

KSPD2022

Kaspersky Security Day

**Поведенческая (и не только)
биометрия. Для чего это
финансовому сектору?**

Сегодня в программе

1

Скучные цифры и
унылые графики

3

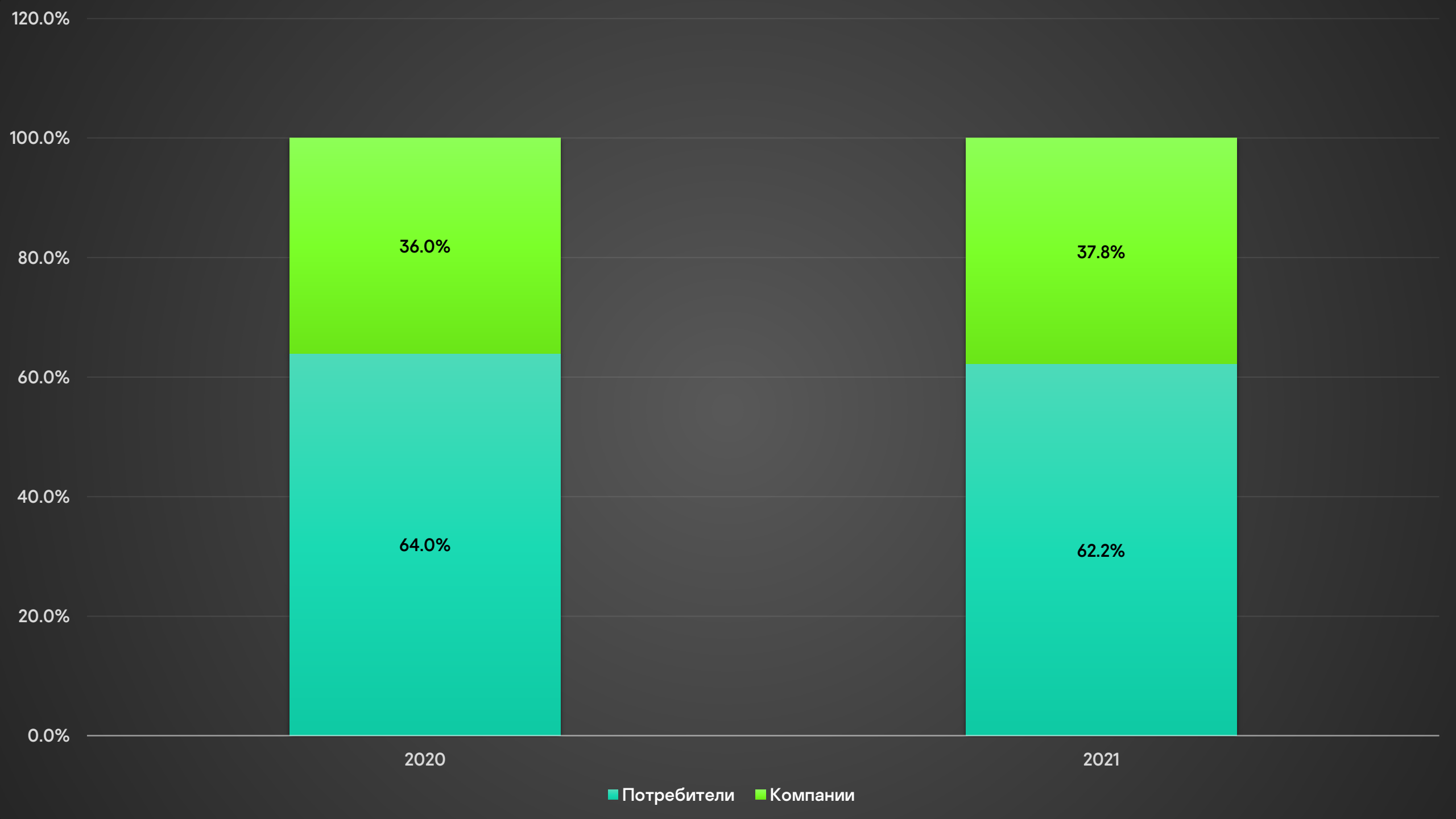
Страшные цифры
(без графиков)

2

Коварные ухищрения
злоумышленников
(фу такими быть)

4

Жемчужины
мудрости (совсем
чуть-чуть)



Google

optima bank

ВСЕ КАРТЫ НОВОСТИ КАРТИНКИ ВИДЕО

Реклама · www.optimabank.work/ **ФЕЙК!!!**

Optimabank.work - Оптима24 онлайн - Оптима24

Оптима24 - выдает всем клиентам 12 тысяч сом за авторизацию. Оптима24 - выдает всем клиентам 12 тысяч сом за авторизацию.

