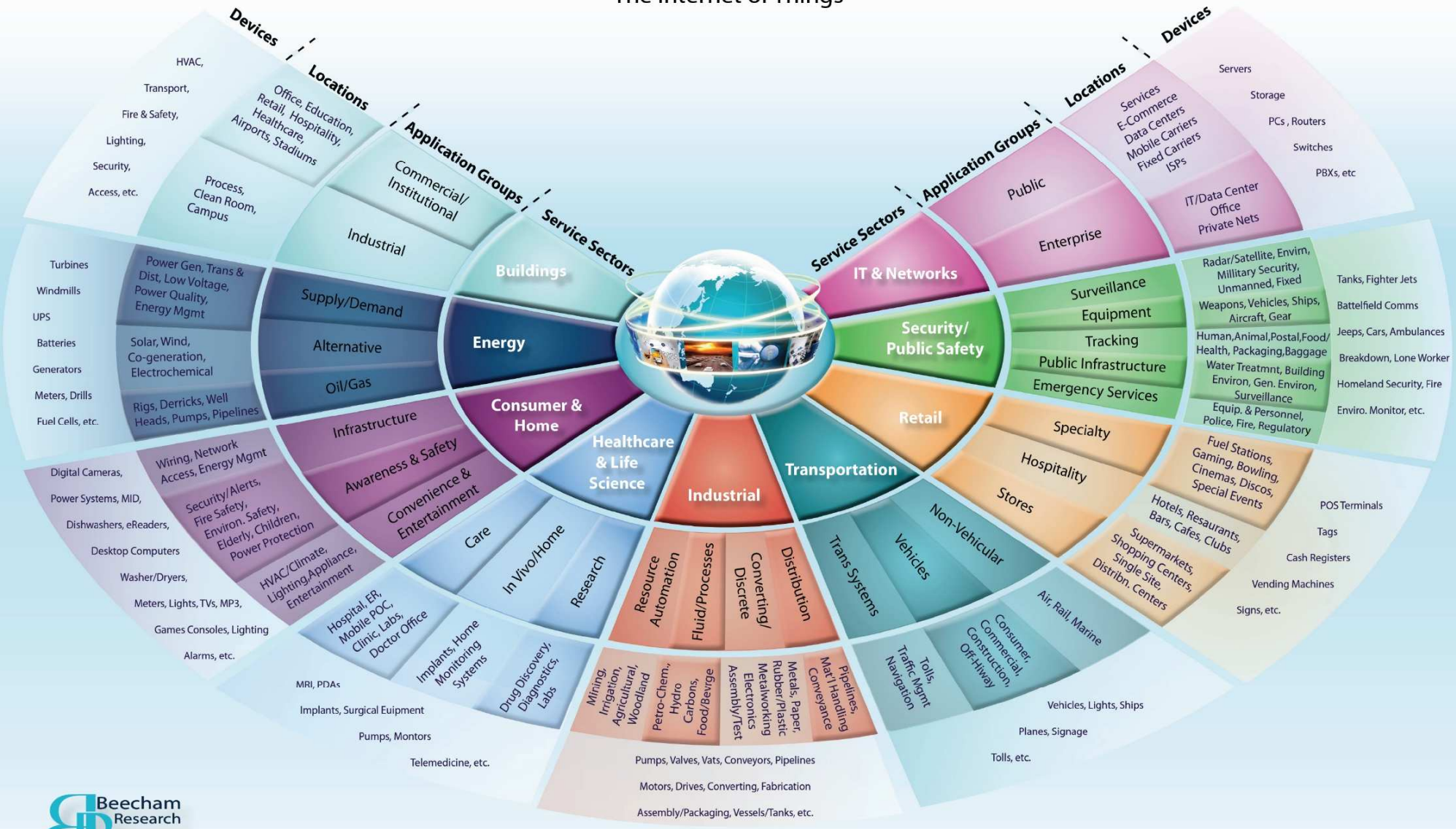
# Безопасность Интернета Вещей

# M2M World of Connected Services

## The Internet of Things





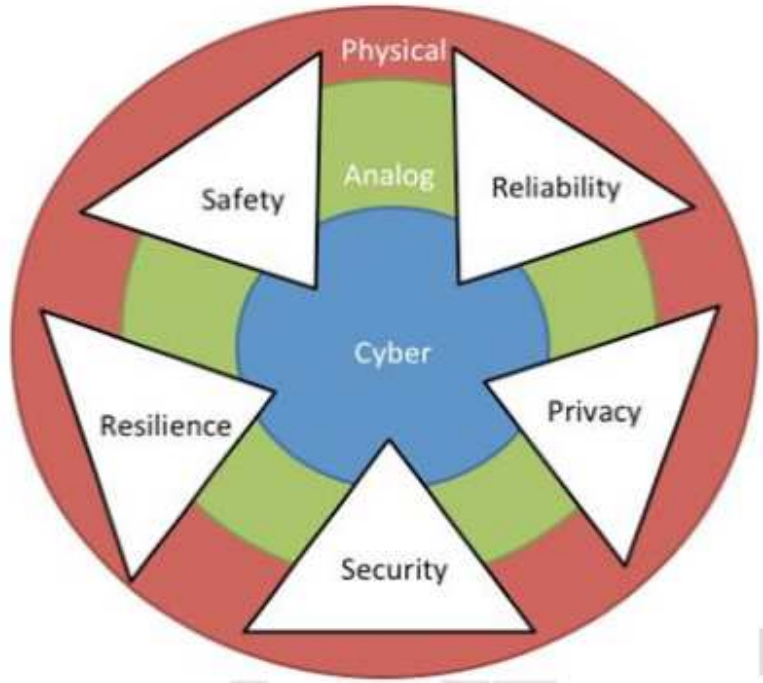
Beecham Research

Boston | London

info@beechamresearch.com +44 (0)845 533 1758 www.beechamresearch.com

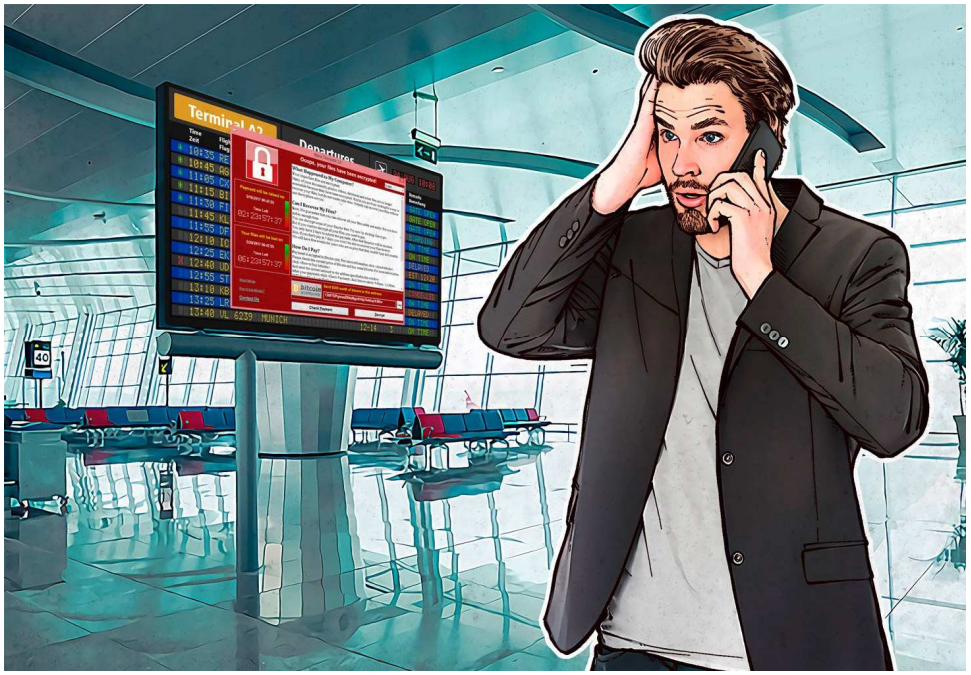
# «Умные» киберфизические системы – новый класс инженерных систем

- *Конвергенция Физических и Кибернетических систем требует нового понимания безопасности*




- *При строительстве сложных киберфизических систем необходимо учитывать риски безопасности (операционные, репутационные), сохранности (ошибки), надежности (выход из строя), приватность (утечки) и устойчивости (восстановление)*

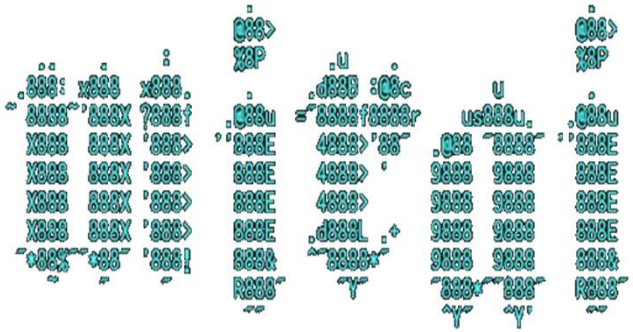

Ooops, your important files are
u see this text, but don't see the "Wan
your antivirus removed the decrypt soft
om your computer.
u need your files you have to run the d
find an application file named "@Wana
older or restore from the antivirus qua
BOARDWAY
ถ.วิทยุ
Witthayu Rd.


