Вызовы цифровой экономики: практические кейсы

билайн

Центр управления безопасностью билайна

49 907

количество спасенных жертв мошенничества

233 410

количество блокированных мошеннических звонков

22 813

количество выявленных телефонных номеров мошенников

4 мин.

средняя продолжительность мошеннической атаки

5

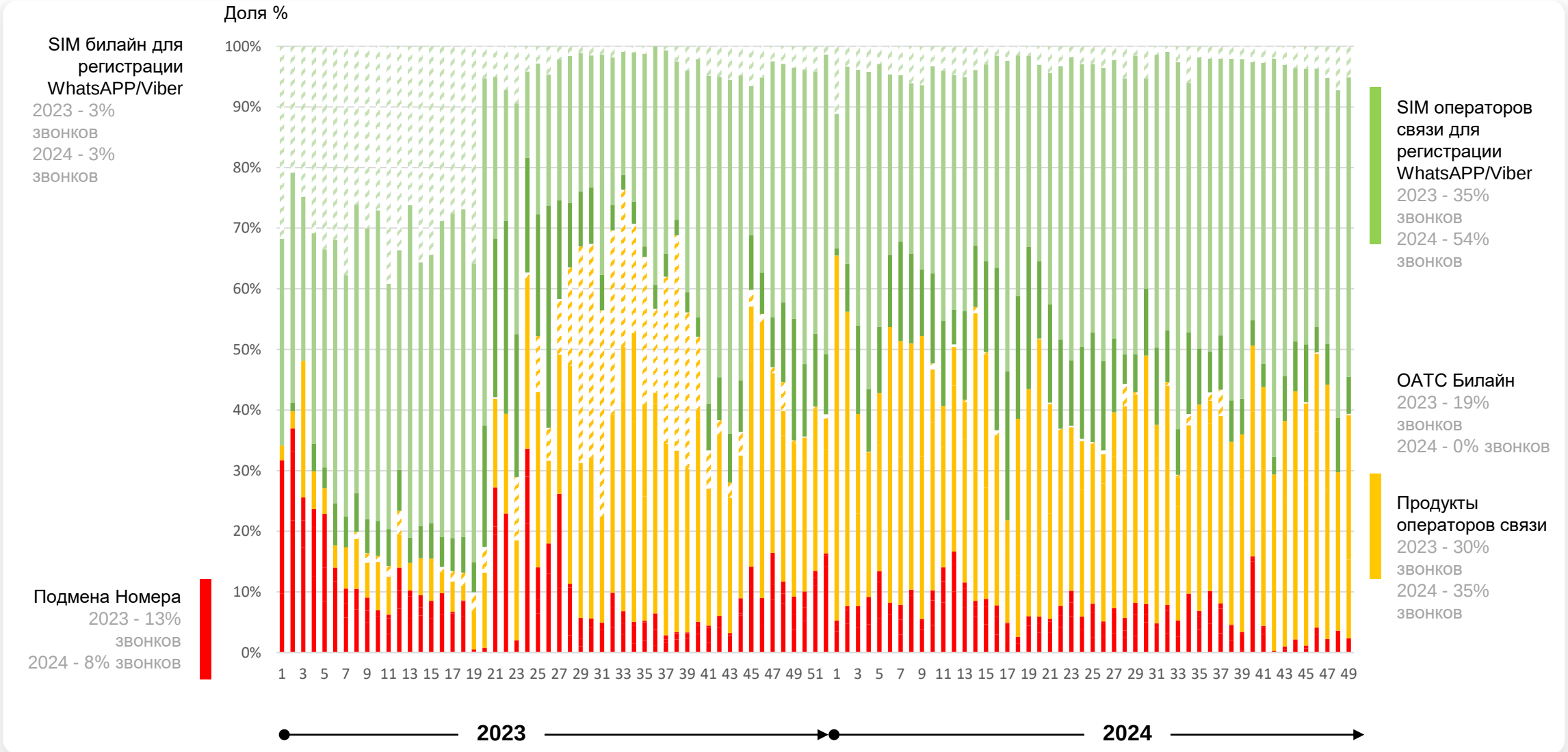
среднее количество звонков во время мошеннической атаки

401

количество обращений абонентов в группу быстрого реагирования

● В эфире

Источники мошеннического трафика (жалобы абонентов)

