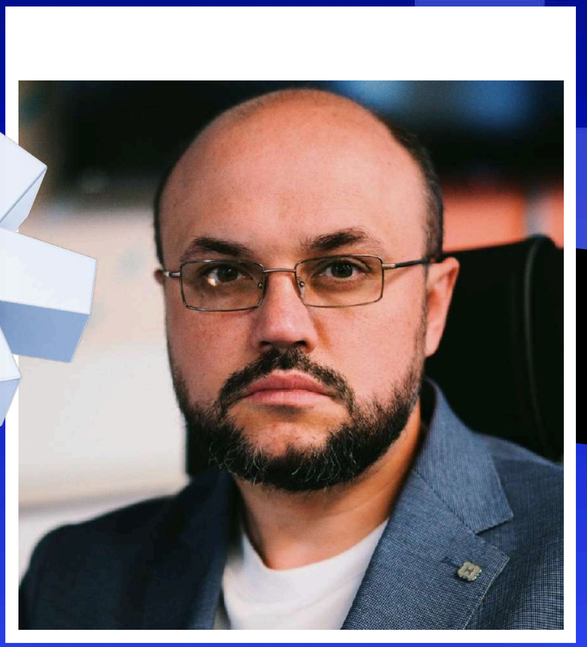
ФРОД VS АНТИФРОД

Актуальные сценарии фрода
и способы противодействия

СОВКОМБАНК ТЕХНОЛОГИИ

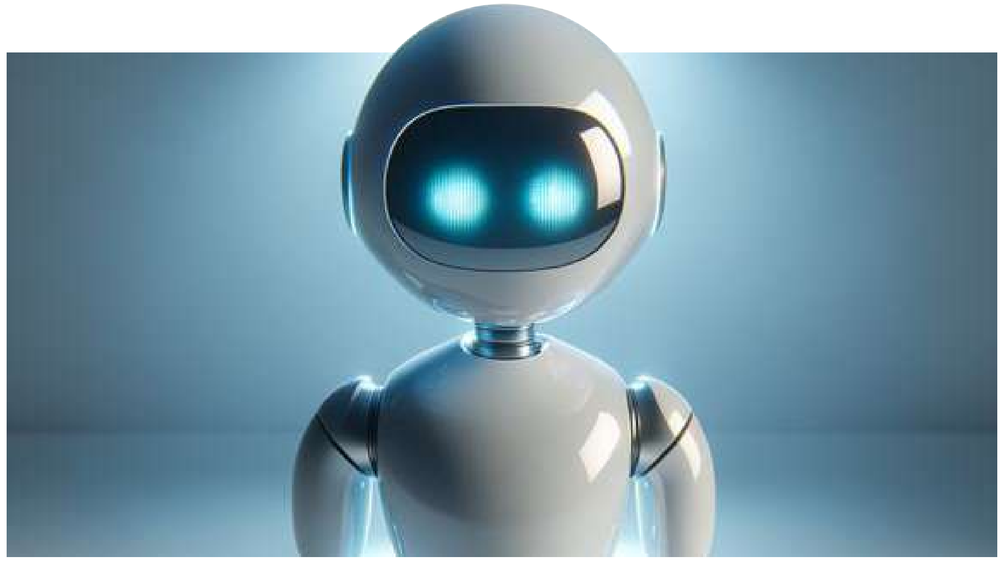


Леонов Семён

ТЕМЫ ВЫСТУПЛЕНИЯ

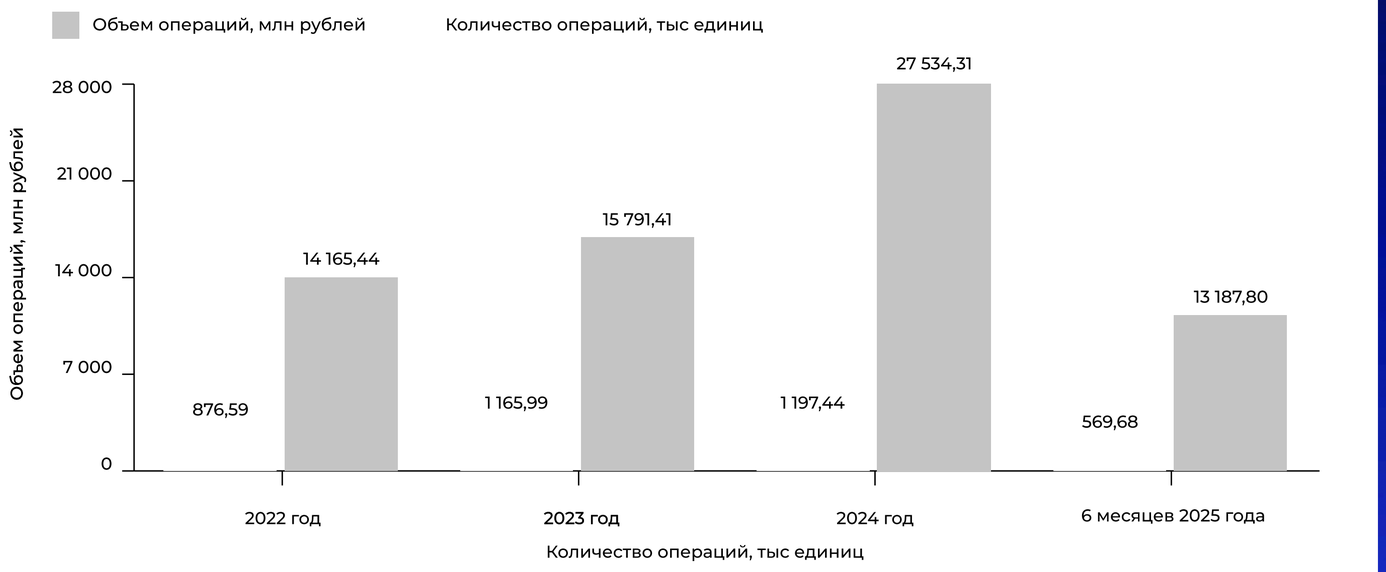
СОВКОМБАНК ТЕХНОЛОГИИ

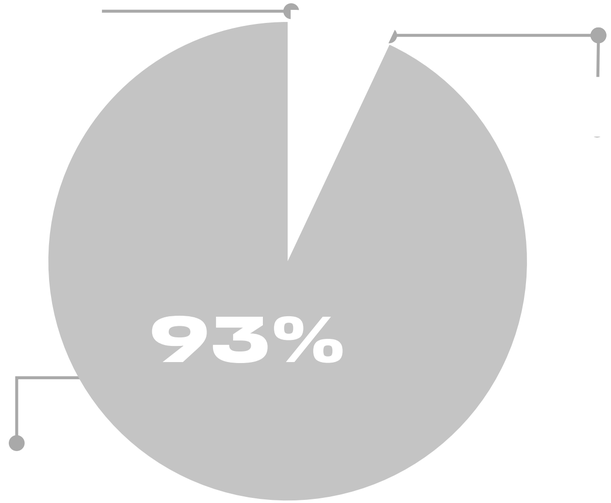
- Потери от кибермошенничества
- Основные сценарии мошенничества
- NFC Gate
- Способы противодействия мошенничеству
- Новые возможности
- Перспективы развития



ОСНОВНЫЕ СЦЕНАРИИ МОШЕННИЧЕСТВА

СОВКОМБАНК ТЕХНОЛОГИИ





Ежегодно увеличивается количество попыток мошенничества, основной тип – социальная инженерия

СЦЕНАРИИ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

СОВКОМБАНК ТЕХНОЛОГИИ

1. Замена домофона, выдача ключей, курьерская доставка и т.д.
2. Оформление кредита и его перевод на **безопасный счет**
3. Инвестиции, доп. заработок (спортивные ставки, криптовалюта, акции и т.д.)

