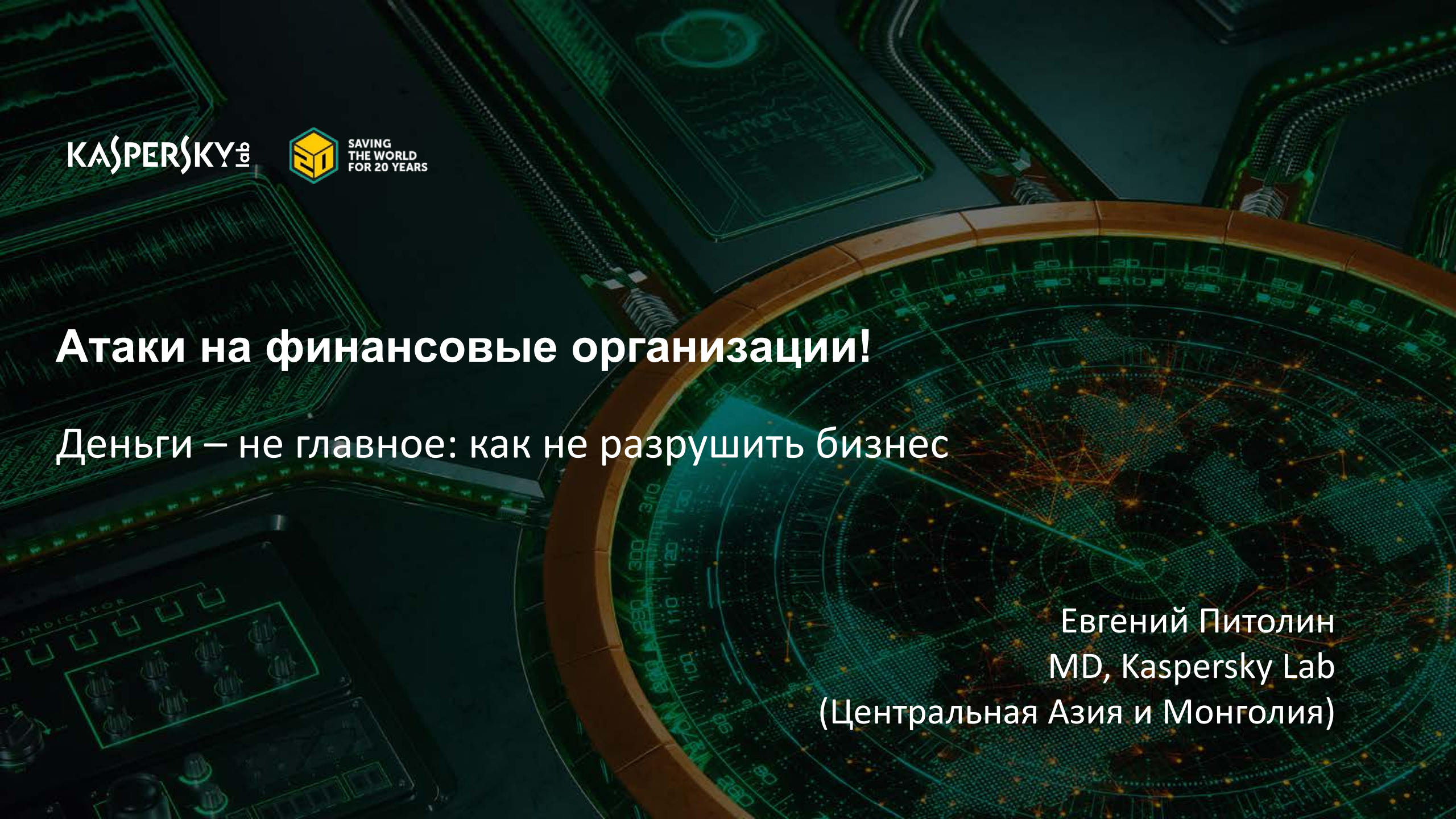


Атаки на финансовые организации!

