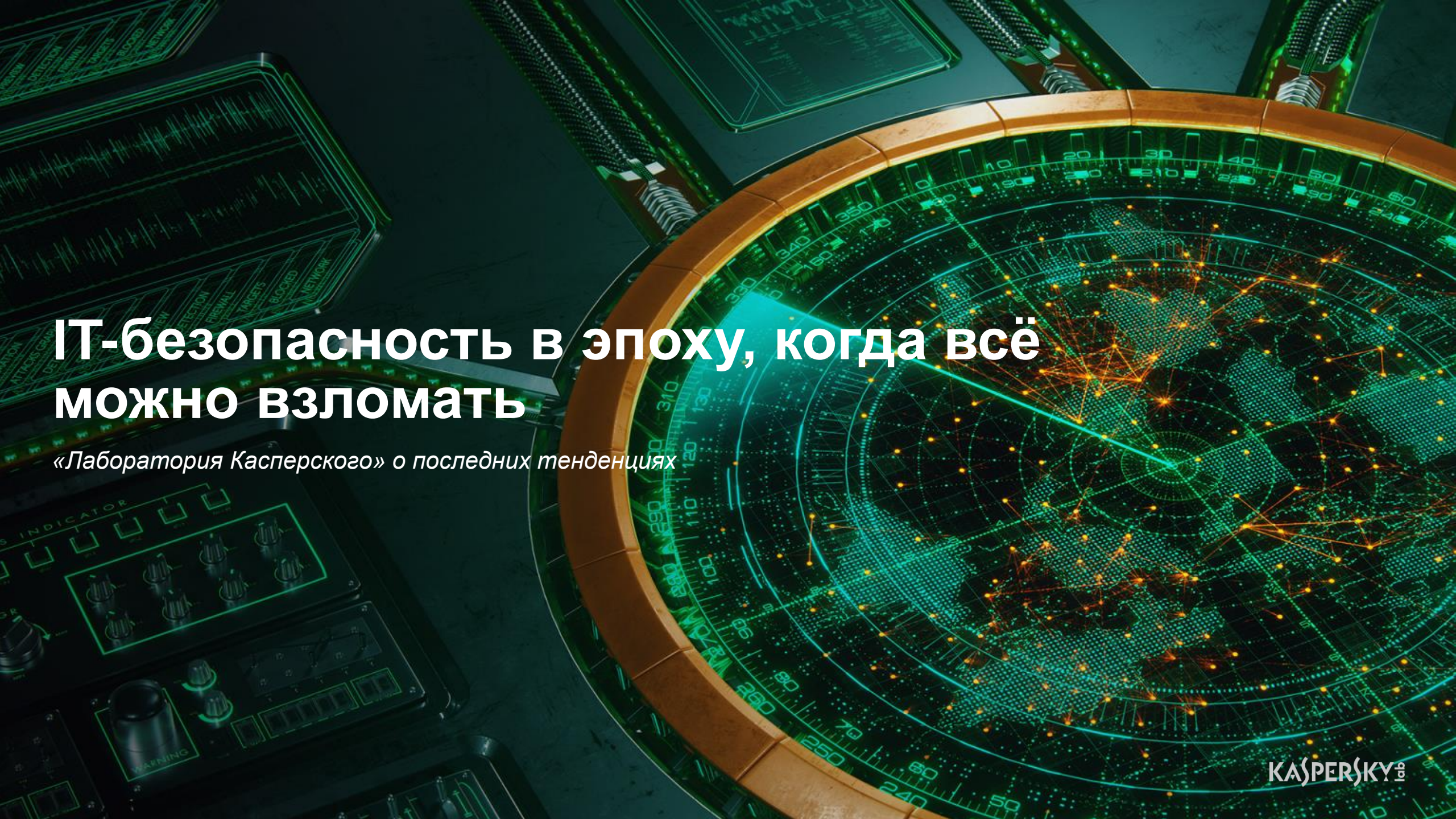


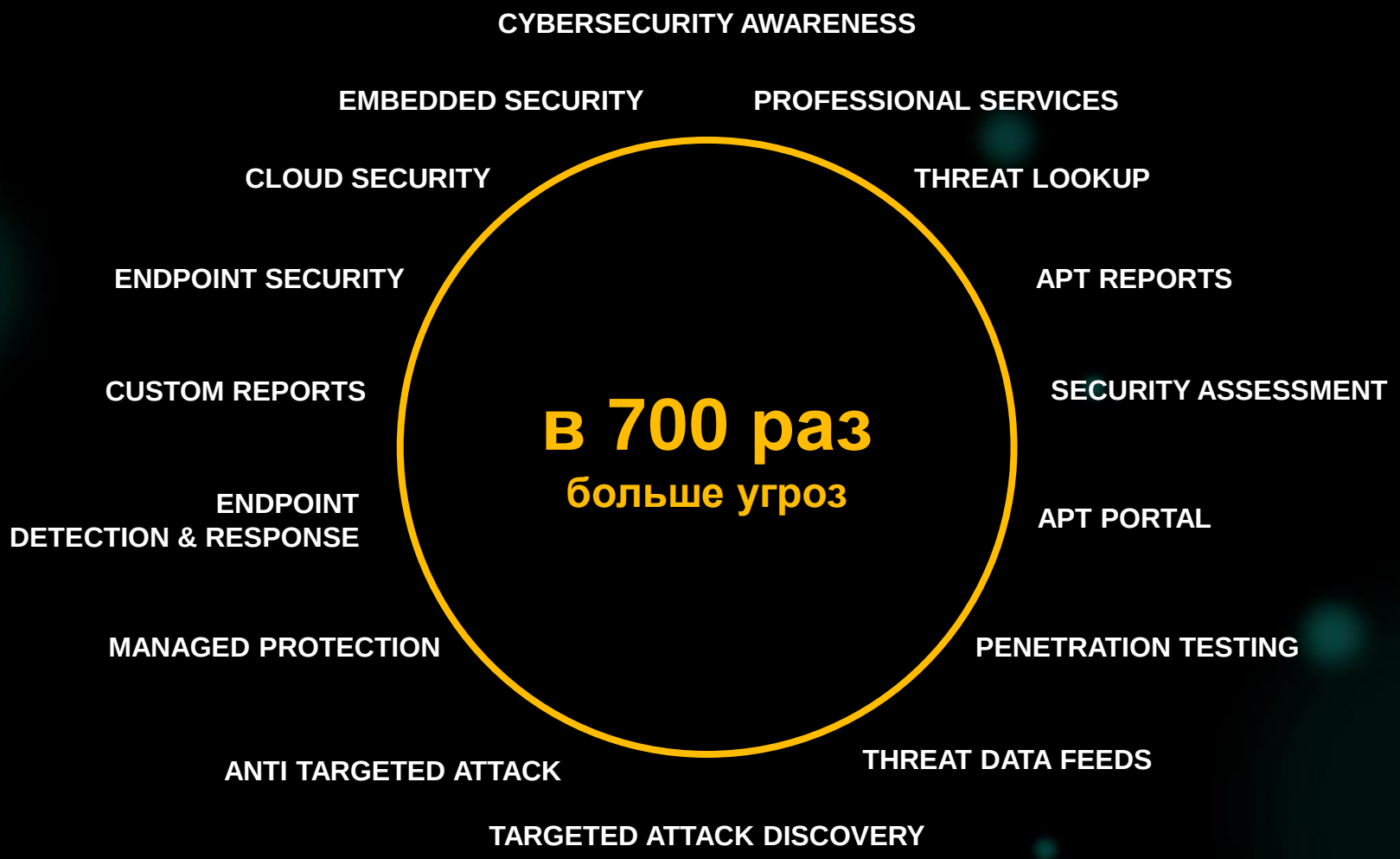
# IT-безопасность в эпоху, когда всё можно взломать

