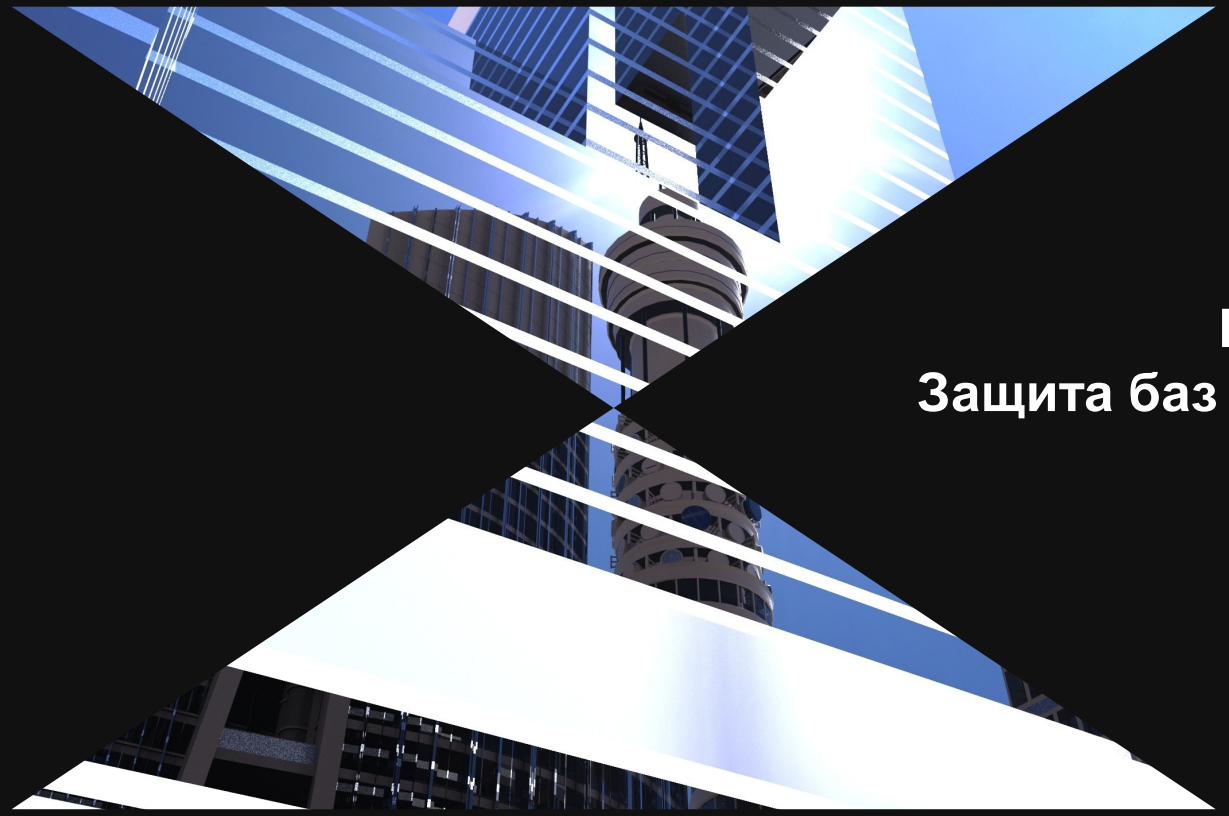


Их данные? ваша проблема!
Защита баз и аутентификация клиентов в ритейле

Евгений Питолин
Управляющий директор
Kaspersky Lab

KASPERSKY lab

Что происходит в данный момент?

Новые фишинг-атаки выявляются каждые 30 секунд. Мировые потери достигают $10.8 млрд.*

Нелегальные транзакции, осуществляемые через мобильные приложения, выросли на 600% с 2015 года.*

Создание мошеннических учетных записей в 15 раз чаще случается на новых аккаунтах, чем на тех, что существуют более месяца.*

Больше половины крупных кибер атак в мире приносят потери на сумму более $100,000.

Объем транзакций, связанных с отмыванием денег, оценивается в 2-5% глобального ВВП, что примерно соответствует $1-2 трлн в год.**

*RSA Q1 2018 Fraud Report
**PwC Global Economic Crime Fraud Survey 2018

KASPERSKY lab

Статистика

- 49% мировых организаций стали жертвами мошенничества за последние 2 года
- 52% всех зарегистрированных случаев мошенничества за последние 24 месяца были случаями внутреннего мошенничества
- Наблюдается огромный рост компрометации в программах лояльности
- Значительный рост меж-банковских группировок по отмыванию денег

* Raconteur Fraud Report 2018 published in The Times

Что происходит в данный момент?

Около 500 миллионов попыток перехода пользователей на фишинговые страницы заблокировали решения «Лаборатории Касперского» в 2018 году.
С мошенничеством на поддельных веб-сайтах столкнулся **почти каждый седьмой пользователь** в Казахстане.

Казахстан оказался **на втором месте в мире по доле пользователей**, атакованных мобильными троянцами-вымогателями. Эти вредоносные программы блокируют экран смартфона и стараются запугать пользователя любым способом

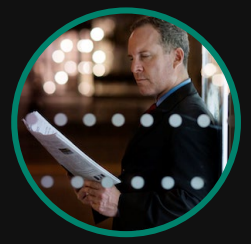
В Республике Казахстан **атаке зловредов этого типа подверглись 0,53% пользователей**. Эксперты объясняют это тем, что злоумышленники стали применять новые техники заражения, а также усилили уже проверенные схемы распространения вредоносного ПО, например через SMS-спам.

KASPERSKY lab

KASPERSKY lab

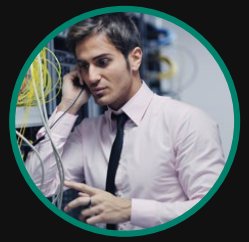
Компании, обладающие онлайн-каналами с использованием виртуальных аккаунтов

Топ-менеджеры – менеджер по борьбе с мошенничеством, цифровой менеджер, CISO



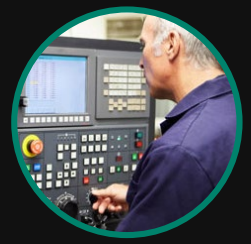
Fraud manager - требует гибкости и сокращения рабочей нагрузки

- Хочет высокие показатели обнаружения мошенничества
- Стремится сократить нагрузку на команду аналитиков, сохраняя при этом уровень обнаружения мошенничества



Brand Manager - хочет, чтобы клиенту было комфортно пользоваться сервисом.

