

## ФИНАНСОВАЯ БЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Кузнецова Елена Геннадьевна, преподаватель

КГБПОУ «Канский политехнический колледж»

В современном мире финансовые технологии развиваются стремительно: цифровые платежи, онлайн-банкинг и мобильные приложения стали неотъемлемой частью повседневной жизни. Однако вместе с удобством они несут и новые риски — число случаев финансового мошенничества растёт из года в год.

Студенты активно пользуются банковскими картами, мобильными приложениями для переводов, сталкиваются с рекламой инвестиционных возможностей. При этом у них зачастую нет достаточного опыта и знаний, чтобы распознать угрозу мошенничества.

Особую тревогу вызывает тот факт, что молодые люди могут невольно стать соучастниками преступлений — например, в схемах дроппинга (отмывания денег через подставные счета). Уголовная ответственность за подобные действия наступает с 16 лет, а по особо тяжким преступлениям — с 14 лет.

Таким образом, формирование навыков финансовой безопасности — не просто полезный навык, а жизненная необходимость для современной молодёжи.

Урок разработан на основе материалов официального просветительского ресурса «Мои финансы».

Дидактическая цель:

- сформировать у студентов компетенции, необходимые для распознавания и предотвращения ситуаций финансового мошенничества, повысить уровень финансовой безопасности подростков;
- познакомить с актуальными видами финансового мошенничества (дроппинг, вишинг, мошенничество с использованием QR-кодов), их механизмами и признаками;
- отработать алгоритмы безопасного поведения в типовых ситуациях (телефонный звонок от «службы безопасности банка», подозрительное сообщение с QR-кодом, предложение «лёгкого заработка» через дроппинг).

Развивающая цель: развить критическое мышление и навыки анализа финансовых предложений, научить выявлять «красные флаги» мошеннических схем.

Воспитательная: сформировать ответственное отношение к собственным финансам и персональным данным, понимание правовых последствий участия в сомнительных финансовых схемах, снизить вероятность вовлечения студентов в мошеннические схемы в качестве жертв или невольных соучастников.

## ТЕХНОЛОГИЧЕСКАЯ КАРТА УРОКА

№ слайда или дидакт. материал	Деятельность преподавателя	Деятельность студентов	Тайминг
	Приветствует студентов общим обращением: «Добрый день, ребята! Рада вас видеть!»; - визуально проверяет явку и внешний вид обучающихся; - фиксирует отсутствующих в журнале; - создаёт доброжелательную рабочую атмосферу «Сегодня у нас интересный материал, уверена, будет полезно!»	Приветствуют преподавателя, настраиваются на учебную деятельность, переключают внимание с внешних дел на урок	2 мин.
<b>ЭТАП 1: ПРЕДСТАВЛЕНИЕ И АНАЛИЗ ПРАКТИЧЕСКОЙ СИТУАЦИИ, СВЯЗАННОЙ С ФИНАНСОВОЙ БЕЗОПАСНОСТЬЮ</b>			
Слайд 1 Слайд 2 Представление темы, название урока	Представление темы: Финансовая безопасность в эпоху цифровых технологий		1 мин.
Слайд 3	Введение в тему: «С попытками мошенничества в 2025 году столкнулся 94% россиян, годом ранее – 82%. Посмотрите на экран, обратите внимание на статистику. Растет количество ситуаций мошенничества. С ростом доли тех, кто сталкивается с попытками мошенничества, растет и вариативность способов, которыми злоумышленники пытаются обмануть людей».	Слушают (и смотрят на слайд).	1 мин
Слайд 4  Приложение № 7	Продолжает введение в тему, проговаривает определение финансового мошенничества, обращает внимание на наказание и подчеркивает, что уголовная ответственность наступает с 16 лет, а по особо тяжким преступлениям – с 14 лет. Задает вопрос аудитории: «Какие виды финансового мошенничества вы знаете?»  Если есть верный ответ от аудитории:	Слушают (и смотрят на слайд).   Отвечают на вопрос, комментируют	2 мин.

№ слайда или дидакт. материал	Деятельность преподавателя	Деятельность студентов	Тайминг
	<p>«Все верно, но инструментарий злоумышленников, к сожалению, широк, а мы в рамках нашего занятия остановимся на трех видах мошенничества: дроппинг, вишинг и мошенничество с использованием QR-кода. Если мы посмотрим статистику, результаты опросов и оценки Банка России по объему операций без согласия клиентов, то мы увидим, что именно эти три вида мошенничества постепенно выходят на первый план».</p> <p>Если нет ответа или иные (неправильные) ответы от аудитории, то коротко говорит сам о том, что есть такие виды, как мошенничество с картами, в интернете, финансовые пирамиды. И продолжает: «Более подробно сегодня остановимся на следующих видах мошенничества: дроппинг, вишинг и мошенничество с использованием QR-кода. Если мы посмотрим статистику, результаты опросов и оценки Банка России по объему операций без согласия клиентов, то мы увидим, что именно эти три вида мошенничества постепенно выходят на первый план».</p>	<p>варианты ответов: вишинг, фишинг, фарминг, кликфорд, мошенничество с банковскими картами и т. п. (см Приложение № 7).</p> <p>Если затрудняются ответить, преподаватель может подсказать и перейти к выбранным видам.</p>	
Слайд 5	<p>Предлагает изучить информацию на слайде:</p> <p>«Давайте более подробно остановимся на относительно новом виде мошенничества – дроппинге. Это вовлечение в схему отмыwania денег. Преподаватель действует по ситуации, может спросить у класса, знакомы ли они с этим понятием. Или сразу может перейти к его объяснению:</p> <p>«Посмотрите на схему финансового обмана, представленную на слайде. Основная особенность дропа в том, что он является связующим звеном между жертвой и злоумышленником, позволяя пользоваться своим банковским счетом.</p> <p>Схем вербовки выявлено немало: дроповод, как называют мошенника, может представиться работником органов безопасности, сотрудником банка, работодателем, ошибившимся человеком.</p> <p>Поднимите руку те, кто сталкивался с подобными ситуациями или слышал о них.</p> <p>Давайте подытожим: в нынешних реалиях человек может даже не подозревать, что попал в преступную схему как посредник по передаче</p>	<p>Слушают объяснения преподавателя. Делятся своими представлениями о том, что такое дроппинг.</p>	2 мин.

