**Методическое сопровождение внеклассного мероприятия**

**«Цифровая самооборона: Твой выбор в сети»**

**Актуальность и педагогический замысел:**

Подростковый возраст — период активной социализации, часто перенесенной в цифровую среду. Мероприятие направлено не на запреты, а на формирование критического мышления, цифровой осознанности и ответственности за свои действия онлайн. Оно строится на принципе «равный — равному» и моделировании реальных ситуаций из жизни подростков.

**Цель**: Сформировать у подростков навыки критической оценки информации, осознанного управления цифровым следом и эффективного противодействия основным киберугрозам.

**Задачи**:

· Проанализировать последствия неосторожного поведения в сети для репутации и безопасности.

· Отработать алгоритмы действий в ситуациях кибербуллинга, фишинга, мошенничества.

· Сформулировать принципы цифровой гигиены и этики.

**Планируемые результаты:**

· Предметные: Знание основных видов киберугроз и правил защиты от них.

· Метапредметные:

· Регулятивные: Составление алгоритма действий в кризисной ситуации.

· Познавательные: Анализ и оценка информации, проектирование решения.

· Коммуникативные: Участие в дискуссии, аргументация позиции, работа в команде.

· Личностные: Развитие чувства ответственности за свои действия в сети, эмпатии к жертвам кибербуллинга.

**Возрастные особенности и принципы**

· 5-7 класс (11-13 лет): Делаем акцент на практических кейсах (игры, соцсети), используем игровые и творческие форматы. Важен авторитет ведущего-эксперта или старшеклассника.

· 8-9 класс (14-15 лет): Смещаем фокус на репутацию, будущее (поступление, работа), личные границы и права. Допустимы дискуссии на более сложные темы (пропаганда, киберэкстремизм). Эффективна работа в группах с презентацией результатов.

· Принципы: Диалог, а не монолог. Отказ от запугивания. Опора на опыт самих подростков. Практическая полезность «здесь и сейчас».

**Материалы и подготовка**

· Технические: Компьютер, проектор, экран, колонки. Возможно использование смартфонов участников для голосования.

· Раздаточные:

  · Карточки с кейсами для каждой станции/группы.

  · Бланки для составления чек-листов или ментальных карт.

  · Маркеры, стикеры, ватманы.

  · Памятки «Цифровая самооборона»

Подготовительная работа: За 1-2 дня можно провести анонимный опрос (Google Forms или Yandex Forms ) по типу «Сталкивались ли вы с...?», чтобы включить в мероприятие наиболее актуальные для данной аудитории проблемы.

Данное мероприятие соответствует задачам воспитательной работы ФГОС ООО, способствует формированию антибуллинговой среды в школе и готовит подростков к жизни в цифровом обществе, развивая их правовую и гражданскую грамотность.

ПРИМЕРНЫЙ СЦЕНАРИЙ ВНЕКЛАССНОГО МЕРОПРИЯТИЯ

**Тема: «Цифровая самооборона: Твой выбор в сети»**

**Целевая аудитория: 5-9 классы**

Форма: Интерактивный практикум с элементами ситуационного анализа и деловой игры.

Время:45-60 минут.

Ведущий: Классный руководитель / педагог-организатор / приглашенный специалист (психолог, IT-эксперт). Возможно участие подготовленных старшеклассников.

ХОД МЕРОПРИЯТИЯ

I. Старт: «Проверка связи» (Введение, 7-10 мин)

· Приветствие. Ведущий начинает не с лекции, а с вопроса: «Как вы думаете, что такое "цифровая самооборона"? Это карате для программистов?» Выслушивает варианты.

· Определение: «Это набор знаний и навыков, которые позволяют защитить себя, свою репутацию и свои устройства в цифровой среде. Сегодня мы не будем читать нудные инструкции — мы будем разбирать реальные ситуации и искать из них выход».

· Интерактивный опрос: С помощью мобильного голосования или простого «встал/сел» ведущий задает вопросы:

· «Кто из вас проверял настройки приватности в соцсетях за последний месяц?»