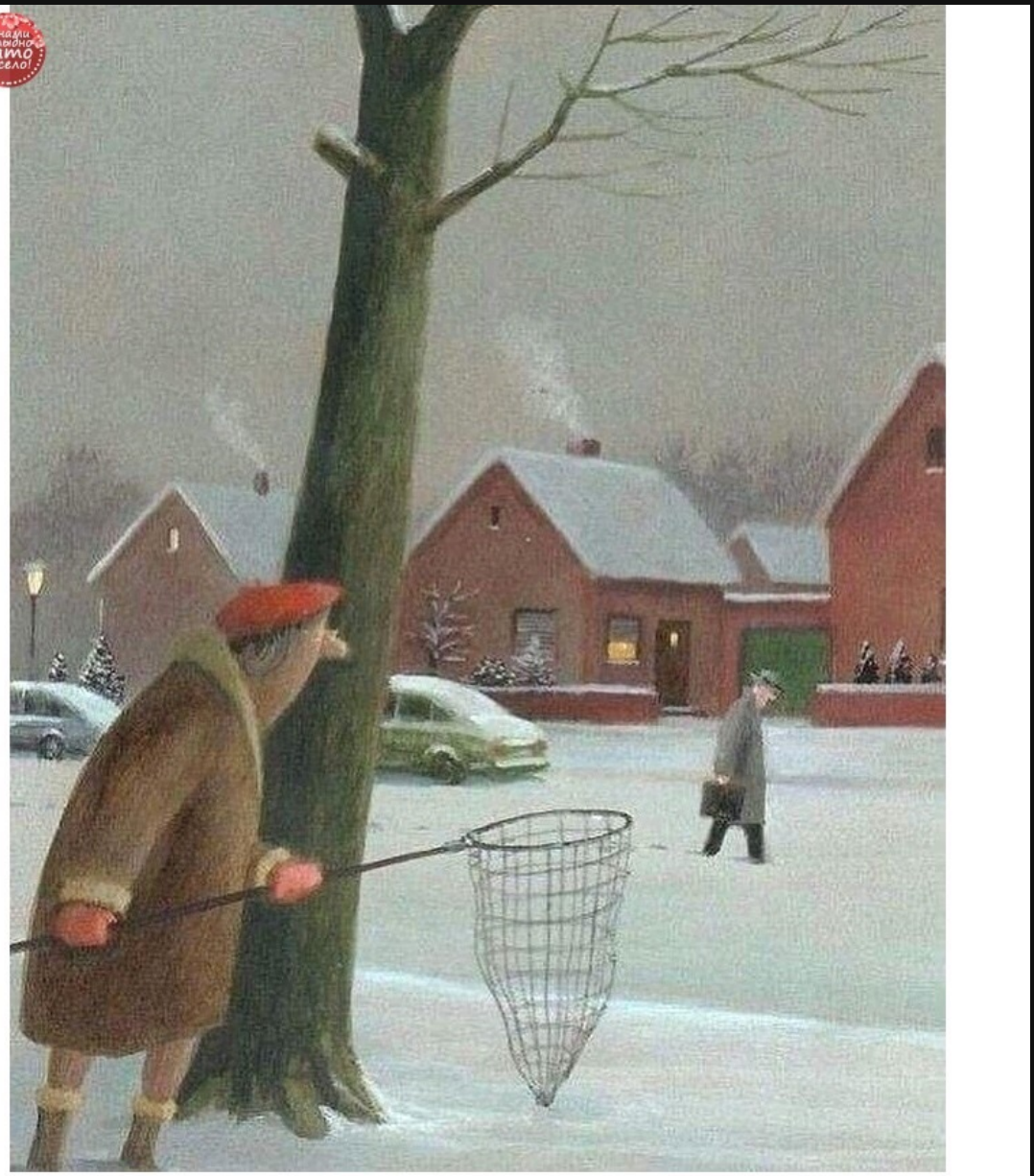
- Основное внимание уделяет увеличению доходов
- Ключом к этому является непрерывный доступ к сервису для пользователя
- Ориентация на удобство сервиса для клиентов, а не меры безопасности / мошенничества



CISO – Ищут лучшее решение, однако часто их мнение не учитывается

- Основное внимание уделяется кибер-защите организации
- Обозначает политику безопасности и обеспечивает ее принятие
- Фокусируется на безопасности, а не на мошенничестве
- Часто в противоречиях с приоритетами Digital Manager

KASPERSKY lab



KASPERSKY lab

Как кибер-мошенник видит бизнес?

Предлагаемые услуги	Возможности для преступников
Доставка на следующий день	Отлично, подставной курьер доставит мне товар, быстрей, чем вы узнаете
Более быстрые платежи в реальном времени	Получу деньги, быстрей чем ваш клиент узнает об этом!
$10 за привлечение новых аккаунтов	1 продвинуть хорошо - 6 000 лучше!
Ссылка “восстановить пароль”	Я знаю 1001 способ проверки учетных записей ...
Всего 5 попыток для логина	Желаю удачи, пока я блокирую ваши аккаунты
Просмотр вашего заявления онлайн	Спасибо за предоставленные личные данные, всего хорошего!

KASPERSKY lab

KASPERSKY lab

Здесь могут быть **оскорблены**
Ваши чувства ©

KASPERSKY lab

KASPERSKY lab

KASPERSKY lab

- Пароль в SMS можно подсмотреть, если у вас включен показ уведомлений на экране блокировки.

- Даже если показ уведомлений отключен, можно извлечь SIM-карту из смартфона, установить в другой смартфон и принять SMS с паролем.

- SMS с паролем может перехватить пробравшийся в смартфон троян.

- Также с помощью различных махинаций (убеждение, подкуп, сговор и так далее) можно заполучить новую SIM-карту с номером жертвы в салоне сотовой связи. Тогда SMS будут приходить на эту карту, а телефон жертвы просто не будет связываться с сетью.

- Наконец, SMS с паролем может быть перехвачена через фундаментальную уязвимость в протоколе SS7, по которому эти SMS передаются.

Увы, разработчики банковских троянцев довольно быстро освоили методы обхода одноразовых паролей, присылаемых в SMS.

Вот как это работает в современных мобильных банковских троянцах:

1. Пользователь запускает подлинное банковское приложение на своем смартфоне.
2. Троянец определяет, приложение какого банка используется, и перекрывает его интерфейс своим, показывая пользователю поддельный экран. Внешне поддельное приложение максимально похоже на настоящее.
3. На поддельном экране пользователь вводит свои логин и пароль.
4. Троянец отправляет эти логин и пароль злоумышленникам — теперь последние могут использовать их для входа в банковское приложение.
5. Злоумышленники инициализируют перевод некоторой суммы денег на свой счет.
6. На смартфон пользователя приходит SMS с одноразовым паролем.
7. Троянец перехватывает пароль из SMS и отправляет его злоумышленникам.
8. При этом на смартфоне SMS скрывается — пользователь не видит сообщение и ни о чем не подозревает, пока не проверит список транзакций.
9. Используя перехваченный одноразовый пароль, преступники подтверждают свою транзакцию и получают деньги на счет.

KASPERSKY lab

KASPERSKY lab

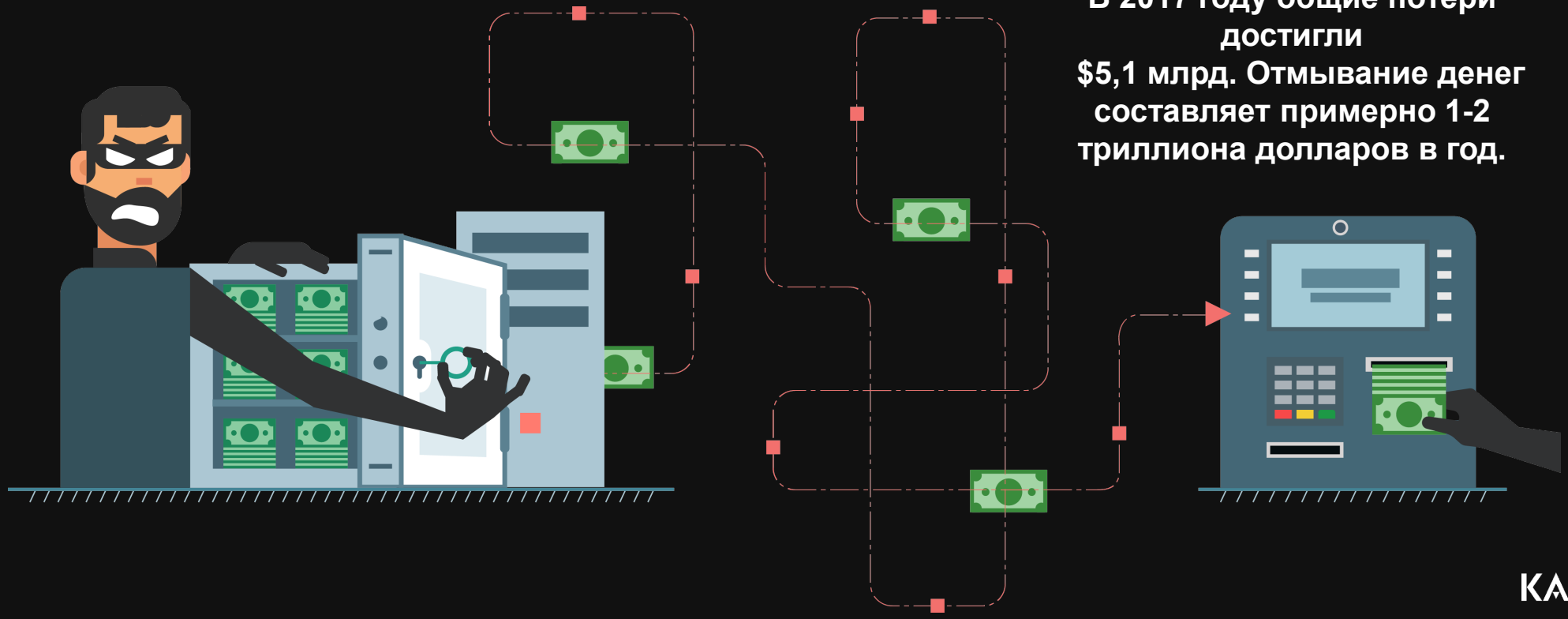
ПРОБЛЕМЫ

- Прямые потери
- Косвенные потери
- Ожидание клиентов
- Вопросы аутентификации
- Операционные издержки
- Вопросы комплайенса

