Информационная безопасность банков 2022

«In phone reputation we trust!? Комплексный подход для предотвращения социальной инженерии»

Брагин Станислав
Менеджер по продукту

kaspersky

Четыре столпа социальной инженерии

Фишинг

Кража данных аккаунта, таргетированные атаки, заражение вредоносами

Вредоносное ПО

Слежка за пользователем, кража данных, удаленный доступ

Звонки мошенников

Использование данных пользователя для принуждения к выполнению операций и установок ПО

Удаленный доступ

Выполнение действий в сессии пользователя, считывание кодов подтверждения и данных аккаунта

Звонки мошенников – верхняя часть пирамиды

9% россиян в результате действий телефонных мошенников понесли денежный ущерб (из них 6% сообщили о значительном ущербе). ***

48% граждан РФ столкнулись с телефонным мошенничеством в 2020, рост YOY - **150%** **

70% звонков с неопознанных номеров в **Q1** 2021 года являются спамом*

6,3% из них мошеннические звонки за **Q1** 2021*

17% рост мошеннических звонков за **Q2** 2021*

34%. полагают, что в будущем могут лишиться средств в результате действий телефонных мошенников ***

~ 10 млрд. руб. объем операций без согласия клиента**

* - по данным статистики Kaspersky WhoCalls
** - по данным опроса ЦБ
*** - опрос ВЦИОМ 07.05.21

Kaspersky Who Calls SDK

Угрозы

- Звонки клиентам с целью выманивания конфиденциальной информации или втягивания в выполнение сценариев мошенников
- Навязчивые звонки и предложение сомнительных услуг

Задачи

- Выявление потенциально мошеннических звонков клиенту (соц. инженерия)
- Уведомление клиента банка о мошенническом и СПАМ звонках
- Предоставление бесшовной технологи обработки звонков

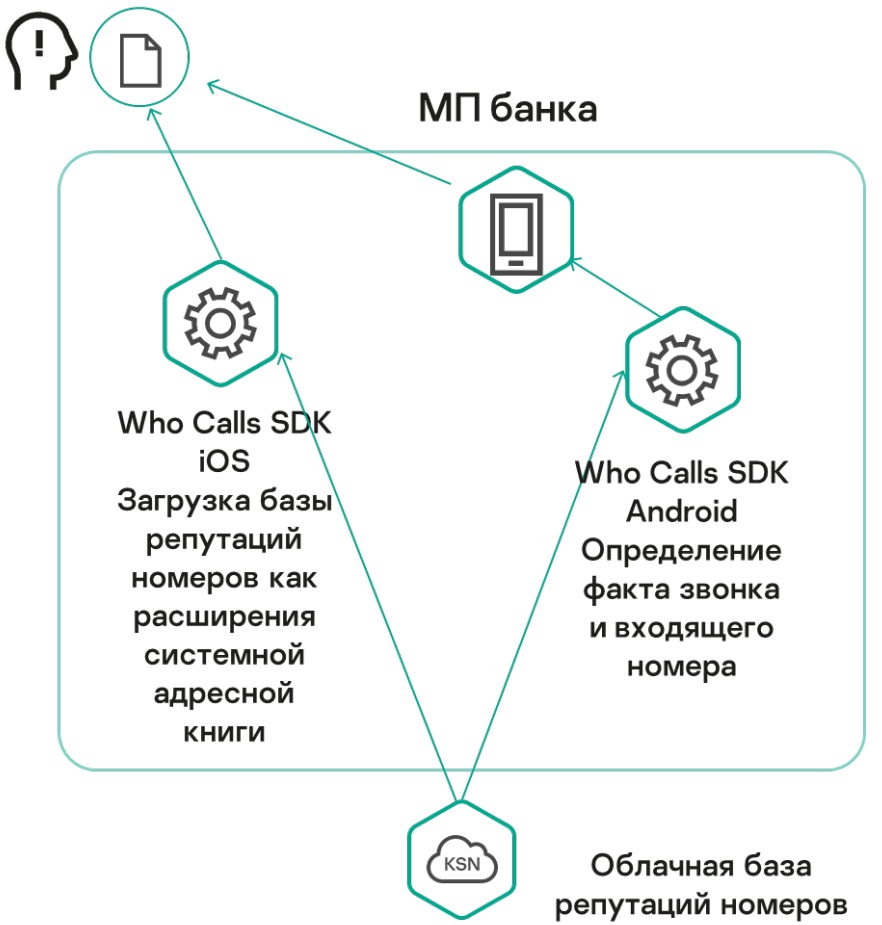
Методы противодействия

- Оповещение о входящем звонке с предоставлением доступных параметров
- Репутация номера по базе на основе машинного обучения и отзывов пользователей