*«Лаборатория Касперского» о последних тенденциях*

KASPERSKY lab

# Простая защита больше не работает

**ЗАЩИТА КОНЕЧНЫХ УСТРОЙСТВ**




2006

2018

KASPERSKY lab

# 2017 – год сложных и разрушительных атак

Быстро эволюционирующие угрозы требуют совершенствования защиты с помощью экспертизы и реагирования на инциденты

#WannaCry
#ExPetr

#targetedattacks

#supplychainattacks

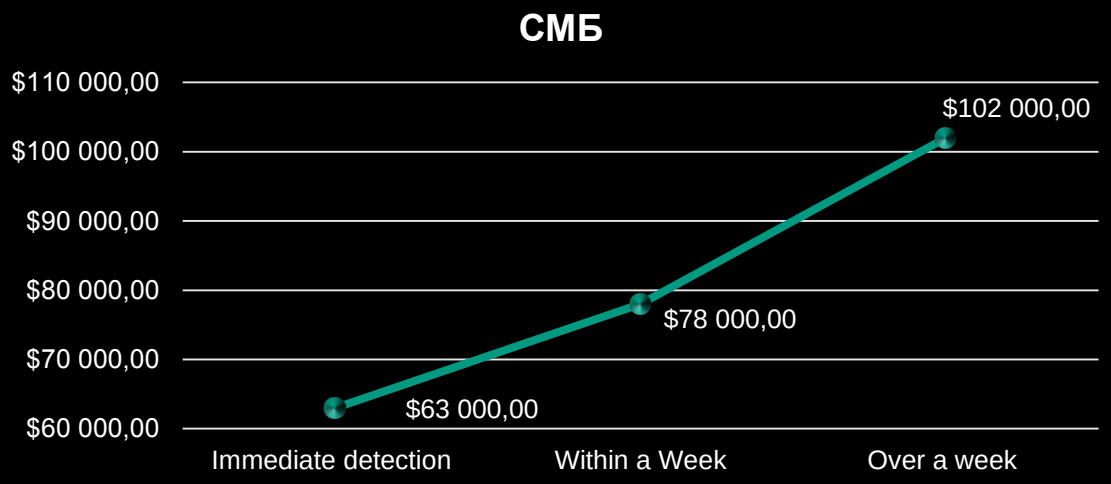
#geopoliticalcrossfire

#leakedvulnerabilities

Взлом системы безопасности –
не «если», а «когда»

KASPERSKY lab

# Компании стараются быстрее обнаруживать инциденты безопасности


*Источник: исследование рисков корпоративной IT-безопасности 2017*

- Компаниям необходимо несколько недель чтобы понять, что их атаковали
- Если крупное предприятие не обнаруживает инцидент сразу, то он обходится ему в 2,6 раза дороже
- Если СМБ компания не обнаруживает инцидент сразу, то он обходится ей в 1,6 раза дороже

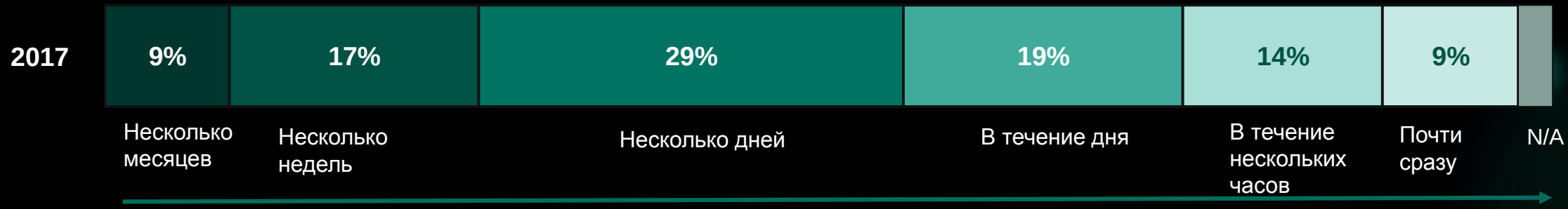
KASPERSKY lab

# Целевые атаки: как с ними бороться?

- Время обнаружения инцидента критично
- Превентивные стратеги не обезопасят вас
- Задержки дорого обходятся

**СОЗДАЙТЕ ВНУТРЕННЮЮ EDR СТРАТЕГИЮ**

## ВРЕМЯ ОБНАРУЖЕНИЯ ИНЦИДЕНТОВ В КОМПАНИЯХ




KASPERSKY lab

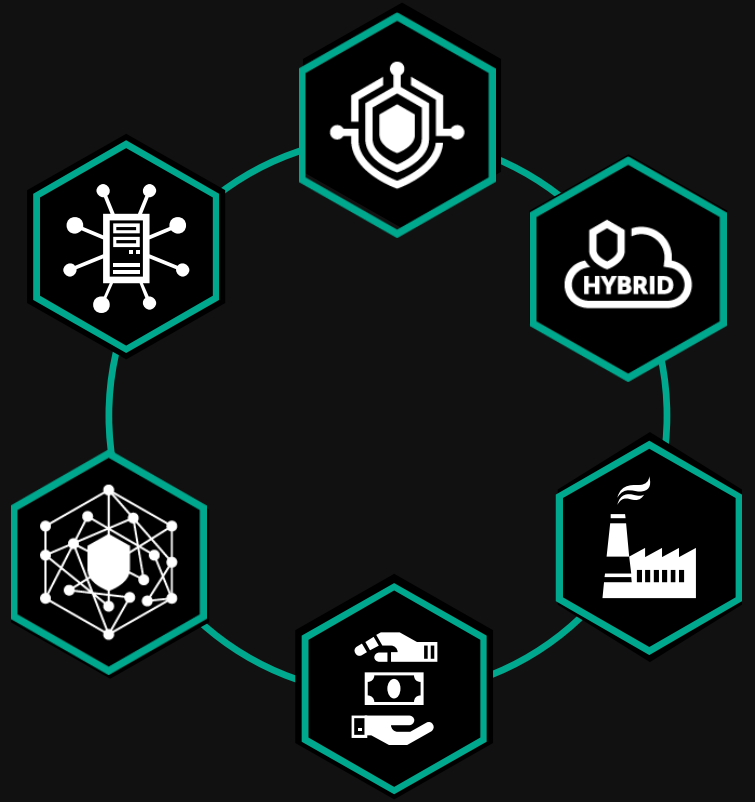
# Как оставаться в безопасности

## Threat Management and Defense

Обнаружение и устранение рисков, связанных со сложными угрозами и целевыми атаками