· «Сталкивался ли ты или твои друзья с оскорблениями в сети?»

· «Приходило ли вам письмо "от администрации" с просьбой перейти по ссылке и проверить аккаунт?»

· Актуализация: «Как видим, большинство из вас уже в зоне действия этих явлений. Значит, тема важная. Давайте разделимся на 3-4 "совета цифровой безопасности" (группы) и начнем работу».

II. Основная часть: «Совет цифровой безопасности» в деле (30-40 мин)

Формат: Работа в группах по станциям (ротация) или параллельное решение разных кейсов с последующей презентацией.

Группам раздаются конверты с «Делом». На обсуждение — 7-10 минут. Задача: выработать конкретный план действий и представить его.

Кейс 1: «Шторм в комментариях» (Тема: Кибербуллинг и репутация)

· Ситуация: «Твоя одноклассница выложила в социальную сеть фото с новой прической. Под фото анонимный аккаунт начал оставлять жестокие комментарии ("страшная", "сжечь бы такую"), к которому присоединились несколько других подписчиков. Девочка расстроена, удалила фото, но скриншоты уже ушли в общие чаты. Она не хочет идти к взрослым, чтобы не усугублять травлю. Твой совет?»

· Задачи для группы:

1. Что посоветовать жертве? (Например: не вступать в перепалку, сделать скриншоты, использовать инструменты «заблокировать», «пожаловаться», рассказать доверенному взрослому).

2. Что может сделать свидетель (одноклассник)? (Поддержать лично, публично заступиться, массово жаловаться на буллеров).

3. Как остановить распространение скриншотов в чатах? (Обратиться к админам чатов).

· Ключевой вывод для всех: Буллинг останавливается только активной позицией свидетелей и взрослых. Молчание — это поддержка агрессора.

Кейс 2: «Слишком щедрое предложение» (Тема: Фишинг и мошенничество)

· Ситуация: «В чате популярной игры тебе пишет пользователь: "Админ конкурса. Ты выиграл редкий игровой предмет! Чтобы получить, перейди по ссылке и авторизуйся через свой игровой аккаунт". Ссылка выглядит почти как официальная, но с опечаткой. Что делать?»

· Задачи для группы:

1. Назвать не менее 3 признаков мошенничества в этой ситуации.

2. Составить пошаговый алгоритм проверки подобных предложений (например: 1. Не кликать. 2. Проверить официальный сайт/группу игры. 3. Спросить у опытных игроков. 4. Если сомневаешься — проигнорировать).

3. Придумать слоган-предупреждение для других игроков (например: «Бесплатный сыр — ты уже в мышеловке? Проверяй!»).

· Ключевой вывод: Ничего по-настоящему ценного и бесплатного в сети не бывает. Цена — твой аккаунт или данные.

Кейс 3: «Цифровой след навсегда» (Тема: Цифровая репутация и этика)

· Ситуация: «На школьной вечеринке друг снял на телефон смешное, но нелепое и слегка компрометирующее видео с тобой. Он хочет выложить его в социальную сеть для хайпа, уверяя, что это же просто шутка. Ты против. Как убедить его не делать этого? Какие могут быть долгосрочные последствия?»

· Задачи для группы:

1. Привести аргументы для друга (нарушение личных границ, потенциальный буллинг, испорченная репутация, которое увидят будущие работодатели/приемная комиссия).
2. Придумать альтернативу (например, выложить видео в закрытый чат класса с твоего согласия, или не выкладывать вовсе).
3. Сформулировать личное правило: я никогда не буду выкладывать в сеть про других без их согласия.

· Ключевой вывод: Твои действия в сети — это твое цифровое резюме. То, что ты выкладываешь про других, характеризует в первую очередь тебя.

Кейс 4: «Взлом» (Тема: Защита аккаунтов)

· Ситуация: «Твой друг в панике: он перешел по ссылке из письма, ввел пароль от соцсети, и теперь не может войти в аккаунт. На его стене появляются странные посты, от его имени рассылаются спам-сообщения. Он просит у тебя помощи. Что делать?»

