



**Девятый этап** Всероссийской просветительской  
Эстафеты «Мои финансы»



МИНФИН  
РОССИИ

мои финансы

# Безопасность денег в цифровой среде





# ЦИФРОВАЯ СРЕДА ФИНАНСОВЫХ УСЛУГ

## Цифровые финансовые сервисы:

- интернет-банк / мобильный банк
- финансовые маркетплейсы
- платежные сервисы



## Ключевые тренды:

- рост числа пользователей цифровых финансовых услуг
- переход финансовых услуг в портативные устройства

**89%** финансовых услуг граждане России получают онлайн\*

**87%** платежей приходится на безналичную форму оплаты\*\*

\* по данным Банка России за 2025 год

\*\* по данным компании Positive Technologies за 2025 год



## РИСКИ ЦИФРОВОЙ СРЕДЫ

1. Риски, связанные с действиями потребителей
2. Риски, связанные с действиями поставщиков услуг
3. Риски, возникающие из-за особенностей используемых технологий
4. Риски, связанные с действиями мошенников





# РИСКИ ДЕЙСТВИЙ ПОТРЕБИТЕЛЕЙ

## 1. Неправильные решения

Недостаточная цифровая финансовая грамотность ведет к принятию неправильных решений или совершению ошибок при самостоятельном проведении финансовых операций

## 2. Импульсивные траты

Легкость совершения финансовых операций и «виртуальность» в восприятии денежных средств провоцирует необдуманные покупки и увеличивает личные расходы

## 3. Чрезмерное кредитование

Легкость получения кредитов в цифровой среде, сочетающаяся с недостатком самоконтроля, может привести к накоплению долговой нагрузки

## 4. Смешивание поставщиков услуг

В цифровой среде потребитель может не всегда четко понимать, услугами какой финансовой организации он пользуется – банк это или не банк, легальная или нелегальная организация

## 5. Смешивание инструментов

Из-за внешней схожести интерфейса приложений потребитель может смешивать разные финансовые инструменты – вклады и инвестиции, долевого и долговые ценные бумаги и т.д.

## 6. «Засвечивание» паролей

Хранение паролей и ПИН-кодов в мессенджерах, заметках в смартфоне или на бумаге делает их доступными для злоумышленников



# РИСКИ ДЕЙСТВИЙ ПОСТАВЩИКОВ УСЛУГ

## 1. «Цифровой след»

Использование компаниями «цифрового следа» потребителя (информации об онлайн-активности) для его подталкивания к той или иной финансовой операции

## 2. Навязывание услуг

В цифровой среде недобросовестный поставщик с целью увеличения своих доходов может незаметно для потребителя «подписать» его на ненужные дополнительные услуги

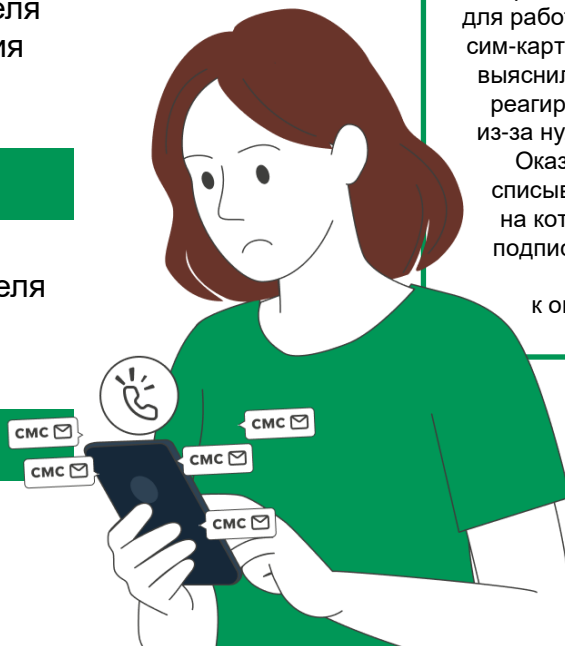
## 3. Слабая защита данных

Некоторые поставщики финансовых услуг недостаточно защищают персональные и конфиденциальные данные, что делает их уязвимыми к утечкам

### ПРАКТИЧЕСКАЯ СИТУАЦИЯ.

В 2017 году один москвич оснастил ворота на своей даче GSM-реле, для работы которого использовалась сим-карта. Через несколько месяцев выяснилось, что ворота перестали реагировать на СМС-сообщения из-за нулевого баланса сим-карты.

