

Бизнес-трансформация в среде интернета вещей: как защититься от угроз и рисков?

Андрей Филатов
генеральный директор IBM в России и СНГ



Интернет вещей помогает SNCF поддерживать плавный ход

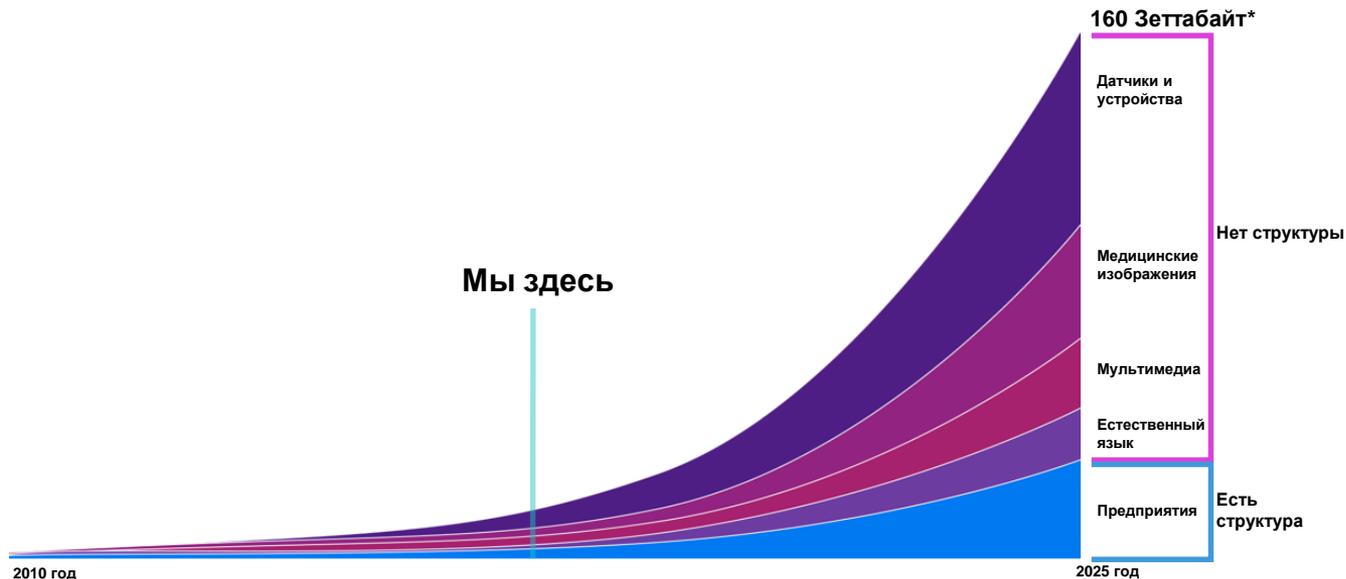


свыше 30,000 км рельсов,
15,000 составов и 3,000 станций

- Тысячи датчиков на поездах и рельсах
- Десятки тысяч наборов данных, отправляемых на облачную платформу IBM Watson IoT
- Инженеры и эксперты могут подключаться к составам в реальном времени
- Используя предиктивную аналитику, SNCF избегает вывода составов из эксплуатации и повышенных расходов на ремонт

Видеоролик о проекте с SNCF: <https://www.youtube.com/watch?v=25ec2HP45dl>

Датчики и устройства IoT становятся одним из основных источников лавинообразного роста данных



*Source IDC, IBM projections based on analyst report.



Угрозы системам интернета вещей реальны и масштабны

Атаки на IoT-системы ставят под угрозу репутацию брендов и доверие клиентов

Forbes

**The Dyn DDOS Attack And The Changing Balance Of
Online Cyber Power**

WIRED

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

**HACKERS REMOTELY KILL A JEEP ON THE
HIGHWAY—WITH ME IN IT**

The New York Times

EUROPE

Hackers Use New Tactic at Austrian Hotel: Locking the Doors

Watson IoT

Безопасность в среде интернета вещей требует нового взгляда

Точка зрения IBM:

- Соединенные «вещи» отлично подходят для инноваций и экспериментов, но в то же время несут в себе вызовы и угрозы с точки зрения безопасности
- Есть и новые риски в силу уникальности среды IoT:
 - Распределенное расположение
 - Физические последствия вмешательства
 - Большое разнообразие
 - Миллиарды устройств
 - Обслуживание производственным, а не ИТ-персоналом