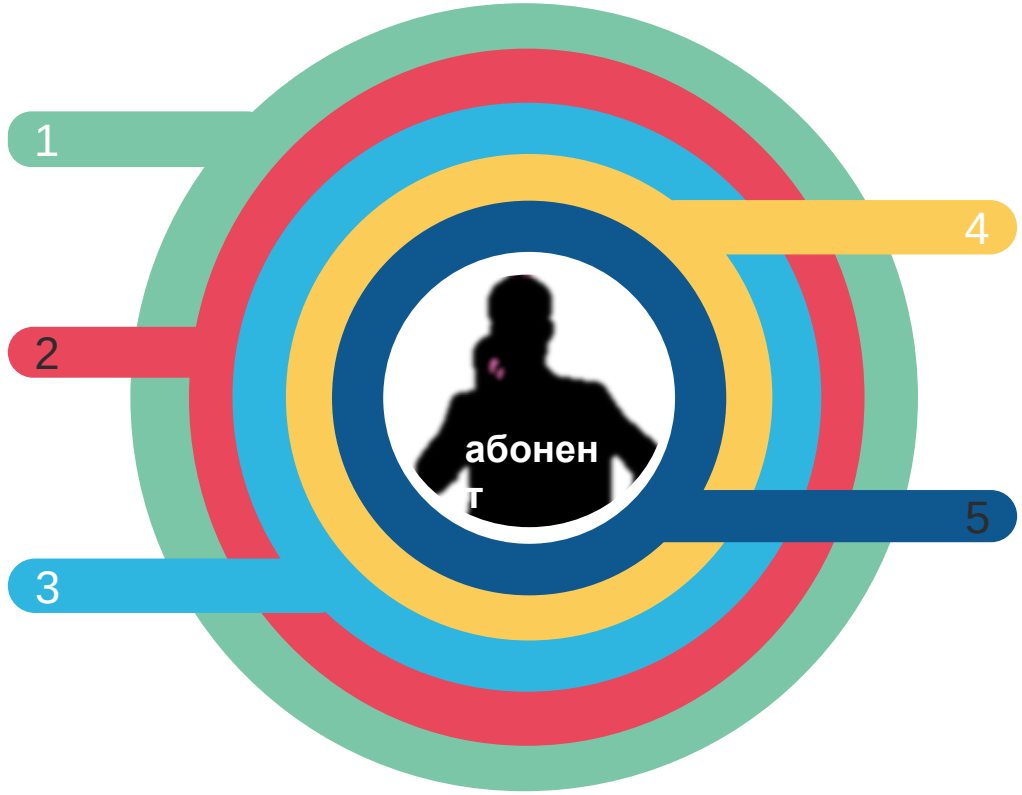


Источники мошеннического трафика определяются по жалобам абонентов билайн полученных от банков, ФинЦЕРТ, Минцифры

Купол безопасности - охлаждение абонентов, находящихся под влиянием мошенников

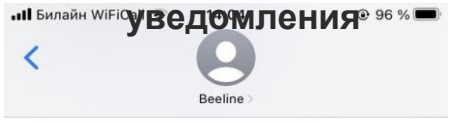
1 **Антифрод купол** – нет входящей связи от других операторов в течении 3 min 10 s

+ Информирование о пропущенных звонках



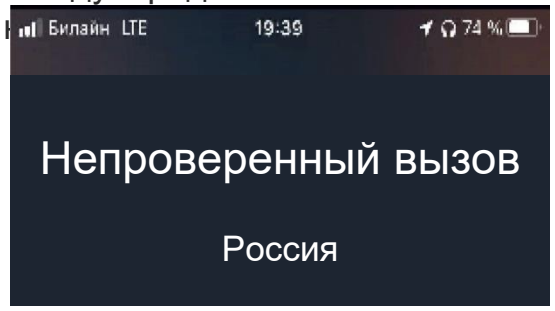
4 **Антифрод купол для WhatsApp -** управление интернет трафиком, трафиком WhatsApp

2 **SMS и Push уведомления**



ВНИМАНИЕ!
Билайн фиксирует атаку мошенников!

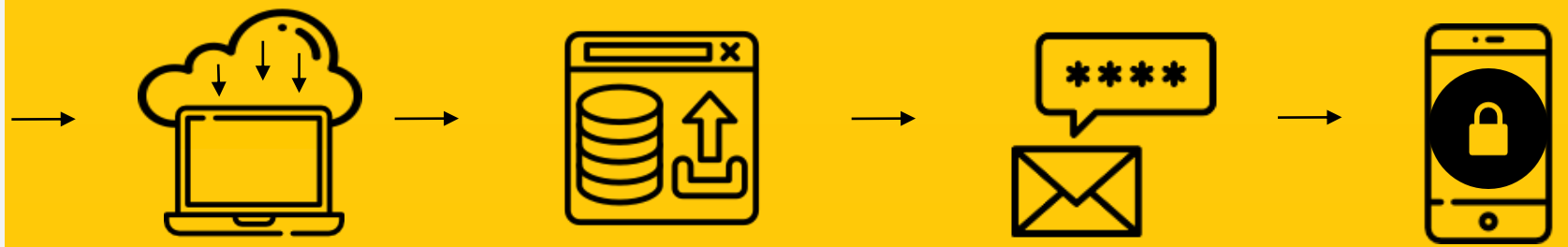
5 **Информационный антифрод купол** - Этикетка для международного и



3 **Межотраслевое взаимодействие** – On-line информирование банка о выявленной мошеннической атаки, направленное на обеспечение непрерывного процесса защиты абонента

Купол безопасности-схема работы

Сбербанк
ФинЦЕРТ
МТС
Т2
Мегафон
Газпром
Тинькоф
ф
и другие



Ежедневное получение на ГПЯ_fraud файлов с номерами мошенников от партнёров

Загрузка номеров в витрину с жалобами и их автоматический анализ посредством ML-модели

Ежедневная разработка новых и корректировка текущих Купольных правил на платформе Антифрод по результату анализа

СМС информирование клиента о начале фрод-атаки в момент срабатывания Купольного правила

Блокировка входящего на клиента трафика на N-минут

Предупреждение о нежелательных звонках «Этикетка»