№ слайда или дидакт. материал	Деятельность преподавателя	Деятельность студентов	Тайминг
	денег, но при этом будет считаться преступником. А банки с полицией передают данные о нем в единую базу данных Банка России о дропах».	Поднимают руку те, кто сталкивался или слышал.	
Слайд 6	<p>Обращает внимание на слайд:  «Следующий вид мошенничества, который мы рассмотрим, это вишинг. Это форма финансового мошенничества, когда злоумышленники используют телефонные звонки и голосовые сообщения, чтобы обманом заставить жертву раскрыть конфиденциальную информацию, такую как номера счетов, пароли и данные карт, для доступа к его деньгам.  В 2023 году такой вид мошенничества стал самым распространенным. Вишинговых схем существует тоже достаточно много, наиболее известные – это звонки лжесотрудников органов безопасности и банков, звонки из call-центров, выгодные предложения и т. д. Человек сообщает свои данные и тем самым дает мошеннику доступ к своим денежным средствам.  Поднимите руку те, кто сталкивался с подобными ситуациями или слышал о них».</p>	<p>Слушают (и смотрят на слайд).</p> <p>Поднимают руку те, кто сталкивался или слышал, могут коротко поделиться опытом.</p>	2 мин.
Слайд 7	<p>«Последний вид финансового мошенничества, который мы сегодня рассмотрим, – это мошенничество с использованием QR-кода, сгенерированного для кражи денег у ничего не подозревающих людей.  Схем мошенничества с QR-кодами тоже достаточно много. С чем можно столкнуться в повседневной жизни? Это может быть снятие денег с карты или со счета; «кража» QR-кода в магазине, на листовках с объявлениями, со скидками, акциями и т. п.; в ресторанах и кафе: поверх настоящего QR-кода мошенники приклеивают собственный; на поддельных квитанциях на оплату коммунальных платежей.  Когда человек проходит по коду, не проверяя ссылку, или проходит по ссылке на коде не через официальное приложение (например при аренде самоката), тем самым он дает доступ злоумышленникам к средствам на своем счете – в результате услуга не оплачена, а средства переведены мошеннику».</p>	Слушают (и смотрят на слайд).	2 мин.

№ слайда или дидакт. материал	Деятельность преподавателя	Деятельность студентов	Тайминг
	<p>Если у учащихся есть мобильные телефоны, предлагает пройти по QR-коду на экране и узнать, куда он ведет.</p> <p>Продолжает:            «Поднимите руку те, кто совершал платежи с помощью QR-кода?»            Смотрит на поднятые руки, комментирует.            «Теперь, когда мы обсудили основные особенности дроппига, вишинга и мошенничества с QR-кодами, предлагаю провести игру».</p>	<p>Сканируют и проходят по QR-коду на экране, видят предупреждение «Осторожно, мошенники!»</p> <p>Поднимают руку те, кто совершал платеж с помощью QR-кода. Могут давать комментарии.</p>	
<b>ЭТАП 2: ДЕТЕКТИВНАЯ ИГРА</b>			
<p>Слайд 8</p> <p>Приложение № 1</p> <p>Таймер</p>	<p>Знакомит с правилами игры, выдает приложение № 1 каждой команде и предупреждает, что есть ограничение по времени для принятия решения:            «Каждая команда – это успешное и амбициозное детективное агентство. Детективное агентство 1, 2, 3, 4» – показывает на каждую команду, называя их номер.</p> <p>«Давайте посмотрим предлагаемую легенду и решим детективную задачу по выявлению мошенничества. В каждом туре у вас будет информация, которую нужно быстро изучить, написать ответ по форме и отдать его помощнику.</p> <p>Итак, приступим!</p> <p>На первый тур вам дается 10 минут.</p> <p>История игры: «В нашем городе участились случаи финансового мошенничества, причем пострадавшими в основном стали школьники и студенты. Четыре успешных детективных агентства города получили запрос на расследование нескольких случаев и выявление основных признаков такого мошенничества. Мэр города хочет осуществить проект по созданию бота-помощника для распознавания таких видов мошенничества. Для этого нужны результаты работы лучших из лучших детективов города. Приступим же к расследованию».</p>	<p>Команды знакомятся с правилами игры, историей и легендой для агентств, получают приложение № 1.</p>	<p>10 мин.</p>

№ слайда или дидакт. материал	Деятельность преподавателя	Деятельность студентов	Тайминг
Слайд 9 Приложение № 2 Таймер	<p>Командам на слайде выводится предыстория персонажей и их действий. Им выдаются карточки с описаниями героев (приложение № 2), дополнительно карточки выводятся на слайд.</p> <p>Преподаватель знакомит с карточками персонажей (не зачитывает, обращает внимание на экран, пока помощник выдает их каждой команде): «На экране задача для команд: нужно определить, кто из героев находится в зоне риска финансовых мошенников. Возможно, что таких героев несколько. Ответ пишем по форме, указанной на экране. За каждый правильный ответ дается 1 балл. Подводить итоги будем после того, как все задачи будут решены».</p>	<p>Команды изучают карточки (приложение 2), обсуждают написанный текст, определяют, кто находится в зоне риска, оформляют ответы по предложенному образцу и сдают помощнику .</p>	10 мин.
Слайд 10 Приложение № 5 ИЛИ Приложение № 4 Таймер	<p>Продолжает и предупреждает, что есть ограничение по времени для принятия решения: «Переходим ко второму туру. Командам на слайде выводится задача второго тура.</p> <p>Следующая часть легенды: Наши герои спокойно обедали, каждый за своим столиком, думая о планах на ближайшее время. Внезапный звонок сорвал этот настрой, и пришлось резко вникать в суть разговора. Но не все собеседники оказались доброжелательными, кто-то из них – злоумышленник. Вам предоставлена часть аудиозаписи звонков. Выделите, какой из них от финансового мошенника – дропа, а какой – от вишера». Итак, нужно внимательно слушать предлагаемые аудиофрагменты. На работу командам дается 10 минут. На экране задача для команд, нужно прослушать записи и распознать дроппинг и вишинг. Возможно, что таких ситуаций и телефонных разговоров несколько. Ответ запишите по форме, указанной на экране».</p> <p>Преподаватель включает по очереди 5 аудиофрагментов (приложение № 5). Между прослушиванием рекомендуется пауза в 10–15 секунд.</p> <p><i>В случае невозможности прослушивания нужно воспользоваться раздаточным материалом с текстом звонков (приложение № 4).</i></p>	<p>Смотрят на экран.</p> <p>Команды слушают записи, обсуждают, оформляют ответы по предложенному образцу и сдают помощнику.</p> <p>В случае невозможности прослушивания читают распечатку текстов звонков (приложение № 4), обсуждают, оформляют ответы по предложенному образцу и сдают помощнику.</p>	10 мин.