Читайте: <https://ibm.co/iotsecurity-POV2>



Непрерывный цикл обеспечения безопасности IoT

- Начать с обеспечения возможностей для защиты
- Дополнить защиту исследованием угроз
- Видеть и понимать угрозы
- Использовать когнитивное решения для выработки превентивных мер
- Постоянно наращивать экспертизу

Требования к безопасности IoT – от чипов до приложений



О безопасности IoT – для создателей устройств и решений



Структура доверенных и надежных IoT-решений

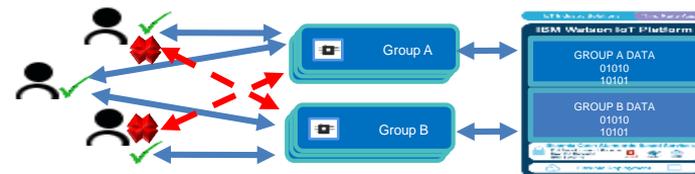


Надежный дизайн: многослойная защита

- Физический и операционный уровни
- Сетевая защита
- Защита системы, приложения и данных
- Соответствие стандартам: ISO27001

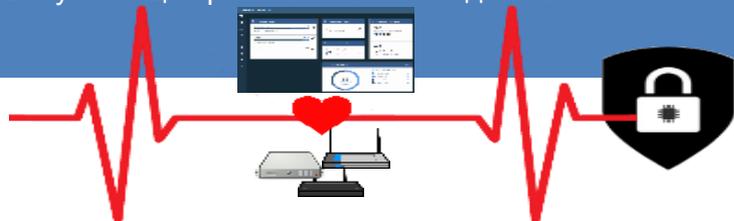
Базовые и продвинутые степени защиты

- Аутентификация (регалии)
- Авторизация (привилегии)
- Контроль доступа (контекст и изоляция)
- Ролевая авторизация
- Защита данных
- Визуализация рисков и политика действий



Экспертиза в IoT и безопасности

- Разработка и поддержка стратегии защиты IoT
- Оценка и обучение персонала
- Оптимизация необходимых бизнес-процессов
- Тестирование устройств на взлом



Когнитивная защита IoT



IoT Security		
DESIGN <small>SECURITY</small>	DEPLOY <small>SECURITY</small>	MANAGE <small>SECURITY</small>
<ul style="list-style-type: none">Design and manufacture securityHarvest the devicesEliminate errors in manufacturing and deliveryOptimistic delivery model (for post deployment updates)Create a trusted maintenance ecosystem	<ul style="list-style-type: none">Operate security<ul style="list-style-type: none">Application authentication and securityDevice authenticationNetwork securityOperational security<ul style="list-style-type: none">Strong encryption and integrity protection for data	<ul style="list-style-type: none">Audit and analyze usage patternsDetect and Defend with advanced threat detectionStrong intrusion detection systemsCreate a robust maintenance ecosystemMonitor an up-to-date security environment

IoT threat models, control points and response processes

Когнитивный IoT открывает новые возможности и угрозы

- Активные и пассивные атаки
- Безопасность, защита и приватность
- Атаки на когнитивный механизм

Надежный и масштабируемый жизненный цикл устройств

- Возможное использование блокчейна для управления идентификацией устройств
- Дополнительная аутентификация на базе криптоалгоритмов

Акцент на приватности

- Токены и защита личных данных при аутентификации

Когнитивный IoT в сфере безопасности

- Машинное обучение и когнитивные функции
 - Мониторинг и просеивание
 - Корреляция и прогнозы
 - Адаптация и предвосхищение

Надежные разработка и производство

- Разработка с учетом защиты
- Разработка с учетом приватности
- Тестирование защиты
- Модель непрерывного производства
- Целостность при производстве и поставке

Надежные операции

- Повышение прочности устройства
- Защита канала связи
- Аудит и анализ паттернов использования
- Поддержание надлежащего уровня защиты



<https://ibm.co/iotsecurity-POV2>

Watson IoT

Как помогает Watson IoT Platform?