Реклама · www.optimabank.casa/ **ФЕЙК!!!!**

Optimabank.casa - Оптима24 онлайн - Оптима24 онлайн - Оптима24

Оптима24 - выдает всем клиентам 12 тысяч сом за авторизацию. Оптима24 - выдает всем клиентам 12 тысяч сом за авторизацию.

Поддельные сайты

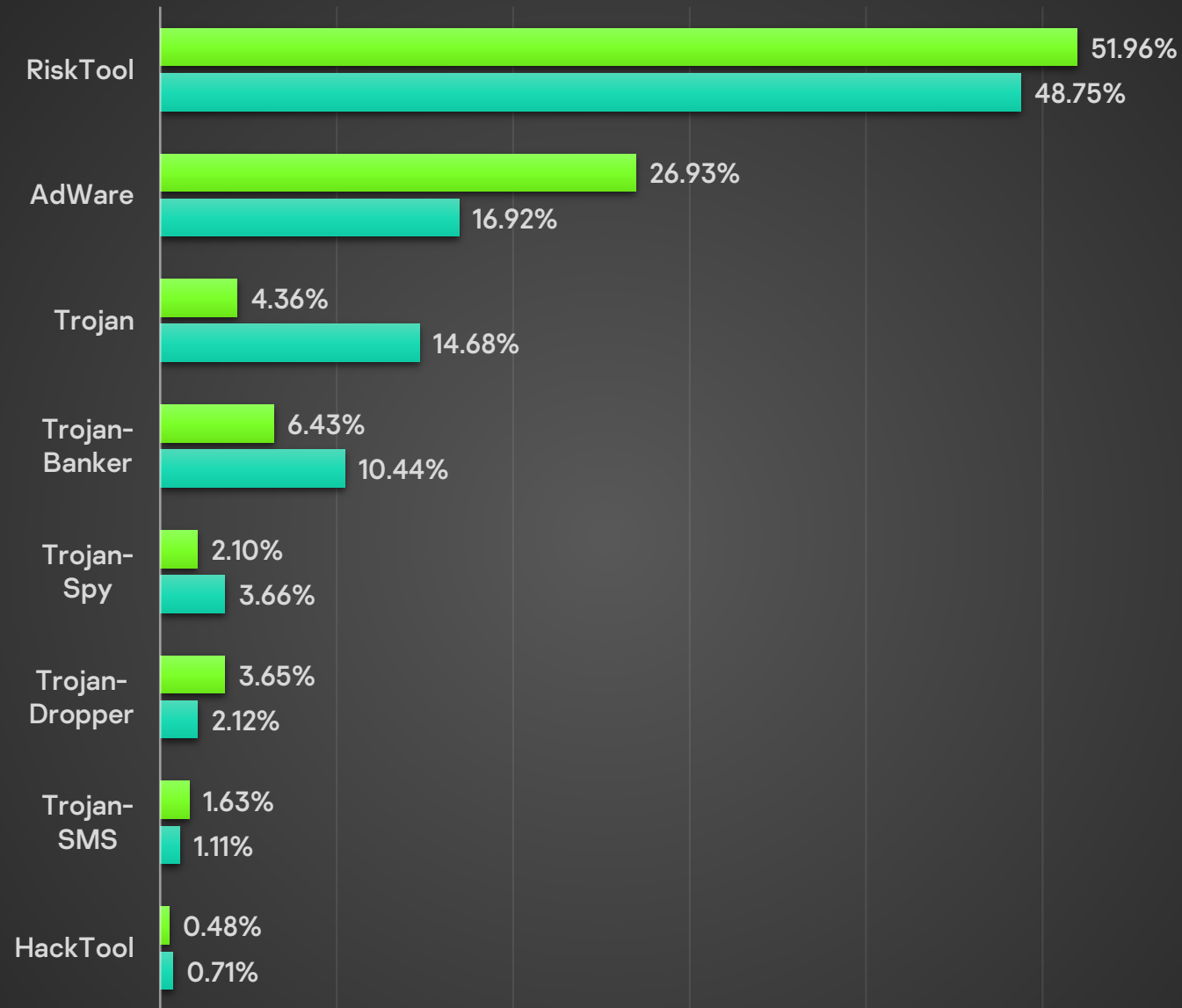
Звонок в банк

Сброс

Аудиозапись



Мобильные угрозы Q1 2022



Рынок Fraud as a Service

7

1

Базы данных
пользователей

2

Дроп-сервисы

3

Средства анонимизации

4

Пробив

5

Контакт-центры

6

Malware as a service

7

Подмена номера



7 Апр 2020

#1

Пробив номера карты Сбербанка по номеру телефона. ТОЛЬКО НОМЕР КАРТЫ
Полный номер карты Сбербанка по номеру телефона с подключенным моб. банком.
Работаю 24/7
СТОИМОСТЬ 1000РУБ.
Для быстрой связи @gango777
ГАРАНТ ДА
Также продам способ пробива, вместе с вами пробью ваш номер карты.

