апрель, 2025

методические рекомендации

по организации в ХМАО-Югре информационно-просветительского проекта для родителей и специалистов «Будем рядом»

Проект реализуется при поддержке Федерального агентства по делам молодёжи (Росмолодёжь) в рамках реализации федерального проекта «Россия — страна возможностей» национального проекта «Молодежь и дети»

Департамент молодежной политики, гражданских инициатив и внешних связей Югры

О!ЮГРА молодёжный центр

Будем рядом

80 Победа!

Россия – страна возможностей

БУДЕМ РЯДОМ

Методические материалы для проведения профилактических мероприятий по предупреждению криминальных угроз в сфере информационно-коммуникационных технологий, интернет-мошенничества и киберпреступности

ЦИФРОВОЙ ЩИТ: ПРОФИЛАКТИКА КИБЕРМОШЕННИЧЕСТВА СРЕДИ МОЛОДЕЖИ

Разработано в рамках Всероссийского информационно-просветительского проекта "Будем рядом"

СОДЕРЖАНИЕ

Разработано в рамках Всероссийского
информационно-просветительского проекта "Будем рядом"

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

По данным УМВД России по Ханты-Мансийскому автономному округу – Югре, в последние годы в регионе зафиксировано значительное число случаев кибермошенничества с участием молодежи. Молодые люди активно используют интернет для общения, учебы и развлечений, но часто не осознают рисков, связанных с цифровой средой. Распространение фишинга, социальной инженерии и финансовых афер подчеркивает необходимость повышения цифровой грамотности среди молодежи региона.

АНО «Молодежный центр Югры» при поддержке Комиссии по делам несовершеннолетних и защите их прав при Правительстве Ханты-Мансийского автономного округа – Югры, Департамента молодежной политики, гражданских инициатив и внешних связей Ханты-Мансийского автономного округа – Югры с 2024 года реализует Всероссийский информационно-просветительский проект «Будем рядом».

Проект направлен на обеспечение родителей и специалистов необходимыми знаниями, навыками и ресурсами для эффективного воспитания, профилактики деструктивного поведения и поддержки позитивного развития детей и молодежи. Проект реализуется через различные каналы коммуникации, включая еженедельные подкасты с экспертами на темы профилактики эмоционального выгорания у родителей, девиантного поведения детей, вредных зависимостей у подростка, жизненных ориентиров, эффективных способов разрешения конфликтов с детьми, безопасности подростков, формирования безопасной и счастливой семейной среды и других вопросов, актуальных для родителей детей всех возрастов. Проект реализовывается в рамках национального проекта «Молодежь и дети».

Ссылки на Проект в социальных сетях: https://t.me/budem_ryadom_ugra, https://vk.com/myryadomdlyavas.

Цель методического материала

Сформировать у молодежи навыки безопасного поведения в цифровой среде через развитие критического мышления и осведомленности о киберугрозах.

Задачи

1. Повысить осведомленность о распространенных схемах кибермошенничества.
2. Научить распознавать потенциальные угрозы в интернете.
3. Развить способность анализировать информацию и принимать осознанные решения.
4. Выработать алгоритм действий при столкновении с киберугрозами.
5. Способствовать формированию привычки безопасного использования технологий.
6. Снизить уязвимость молодежи к манипуляциям в цифровой среде.

Ожидаемые результаты

1. Рост уровня цифровой грамотности среди молодежи.
2. Снижение числа случаев вовлечения в киберпреступления как жертв.
3. Формирование привычки проверять информацию перед действиями в интернете.
4. Развитие навыков самостоятельной защиты от киберугроз.

Разработано в рамках Всероссийского информационно-просветительского проекта "Будем рядом"

2. ВОЗРАСТНАЯ АДАПТАЦИЯ МАТЕРИАЛА

Для подростков (14-17 лет)

Акцент: Социальные сети и онлайн-игры как основные зоны риска.