Ваш сценарий

- Гибкая реализация взаимодействия с пользователем
- Возможность приводить пользователя в приложение за расширенной информацией или обновлениями
- Проверка произвольных номеров и возможность доступа к другим сервисам репутации «Лаборатории Касперского»

Использование Kaspersky Who Calls SDK и REST API



iOS

- Нет доступа к журналу звонков и информации о входящем вызове из приложения
- Базы с информацией о номерах загружаются на устройство как расширение адресной книги
- Обработка звонка и отображение информации о номере из базы выполняется системными методами без запуска приложения.

Android

- SDK может оповещать приложение о поступлении звонка и получать входящий номер
- Реализация отличается в зависимости от версии ОС
- Взаимодействие с пользователем на стороне приложения владельца сервиса

Web

- Репутация может запрашиваться для пакета номеров через REST API.

Какие данные предоставляем

В мобильном SDK и REST API предоставляется примерно одинаковый набор данных, соответствующих premium режиму приложения Kaspersky Who Calls

- **Категория:**

  Салоны красоты; медицинские услуги; подозрение на мошенничество; финансовые риски etc.

- **Желтые страницы:**

  Название организации.

- **СПАМ:**

  Признак нежелательного звонка.

- **Ситуационный текст:**

  “Вероятно полезный звонок”; “Возможно звонок из банка, не сообщайте pin коды и пароли”

Победа?

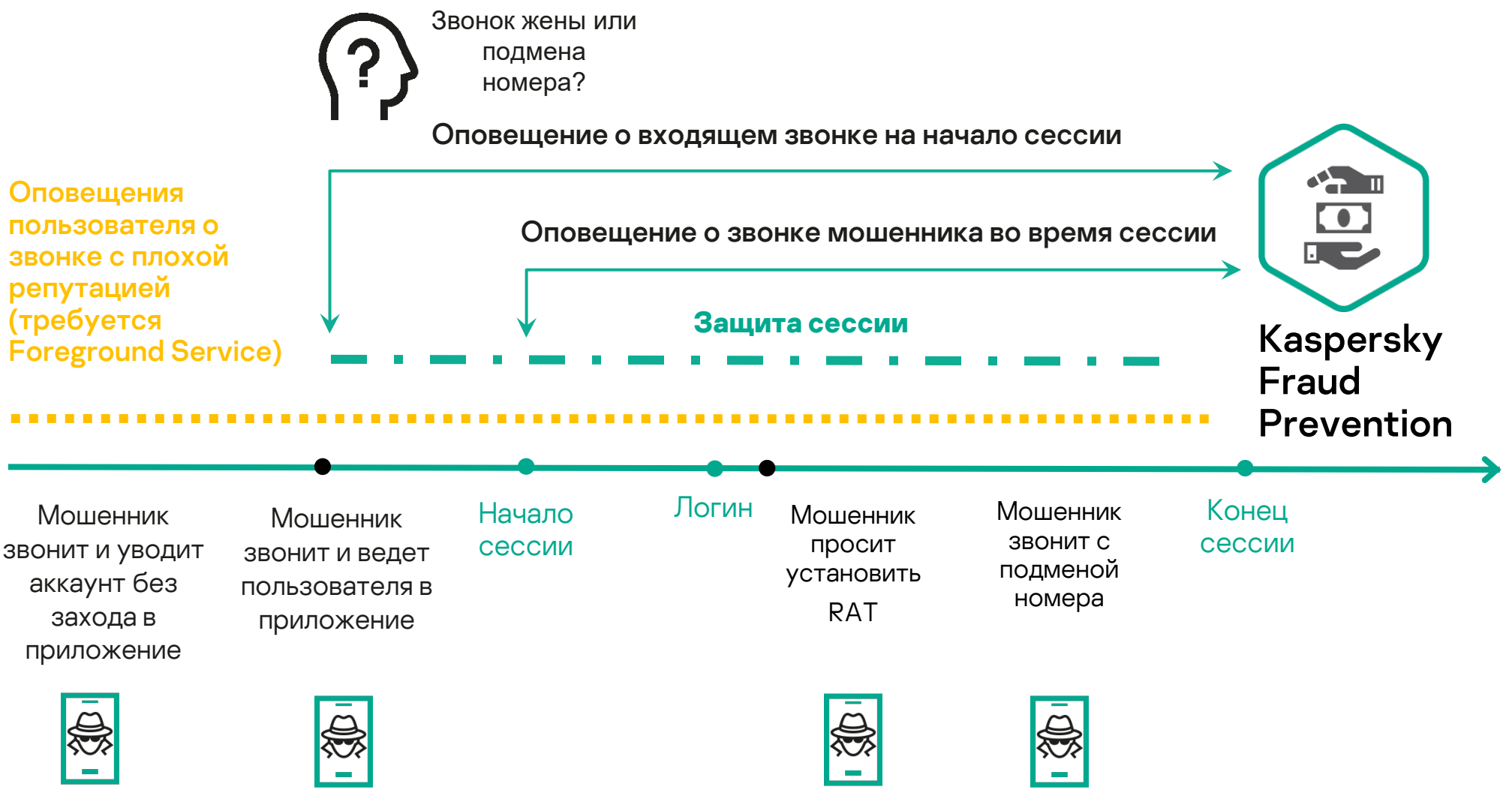
- Высокая гибкость мошенников
- Звонки с подменой номера
- Асимметрия защитник – атакующий