## Защита конечных устройств

Передовая многоуровневая платформа для защиты конечных устройств, в основе которой технологии нового поколения




## Защита гибридного облака

Безграничная безопасность, созданная для вашей гибридной облачной среды

## Защита IoT

Комплексная безопасность, созданная специально для IoT-систем

## Промышленная кибербезопасность

Специализированная защита систем промышленного контроля

## Борьба с мошенничеством

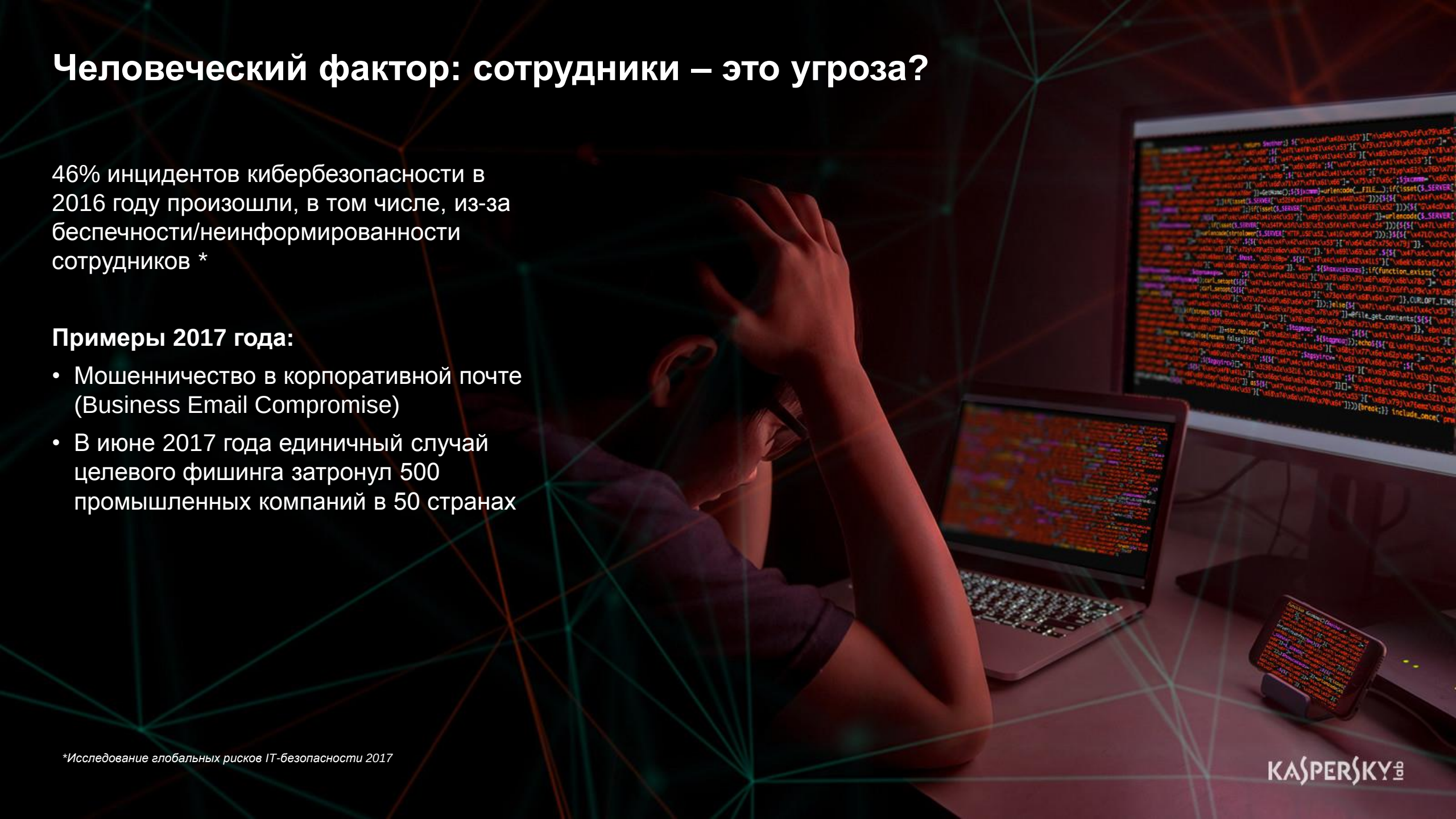
Проактивное детектирование кросс-канального мошенничества в режиме реального времени

# Человеческий фактор: сотрудники – это угроза?

46% инцидентов кибербезопасности в 2016 году произошли, в том числе, из-за беспечности/неинформированности сотрудников *