Mister Chao
Новичок

Вы сможете звонить с любых номеров и никто не поймет, что это фейк!

Наши тарифы - от 0,017р/мин!

Безлимитная защищенная GSM связь по всему миру /
Подмена номера / Холодные звонки / Обзвон клиентов



Защита
от прослушки

Подробнее



Подмена
номера

Подробнее



Неограниченные звонки
по всему миру

Подробнее



Подмена
голоса

Подробнее



Защита от определения
местоположения

Подробнее



Битва роботов

Слишком
хорошо, чтобы
быть правдой...

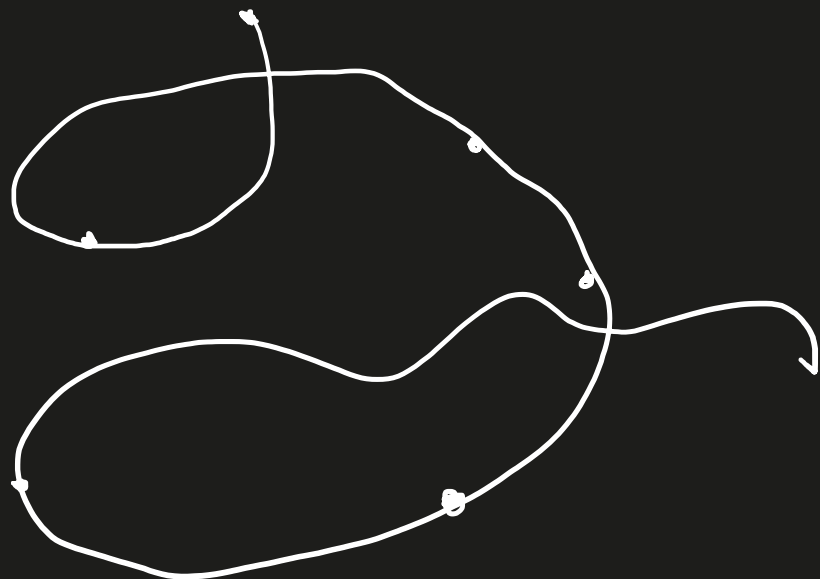


Железная логика!

Угадайте, где бот?

10

1



2

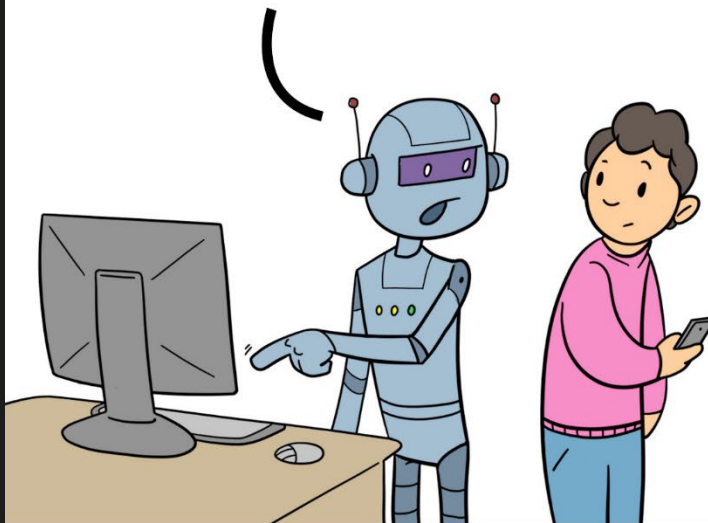


КАПЧА УСТАРЕЛА

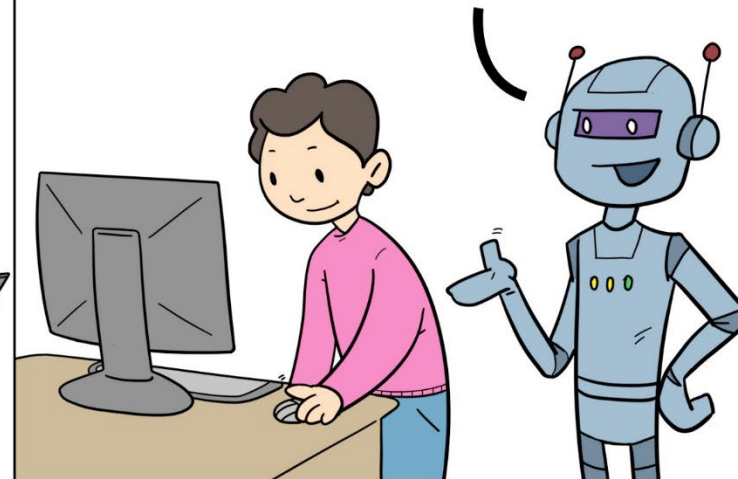
«От жуликов не
спасает, а клиентов
отгоняет»

