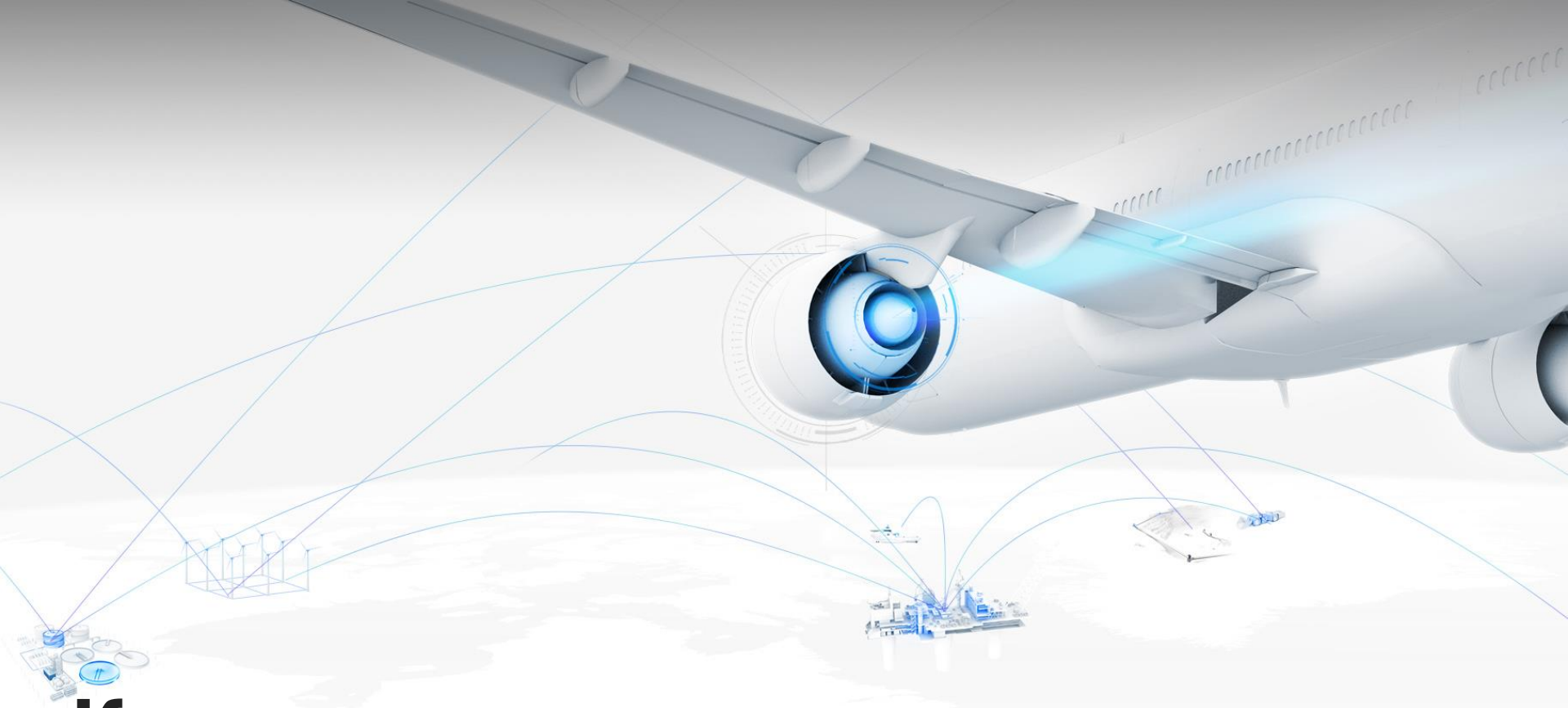


Как внедрять современные технологии в российских реалиях

или можно ли доверять встроенной безопасности?