KASPERSKY lab

ПРОБЛЕМЫ

- Прямые потери
- Косвенные потери
- Ожидание клиентов
- Вопросы аутентификации
- Операционные издержки
- Вопросы комплайенса



В 2017 году общие потери достигли $5,1 млрд. Отмывание денег составляет примерно 1-2 триллиона долларов в год.

ПРОБЛЕМЫ

Direct financial losses

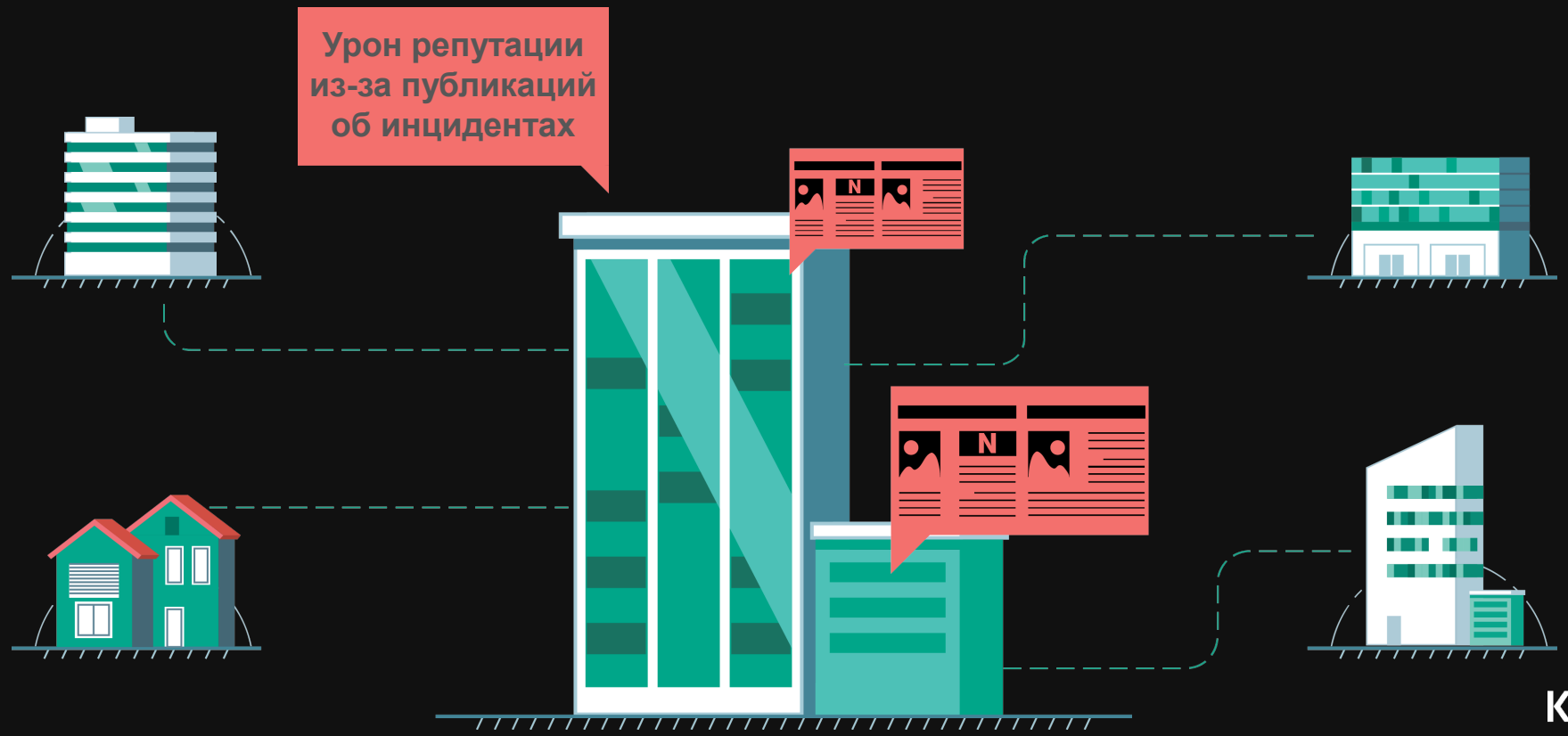
Косвенные потери

Consumer expectations

Authentication problems

Operating costs

Compliance issues



ПРОБЛЕМЫ

Direct financial losses

Indirect costs

Ожидания клиентов

Authentication problems

Operating costs

Compliance issues

KASPERSKY lab

ПРОБЛЕМЫ

Direct financial losses

Indirect costs

Consumer expectations

Вопросы аутентификации

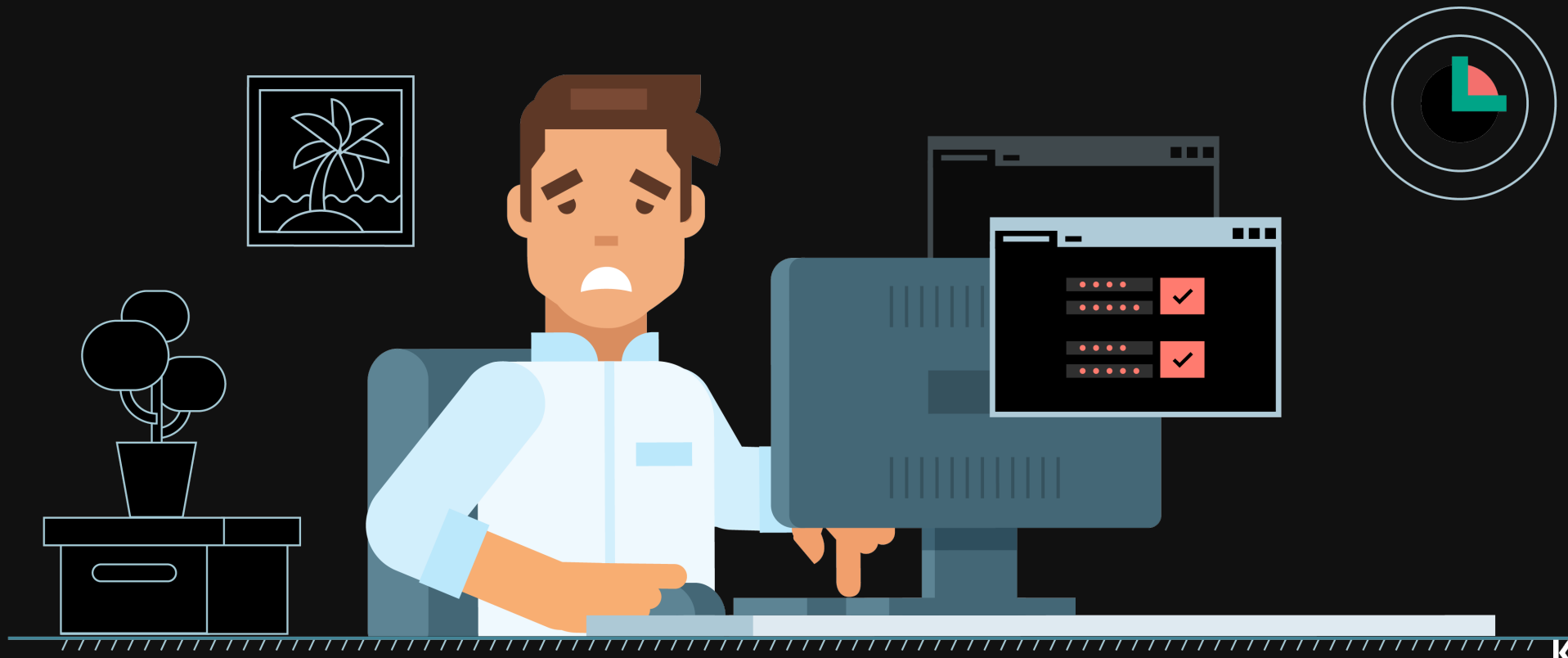
Operating costs

Compliance issues

KASPERSKY lab

ПРОБЛЕМЫ

- Direct financial losses
- Indirect costs
- Consumer expectations
- Authentication problems
- Операционные издержки
- Compliance issues



ПРОБЛЕМЫ

Direct financial losses

Indirect costs

Consumer expectations

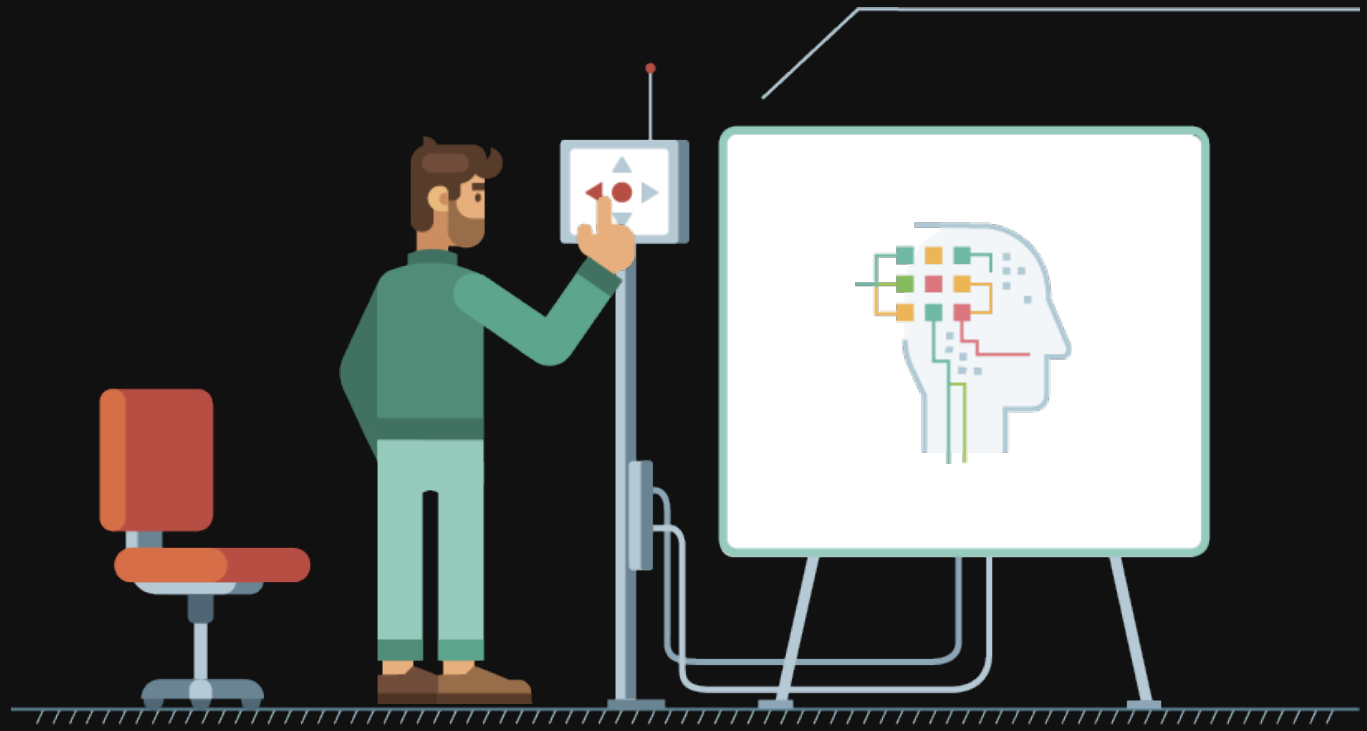
Authentication problems

Operating costs

Вопросы комплайенса

KASPERSKY lab

Kaspersky Fraud Prevention



KASPERSKY lab

Advanced
Authentication

Automated
Fraud Analytics

Machine
learning

ЧТО ТАКОЕ ADVANCED AUTHENTICATION И КАК ЭТО РАБОТАЕТ?

