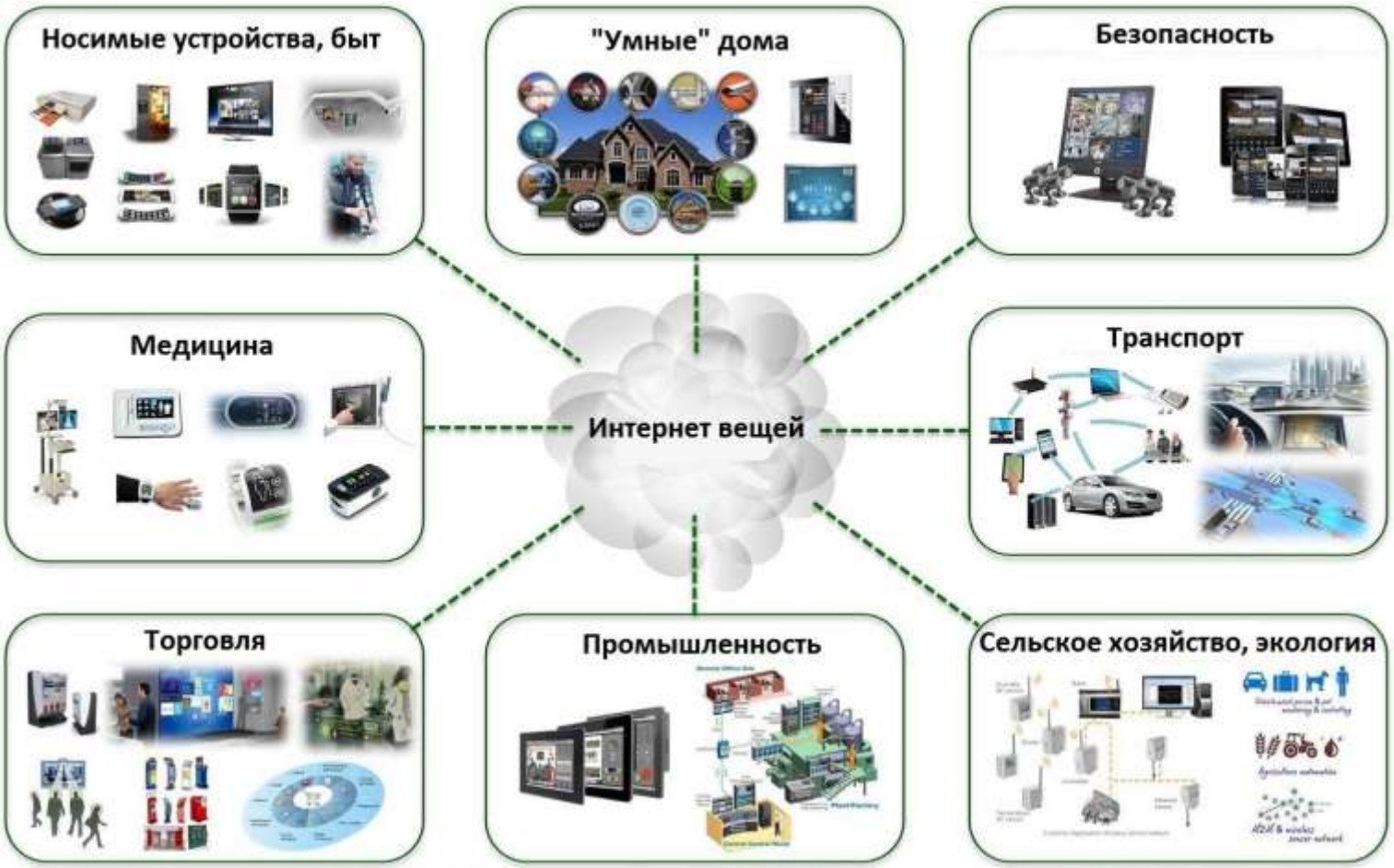
Информационная безопасность интернета вещей

Росинфоком-2016

От «Интернет людей» к «Интернету вещей»