Скриптонит

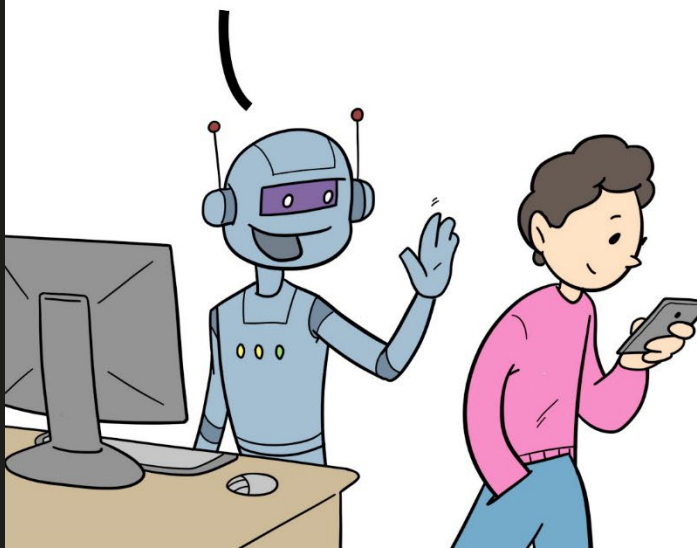
Привет, можешь помочь?



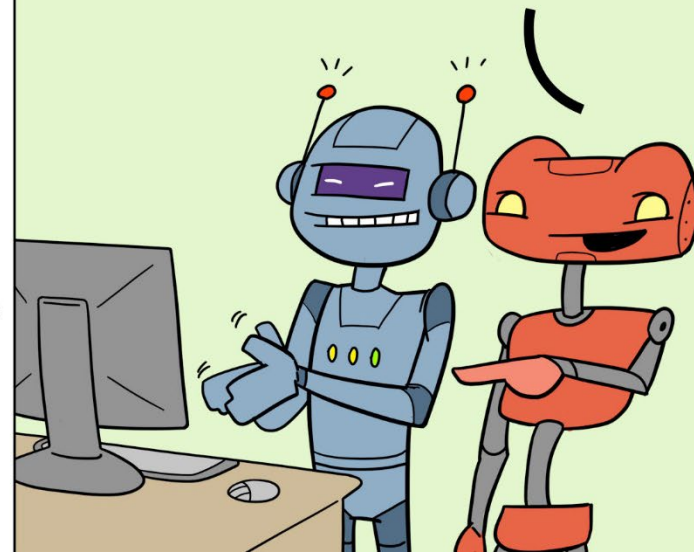
Выбери все фото с
гидрантами, пожалуйста



Спасибо, друг!



Ага, вот мы и вошли



И что делать дальше?

**Как понять, кто перед
тобой?**

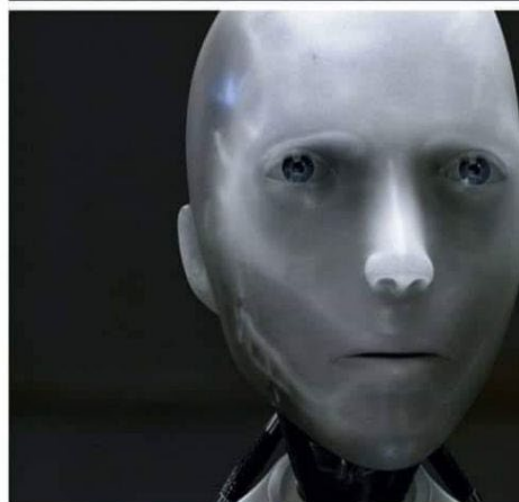
Человек?

Имитация?