Оказалось, что деньги с нее списывались за платные услуги, на которые ворота якобы сами подписались. После обращения потребителя к оператору связи деньги были возвращены





# РИСКИ ТЕХНОЛОГИЙ

## 1. Несовершенные алгоритмы

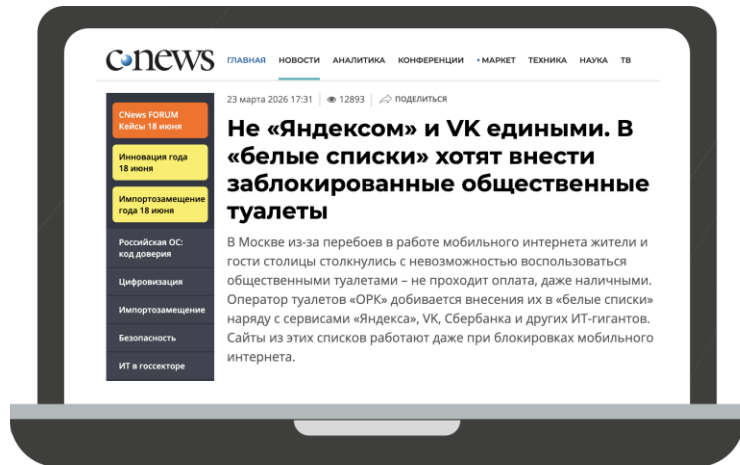
Принятие решений на основе цифровых алгоритмов может приводить к отказу в предоставлении услуги или к предложению ее на несправедливых условиях (завышенная ставка по кредиту, завышенный страховой тариф)

## 2. Технические сбои

Ненадежность связи, сбои в работе программ или цифровых финансовых платформ могут приводить к невозможности получить критически важную финансовую услугу в нужный момент

## 3. Уязвимости сервисов

Утечка данных, связанная с уязвимостями в цифровых сервисах, например, при использовании публичных Wi-Fi сетей





# РИСКИ МОШЕННИЧЕСТВА

## 1. Социальная инженерия

Манипуляции на чувствах и эмоциях человека: доверии, страхе, жадности, желании помочь, уверенности в себе или любопытстве

## 2. Дипфейки

Созданный с помощью нейросетей фото-, аудио- и видео- контент, имитирующий реальные записи и направленный на введение в заблуждение

## 3. Фишинг и фарминг

Выманивание персональных и конфиденциальных данных через электронные письма, СМС-сообщения в социальных сетях и мессенджерах. А также перенаправление пользователя на ложную страницу

## 4. Программы-шпионы

Установка вредоносного программного обеспечения, передающего злоумышленникам персональные данные с компьютера или смартфона

## 5. Взлом учетных записей

Незаконное получение доступа к аккаунтам в социальных сетях и цифровых сервисах с целью кражи конфиденциальной информации

## 6. Финансовые пирамиды

Организация мошеннических схем, маскирующихся под передовые финансовые сервисы – краудлендинг, инвестиции в криптовалюту и цифровые финансовые активы



# ЦИФРОВАЯ ФИНАНСОВАЯ ГИГИЕНА

1. Безопасность устройств и приложений
2. Безопасность аутентификации
3. Безопасность выбора поставщиков финансовых услуг
4. Защита от мошенничества и импульсивных решений





## БЕЗОПАСНОСТЬ УСТРОЙСТВ И ПО

- 1) установка только официальных приложений из проверенных источников
- 2) использование антивирусного программного обеспечения
- 3) регулярное обновление операционной системы и приложений

### Практические советы:

Скачивайте приложения исключительно из официальных магазинов – RuStore, App Store, Google Play, AppGallery.