Подход: Игровые элементы, короткие занятия (45 минут – 1 час).

Примеры: Угрозы в популярных приложениях (например, фишинг в соцсетях).

Для молодежи (18-24 года)

Акцент: Финансовая безопасность и реальные случаи мошенничества.

Подход: Разбор кейсов, обсуждения (1-1,5 часа).

Примеры: Защита банковских данных, анализ афер с «инвестициями».

Для молодых специалистов (25-35 лет)

Акцент: Защита рабочих данных и профессиональной репутации.

Подход: Практические тренинги, аналитика (1,5-3 часа).

Примеры: Предотвращение утечек в рабочей среде, фишинг на корпоративную почту.

Разработано в рамках Всероссийского информационно-просветительского проекта "Будем рядом"

3. МЕТОДИКА ПРОВЕДЕНИЯ МЕРОПРИЯТИЙ

Методичка предлагает три формата мероприятий – интерактивную игру «Кибердетектив», форсайт-сессию «Безопасное цифровое будущее» и квест «Цифровой след». Каждый формат сочетает практические задания и обсуждения для формирования навыков защиты от кибермошенничества.

Задачи, решаемые в рамках мероприятий

1. Повышение осведомленности о типах киберугроз (фишинг, социальная инженерия).
2. Развитие навыков анализа цифровых угроз и принятия решений.
3. Формирование алгоритмов действий в ситуациях риска.
4. Стимулирование критического отношения к информации в интернете.

Область применения

— когда нужно повысить цифровую грамотность без морализаторства;

— когда требуется практическая отработка навыков защиты от киберугроз;

— когда важно вовлечь молодежь в обсуждение актуальных рисков.

Целевая аудитория

Рекомендуемое количество участников: 15-20 человек (максимум 25).

Разработано в рамках Всероссийского информационно-просветительского проекта "Будем рядом"

Длительность мероприятия

Время проведения: 1-3 часа (в зависимости от формата и возрастной группы).

Ресурсы

- Просторное помещение.
- Устройства с доступом в интернет (для квеста).
- Карточки с кейсами, флипчарты, маркеры, стикеры.

4. ТЕХНОЛОГИЧЕСКАЯ КАРТА МЕРОПРИЯТИЯ

Цель: обеспечить четкую организацию мероприятия для эффективного проведения.

Элемент	Описание
Максимальное количество участников	До 25 человек (оптимально 15-20). При большем числе – разделение на группы с дополнительным ведущим.
Рассадка	Стулья в форме круга или полукруга для обсуждений. Свободное пространство в центре для активностей (например, квеста или игры).
Подготовка помещения	Аудитория мин. 30 м², хорошая вентиляция. Столы для команд (при необходимости), место для флипчартов.
Материалы и оборудование	Карточки с кейсами (для «Кибердетектива»). Флипчарты, маркеры, стикеры (для «Форсайт-сессии»). Устройства с интернетом и чат в соцсетях (для «Квеста»). Бумага, ручки, часы. Раздаточные материалы (памятки, тесты).
Время подготовки	20-30 минут (расстановка мебели, проверка оборудования, раздача материалов).
Роли и обязанности	Ведущий: объясняет правила, модерирует, следит за временем. Помощник (при необходимости): раздает материалы, помогает с техникой.

Примечание: при превышении 25 участников используйте два этапа или подгруппы с отдельными ведущими.

Разработано в рамках Всероссийского информационно-просветительского проекта "Будем рядом"

5. Ход мероприятия

I.Подготовка

Кто может проводить мероприятие?

Педагог-психолог, специалист по работе с молодежью, социальный педагог, педагог дополнительного образования.

Каких участников привлекать?

Все желающие соответствующей возрастной категории.

Организация пространства

1. Стулья в кругу или полукругу, свободное пространство в центре.

2. Подготовлены материалы и оборудование в зависимости от формата.

