МБОУ «Средняя общеобразовательная школа № __»
Предметная область «Общественно-научные предметы»

ИНДИВИДУАЛЬНЫЙ ПРОЕКТ

по предмету «Обществознание»
на тему: «Финансовое мошенничество: как старшекласснику распознать обман и защитить себя и близких»
Тип проекта: социальный (практико-ориентированный)
Продукт проекта: памятка и чек-лист «Пять вопросов перед переводом»

Выполнил(а): обучающийся(аяся) 11 «__» класса
_____ / И. О. Фамилия

Руководитель: учитель обществознания
_____ / И. О. Фамилия

[Город] 2026

Пример работы, выполненной в Универ AI · univerai.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....3
1. Финансовое мошенничество как социальная проблема.....5
1.1 Понятие и основные схемы мошенничества.....5
1.2 Масштаб проблемы по данным Банка России.....7
1.3 Как государство защищает граждан.....9
2. Разработка и апробация продукта проекта.....12
2.1 Опрос старшеклассников.....12
2.2 Памятка и чек-лист «Пять вопросов перед переводом».....13
2.3 Апробация продукта.....15
ЗАКЛЮЧЕНИЕ.....17
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....18
Приложение А. Анкета для опроса.....20
Приложение Б. Текст памятки.....20

ВВЕДЕНИЕ

Прошлой зимой бабушке моего одноклассника позвонил «сотрудник службы безопасности банка». Он знал её имя, назвал последние цифры карты и очень вежливо попросил продиктовать код из СМС, чтобы «отменить подозрительный перевод». Бабушка уже начала диктовать, но внук, оказавшийся рядом, успел забрать телефон. История закончилась хорошо. Тысячи похожих историй заканчиваются иначе.

Актуальность. По данным Банка России, в 2024 году объём операций, совершённых без добровольного согласия клиентов, вырос по сравнению с 2023 годом на 74,36 % [7]. Банки вернули пострадавшим лишь 9,9 % похищенного [7]. Это означает, что за ошибку человек почти всегда платит сам. Подростки здесь не только возможные жертвы. Мошенники ищут среди них и помощников: предлагают «лёгкий заработок» за передачу своей банковской карты, а за это предусмотрена уголовная ответственность [1].

Проблема. Почти у каждого старшеклассника есть банковская карта и смартфон, и многие из них лучше родителей разбираются в приложениях. Но умение пользоваться техникой не равно умению распознать обман. Советов о мошенниках много, они разбросаны по сайтам банков и новостям, а короткого и понятного текста, который можно за минуту прочитать перед переводом, у ребят нет.

Цель проекта — выяснить, какие схемы финансового мошенничества наиболее распространены и как от них защищает закон, и на этой основе создать памятку и чек-лист для старшеклассников и их родственников.

Задачи:

1) раскрыть понятие мошенничества в российском праве и описать основные схемы обмана;

2) проанализировать статистику Банка России за 2023–2024 годы;

3) изучить меры, которые государство приняло для защиты граждан от мошенников;

4) провести опрос учащихся 10–11 классов и выявить пробелы в их знаниях;

5) разработать памятку и чек-лист «Пять вопросов перед переводом» и проверить их на классном часе.

Объект исследования — финансовое мошенничество с использованием телефона и интернета. **Предмет** — способы защиты от него, доступные школьнику и его семье.

Гипотеза: большинство старшеклассников знает о мошенничестве в общем виде, но плохо знает конкретные меры защиты, которые даёт закон, а короткий чек-лист повышает число правильных решений в типичных ситуациях обмана.

Методы: анализ нормативных актов и статистики, сравнение, анкетирование, тестирование до и после классного часа.

Продукт проекта — памятка на одном листе А4 и чек-лист «Пять вопросов перед переводом» в формате карточки для телефона. Их текст приведён в приложении Б. Работа велась с октября 2025 по февраль 2026 года.

1. Финансовое мошенничество как социальная проблема

1.1 Понятие и основные схемы мошенничества

Уголовный кодекс Российской Федерации определяет мошенничество как хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием (ст. 159 УК РФ) [1]. Главное в этом определении — способ. Мошенник не взламывает сейф и не отбирает кошелёк силой. Человек сам отдаёт ему деньги, потому что поверил.