Departures

# Вредоносное ПО для IoT в действии

**Remaiten** это вредоносное ПО, которое инфицирует Линукс на встроенных системах путем лобового перебора имен и паролей пользователей

**Linux.Darlloz** это червь, инфицирующий устройства Интренета Вещей – маршрутизаторы, камеры видеонаблюдения, STB, построенные на основе встроенного Линукса, путем атаки на уязвимости PHP



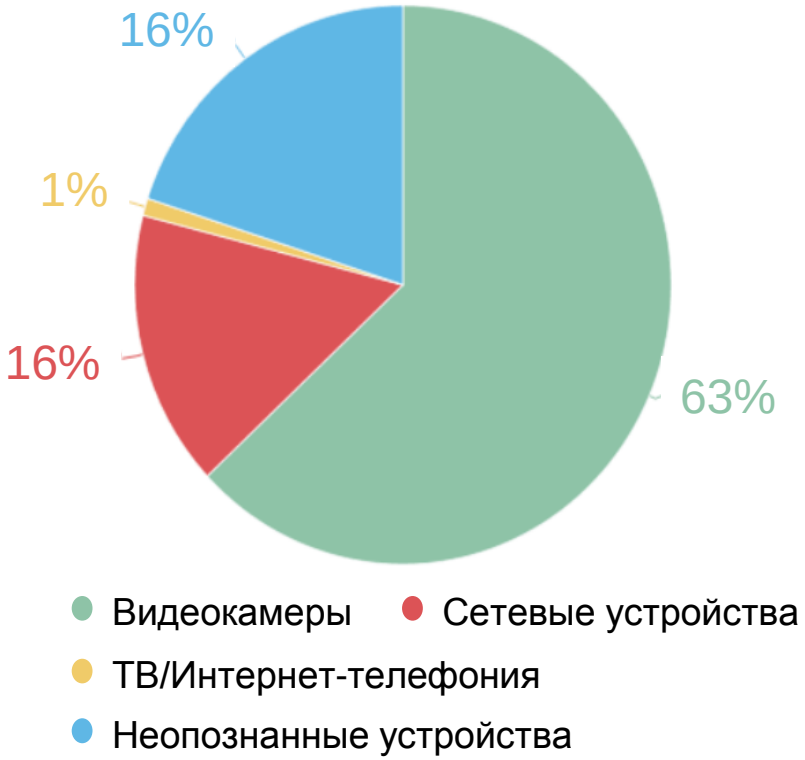
**Mirai** является наиболее известным BotNet-ом, поразившим 900 тыс заказчиков Deutsche Telekom и 2400 домашних роутеров в Англии

В 2016 1 миллион устройств был инфицирован вредоносным ПО **BASHLITE.**

96 % являются IoT-устройствами (камеры, DVR)

4% - домашние роутеры

1% - скомпроментированные Линукс-серверы



# Ландшафт Безопасности IoT

- *Для обеспечения безопасности необходимы все компоненты*


**Edge** ⟷ **Gateways / Smart Devices** ⟷ **Network** ⟷ **DataCenter/ Cloud**

- Authentication (verified)
- Service discovery / provisioning / pairing
- Trusted execution environment
- Network security / firewall
- Secure Boot

