Защита информации 2030: к чему готовиться уже сейчас?

Алексей Лукацкий, бизнес-консультант по безопасности, Cisco

С ЧЕМ МЫ СТАЛКИВАЕМСЯ УЖЕ СЕЙЧАС?

Ведомственная роботизация уже сегодня

- Робот-Telepresence позволяет организовать дистанционное общение в условиях экономии на персональных системах Telepresence
- Новые условия для ИБ – динамичность, мультимедиа, многопользовательность, отсутствие выраженного владельца

Морская платформа подключена к Интернету вещей

Управление активами

Охрана труда

Взаимодействие на платформе / буровой

Управление инцидентами

Удаленные эксперты

Удаленные операции

Контроль процессов

Индустриальное взаимодействие

Безопасность

Здоровье

Взаимодействие экспертов

Мобильность

Множество устройств

Отдых

Взаимодействие с руководством

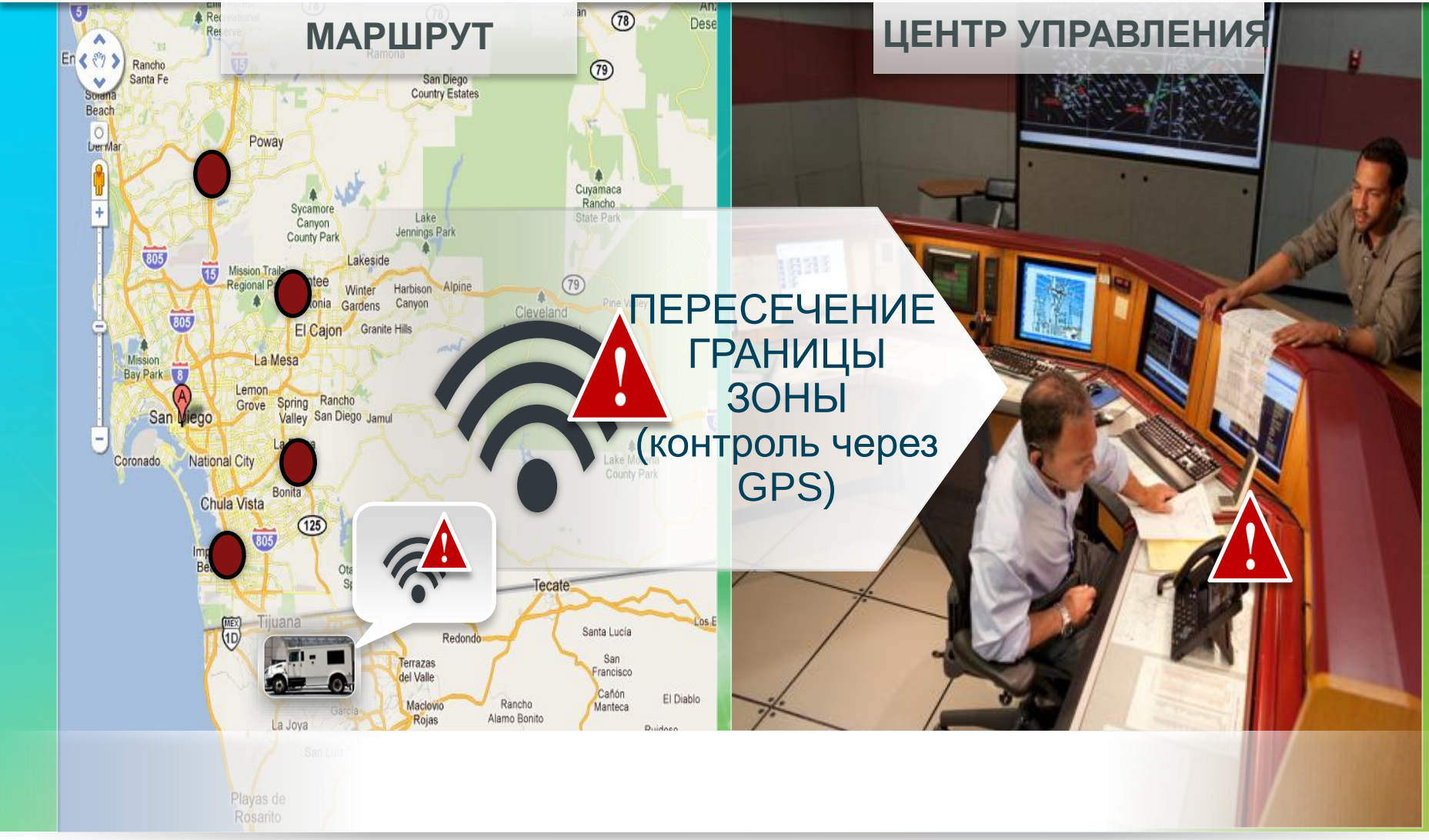
Быстрое реагирование

Сенсоры

Обучение / Распределение лучших практик

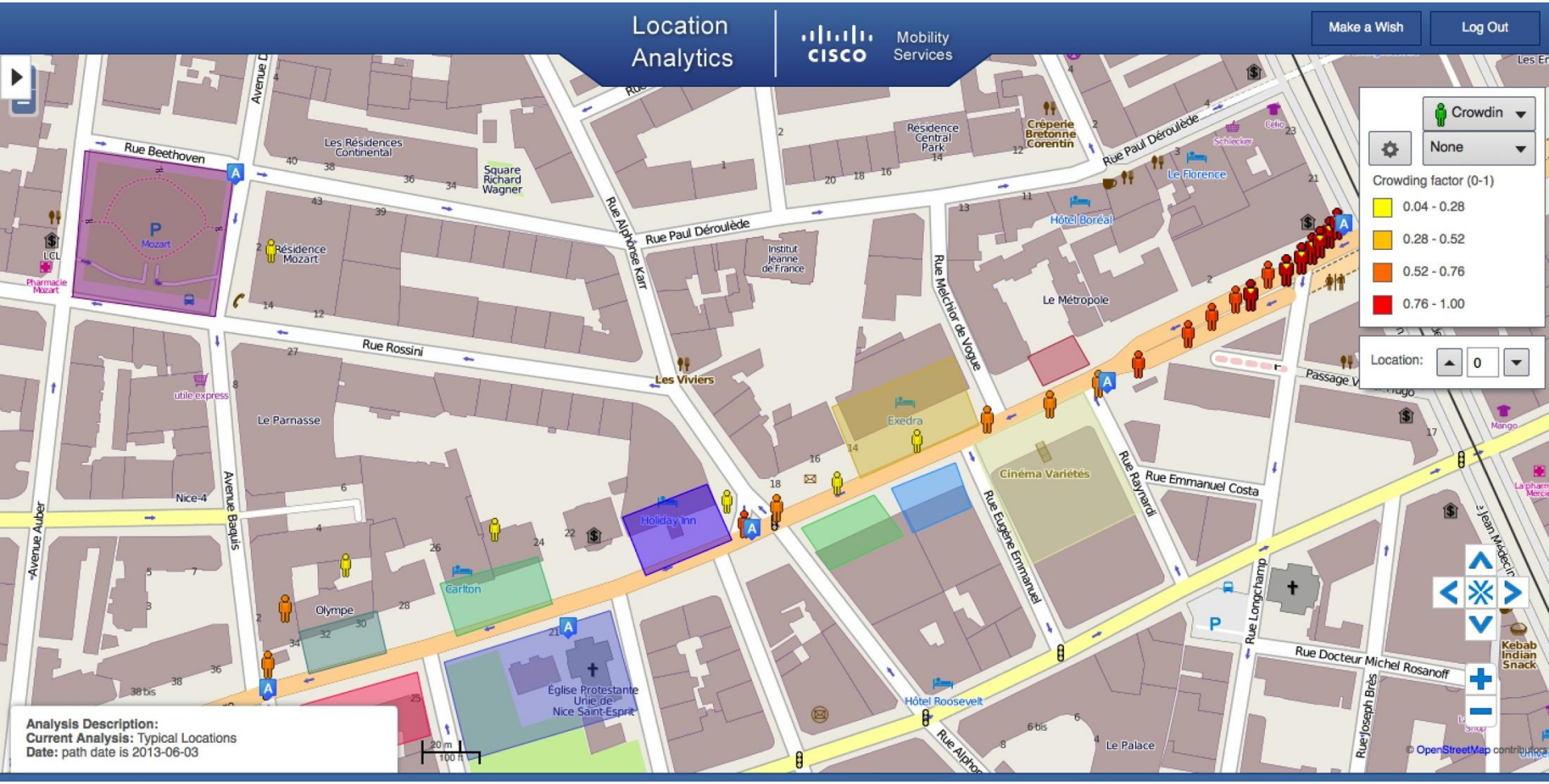
Enterprise Wide Connectivity

