учетных записей.

5. Установите антивирусную программу: регулярно обновляйте антивирусные базы и проверяйте свой компьютер на наличие вирусов.

6. Будьте вежливы и уважительны: не оскорбляйте других пользователей и не участвуйте в кибербуллинге.

7. Сообщайте о нарушениях: если вы столкнулись с подозрительной или опасной ситуацией в интернете, сообщите об этом своим родителям, учителям или в службу поддержки сайта.

Экспертный лист
оценивания методических разработок, представленных на V городской конкурс методических разработок по информатике «Вернисаж педагогических идей»

_____
(Фамилия, имя, отчество участника Конкурса)

_____
(Название методической разработки)

Максимальная оценка по каждому показателю – 5 баллов.

п/п	Критерии оценивания методических разработок	Баллы
1.	Актуальность и значимость темы методической разработки	
2.	Соответствие содержания методической разработки требованиям ФГОС общего образования	
3.	Соответствие содержания (представленных в методической разработке форм работы, педагогических технологий и т.д.), поставленным целям и задачам	
4.	Методическая новизна	
5.	Методическая сложность работы	
6.	Оригинальность представленного материала (наличие авторства)	
7.	Стиль изложения: доступность, наглядность, логичность	
8.	Наличие региональной составляющей в содержании	
9.	Ресурсная обеспеченность (использование современных информационных ресурсов, в том числе собственных разработок)	
10	Творческий характер работы, нестандартность решения педагогической проблемы	
11	Культура оформления материалов, соответствие нормам русского языка и стиля изложения, соответствие ГОСТ	
12	Практическая значимость	
13	Транслируемость, тиражируемость или перспективность применения данной методической разработки в практике образовательных организаций	
14	Полнота структуры и содержания методической разработки: титульный лист, введение (статья от автора, составителя), основная содержательная часть, заключение (вывод) с рекомендациями по использованию методической разработки в образовательном (воспитательном) процессе, список использованной литературы, приложения	
	Итого:	

Дата «___»_____2025 г.

_____ /_____/
Подпись Ф.И.О. эксперта