Защита в двух направлениях

Оповещение пользователя

Источник данных для антифрод системы

Сценарии атак и возможности предотвращения.



Красные флажки для сессионного антифрода.

Только на их сочетании можно построить достаточно стойкую и адаптивную модель для детектирования такого многогранного явления как социальная инженерия

Признаки Account takeover

Аномальная активность пользователя в сессии

Зараженное устройство

Переход по фишинговым ссылкам и платежи с фишинговых сайтов

Признаки удаленного контроля и трансляции экрана

Биометрические аномалии ?

Телефонная активность в окрестностях сессии

Звонки с номеров с плохой репутацией

170+ категорий подозрительной активности

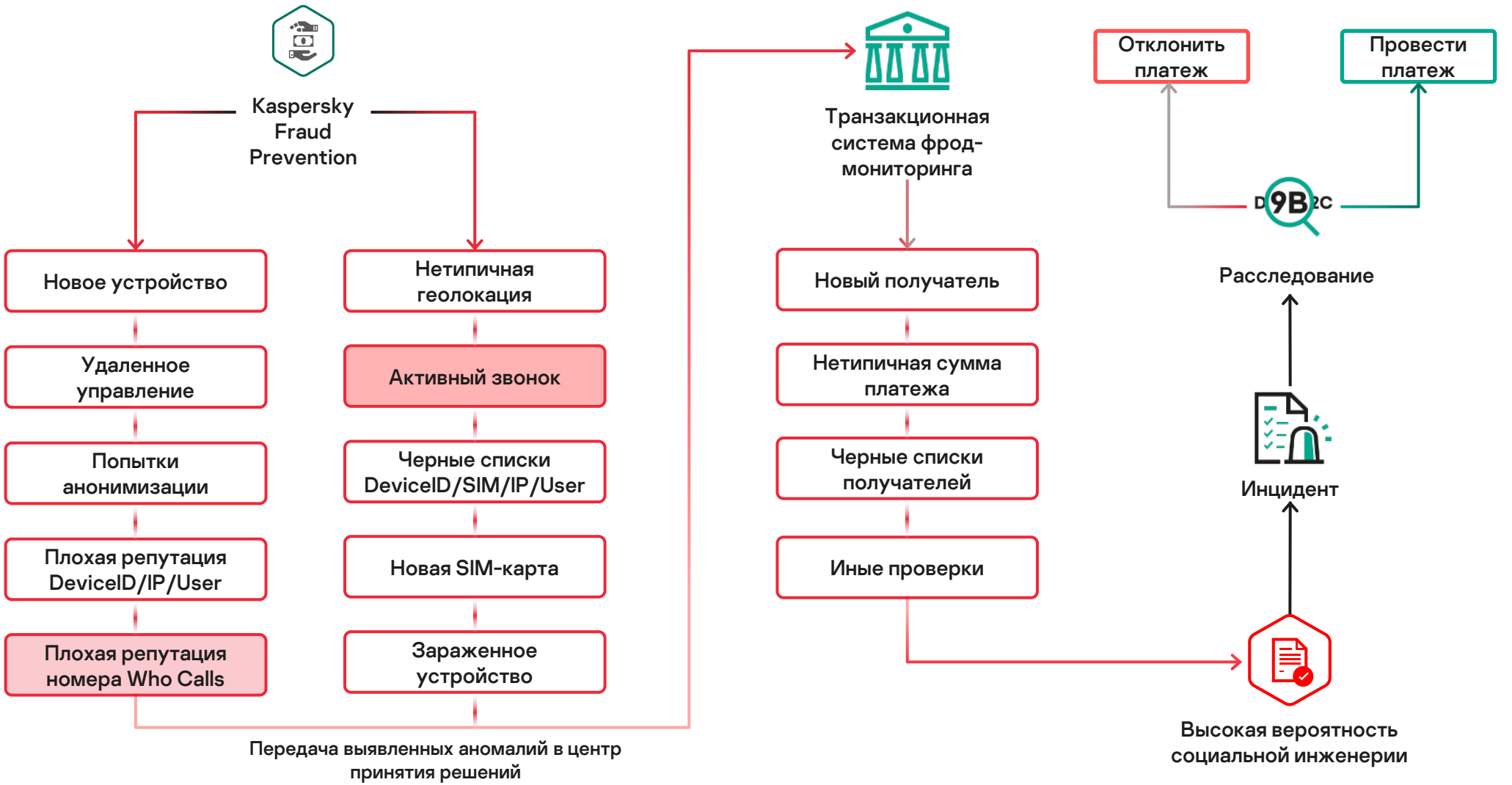
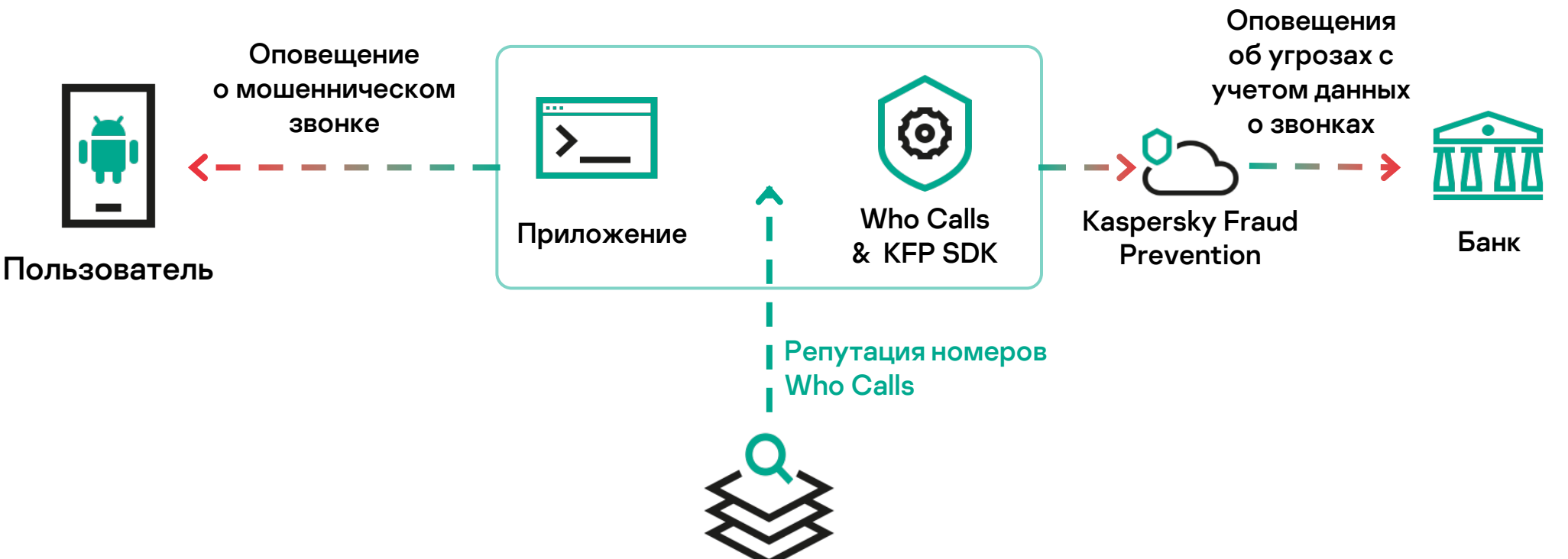


Иллюстрация взаимодействия Kaspersky Who Calls SDK и Kaspersky Fraud Prevention на примере Android



Спасибо за внимание!

Kaspersky Who Calls SDK, Who Calls REST API и Kaspersky Fraud Prevention доступны для пилотного и коммерческого использования.

Будем рады рассказать подробнее на нашем мобильном стенде.

Брагин Станислав **Менеджер по продукту** **Stanislav.bragin@Kaspersky.com**

kaspersky