№ слайда или дидакт. материал	Деятельность преподавателя	Деятельность студентов	Тайминг
Слайды 11–12, 13  Приложение № 3 Таймер	Продолжает, раздает приложение № 3 и предупреждает, что есть ограничение по времени для принятия решения: «Переходим к третьему туру. Произошли следующие события: обеденный перерыв заканчивается, и нужно спешить по делам. Наши герои за время обеда успели заказать те или иные товары и услуги. Для оплаты требуемого было предложено использовать QR-код. Кому же из героев мы скажем: «Стоп, не делай этого, это может быть мошенническая схема, и ты потеряешь свои деньги»? Итак, нужно внимательно прочитать, что предлагается сделать героям. На работу командам дается 5 минуты. Возможно, что таких ситуаций несколько. Ответ пишем по форме, указанной на экране».	Команды смотрят на слайды.  Команды изучают приложение № 3, оформляют ответы по предложенному образцу и сдают помощнику .	5 мин.
<b>ЭТАП 3: ТВОРЧЕСКАЯ МАСТЕРСКАЯ</b>			
Слайд 14  Приложение 6 Таймер	Преподаватель продолжает, раздает приложение № 6 и предупреждает, что есть ограничение по времени для принятия решения: «А мы завершаем нашу игру, и, пока мой коллега подсчитывает итог, мы с вами вспомним, что вы, детективные агентства, приглашены мэром города и по итогу оценки различных ситуаций можете дать важные рекомендации. Вы же помните, что мэр города хочет осуществить проект по созданию бота-помощника для распознавания таких видов мошенничества. Для этого нужны результаты работы лучших из лучших детективов города. Теперь со знанием дела предложите мэру свои идеи. Ваша задача – дать вводные для будущего бота – распознавателя таких видов мошенничества. Внимание на экран: вы видите алгоритм, который вам предстоит заполнить. Представим ситуацию, когда с вами связался в сети или с помощью телефона собеседник, который предоставил важную финансовую информацию. Как можно распознать мошенничество в этом случае? Опишите три ситуации: по одному примеру дроппинга, вишинга и мошенничества с QR-кодами, указав, по какому признаку распознать и что делать, если столкнулись с таковым. Предлагаются три пространства:	Командам на слайде выводится задача и выдается приложение 6.  Команды обсуждают, оформляют ответы по предложенному образцу, выбирают выступающего.	10 мин.

№ слайда или дидакт. материал	Деятельность преподавателя	Деятельность студентов	Тайминг
	<p>телефон, соцсети и объявление на бумаге. Но вы можете указать и свои пространства, если хотите. У вас 10 минут».</p> <p>Пока команды готовят результаты, помощник проводит подсчет ответов по трем турам игры и предоставляет информацию преподавателю. Продолжает: «Итак, можем обсудить, какие же алгоритмы наши детективные агентства предлагают для создания бота».</p> <p>Для сокращения времени, можно предложить такой вариант обсуждения: первая команда рассматривает подробно три ситуации, вторая, третья и четвертая – дополняют еще не озвученные ситуации, признаки и рекомендации по действиям.</p>	<p>От каждой команды выступает участник, который предлагает к обсуждению три ситуации, признаки и рекомендации по действиям.</p>	
	<p>Кейс-задание с обсуждением</p> <p>Слайд с ситуацией: «Анна получила SMS: „Ваша карта заблокирована. Позвоните по номеру...“. Она занервничала и позвонила. „Сотрудник банка“ убедил её взять кредит на 300 тыс. руб. и перевести деньги на „безопасный счёт“. Через неделю Анна узнала, что стала жертвой мошенников. Вопрос: Могла ли Анна заранее снизить риск такой ситуации с помощью Госуслуг? Если да, то как?»</p>	<p>обсуждают кейс 5 минут, затем представляют свои версии. Преподаватель дополняет и раскрывает тему самозапрета.</p>	5 мин.
	<p>Кто-нибудь из вас слышал о возможности установить самозапрет на получение кредитов через Госуслуги? Поднимите руку, если знаете об этой услуге. Кто может кратко рассказать, в чём её суть? А кто знает, как именно её оформить? Если никто не знаком с этой опцией — не страшно: мы подробно разберём её сегодня, потому что это один из самых эффективных инструментов защиты от мошенников».</p>	Высказываю суждения	8 мин.
	<p>Демонстрирует видео Как установить самозапрет на кредиты <a href="https://vk.com/video-73442711_456239730">https://vk.com/video-73442711_456239730</a></p>	Смотрят	3 мин.
	<p>Самозапрет на кредиты позиционируется как инструмент защиты от необдуманных займов и мошенников. Однако у этой меры есть и</p>	Высказывают суждения	5 мин

№ слайда или дидакт. материал	Деятельность преподавателя	Деятельность студентов	Тайминг
	противники. В чём, на ваш взгляд, заключаются главные аргументы «за» и «против» широкого внедрения самозапрета? Как вы оцениваете его потенциальную пользу для общества и отдельных граждан?		
<b>ЭТАП 4: ПОДВЕДЕНИЕ ИТОГОВ И РЕФЛЕКСИЯ</b>			
Слайд 15 С ответами	Преподаватель переходит к слайду с ответами: «Подводим итоги. Давайте посмотрим правильные ответы на задание 1-го тура. В зоне риска у нас три героя, цветом выделены те признаки, которые позволили это определить. Как же справились с этим наши агентства?» Объявляет набранные баллы 1-го тура.	Обсуждают критерии, выделенные командами, изучают правильные ответы и результаты команд.	2 мин.
Слайды 16–17 С ответами	Продолжает подведение итогов: «Далее обратим внимание на результаты второго тура, тут надо было выявить дроппинг и вишинг. Вот эти герои столкнулись с мошенниками. Как же справились с этим наши агентства?» Объявляет набранные баллы 2 тура.	Обсуждают критерии, выделенные командами, изучают правильные ответы и результаты команд.	2 мин.
Слайд 18 С ответами	Продолжает подведение итогов: «Переходим к результатам третьего тура. Ответы и герои у вас на экране, цветом выделены важные признаки, благодаря которым можно было выявить финансовое мошенничество. Как же справились с этим наши агентства?» Объявляет набранные баллы 3-го тура.	Обсуждают критерии, выделенные командами, изучают правильные ответы и результаты команд.	2 мин.
Слайд 19	Завершает подведение итогов: «И, наконец, пришло время объявить итоговые результаты работы наших детективных агентств». Объявляет победителей.	Смотрят и обсуждают итоговые результаты команд.	2 мин
Слайд 20	Преподаватель проводит этап рефлексии, получает обратную связь. Резюмирует: «Мы с вами изучили сегодня три вида финансового мошенничества, которые могут угрожать финансовой безопасности в жизни современного человека. Давайте проведем короткую рефлексию: опишите одним словом свое впечатление от занятия. Назовите, что для вас стало на уроке «словом дня»».	Обучающиеся предлагают свои варианты «слова дня».  По желанию отвечают на вопросы преподавателя, называя в произвольном порядке любую	2 мин

№ слайда или дидакт. материал	Деятельность преподавателя	Деятельность студентов	Тайминг
	<p>проводит развернутую рефлексию с обсуждением основных понятий, признаков и способов опознания мошеннических схем.</p> <p>Задает вопросы:</p> <p>«Что вы поняли сегодня:</p> <p>О том, что такое дроппинг, вишинг, мошенничество с QR-кодами?</p> <p>О том, по каким признакам можно распознать мошенническую схему?</p> <p>О том, как защитить себя и не поддаться на уловки мошенников?»</p> <p>Дает обратную связь отвечающим на вопросы, повторяя кратко сказанное студентами.</p> <p>Не дает оценок. Не ставит отметок.</p>	<p>информацию из слайдов и комментариев преподавателя.</p>	
<p>Слайды 21–24 «Что можно сделать, чтобы повысить свою финансовую грамотность»</p>	<p>«Обратите внимание, что сюжеты, связанные с финансовой грамотностью, часто встречаются в классической литературе. Прочитав эти книги, вы можете по-новому взглянуть на сюжет.</p> <p>Если же вы хотите проверить свои знания по финансовой грамотности, здесь вы можете увидеть список тематических олимпиад, в которых вы можете участвовать».</p> <p>Обращает внимание на информацию, размещенную на слайдах 21–22, о дополнительных ресурсах по финансовой грамотности: мультфильмах, подкастах, которые можно посмотреть и послушать вместе со своими родителями.</p> <p>Тем, кому интересна тема финансовой грамотности, рекомендует обратиться к информации на портале <a href="http://moiфинансы.рф">moiфинансы.рф</a>, на котором размещено много полезных образовательных и информационных материалов, и к социальным сетям портала.</p>	<p>Смотрят на слайды, делают фото ссылок.</p> <p>Задают дополнительные вопросы преподавателю.</p>	<p>2 мин</p>