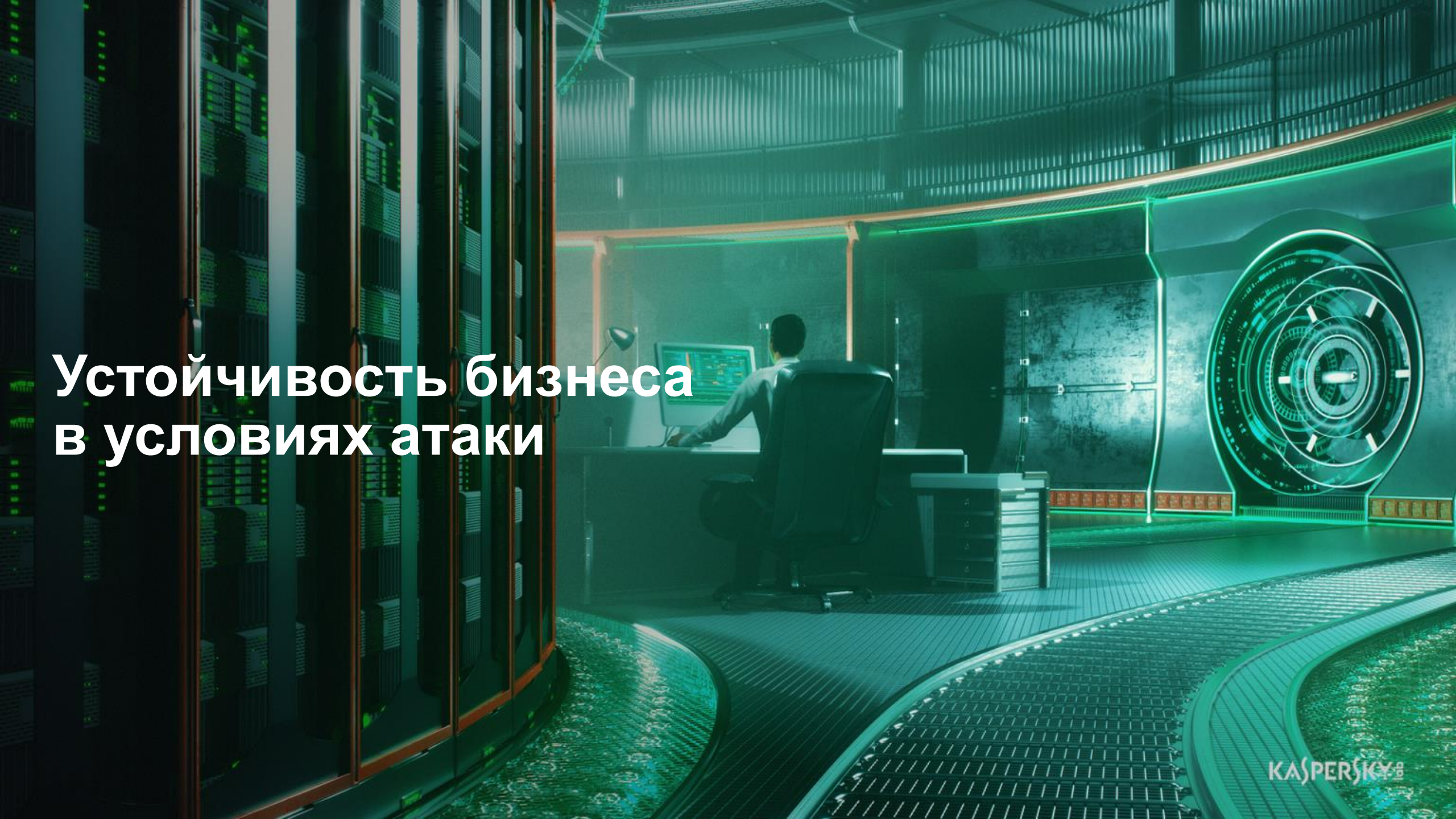
**Примеры 2017 года:**

- Мошенничество в корпоративной почте (Business Email Compromise)
- В июне 2017 года единичный случай целевого фишинга затронул 500 промышленных компаний в 50 странах



**Исследование глобальных рисков IT-безопасности 2017*

KASPERSKY lab


Устойчивость бизнеса
в условиях атаки
KASPERSKY

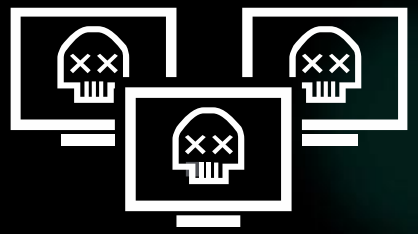
# DDoS: гораздо больше, чем просто неприятность

Средняя стоимость кибератаки с применением DDoS – **$123 000** для небольших компаний и **$2,3 млн** для крупных предприятий. **70%** компаний были атакованы больше одного раза за год.

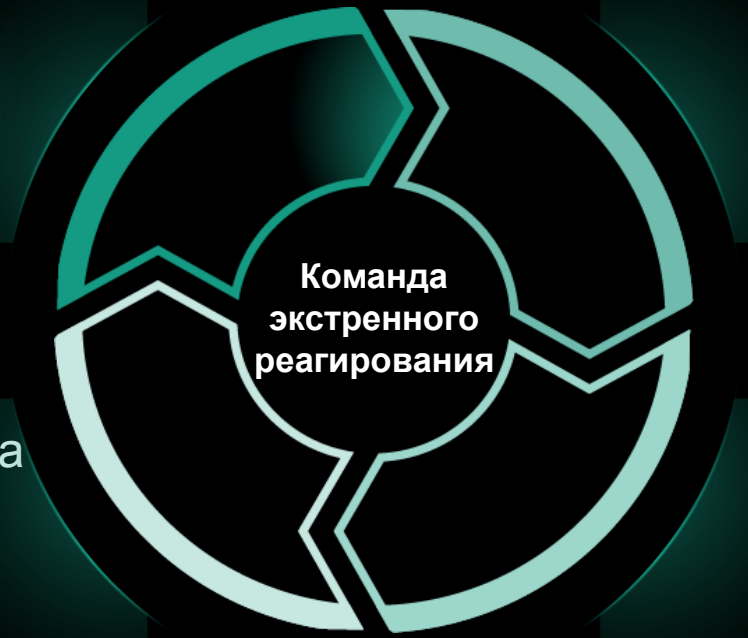
KASPERSKY lab

# Как мы помогаем бороться с DDoS-атаками

Kaspersky DDoS Intelligence



Мониторинг трафика и поддержка в режиме 24x7x365




Постоянная защита или защита по требованию

Более 20 лет уникального опыта

KASPERSKY lab

# Шифровальщики: массовые заражения

## 2017:

11% рост числа людей, атакованных шифровальщиками

23% компаний пострадали от шифровальщиков

Более трети атакованных потеряли все данные (9%) или значительную часть их (29%)

| | | | | |
|---|---|---|---|---|
| **3 масштабных атаки шифровальщиков** | **WannaCry** | **ExPetr** | **BadRabbit** | **использование шифровальщиков в целевых атаках** |

KASPERSKY lab

# Как мы помогаем бороться с шифровальщиками

## Специальные технологии:

Kaspersky Security Network

Анализ поведения (раньше – часть компонента Мониторинг системы)

Откат вредоносных действий (раньше – Откат)

Во всех корпоративных решениях «Лаборатории Касперского» содержатся технологии борьбы с шифровальщиками


Kaspersky Anti-Ransomware Tool (бесплатная утилита)

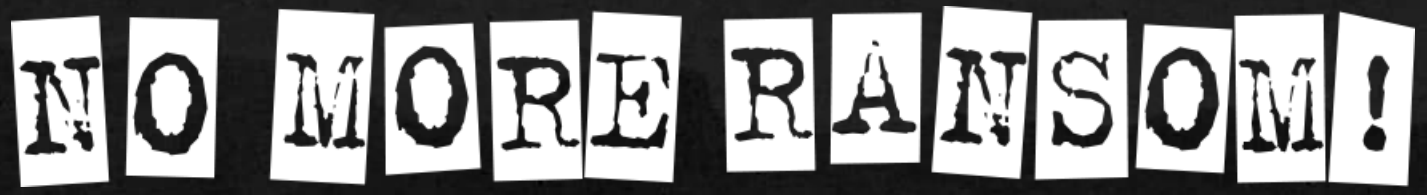
Kaspersky Security для бизнеса


Kaspersky Security для виртуальных и облачных сред

Kaspersky Endpoint Detection and Response

Kaspersky Security для мобильных устройств

# Ответный удар: инициатива No More Ransom




Проект No More Ransom был запущен в июле 2016 года силами полиции Нидерландов, Европола, McAfee и «Лаборатории Касперского»