Деньги – не главное: как не разрушить бизнес

Евгений Питолин
MD, Kaspersky Lab
(Центральная Азия и Монголия)

Тип угрозы

Веб-угрозы

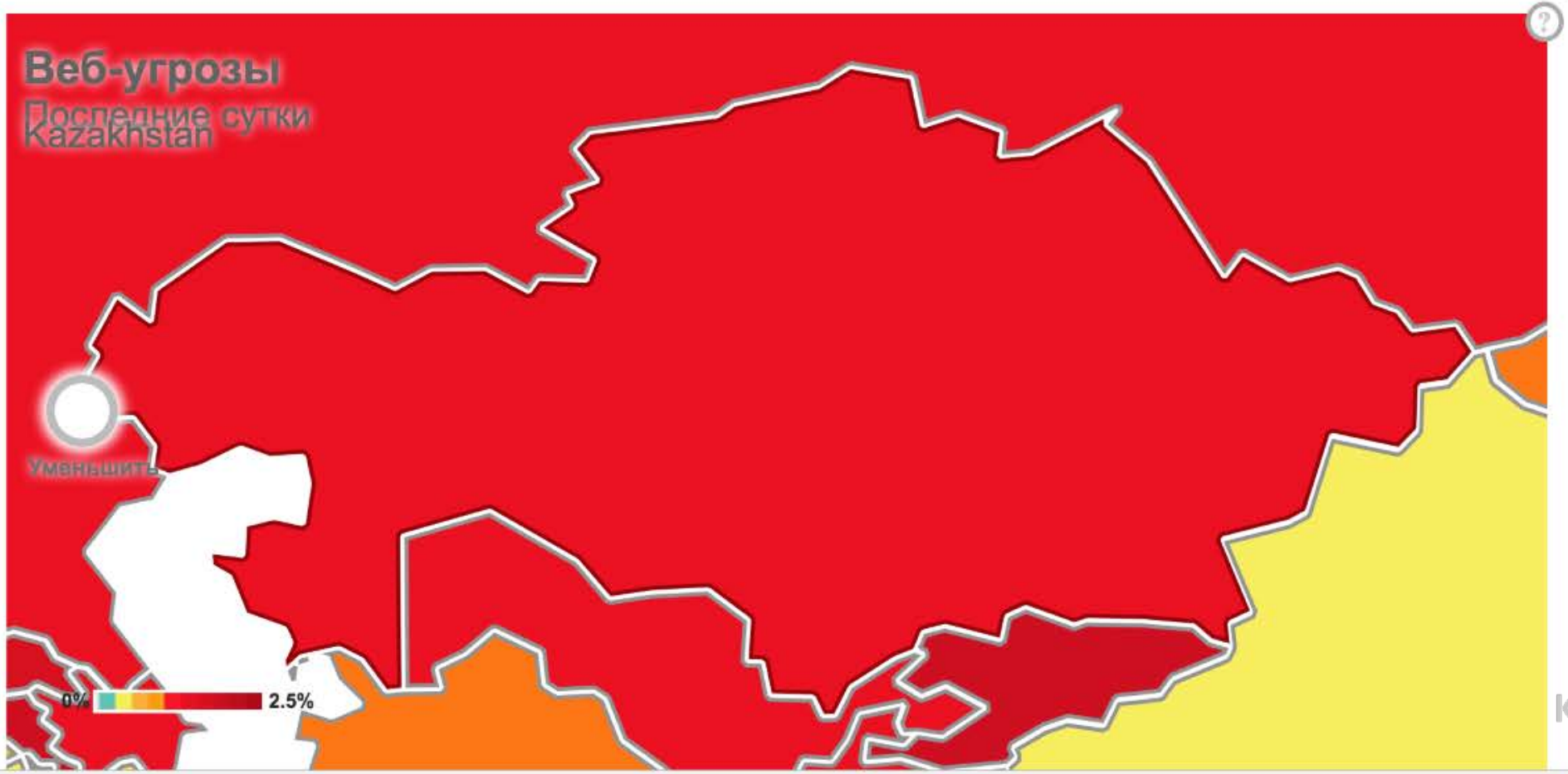
Вид отображения

Карта | Диаграммы | Топ

Период показа

Сутки | Неделя | Месяц

экспорт в PNG



Атаки на финансовые организации

Фишинг:

- В 2017 году доля фишинговых атак на финансовый сектор увеличилась с 47,5% до почти 54% от всех обнаруженных фишинговых атак. По данным «Лаборатории Касперского», это рекордное значение для финансового фишинга.
- Почти каждая четвертая попытка загрузки фишинговой страницы, заблокированная продуктами «Лаборатории Касперского», связана с банковским фишингом.
- В 2017 году доля фишинга, связанного с платежными системами и интернет-магазинами, составила почти 16% и 11% соответственно. Это немного больше (на один процентный пункт), чем в 2016 году.
- Доля фишинга, приходящегося на пользователей MacOS, удвоилась и составляет почти 56%

Атаки на финансовые организации

Вредоносное банковское ПО:

- В 2017 году число пользователей, атакованных банковскими троянскими программами, составило 767 072, что на 30% меньше, чем в 2016 году (1 088 900).
- 19% пользователей, атакованных вредоносным банковским ПО, являлись корпоративными пользователями.
- Чаще всего атакам с использованием вредоносного банковского ПО подвергались пользователи в Германии, России, Казахстане, Китае

Вредоносное банковское ПО для Android

- В 2017 году количество пользователей во всем мире, атакованных вредоносным банковским ПО для Android, снизилось почти на 15% до 259 828.
- В подавляющем количестве атаках на пользователей (более 70%) участвовали всего три семейства вредоносных банковских программ.
- Странами с самым высоким процентом пользователей, подвергшихся атакам вредоносного банковского ПО для Android, стали Россия, Австралия. Казахстан и Германия

Атаки на финансовые организации

Атаки на банкоматы
В 2017 году атаки на банкоматы становились все более привлекательными для киберпреступников, и их количество продолжало расти.

- сложные бесфайловые вредоносные программы
- заклеивание объектива камеры наблюдения и сверление отверстий

- зловред для удаленного управления банкоматами Mitch
- вредоносное ПО для атак на ATM под называнием Cutlet Maker
- (открыто продавалось на рынке Darknet за несколько тысяч долларов)

