Методическое сопровождение внеклассного мероприятия

«Правовое поле цифрового гражданина»

Старшеклассники и студенты СПО — не просто пользователи сети, а полноценные цифровые граждане, несущие ответственность за свои действия в правовом поле. Мероприятие выходит за рамки бытовой безопасности и поднимает вопросы цифровой этики, права, личного бренда и социальной ответственности. Акцент делается на будущее: поступление, карьера, финансовая и репутационная безопасность.

Цель: Сформировать у старшеклассников комплексное представление о безопасности в сети как о сочетании правовой, финансовой, репутационной и психологической грамотности, а также стимулировать профессиональное самоопределение в сфере IT.

Задачи:

· Проанализировать долгосрочные последствия цифрового следа для образовательных и карьерных перспектив.

· Отработать навыки противодействия сложным формам мошенничества (финансового, с использованием социальной инженерии).

· Обсудить правовые границы допустимого поведения в сети (кибербуллинг, экстремизм, авторское право).

· Познакомить с профессиями в сфере кибербезопасности и цифрового права.

Метапредметные и личностные результаты:

· Развитие критического и прогностического мышления (оценка долгосрочных рисков).

· Формирование правосознания и гражданской позиции в цифровой среде.

· Повышение финансовой и медиаграмотности.

· Развитие навыков публичной дискуссии, аргументации и ведения переговоров (в моделируемых ситуациях).

Возрастные особенности и формат

· 10-11 класс, 1-2 курс СПО (16-18 лет): Мировоззренческий уровень. Эффективны форматы, где они выступают в роли экспертов, аналитиков, стратегов.

· Формат: Деловая игра, симуляция, стратегическая сессия, дискуссия

· Тон: Взрослый, партнерский. Признание их компетенции в пользовательском опыте и перевод этого опыта в системное знание.

· Принцип: «Не страх, а стратегия». Не «что нельзя», а «какие возможности и риски это несет и как ими управлять».

Материалы и подготовка

· Технические: Ноутбуки/телефоны для командной работы (поиск правовой информации, создание презентаций), проектор, таймер.

· Раздаточные:

· Папки с кейсами (подробными, на 2-3 страницы).

· Выдержки из законов (ФЗ-152 «О персональных данных», ст. 128.1 УК РФ «Клевета», ст. 282 УК РФ «Возбуждение ненависти», ГК РФ об авторском праве).

· Чек-листы для аудита цифрового следа.

· Памятки «Цифровой антикризисный план».

· Экспертный компонент: Желательно привлечение внешних экспертов (юрист, HR-специалист, представитель вуза, психолог-конфликтолог).

Данное мероприятие соответствует требованиям ФГОС СОО, способствует формированию правовой и финансовой культуры, готовит учащихся к осознанному профессиональному выбору и жизни в условиях цифровой экономики, развивая навыки стратегического мышления и управления рисками.

ПРИМЕРНЫЙ СЦЕНАРИЙ ВНЕКЛАССНОГО МЕРОПРИЯТИЯ

Тема: «Кибербезопасность 2.0: Стратегия, право, репутация»

Целевая аудитория:10-11 классы, 1-2 курс СПО

Форма:Стратегическая деловая игра в формате «кризисного совещания».

Время:60-80 минут.

Ведущий/Модератор:Классный руководитель / учитель обществознания или права / приглашенный эксперт.

ХОД МЕРОПРИЯТИЯ

I. Пролог: «Входящая угроза» (5-7 мин)

· На экране — стилизованное заставка с логотипом условной компании «Future You Inc.».

· Вступительное слово модератора: «Добрый день. Я рад приветствовать вас на стратегическом совещании. Сегодня мы — не ученики. Вы — совет директоров компании "Future You Inc.", активы которой — ваше время, ваши данные, ваша репутация и ваши будущие возможности. Только что нам поступил входящий сигнал о комплексной кибератаке на наши активы. Наша задача за час — разработать антикризисный план по четырем ключевым фронтам. Готовы принять вызов?»

· Формирование «кризисных групп» (команд) по 4-5 человек: Группы формируются случайно или по интересам. Каждая получает папку с одним из четырех сложных кейсов.

II. Работа «кризисных групп» (30-35 мин)

Группы работают параллельно. Задача: за 25 минут проанализировать кейс, используя предоставленные материалы (выдержки из законов, статистику), и подготовить 3-минутный брифинг для «совета директоров» с рекомендациями: 1) Немедленные действия, 2) Стратегические меры, 3) Превенция на будущее.

Кейс 1: ФРОНТ РЕПУТАЦИИ («Цифровой след и карьера»)

· Ситуация: Кандидат на позицию стажера в крупной IT-компании прошел все собеседования. HR перед оформлением проводит глубокий аудит соцсетей за 5 лет. Обнаружены: радикальные политические посты в 14 лет (сейчас 17), участие в хейт-обсуждениях, нецензурная лексика, фото с вечеринок с сомнительным

контентом. Результат — отказ. Кандидат в шоке: «Это же было давно и в личном профиле!».

· Задачи для группы:

1. Проанализировать правомерность действий HR с точки зрения закона и этики.
2. Разработать инструкцию по «цифровой гигиене» для абитуриента/соискателя.
3. Предложить шаги по «реабилитации» уже существующего цифрового следа.

Кейс 2: ФИНАНСОВЫЙ ФРОНТ («Социальная инженерия и мошенничество»)

· Ситуация: Студент получил звонок от «сотрудника банка»: данные карты якобы скомпрометированы. Звонивший знал ФИО, последние 4 цифры карты, адрес. Для «защиты» нужно назвать код из SMS, перевести деньги на «технический счет» через мобильное приложение под диктовку, а также установить программу «удаленного доступа» для «настройки безопасности». Результат — опустошенная карта и кредит, взятый на его имя.