Кодекс выделяет несколько специальных составов. Статья 159.3 касается мошенничества с использованием электронных средств платежа, статья 159.6 — мошенничества в сфере компьютерной информации, когда преступник вмешивается в работу программ или вводит в систему ложные данные [1]. Для пострадавшего разница между ними невелика: деньги исчезают со счёта за несколько минут.

Сегодня большинство обманов строится на социальной инженерии. Так называют приёмы, при которых преступник воздействует не на технику, а на психику человека. Он создаёт ощущение срочности («деньги уже списываются»), опирается на авторитет («говорит следователь»), пугает («на вас оформлен кредит») или, наоборот, обещает выгоду. Человек в таком состоянии перестаёт рассуждать и делает то, что ему говорят.

Самые распространённые схемы показаны на рисунке 1. Их можно разделить на три группы: звонки и сообщения от имени организаций, поддельные сайты и предложения «заработать».

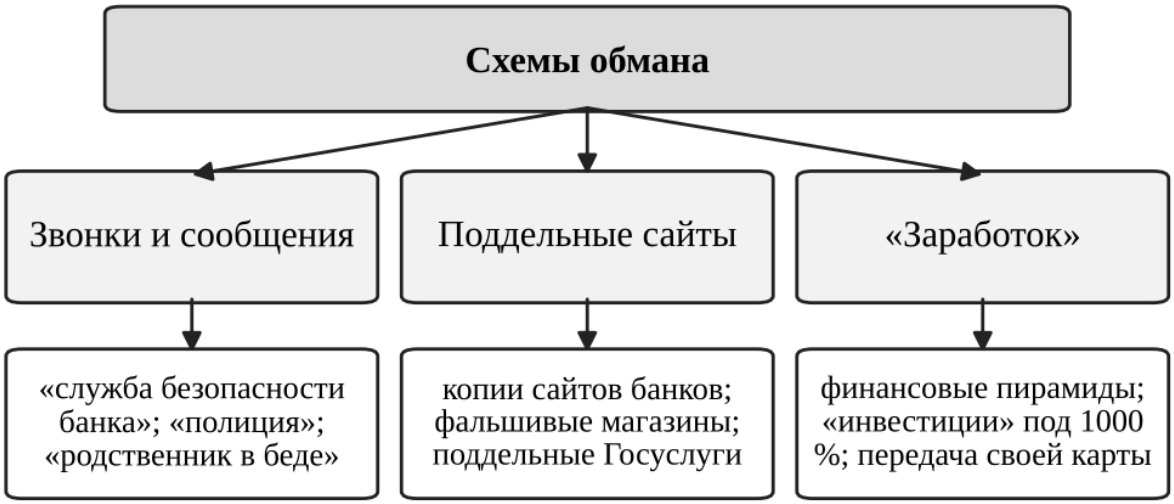


Рисунок 1 – Основные схемы финансового мошенничества

Источник: составлено автором по [6; 7].

Звонок от «службы безопасности банка» — классика последних лет. Собеседник сообщает о подозрительной операции и просит назвать код из СМС или перевести деньги на «безопасный счёт». Вариант для пожилых людей — звонок «внука», попавшего в аварию, или «следователя», которому нужно срочно передать деньги. В 2023 году мошенники стали реже звонить с городских номеров, но в два с лишним раза чаще использовать номера 8-800, которые вызывают больше доверия [6].

Поддельные сайты копируют страницы банков, интернет-магазинов и государственных порталов. Человек сам вводит на них данные карты или пароль. По итогам 2024 года фишинговые сайты составили 58 % ресурсов, против которых Банк России инициировал меры, финансовые пирамиды — 23 %, ещё около 16 % пришлось на нелегальных участников рынка [7].