Избегайте установки программ по ссылкам из мессенджеров или СМС – это один из основных способов распространения шпионского программного обеспечения (ПО), которое крадет данные банковских карт и пароли.





## БЕЗОПАСНОСТЬ УСТРОЙСТВ И ПО

- 1) установка только официальных приложений из проверенных источников
- 2) использование антивирусного программного обеспечения
- 3) регулярное обновление операционной системы и приложений

### Практические советы:

Устанавливайте на смартфон и компьютер лицензионное антивирусное программное обеспечение (ПО). Современные антивирусы не только обнаруживают угрозы, но и предупреждают о переходе на фишинговые сайты, а также проверяют, не попали ли ваши пароли в открытые базы утечек.





## БЕЗОПАСНОСТЬ УСТРОЙСТВ И ПО

- 1) установка только официальных приложений из проверенных источников
- 2) использование антивирусного программного обеспечения
- 3) регулярное обновление операционной системы и приложений

### Практические советы:

Включите автоматическое обновление ОС и всех приложений. Разработчики регулярно выпускают патчи безопасности, закрывающие уязвимости, которые используют хакеры для взлома устройств. Откладывание обновления – это сознательное оставление «двери» для злоумышленников.



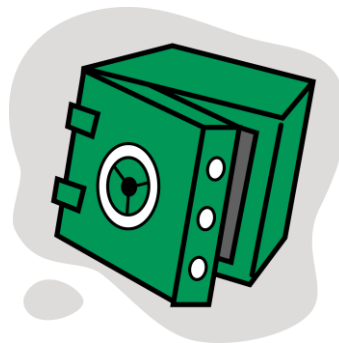


## БЕЗОПАСНОСТЬ АУТЕНТИФИКАЦИИ

- 1) использование сложных и уникальных паролей для каждого сервиса
- 2) регулярная смена паролей и проверка их на утечки
- 3) отказ от хранения паролей в мессенджерах и на бумаге
- 4) двухфакторная аутентификация как обязательный стандарт защиты
- 5) использование биометрической аутентификации

### Практические советы:

Длина пароля должна быть не менее 12–16 символов, с использованием заглавных и строчных букв, цифр и специальных символов. Никогда не используйте один и тот же пароль для почты, Госуслуг и банковских приложений (иначе после взлома одного сервиса мошенники получат доступ ко всем остальным).



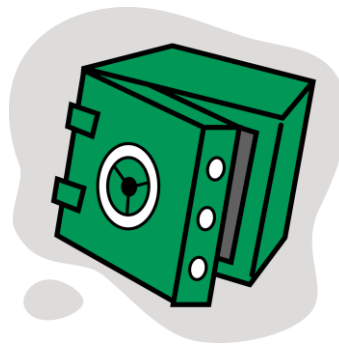


## БЕЗОПАСНОСТЬ АУТЕНТИФИКАЦИИ

- 1) использование сложных и уникальных паролей для каждого сервиса
- 2) регулярная смена паролей и проверка их на утечки
- 3) отказ от хранения паролей в мессенджерах и на бумаге
- 4) двухфакторная аутентификация как обязательный стандарт защиты
- 5) использование биометрической аутентификации

### Практические советы:

Меняйте пароли не реже одного раза в 3–6 месяцев. Используйте функцию проверки безопасности в своем аккаунте в смартфоне или в браузере персонального компьютера – система покажет, какие из ваших паролей были скомпрометированы и попали в публичные базы утечек.