VOLTE

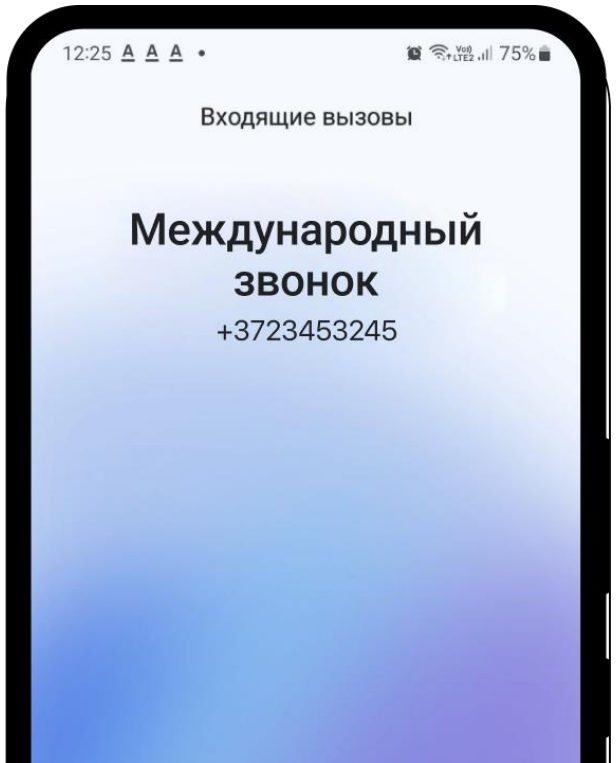
Вся сеть

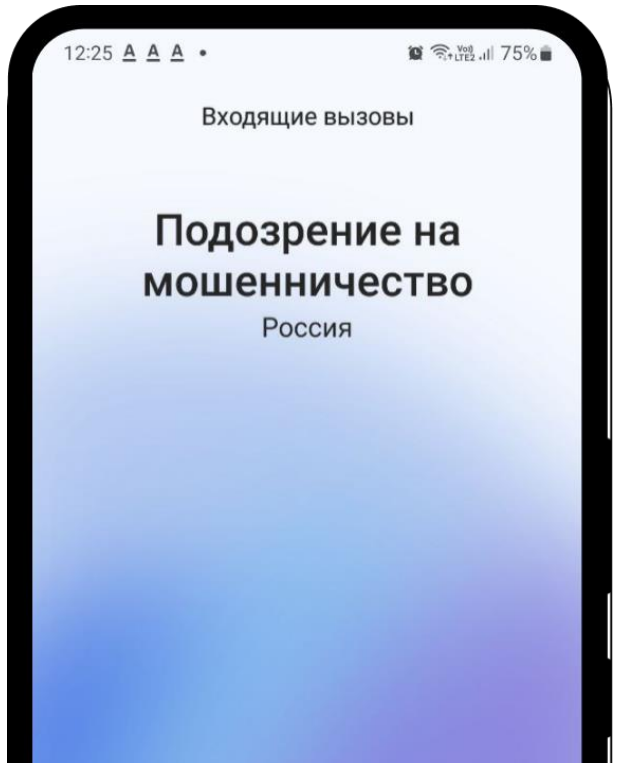
Везде, где есть VoLTE

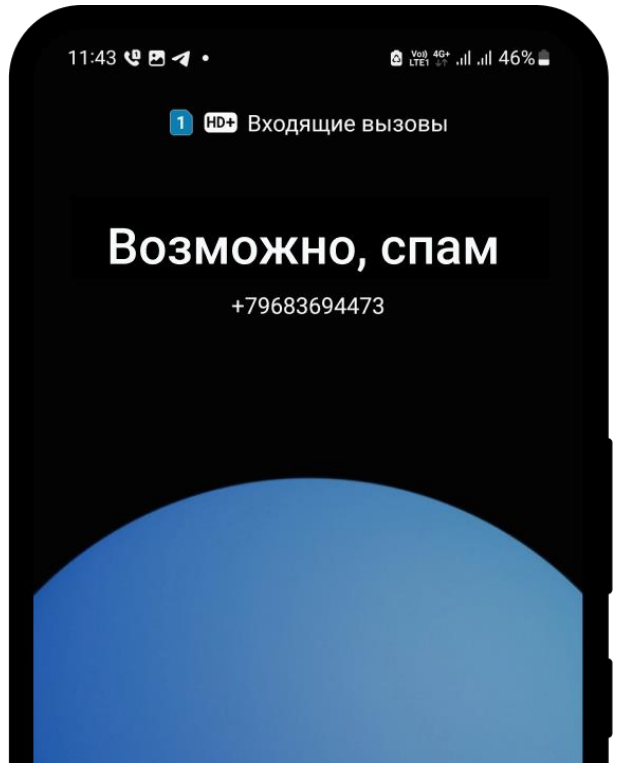
3G / 2G

88% сети

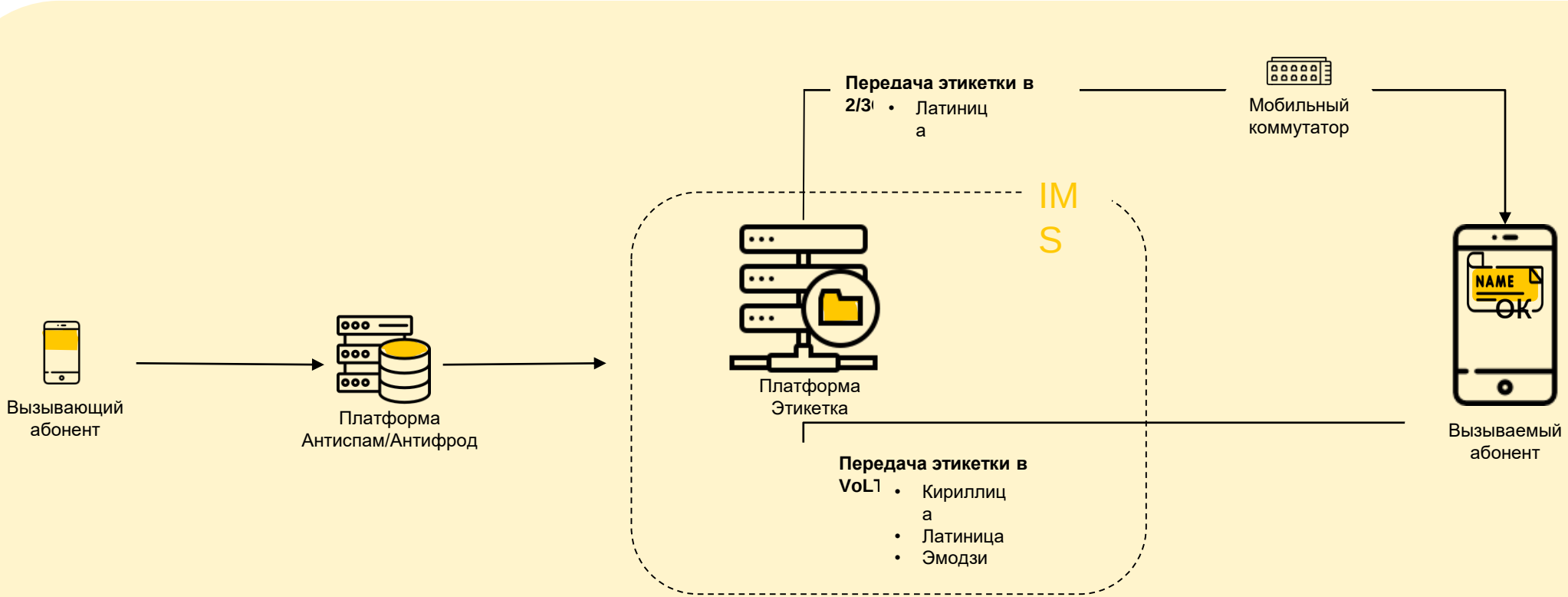
Везде, где есть поддержка оборудования







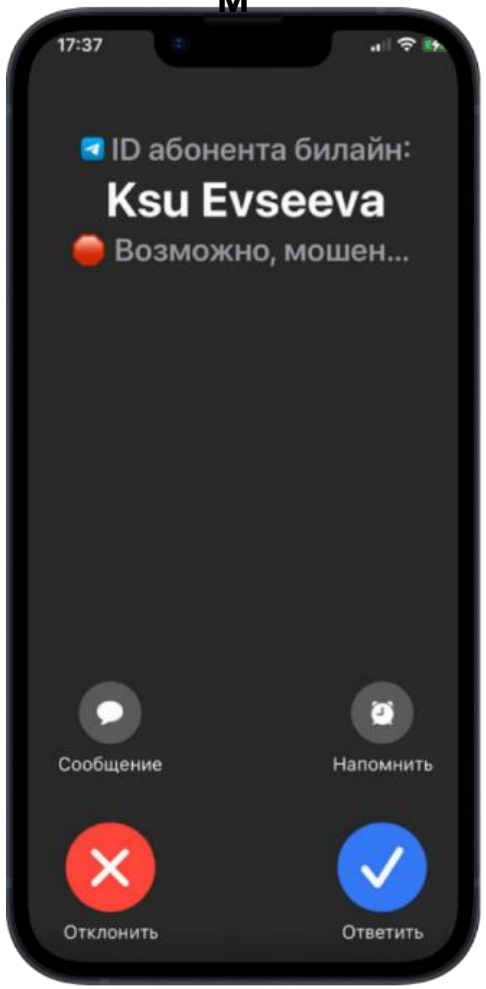
Этикетка-схема работы



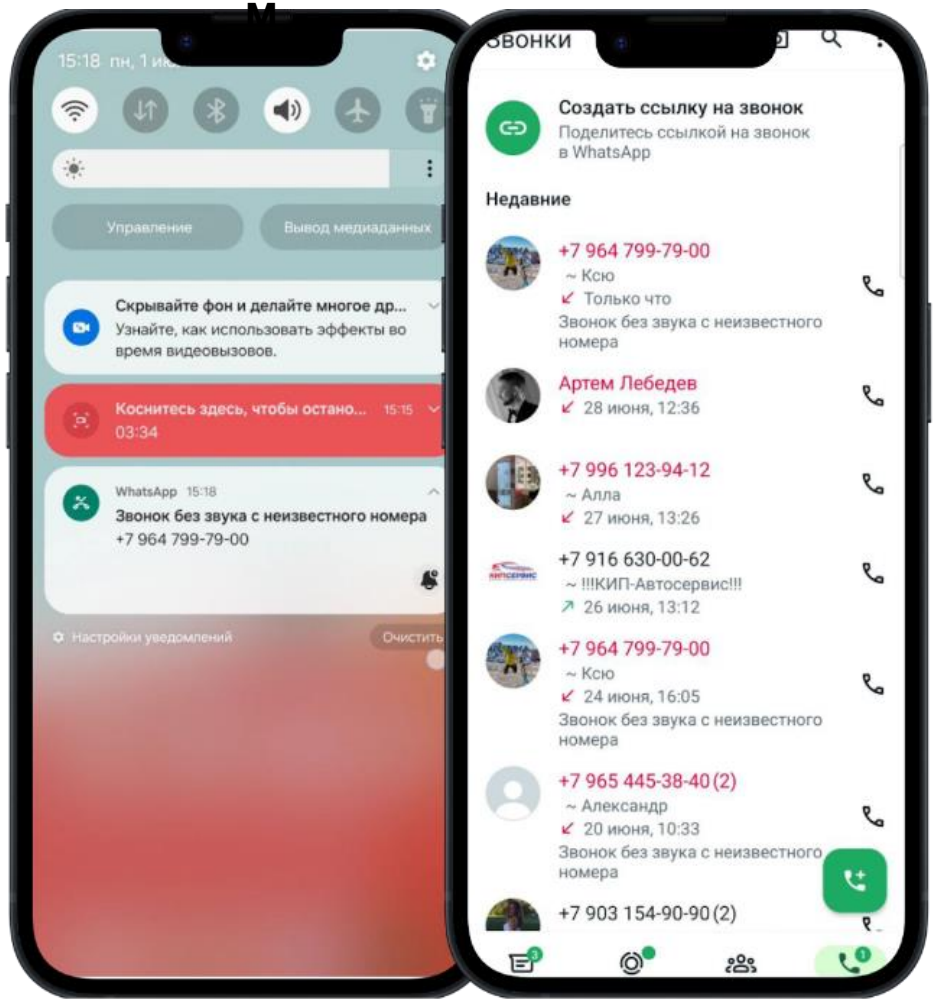
Платформа Антиспам и Антифрод на основе Модели данных вычисляет звонки потенциально не безопасные и не желательные для клиента и в случае обнаружения направляет звонок на платформу Этикетка, которая в свою очередь производит маркировку звонка этикеткой с предупреждением о спаме или мошенничестве. В случае нахождения абонента в сети 2/3G на устройство направляется этикетка в латинском написании, в сети VoLTE на кириллице (особенности технологии)