II. Проведение

Вводная часть (15-20 минут)

Цель: создать комфортную атмосферу, познакомить участников и настроить на работу.

1. **Приветствие (2-3 минуты)**

Ведущий: «Здравствуйте! Сегодня мы собрались на мероприятие «Цифровой щит», чтобы узнать, как защитить себя от кибермошенников. Здесь важно ваше мнение и опыт. Давайте познакомимся и начнем!»

2. **Айсбрейкер: «Кто я?» (5-7 минут)**

Описание: каждый называет имя и одно слово, характеризующее его (например, «Аня – музыка»).

Цель: быстрое знакомство, снятие напряжения.

Ресурсы: не требуется, проводится в кругу.

Разработано в рамках Всероссийского информационно-просветительского проекта "Будем рядом"

3. **Упражнение для групповой динамики: «Общее дело» (5-7 минут)**

Описание: участники за 1 минуту находят общее увлечение (например, «мы любим соцсети»). При большой группе – деление на подгруппы по 5-7 человек.

Цель: создать ощущение команды.

Ресурсы: не требуется.

4. **Объяснение формата и правил (3-5 минут)**

Ведущий: «Мы будем работать в одном из трех форматов: игра «Кибердетектив», форсайт-сессия или квест «Цифровой след». Вы будете анализировать ситуации, обсуждать угрозы и искать решения. Главное – уважать мнение друг друга. Правила: говорит один человек, используем «Я-высказывания», все мнения важны.

Основная часть (60-90 минут)

Формат выбирается ведущим в зависимости от группы и целей:

1. **Интерактивная игра «Кибердетектив» (60 минут)**

Вводная часть (10 минут): деление на команды (3-5 человек), раздача карточек с кейсами, просмотр ролика о киберугрозах (1-2 минуты).

Основная часть (35 минут): команды анализируют 3 кейса, определяют признаки мошенничества, тип угрозы и действия. Ведущий дает подсказки (например, «Проверьте адрес сайта»).

Заключительная часть (15 минут): презентация выводов, обсуждение, раздача памяток.

Примеры кейсов:

Для подростков 14-17 лет: «Сообщение в соцсети: «Ты выиграл подписку, введи данные»» (фишинг).

Для молодежи 18-24 года: «Звонок: «Ваша карта заблокирована, назовите код»» (социальная инженерия).

Для молодых специалистов 25-35 лет: «Письмо от «ИТ-отдела»: обновите доступ по ссылке» (фишинг).

2.**Форсайт-сессия «Безопасное цифровое будущее» (90 минут)**

Вводная часть (15 минут): обзор киберугроз, деление на группы (5-7 человек).

Основная часть (60 минут):

Этап 1 (25 минут): Прогноз угроз через 1, 3, 5 лет (запись на флипчартах).

Этап 2 (15 минут): Личные уязвимости участников.

Этап 3 (20 минут): План защиты (на стикерах).

Заключительная часть (15 минут): презентация планов, обобщение.

3. **Квест «Цифровой след» (70 минут)**

Вводная часть (10 минут): инструктаж, деление на команды (по желанию).

Основная часть (45 минут): 7 заданий через чат или оффлайн:

— создание надежного пароля (например, «Зима2025Югра»);

— распознавание поддельных сайтов (например, «sberrbank.ru»);

— противодействие манипуляциям (например, звонок «из банка»);

— защита профиля в соцсетях;

— безопасность финансовых данных;

— настройка защиты устройств;

— действия при угрозе.

Заключительная часть (15 минут): итоги, награждение (например, памятками).

Разработано в рамках Всероссийского информационно-просветительского проекта "Будем рядом"

Упражнение для динамики: «Передай мяч» (опционально, 5 минут)

Описание: ведущий бросает мяч и задает вопрос (например, «Что важнее – удобство или безопасность?»). Участник отвечает и передает мяч.

Цель: разрядка напряжения.

Ресурсы: мяч.