## БЕЗОПАСНОСТЬ АУТЕНТИФИКАЦИИ

- 1) использование сложных и уникальных паролей для каждого сервиса
- 2) регулярная смена паролей и проверка их на утечки
- 3) отказ от хранения паролей в мессенджерах и на бумаге
- 4) двухфакторная аутентификация как обязательный стандарт защиты
- 5) использование биометрической аутентификации

### Практические советы:

Не сохраняйте пароли на листках бумаги или в заметках смартфона и не пересылайте себе в мессенджере. Если злоумышленник получит доступ к вашему аккаунту, он получит все ключи от ваших финансовых сервисов. Разумной альтернативой является использование менеджеров паролей (например, Kaspersky Password Manager). Вам нужно запомнить только один мастер-пароль, а остальные хранятся в зашифрованном виде.



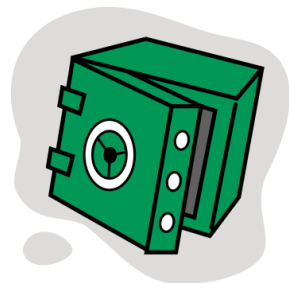
## БЕЗОПАСНОСТЬ АУТЕНТИФИКАЦИИ

- 1) использование сложных и уникальных паролей для каждого сервиса
- 2) регулярная смена паролей и проверка их на утечки
- 3) отказ от хранения паролей в мессенджерах и на бумаге
- 4) двухфакторная аутентификация как обязательный стандарт защиты
- 5) использование биометрической аутентификации

### Практические советы:

Подключите двухфакторную аутентификацию везде, где это возможно: Госуслуги, почта, социальные сети, банковские приложения.

При входе в аккаунт вы получите код подтверждения на ваш смартфон. Сообщать его третьим лицам нельзя. Помните: сотрудники банка или госорганов никогда не спрашивают коды из SMS или приложения. Если вас просят назвать код – это мошенники.





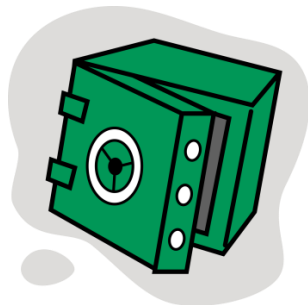
## БЕЗОПАСНОСТЬ АУТЕНТИФИКАЦИИ

- 1) использование сложных и уникальных паролей для каждого сервиса
- 2) регулярная смена паролей и проверка их на утечки
- 3) отказ от хранения паролей в мессенджерах и на бумаге
- 4) двухфакторная аутентификация как обязательный стандарт защиты
- 5) использование биометрической аутентификации

### Практические советы:

Включите вход по отпечатку пальца или Face ID в банковских приложениях и менеджерах паролей. Это не только удобно, но и безопасно: биометрию нельзя подсмотреть или украсть удаленно.

Однако помните: в отличие от пароля, сменить биометрию в случае утечки невозможно, поэтому используйте её как дополнение к паролю, а не как единственный метод защиты.





## БЕЗОПАСНОСТЬ ВЫБОРА ПОСТАВЩИКОВ

- 1) проверка лицензий поставщиков финансовых услуг
- 2) изучение репутации поставщиков финансовых услуг



### Практические советы:

Все легальные участники финансового рынка – кредитные, микрофинансовые, страховые организации и т.п. – должны иметь действующую лицензию Банка России.

Для проверки зайдите на официальный сайт Банка России ([cbr.ru](http://cbr.ru)) в раздел «Проверить участника финансового рынка» и введите название или ИНН поставщика.



## БЕЗОПАСНОСТЬ ВЫБОРА ПОСТАВЩИКОВ

- 1) проверка лицензий поставщиков финансовых услуг
- 2) изучение репутации поставщиков финансовых услуг



### Практические советы:

Перед тем как доверить деньги, проверьте, не включен ли поставщик финансовых услуг в «Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке», который доступен на сайте Банка России. При чтении отзывов потребителей на независимых площадках (например, Банки.ру) обращайте внимание на упоминания о задержках выплат, проблемах с выводом средств и навязывании услуг.



