Концепция доверия и безопасности для критических инфраструктур

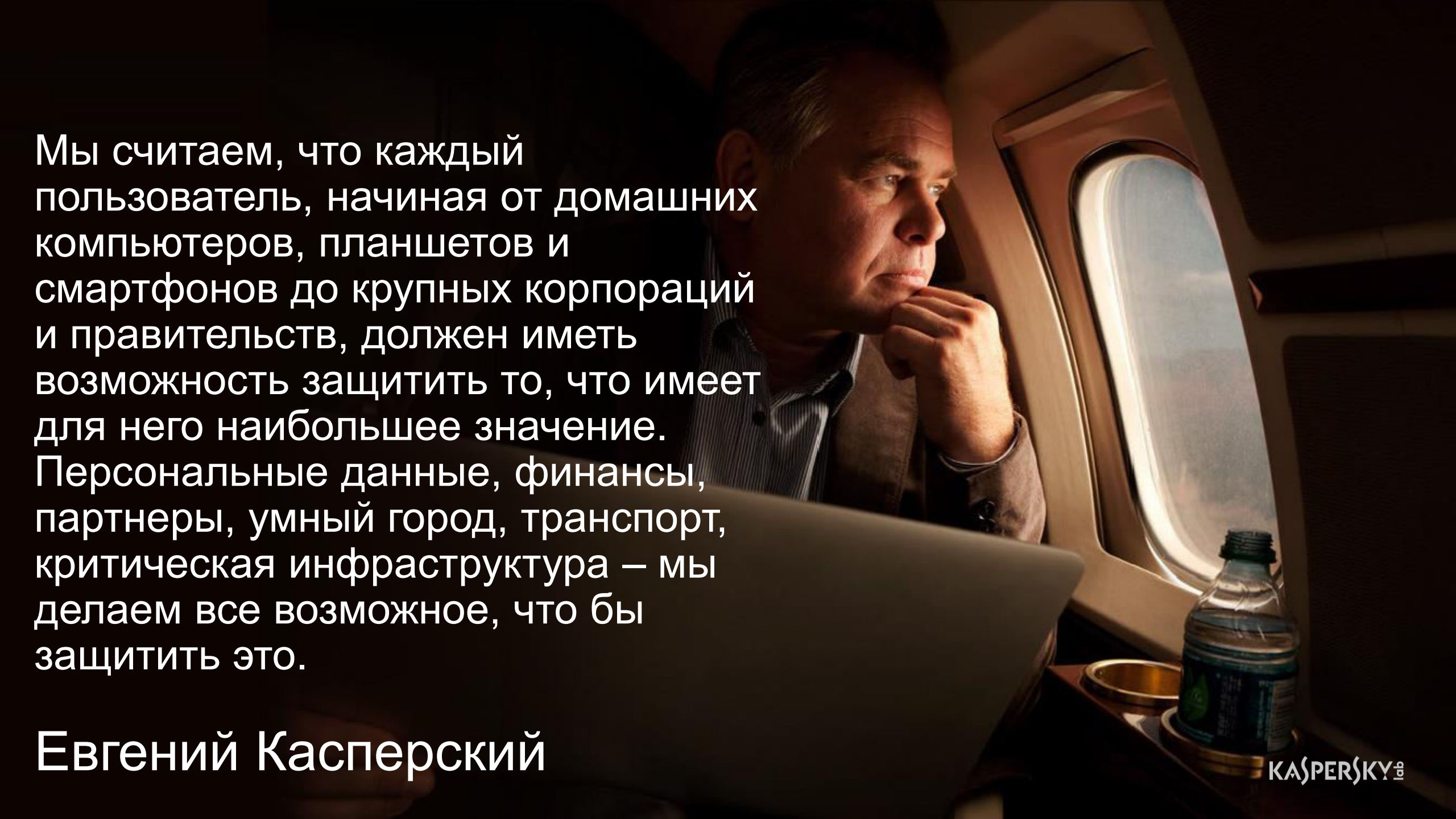
Андрей Духвалов,

Руководитель Департамента Перспективных Технологий

Лаборатория Касперского

ТБ Форум, Москва

14 февраля 2018

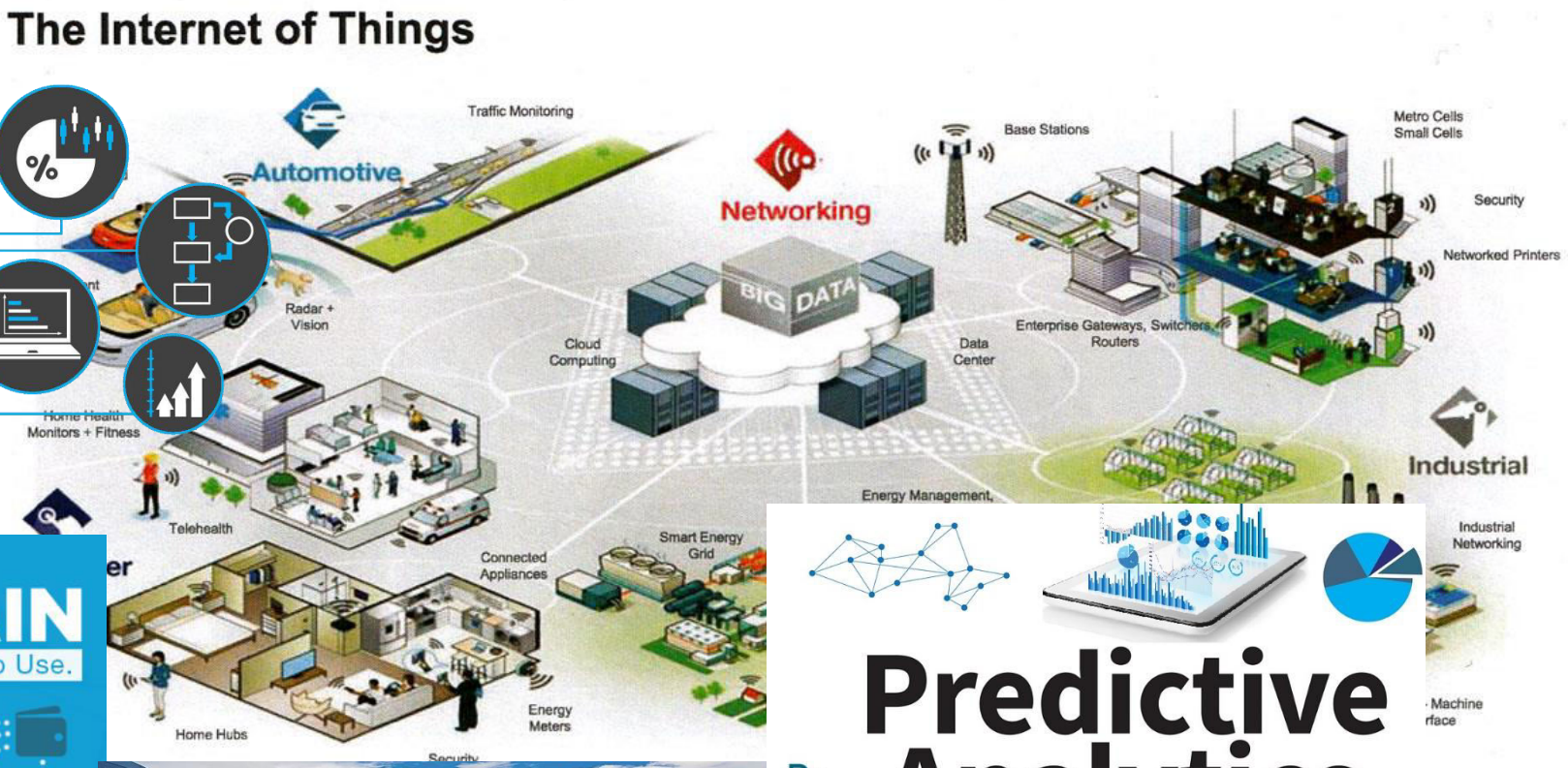


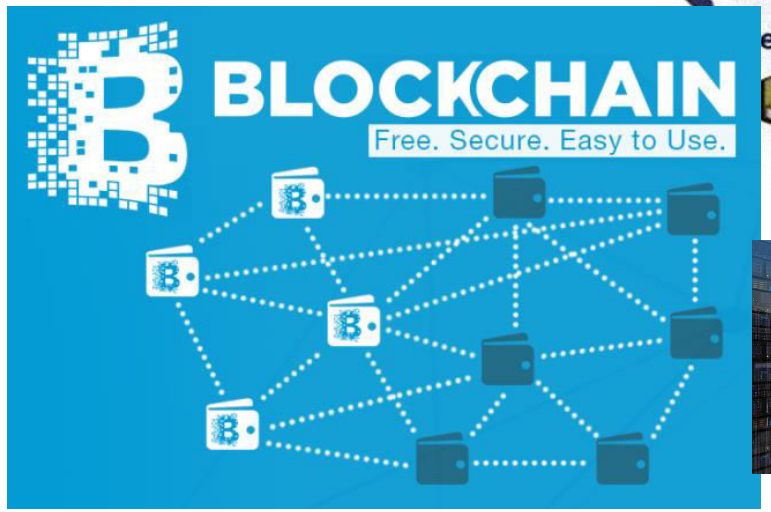
Мы считаем, что каждый пользователь, начиная от домашних компьютеров, планшетов и смартфонов до крупных корпораций и правительств, должен иметь возможность защитить то, что имеет для него наибольшее значение. Персональные данные, финансы, партнеры, умный город, транспорт, критическая инфраструктура – мы делаем все возможное, что бы защитить это.