Перечень вопросов для обсуждения (для всех форматов):

Для подростков 14-17 лет:

1. Я люблю пробовать новые приложения (разминочный).
2. Соцсети – это весело (разминочный).
3. Ссылки с призами в соцсетях безопасны.
4. Скачивать файлы из чатов – это нормально.
5. Если друг просит денег в чате, надо помочь.
6. Пароль «1234» подходит для игр.
7. Мошенники не трогают подростков.
8. Сообщать данные по телефону – это безопасно.
9. Проверка сайтов – это лишняя трата времени.
10. Интернет безопасен, если быть осторожным.

Для молодежи 18-24 года:

1. Мне нравится узнавать новое в интернете (разминочный).
2. Онлайн-шопинг удобен (разминочный).
3. Звонки "из банка" – это нормально.
4. Инвестиции в интернете всегда выгодны.
5. Поддельные сайты легко распознать.
6. Код из СМС можно сообщать по телефону.
7. Мошенники не могут взломать карту.
8. Проверка адреса сайта необязательна.

Разработано в рамках Всероссийского информационно-просветительского проекта "Будем рядом"

9. Финансовая безопасность важнее удобства.
10. Интернет-аферы – это редкость.

Для молодых специалистов 25-35 лет:

1. Я люблю современные технологии (разминочный).
2. Работа онлайн удобна (разминочный).
3. Письма с просьбой обновить доступ безопасны.
4. Взлом рабочего аккаунта – это не моя проблема.
5. Сообщать пароль коллеге по чату – нормально.
6. Мошенники не трогают рабочие данные.
7. Защита устройств – это лишние хлопоты.

Заключительная часть (20-30 минут)

Участники садятся в круг. Ведущий задает вопросы для рефлексии: Что нового узнали о киберугрозах? Изменилось ли ваше отношение к безопасности в интернете? Какие действия запомнили для защиты? Что было самым полезным?

Упражнение «Одно слово» (5 минут): каждый называет слово, отражающее вывод (например, «осведомленность»).

III. Анализ результатов

Ведущий фиксирует реакции на кейсы и задания. Отмечает усвоенные навыки и популярные заблуждения.

Разработано в рамках Всероссийского информационно-просветительского проекта "Будем рядом"

6. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ВЕДУЩИХ

Подготовка к мероприятию

1. Изучите актуальные данные о киберпреступлениях в регионе (например, сайт УМВД).
2. Ознакомьтесь с кейсами из раздела 7 и приложений.
3. Подготовьте оборудование: устройства, карточки, флипчарты.
4. Адаптируйте задания под группу (соцсети для подростков, финансы для молодежи).
5. Проверьте доступность чата для квеста (разрешенные соцсети).

Проведение мероприятия

1. Используйте нейтральный тон, избегая запугивания.
2. Поощряйте участников делиться опытом.
3. Следите за временем, помогайте при затруднениях.
4. Поддерживайте уважительную атмосферу.
5. Закрепляйте знания через вопросы и раздаточные материалы.

Оценка эффективности

1. Проведите тест до и после (Приложение 3).
2. Соберите обратную связь через анкету.
3. Проанализируйте ошибки в кейсах и усвоенные алгоритмы.

Разработано в рамках Всероссийского информационно-просветительского проекта "Будем рядом"

7. ИНФОРМАЦИОННЫЕ МАТЕРИАЛЫ

1. Памятка «Как защититься от кибермошенников».
2. Тест «Проверка знаний о кибербезопасности» .

8. ПРИЛОЖЕНИЯ

Приложение 1: Памятка «Как защититься от кибермошенников».

Приложение 2: Тест «Проверка знаний о кибербезопасности».

Приложение 3: Ответы на частые вопросы.

Приложение 4: Нормативно-правовая база по профилактике киберпреступности.

Все приложения к методическим рекомендациям
можно найти по QR-коду:

Разработано в рамках Всероссийского
информационно-просветительского проекта "Будем рядом"