## ЗАЩИТА ОТ МОШЕННИЧЕСТВА

- 1) правило «Трех С»
- 2) контроль истории операций
- 3) настройка лимитов и уведомлений
- 4) использование виртуальных карт
- 5) контроль кредитной истории
- 6) минимизация публикации личных данных
- 7) самозапрет на получение кредита
- 8) сервис «второй руки» в банке

### Практические советы:

«Три С» расшифровываются как «Стоп, Сброс, Созвон»:

- **Стоп:** прервать разговор, если речь идет о деньгах.
- **Сброс:** положить трубку и не перезванивать по номеру звонящего.
- **Созвон:** самостоятельно перезвонить в банк (по номеру, указанному на обороте карты или официальном сайте) или близкому человеку, от которого исходит просьба денег.

Учтите, что мошенники могут использовать нейросети для подделки голоса и подмены номеров.



## ЗАЩИТА ОТ МОШЕННИЧЕСТВА

- 1) правило «Трех С»
- 2) контроль истории операций
- 3) настройка лимитов и уведомлений
- 4) использование виртуальных карт
- 5) контроль кредитной истории
- 6) минимизация публикации личных данных
- 7) самозапрет на получение кредита
- 8) сервис «второй руки» в банке

### Практические советы:

Установите привычку проверять выписки по картам ежедневно или через день. Если заметили подозрительную операцию:

- немедленно заблокируйте карту через мобильное приложение или по телефону горячей линии банка;
- напишите заявление в банк об оспаривании операции (до 24 часов с момента списания — шансы вернуть деньги выше);
- обратитесь в полицию, если сумма значительная.



## ЗАЩИТА ОТ МОШЕННИЧЕСТВА

- 1) правило «Трех С»
- 2) контроль истории операций
- 3) настройка лимитов и уведомлений
- 4) использование виртуальных карт
- 5) контроль кредитной истории
- 6) минимизация публикации личных данных
- 7) самозапрет на получение кредита
- 8) сервис «второй руки» в банке

### Практические советы:

В мобильном приложении банка установите суточные лимиты на:

- снятие наличных;
- переводы (особенно на счета третьих лиц);
- онлайн-покупки.

Даже если мошенники получают доступ, они не смогут вывести сумму выше установленного лимита.

SMS- или push-уведомления должны быть включены для операций на любую сумму – это позволит мгновенно заметить подозрительную транзакцию.



## ЗАЩИТА ОТ МОШЕННИЧЕСТВА

- 1) правило «Трех С»
- 2) контроль истории операций
- 3) настройка лимитов и уведомлений
- 4) использование виртуальных карт
- 5) контроль кредитной истории
- 6) минимизация публикации личных данных
- 7) самозапрет на получение кредита
- 8) сервис «второй руки» в банке

### Практические советы:

Для интернет-покупок заведите отдельную виртуальную («цифровую») карту в банковском приложении) и держите на ней ровно столько денег, сколько готовы потратить.

Многие банки позволяют выпускать виртуальные карты мгновенно и бесплатно, а также блокировать их в один клик.

Если мошенники украдут данные этой карты, на ней не будет крупной суммы, а ваша основная зарплатная карта останется в безопасности.



## ЗАЩИТА ОТ МОШЕННИЧЕСТВА

- 1) правило «Трех С»
- 2) контроль истории операций
- 3) настройка лимитов и уведомлений
- 4) использование виртуальных карт
- 5) контроль кредитной истории
- 6) минимизация публикации личных данных
- 7) самозапрет на получение кредита
- 8) сервис «второй руки» в банке

### Практические советы:

Регулярно проверяйте свою кредитную историю. Это можно сделать бесплатно дважды в год. Чтобы получить свою кредитную историю, сначала нужно узнать, в каком бюро кредитных историй (БКИ) она хранится, направив запрос в Центральный каталог кредитных историй (ЦККИ) через портал Госуслуги или сайт Банка России. Зная, в каких БКИ хранится кредитная история, можно запросить ее напрямую в БКИ либо через финансово-кредитные организации, заключившие договор с БКИ. Если в кредитной истории вы видите кредит, который не оформляли – срочно сообщите об этом в банк и в полицию.