Третья группа особенно касается подростков. В социальных сетях и мессенджерах предлагают заработок «на пару дней»: принять на свою карту деньги и перевести их дальше или просто отдать карту на время. Таких людей называют дропами. Через их счета мошенники выводят похищенные деньги, а сам дроп становится соучастником. Неправомерный оборот средств платежей наказывается по статье 187 УК РФ [1]. Сведения о таких счетах

банки и правоохранительные органы передают в базу данных Банка России о случаях и попытках переводов без согласия клиентов [2; 7].

1.2 Масштаб проблемы по данным Банка России

Банк России ежегодно публикует обзор операций, совершённых без согласия клиентов финансовых организаций. Это лучший открытый источник о масштабе проблемы: в нём учтены сведения, которые банки обязаны передавать регулятору [6; 7].

Цифры за последние годы показывают, что ущерб растёт быстрее, чем сами денежные переводы. В 2023 году объём операций без согласия клиентов вырос на 11,48 % при росте переводов с использованием карт на 10,54 %, до 136,38 трлн рублей [6]. В 2024 году прирост составил уже 74,36 % [7]. Если сопоставить суммы, которые банки вернули клиентам, с долей возврата, получится, что общий объём похищенного составил около 15,8 млрд рублей в 2023 году и около 27,4 млрд рублей в 2024 году (расчёт автора по [6; 7]).

Доля возвращённых средств растёт, но остаётся небольшой (рисунок 2). В 2022 году банки вернули клиентам 4,4 % похищенного, в 2023 году — 8,7 %, в 2024 году — 9,9 % [6; 7].

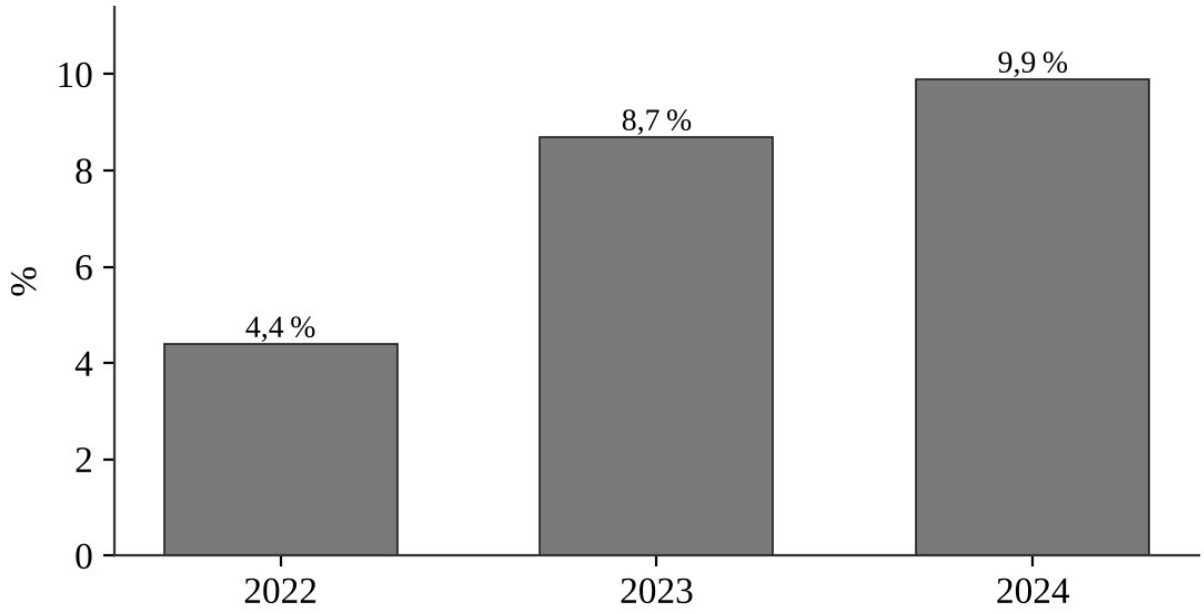


Рисунок 2 – Доля средств, возвращённых банками клиентам, % от объёма операций без согласия

Источник: составлено автором по данным Банка России [6; 7].

