



РЕГИОНАЛЬНАЯ ИННОВАЦИОННАЯ ПЛОЩАДКА

государственное бюджетное профессиональное образовательное учреждение Самарской области "Богатовский государственный сельскохозяйственный техникум имени Героя Советского Союза Смолякова Ивана Ильича"

Методическая разработка классного часа

«Цифровые деньги и безопасность: как не стать жертвой мошенников»

Выполнила:

**Чешко Татьяна Николаевна
преподаватель первой
квалификационной категории**

Тема: «Цифровые деньги и безопасность: как не стать жертвой мошенников» (с разбором схем обмана, правил цифровой гигиены и блоком про цифровые рубли; с участием медиаторов РИП).

Целевая аудитория: студенты СПО (2 курса, по профессии «Мастер сельскохозяйственного производства»).

Продолжительность: 90 минут.

Формат: интерактивное занятие с элементами дискуссии, групповой работы и ролевой практики.

Цели и задачи

Цель: сформировать у студентов навыки распознавания мошеннических схем в финансовой сфере и устойчивые привычки цифровой гигиены, дать базовые знания о цифровых рублях и их особенностях с точки зрения безопасности.

Задачи:

- познакомить с понятием «цифровые деньги», кратко раскрыть природу безналичных, электронных и цифровых рублей;
- разобрать актуальные схемы мошенничества (телефонные, мессенджеры, «ложные инвестиции», фишинг, дропперство);
- отработать алгоритмы безопасного поведения при подозрительных предложениях и звонках;
- закрепить правила цифровой гигиены (пароли, двухфакторная аутентификация, проверка ссылок);
- дать чёткие ориентиры, куда обращаться при попытке мошенничества;
- вовлечь медиаторов РИП в модерацию дискуссий и разбор кейсов.

Планируемые результаты

- **Знания:** студенты понимают, что такое цифровые рубли, чем они отличаются от привычных безналичных денег, знают типовые схемы обмана и признаки опасности.
- **Умения:** распознают признаки мошенничества, умеют корректно прервать разговор/диалог, знают, как проверить информацию и куда сообщить о подозрительном случае.
- **Личностные результаты:** формируется критическое мышление, ответственность за личные финансы и данные, готовность обращаться за помощью.

Оборудование и материалы

- мультимедийный комплекс (проектор/экран, колонки);
- презентация (слайды с признаками мошенничества, схемами, памяткой);
- короткие видеоролики/скриншоты (примеры фишинговых писем, поддельных сайтов, «звонков из банка»);
- карточки с кейсами для групповой работы;

- «Памятка цифровой гигиены» (вывести на экран для совместного заполнения);
- флипчарт/доска, маркеры.

Ход занятия

1. Вводная часть (15 минут)

Деятельность педагога:

- Приветствие, обозначение темы и её актуальности (статистика кибермошенничества, рост числа атак на молодёжь).
- Быстрый мини-опрос: «С какими подозрительными звонками/сообщениями вы сталкивались?» (2–3 коротких примера от студентов).
- Постановка проблемы: «Почему даже умные люди попадают на уловки мошенников?» (кратко о психологии манипуляций: срочность, страх, “выгода”).

Роль медиаторов РИП: помогают фиксировать ответы студентов, мягко направляют обсуждение, следят, чтобы никто не высмеивал чужой опыт («это не про глупость, это про то, как устроены ловушки»).

Ключевой тезис для старта: «Безопасность в цифровой среде — это не “если”, а “когда” тебе придёт подозрительное сообщение. Важно знать алгоритм действий».

2. Блок «Цифровые рубли: что это и как с ними безопасно» (15 минут)

Содержание:

- **Что такое цифровые рубли.** Это третья форма российской валюты (наличные, безналичные, цифровые). Хранятся на платформе Банка России, а не на счёте в коммерческом банке.
- **Чем отличаются.** Упор на то, что **Банк России никогда не звонит гражданам** и не предлагает «перевести деньги на цифровой счёт по телефону». Любые такие предложения — мошенничество.
- **Мифы и манипуляции.** Мошенники могут использовать тему «цифровизации» и «перевода на цифровые рубли» как предлог для выманивания данных, кодов, установки вредоносных приложений.
- **Как узнать достоверную информацию.** Официальные источники: сайт Банка России, портал «Финансовая культура».

Форма подачи: мини-лекция + разбор 2–3 «объявлений/сообщений», где мошенники прикрываются «цифровыми рублями». Студенты называют признаки обмана (срочность, требование кода, «звонок от ЦБ», обещание бонусов за «быстрый перевод»).