## ЗАЩИТА ОТ МОШЕННИЧЕСТВА

- 1) правило «Трех С»
- 2) контроль истории операций
- 3) настройка лимитов и уведомлений
- 4) использование виртуальных карт
- 5) контроль кредитной истории
- 6) минимизация публикации личных данных
- 7) самозапрет на получение кредита
- 8) сервис «второй руки» в банке

### Практические советы:

Не публикуйте в социальных сетях:

- номер телефона и адрес;
- фотографии паспорта, водительских прав, банковских карт;
- дату рождения (особенно полные – число, месяц, год);
- Информацию об отъезде и крупных покупках.

Мошенники используют эту информацию для подбора ответов на контрольные вопросы в банках и для создания убедительных сценариев социальной инженерии.



## ЗАЩИТА ОТ МОШЕННИЧЕСТВА

- 1) правило «Трех С»
- 2) контроль истории операций
- 3) настройка лимитов и уведомлений
- 4) использование виртуальных карт
- 5) контроль кредитной истории
- 6) минимизация публикации личных данных
- 7) самозапрет на получение кредита
- 8) сервис «второй руки» в банке

### Практические советы:

Если вы не планируете брать кредит в обозримом будущем, имеет смысл через портал Госуслуг установить самозапрет на получение кредита.

Если, несмотря на установленный самозапрет, банк оформит кредит, он не сможет потребовать от вас его возврата.

Если же вам понадобится кредит, запрет можно снять, но отмена вступает в силу не сразу, а на следующий день – это период охлаждения, который защищает от импульсивных решений.



## ЗАЩИТА ОТ МОШЕННИЧЕСТВА

- 1) правило «Трех С»
- 2) контроль истории операций
- 3) настройка лимитов и уведомлений
- 4) использование виртуальных карт
- 5) контроль кредитной истории
- 6) минимизация публикации личных данных
- 7) самозапрет на получение кредита
- 8) сервис «второй руки» в банке

### Практические советы:

Сервис «второй руки» позволяет клиенту банка назначить уполномоченное лицо (помощника), которое сможет подтверждать или отклонять некоторые операции (переводы, снятие наличных), предотвращая хищения средств или импульсивные траты крупных сумм. При подозрительных операциях у «второй руки» есть 12 часов на решение: при подтверждении банк проведет операцию, в противном случае – отклонит.

Однако самостоятельно распоряжаться деньгами своего доверителя помощник не может.



# КАК РАСПОЗНАТЬ ДИПФЕЙКИ

- это контент (видео, аудио или фото), созданный с помощью нейросетей и машинного обучения, который с высокой степенью реалистичности имитирует реальные записи

Как определить:

- Глаза: неестественное моргание, расфокусированный взгляд
- Голос: рассинхронизация звука и движений губ
- Овал лица: размытые края, неестественный тон лица
- Уникальное поведение человека не копируется

Что делать:

попросить человека выполнить неожиданное действие (повернуть голову в профиль или провести рукой перед лицом)

Правило «Три С»: «Стоп, Сброс, Созвон»



## ЦИФРОВОЙ РУБЛЬ

- цифровая форма российской национальной валюты
- его массовое внедрение запланировано с 1 сентября 2026 года



### Средства в цифровых рублях:

- предназначены исключительно для платежей и переводов, их нельзя разместить на вкладе, использовать для получения кредита или инвестировать
- хранятся в цифровых кошельках на платформе Банка России, но пользоваться ими можно через приложение любого банка



## Безопасность цифрового рубля

Внедрение цифрового рубля позволяет повысить безопасность денег в цифровой среде:

- каждому цифровому рублю присваивается уникальный код (аналог номера на обычной бумажной купюре), что позволяет отслеживать транзакции, бороться с отмыванием денег и другими незаконными операциями
- используются средства криптографической защиты, сертифицированные ФСБ, и защищённые каналы связи
- применяются смарт-контракты – алгоритмы, которые автоматически выполняют переводы денежных средств между пользователями при соблюдении заранее заданных параметров (условий сделки)



# ПРАКТИКУМ





# ПРАКТИКУМ

## Задание № 1

Светлана получила СМС с номера, похожего на номер её банка: «Ваша карта участвует в акции! Нажмите на [ссылку](#), чтобы активировать кешбэк 25% на все покупки. Ссылка активна 1 час».