Контроль перемещения грузов и передвижения мобильных групп



Видеоконтроль перемещающегося объекта

«Подключенный бульвар» в Ницце



«Умные» автомобили

- «Умное» управление движением автомобилей
  - Выстраивание маршрутов
- Контроль состояния автомобиля
- Информация об использовании и расчеты за услуги
- ИБ практически отсутствует

Подключенный к IoT автомобиль

С ЧЕМ МЫ СТОЛКНЕМСЯ В СРЕДНЕСРОЧНОЙ ПЕРСПЕКТИВЕ?

Куда идет ИБ в среднесрочной перспективе?

- A Roadmap for Cybersecurity Research от US DHS

  11 направлений исследований

- National Cyber Leap Year

  Инициатива по сбору проблем, стоящих перед отраслью ИБ, и способов и идей их решения

  В рамках программы Federal Networking and Information Technology Research and Development

Scalable trustworthy systems

- Масштабируемые системы, вызывающие доверие
- Trustworthy – это
  - Целостность
  - Доступность
  - Конфиденциальность
  - Жизнеспособность (живучесть)
  - Гарантированная производительность
  - Подотчетность
  - Удобство использования
- Это не просто АС в защищенном исполнении

Метрики ИБ уровня предприятия

1. Уровень опасности или сколько мы потеряем?
2. Сколько денег на ИБ достаточно?
3. Мы достигли цели?
4. Насколько оптимально мы движемся к цели?
5. Сколько стоит информация?
6. Насколько мы соответствуем стандартам или требованиям?
7. Какая из мер защиты выгоднее/лучше?
8. Как мы соотносимся с другими?
9. …

Жизненный цикл оценки систем

- Приемлем ли срок сертификации СКЗИ в 5 человеко/лет или срок сертификации СЗИ в 6-9 месяцев?

  За это время выйдет не одно обновление

- Можно ли в современных условиях очертить границы контролируемой зоны?
- Как оперативно оценивать динамично изменяемые системы с точки зрения информационной безопасности?

Живучесть критичных систем

- Живучесть – способность системы выполнять свою миссию в установленное время в условиях нападений, отказов и несчастных случаев

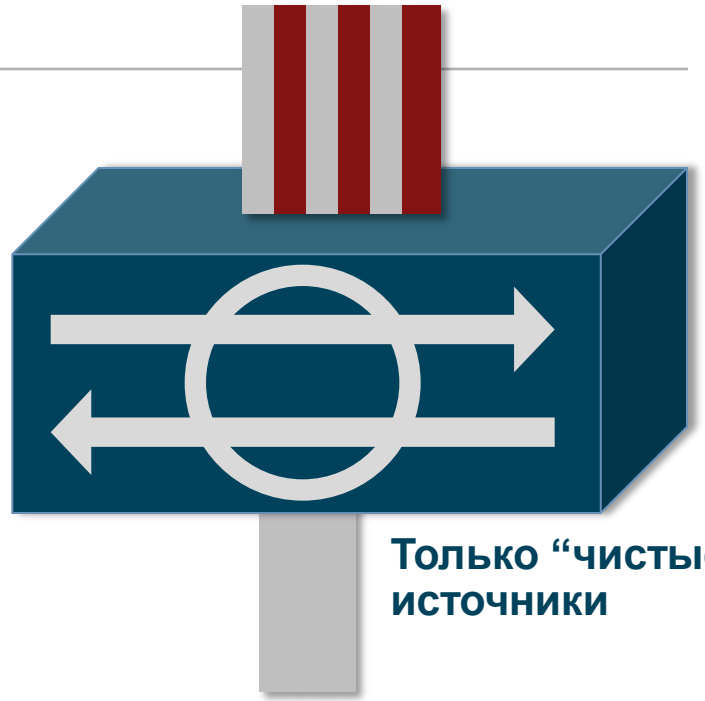
  Противоречит принципу “AS IS”

