ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФМЦ ИФГ

Федеральный методический центр по финансовой грамотности населения на базе Институт финансовой грамотности Финуниверситета

Новое в технологиях мошенничества

Спикер: Трофимов Дмитрий Викторович
к.э.н., доцент Департамента банковского дела и финансовых рынков, эксперт ФМЦ ИФГ

Схемы мошенничества

В 2024-2025 годах мошенничество в платежной сфере приобрело новые масштабы и формы, обусловленные стремительным развитием технологий и социальной инженерии.

Злоумышленники активно используют:

- нейросети для создания фейков,
- фишинговые схемы с поддельными QR-кодами
- эксплуатируют доверие граждан через псевдо-трудоустройство и восстановление карт
- используют новые схемы, связанные с введением цифрового рубля

Эти методы стали более изощренными, ориентированными на обход традиционных систем безопасности и манипуляцию человеческим фактором.

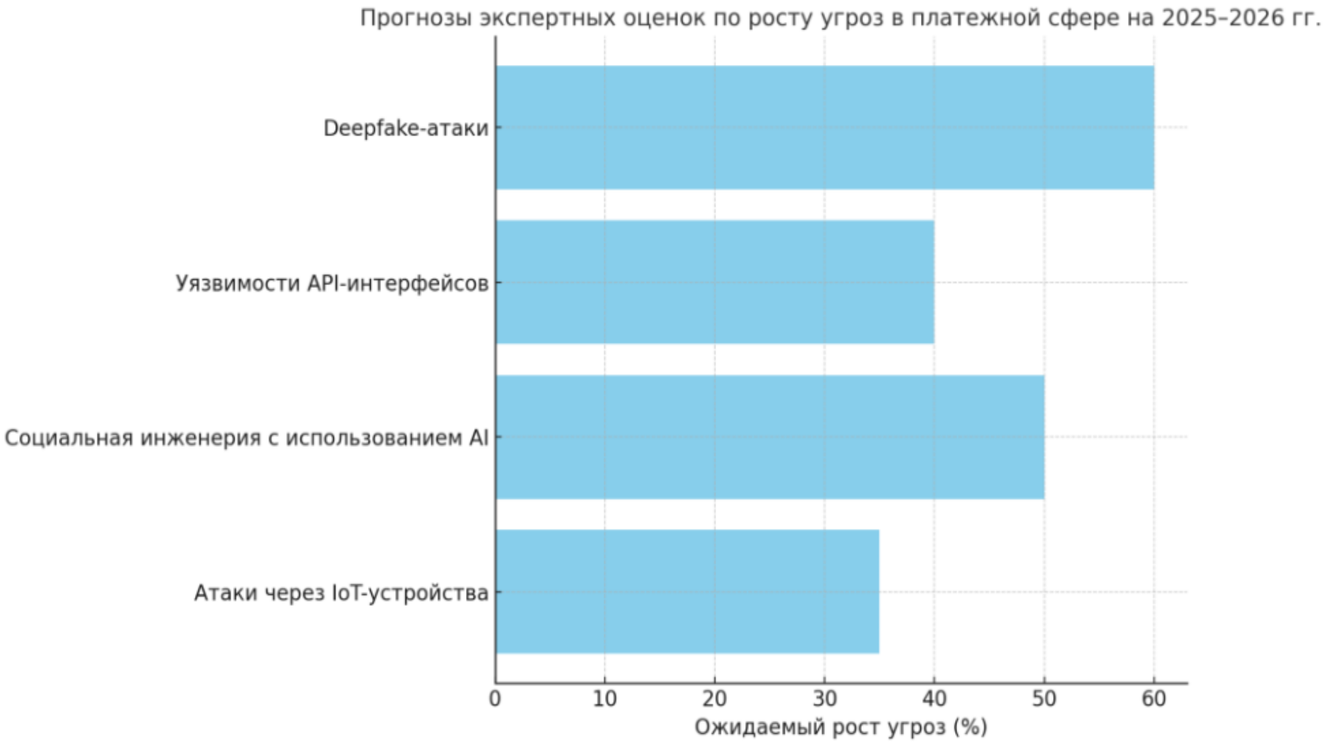
Схемы мошенничества

В 2024 году число мошеннических операций **в платёжных системах** увеличилось на 27% (данные FinCERT ЦБ РФ).