## За один год:

**Более**

**28 000**

устройств были дешифрованы

**54**

инструмента дешифровки

**Более**

**100**

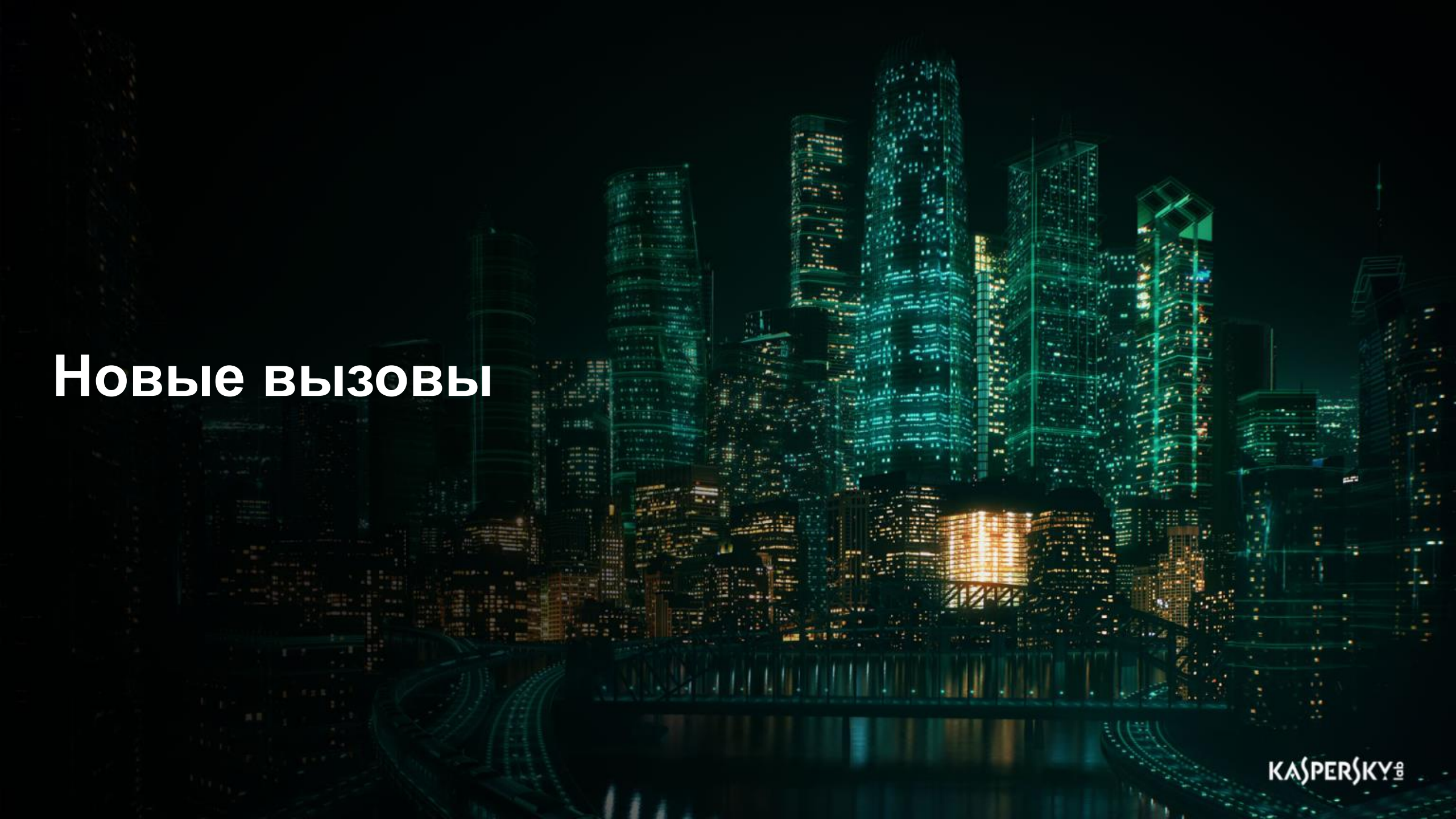
партнёров

**26**

языков

KASPERSKY lab

# Новые вызовы



# Облако: расширенный периметр

РАСПРОСТРАНЁННОСТЬ ВИРТУАЛИЗАЦИИ… **75%** | В ПРОЦЕССЕ

- vmware® — 45%
- Microsoft — 35%
- CITRIX® — 12%
- KVM — 8%


- Microsoft Azure
- amazon web services

KASPERSKY lab

# Безопасность облака вызывает беспокойство

**59%** компаний (как СМБ, так и крупного бизнеса) полагают, что аутсорсинг и облачные сервисы могут создать новые риски для безопасности их IT инфраструктур.