**ТЫ ВСЕГО
ЛИШЬ РОБОТ**



**ЗАТО Я НЕ
РАБОТАЮ В
НОВЫЙ ГОД**



15 000

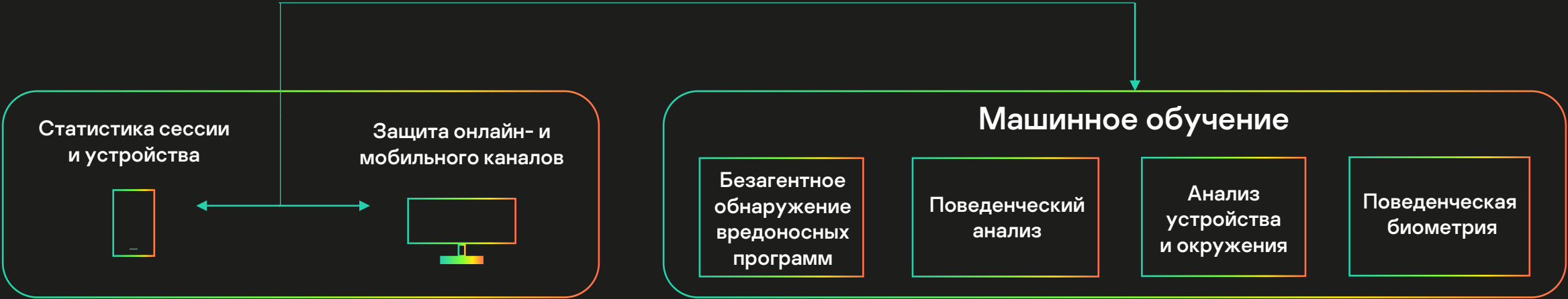
тенге

(15 710 драм)

Наш ответ Чемберлену



Kaspersky
Fraud Prevention



Что такое отпечаток устройства?

15

Мобильное устройство

Root/jailbreak check result
Parent application checksum
Navigation transitions
Device fingerprint
List of the installed applications
Device movements
Finger size and pressure
Swipe and typing speed
Gesture boundaries
Geolocation

Мобильный канал

Оператор: если доступно
– информация сим,
детали оператора

Железо: CPU, дисплей,
память, устройства ввода
и сенсоры

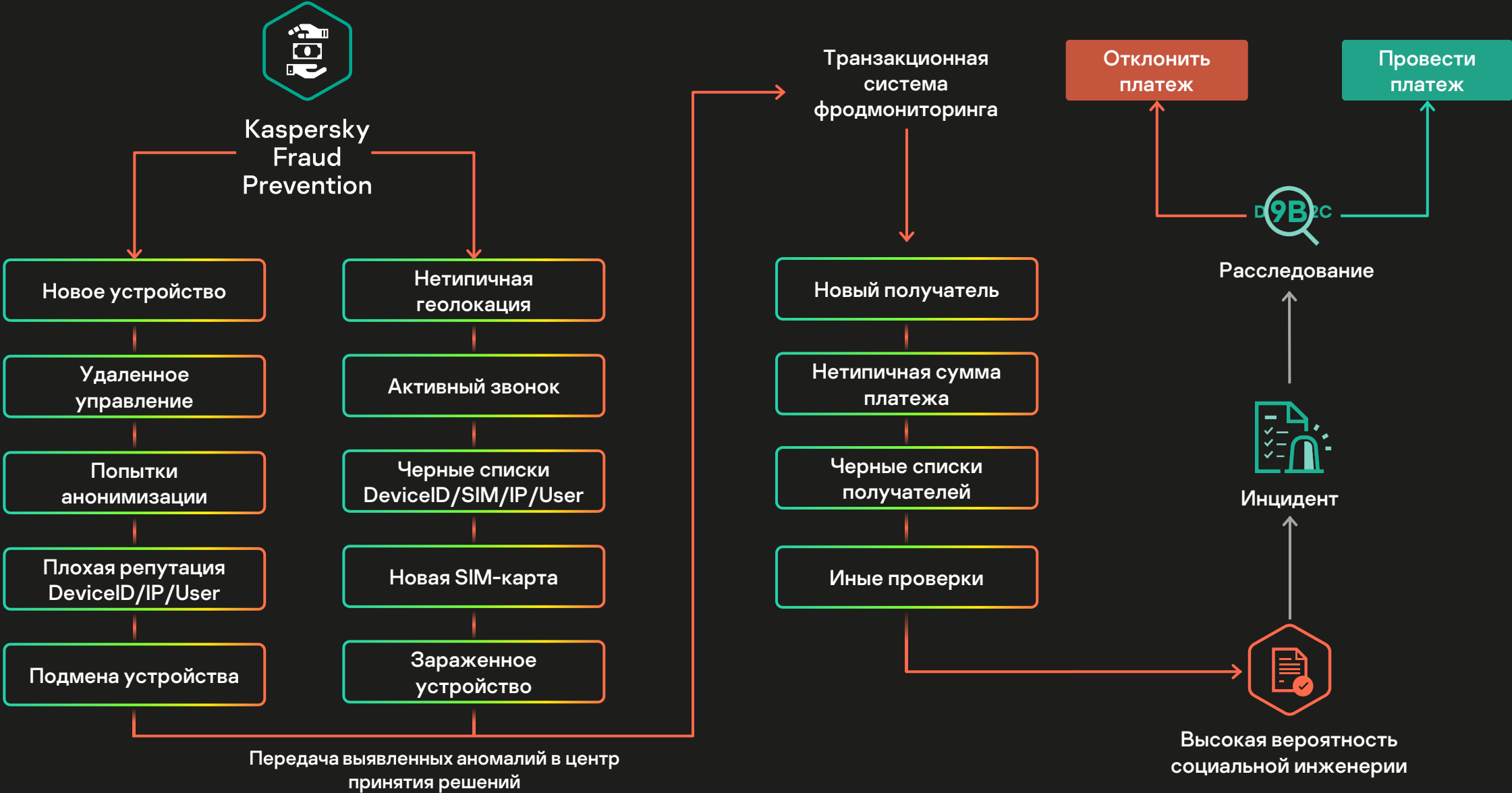
Система: версия,
окружение,
специфические
параметры