24 мая 2018

Алмаз Хисамов, CISSP, GICSP
Директор по информационной безопасности, GE Россия/СНГ

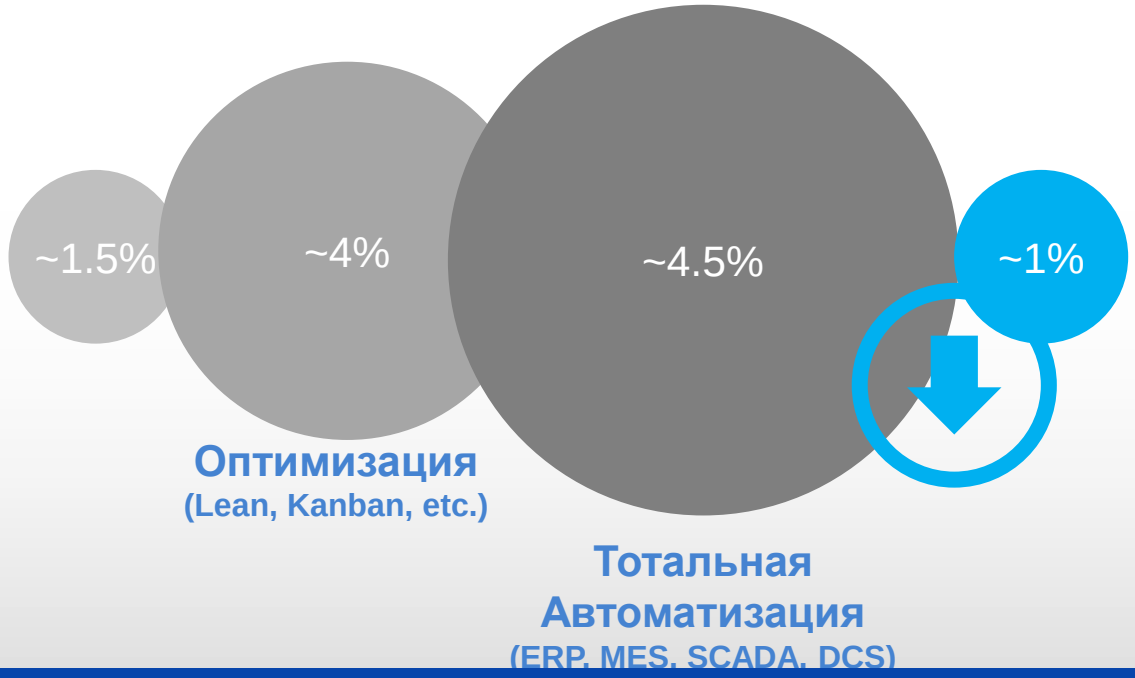
Современные технологии: история

На пороге следующей индустриальной революции?

Современные технологии: причины

Годовой прирост продуктивности

1980 - 2000 **2000-2007** **2007-2018**



Причины Индустриальной трансформаци

Классические подходы по оптимизации и автоматизации достигают своих возможных максимумом

Вычислительные технологии и подходы достигли новых высот

Слияние ИТ и ОТ может привести к новым возможностям по уровням эффективности и бизнес-инновациям