- Атаки с использованием социальных сетей и мессенджеров составили до 45% от общего числа случаев.
- AI-атаки и deepfake-мошенничества выросли более чем в 3 раза относительно 2023 года (отчёт Positive Technologies, Kaspersky).
- Потери финансовых учреждений СНГ от платёжного мошенничества превысили $120 млн (2024, ENISA).
- Эти методы стали более изощренными, ориентированными на обход традиционных систем безопасности и манипуляцию человеческим фактором.

Схемы мошенничества

- ✓ Ожидается увеличение атак через IoT-устройства, встроенные платёжные сервисы автомобилей и бытовой техники (2025–2026).
- ✓ Усиление роли социальных и психологических аспектов мошенничества (психологическое давление, использование AI-ботов).
- ✓ Повышение сложности противодействия ввиду массового распространения API-интеграций и моментальных платежей.



Источник: Экспертный отчёт Positive Technologies, Kaspersky Lab (2024)

Схемы мошенничества

Виртуальные образы банковских карт через вредоносные приложения

Под предлогом «защиты средств» мошенники убеждают установить поддельные приложения, маскирующиеся под программы ЦБ или банков. В процессе «настройки» жертва прикладывает карту к телефону и вводит CVV-код, что позволяет создать её виртуальный дубликат для бесконтактных платежей через NFC.

Масштаб угрозы:

- С ноября 2024-го по февраль 2025-го ущерб вырос в 5 раз — с 40 млн до 200 млн рублей.
- К марту 2025 года заражены более 180 000 устройств в России.
- В топе поддельных приложений — фейковые программы госорганов, антивирусы и даже «модули» для диагностики автомобилей.

Для предотвращения кражи средств стоит скачивать приложения **только из официальных магазинов** и игнорировать требования незнакомцев.

Схемы мошенничества

Виртуальные образы банковских карт через вредоносные приложения

Мошенники используют сложную цепочку действий для кражи средств через NFC-платежи.

1. **Рассылка вредоносных файлов.** Злоумышленники отправляют через WhatsApp или Telegram APK-файлы, замаскированные под популярные приложения (например, «Госуслуги», «Центральный банк РФ», «Telegram Video Player»), фотоархивы («Фотографии.арк») или провокационный контент.
2. **Установка трояна.** Жертва скачивает и устанавливает файл, игнорируя предупреждения системы о рисках. Приложение запрашивает разрешения на доступ к NFC, уведомлениям и административным функциям смартфона.
3. **Активация CraxsRAT.** После установки троян CraxsRAT скрытно внедряется в систему. Он передает злоумышленникам полный контроль над устройством: доступ к SMS, банковским уведомлениям, а также возможность удаленно управлять функциями смартфона.
4. **Кража данных карты.** Под предлогом «настройки защиты» мошенники через поддельное приложение просят пользователя приложить карту к смартфону (для считывания через NFC) и ввести CVV. Данные автоматически передаются злоумышленникам.
5. **Создание виртуального дубликата.** С помощью приложения NFCGate преступники формируют цифровую копию карты, привязанную к мошенническому кошельку.
6. **Перехват кодов подтверждения.** CraxsRAT блокирует или перенаправляет SMS с OTP-кодами на другой номер, позволяя списывать деньги без ведома жертвы.

Схемы мошенничества

Мошенничество под видом операторов сотовой связи

В 2024-2025 годах участились случаи мошенничества, при котором злоумышленники, выдавая себя за **сотрудников телекоммуникационных компаний**, получают доступ к аккаунтам на портале «Госуслуги» или персональным данным абонентов.

Прецедент:

Пенсионерка из Краснодара получила звонок от «МТС» с угрозой потери номера. Она продиктовала код из SMS, перешла по ссылке и ввела «подтверждающий код». Через час её аккаунт на «Госуслугах» был взломан, а на имя жертвы оформили микрозайм в 300 тыс. рублей.

Схемы мошенничества

Мошенничество под видом операторов сотовой связи

Схема 1: **«Продление договора»** — пошаговый сценарий

1. **Звонок под ложным предлогом.** Мошенник представляется сотрудником оператора связи и сообщает, что срок действия договора на номер жертвы «истекает», а без срочного продления номер будет передан другому лицу. Для усиления давления использует фразы: «Ваш номер заблокируют через 2 часа», «Иначе вы потеряете все данные» и др.