Определите, какие признаки указывают на фишинговую атаку в этом сообщении.

Опишите алгоритм действий Светланы: что ей нужно сделать, чтобы проверить информацию, и чего ей нельзя делать ни в коем случае.





# ПРАКТИКУМ

## Ответ на задание № 1

**Признаки:** подчеркивание необходимости срочного действия («ссылка активна 1 час»); слишком высокий процент кешбэка (25%); ссылка в СМС, требующая перехода.

**Действия:** не переходить по ссылке; открыть официальное приложение банка (или позвонить на горячую линию по номеру, указанному на карте) и уточнить информацию об акции; удалить СМС.





# ПРАКТИКУМ

## Задание № 2

Юрий установил на свой смартфон упрощенный графический ключ (3 точки), сохранил в приложении «Заметки» все PIN-коды банковских карт и пароль от онлайн-банка, чтобы не забыть их. Его 10-летний сын часто играет в игры на этом телефоне. Однажды Юрий потерял телефон в транспорте.

Какие три нарушения правил цифровой безопасности допустил Юрий?

Какие меры нужно предпринять сразу после утери телефона, чтобы обезопасить свои деньги?





# ПРАКТИКУМ

## Ответ на задание № 2

**Нарушения:** простой графический ключ (легко подобрать по следам на экране); хранение PIN-кодов и паролей в открытом виде в заметках; предоставление ребенку бесконтрольного доступа к устройству, где есть банковские приложения.

**Меры:** немедленно позвонить оператору сотовой связи для блокировки сим-карты, заблокировать банковские карты через колл-центр банка (даже если телефон не разблокирован).





# ПРАКТИКУМ

## Задание № 3

Иван увидел в интернете рекламу: «МФК  
ТопДоход. Вложи 50 000 рублей, через месяц  
получи 75 000 рублей. Гарантия дохода 100%»  
Сайт выглядит красиво, есть кнопка «Личный  
кабинет».

Назовите минимум три признака  
мошенничества в этом предложении.

Предложите Ивану легальный способ  
проверить организацию, прежде  
чем переводить деньги.





# ПРАКТИКУМ

## Ответ на задание № 3

**Признаки:** обещание гарантированного дохода (закон запрещает гарантировать доходность на финансовом рынке); чрезмерно высокая доходность (50% в месяц); низкая минимальная сумма вклада (микрофинансовые организации по закону не имеют права привлекать средства физических лиц на сумму менее 1,5 млн рублей).

**Проверка:** зайти на официальный сайт Банка России в раздел «Проверить участника финансового рынка» и ввести название организации.





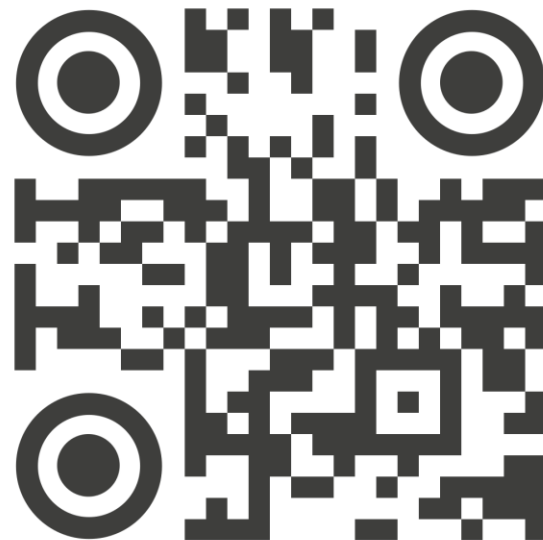
# ПРАКТИКУМ

## Задание № 4

С помощью портала «Госуслуги» ([www.gosuslugi.ru/](http://www.gosuslugi.ru/)) найдите информацию по электронной услуге «Установление запрета на получение кредита».