**IoT Device Security**

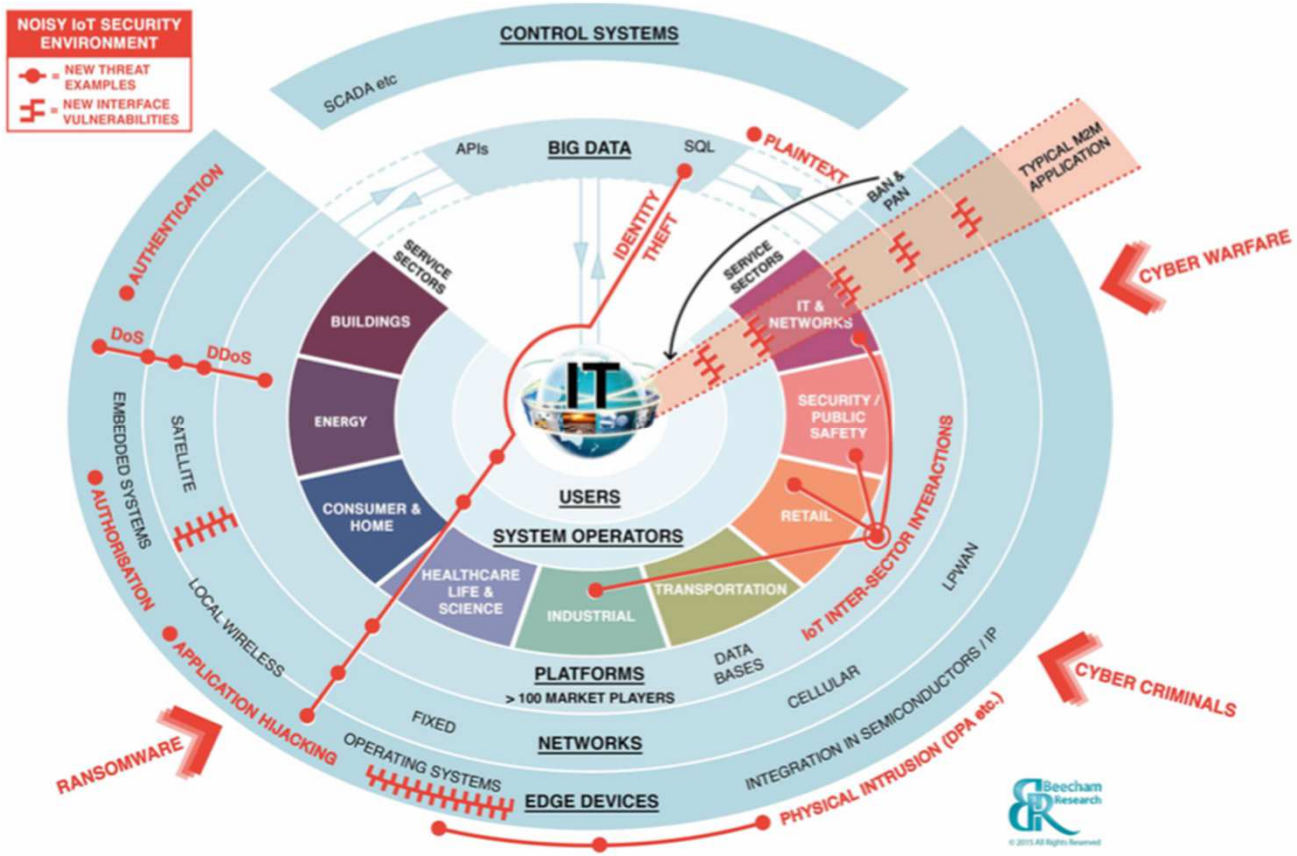
- Authentication (verified)
- Encryption
- Message integrity
- MitM protection
- DNS spoofing protection

**Communication Security**

Authentication (verified)
- PKI / certificate management
- Trusted execution environment
- Network security / firewall
- Access control (role based)