Аутентификация
на основе рисков

Непрерывная
аутентификация

Advanced Authentication

Automated Fraud Analytics

Machine learning

Advanced Authentication

Повышение удобства использования

Сокращение издержек на дополнительную аутентификацию

Аутентификация на основе рисков

Непрерывная адаптивная аутентификация

Обнаружение кражи учетной записи в режиме реального времени

Stronger authentication in case of anomaly detection

Бэк-офис клиента

Аккаунт пользователя

Advanced Authentication

Automated Fraud Analytics

Machine learning

ПРЕИМУЩЕСТВА

Защита от мошеннической активности

Уменьшение расходов на второй фактор аутентификации

Удобство для пользователя

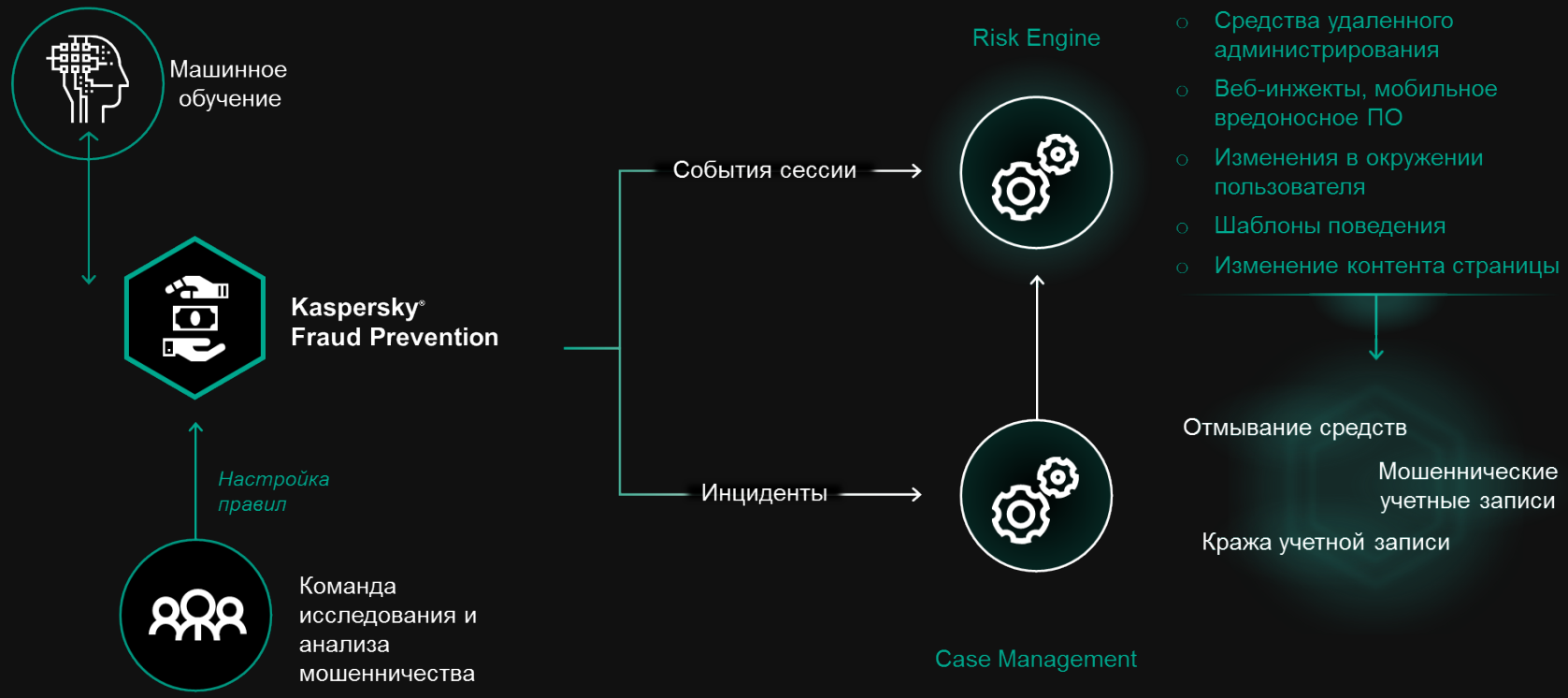
Advanced Authentication

Automated Fraud Analytics

Machine learning

ЧТО ТАКОЕ AUTOMATED FRAUD ANALYTICS И КАК ЭТО РАБОТАЕТ?


Advanced Authentication
Automated Fraud Analytics
Machine learning

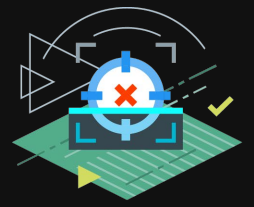

Машинное обучение
Kaspersky® Fraud Prevention
Настройка правил
Команда исследования и анализа мошенничества
События сессии
Инциденты
Risk Engine
Case Management
Боты
Средства удаленного администрирования
Веб-инжекты, мобильное вредоносное ПО
Изменения в окружении пользователя
Шаблоны поведения
Изменение контента страницы
Отмывание средств
Мошеннические учетные записи
Кража учетной записи

Advanced Authentication

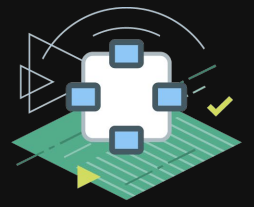
Automated Fraud Analytics

Machine learning

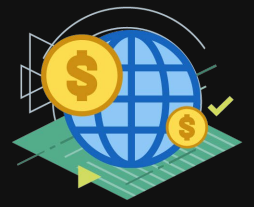
ПРЕИМУЩЕСТВА



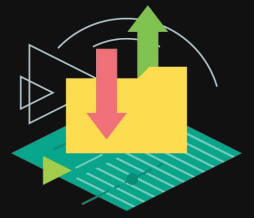
Выявление аномалий и подозрительного поведения