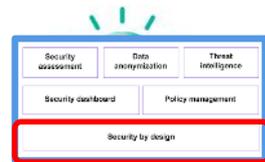
Платформа помогает обеспечить необходимый уровень защиты при внедрении среды интернета вещей



Управление устройствами

Обеспечивайте постоянную работу и защиту устройств благодаря *Watson IoT Device Management*

- Управляйте IoT-устройствами при помощи Watson IoT Platform
- Иницируйте действия с дэшборда или автоматически через API
- Одновременно управляйте тысячами устройств
- Создавайте свои команды управления
- Подсоединяйте другие платформы управления через дэшборд (Jasper Control Centre, AT&T Control Center, Orange)
- Управление устройствами платформы Arm® Mbed™



Набор возможностей и сервисов для построения эффективной стратегии и программы тестирования



ТЕСТЫ

- Начальные
- Стандартные
- Продвинутые



ОЦЕНКА

- Приложения
- Сеть
- Оборудование
- Персонал



АНАЛИЗ

- Ручная проверка кода
- Автоматизированная проверка в статике



- **Программный подход** упрощает внедрение программ
- **Аналитика слабых мест** помогает эффективно определять риски и создавать планы реагирования
- **Удобное тестирование** кастомизация тестирования любой области



Приложение

- Веб
- Мобильное
- Терминал
- Толстый клиент
- Мейнфрейм
- Промежуточное ПО



Сеть

- Внутренняя
- Внешняя
- Беспроводная
- Прочие радиочастоты
- SCADA†



Персонал

- Личное взаимодействие
- Социальный инжиниринг
- Фишинг



Оборудование и встраиваемые системы

- **Интернет вещей**
- Носимые устройства
- POS-устройства
- Банкоматы
- Киоски самообслуживания

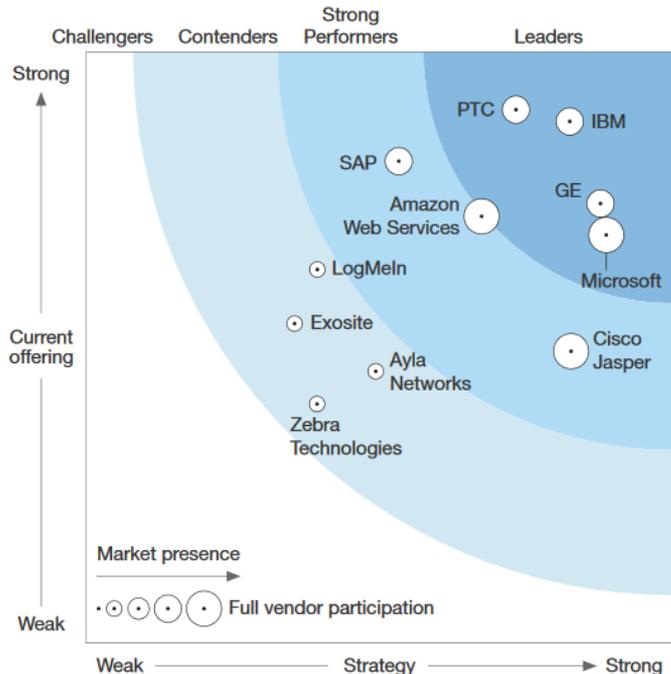
†Supervisory control and data acquisition (SCADA)

Тестирование защиты и интернет вещей

- **Watson IoT Platform** нацелена на четыре указанные области
- **X-Force Red** обладает экспертизой для тестирования любого устройства, сети, кода или взаимодействия людей в IoT-решении
- Каждое тестирование подстроено под конкретный проект, эксперты покажут, как системы могут быть взломаны не автоподбором, а руками
- X-Force Red использует широкий набор инструментов, как стандартных, так и уникальных
- X-Force Red публикует результаты исследований на сайте **The Red Portal**. Заказчики оперативно получают необходимую информацию по угрозам и мерам предотвращения



По данным The Forrester Wave™, IBM является одним из лидеров в программных IoT-платформах



Source: Forrester Research Inc. "The Forrester Wave™: IoT Software Platforms, Q4 2016," by Michele Pelino and Andrew Hewitt with Christopher Voce, Merritt Maxim, Frank E. Gillett, Jeffrey S. Hammond, Michael Caputo and Diane Lynch, November 15, 2016

The Forrester Wave is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Факторы безопасности в среде интернета вещей

- **Безопасность компьютерных систем остается приоритетной задачей**
 - **Постоянная работа на протяжении всего жизненного цикла решения**
- **Обеспечение безопасности устройств и решений интернета вещей требует новых возможностей**
 - **Новые возможности адресуют уникальные аспекты IoT-решений**
- **Безопасность, приватность и защита взаимосвязаны**
 - **Внедряйте по умолчанию безопасные решения**
- **Новые технологии и подходы помогут снизить риски для бизнеса**



СПАСИБО!