Почему возвращается так мало? Дело в том, что большинство переводов человек делает сам. Он сам заходит в приложение, сам вводит сумму и сам подтверждает операцию. С точки зрения банка это законное распоряжение клиента. Вернуть деньги удаётся в основном тогда, когда операция прошла без участия владельца счёта или когда банк нарушил свои обязанности.

Есть и хорошие новости. Банки научились останавливать значительную часть мошеннических операций до того, как деньги уйдут. В 2023 году злоумышленникам не удалось совершить 34,77 млн операций, в 2024 году — уже 72,17 млн [6; 7]. Основные показатели сведены в таблицу 1.

Таблица 1 – Операции без согласия клиентов: основные показатели

Показатель	**2023 год**	**2024 год**
Прирост объёма операций без согласия к предыдущему году, %	11,48	74,36
Возвращено клиентам, млн руб.	1 378,8	2 713,58
Возвращено клиентам, % от объёма	8,7	9,9
Предотвращено мошеннических операций, млн	34,77	72,17
Телефонных номеров направлено операторам связи для блокировки	575 669	171 977
Фишинговые сайты, % от ресурсов, по которым приняты меры	55	58

Источник: составлено автором по [6; 7].

Обращает на себя внимание резкое снижение числа телефонных номеров, переданных операторам связи: с 575 669 в 2023 году до 171 977 в 2024 году [6; 7]. Это не значит, что мошенники перестали звонить. Скорее, они переходят в мессенджеры, где звонок выглядит как обычный вызов знакомого контакта, а проверить номер труднее.

Статистика Банка России касается только денег, украденных через банковские каналы. Наличные, переданные «курьеру», или деньги,

вложенные в фальшивую «инвестиционную платформу», в этот учёт не всегда попадают. Поэтому реальный ущерб, вероятно, выше опубликованных цифр.

1.3 Как государство защищает граждан

Основные правила защиты от переводов без согласия клиента содержит Федеральный закон «О национальной платёжной системе» [2]. Он обязывает банки выявлять подозрительные операции по признакам, которые устанавливает Банк России, и обмениваться сведениями о мошенниках через специальную базу данных регулятора.

Важное изменение внёс Федеральный закон от 24 июля 2023 года № 369-ФЗ, вступивший в силу 25 июля 2024 года [3; 7]. Он дополнил статью 8 закона о платёжной системе подробным порядком действий банка. Прежде чем списать деньги, банк обязан проверить, нет ли у перевода признаков операции без добровольного согласия клиента. Если признаки есть, приём распоряжения приостанавливается на два дня, а клиента незамедлительно уведомляют и объясняют, как подтвердить операцию. Если же сведения о получателе есть в базе Банка России, банк приостанавливает на два дня даже подтверждённое распоряжение [2].

Эти два дня и есть главная защита. За это время человек может успокоиться, позвонить родным и понять, что разговаривал с мошенником. Закон предусматривает и ответственность самого банка: если он не выполнил эти обязанности, он должен в течение 30 дней после обращения клиента возместить ему сумму перевода (ч. 3.13 ст. 8) [2]. Правда, по этому основанию в 2024 году банки вернули клиентам всего 1,23 млн рублей. Банк России объясняет это тем, что банки в основном соблюдают установленные правила [7]. Иными словами, если банк всё сделал правильно, а человек сам подтвердил перевод, вернуть деньги через банк почти невозможно.

Вторая мера — самозапрет на кредиты. Его ввёл Федеральный закон от 26 февраля 2024 года № 31-ФЗ, дополнивший закон «О кредитных историях»

статьёй о внесении в кредитную историю сведений о запрете и о его снятии [4; 5]. Теперь любой гражданин может бесплатно, через портал Госуслуг или МФЦ, установить запрет на заключение с ним договоров потребительского кредита и займа банками и микрофинансовыми организациями [5]. На ипотеку, автокредит и образовательный кредит с господдержкой запрет не распространяется, а снять его можно тем же путём. Порядок самозапрета продолжают уточнять: в 2025 году в эту статью внёс изменения Федеральный закон от 1 апреля 2025 года № 41-ФЗ, посвящённый борьбе с правонарушениями в сфере информационных технологий [10]. Мошенникам, которые уговаривают человека «срочно оформить кредит, чтобы спасти деньги», становится гораздо труднее. Для пожилых родственников эта мера особенно полезна.