Рост индустриальной производительности на минимуме

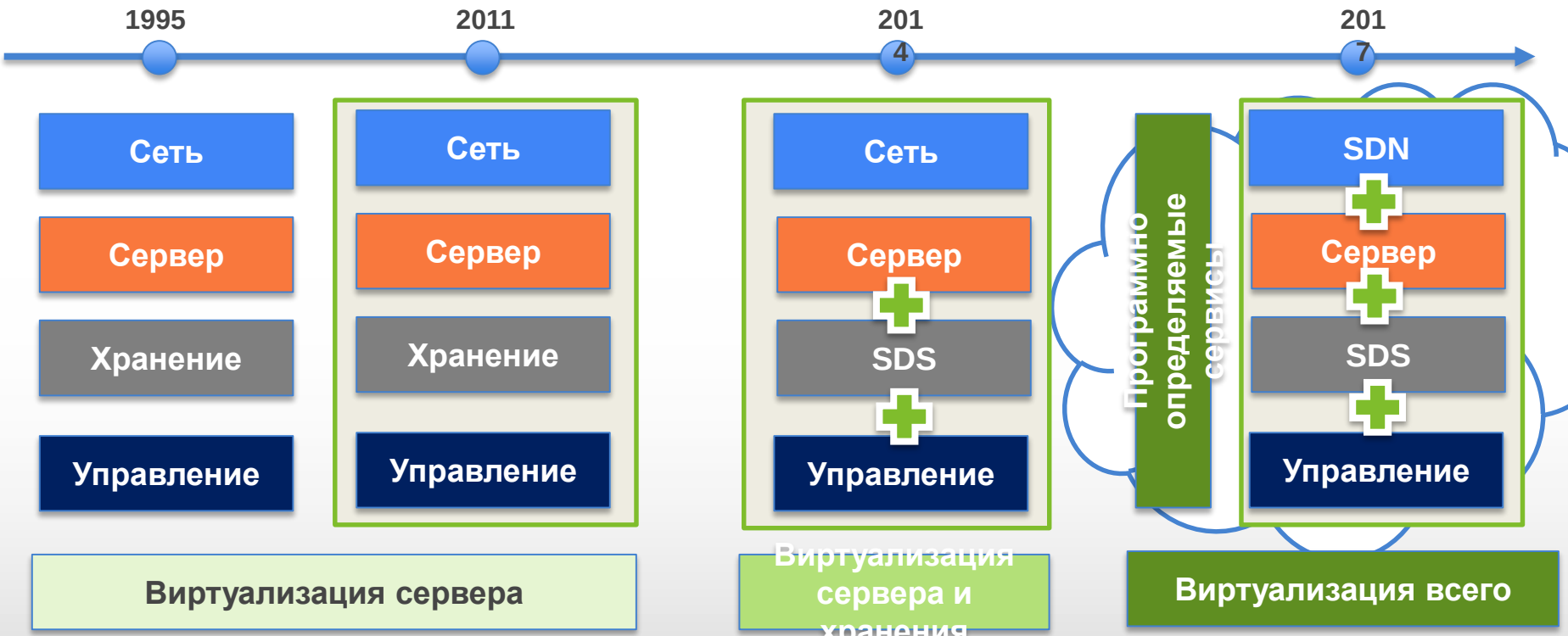
Современные технологии: «железный» пример

Традиционная
Покупка отдельных частей
Сложна в развертывании

Конвергентная
Покупка одного объекта
Быстрее в развертывании

Гиперконвергентная
Хранение становиться составной частью сервера

Программно определяемая
Виртуализация сервера, хранения, сети



Современные технологии: российские реалии

Топ-10 компаний по инвестициям в R&D

2017 Rank	Company Name	Country	Industry group	R&D Expenditures ($US Billions) 2016	R&D Expenditures ($US Billions) 2017	Revenue ($US Billions) 2016	Revenue ($US Billions) 2017
1	Amazon.com, Inc.	United States	Retailing	12.5	16.1	107.0	136.0
2	Alphabet Inc.	United States	Software and Services	12.3	13.9	75.0	90.3
3	Intel Corporation	United States	Semiconductors and Semico...	12.1	12.7	55.4	59.4
4	Samsung Electronics Co., Ltd.	South Korea	Technology Hardware and Eq...	12.0	12.7	166.7	167.7
5	Volkswagen Aktiengesellschaft	Germany	Automobiles and Components	12.5	12.1	225.2	229.4
6	Microsoft Corporation	United States	Software and Services	12.0	12.0	93.6	85.3
7	Roche Holding AG	Switzerland	Pharmaceuticals, Biotechnolo...	9.4	11.4	49.6	51.8
8	Merck & Co., Inc.	United States	Pharmaceuticals, Biotechnolo...	6.7	10.1	39.5	39.8
9	Apple Inc.	United States	Technology Hardware and Eq...	8.1	10.0	233.7	215.6
10	Novartis AG	Switzerland	Pharmaceuticals, Biotechnolo...	9.5	9.6	50.4	49.4