· Задачи для группы:

1. Составить для него пошаговый план «Первая помощь при взломе» (Например: 1. Срочно сообщить друзьям, что аккаунт взломан. 2. Восстановить доступ через привязанную почту/телефон. 3. Сменить пароль на сложный. 4. Проверить активные сессии и завершить все. 5. Проверить настройки и удаленные приложения. 6. Настроить двухфакторную аутентификацию).
2. Придумать правила создания «невзламываемого» пароля (фраза+цифры+символы, не связанная с личными данными).

3. Ключевой вывод: Пароль — ключ от цифровой жизни. Его нужно беречь и укреплять.

III. Презентация решений и выработка кодекса (10-15 мин)

· Каждая группа представляет свое решение кейса за 2-3 минуты. Ведущий дополняет, корректирует, дает экспертный комментарий.

· Общий итог: После всех выступлений ведущий предлагает создать «Кодекс цифровой самообороны нашего класса».

· На ватмане или на слайде в режиме реального времени записываются основные правила, выработанные группами:

1. Защищай: Используй сложные пароли и двухфакторную аутентификацию.

2. Проверяй: Не верь сенсациям и щедрым предложениям. Анализируй источник.

3. Уважай: Не распространяй информацию (фото, видео, слухи) о других без их согласия.

4. Поддержи: Не оставайся в стороне, если видишь травлю. Поддержи жертву, сообщи взрослым.

5. Доверяй: Если столкнулся с проблемой — обращайся к родителям, учителям, на линию помощи.

· Все участники символически подписывают кодекс (можно сфотографировать на память).

IV. Рефлексия и итоги (5 мин)

· Микрофон: Ведущий передает условный микрофон (или мячик) с вопросом: «Что из сегодняшнего обсуждения стало для тебя самым важным открытием или напоминанием?»

· Информация о помощи: контакты доверия (Телефон доверия для детей, подростков и их родителей).

· Заключительное слово: «Цифровая среда — это наша общая реальность. Она может быть комфортной и безопасной только если каждый из нас будет проявлять осознанность, уважение и готовность помочь. Вы сегодня доказали, что способны быть не только пользователями, но и ответственными цифровыми гражданами. Спасибо!»

***Приложения к сценарию***

*1. Памятка для подростка «Цифровая самооборона» (кратко):*

| |
|---|
| **Пароль**: Как зубная щетка — никому не давай и меняй раз в 3 месяца. Включи 2FA. |
| **Приватность**: Настрой, кто что видит. Адрес, телефон, геометки — только для самых близких. |
| **Доверие**: Незнакомец в сети = незнакомец на улице. Не верь, не встречайся, не отправляй фото. |
| **Репутация**: Работодатели и вузы проверяют соцсети. Думай, прежде чем постить. |
| **Этика**: Не пиши того, что не сказал бы в лицо. Не распространяй контент без согласия человека. |
| **Помощь**: Если травля, шантаж, угрозы — скриншот, блок, жалоба, расскажи взрослому. Ты не один. |

*2. Советы ведущему (педагогу):*

*· Тон: Будьте в роли модератора и эксперта-консультанта, а не лектора или контролера.*

*· Конфиденциальность: Если в ходе обсуждения подростки делятся личным опытом, пресекайте любые попытки осуждения или обсуждения этого за пределами мероприятия. Подчеркивайте ценность доверия.*

*· Гибкость: Если видите, что одна тема «зацепила» больше, дайте ей больше времени, сократив другие.*

*· Работа с сопротивлением: Если есть скептически настроенные подростки, вовлекайте их в дискуссию: «А как бы ты поступил?», «Какие тут могут быть риски?».*

*· Безопасная среда: Четко обозначьте в начале: «Здесь нет глупых вопросов и ответов. Мы учимся на ситуациях, а не оцениваем друг друга».*

*3. Ссылки на ресурсы для углубленного изучения:*

*· Проект «Роскомнадзор: Персональные данные.дети».*

*· «Урок цифры» — уроки по безопасности для старших классов.*