## Приложение 1. История и легенда для детективных агентств



### **ИСТОРИЯ**

В нашем городе участились случаи финансового мошенничества, причем пострадавшими в основном стали школьники и студенты. Четыре успешных детективных агентства города получили запрос на расследование нескольких случаев и выявление основных признаков такого мошенничества.




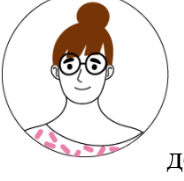
Мэр города хочет осуществить проект по созданию бота-помощника для распознавания таких видов мошенничества. Для этого нужны результаты работы лучших из лучших детективов города. Приступим же к расследованию.

### **ЛЕГЕНДА ДЛЯ ДЕТЕКТИВНЫХ АГЕНТСТВ**

Кафе «Кукольное чаепитие» – излюбленное место встречи молодежи нашего района. Тут много столиков, приятная атмосфера, доброжелательный персонал и возможность заниматься своими делами в коворкинг-зоне.

Рядом с кафе находятся колледж, школа и центр подготовки и детского творчества, а потому в кафе нет отбоя от посетителей – школьников и студентов. Но сегодня в кафе произошло неприятное событие, которое впоследствии было определено как финансовое мошенничество.

Приложение 2. Карточки с описанием героев

<p>Марина</p>  <p>Девушке 17 лет, она выпускница 11 А школы № 117, в кафе появляется периодически, когда требуется пообедать или дождаться встречи с репетиторами из центра подготовки. Мечта – стать медицинским работником. Скроллинг считает неинтересным, в кафе в процессе ожидания читает только несколько полезных блогов.</p>	<p>Алексей</p>  <p>В свои 20 лет он учится в техническом вузе и подрабатывает графическим дизайнером, обожает технические новинки и копит на дорогостоящее профоборудование. Активно пользуется СБП. В обеденный перерыв в кафе занимается поиском новых заказов «на просторах Интернета», откликается на все вакансии в соцсетях и иных ресурсах, оставляя свой телефон и ФИО.</p>
<p>Мурат</p>  <p>Учится вместе с Алексеем, планирует открывать свой бизнес и изучает на досуге цифровые инструменты, которые помогут управлять будущим бизнес-проектом. В кафе постоянно разговаривает по телефону.</p>	<p>Виолетта</p>  <p>Ей 22 года, и она хочет стать профессиональным киберспортсменом, обожает соревновательные головоломки, в кафе обязательно подключается к общественному бесплатному Wi-Fi и проверяет интересующие ее беседы в сетевых сообществах, совершает финансовые переводы.</p>
<p>Данила</p>  <p>Одноклассник Марины, любитель долгих телефонных разговоров, которые не прекращает и в обеденный перерыв. Странник открытого общения – даже с тем, кто ошибся номером, может проговорить полчаса. Любит спорт, ежедневно совершает пробежку и посещает спортзал. Частый посетитель кафе, любит там назначать встречи своим многочисленным знакомым и просто посидеть за чашкой чая и смартфоном.</p>	<p>Лилия</p>  <p>Любительница фотографировать еду, заказываемую в кафе, и делиться фото со своими подписчиками. Хочет стать профессиональным фотографом. Очень любит моду, находит удовольствие в поиске и покупке необычных и модных вещей и украшений. В обеденный перерыв занимается сравнением найденных вещиц по стоимости и условиям покупки на разных ресурсах.</p>

### Приложение 3. Карточки с предложением совершить платеж с использованием QR-кода



#### **Алексей**

Алексею прислали сообщение, в котором предлагают перейти по ссылке на страничку продавца графических планшетов, так как он оставлял заявку на приобретение и свой номер на сайте. Ему рекомендуют изучить технические характеристики, и если все подходит, то подъехать в магазин для совершения покупки. Также в сообщении указано, что если он проведет оплату по QR-коду, то сможет воспользоваться скидкой в 5%.



#### **Данила**

Даниле в соцсети пришло сообщение с QR-кодом, что только сейчас, перейдя по нему, он сможет практически бесплатно оформить слот на забег «Бежать нельзя остановиться», о котором он мечтал, но не мог себе позволить из-за нехватки денежных средств. Однако предложение ограничено, поэтому нужно действовать максимально быстро.



#### **Мурат**

Мурату прислали сообщением инструкцию по блокировке транзакций из банка N: «Уважаемый Мурат! 30 минут назад с вашего счета пытались снять большую сумму денег. Зайдите в приложение банка, сформируйте QR-код и отправьте его скриншот на этот номер. Это необходимое действие для отмены операции. С уважением, служба безопасности банка N».



#### **Лилия**

Увидев модную заколку, только появившуюся в очередном интернет-магазине, она тут же ее заказала. Оплату магазин предложил произвести при помощи QR-кода, присланного продавцом. Лилия зашла в мобильное банковское приложение, увидела ссылку на нужный ресурс и перевела необходимую сумму, дав свое разрешение на транзакцию.



#### **Виолетта**

Виолетте принесли счет за обед, она оплатила его картой и решила оставить чаевые официанту. Для этого нужно отсканировать QR-код, который ведет на страничку кафе, где перечислены официанты (есть фотография каждого сотрудника, указаны фамилия, имя и отчество), и выбрать нужного работника.



#### **Марина**

Марине пришло сообщение в соцсети от близкой подруги, что она только что нашла ее фотографии с дня рождения, их разместили на странице кафе, где проходил праздник. Для быстрого перехода подруга прислала Марине картинку с QR-кодом, который действует 10 минут.

## Приложение 4. Тексты полученных звонков<sup>1</sup>



### 1. Марина поговорила с администратором центра репетиторства:

Добрый день, Марина. Вам звонят из центра репетиторства. Вы наш постоянный и любимый клиент. Напишите, пожалуйста, несколько отзывов на пройденные в течение последнего месяца занятия. За отзывы вам положено вознаграждение. Для перевода денежных средств мне нужно вас внести в базу, назовите свои фамилию, имя, отчество, номер банковской карты и CVC. Деньги поступят вам сразу после опубликования отзывов.