2017 Rank	Company Name	Country	Industry group	R&D Expenditures ($US Billions) 2016	R&D Expenditures ($US Billions) 2017	Revenue ($US Billions) 2016	Revenue ($US Billions) 2017
267	Public Joint Stock Company ...	Russia	Energy	0.5	0.5	99.2	99.8
431	Yandex N.V.	Russia	Software and Services	0.2	0.3	1.0	1.2

Источник: https://www.strategyand.pwc.com/innovation1000

<0,0006 от мировых затрат на НИОКР (R&D) в год

Встроенная безопасность: что это

Принципы, что и в концепции «Встроенное качество»:

- Уровнем безопасности можно *управлять – планировать, внедрять и поддерживать*
- Безопасность *встроена* в «процесс производства» конечного продукта
- Уход от последующих проверок или необходимости в «навесных» средствах

Уровни в ИТ

- Компоненты: Процессор, Память, Устройства ввода-вывод, плата
- Вычислительное устройство: Компьютер | Микроконтроллер
- Операционная система | прошивка
- Драйверы | Прикладные программы
- Сеть, сервисы
- Информационная система
- Бизнес-процесс

Подходы:

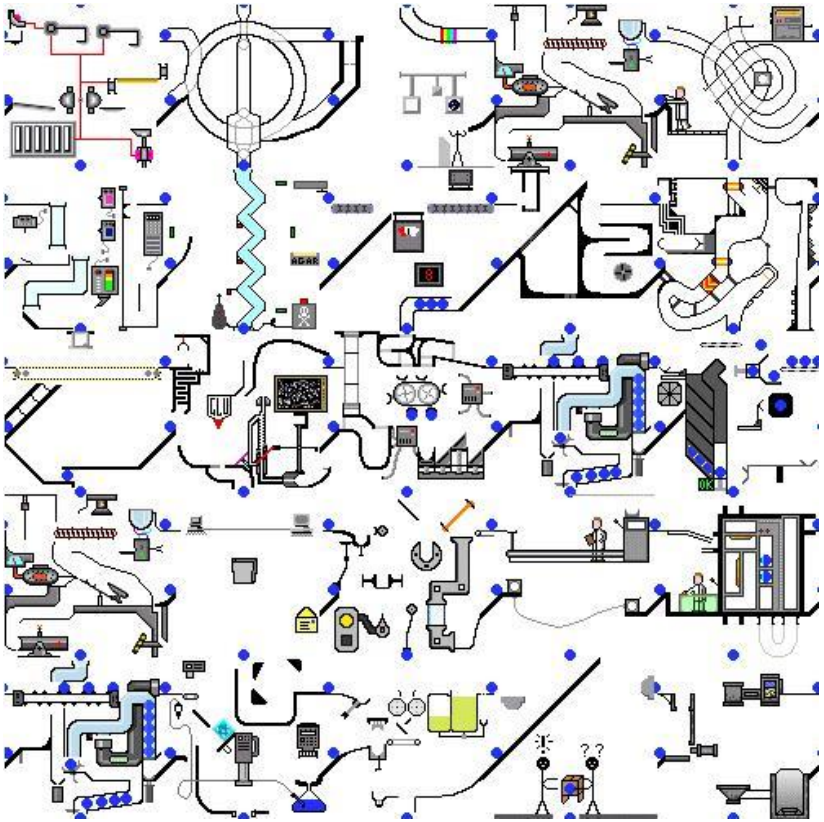
- Модель угроз и требования безопасности. А они все учитывают?
- Дизайн и архитектура. Кто проверит архитектора?
- Анализ и исследование на ошибки (анализ кода, тестирование на проникновение, статистические тесты, динамические тесты, нагрузочные тесты): полнота?
- Обучение разработчиков, архитекторов, пользователей безопасным подходам. А кто обучит тренеров?
- Правильное конфигурирование. А у вас есть change management?
- Мониторинг и реагирование (DevOps, SOC). Что есть аномалия?
- …

Встроенная защита эффективнее «навесных» средств защиты

Встроенная безопасность: реальность

Уровни в ИТ	Сколько видов
Компоненты: Процессор, Память, Устройства ввода-вывод, плата	10^6?
Вычислительное устройство: Компьютер | Микроконтроллер	10^3?
Операционная система | прошивка	10^3?
Драйверы | Прикладные программы	10^6?
Сеть, сервисы	10^4?
Информационная система	10^7?
Бизнес-процесс	10^7?