Евгений Касперский

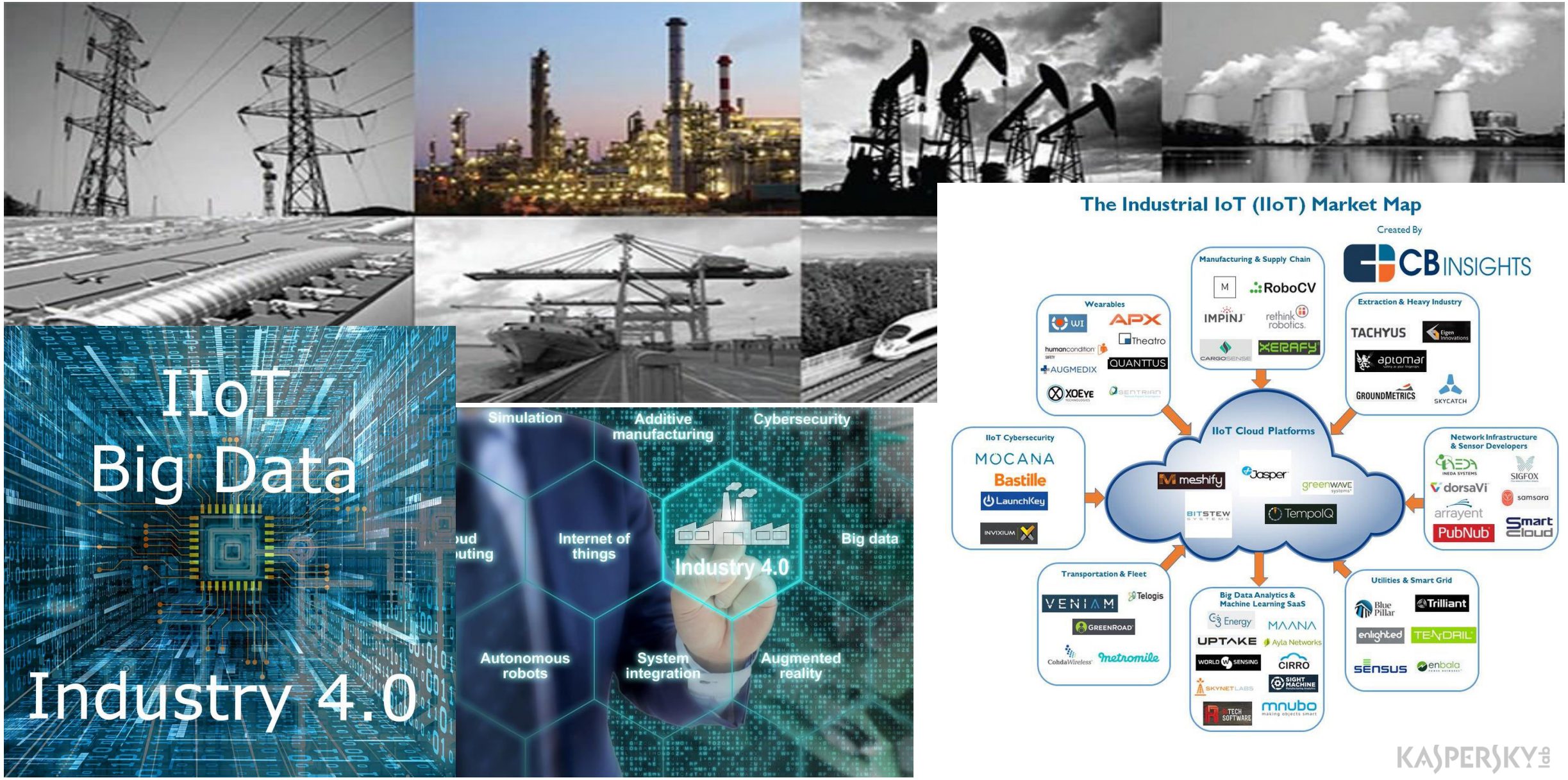
KASPERSKY lab

Сложность современных информационных технологий