- ИТ проникает во все сферы жизни

  И особенно на критически важные объекты

Ситуационный анализ атак

	Что находит IPS	Вердикт: блокировать
Что?	Фрагменты SQL внутри веб-трафика	
Как?	Первое подключение HTTP	
Кто?	Динамический IP адресс Динамический DNS История веб-атак	
Откуда?	Из скомпрометированной азиатской сети Есть история ботнетовской активности	



Только “чистые” источники

- Оценка не только сигнатур, но и роли атакуемого и атакующего, окружающей среды, доступных ресурсов, мотивации и т.п.

Происхождение…

- Мы принимаем решения на основании информации, полученной в разное время из разных источников
  - Другой язык
  - Компиляция из разных источников
  - Неактуальные или недостоверные источники
  - Преднамеренная фальсификация
- Необходимо четко понимать происхождение информации, систем и аппаратуры
  - Закладки в оборудовании, купленном «по дешевке»

Удобство и безопасность

- Очень важно, чтобы интерфейс взаимодействия с пользователем был удобным в использовании; чтобы пользователи запросто и «на автомате» использовали механизмы защиты правильным образом. Если образ защиты в уме пользователя будут соответствовать тем механизмам, которые он использует на практике, то ошибки будут минимизированы. Если же пользователь должен переводить представляемый им образ на совершенно иной «язык», он обязательно будет делать ошибки

  Джером Зальтцер и Майкл Шредер, 1975 (!) год

Направления исследований NITRD

- Происхождение информации, систем и аппаратуры
- Динамическая безопасность

  Изменяющаяся система сложнее во взломе
- Аппаратное доверие

  Закладки в процессорах Intel, недоверенные среды
- Киберздоровье, вдохновленное природой

  Иммунная система – автоматизация реакции на аномальные явления в информационных системах
- Киберэкономика

  Как сделать преступления дорогостоящими и более рискованными при снижении нормы прибыли?

А что в России… было совсем недавно?

- Приоритетные направления научных исследований в области обеспечения ИБ РФ
- Основные направления научных исследований в области обеспечения ИБ РФ

  Проблемы нормативно-правового обеспечения безопасности информационных и телекоммуникационных систем

  Научно-технические проблемы использования информационных технологий в оперативно-розыскной деятельности

  И т.д.…
- Закрытость и неконкретность ;-(

С ЧЕМ МЫ СТОЛКНЕМСЯ В ДОЛГОСРОЧНОЙ ПЕРСПЕКТИВЕ?