Мониторинг событий и инцидентов в сессии



Обнаружение схем по отмыванию денег



Снижение операционных издержек

CASE STUDY: INTERBANK CASH TRANSIT

Жертвы

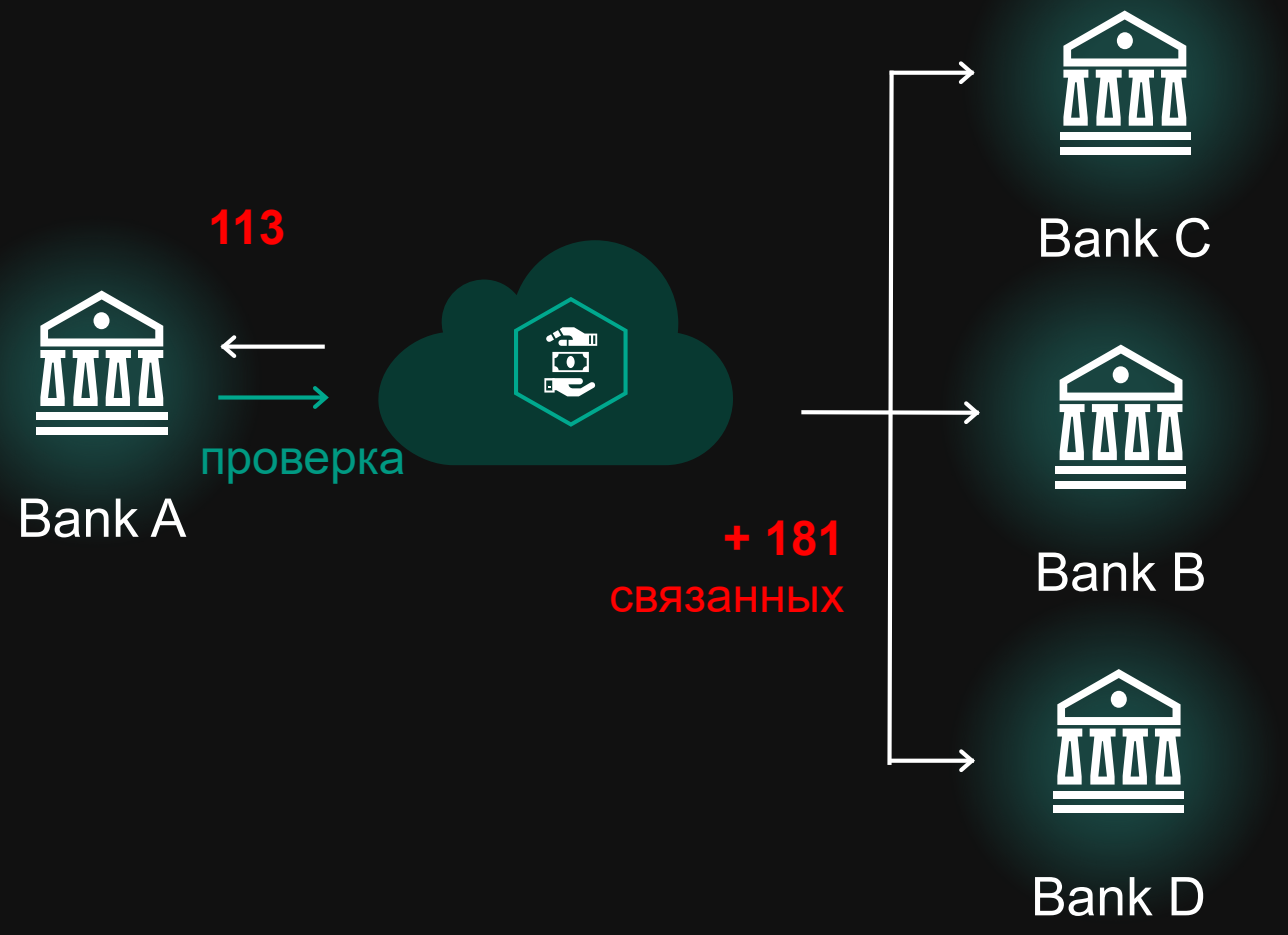
4 банка в 1 стране

294 эккаунта дропперов

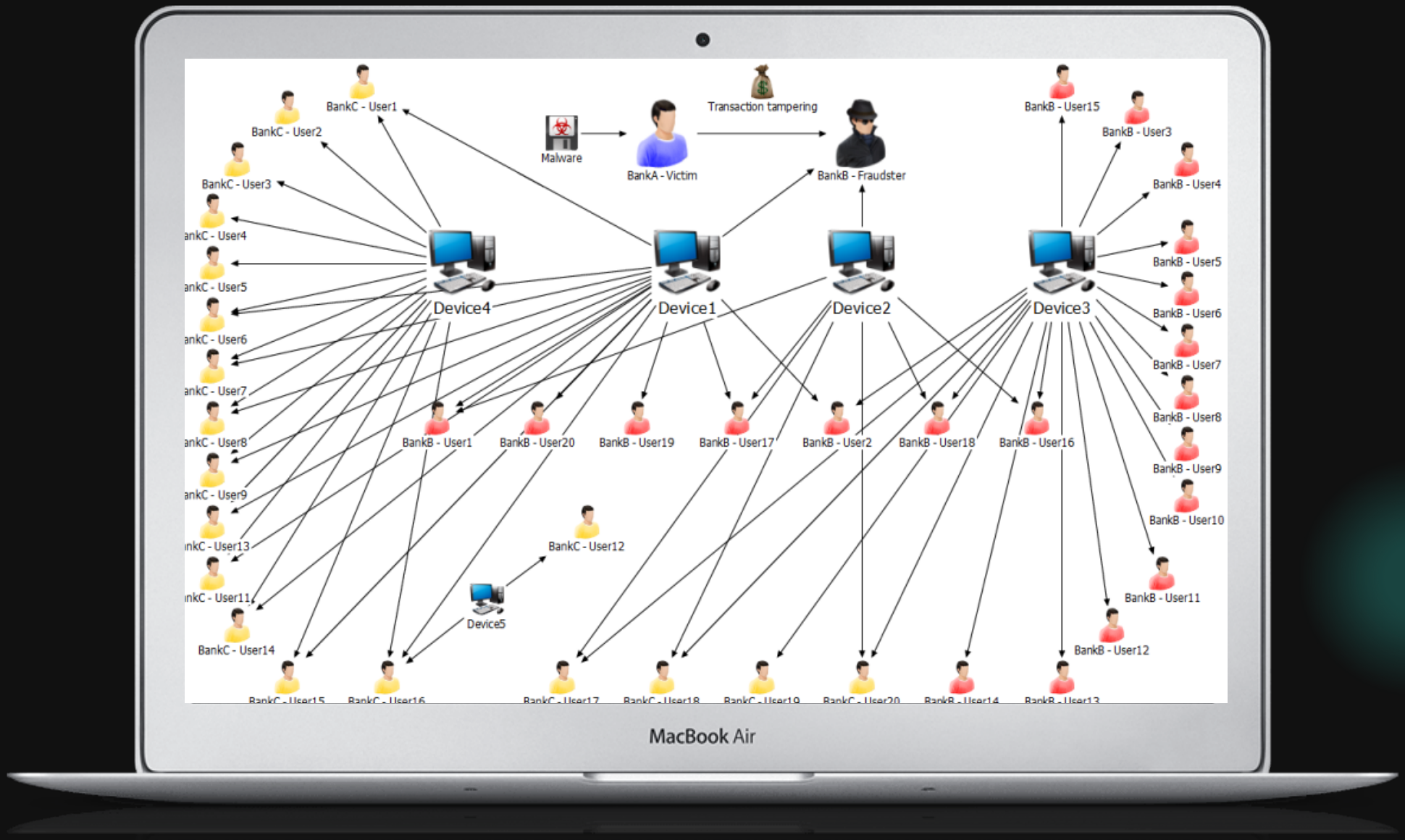
- 113 - в банке A
- 181 - в банках B, C, D

Методы детекта

- Глобальная репутация устройств
- Связи банковских эккаунтов