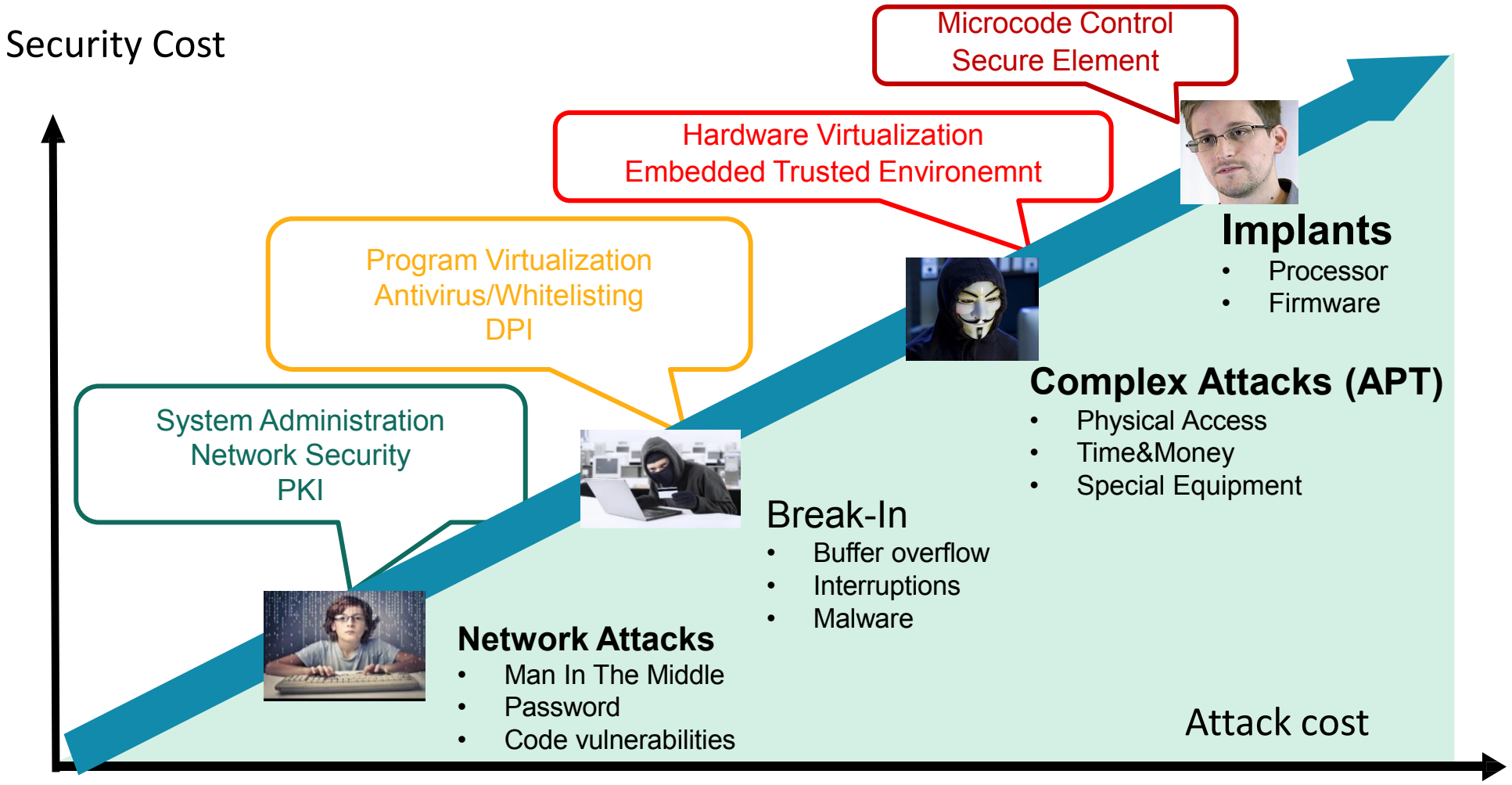




Компании всего мира вносят вклад в развитие



Сколько секьюрити нам нужно?