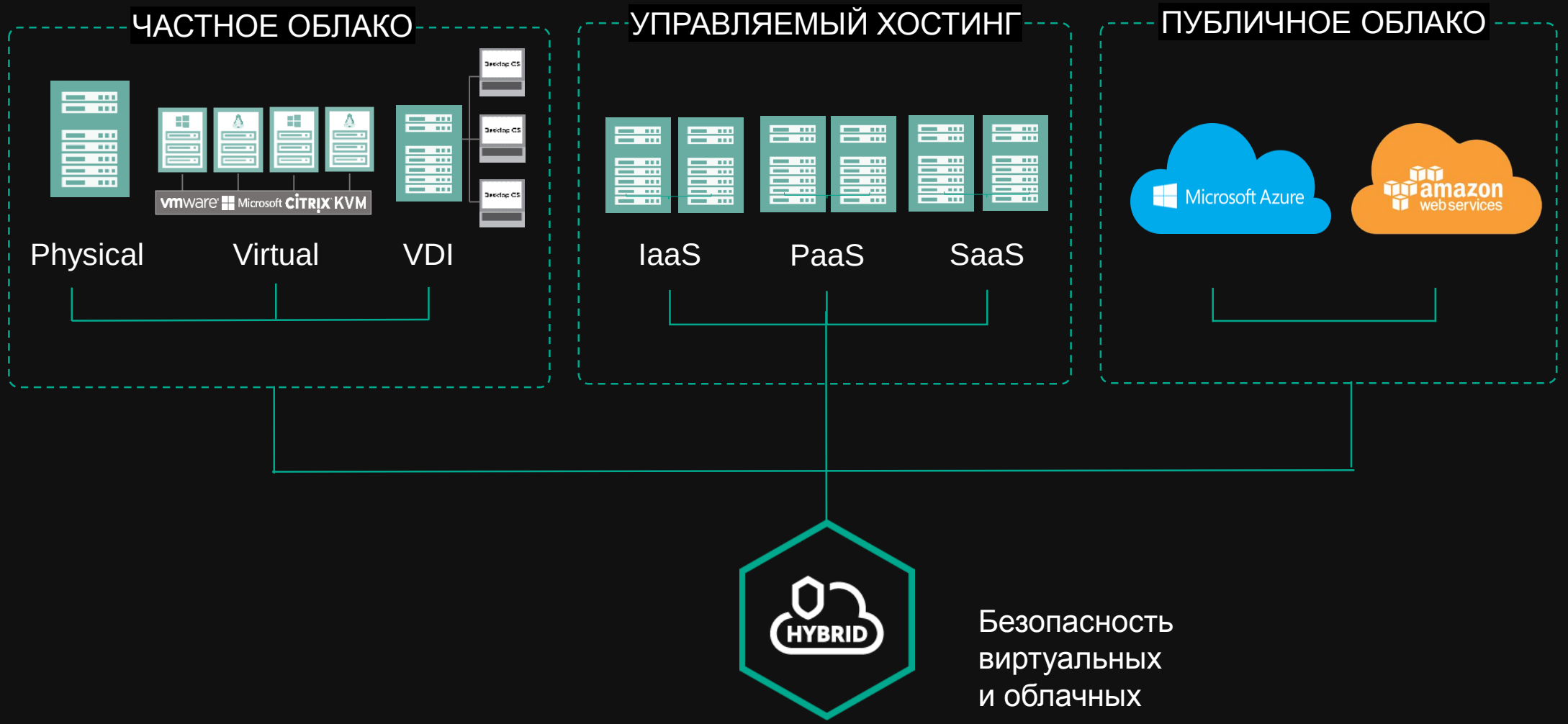
Инциденты, которые затрагивают IT инфраструктуры, управляемые третьей стороной, входят в топ 3 быстро нарастающих проблем – за последние 12 месяцев с такими инцидентами столкнулось 24% компаний.

45% пострадавших столкнулись с потерей или утечкой данных в результате взлома облачной инфраструктуры, находящейся на аутсорсинге.

Источник: глобальное исследование рисков IT-безопасности 2017

KASPERSKY lab

# Как защитить гибридное облако




Безопасность виртуальных и облачных сред

KASPERSKY lab

# Финансы: новые векторы атак

Тенденции

Атаки на банкоматы – например, снятие наличных через удалённое управление

Предприятия с POS терминалами становятся отдельной целью

30% рост числа людей, атакованных банковскими троянцами

Криптовалюты и финансовые системы на блокчейне – новые цели для киберпреступников


KASPERSKY lab

# Как защититься от финансовых угроз

Финансовые организации должны знать, что их безопасность не ограничивается только их периметром:

## Защита банкоматов и POS-терминалов

Kaspersky Embedded Systems Security

## Защита от всех угроз

- Kaspersky Endpoint Security
- Kaspersky Hybrid Cloud Security
- Kaspersky Anti Targeted Attack
- Kaspersky Cybersecurity Services

## Защита каналов цифрового банкинга

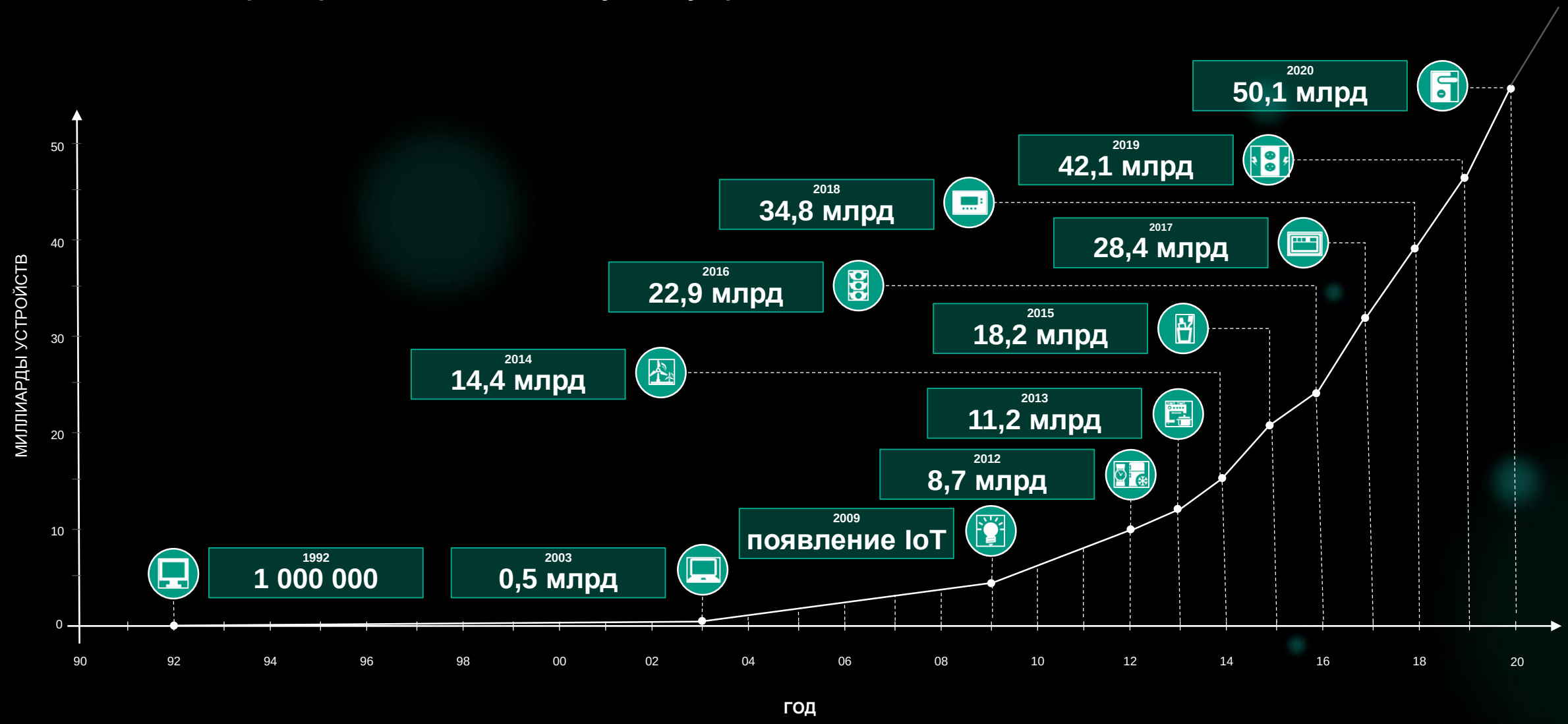
Kaspersky Fraud Prevention

## Защита на стороне клиентов банков

Kaspersky Total Security (решение для дома)