Третье направление — обмен информацией. В базу данных Банка России о случаях и попытках переводов без согласия клиентов попадают сведения не только от банков, но и от правоохранительных органов, даже если пострадавший не обращался в свой банк [7]. По сведениям регулятора, в 2024 году на основании его данных был ограничен доступ к 44 713 мошенническим ресурсам, а в социальных сетях — к 5 893 страницам и группам [7].

Наконец, государство вкладывается в просвещение. Стратегия повышения финансовой грамотности и формирования финансовой культуры до 2030 года уделяет особое внимание финансовой кибербезопасности на фоне роста кибермошенничества и предусматривает обучение финансовой грамотности всех школьников и студентов колледжей [8]. Банк России ведёт для этого просветительский портал «Финансовая культура» [9].

Как видно из таблицы 2, закон уже защищает гражданина довольно многими способами. Но почти все они срабатывают только тогда, когда человек сделал паузу: дождался двух дней, проверил номер, не стал брать кредит. Именно эту паузу и должна подсказать памятка.

Таблица 2 – Правовые меры защиты от финансового мошенничества

Мера	**Документ**	**Что даёт гражданину**
Приостановка перевода на два дня	Федеральный закон № 161-ФЗ, изменения № 369-ФЗ	время одуматься; возврат средств, если банк не выполнил обязанность
Самозапрет на кредиты	Федеральные законы № 218-ФЗ и № 31-ФЗ	на человека нельзя оформить кредит без снятия запрета
База данных Банка России о переводах без согласия	Федеральный закон № 161-ФЗ	банки узнают о счетах мошенников, сайты и страницы блокируются
Уголовная ответственность	ст. 159, 159.3, 159.6, 187 УК РФ	наказание мошенников и их помощников

Источник: составлено автором по [1–5; 7].

2. Разработка и апробация продукта проекта

2.1 Опрос старшеклассников

Чтобы понять, что именно нужно объяснять в памятке, мы составили анкету из восьми вопросов (приложение А). Опрос проводился анонимно, в электронной форме, среди учащихся 10–11 классов. Все результаты в этом параграфе — условные данные для примера: они показывают, как обрабатывается анкета, и не являются итогами реального опроса.

В опросе приняли участие 64 человека. Карта или счёт в банке есть у 57 из них, банковским приложением на телефоне пользуются 52. Подозрительные звонки или сообщения хотя бы раз получали 39 человек, а у 11 опрошенных мошенники пытались обмануть кого-то из родственников.

Таблица 3 – Ответы старшеклассников на вопросы о защите от мошенников (n = 64)

Вопрос	Ответили верно, чел.	Доля, %
Можно ли сообщать код из СМС сотруднику банка	58	91
Что сделает банк, если получатель перевода есть в базе мошенников	14	22
Существует ли самозапрет на кредиты	19	30
Законно ли передать свою карту знакомому за плату	33	52
Как проверить, что звонок действительно из банка	27	42

Примечание – Условные данные для примера: опрос в таком виде не проводился, числа показывают, как оформляются результаты анкетирования.

Результаты хорошо показывают, где проходит граница знаний (рисунок 3). Правило «никому не сообщать код из СМС» знают почти все. А вот о том, что закон даёт двухдневную паузу и самозапрет, знает меньшинство. Почти половина опрошенных не считает передачу своей карты за деньги чем-то опасным.