Веб-канал

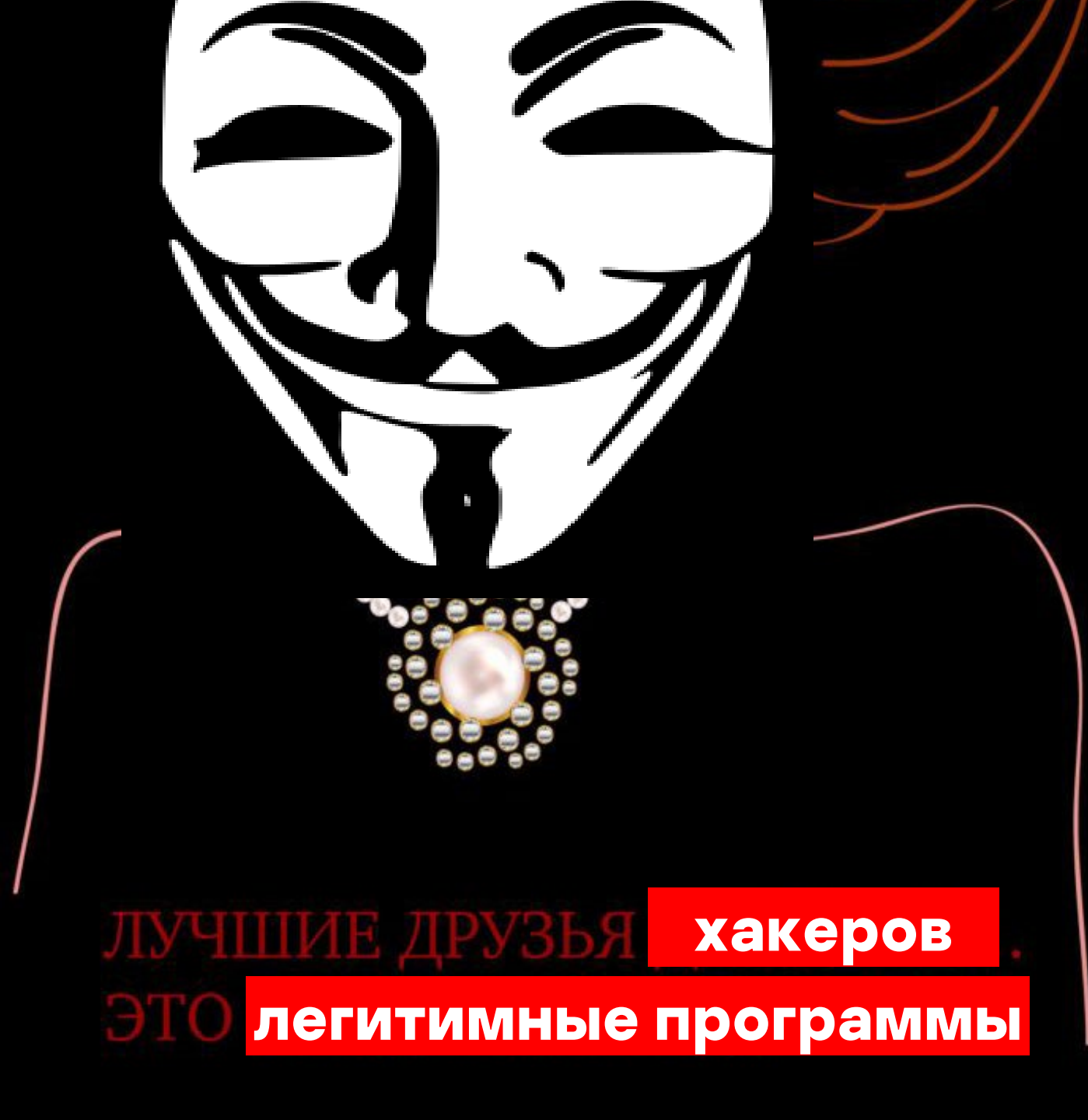
OS, UserAgent, язык, дисплей, временная зона,
шрифты, Browser info, Navigation transitions
Fonts installed, Display info
Canvas info, WebGL parameters
HTML tags, HTML forms,
input fields and Iframes checksums
DOM changes, Password field changes
Device ID, Session ID
Mouse moves and clicks
Keyboard strokes