- Анализ цифрового слепка устройств



INTERBANK CASH TRANSIT



ЦИФРОВОЙ СЛЕПОК

НАБОР ЦИФРОВЫХ ПАРАМЕТРОВ

Mobile app

- Operator:

  SIM information (if available), operator details, etc.

- Hardware:

  CPU, display, memory, input devices and sensors

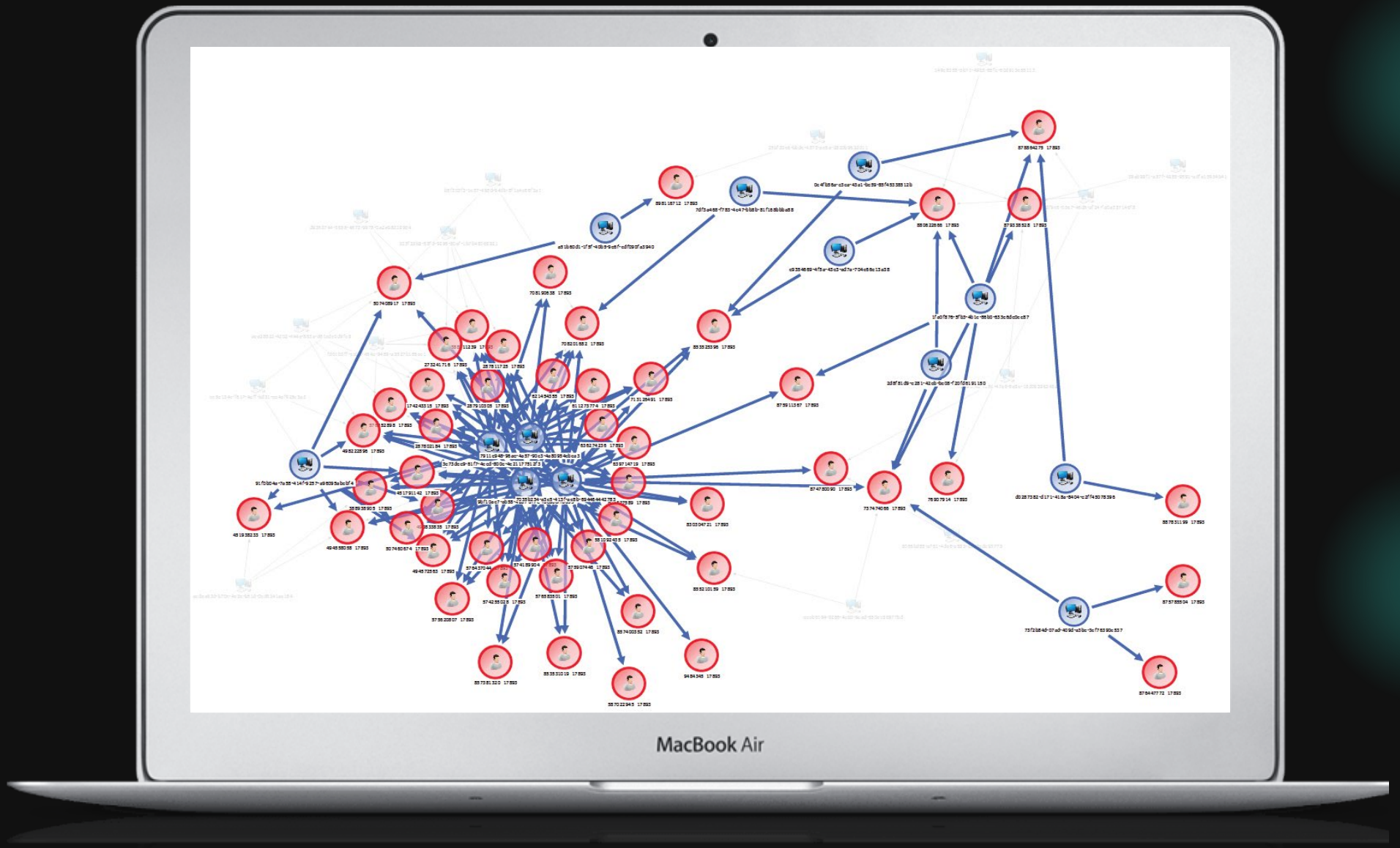
- System:

  Version, environment, specific parameters

Web

- OS, browser UserAgent, language, display, time zone, fonts and more.