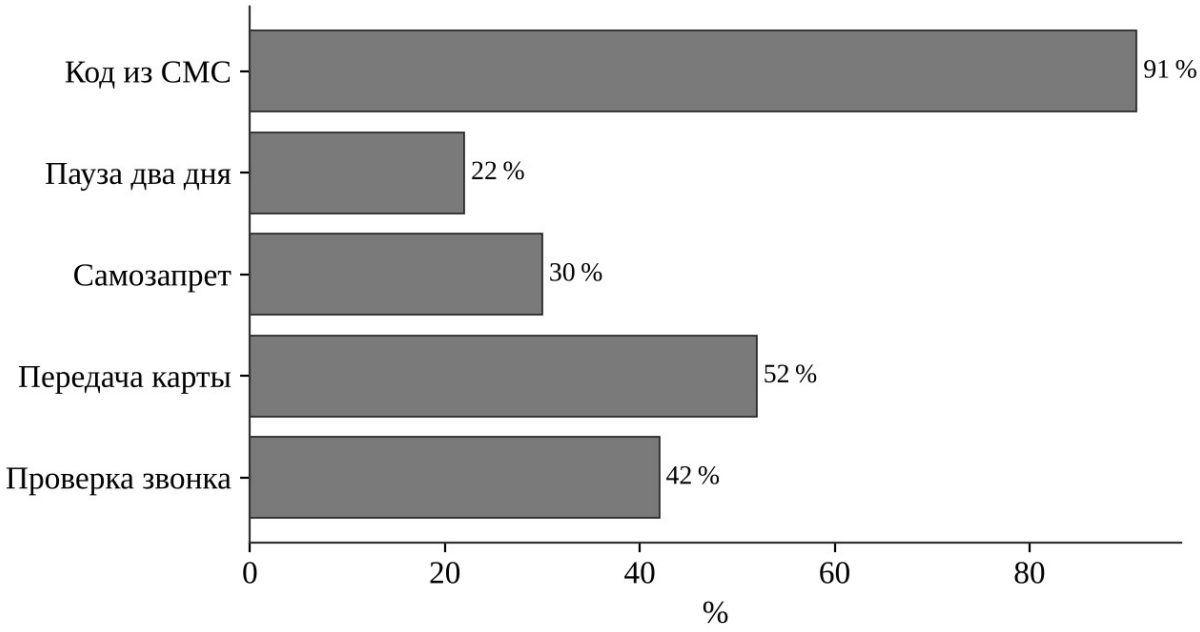


Рисунок 3 – Доля верных ответов по темам анкеты, %

Условные данные для примера.

Последний вопрос анкеты был открытым: «Почему люди поддаются мошенникам?». Чаще всего отвечали «испугались», «торопились» и «поверили, что звонит банк». Ответы совпали с тем, что описано в теоретической части. Мошенник выигрывает не хитростью технологий, а тем, что не даёт человеку времени подумать.

Отсюда вывод для продукта. Повторять в памятке общеизвестное «не говорите код» нет смысла. Нужно объяснить, какие права даёт закон, предупредить о рисках дропперства и, главное, дать простой способ остановиться перед переводом.

2.2 Памятка и чек-лист «Пять вопросов перед переводом»

Продукт проекта состоит из двух частей. Памятка — лист А4 для информационного стенда и для родителей. Чек-лист — карточка размером с экран телефона, которую можно сохранить в галерею и открыть в момент, когда тебя торопят с переводом.

При работе над текстом мы поставили себе три ограничения. Каждое правило — не длиннее одной строки. Никаких юридических терминов без

пояснения. Каждое утверждение о законе сверено с первоисточником [2–4]. Структура памятки приведена в таблице 4.

Таблица 4 – Структура памятки

Раздел	Содержание
«Как звучит мошенник»	четыре фразы-сигнала: срочно, секретно, страшно, выгодно
«Банк никогда не попросит»	код из СМС, перевод на «безопасный счёт», установку приложений по звонку
«Что даёт закон»	пауза два дня, возврат при нарушении банком обязанностей, самозапрет на кредиты
«Если тебе предлагают заработать на карте»	это дропперство, ст. 187 УК РФ, куда сообщить
«Если обманули»	позвонить в банк по номеру с карты, заблокировать карту, обратиться в полицию

Центральная часть продукта — чек-лист. Он построен на идее паузы. Чтобы перейти к следующему вопросу, нужно честно ответить на предыдущий, и уже на втором-третьем вопросе становится ясно, что ситуация подозрительна.