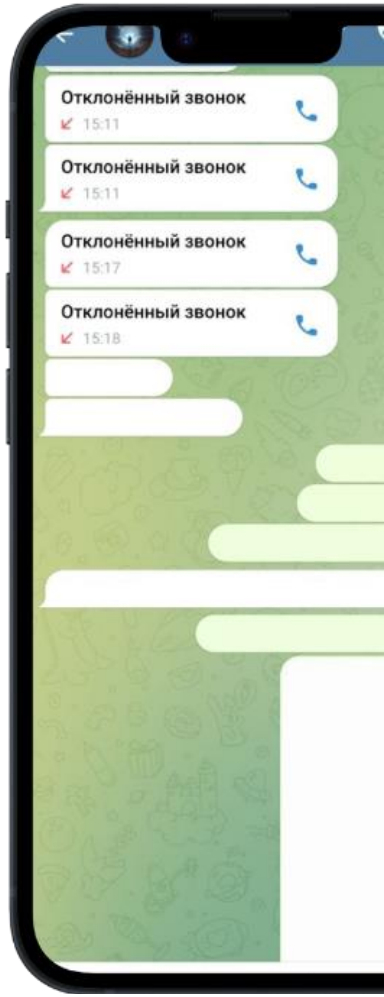
Блокировка мошенников в мессенджерах

IOS
Предупреждаем



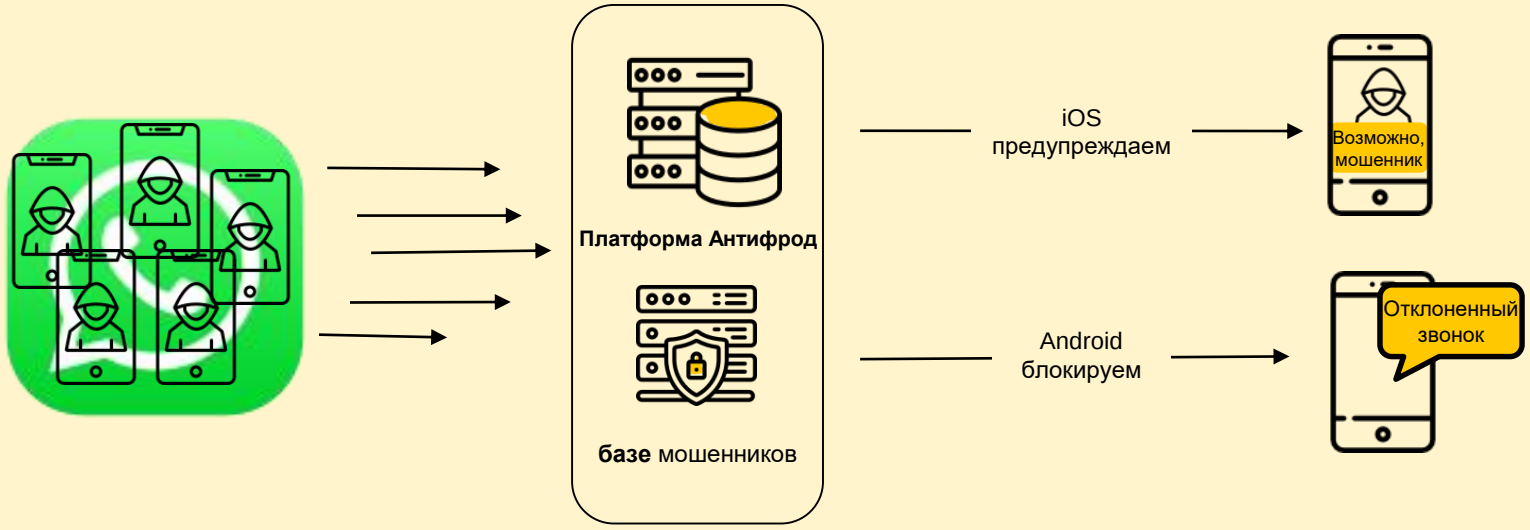
Android
Блокируем





Блокировка мошенников в мессенджерах- схема работы

Для работы продукта клиент открывает доступы в настройках телефона и предоставляет доступы к МП билайн.



При каждом входящем звонке в мессенджерах, билайн проверяет номер на наличие в базе мошенников на платформе Антифрод, при наличии номера в зависимости от операционной системы телефонного аппарата звонок мошенника блокируется и отправляется уведомление абоненту или звонок помечается как потенциально мошеннический.