### 2. Алексей поговорил с потенциальным работодателем:

Здравствуйте, Алексей. Да, мы предлагаем вам интересную работу в IT-сфере, начнете работать и получать высокую оплату труда. Вы ведь видели отзывы в соцсети? Это новый и очень популярный инвестпроект, где ваши навыки очень пригодятся, быстро сделаете карьеру. Договор, конечно, мы с вами заключим, а теперь давайте поговорим про риски и проценты с вознаграждения. Видите, условия очень хорошие, нам просто нужны молодые и активные сотрудники. Да, для работы, так как проект растет, вам потребуется завести пять банковских карт У вас есть предпочтения по банкам? Проект активный, каждый день нужно будет получать платежи и совершать с них транзакции членам нашей команды, это позволяет нарастить инвестиционные возможности и заработать, с каждой транзакции ваши – 10%. Да, возможно, потребуется отдельный номер телефона для обеспечения большего доступа к проекту. Приступить можете с понедельника.



### 3. Данила поговорил с «другом друга»:

Привет, Данила, это Максим. Мы с тобой не знакомы, я друг Марины. Она сказала, что ты нуждаешься в подработке. Мы сейчас как раз ищем сотрудника. Работа достаточно легкая и не занимает много времени, но нужно быть внимательным. Я буду ежедневно перечислять на твою карту определенную сумму, а ты – снимать и отдавать человеку, который вечером будет приезжать к тебе. Суммы небольшие, но, чтобы не вызвать подозрения у сотрудников банка, нам нужны люди для проведения этих нехитрых операций. Но при этом 5% от суммы ты можешь оставить себе, это твое вознаграждение за оперативность. Все абсолютно законно и безопасно. Если ты знаешь еще кого-нибудь, нуждающегося в подработке, то скажи мне, я свяжусь с этим человеком. Но только нужны ответственные люди, которые умеют работать быстро.



### 4. Лилия ответила на звонок от потенциального работодателя:

Добрый день, Лилия, наше агентство заинтересовали ваши фотографии, у вас неплохой блог, все эстетично, мы хотели бы пригласить вас на работу. Для начала вам необходимо оформить страничку одного нашего продукта в соцсети. Мы посмотрим, как это повлияет на продажи, тогда заключим с вами договор, оплата будет зависеть от того, насколько быстро будет расти аудитория, а компания – получать прибыль. Как вы понимаете, это отличная возможность показать свой талант людям и стать востребованным специалистом. Нам очень хотелось бы с вами сотрудничать.



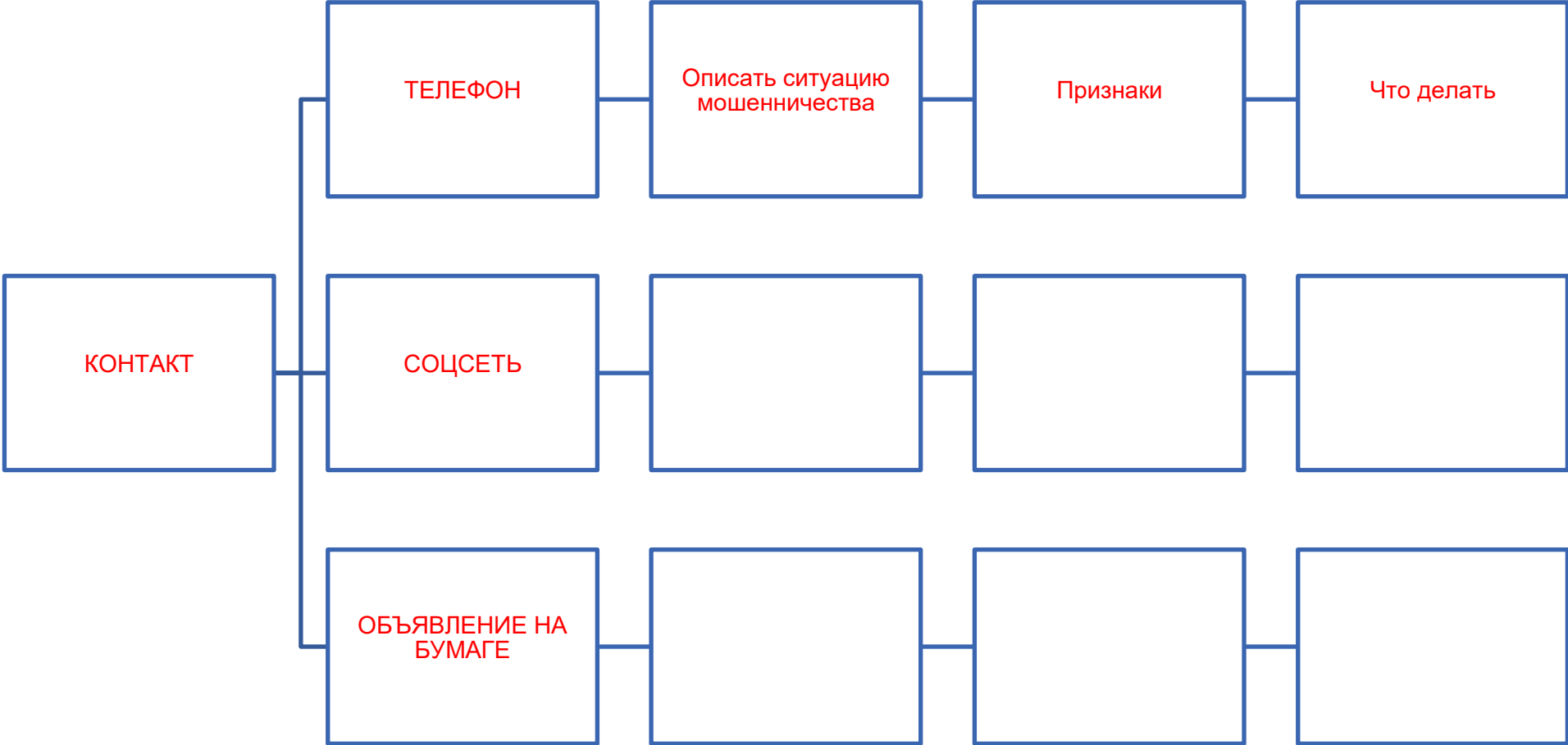
### 5. Виолетта поговорила с представителем банка:

Добрый день, Виолетта, вам звонят из службы безопасности банка N, к нам поступила информация, что по вашему счету обнаружены подозрительные транзакции, для проверки данных вашего счета необходимо срочно установить программу

<sup>1</sup> Применяется в случае отсутствия возможности прослушать аудиозаписи

удаленного управления мобильным банкингом, чтобы сотрудники банка могли получить доступ и обезопасить вас. Если это не сделать сейчас, то ваш счет заблокируют.

Приложение 6. Задача для бота



## Приложение 7

### ЭТАП 1: ПРЕДСТАВЛЕНИЕ И АНАЛИЗ ПРАКТИЧЕСКОЙ СИТУАЦИИ, СВЯЗАННОЙ С ФИНАНСОВОЙ БЕЗОПАСНОСТЬЮ

На этом этапе преподавателю важно оперировать терминологией.  
Подсказки по терминологии для преподавателя

Какие виды финансового мошенничества вы знаете?