Разнообразные схемы, мошенники идут в ногу со временем и подстраиваются под окружающую действительность

NFC GATE

СОВКОМБАНК ТЕХНОЛОГИИ

Relay-атака, при которой информационный обмен между картой и банкоматом осуществляется через сеть Интернет. Такие атаки эксплуатируют уязвимость протокола NFC, позволяя злоумышленникам инициировать транзакции, находясь далеко от Держателя карты

Обманом заставляют жертву:

- Установить ПО
- Приложить карту к смартфону
- Ввести пин-код от карты (или предварительно его меняют)

- На смартфон жертвы устанавливается ВПО на которые мошенники транслируют свою карту и обманом заставляют жертву вносить на нее деньги

Многоэтапная атака, активно используются мошенниками со второй половины 2024 года

ПРОТИВОДЕЙСТВИЕ NFC GATE

СОВКОМБАНК ТЕХНОЛОГИИ

Банки научились эффективно бороться с новым сценарием мошенничества

Технические меры направленные на запрет реализации подобного сценария на банкоматах

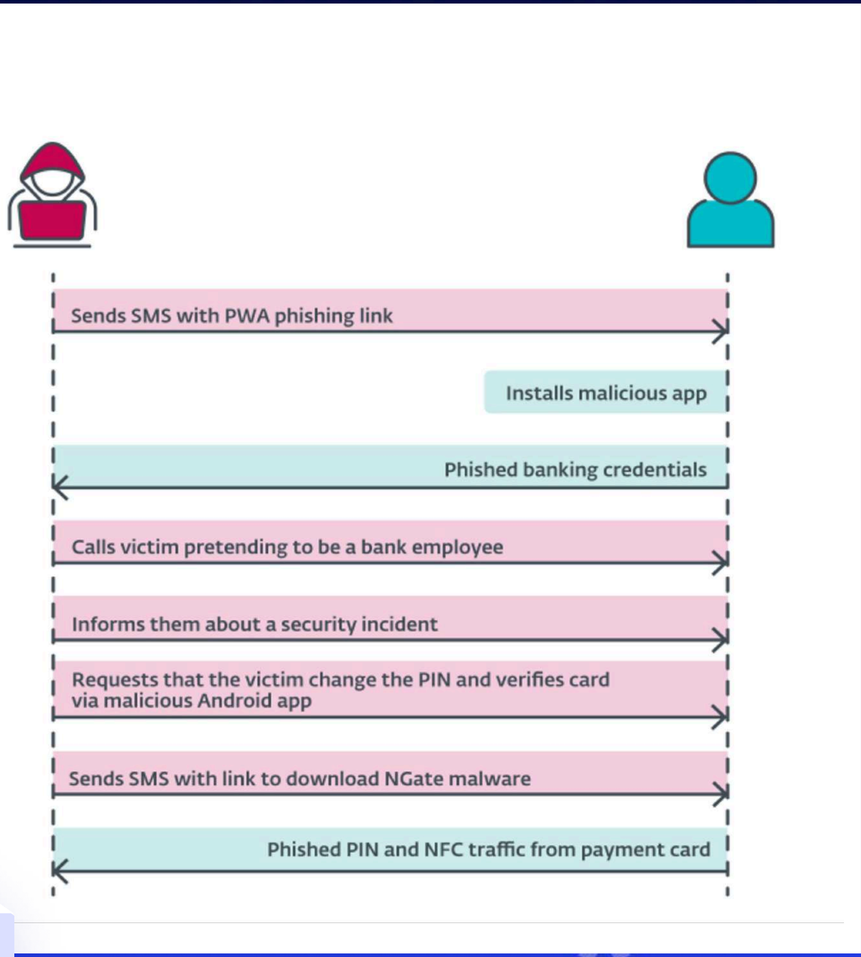
- Ограничения на максимальное время ответа карты