Мы находимся в процессе борьбы за контроль над безопасностью

KASPERSKY lab

НОВЫЙ КЛАСС «УМНЫХ» КИБЕРФИЗИЧЕСКИХ СИСТЕМ

- *Инженерные комплексы на основе Интернета Вещей, объединяющие человеческие, физические и информационные ресурсы в рамках «Умных Систем»*

- Безопасность становится все более комплексной дисциплиной. Угрозы кибербезопасности могут иметь последствия в физическом мире, ставя под вопрос жизнь и здоровье людей

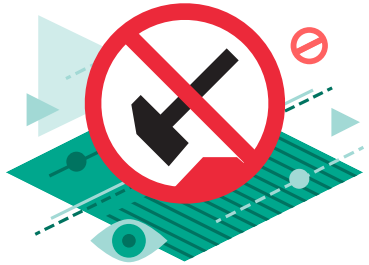
KASPERSKY lab

Основная цель

Обеспечить возможность построения доверенной системы из не доверенных компонентов

Вредоносное не доверенное содержащее не документированную функциональность

Доверенное приложение, возможно содержащее уязвимости



Приложение с не документированным или вредоносное поведением

Общепринятый подход

Прямые взаимодействия между компонентами сложной системы

Два основных принципа:

1. Изоляция доменов безопасности

Два основных принципа

1. Изоляция доменов безопасности

Separation Kernel (SK)

Ядро изоляции

Два основных принципа:

1. Изоляция доменов безопасности

2. Две фазы принятия решения
   - вычисление секьюрити вердикта
   - и его применения

Разделены на два независимых пространства

Separation Kernel (SK)