Группа быстрого реагирования

Контактный центр билайн

- Выделенные сотрудники контактного центра (не роботы)
- Приоритетное обслуживание (fast track) по вопросам мошенничества
- Расширенные технические возможности сотрудников
- Исследование, изменяющихся сценариев фрода

Межотраслевое взаимодействие

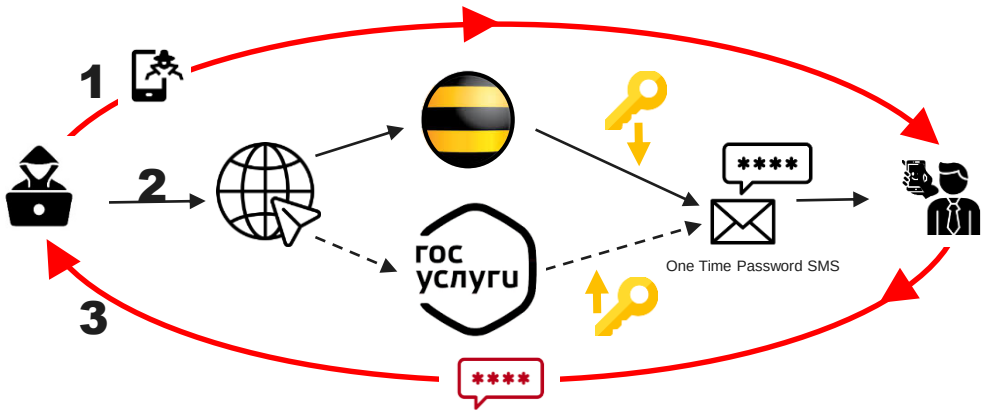
- Создание бесшовного клиентского пути по вопросам мошенничества

Запущенно:
- Тбанк
- Сбер
- Альфа банк
- VK

В работе:
- ГосУслуги

Защита цифровой личности- Умный ключ

Боль идентификация пользователей – двухфакторная идентификация не обеспечивает защиту от социальной инженерии, так как жертва мошенничества под воздействием передает все ключи идентификации мошенникам



Решение боли «Умный ключ»

Билайн APP реализовано

- Абонент находится в режиме звонка
- Сквозное шифрование sim и сети оператора - без кода Абонент

анализ

- Абонент онлайн или в режиме разговора в мессенджерах
- IP абонента не совпадает с IP запрашивающего пароль

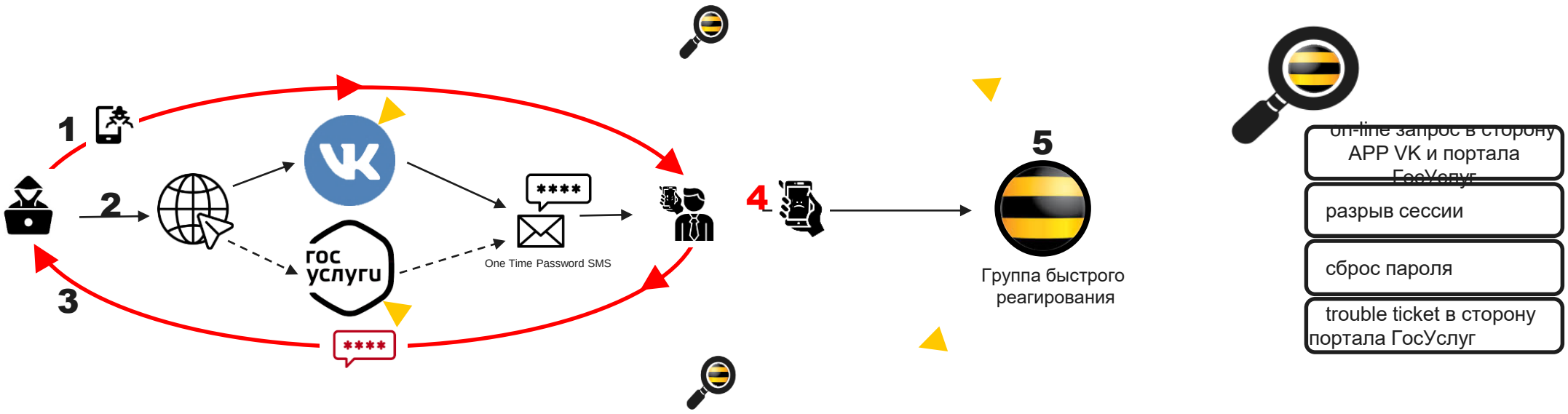
результат

- SMS : Перезвоните в контактный центр билайн
- Переадресация доверенному лицу (настраивается абонентом)

Проверка гипотезы – при входе в приложение Билайн ежедневно не доставляется порядка 1 000 одноразовых паролей, что существенно повлияло на защищенность приложения при полном отсутствии негативной обратной связи. Ретро тест по запросу одноразового пароля к порталу ГосУслуги. За два дня было выявлено 933 (2,2%) подтвержденные кейсы взлома. 38 059 (93%) мошеннических запросов кодов авторизации, но клиент не передал код мошеннику. 1 949 (4,8%) получили код аутентификации вовремя звонка и не имеют мошеннических признаков. Для уменьшения доли ложно положительных примеров надо скорректировать условие получения SMS в течении 1 мин после звонка.

Защита цифровой личности- Аутсорсинг

Использование внешнего ресурса для оперативной помощи жертвам мошенничества аккумулируя и распределяя звонки независимо от места начала атаки мошенников (приложение оператора, ГосУслуги, банки, мессенджеров и т.д.)



Аутсорсинг– создание возможности перевода звонка профильному специалисту другого контактного центра. On-line обмен информаций о жертвах мошенничества между операторами, ГосУслугами, банками и т.д. Пример интеграции – в настоящий момент билайн реализовал интеграцию с ТБанк, в рамках которой обеспечивается бесшовный перевод звонка между профильными специалистами, что позволяет минимизировать общее время необходимое для устранения последствий мошенничества, возврата доступов к приложениям и т.д. В проработке аналогичная интеграция с Сбер Банком и Альфа Банком. Так же со Сбер Банком реализован On-line обмен информаций о жертвах мошенничества, в рамках которого билайн моментально передает в Сбер информацию о начавшейся мошеннической атаки, и защита клиента происходит одновременно со стороны банка и оператора.