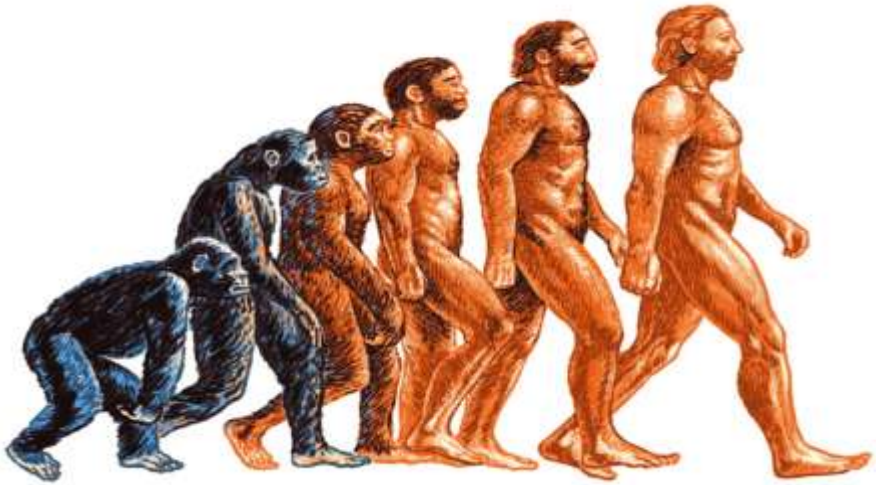
- Основной целью традиционного Интернета было обеспечение взаимодействие людей между собой через различные каналы коммуникаций
- Термин IoT впервые был сформулирован в 1999 году в Массачусетском университете
- Отсутствие единого определения IoT
- 2008-2009 фактическое рождение IoT – количество подключенных к Интернетут вещей превысило число подключенных людей: 1,84 устройства на душу населения
- «Интернет людей» трансформировался и продолжает трансформироваться в «Интернет-вещей»

Применение интернета вещей



Новые проблемы ИБ

- Развитие IoT – шаг на следующий ступень развития общества (аналогично изобретению электричества, появления Интернета и т.д.)
- Изменение человеческого общества



Новые задачи в области обеспечения безопасности личности и общества!

Инфраструктура интернета вещей

- Датчики и сенсоры со специализированными ОС (Windows 10, Tizen, RIOT, Lite OS, Contiki, Raspbian и т.д.)
- IoT-платформы, позволяющие подключать и управлять удаленными устройствами (SAP HANA (SAP), ThingsWorx (PTS), iMotion Edgeware (Fujitsu) и др.)
- Адаптированные протоколы взаимодействия датчиков (Thread, MQTT, AMQP, DDS и др.)

Особенность ИБ IoT

- Масштаб угроз

  Атаки на информационные системы город, транспортных систем, системы здравоохранения и т.д.

- Новые виды угроз

  Принципиально новый класс угроз, характерных только для IoT. Например, угон беспилотного автомобиля и т.д.

Технические аспекты

Объекты для атак:

- Датчики, сенсоры и другие объекты IoT
- Перехват протоколов
- Системы управления инфраструктурой IoT

Отдельные угрозы могут быть ликвидированы стандартными средствами защиты (шифрование канала связи, аутентификация и т.д.), но для самых серьезных угроз требуются специфические средства и механизмы защиты.

Технологические решения по обеспечению ИБ

- В настоящее время ряд вендоров (Cisco, Huawei, SAP и т.д.) предлагают свои концепции и решения для обеспечения безопасности инфраструктуры IoT
- «IoT Security Foundation» - международная ассоциация по разработки информационной безопасности IoT
- Вопросы сертификации решений IoT в области информационной безопасности

Правовые аспекты

Необходимость законодательного регулирования:

- Ответственность за получения доступа к объекту IoT

Незаконное управление беспилотным автомобилем.

- Гражданская ответственность за неправомерное представление доступа к объекту IoT

Непринятие мер для защиты объекта IoT.

Получение лицензий на использование объектов IoT.

- Своевременность принятия законодательных актов

Опыт работы с социальными сетями и интернет-мессенджарами (Skype, Viber, WhatsApp)

СПАСИБО ЗА ВНИМАНИЕ!