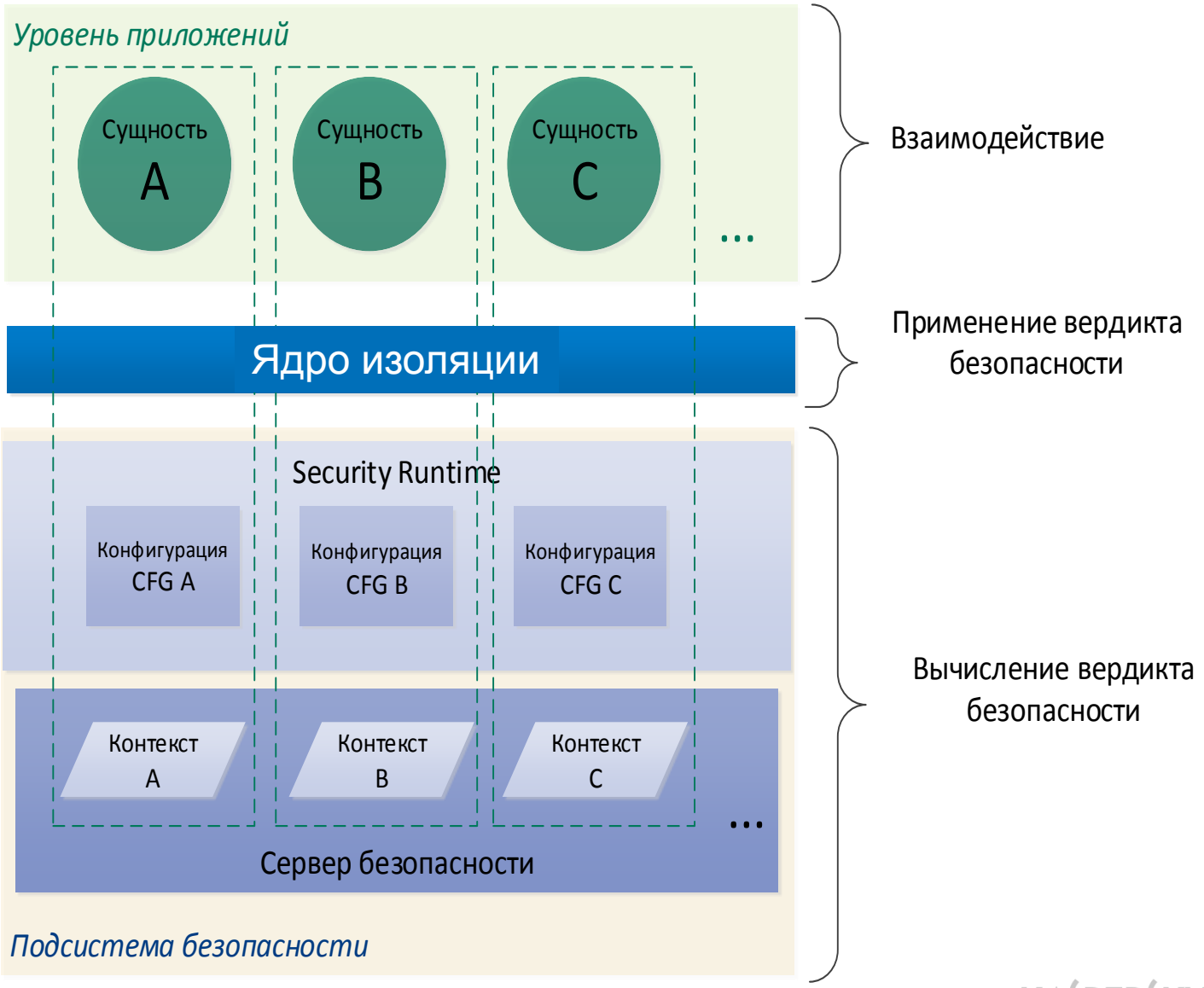
Ядро изоляции

Security Verdict Engine (SVE)

KASPERSKY lab

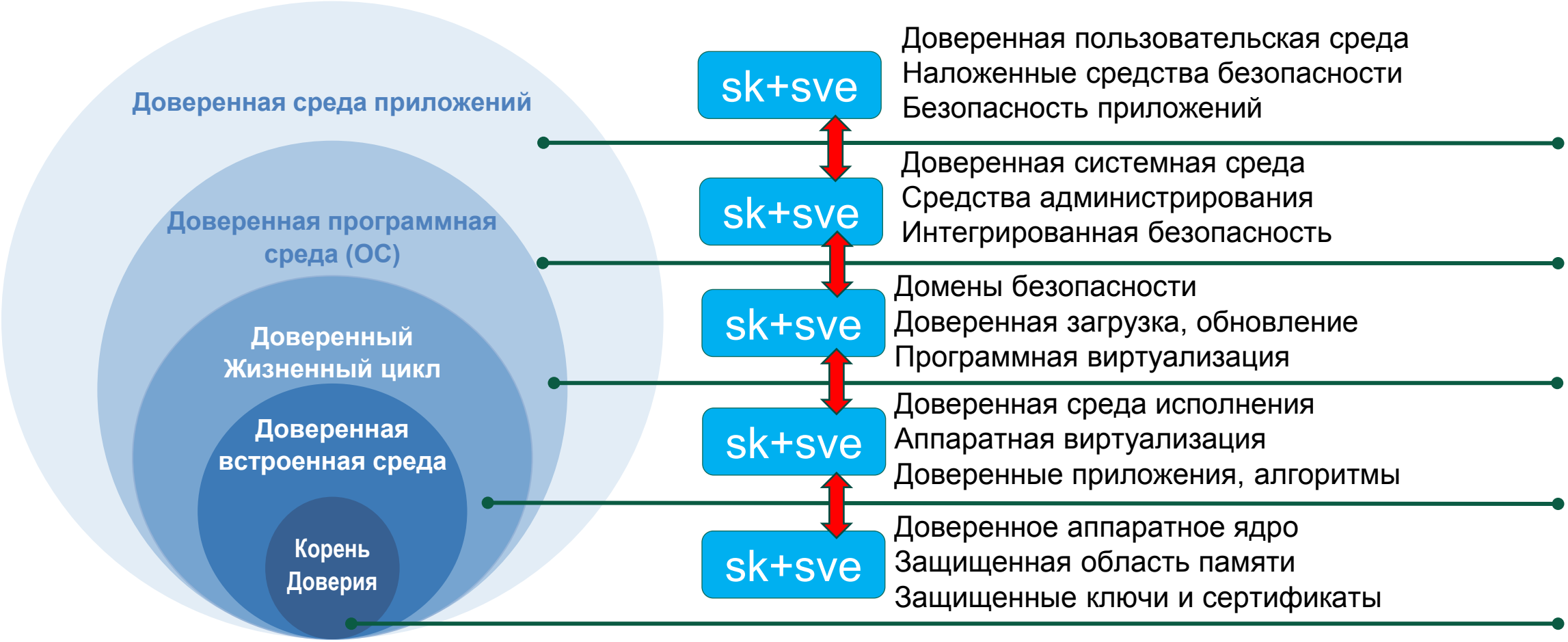
Kaspersky Security System

- Модуль расчета вердикта безопасности
- Отделение бизнес логики ПО от функций кибер безопасности
- Политики «знают» о структуре и контексте взаимодействий Комбинирование политик на уровне конфигураций
- Статический анализ и генерация кода по спецификации
- Работает как валидатор функциональной части ПО Может выступать как IDS
- Отделяема и легко переносима