Анализ транзакционной активности

- Соответствие типа и места проведения предыдущим операциям Клиента

Выявление вирусного ПО на смартфоне Клиента

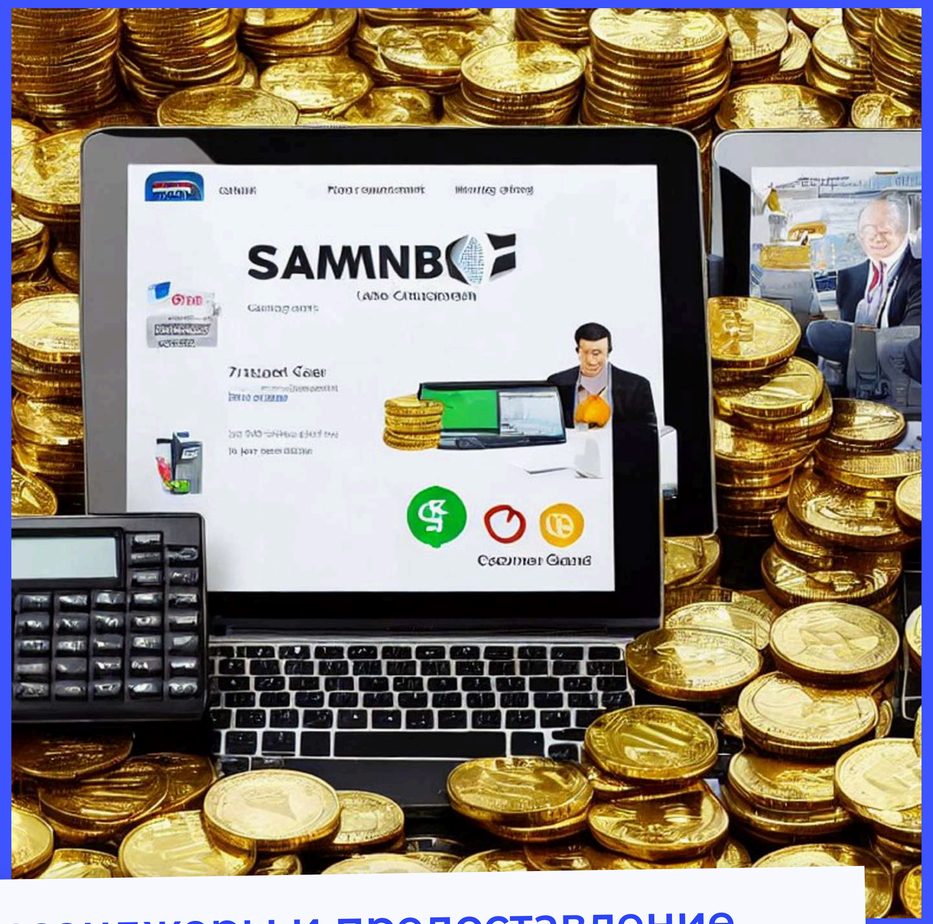
Информирование и обучение противодействию мошенничеству



ФИШИНГ

Основные сценарии фишинга

1. Маркетплейсы
2. Fake Date (сервисы знакомств, фальшивый OnlyFans)
3. Bla-bla-car
4. Доски объявлений, в том числе звонки через данные сервисы
5. Прочее (Оплата парковки, платные дороги, переходы по QR и т.п.)



Перевод общения в мессенджеры и предоставление ссылки на фишинговый ресурс

ОСНОВНЫЕ ИЗМЕНЕНИЯ В СХЕМАХ МОШЕННИЧЕСТВА

СОВКОМБАНК ТЕХНОЛОГИИ

ДЛЯ … НА ГОСУСЛУГИ НЕ ДОСТАВЛЯЕТСЯ ВО ВРЕМЯ АКТИВНОГО ЗВОНКА

Как результат мошенники начинают с доступов в ЛК финансовых маркетплейсов

И SIM-БОКСАМИ

Мошенники переключились на звонки через мессенджеры, а при их блокировке – международные вызовы, заставляют Клиентов звонить на номера мошенников

Банки научились эффективно бороться с «проксированием» nfc трафика от карты – обманом заставляют Клиентов пополнять карты мошенников

(при этом Клиент думает что пополняет собственную для спасения денег)

Мошенники быстро адаптируются к новым мерам противодействия, придумывают новые схемы

ПРОТИВОДЕЙСТВИЕ КИБЕРМОШЕННИЧЕСТВУ

СОВКОМБАНК ТЕХНОЛОГИИ

Антифрод:

- Транзакционный
- Сессионный

Больше данных в антифроде – выше эффективность, ниже ложные срабатывания.