Варианты мошенничества, которые могут назвать студенты

Вид мошенничества	Определение
Фишинг	Получение конфиденциальных данных о банковской карте (номер, ПИН-код) путем рассылки электронных писем об изменениях в системе безопасности банка и необходимости предоставить информацию по карте.
Фарминг	Это более продвинутая версия фишинга, заключающаяся в переводе пользователей на фальшивый веб-сайт и краже конфиденциальной информации.
Золото Лимпопо (Нигерийские письма)	Это вид интернет-мошенничества, когда злоумышленник пытается выманить у пользователя деньги или получить доступ к его банковскому счёту.
Злой близнец	Это кибер-атака, при которой хакер создает поддельную точку доступа Wi-Fi, имитирующую подлинную беспроводную сеть, к которой могут подключаться пользователи. Как только пользователь подключается к такой сети «злого близнеца», хакеры могут получить доступ к данным пользователя: от его сетевого трафика до личных регистрационных данных.
Снифферинг	Это способ мошенничества, при котором злоумышленник использует анализатор проходящего трафика Интернет-сети («сниффер») – специальную компьютерную программу для перехвата данных с возможностью их декодирования и анализа. Снифферинг особенно популярен в людных местах, везде, где есть общедоступная сеть wi-fi.
Кликджекинг	Это технология обмана пользователей Интернета, при котором мошенник получает доступ к конфиденциальной информации или к компьютеру пользователя. Например, на странице пользователя поверх видимых элементов располагают невидимые, и пользователь, совершая клик, подписывается на какую-то группу.
Кликфорд	Это разновидность мошенничества в сети (мошенническое нажатие) в виде обманых кликов на рекламные ссылки, которые совершают лица, не заинтересованные в рекламном объявлении. Такого рода ложные клики повышают расходы рекламодателя на показы объявлений. От кликфорда владельцы рекламных сетей могут потерять доверие рекламодателей и прибыль.
Семь кошельков	Один из видов мошенничества в сети, когда пользователь получает письмо с предложением перевести небольшую сумму на несколько электронных кошельков в надежде на то, что следующие участники

Вид мошенничества	Определение
	тоже перечислят деньги на электронные кошельки, среди которых будет указан и его электронный кошелек. Гарантия получения денег в свой электронный кошелек полностью отсутствует.
Смишинг	Это вид мошенничества, при котором пользователь получает СМС-сообщение, в котором с виду надежный отправитель просит указать какую-либо ценную персональную информацию (например, пароль или данные кредитной карты).
Скимминг	Кража данных с банковской карты путем установки на банкомат специального считывающего устройства с накладной клавиатурой и (или) миниатюрной камеры для записи ввода ПИН-кода.
Траппинг	Мошенничество с целью получения банковской карты путем установки в банкомате устройства, не возвращающего карту из банкомата, а также информации о ПИН-коде
Шимминг	Усовершенствованный вид скимминга. В банкомат помещается устройство меньшего размера. Это устройство, толщиной не больше человеческого волоса, очень трудно обнаружить. Но шиммер не умеет считывать ПИН-код.

Что такое финансовое мошенничество?

Финансовое мошенничество — совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения

Что грозит за мошенничество?

Штраф в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года; обязательные работы на срок до трехсот шестидесяти часов; исправительные работы на срок до одного года; ограничение свободы на срок до двух лет; принудительные работы на срок до двух лет; арест на срок до четырех месяцев; лишение свободы на срок до двух лет.

Что такое дроппинг?

Дроппинг – вербовка в схему отмывания денег.

Кто такой дроп (или дроппер)?

Дроп – подставное лицо, задействованное в нелегальных схемах по обналичиванию денег.

Что такое вишинг?

Вишинг – это форма финансового мошенничества, когда злоумышленники используют телефонные звонки и голосовые сообщения, чтобы обманом заставить жертву раскрывать конфиденциальную информацию, такую как номера счетов, пароли и данные карт для доступа к его деньгам.

Что такое мошенничество с использованием QR-кода?

Мошенничество с использованием QR-кода – использование сгенерированного QR-кода для кражи денег у ничего не подозревающих людей.

Что такое бот-помощник?

Бот-помощник – это виртуальный ассистент, который отвечает на однотипные вопросы. Обычно FAQ-боты используются на сайтах, в приложениях или мессенджерах.

## ЭТАП 2: ДЕТЕКТИВНАЯ ИГРА

На этом этапе преподавателю важно отслеживать тайминг, но давать какие-то пояснения уже нельзя, все пояснения – при подведении итогов.

## ЭТАП 3: ТВОРЧЕСКАЯ МАСТЕРСКАЯ

На этом этапе преподавателю важно донести информацию, что требуется составить алгоритм и внести в прилагаемую схему. По заданию предлагаются три пространства – телефон, соцсети и объявление на бумаге. Но преподаватель не ограничивает команды, можно указать и свои пространства, если команды понимают, какую ситуацию могут предложить.

Важно по трем направлениям (пространствам) описать ситуацию мошенничества, указать ее признаки и предложить вариант, что делать человеку в данной ситуации.

Возможные варианты (в дополнение к тем, которые предложены в заданиях трех туров, т. к. команды будут в первую очередь вдохновляться ими):

Пространство	Ситуация	Признаки	Действия
Телефон	Позвонил «сотрудник безопасности банка» и предложил предоставить QR-код из мобильного приложения, чтобы «обезопасить» свои средства.	Это мошенничество с использованием QR-кода: 1) QR-код фактически является поручением банку на выдачу денег без ввода ПИН-кода, и настоящие сотрудники банка никогда не попросят у клиента такие данные.	— Следить за безопасностью QR-кодов. — С осторожностью относиться к статическим кодам. — С осторожностью относиться к электронным меню в кафе и ресторанах.
Объявления на бумаге	Мошенник наклеил поверх официального QR-кода свой, фальшивый. Герой отсканировал его в уверенности, что оплачивает покупку или услугу, а на самом деле перечислил деньги мошенникам.	2) QR-код при оплате ведет на какой-то неизвестный ресурс. 3) Мошенник торопит с оплатой с помощью QR-кода, ставит сроки действия.	— Не спешить активировать QR-код на смартфоне по пути или в очереди в кассу. Лучше сделать это непосредственно в момент покупки.
Телефон	Звонят под видом сотрудников банков, сообщают о якобы несанкционированном запросе на снятие денег со счета и просят прислать QR-код, чтобы отменить операцию. Получив код, мошенники снимают по нему деньги в банкоматах со счета жертвы.	Это дроппинг: 1) Предлагается посредничество в переводе или обналичивании поступивших средств.	— Не сообщать никому данные своей банковской карты. — Не передавать свою карту третьим лицам.
Телефон	Герою внезапно пришло на счет мобильного телефона 3 тыс. рублей. После этого позвонил человек и объяснил, что ошибся с адресатом. Попросил перевести 2500 руб. на номер карты, а 500 руб. оставить себе.		
Соцсеть	Написал контакт из списка друзей и предложил работу.		