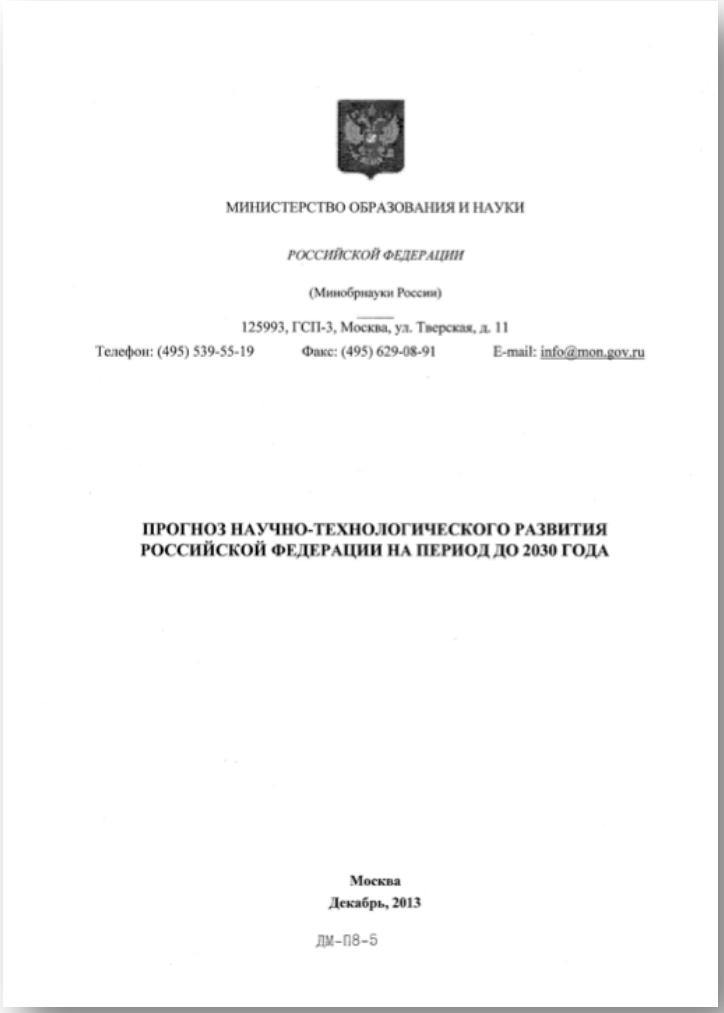
Долгосрочная перспектива

- Прогноз научно-технического развития РФ на период до 2030 года

  7 направлений

- О приоритетных научных задачах, для решения которых требуется задействовать возможности федеральных центров коллективного пользования научным оборудованием

  16 задач



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

РОССИЙСКОЙ ФЕДЕРАЦИИ

(Минобрнауки России)

125993, ГСП-3, Москва, ул. Тверская, д. 11

Телефон: (495) 539-55-19 Факс: (495) 629-08-91 E-mail: info@mon.gov.ru

ПРОГНОЗ НАУЧНО-ТЕХНОЛОГИЧЕСКОГО РАЗВИТИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ НА ПЕРИОД ДО 2030 ГОДА

Москва

Декабрь, 2013

ДМ-П8-5

Прогнозы Российской академии наук

Экспоненциальный рост технических характеристик	Миниатюризация	Снижение стоимости компонентов
Рост вычислительных мощностей и интеллектуальных возможностей техники	Быстрая смена стандартов и технологических платформ ИС и сетей	Появление всепроникающих и сверхвысокоскоростных сетей, устройств и систем глобального масштаба
Развитие новых архитектур и принципов организации вычислений (например, облачных или распределенных грид-систем)	Повышение доли freelance-разработчиков	Смещение центров разработки, компетенций и производства за пределы развитых стран

Прогнозы Российской академии наук

Языки и системы программирования, реализующие новые принципы	Системы машинного обучения	Новые принципы биометрической идентификации
Глобальная идентификация информационных объектов	Новые интерфейсы «человек-машина»	Виртуализация рабочих мест
Коллективный интеллект	Big Data	Всеобъемлющий Интернет

Прогнозы Российской академии наук

Мобильные устройства	Децентрализованные сети персональных компьютеров и мобильных устройств	Новые принципы организации сетей (например, когнитивные, адаптивные)
Технологии дополненной реальности	Краудсорсинг	Квантовые технологии
Новое поколение мобильной связи	Роботы-помощники	Цифровые устройства с функциями самовосстановления