Рисунок 4 – Чек-лист «Пять вопросов перед переводом»

Если хотя бы на один из первых трёх вопросов ответ «да», а на один из двух последних — «нет», операцию нужно остановить. Положить трубку не

грубо. Настоящий сотрудник банка или полиции поймёт, а мошенник потеряет единственное своё оружие — время.

Памятку и карточку мы сверстали в бесплатном онлайн-редакторе, напечатали 40 экземпляров для стенда и классных руководителей и разослали электронную версию в родительские чаты двух классов. Затраты свелись к печати на школьном принтере.

2.3 Апробация продукта

Продукт проверили на классном часе в 10 классе. Перед занятием ученики решили короткий тест из шести ситуаций: например, «звонит „следователь“ и просит перевести деньги на защищённый счёт» или «знакомый предлагает 3000 рублей за то, чтобы принять перевод на твою карту». Для каждой нужно было выбрать правильное действие. Затем мы 15 минут разбирали памятку и чек-лист, а в конце урока ученики решили тест с другими ситуациями той же трудности.

Все числа в этом параграфе — условные данные для примера. В занятии участвовали 26 человек. До разбора памятки средний результат составил 3,4 правильных ответа из 6, после — 5,1. Больше всего выросло число правильных ответов в ситуации с передачей карты: с 12 до 23 человек.

Таблица 5 – Результаты теста до и после классного часа (n = 26)

Показатель	До	После
Средний балл (из 6)	3,4	5,1
Решили все шесть ситуаций верно, чел.	2	13
Верно ответили о передаче карты, чел.	12	23
Верно ответили о паузе в два дня, чел.	6	20

Примечание – Условные данные для примера: тест в таком виде не проводился, числа показывают, как оформляются результаты тестирования.

Такой рост нельзя считать строгим доказательством: тест после урока ученики решали сразу, пока материал был свежим, и не было контрольной

группы. Но он показывает, что короткий и конкретный текст работает лучше, чем общие призывы к бдительности.

После урока ученики предложили два улучшения: добавить в памятку пример настоящего фишингового сообщения и номер горячей линии Банка России. Первое мы сделали, второе тоже — номер взят с официального сайта регулятора. Учитель обществознания решил использовать материалы на уроках по теме «Финансовая грамотность» в 10 классах.

Проверка гипотезы. На условных данных гипотеза подтвердилась: старшеклассники хорошо знают общее правило о коде из СМС, но мало знают о правовых мерах защиты, а работа с чек-листом заметно повысила число правильных решений.

ЗАКЛЮЧЕНИЕ

Финансовое мошенничество в России сегодня — это в первую очередь обман, при котором человек сам отдаёт деньги. Уголовный кодекс относит такие действия к мошенничеству и наказывает не только самих обманщиков, но и тех, кто помогает выводить похищенное [1].

Анализ обзоров Банка России показал, что в 2024 году объём операций без согласия клиентов вырос на 74,36 %, а банки вернули пострадавшим лишь 9,9 % похищенного [7]. Одновременно банки предотвратили 72,17 млн мошеннических операций, вдвое больше, чем годом раньше.

Государство защищает граждан несколькими способами: двухдневной паузой при переводе получателю из базы мошенников, самозапретом на кредиты, обменом данными о мошенниках и программами финансового просвещения [2–5; 8]. Однако все эти меры работают лишь тогда, когда человек делает паузу и не действует под давлением.

Опрос и тест на условных данных показали, как можно выявить пробелы в знаниях старшеклассников и проверить действие продукта. Результат проекта — памятка и чек-лист «Пять вопросов перед переводом» — размещён на школьном стенде и передан классным руководителям. Цель достигнута, задачи выполнены. В дальнейшем проект можно развить: провести такой же урок для родителей и бабушек с дедушками и подготовить версию памятки крупным шрифтом.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Уголовный кодекс Российской Федерации : Федеральный закон от 13.06.1996 № 63-ФЗ : [ред. от 04.08.2026]. – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 22.10.2026). – Текст : электронный.

2. О национальной платёжной системе : Федеральный закон от 27.06.2011 № 161-ФЗ : [ред. от 04.08.2026]. – URL: https://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 20.10.2026). – Текст : электронный.