CASE 2: 50 эккаунтов

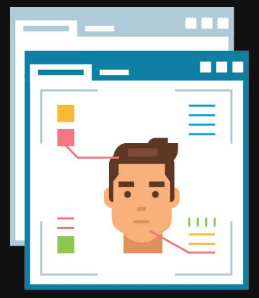


Advanced Authentication

Automated Fraud Analytics

Машинное обучение

ТЕХНОЛОГИИ МАШИННОГО ОБУЧЕНИЯ

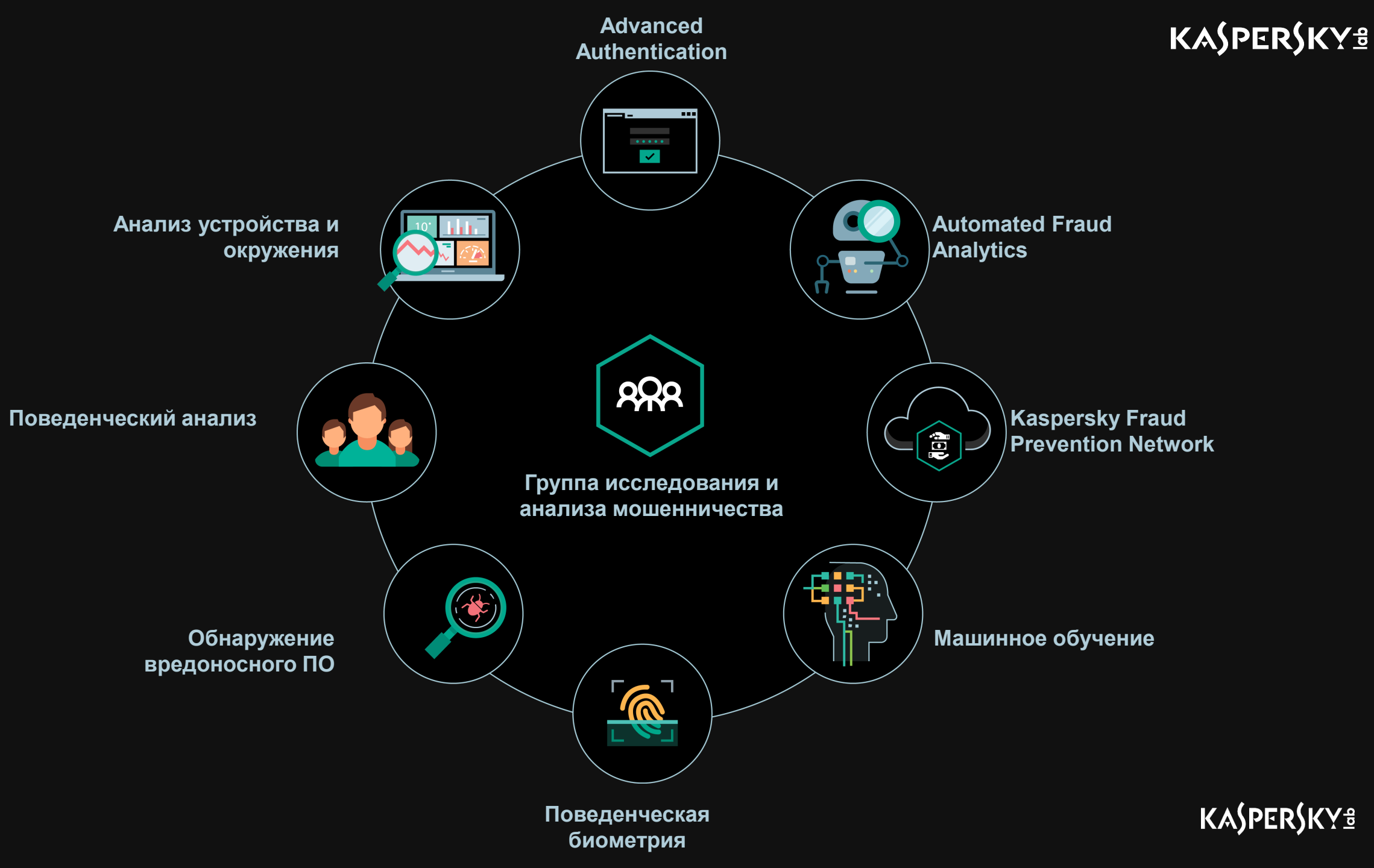


Поведенческая биометрия

Поведенческий анализ

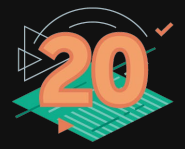
Анализ устройства и окружения

Обнаружение вредоносного ПО

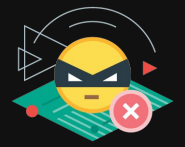

Advanced Authentication
Анализ устройства и окружения
Automated Fraud Analytics
Поведенческий анализ
Kaspersky Fraud Prevention Network
Группа исследования и анализа мошенничества
Обнаружение вредоносного ПО
Машинное обучение
Поведенческая биометрия
KASPERSKY lab
KASPERSKY lab

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА ПОДХОДА

Возможности машинного обучения обеспечивают более низкие эксплуатационные расходы и передовое расследование мошенничества



Основывается на обширном экспертном опыте «Лаборатории Касперского» в сфере кибербезопасности



Защищает от мошенничества без какого-либо программного обеспечения на устройстве конечного пользователя

Наш метод непрерывной аутентификации «всегда включен», а не просто ориентирован на логин и транзакционные точки

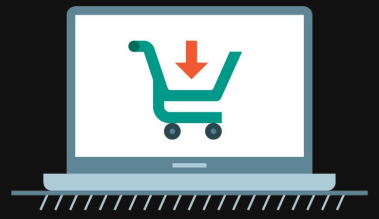
Один продукт, который обеспечивает более широкий спектр анализа и технологий

KASPERSKY lab

ШИРОКИЙ СПЕКТР ОТРАСЛЕЙ

Финансовые учреждения

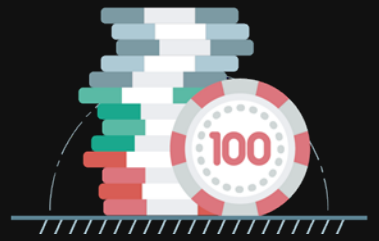
Программы лояльности



Онлайн-магазины

Здравоохранение

Телеком



Онлайн-казино и букмекерские компании

Онлайн-игры

E-commerce

KASPERSKY lab

Применимость для бизнеса

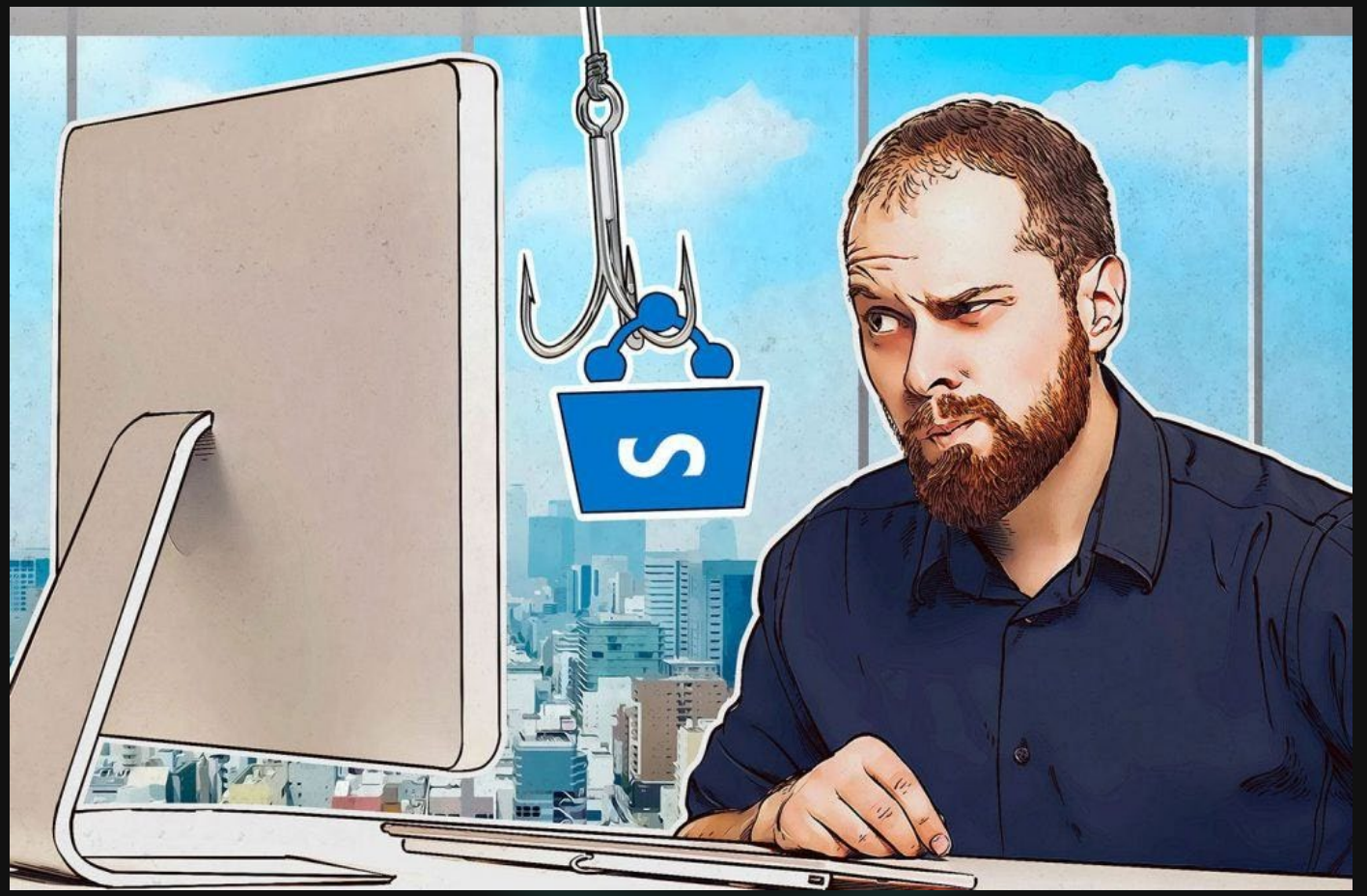
Определение «хорошего» пользователя – высокий уровень удобства использования для легитимных клиентов