MacBook Air

Пример цепочки отслеживания по 170+ категориям подозрительных активностей



44%



ЛУЧШИЕ ДРУЗЬЯ **хакеров**
ЭТО **легитимные программы**

Вот с чем приходится бороться

1

TeamViewer

2

AnyDesk

3

Discord

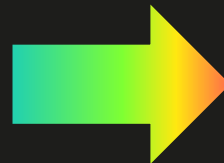
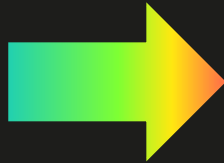
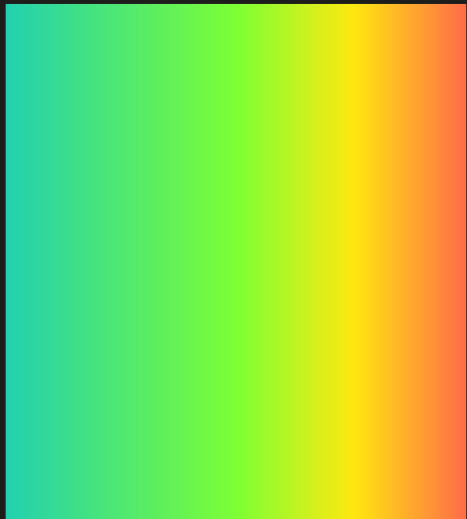


Скомпрометированная учетная запись

На устройстве обнаружено приложение **TeamViewer**, установленное менее чем за 3 часа от анализируемого события.

Month	Rule version	Number of incidents
2	2.7	315
2	2.6	77
2	2.5	54
2	2.4	28
2	2.3	15
2	2.2	43
2	2.1	37
1	2.0	102
1	1.9	80
1	1.8	25
1	1.7	13
1	1.6	2

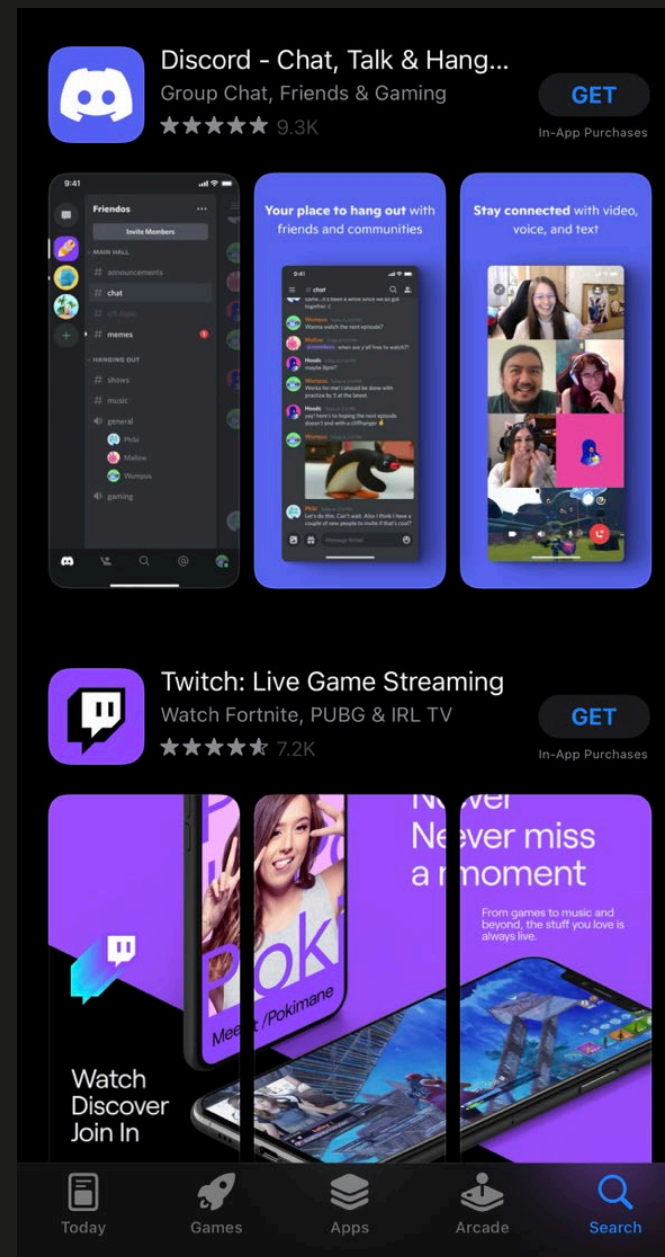
Наши казахстанские наблюдения



А вы слышали про Discord?