- Запрет трансляции экрана при удаленном доступе в МП
- Черные списки отпечатков устройств
- NFC Gate - не типичные для Клиента операции\место их совершения, выявление вирусного ПО для NFC Gate
- Защита от подмены страниц 3Ds
- Анализ поведения Клиента в ДБО для выявления мошеннических регистраций
- Оперативное выявление дропов (в т.ч. с использованием AI\ML-инструментов)

ДАННЫЕ ДЛЯ АНТИФРОДА

СОВКОМБАНК ТЕХНОЛОГИИ

Поведение Клиентов в МП\ЛК

1. Характер работы в ДБО
2. Нетипичные операции
3. Наличие удаленного доступа
4. Гео-позиция, выявление хостингов, VPN и т.п.

Внешние источники данных

1. Скоринговые данные от операторов
2. Модели поведения\общения клиента (на основе анализа аудио\видео потока при личном звонке\посещении офиса)
3. Списки ФинЦерта
4. Оперативное взаимодействие с участниками рынка

В Банке используются современные технологий – большие языковые модели, машинное обучение, скоринговые модели, сбор информации с устройств (геопозиция, вирусное ПО) и т.д.

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

СОВКОМБАНК ТЕХНОЛОГИИ

УЖЕСТОЧЕНИЕ ПОЛИТИК СБОРА ДАННЫХ СОВРЕМЕННЫМИ ОС

ДАВЛЕНИЕ НА ПОДРОСТКОВ ДЛЯ КРАЖИ

ПОДТВЕРЖДЕНИЕ ОПЕРАЦИЙ КЛИЕНТАМИ ПОД ВОЗДЕЙСТВИЕМ МОШЕННИКОВ

МОШЕННИКИ ЗАСТАВЛЯЮТ КЛИЕНТОВ ЗВОНИТЬ НА НОМЕР МОШЕННИКА

«ОБРАБОТКА» КЛИЕНТОВ МОШЕННИКАМИ – КЛИЕНТЫ ПОД ВОЗДЕЙСТВИЕМ МОШЕННИКОВ ПОДТВЕРЖДАЮТ ОПЕРАЦИИ КОТОРЫЕ БАНК ОСТАНОВИЛ КАК МОШЕННИЧЕСКУЮ

НОВЫЕ ВОЗМОЖНОСТИ И ОБЯЗАННОСТИ

СОВКОМБАНК ТЕХНОЛОГИИ

«Период охлаждения» при выдаче кредита – с 01.09.2025

Ограничение внесения денег на вновь токенизированную платежную карту – не более 50 т.р. в первые 48 часов

Ограничения для тех, кто в ЧС ФинЦерта:

- Запрет на выдачу новых электронных средств платежа;
- Ограничения на перевод ДС – не более 100 тыс\месяц;
- Ограничения на снятие ДС в банкомате - не более 100 тыс\месяц;

Признаки ОБДС при снятии ДС в банкоматах – возможность ограничений на снятие 50 т.р.\сутки на 48 часов

Доверенные лица – возможность установки доверенного лица для подтверждения операций

Запрет доставки СМС от Госуслуг во время телефонного звонка

Микрофинансовыеорганизации должны проверять, действительно ли реквизиты для перечисления онлайн-займа принадлежат заемщику

ДАЛЬНЕЙШИЕ ПЕРСПЕКТИВЫ

СОВКОМБАНК ТЕХНОЛОГИИ

ГИС АНТИФРОД

- Банки
- Операторы связи
- Маркетплейсы
- Соцсети
- Мессенджеры
- Госорганы

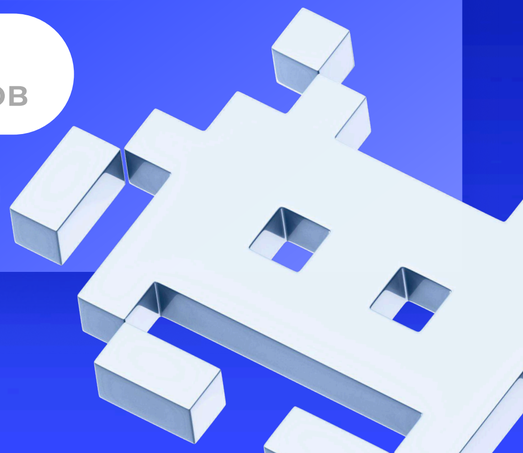
ЗАПРЕТ УПРОЩЕННОЙ ИДЕНТИФИКАЦИИ ДЛЯ МФО – УДАЛЁННАЯ ИДЕНТИФИКАЦИЯ/ АУТЕНТИФИКАЦИЯ ТОЛЬКО ЧЕРЕЗ ЕБС