**Cloud Security**

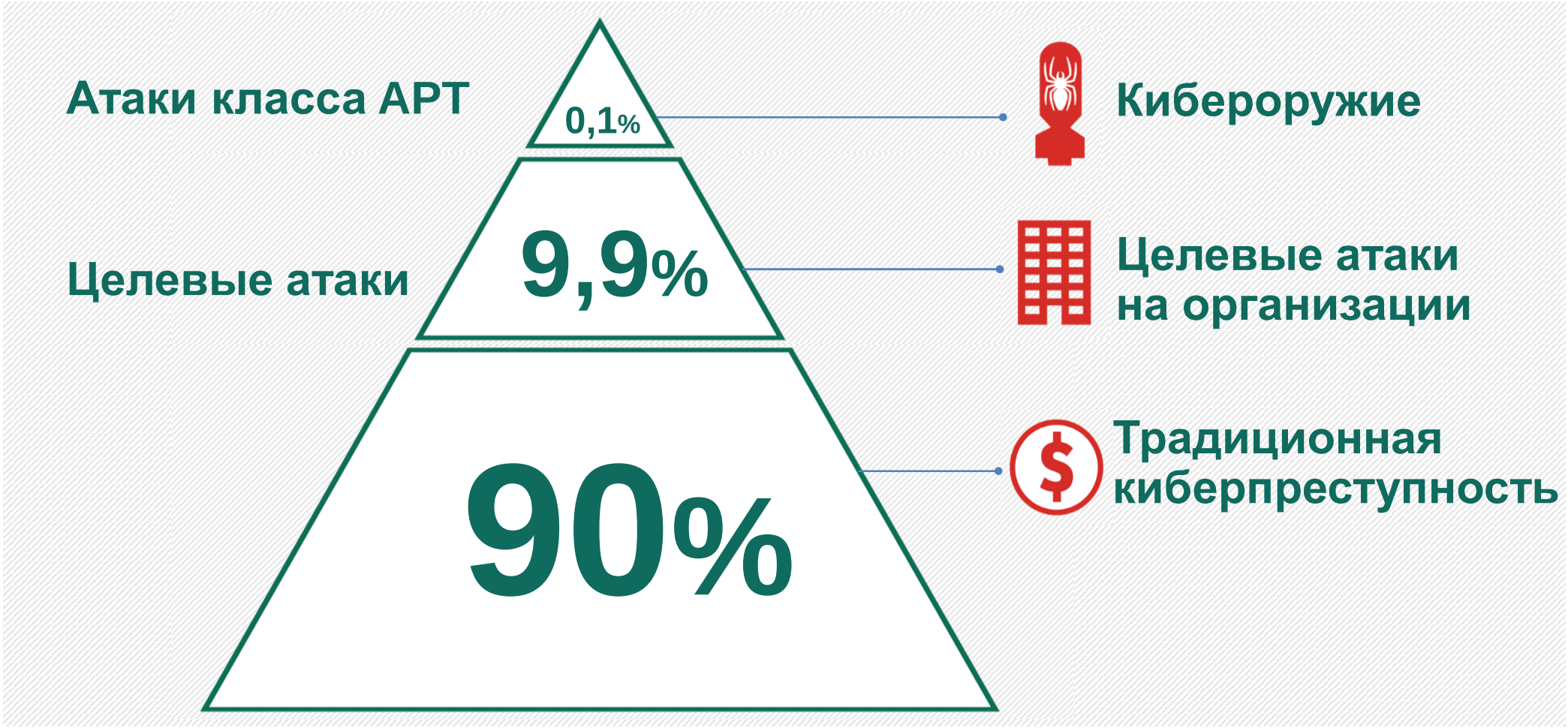
# Карта угроз Интернета Вещей




- Регламенты
- Уязвимости приложений
- Уязвимости интерфейсов
- Уязвимости Авторизации
- Уязвимости Библиотек
- Уязвимости ОС
- Уязвимости Firmware
- Закладки в Firmware
- Закладки в процессорах