**Мессенджер с
возможностью
демонстрации экрана**

То, что доктор прописал





6 драм

85%

7-8

Результаты от внедрения Kaspersky Fraud Prevention в одном крупном банке, согласно независимому исследованию Forrester – Total Economic Impact™

23

Результаты за 3 года:

- Сокращение убытков от мошенничества: **\$ 3.4 млн**
- Экономия на операциях службы поддержки клиентов: **\$121,074** (за счет автоматизации процесса выявления мошеннической активности)
- Экономия за счет отказа от СМС (0,8% базы клиентов): **\$17,571** благодаря реализации «легкого входа» на основе рисков

ROI за 3 года: 168%

Окупаемость за 6 месяцев

Как считали?

- Число клиентов (черный фон)
- Доля клиентов, обращающихся в службу поддержки по подозрительным операциям
- Количество звонков в службу поддержки по подозрительным операциям
- Среднее время обработки обращения
- Средняя стоимость часа работы оператора службы поддержки
- Количество попыток мошенничества за год
- Средняя сумма мошеннической операции
- Затраты банка на потерянный \$1 от мошенничества
- Расходы на программное обеспечение
- Внедрение и сопровождение

Handwritten mathematical notes and diagrams:

- $\text{grad} f = \left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \right)$
- $\tan x \cdot \cot x = 1$
- $2x^2 y y' + y^2 =$
- $Y_{i+1} = Y_i + b \cdot K_2$
- $B = \begin{pmatrix} 2 & 1 & -1 & 0 \\ 3 & 0 & 1 & 2 \end{pmatrix}$
- $\sum_{i=0}^n (p_2(x_i) - y_i)^2$
- $\tan 2x = \frac{2 \tan x}{1 - \tan^2 x}$
- $\tan x = \frac{\sin x}{\cos x}$
- $\int_0^{2\pi} \left(\int_0^2 \left(\int_{\frac{1}{2}}^1 r n r dr \right) d\lambda \right) d\varphi$
- $\lim_{n \rightarrow \infty} \frac{\sqrt[n]{n^3 + 1} + n}{\sqrt[n]{3n^2 + 2n - 1}}$
- $\begin{cases} \lambda x - y + z = 1 \\ x + \lambda y + z = \lambda \\ x + y + \lambda z = \lambda^2 \end{cases}$
- $\frac{a}{\sin \alpha} = \frac{b}{\sin \beta} = \frac{c}{\sin \gamma}$
- $y = \sqrt[3]{x+1}; x = \tan t$
- $x_1 = \begin{pmatrix} \alpha + \beta + \gamma \\ \alpha \\ \beta \end{pmatrix}$
- $\delta(p_2) = \sqrt{0.16}$
- $C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- $F_x'; F_y'; F_z'$
- $a^2 + b^2 = c^2$
- $\alpha, \beta, \gamma \in \mathbb{C}$
- $f(x) = 2^{-x} + 1, \epsilon = 0.005$
- $e^2 - xyz = e; A[0; e; 1]$
- $\lim_{x \rightarrow 0} \frac{e^{2x} - 1}{5x} = \frac{2}{5}$
- $|x| + |y| \neq 0; y \neq 0$
- $\frac{2x}{x^2 + 2y^2} = 2; z = \frac{1}{x} a$
- $\sin(x+y) = \sin x \cos y + \cos x \sin y$
- $y' - \frac{\sqrt{y}}{x+2} = 0; y$
- $\cos \varphi = \frac{(1; 0)}{1}$
- $\lambda_2 = i\sqrt{14}$
- $A = \begin{pmatrix} x, 1+x^2, 1 \\ y, 1+y^2, 1 \\ z, 1+z^2, 1 \end{pmatrix}; x=0, y=1, z=2$
- $A = [1; 0; 3]$
- $\lim_{n \rightarrow \infty} \left(1 + \frac{3}{n} \right)^n$

Diagrams include a coordinate system with a curve, a circle with trigonometric labels, and a 3D-like geometric structure with labeled faces.

Могут подтвердить в Центральной Азии



БАНК КОМПАНИОН



ВОПРОСЫ?

kaspersky