ФОРМИРОВАНИЕ ДОВЕРЕННОЙ СРЕДЫ

- *На каждом уровне системы есть свои методики и механизмы повышения уровня доверия (пример - ГОСТ Р 56939-2016 *)*



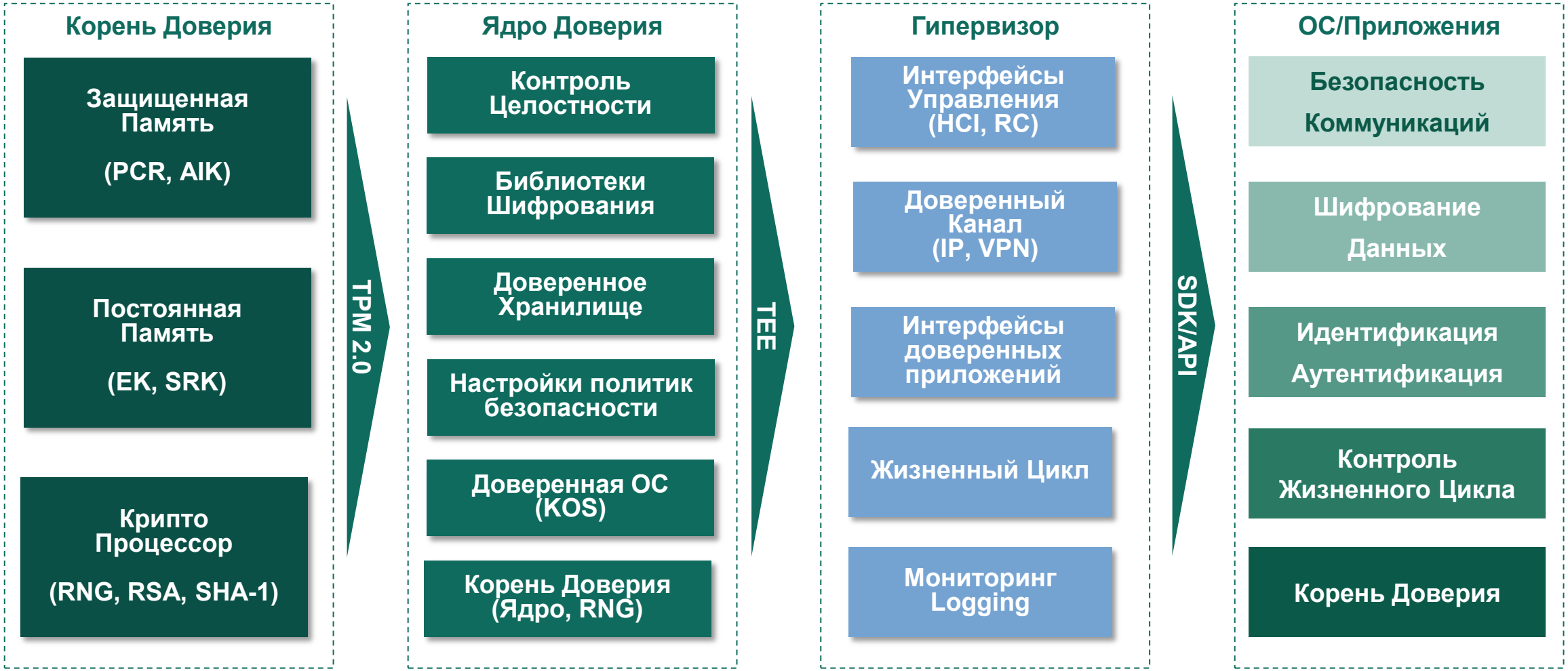
- Необходимо поддерживать доверие как внутри так и между уровнями системы

(*) «Защита информации. Разработка безопасного программного обеспечения. Общие требования»