# Интернет вещей

**Что если в вашем периметре есть подключённые умные устройства?**




KASPERSKY lab

# Сделать IoT безопасным по умолчанию

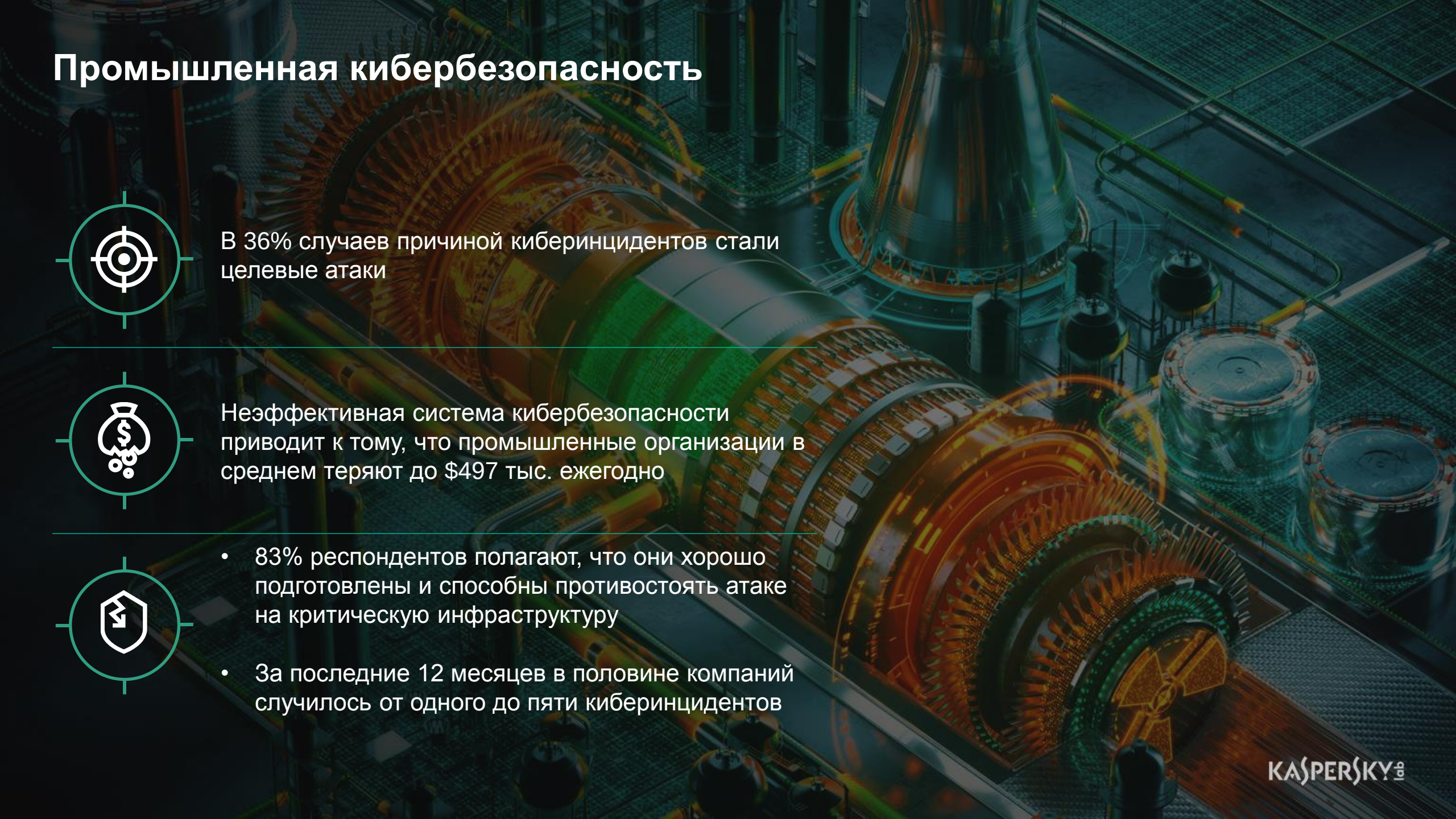
KasperskyOS®

Значительно снижает возможность недокументированной функциональности

Адаптируется под потребности разработчика

Делает разработку ПО для IoT устройств изначально безопасной

# Промышленная кибербезопасность



В 36% случаев причиной киберинцидентов стали целевые атаки

Неэффективная система кибербезопасности приводит к тому, что промышленные организации в среднем теряют до $497 тыс. ежегодно

- 83% респондентов полагают, что они хорошо подготовлены и способны противостоять атаке на критическую инфраструктуру
- За последние 12 месяцев в половине компаний случилось от одного до пяти киберинцидентов

KASPERSKY lab

# Границы безопасности критической инфраструктуры

МОДЕЛЬ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ (ISA-95)*

**Уровень 4**

Бизнес-планирование и логистика

**Уровень 3**

Управление производственными операциями

**Уровень 1 / Уровень 2**

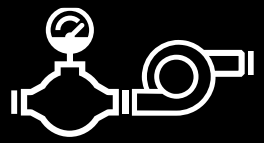
Контроль пакетов / Постоянное регулирование / Автономное управление