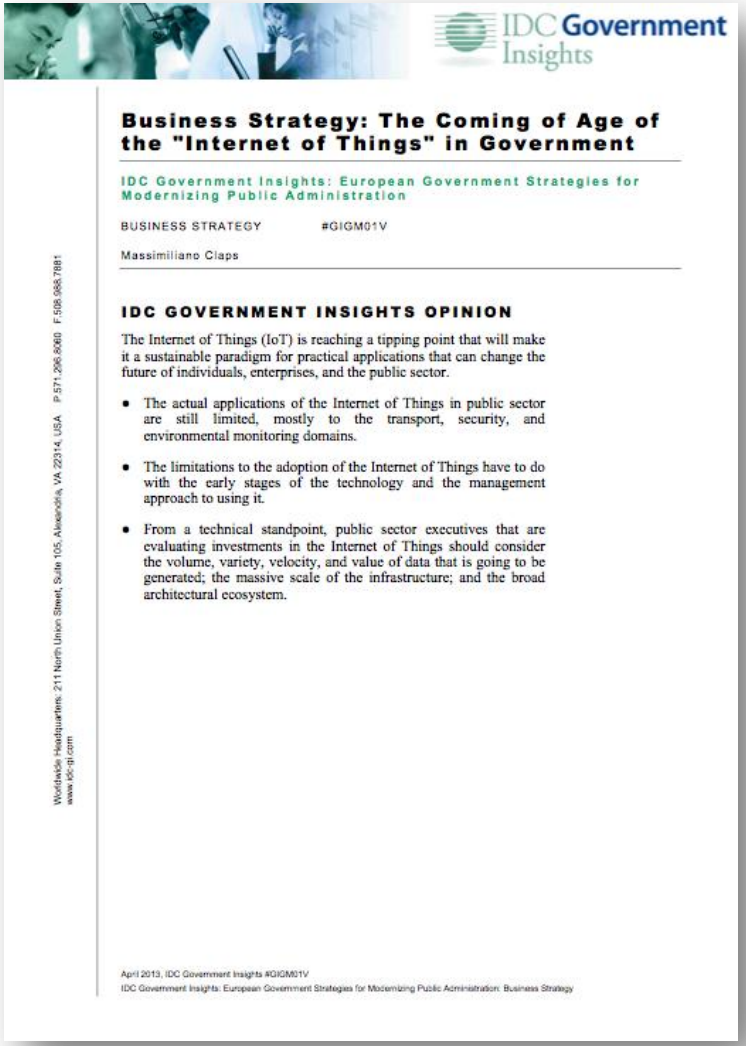
Прогнозы Российской академии наук

Smart Grid	«Умный дом»	Интеллектуальное управление трубопроводными потоками
Интеллектуальное управление транспортом	Автономные необслуживаемые микромощные радиоэлектронные устройства	Устройства для работы с пространственными данными
Носимые беспроводные медицинские датчики	Цифровизация бытовых устройств	Программируемые сети (SDN) и виртуализация сетевых сервисов

В качестве заключения

- Тенденции технологического развития известны заранее
- Процесс информатизации нарастает, включая и госорганы
- Знать, понимать и учитывать тенденции нужно уже сейчас

  Особенно при разработке нормативных документов



IDC Government Insights

Business Strategy: The Coming of Age of the "Internet of Things" in Government

IDC Government Insights: European Government Strategies for Modernizing Public Administration

BUSINESS STRATEGY #GIGM01V

Massimiliano Claps

IDC GOVERNMENT INSIGHTS OPINION

The Internet of Things (IoT) is reaching a tipping point that will make it a sustainable paradigm for practical applications that can change the future of individuals, enterprises, and the public sector.

- The actual applications of the Internet of Things in public sector are still limited, mostly to the transport, security, and environmental monitoring domains.
- The limitations to the adoption of the Internet of Things have to do with the early stages of the technology and the management approach to using it.
- From a technical standpoint, public sector executives that are evaluating investments in the Internet of Things should consider the volume, variety, velocity, and value of data that is going to be generated; the massive scale of the infrastructure; and the broad architectural ecosystem.

Worldwide Headquarters: 211 North Union Street, Suite 105, Alexandria, VA 22314, USA P:571.296.8060 F:508.988.7881 www.idc-gi.com

April 2013, IDC Government Insights #GIGM01V
IDC Government Insights: European Government Strategies for Modernizing Public Administration: Business Strategy