KASPERSKY lab

Состав приложений и интерфейсов

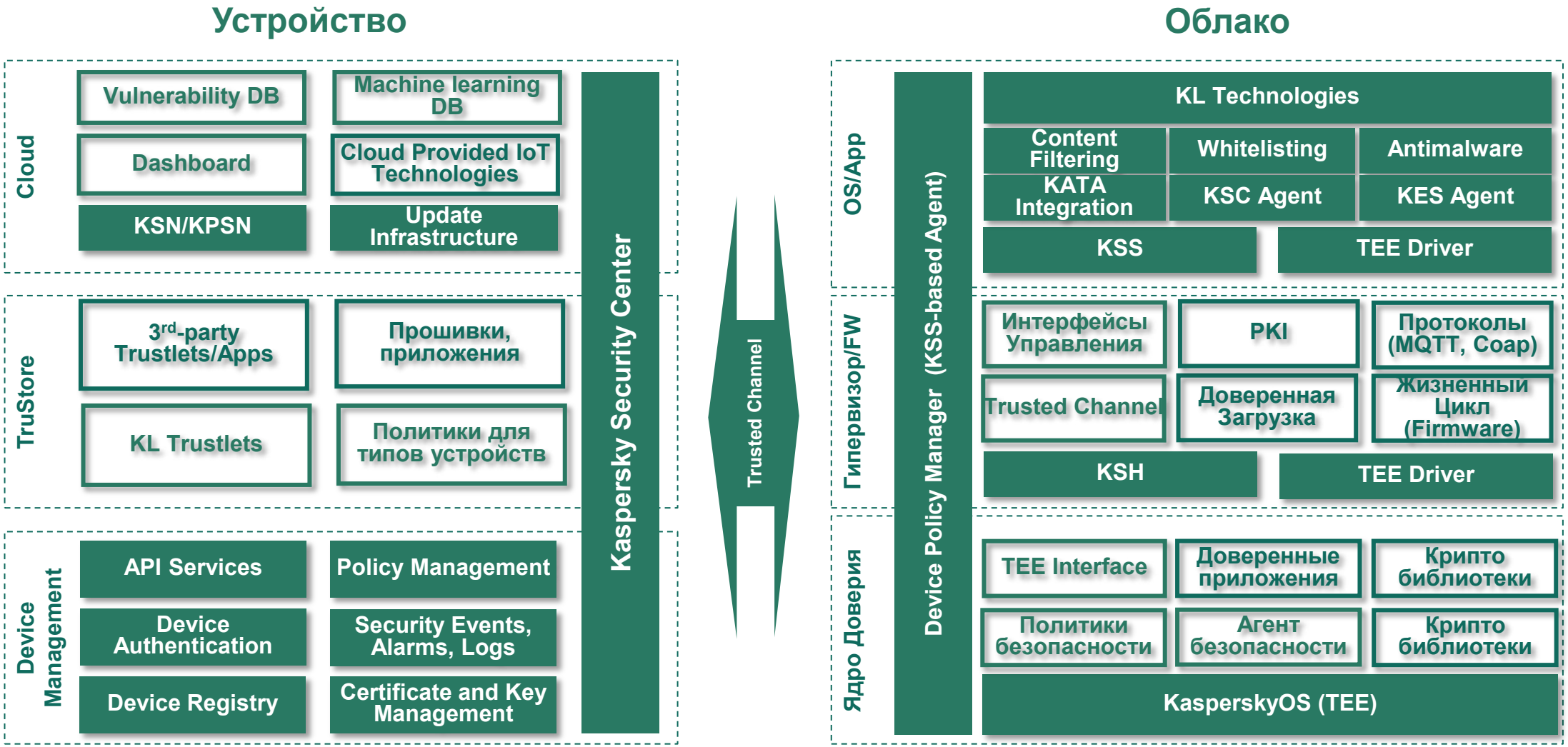
- *Реализация ключевых модулей на основе российских технологий и международных стандартов*



KASPERSKY lab

МНОГОУРОВНЕВАЯ ЗАЩИТА – ИСПОЛЬЗУЕМ МАКСИМУМ ТЕХНОЛОГИЙ

Экосистема подразумевает использование всех наработанных технологий



KASPERSKY lab

Экосистема

- *Партнерство лидеров индустрии и поддержка со стороны государственных программ*

Институты Инноваций

Регуляторы

ФОИВы

Программы

ФОИВы, Регуляторы и Институты Инновационного Развития

Международные Стандарты

Рынок/отрасль/партнеры

Центры ресурсов

Кадры

Методология

Компетенции

Вопросы?

Андрей Духвалов
Руководитель Департамента Перспективных Технологий
Andrey.Doukhvalov@kaspersky.com
www.kaspersky.com

ТБ Форум, Москва

14 февраля 2018

KASPERSKY lab