· Задачи для группы:

1. Разобрать схему мошенничества, выделив этапы манипуляции.
2. Составить максимально подробный алгоритм действий при подобном звонке (что проверить, что сказать, куда обратиться).
3. Предложить способы защиты персональных данных, которые могли привести к утечке.

Кейс 3: ПРАВОВОЙ ФРОНТ («Границы дозволенного: шутка или преступление»)

· Ситуария: В школьном чате как шутка было распространено fake-видео с учителем в компрометирующей ситуации, созданное в нейросети. Видео быстро ушло в публичный доступ. Учитель подал заявление в полицию. Авторы (выпускники) утверждают, что это был просто «прикол».

· Задачи для группы:

1. Квалифицировать возможные составы преступлений/правонарушений (клевета, оскорбление, неправомерный доступ к информации).
2. Оценить последствия для создателей (уголовная/административная ответственность, гражданский иск о возмещении морального вреда).
3. Сформулировать правила цифрового общения, разграничивающие юмор и нарушение закона.

Кейс 4: ПСИХОЛОГИЧЕСКИЙ ФРОНТ («Кибербуллинг и информационная гигиена»)

· Ситуация: Успешный блогер-старшеклассник стал объектом скоординированной травли со стороны хейтеров: массовые негативные комментарии, создание унижающих мемов, доксинг (публикация адреса), фейковые аккаунты с оскорбительным контентом от его имени. Начались панические атаки, выгорание.

· Задачи для группы:

1. Разработать пошаговый план для жертвы: технический (блокировки, жалобы), юридический (фиксация, обращение в правоохранительные органы), психологический.
2. Предложить стратегию поведения для сообщества подписчиков/друзей.
3. Обсудить меры превенции: как выстроить личные границы и психологическую устойчивость при публичной деятельности.

III. Стратегическая сессия: Презентация брифингов (15-20 мин)

· Каждая группа представляет свой анализ и рекомендации. Выступление строго регламентировано (3-4 минуты).

· После каждого выступления — короткие вопросы от других групп и модератора на уточнение.

· Модератор выполняет роль суммирующего эксперта: дополняет правовыми нюансами, приводит реальные примеры из судебной практики, обращает внимание на упущенные аспекты.

IV. Выработка «Кодекса цифрового гражданина» и рефлексия (10-15 мин)

· На основе всех презентаций модератор предлагает сформулировать ключевые принципы.

· Совместное заполнение итоговой схемы/памятки на экране или ватмане:

· Принцип осознанности: Мои действия в сети имеют долгосрочные последствия.

· Принцип верификации: Любую информацию, особенно финансовую, проверяю по официальным каналам.

· Принцип правовой определенности: Знаю границы шутки и правонарушения.

· Принцип цифровой гигиены: Регулярно проверяю настройки приватности и очищаю цифровой след.

· Принцип солидарности: Не остаюсь безучастным к кибербуллингу, знаю, как помочь.

· Профориентационная минутка: Модератор кратко перечисляет профессии, связанные с рассмотренными кейсами: киберследователь, digital-юрист, специалист по digital-репутации, HR-аналитик, кризис-менеджер в соцсетях, психолог в сфере кибербезопасности. Дает ссылки на профильные ресурсы (например, «Проектория», «Урок Цифры» для старших классов).

· Заключительная рефлексия «Незаконченное предложение»: «Сегодня я осознал, что...», «Самым полезным для моего будущего стало...», «Я планирую изменить в своем онлайн-поведении...».

· Раздача итоговых материалов: Памятки «Аудит цифрового следа за 30 минут», контакты правовой и психологической помощи (включая специализированные киберправовые сервисы).

Приложения к сценарию

1. Памятка для старшеклассника «Цифровой антикризисный план»:

· **До... (Превенция):**
1. Аудит: Погугли себя. Удали/скрой компрометирующий контент.
2. Настройки: Максимальная приватность в соцсетях. Разные сложные пароли + 2FA везде.
3. Финансы: Отдельная карта для онлайн-платежей с небольшим лимитом. Никогда — CVV-код и коды из SMS.
4. Юмор: Перед отправкой спроси: «А если это увидит декан/работодатель/полиция?».
· **Во время... (Реакция):**
1. Стоп: Не паниковать, не отвечать агрессору/мошеннику.
2. Скриншот: Фиксация всего (сообщения, транзакции, логи).
3. Блок: Бан, жалоба платформе.
4. Оповещение: Сообщить близким, если затронуты они; в банк — если деньги; в полицию — если угрозы/шантаж/фейки.
· **После... (Восстановление):**
1. Анализ: Как данные утекли? Устранить брешь.
2. Помощь: Обратиться к психологу, если травма.
3. Репутация: При необходимости — работа с экспертами по digital-репутации.

2. Рекомендации ведущему (педагогу/модератору):

·Экспертная позиция: Если вы не специалист в IT-праве, не бойтесь сказать: «Мой экспертный комментарий как педагога... Юридические детали мы уточним в предоставленных материалах/спросим у приглашенного эксперта». Лучше сосредоточиться на модерации дискуссии.

·Работа с сопротивлением: Возможны комментарии «Мне все равно, что там найдут», «Это нарушает мою свободу». Аргументируйте не моралью, а прагматикой: «Твое право. Это риск, которым можно управлять или игнорировать. Давай просчитаем потенциальные издержки этого выбора для твоих конкретных целей».

Конфиденциальность и безопасность: Кейсы острые. Подчеркните, что обсуждение ведется в учебных целях. Если кто-то захочет поделиться личной историей, перенаправьте обсуждение в общие принципы, а после мероприятия предложите индивидуальную беседу.