2. **Запрос SMS-кода.** Злоумышленник просит продиктовать код из SMS, который якобы необходим для «продления договора». На самом деле это код подтверждения входа в аккаунт «Госуслуг» или личный кабинет оператора, инициированный мошенниками.

3. **Фишинговый переход по ссылке.** Жертве отправляют ссылку (например, «gosuslugi-renew.ru»), маскирующуюся под официальный сайт. На поддельной странице требуется ввести «дополнительный код», который на самом деле является паролем для сброса или подтверждения изменений в аккаунте.

4. **Захват аккаунта «Госуслуги».** Используя полученные коды, мошенники полностью берут контроль над учётной записью жертвы. Через портал они получают доступ к паспортным данным, ИНН, информации о собственности и даже электронной подписи.

Схемы мошенничества

Мошенничество под видом операторов сотовой связи

Схема 2: «Смена тарифа/SIM-карты» — пошаговый сценарий

1. **Ложное предложение выгоды.** Мошенник звонит абоненту, предлагая «уникальный тариф» или сообщает о необходимости замены SIM-карты из-за «утечки данных». Часто звучат фразы: «Для вас действует спецпредложение», «Ваша карта скомпрометирована».

2. **Перехват SMS-кода.** Жертву просят продиктовать код из сообщения, который якобы подтверждает смену тарифа. На деле это код авторизации в личном кабинете оператора.

3. **Настройка переадресации.** Получив доступ, мошенники активируют скрытую переадресацию звонков и SMS на свои номера через настройки оператора. Это позволяет перехватывать коды двухфакторной аутентификации от банков.

4. **Оформление кредитов.** Используя доступ к SMS, злоумышленники подтверждают операции в банковских приложениях, оформляют кредиты или переводят деньги на подконтрольные счета.

Схемы мошенничества

Мошенничество под видом операторов сотовой связи

Схема 2: «Смена тарифа/SIM-карты» — пошаговый сценарий

Прецедент:
Житель Москвы согласился «подключить новую опцию» и сообщил код из SMS. Через сутки он обнаружил, что не получает звонки и сообщения. Позже выяснилось, что мошенники оформили три кредита на его имя, используя перехваченные SMS-коды от банков.

Как защититься?

- Никогда не сообщайте коды из SMS, даже если звонящий называет ваши персональные данные (это может быть информация из утечек).
- Не переходите по ссылкам из сообщений или звонков — проверяйте информацию через официальные приложения или сайты.
- Отключите переадресацию через USSD-команду (например, ##002# для большинства операторов).
- Включите двухэтапную аутентификацию на «Госуслугах» и в банковских сервисах.

Схемы мошенничества

Эволюция мошенничества в 2024-2025 годах демонстрирует, что злоумышленники всё чаще атакуют через социальную инженерию и уязвимости цифровых сервисов.

Помимо нейросетевых подделок и фишинга, угрозы включают манипуляции под видом операторов связи, позволяющие захватывать аккаунты на «Госуслугах» и перехватывать SMS-коды для финансовых махинаций.

Гражданам необходимо помнить: никогда нельзя передавать коды из сообщений, даже если звонящий ссылается на «официальные процедуры».

Финансовым организациям и государству стоит усилить защиту персональных данных, внедрить дополнительные механизмы верификации и активнее информировать население о новых схемах обмана

Только сочетание технологической бдительности и личной осторожности поможет снизить риски в условиях растущей изощренности киберпреступников.

Противодействие мошенничеству

Создание государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий

Федеральный закон от 1 апреля 2025 г. № 41-ФЗ

Основные положения:

1. Пользователями государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, являются

- Генеральная прокуратура Российской Федерации
- Следственный комитет Российской Федерации
- Центральный банк Российской Федерации
- кредитные организации
- операторы связи
- федеральные органы исполнительной власти
- организации, перечень которых утверждается Правительством Российской Федерации

Противодействие мошенничеству

2. Мероприятия по противодействию выдаче наличных денежных средств без добровольного согласия клиента с использованием банкоматов

Кредитная организация, предоставившая клиенту платежную карту, до выдачи наличных денежных средств с банковских счетов клиента с использованием банкоматов **обязана осуществить проверку** на наличие признаков выдачи наличных денежных средств без добровольного согласия клиента с использованием банкоматов.