# Угрозы кибербезопасности

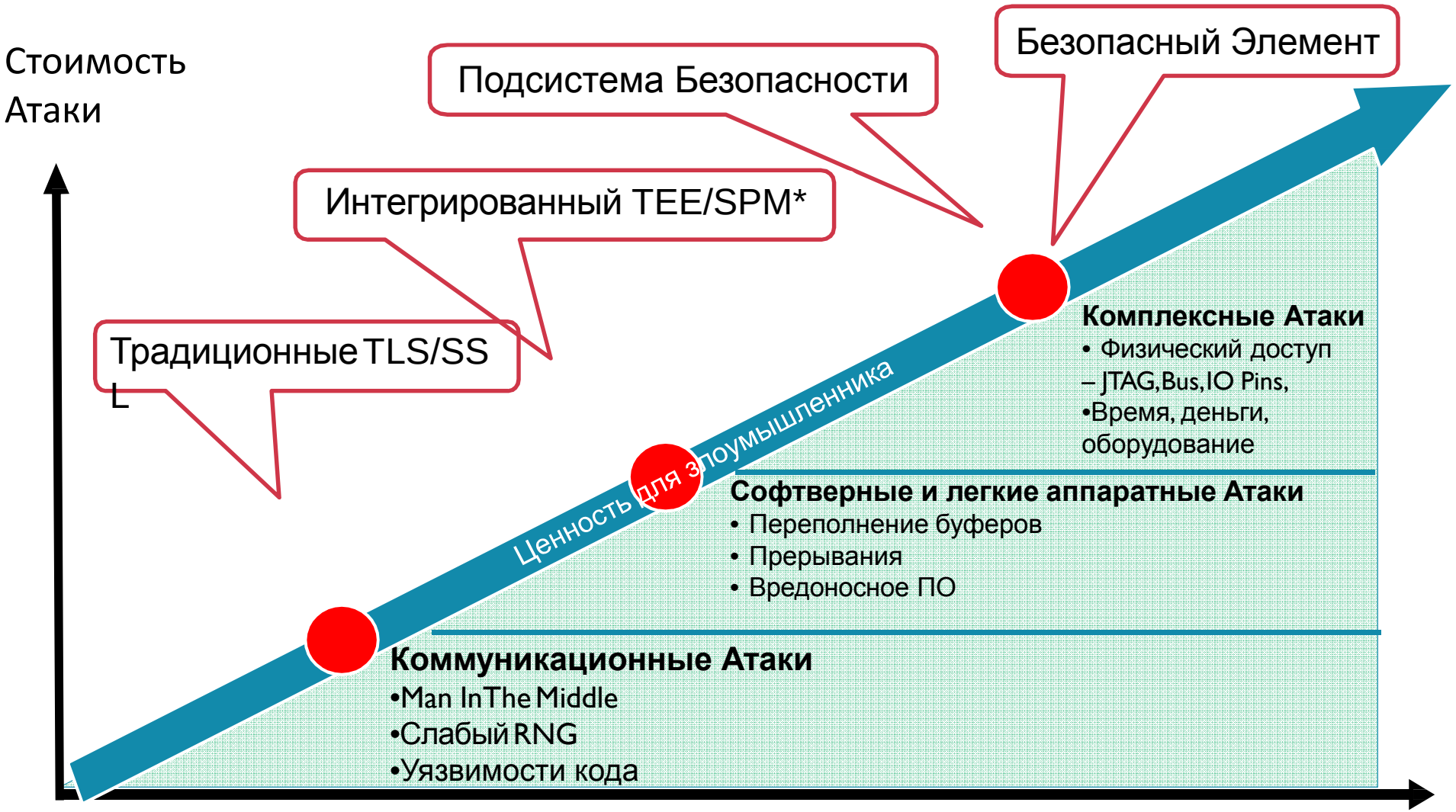
- *Киберпреступность – это индустрия…*






8

# Сколько безопасности реально необходимо ?

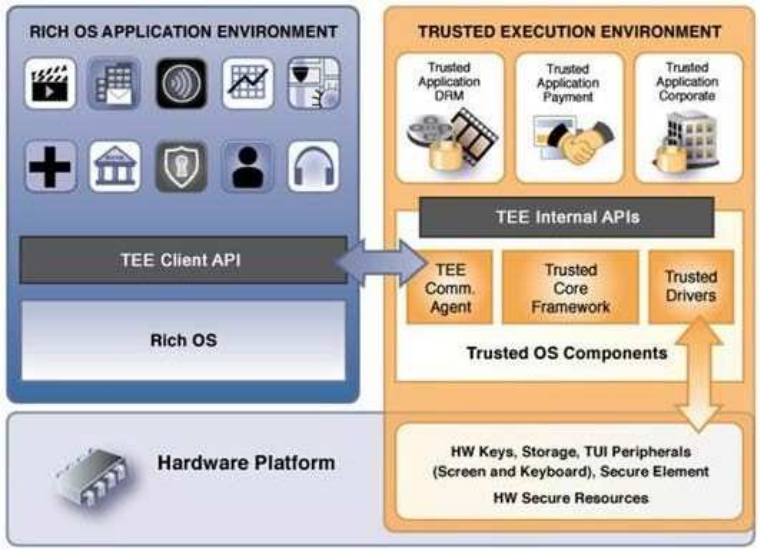



*Trusted Execution Environment / Secure PartitioningManager

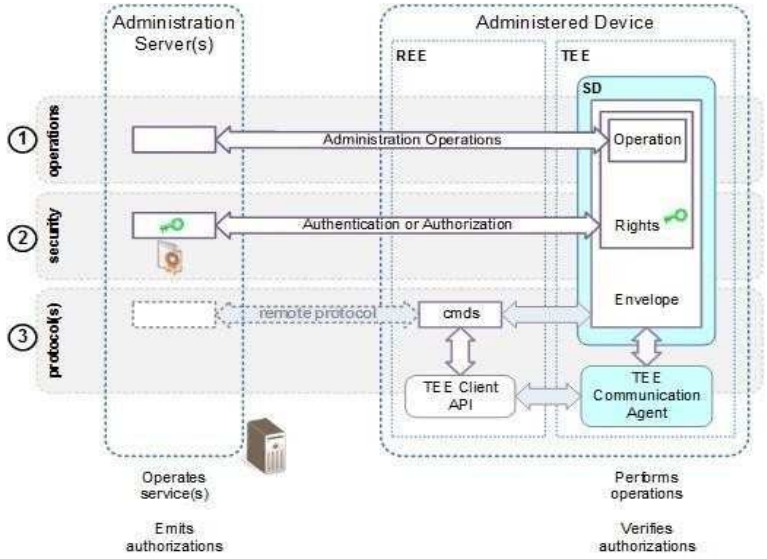
# Пример – GlobalPlatform Trusted Execution Environment