Обнаружение мошеннических аккаунтов – обнаружение групп мошеннических аккаунтов, использующихся для злоупотребления программой лояльности

Обнаружение кражи учетной записи – обнаружение ранних признаков кражи в реальном времени

Предотвращение отмывания средств – кросс-канальное обнаружение схем отмывания средств и связанных действий

Исследование мошенничества – дополнительный уровень данных, обогащающий внутренние системы мониторинга



Статистика

Облако KFP, работая в режиме реального времени, обрабатывает трафик сервисов дистанционного обслуживания в разрезе:

Название метрики	Уникальные единицы в сутки
Устройство	~ 503k
Пользователь	~ 487к
Онлайн-сессия	~ 873к
Обработанное событие	~ 34.1м

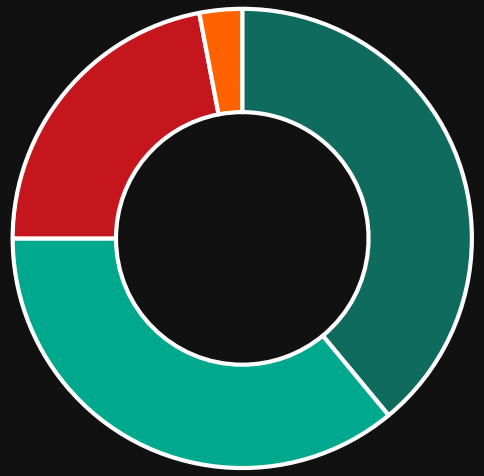
Основные угрозы, детектируемые облаком KFP:

Скомпрометированная учетная запись(Account Takeover) – использование учетной записи пользователя третьими лицами;

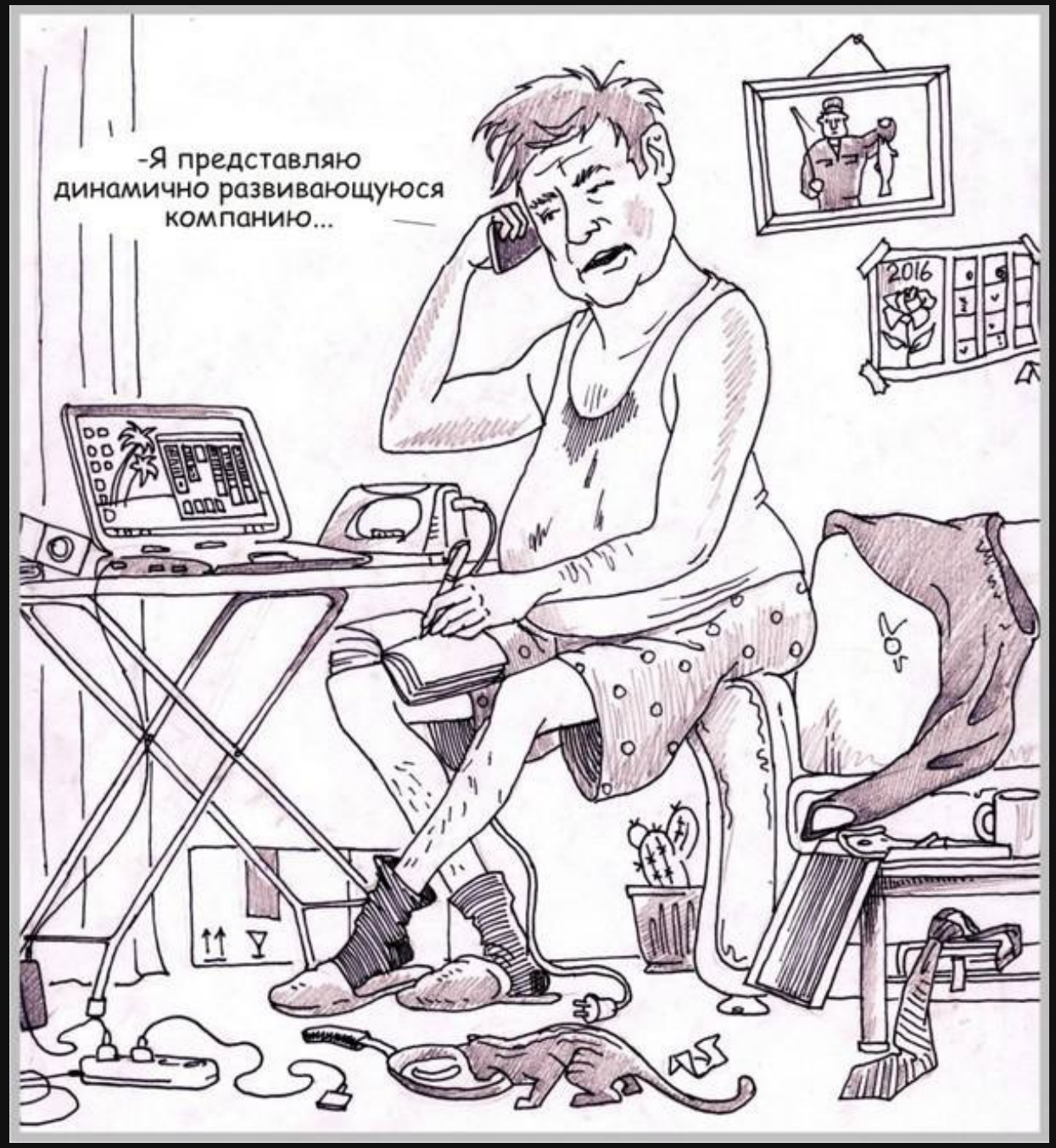
Мошенническая учетная запись (New Account Fraud) – создание новых учётных записей с целью осуществления мошеннических действий;

Отмывание денег или дроп-сервис (Money laundering or money mule) – использования банковских аккаунтов с целью транзита или обналичивания денежных средств;

Средства автоматизации (Hacking tool) – автоматизация пользовательских действий в системах дистанционного обслуживания.



- Отмывание средств или дроп-сервис
- Украденная учетная запись
- Мошенническая учетная запись
- Средства автоматизации



KASPERSKY lab