Всех ли видов кредита коснётся запрет, установленный с помощью этой услуги?

Какие виды запретов можно установить?





# ПРАКТИКУМ

## Ответ на задание № 4

### Установление запрета на получение кредита

Услуга поможет установить запрет на заключение с вами кредитных договоров

#### Чего не коснётся запрет

Ипотечных, образовательных и автокредитов

#### Какой запрет можно установить

- Полный, который включает в себя все виды запретов
- На дистанционное и очное получение кредита в кредитной или микрофинансовой организации





# ТЕСТИРОВАНИЕ





# ТЕСТИРОВАНИЕ

## Тест № 1

Как расшифровывается правило «Трех С»?

- а) Сомнение, Следствие, Суд
- б) Стоп, Сброс, Созвон
- в) Созвон, Сбор, Сброс
- г) Созвон, Совет, След





# ТЕСТИРОВАНИЕ

## Тест № 1

Как расшифровывается правило «Трех С»?

- а) Сомнение, Следствие, Суд
- б) **Стоп, Сброс, Созвон**
- с) Созвон, Сбор, Сброс
- д) Созвон, Совет, След





# ТЕСТИРОВАНИЕ

## Тест № 2

Легальность деятельности каких организаций можно проверить на сайте Банка России? (отметьте все верные ответы)

- а) кредитные организации
- б) микрофинансовые организации
- с) торговые организации
- д) страховые организации





# ТЕСТИРОВАНИЕ

## Тест № 2

Легальность деятельности каких организаций можно проверить на сайте Банка России? (отметьте все верные ответы)

- a) **кредитные организации**
- b) **микрофинансовые организации**
- c) торговые организации
- d) **страховые организации**





# ТЕСТИРОВАНИЕ

## Тест № 3

Проверить свою кредитную историю онлайн можно, используя... (отметьте все верные ответы)

- а) сайт Банка России
- б) сайты бюро кредитных историй
- с) портал Госуслуг
- д) сайт Минфина России





# ТЕСТИРОВАНИЕ

## Тест № 3

Проверить свою кредитную историю онлайн можно, используя... (отметьте все верные ответы)

- a) сайт Банка России
- b) сайты бюро кредитных историй
- c) портал Госуслуг
- d) сайт Минфина России





# ТЕСТИРОВАНИЕ

## Тест № 4

При подключении сервиса «второй руки» в банке уполномоченное лицо может:

- а) открывать банковские счета
- б) подтверждать или блокировать финансовые операции
- с) самостоятельно определить список операций и лимиты для контроля
- д) самостоятельно распоряжаться деньгами своего доверителя





# ТЕСТИРОВАНИЕ

## Тест № 4

При подключении сервиса «второй руки» в банке уполномоченное лицо может:

- а) открывать банковские счета
- б) **подтверждать или блокировать финансовые операции**
- с) самостоятельно определить список операций и лимиты для контроля
- д) самостоятельно распоряжаться деньгами своего доверителя





# ТЕСТИРОВАНИЕ

## Тест № 5

Средства в цифровых рублях... (отметьте все верные ответы)

- а) предназначены для платежей и переводов
- б) могут быть помещены во вклад под проценты
- в) хранятся на цифровых банковских счетах
- г) хранятся в цифровых кошельках на платформе Банка России





# ТЕСТИРОВАНИЕ

## Тест № 5

Средства в цифровых рублях... (отметьте все верные ответы)

- a) **предназначены для платежей и переводов**
- b) могут быть помещены во вклад под проценты
- c) хранятся на цифровых банковских счетах
- d) **хранятся в цифровых кошельках на платформе Банка России**





# Больше полезной информации можно найти

на портале [моифинансы.рф](http://моифинансы.рф)  
и в социальных сетях