Роль медиаторов РИП: модерировать вопросы, помогают формулировать «красные флаги» и фиксируют их на флипчарте.

3. Разбор актуальных схем мошенничества (20 минут)

Основные схемы (с примерами):

- **«Звонок из “службы безопасности банка”».** Сценарий: «с вашей карты идёт перевод», «нужно срочно назвать код из СМС». Алгоритм защиты: положить трубку, перезвонить в банк по номеру с карты.
- **«Выигрыш/подарок/возврат денег».** Требование «оплатить комиссию/налог/ доставку» или ввести данные карты на «сайте возврата».
- **«Работа с переводами» (дропперство).** «Нужно получать деньги и отправлять дальше, это просто посредничество». Объяснение: это участие в обналичивании преступных средств, уголовная ответственность.
- **Фишинг.** Поддельные сайты, похожие на банки/маркетплейсы; письма «от Госуслуг» с просьбой ввести логин/пароль. Признаки: ошибки в адресе сайта, срочность, «уникальное предложение».
- **Мессенджеры и соцсети.** «Друг просит срочно перевести деньги», «выиграли приз в конкурсе группы». Проверка: позвонить человеку, не переходить по ссылкам.

Интерактив: показ 2–3 скриншотов/коротких роликов. Студенты в парах называют 3–4 признака мошенничества. Медиаторы РИП собирают ответы и выводят «Топ-5 самых частых уловок».

4. Практический блок: групповая работа и ролевые игры (20 минут)

Групповая работа (3–4 группы по 4–6 человек):

Каждой группе выдаётся кейс (см. примеры ниже). Задача:

1. определить схему и цель мошенника;
2. назвать 2–3 признака обмана;
3. составить безопасный алгоритм действий (что сказать/сделать);
4. сформулировать 1 вопрос к «эксперту» (медиатору РИП), если есть неясности.

Примеры кейсов:

- Кейс 1. «Вам одобрен кредит на выгодных условиях. Для активации нажмите ссылку и введите данные карты».
- Кейс 2. «Здравствуйте, я из ЦБ. Идёт перевод на цифровой рубль, назовите код из СМС для подтверждения».
- Кейс 3. «Ваш друг пишет в мессенджере: “Скинь 5000 рублей, потом всё объясню, срочно!” и даёт ссылку на “возврат”.»
- Кейс 4. «Работодатель предлагает “лёгкий заработок”: получать деньги на карту и переводить дальше, комиссия 10%».

Ролевая игра (5–7 минут):

В каждой группе один студент играет «мошенника», другой — «потенциальную жертву», остальные — наблюдатели. Задача «жертвы» — корректно прервать диалог и предложить безопасный способ проверки. Задача наблюдателей — назвать 2 приёма манипуляции, которые использовал «мошенник».

Роль медиаторов РИП: выступают модераторами групп, помогают уточнить формулировки, подводят итоги по каждой группе, фиксируют «лучшие фразы для отказа» (например: «Я перезвоню в банк по официальному номеру», «Не сообщаю коды из СМС никому»).

5. Правила цифровой гигиены и памятка (10 минут)

Совместно с группой и медиаторами РИП формируется «Памятка цифровой гигиены» (выводится на экран/флипчарт):

- Никогда не сообщайте коды из СМС/пуш-уведомлений, CVV/пин-коды.
- Не переходите по ссылкам из сомнительных сообщений, проверяйте адрес сайта.
- Используйте двухфакторную аутентификацию.
- Регулярно обновляйте приложения и ОС.
- Проверяйте информацию через официальные источники.
- Если сомневаетесь — положите трубку и позвоните в банк/организацию по номеру с официального сайта.

Медиаторы РИП помогают ранжировать пункты по «самой частой ошибке» и «самому простому действию».

6. Заключительная часть (10 минут)

- Рефлексия: «Одно правило, которое я точно запомнил(а)» (каждый называет по 1 пункту).
- Информация о том, куда обращаться: банк, полиция (112), портал «Финансовая культура», горячие линии по кибербезопасности.
- Раздача/показ QR-кода на памятку (если подготовлена в электронном виде).
- Благодарность медиаторам РИП за участие и модерацию.

Роль медиаторов РИП

Чтобы участие медиаторов было содержательным, распределяются роли на:

- **Модератор групп:** следит за временем, помогает формулировать выводы, не даёт обсуждению уйти в эмоции.
- **Эксперт по безопасности:** отвечает на сложные вопросы, даёт короткие уточнения по правовым аспектам (например, про ответственность за дропперство).
- **Фасилитатор рефлексии:** помогает студентам сформулировать «что я сделаю иначе», переводит опыт в конкретные действия.