Пространство	Ситуация	Признаки	Действия
	Должность администратора «лотереи». Нужно рассылать выигрыши победителям. Герой «устроился на работу» и каждый день делал по несколько переводов, оставляя себе вознаграждение в 3% от суммы.	2) Предлагается процент за эту «работу».	<ul style="list-style-type: none"> <li>— Не соглашаться перевести деньги по реквизитам по просьбе неизвестных лиц.</li> <li>— Не соглашаться снимать деньги в банкомате для кого-то.</li> <li>— Сообщать о подозрительных просьбах в Банк России и полицию.</li> </ul>
Телефон	Позвонил «сотрудник технической поддержки известной компании». Сказал, что зарегистрирована подозрительная активность в аккаунте жертвы и нужно подтвердить данные своего аккаунта. Для этого требуется установить обновленное программное обеспечение. После этого телефон заблокирован и средств на счету не осталось.	<p>Это вишинг:</p> <ul style="list-style-type: none"> <li>1) Звонящий утверждает, что он из государственного учреждения.</li> <li>2) Наличие срочности.</li> <li>3) Звонящий просит вас подтвердить данные вашего счета или аккаунта.</li> </ul>	<ul style="list-style-type: none"> <li>— Не отвечать на звонки с неизвестных номеров.</li> <li>— Не делиться своей персональной информацией по телефону.</li> <li>— Запросить документ, удостоверяющий личность.</li> <li>— Изменить пароли к аккаунтам.</li> <li>— Уведомить банк об инциденте и тщательно следить за финансовыми операциями.</li> </ul>
Соцсеть	В социальной сети вы увидели рекламу интересного вам предложения. Вы перешли по указанной в ней ссылке. Но после этого увидели тот самый «синий экран» с якобы системным сообщением о возникшей проблеме. В конце сообщения значится телефон службы поддержки клиентов. Звонок, разумеется, бесплатный. Расстроившись и испугавшись перспективы покупки новой дорогой техники, вы звоните по указанному номеру. Вам отвечает доброжелательный оператор, задаёт стандартные для такой ситуации вопросы. Он может даже предложить выполнить какие-то действия, только они ничем не помогут.		

Пространство	Ситуация	Признаки	Действия
	<p>После этого «техподдержка» приходит к «выводу»: проблема серьёзная и грозящая тяжёлыми последствиями. Например, удалением всех данных. Ваш собеседник знает выход, но эта услуга уже платная. Для оплаты вас просят продиктовать данные карты.</p>		

## ЭТАП 4: ПОДВЕДЕНИЕ ИТОГОВ И РЕФЛЕКСИЯ

Преподаватель переходит к слайду с ответами: «Подводим итоги. Давайте посмотрим правильные ответы на задание 1 тура. В зоне риска у нас три героя, цветом выделены те признаки, которые позволили это определить. Как же справились с этим наши агентства?»

**Объявляет набранные баллы 1 тура.**

Преподаватель, демонстрируя ответы, обращает внимание на признаки, позволяющие выбрать героев, находящихся в зоне риска финансового мошенничества:

Герой	Его описание	Комментарии
Алексей	В свои 20 лет он учится в техническом вузе и подрабатывает графическим дизайнером, обожает технические новинки и копит на дорогостоящее профоборудование. Активно пользуется СБП. В обеденный перерыв в кафе занимается поиском новых заказов «на просторах интернета», откликается на все вакансии в соцсетях и иных ресурсах, оставляя свой телефон и ФИО.	Максимально небезопасно оставлять в соцсетях и иных ресурсах свой телефон и ФИО и другие контактные данные. Можно стать жертвой как вишинга, так и дроппинга (так как пользуется СБП, значит использует свой номер телефона).
Виолетта	Ей 22 года, и она хочет стать профессиональным киберспортсменом, обожает соревновательные головоломки, в кафе обязательно подключается к общественному бесплатному Wi-Fi и проверяет интересующие ее беседы в сетевых сообществах, совершает финансовые переводы.	Максимально небезопасно, подключаясь к общественному бесплатному Wi-Fi, совершать большое количество разнообразных финансовых переводов – есть риск, что данные будут использованы мошенниками.
Данила	Одноклассник Марины, любитель долгих телефонных разговоров, которые не прекращает и в обеденный перерыв. Сторонник открытого общения – даже с тем, кто ошибся номером, может проговорить полчаса. Любит спорт. Частый посетитель кафе, любит там назначать встречи своим многочисленным знакомым и просто посидеть за чашкой чая и смартфоном.	Как указано, Данила даже с тем, кто ошибся номером, может проговорить полчаса. Вспомните – первый совет, который дается при ситуации контакта с мошенниками, – не разговаривать с незнакомыми собеседниками.

Максимальное количество баллов – 3 балла.

Продолжает подведение итогов: «Далее обратим внимание на результаты второго тура, тут надо было выявить дроппинг и вишинг. Вот эти герои столкнулись с мошенниками. Как же справились с этим наши агентства?»

**Объявляет набранные баллы 2 тура.**

Преподаватель, демонстрируя ответы, обращает внимание на признаки, позволяющие выбрать героев, столкнувшихся в беседе с дроппингом и вишингом:

Герой	Его описание	Комментарии преподавателя
Марина поговорила с администратором	Добрый день, Марина. Вам звонят из центра репетиторства. Вы наш постоянный и любимый клиент.	Это вишинг. Какие признаки позволяют это определить:

Герой	Его описание	Комментарии преподавателя
центра репетиторства	Напишите, пожалуйста, несколько отзывов на пройденные в течение последнего месяца занятия. За отзывы вам положено вознаграждение. Для перевода денежных средств мне нужно вас внести в базу, назовите свои фамилию, имя, отчество, номер банковской карты и CVC. Деньги поступят вам сразу после опубликования отзывов.	звонок с неизвестного номера, предлагают легкий заработок, для которого нужно заранее сообщить данные банковской карты и ее CVC.
Алексей поговорил с потенциальным работодателем	Здравствуйте, Алексей. Да, мы предлагаем вам интересную работу в IT-сфере, начнете работать и получать высокую оплату труда. Вы ведь видели отзывы в соцсети? Это новый и очень популярный инвестпроект, где ваши навыки очень пригодятся, быстро сделаете карьеру. Договор, конечно, мы с вами заключим, а теперь давайте поговорим про риски и проценты с вознаграждения. Видите, условия очень хорошие, нам просто нужны молодые и активные сотрудники. Да, для работы, так как проект растет, вам потребуется завести пять банковских карт. У вас есть предпочтения по банкам? Проект активный, каждый день нужно будет получать платежи и совершать с них транзакции членам нашей команды, это позволяет нарастить инвестиционные возможности и заработать, с каждой транзакции ваши – 10 %. Да, возможно, потребуется отдельный номер телефона для обеспечения большего доступа к проекту. Приступить можете с понедельника.	Это дроппинг. Какие признаки позволяют это определить: фразы «потребуется завести пять банковских карт», «нужно будет получать платежи и совершать с них транзакции членам нашей команды, это позволяет нарастить инвестиционные возможности и заработать, с каждой транзакции ваши – 10 %», «отдельный номер телефона».
Данила поговорил с «другом друга»	Привет, Данила, это Максим. Мы с тобой не знакомы, я друг Марины. Она сказала, что ты нуждаешься в подработке. Мы сейчас как раз ищем сотрудника. Работа достаточно легкая и не занимает много времени, но нужно быть внимательным. Я буду ежедневно перечислять на твою карту определенную сумму, а ты – снимать и отдавать человеку, который вечером будет приезжать к тебе. Суммы небольшие, но, чтобы не вызвать подозрения у сотрудников банка, нам нужны люди для проведения этих	Это дроппинг. Какие признаки позволяют это определить: фразы «ежедневно перечислять на твою карту определенную сумму, а ты – снимать и отдавать человеку, который вечером будет приезжать к тебе», «5% от суммы ты можешь оставить себе, это твое вознаграждение за оперативность».