3. О внесении изменений в Федеральный закон «О национальной платежной системе» : Федеральный закон от 24.07.2023 № 369-ФЗ. – URL: http://publication.pravo.gov.ru/ (дата обращения: 20.10.2026). – Текст : электронный.

4. О внесении изменений в Федеральный закон «О кредитных историях» и Федеральный закон «О потребительском кредите (займе)» : Федеральный закон от 26.02.2024 № 31-ФЗ. – URL: http://publication.pravo.gov.ru/ (дата обращения: 20.10.2026). – Текст : электронный.

5. О кредитных историях : Федеральный закон от 30.12.2004 № 218-ФЗ : [ред. от 2026 г.]. – URL: https://www.consultant.ru/document/cons_doc_LAW_51043/ (дата обращения: 20.10.2026). – Текст : электронный.

6. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2023 год / Банк России. – URL: https://www.cbr.ru/analytics/ib/operations_survey/2023/ (дата обращения: 20.10.2026). – Текст : электронный.

7. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций за 2024 год / Банк России. – URL: https://www.cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения: 20.10.2026). – Текст : электронный.

8. Об утверждении Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года : распоряжение Правительства Российской Федерации от 24.10.2023 № 2958-р. – Текст : электронный // ГАРАНТ.РУ : информационно-правовой портал. – URL: https://base.garant.ru/407887147/ (дата обращения: 22.10.2026).

9. Финансовая культура : информационно-просветительский ресурс Банка России. – URL: https://fincult.info/ (дата обращения: 20.10.2026). – Текст : электронный.

10. О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 01.04.2025 № 41-ФЗ. – URL: http://www.kremlin.ru/acts/bank/51783 (дата обращения: 22.10.2026). – Текст : электронный.

ПРИЛОЖЕНИЕ А. АНКЕТА ДЛЯ ОПРОСА

Анкета анонимная. Отметьте один вариант ответа, если не сказано иное.

1) Есть ли у вас банковская карта или счёт? (да / нет)

2) Пользуетесь ли вы банковским приложением на телефоне? (да / нет)

3) Получали ли вы подозрительные звонки или сообщения о деньгах? (да / нет / не помню)

4) Можно ли сообщить код из СМС сотруднику банка, если он сам позвонил? (да / нет / не знаю)

5) Что сделает банк, если получатель вашего перевода есть в базе мошенников Банка России? (выполнит перевод / приостановит перевод на два дня / не знаю)

6) Можно ли запретить оформлять на себя кредиты? (да / нет / не знаю)

7) Законно ли за плату передать свою карту знакомому для «приёма переводов»? (да / нет / не знаю)

8) Почему, по-вашему, люди поддаются мошенникам? (открытый вопрос)

ПРИЛОЖЕНИЕ Б. ТЕКСТ ПАМЯТКИ

СТОП, МОШЕННИК! ПАМЯТКА ДЛЯ СТАРШЕКЛАССНИКОВ И ИХ БЛИЗКИХ

Как звучит мошенник

«Срочно!», «Никому не говорите», «На вас оформляют кредит», «Гарантированный доход». Если слышите хотя бы одно — кладите трубку.

Банк никогда не попросит

– назвать код из СМС или пароль;

– перевести деньги на «безопасный» или «резервный» счёт;

– установить приложение или включить демонстрацию экрана.

Что даёт закон

– если перевод похож на мошеннический или получатель есть в базе Банка России, банк остановит его на два дня;

– если банк этого не сделал, он обязан вернуть деньги в течение 30 дней после обращения;

– на Госуслугах можно установить самозапрет на кредиты — посоветуйте это бабушке и дедушке.

Тебе предлагают заработать на своей карте?

Это дропперство. Через твою карту выводят украденные деньги. Карту могут заблокировать, а тебе грозит уголовная ответственность по статье 187 УК РФ.

Если обманули

1) Позвоните в банк по номеру на обороте карты и заблокируйте её.

2) Сохраните переписку, номера и чеки.

3) Обратитесь в полицию.