- *Trusted Execution Environment стала стандартом мобильной безопасности*


## Реализация Доверенной Среды

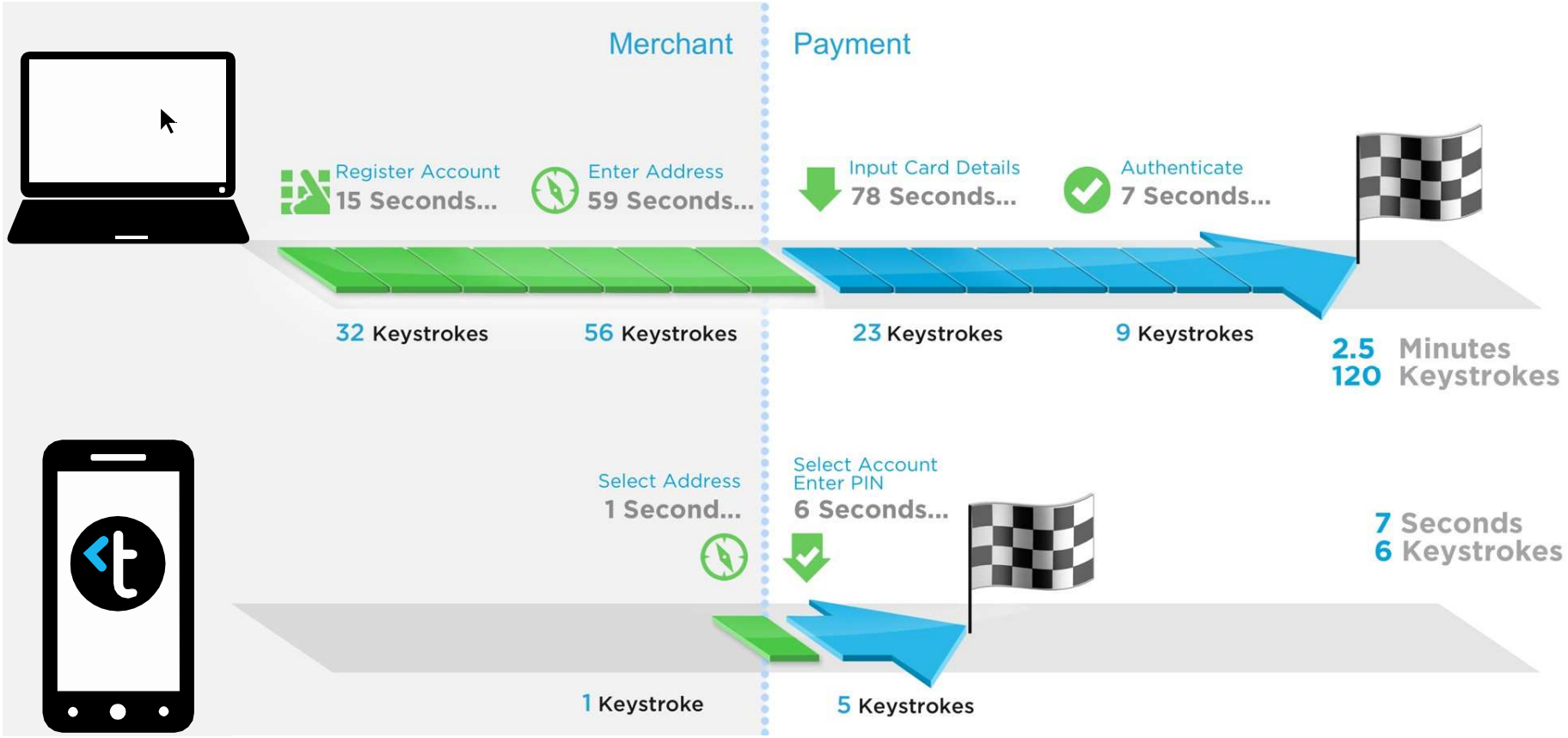



## Управление Доверенной Средой



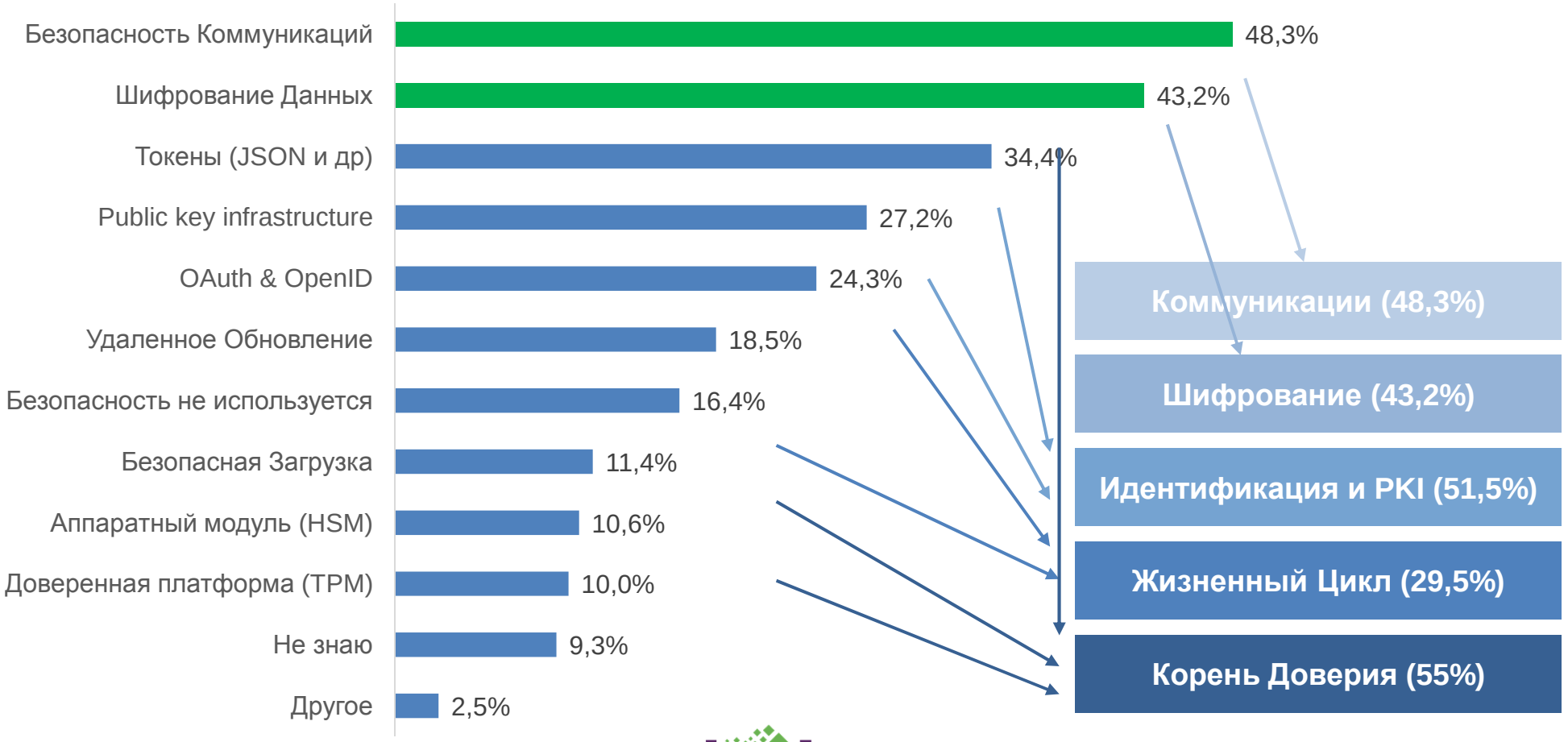
# Интегрированная безопасность в действии

- *Со времени основания в 2012 году компания Trustonic достигла инсталлированной базы в 1 миллиард устройств*



# Технологии Безопасности Интернета Вещей

- *Разработчики систем IoT определили основные области проблем безопасности*



# Безопасность IoT должна быть интегрированной


## Ситуация

Большая часть IoT-разработчиков не являются экспертами в безопасности

Минимальные знания аппаратной платформы

Некоторый опыт в разработке мобильных приложений

Безопасностью жертвуют в пользу функциональности и сроков

## Стратегия

Простота требований и инструментария IoT Платформы

«Прятать» сложность аппаратной безопасности

Обеспечить встроенные функции безопасности

Использовать стандартные методы и строительные блоки

# Российские технологии, Международные стандарты

- *Реализация интегрированной безопасности позволит повысить уровень доверия; гибко адаптируясь к существующей IoT-инфраструктуре*