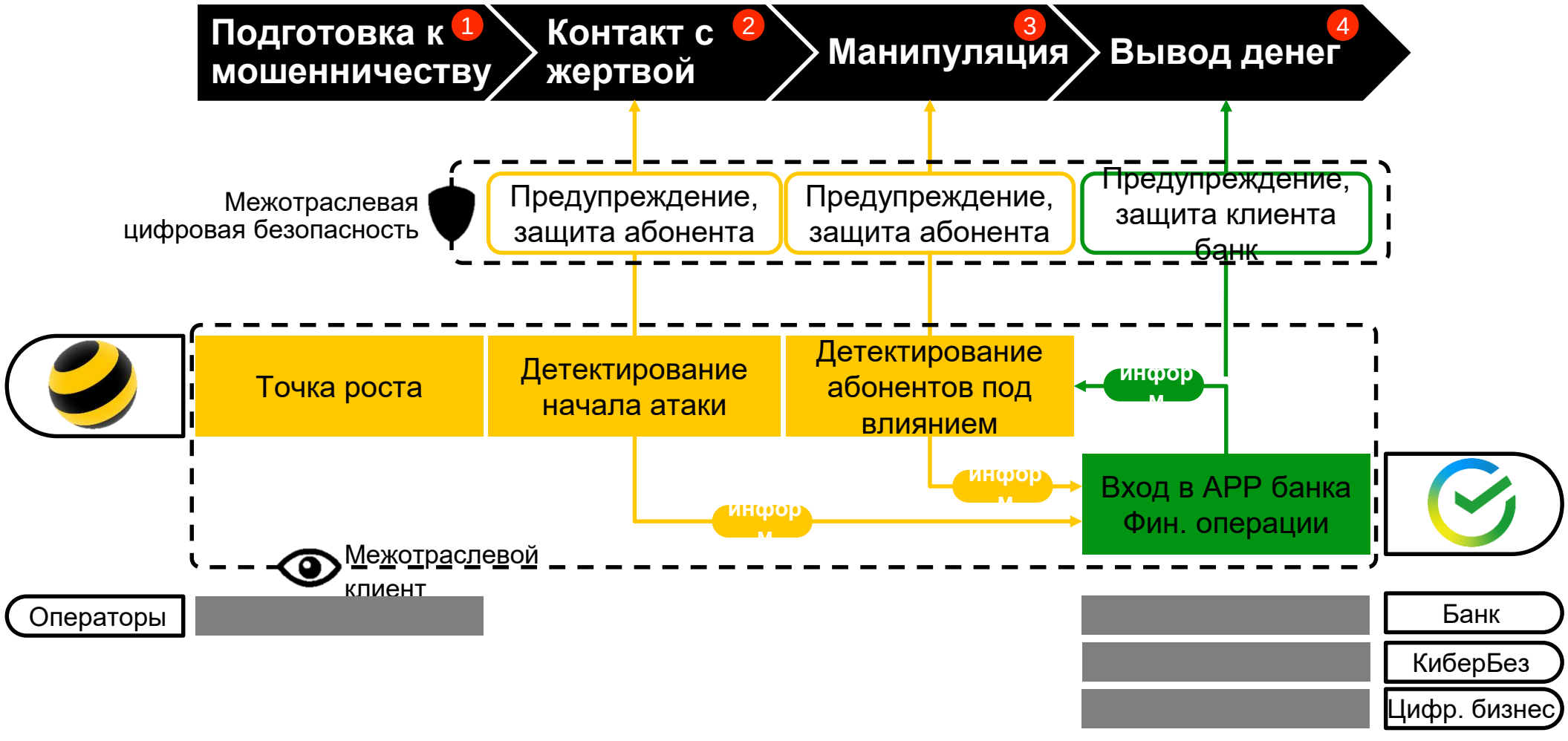
Защита цифровой личности-Единая база мошенников

Организация обмена информацией о выявленной жертве мошенничества в режиме реального времени между всеми участниками цифровой экономики