Под угрозой – не только деньги и данные

ГЛОБАЛЬНЫЕ УГРОЗЫ


Кража денег


Нарушение бизнес-процессов


Потеря доли рынка


Шантаж


Кража цифровой личности

ОПЕРАТОРЫ СВЯЗИ


Атаки на клиентов


Мошеннические рассылки от лица оператора


Подделка веб-ресурсов с целью фишинга


Контроль над биллингом

МЕДИЦИНСКИЕ ОРГАНИЗАЦИИ


Кража данных о пациентах


Атаки на проекты телемедицины

ФИНАНСОВЫЕ СТРУКТУРЫ


Кража денег


Кража личности

ГОСУДАРСТВЕННЫЕ ОРГАНИЗАЦИИ


Шпионаж


Манипуляция открытыми данными


Ограничение доступа к государственным услугам

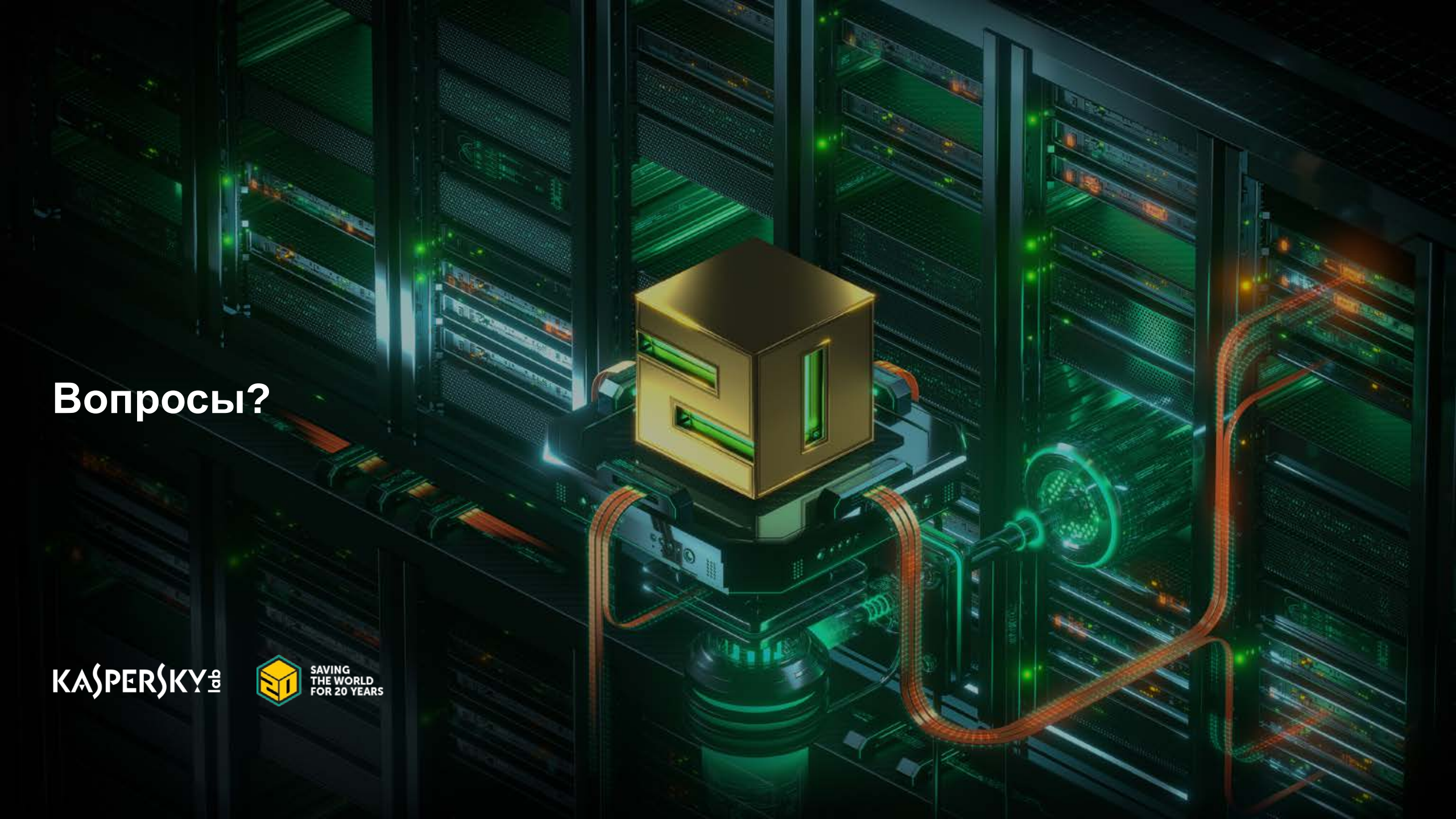

Кража личности

Вопросы для вашего CEO

Подумали ли Вы о человеческом факторе?

1. Каждый ли сотрудник осознает свою ответственность за цифровые активы компании?
2. Обучали ли вы хоть раз сотрудников цифровой гигиене? Проверяли ли потом их знания?
3. Установлены ли политики безопасности и регламенты внутри организации?
4. Какая ответственность предусмотрена за нарушение ИБ-политик, включая уровень руководства

Понимает ли CEO,
что он несет персональную
ответственность за ИБ в компании,
и должен своим примером
задавать высокие стандарты?


Вопросы?
KASPERSKY lab
SAVING
THE WORLD
FOR 20 YEARS