При наличии признаков выдачи наличных денежных средств без добровольного согласия клиента с использованием банкоматов кредитная организация, предоставившая клиенту платежную карту, **на 48 часов** с момента направления запроса на выдачу наличных денежных средств **обязана ограничить** выдачу наличных денежных средств на сумму ***не более 50 тысяч рублей в сутки*** и незамедлительно уведомить клиента о причинах такого ограничения.

Кредитная организация обязана ограничить выдачу наличных денежных средств с использованием банкоматов на сумму не более 100 тысяч рублей в месяц, если от Банка России получена информация, содержащаяся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, которая содержит сведения, относящиеся к клиенту и (или) его электронному средству платежа.

Противодействие мошенничеству

3. Введение уполномоченных лиц

Кредитная организация обязана обеспечить клиенту - физическому лицу по соглашению с такой кредитной организацией и лицом, уполномоченным клиентом, возможность наделить такое лицо статусом **уполномоченного лица** для получения подтверждения совершения:

- операции по переводу денежных средств с банковских счетов (вкладов), открытых указанному клиенту в этой кредитной организации
- операции по получению клиентом - физическим лицом наличных денежных средств с банковских счетов (вкладов), открытых указанному клиенту в этой кредитной организации,

Клиент - физическое лицо вправе выбрать одну или несколько операций по переводу денежных средств или операций по получению наличных денежных средств, определить критерии операций, требующих подтверждения уполномоченным лицом, а также банковские счета (вклады) клиента - физического лица, операции по которым требуют подтверждения уполномоченным лицом.

Противодействие мошенничеству

4. Предоставление микрозаймов

Использование упрощенной идентификации **не допускается** в целях заключения договора потребительского кредита (займа) микрофинансовой организацией.

Микрофинансовые организации при дистанционном приеме на обслуживание клиента - физического лица **обязаны** осуществлять идентификацию клиента, представителя клиента путем установления и подтверждения достоверности сведений о них с использованием единой системы идентификации и аутентификации и единой биометрической системы.

При дистанционном заключении каждого договора потребительского кредита (займа) микрофинансовые организации **обязаны** обеспечить аутентификацию клиента с использованием единой системы идентификации и аутентификации и единой биометрической системы.

Микрофинансовая организация в целях заключения договора потребительского займа в электронной форме **обязана** осуществлять идентификацию или аутентификацию заемщика с использованием государственной информационной системы "Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных

Противодействие мошенничеству

5. Массовые телефонные вызовы

Массовые или автоматические телефонные вызовы в сети связи общего пользования должны осуществляться при условии получения предварительного согласия абонента, выраженного посредством совершения им действий, однозначно идентифицирующих этого абонента и позволяющих достоверно установить его волеизъявление на получение массовых вызовов.

Массовые вызовы признаются осуществленными без предварительного согласия абонента, если заказчик массовых вызовов в случае осуществления массовых вызовов по его инициативе или оператор связи в случае осуществления массовых вызовов по инициативе оператора связи не докажет, что такое согласие было получено.

Оператор связи, с сети связи которого инициируется телефонный вызов, **обязан передавать** на пользовательское оборудование информацию об абоненте - юридическом лице либо индивидуальном предпринимателе, инициировавших телефонный вызов.

Оператор связи обязан осуществлять взаимодействие с государственной информационной системой противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий.

Противодействие мошенничеству

6. Сообщения в мессенджерах и сети Интернет

Организатор сервиса обмена мгновенными сообщениями, являющийся российским юридическим лицом или гражданином Российской Федерации, обязан осуществлять взаимодействие с государственной информационной системой противодействия правонарушениям.

Провайдер хостинга обязан осуществлять взаимодействие с государственной информационной системой противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий.

ИНСТИТУТ ФИНАНСОВОЙ ГРАМОТНОСТИ

КАНАЛЫ КОММУНИКАЦИИ

ОФИЦИАЛЬНЫЕ СООБЩЕСТВА В СОЦИАЛЬНЫХ СЕТЯХ

VK.COM/IFGFU

T.ME/FINGRAMOTA_IFG

ОФИЦИАЛЬНЫЙ САЙТ

IFG@fa.ru

- методические материалы
- разбор кейсов, практик, сложных ситуаций по финансовой грамотности
- ответы на вопросы
- анонсы мероприятий
- новости ИФГ и не только

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФМЦ ИФГ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФМЦ ИФГ

Институт финансовой грамотности – федеральный методический центр повышения финансовой грамотности

IFG@fa.ru