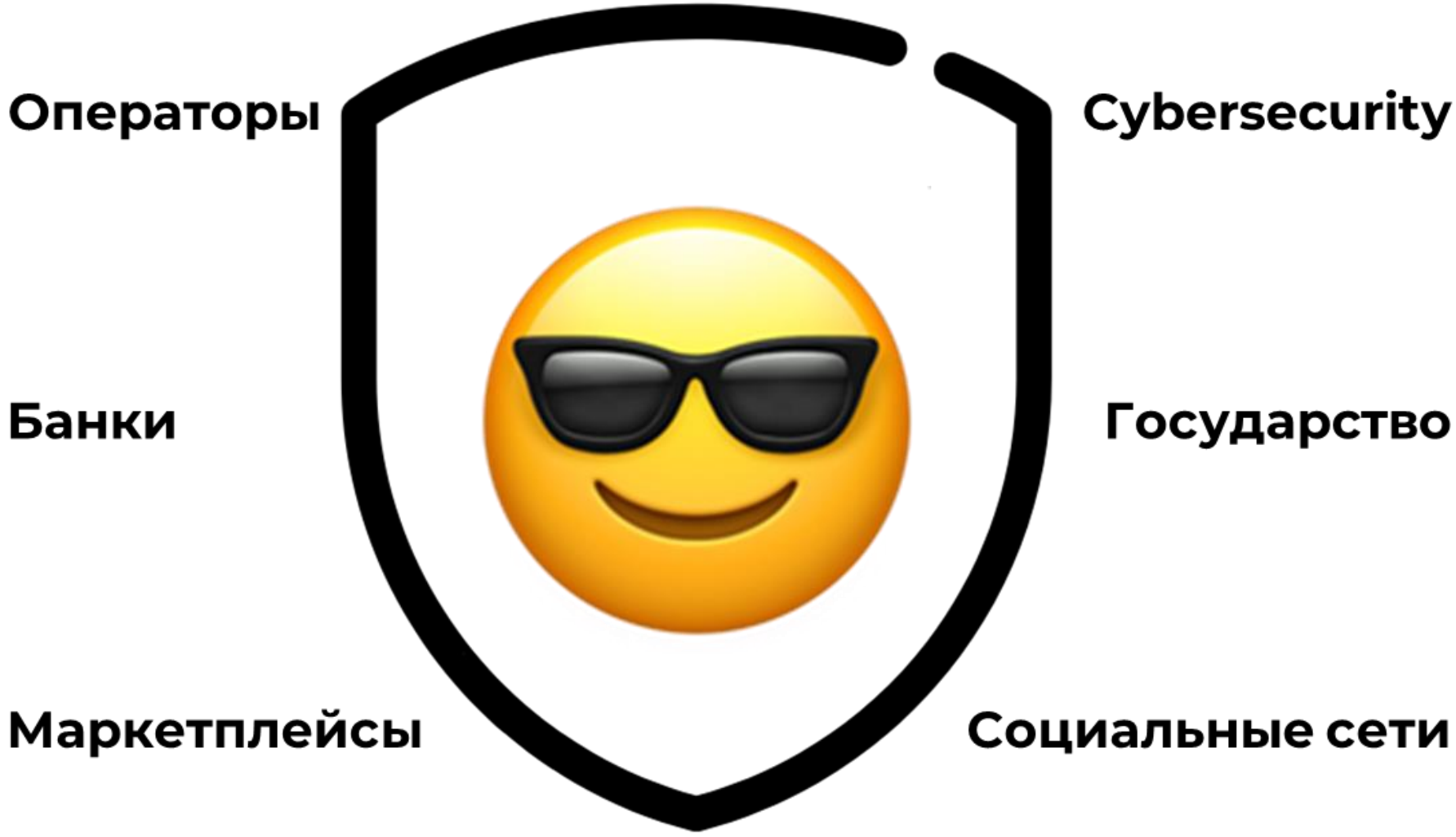
Участники	Хранение	Обработка	Взаимодействие
Операторы Банки Маркетплейсы Соцсети Мессенджеры Госорганы Кибербез	Номер мошенника А Номер мошенника В Номер в мессенджерах Nıkneım в мессенджерах	Очистка от спам по запросам оператора Формирование единого списка Автоматический прозвон мошеннических номеров	OnLine обмен базы: запись чтение Формирование OffLine базы для антифрод систем

Мошенническая атака развивается последовательно в разных приложениях цифровой экономики, начинаясь с контакта с жертвой, манипулирования, похищения цифровой личности и ввода денежных средств. На каждом этапе разные антифрод команды проводят полный цикл выявления и о защиты жертв мошенничества. **Единая база мошенников** поможет прервать мошенническую атаку, обеспечит период охлаждение жертвы мошенничества и предотвратит повторные попытки атаковать жертву.

Межотраслевая карта цифровой безопасности клиента



Единый клиент



Тепловая карта развития межотраслевого взаимодействия

Антифрод процесс	Банки									Государство			Операторы связи			КиберБез	Цифровой бизнес	
	Сбер	ТБанк	Альфа	ВТБ	ГазПром	ЦБ	МКБ	АБР	ПСБ	Минцифра	МВД	ГосУслуги	Мегафон	Т2	МТС	Касперский	VK	Авито
Исследование болей клиентов и технологий взлома	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●	●	●
Источники данных																		
01 Обмен данными по жертвам - еженедельно	●	●	●	●	●	●	●	○	●	●	●	●	●	●	○	●	★	○
02 Обмен данными по жалобам - ежедневно	●	●	●	●	●	○	●	○	●	●	○	●	○	○	○	○	●	○
03 Обмен данными по дропперам - еженедельно	●	●	●	○	○	●	○	○	●	○	○	○	○	○	○	○	○	○
04 On-line alarming по межотраслевым клиентам находящимся под влиянием (купол, ML модель, данные от банка)	●	●	○	○	●	●	○	○	○	●	○	●	●	●	○	●	●	○
Еженедельная метрика «Количество жертв»	●	●	●	●	●	●	●	○	●	●	●	●	○	○	○	○	●	○
Решение боли клиента																		
01 Формирование antifraud backlog	●	●	●	●	●	○	○	○	●	○	○	★	○	○	○	○	★	○
02 Единая среда расследования инцидентов	●	●	●	●	●	○	●	○	●	●	●	●	●	●	●	●	★	○
03 Единая база мошенников	●	●	○	○	○	○	○	○	○	○	○	●	○	○	○	●	○	○
04 Цель 1 – Снижение количества телефонных звонков мошенников до целевого уровня	●	●	●	●	○	○	●	○	○	○	○	○	○	○	○	○	○	○
05 Цель 2 – Снижение количества звонков мошенников в мессенджерах до целевого уровня	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
06 Прототипирование технологии транскрибации	●	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Группа быстрого реагирования																		
01 Интеграция кол-центров	●	●	●	○	○	○	○	○	○	○	○	★	○	○	○	○	★	○

● сделано ● в работе ○ в плане