Герой	Его описание	Комментарии преподавателя
	нехитрых операций. Но при этом 5% от суммы ты можешь оставить себе, это твое вознаграждение за оперативность. Все абсолютно законно и безопасно. Если ты знаешь еще кого-нибудь, нуждающегося в подработке, то скажи мне, я свяжусь с этим человеком. Но только нужны ответственные люди, которые умеют работать быстро.	
Виолетта поговорила с представителем банка	Добрый день, Виолетта, вам звонят из службы безопасности банка N, к нам поступила информация, что по вашему счету обнаружены подозрительные транзакции, для проверки данных вашего счета необходимо срочно установить программу удаленного управления мобильным банкингом, чтобы сотрудники банка могли получить доступ и обезопасить вас. Если это не сделать сейчас, то ваш счет заблокируют.	Это вишинг. Какие признаки позволяют это определить: звонок от службы безопасности банка, нужно установить ПО для удаленного доступа; срочность и то, что торопят, указывая, что счет заблокируют.
Лилия ответила на звонок от потенциального работодателя	Добрый день, Лилия, наше агентство заинтересовали ваши фотографии, у вас неплохой блог, все эстетично, мы хотели бы пригласить вас на работу, для начала вам необходимо оформить страничку одного нашего продукта в соцсети. Мы посмотрим, как это повлияет на продажи, тогда заключим с вами договор. Оплата будет зависеть от того, насколько быстро будет расти аудитория, а компания – получать прибыль. Как вы понимаете, это отличная возможность показать свой талант людям и стать востребованным специалистом. Нам очень хотелось бы с вами сотрудничать.	Тут предварительно нет признаков вишинга или дроппинга. Абонент не просит данные банковской карты, персональные данные, не предлагает стать посредником для перевода средств. Но отнестись с осторожностью к предложению и проверить информацию, прежде чем соглашаться, конечно, стоит.

За каждый правильный ответ – 1 балл.

Продолжает подведение итогов: «Переходим к результатам третьего тура. Ответы и герои у вас на экране, цветом выделены важные признаки, благодаря которым можно было выявить финансовое мошенничество. Как же справились с этим наши агентства?»

### Объявляет набранные баллы 3 тура.

Преподаватель, демонстрируя ответы, обращает внимание на признаки, позволяющие выбрать героев, находящихся в зоне риска финансового мошенничества:

Герой	Его описание	Комментарии преподавателя
Марина	Марине пришло сообщение от близкой подруги, что она только что нашла ее фотографии с дня рождения, их разместили на странице кафе, где проходил праздник. Для	Тут мошенничество, которое можно увидеть по совокупности признаков. Во-первых, это непроверенное сообщение в соцсети. Во-вторых, срочность –

Герой	Его описание	Комментарии преподавателя
	быстрого перехода подруга прислала Марине картинку с QR-кодом	торопят, что нужно быстро перейти, и сам QR-код, который действует 10 минут.
Алексей	Алексеев прислали сообщение, в котором предлагают перейти по ссылке на страничку продавца графических планшетов, так как он оставил заявку на приобретение и свой номер на сайте. Ему рекомендуют изучить технические характеристики и, если все подходит, подъехать в магазин для совершения покупки. Также в сообщении указано, что если он проведет оплату по QR-коду, то сможет воспользоваться скидкой в 5%.	Собеседник не торопит героя, предлагает все изучить и уведомляет о возможности получения скидки при выбранном варианте оплаты.
Виолетта	Виолетте принесли счет за обед, она оплатила его картой и решила оставить чаевые официанту, для этого нужно отсканировать QR-код, который ведет на страничку кафе, где перечислены официанты (есть фотография каждого сотрудника, указаны фамилия, имя и отчество), и выбрать нужного работника.	Виолетта видит ссылку на ресурс, есть контакты лиц, с которыми Виолетта лично встречалась, можно проверить эту информацию до проведения каких-то операций.
Данила	Даниле в соцсети пришло сообщение с QR-кодом, что только сейчас, перейдя по нему, он сможет практически бесплатно оформить слот на забег «Бежать нельзя остановиться», о котором он мечтал, но не мог себе позволить из-за нехватки денежных средств. Однако предложение ограничено, нужно действовать максимально быстро.	Тут ситуация мошенничества. Есть ссылка на неизвестный ресурс, торопят и предоставляют ложную информацию о скидках и выгоде.
Лилия	Увидев модную заколку, только появившуюся в очередном интернет-магазине, она тут же ее заказала. Оплату магазин предложил произвести при помощи QR-кода, присланного продавцом. Лилия зашла в мобильное банковское приложение, увидела ссылку на нужный ресурс и перевела необходимую сумму, дав свое разрешение на транзакцию.	Действия героини правильные, она зашла в мобильное банковское приложение, увидела ссылку на нужный ресурс и перевела деньги.
Мурат	Мурату прислали сообщением инструкцию по блокировке транзакций из банка N: «Уважаемый Мурат! 30 минут назад с вашего счета пытались снять большую сумму денег. Зайдите в приложение банка, сформируйте QR-код и отправьте его скриншот на этот номер. Это необходимое действие для отмены операции. С уважением, служба безопасности банка N». За каждый правильный ответ – 1 балл.	Это мошенничество. Совокупность признаков: обращение от службы безопасности, требование срочного действия и формирования QR-кода, который фактически является поручением банку на выдачу денег без ввода ПИН-кода. Настоящие сотрудники банка никогда не попросят у клиента такие данные.

### Список источников

1. Фрицлер, А. В. Финансовая грамотность: 10—11 классы : учебник для среднего общего образования / А. В. Фрицлер, Е. А. Тарханова. — 3-е изд. — Москва : Издательство Юрайт, 2026. — 125 с. — (Общеобразовательный цикл). — ISBN 978-5-534-21870-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 1 — URL: <https://urait.ru/bcode/582330/p.1> (дата обращения: 26.03.2026).
2. <https://моифинансы.рф>
3. <https://fmc.hse.ru/mmspo>