**Уровень 0**

Физический

Kaspersky Endpoint Security for Business + Kaspersky Cybersecurity Services

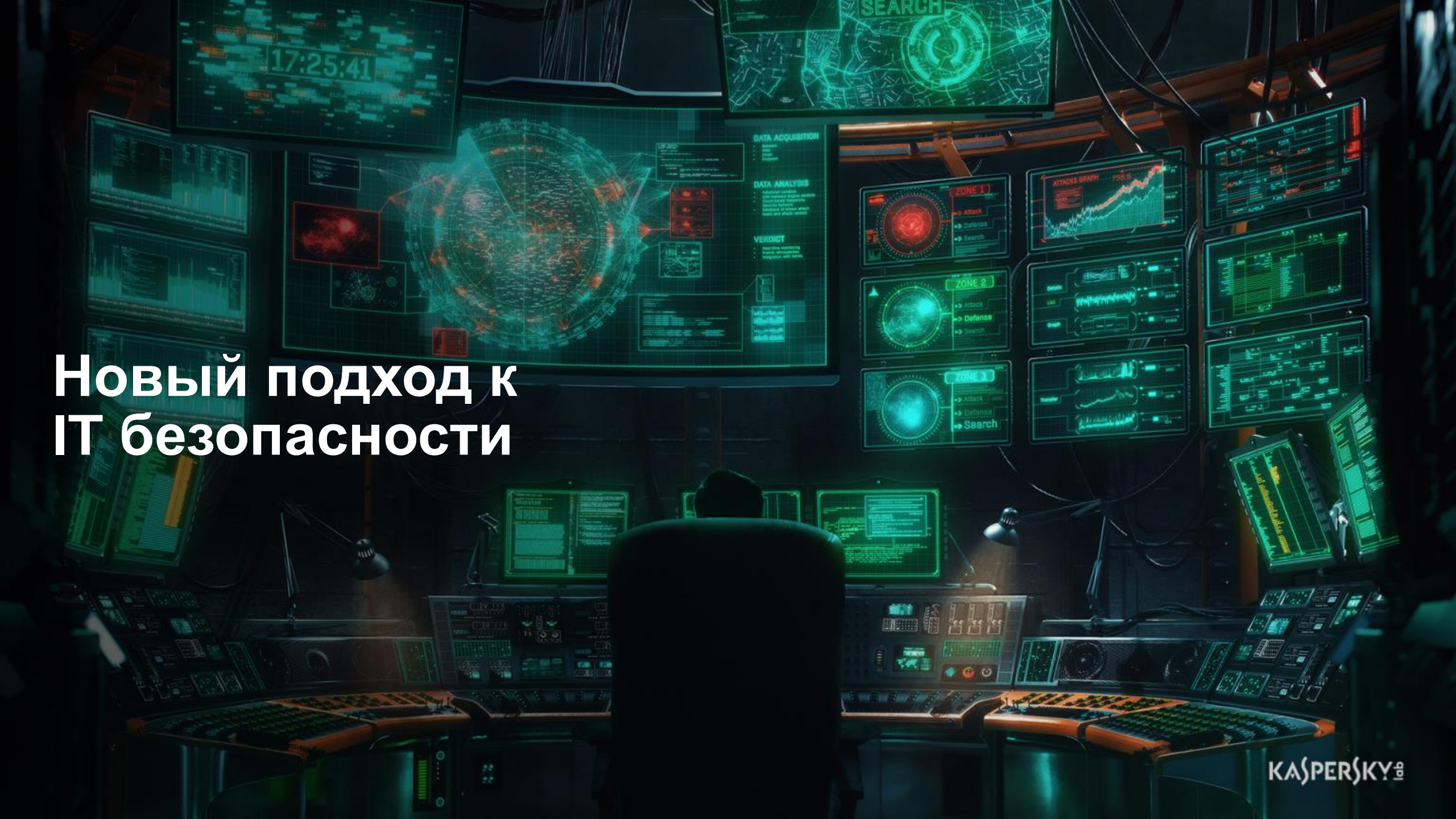
Kaspersky Industrial CyberSecurity



Физическая безопасность

* ISA-95 – международный стандарт от Международного сообщества автоматизации, принятый для разработки автоматизированного интерфейса между предприятием и системами промышленного контроля

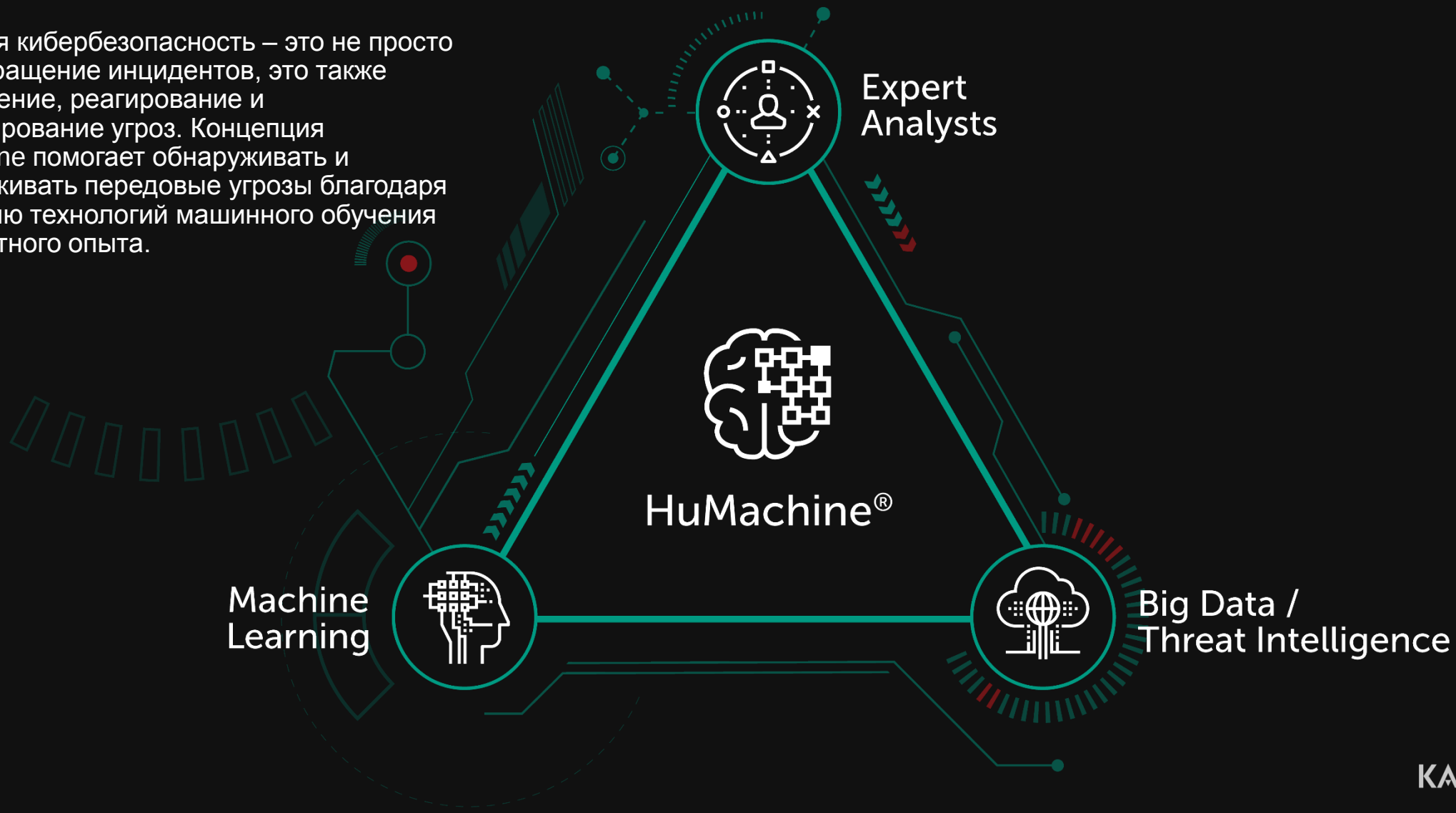
KASPERSKY lab




# Новый подход к IT безопасности

# Истинная кибербезопасность

Истинная кибербезопасность – это не просто предотвращение инцидентов, это также обнаружение, реагирование и прогнозирование угроз. Концепция HuMachine помогает обнаруживать и обезвреживать передовые угрозы благодаря сочетанию технологий машинного обучения и экспертного опыта.




KASPERSKY lab


Поговорим?
KASPERSKY lab