РАЗВИТИЕ СЕРВИСОВ БИОМЕТРИИ

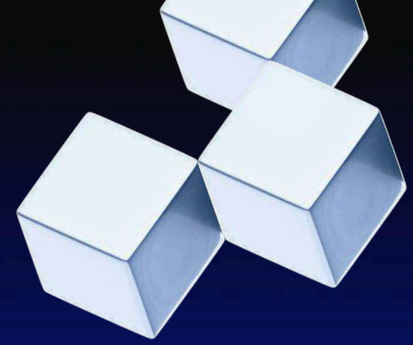
- Возможность прохождения аутентификации с использованием ЕБС\КБС
- Подтверждение отдельных операций с использованием биометрии лица

ВОЗМОЖНО

- Самозапрет на звонки из-за границы
- Внесудебная оперативная блокировка фишинговых сайтов
- Не более 10 карт на человека



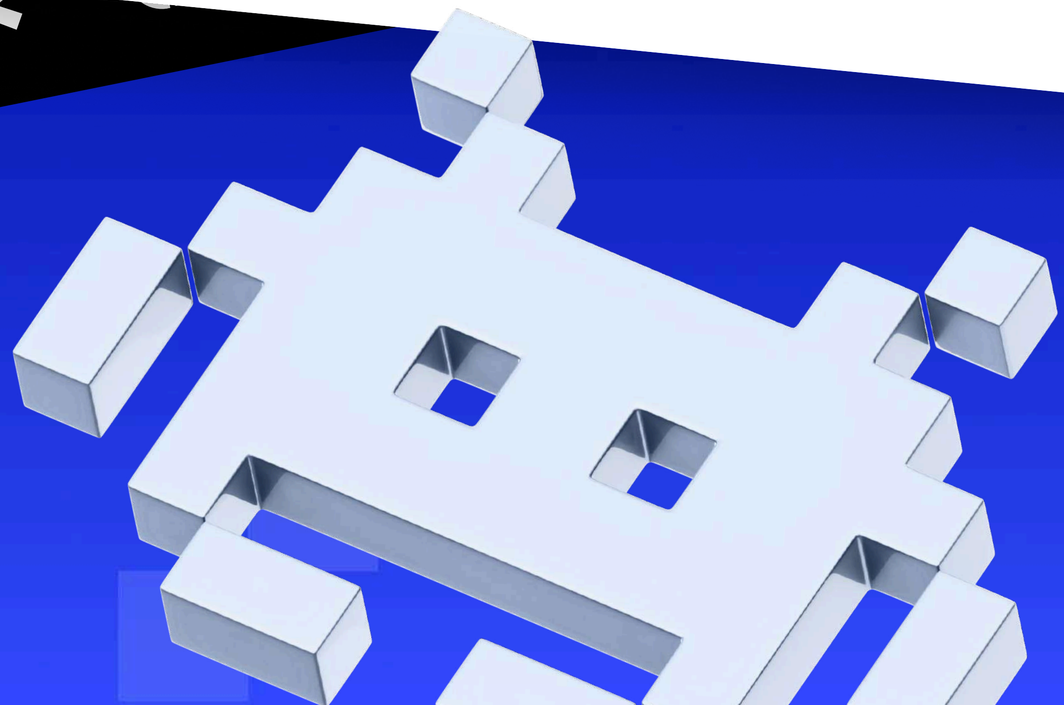
СОВКОМБАНК ТЕХНОЛОГИИ



СОВКОМБАНК ТЕХНОЛОГИИ

СОВКОМБАНК ТЕХНОЛОГИИ

СОВКОМБАНК ТЕХНОЛОГИИ



Готов ответить на вопросы