Как работает в реальности



Уровень сложности, когда ни один участник не может быть экспертом во всем

Image source: https://blog.kinaxis.com/wp-content/uploads/2011/10/diagram1.jp

Встроенная безопасность: вопросы доверия

Уверенность в безопасности (теория):
Независимая оценка и подтверждение соответствия профессиональным участником которому есть доверие (Общие критерии, испытания, сертификация и т.п.)

Реальность в случае передовых технологий:

- 1-5 игроков-разработчиков в мире
- Формирование требований к новому
- Методик оценки мало или нет вообще
- Плохо масштабируется (индивидуально, изменение версий/конфигураций, юрисдикции)
- Отсутствие мотивации продавца (должно окупаться, короткий жизненный цикл продукта)
- Отсутствие мотивации бизнес-заказчика (долго, дорого, неясная отдача)

Уверенность в безопасности (практика):

- Эшелонированная оборона = совокупность небольших лучше (и дешевле) чем одно большое
- Уровень безопасности = уровень безопасности самого слабого звена. Сначала основы:
  - Выделенный сотрудник ИБ (лучше подразделение) и культура
  - Политики, стандарты
  - Правильная конфигурация
  - …

Абсолютной безопасности не существует… Встроенная безопасность не панацея, а составная часть

Безопасность: российские реалии

2016: 20+ значимых законодательных актов

2017: 15+

- ФЗ-187, ФЗ-193 и ФЗ-194
- Указ Президента №620 (ГосСОПКА)
- Распоряжение Правительства №1632 (Цифровая экономика)
- Постановление Правительства №555 (ГИС)
- ФСТЭК 31-й приказ (не АСУТП! ОПК)
- ФСТЭК: изменения в 17, 21, 31,
- Стратегия развития информационного общества
- ФЗ об удаленной/биометрической, идентификации клиентов фин.
- …

2018: 15+

Встроенная безопасность в российских реалиях

Часто:

- Слышал, что мне надо все сертифицированное…
- Мы никому не доверяем. А чем докажете?
- Хочется и встроенную, и проверенную и… сами настройте
- Куплю только 1 экземпляр и… за дешево ☺

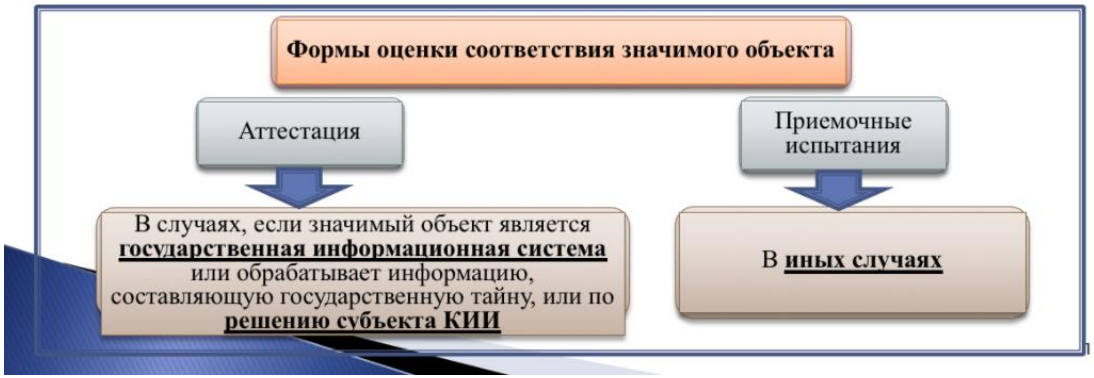
Правильно:

- Знать свой бизнес и процессы:
  - Зачем технология (в денежном эквиваленте)? Правило «5 почему»
  - Относится к ВПК? Есть государственная тайна?
  - ГИС? КИИ?
- Знать применимое обязательное регулирование
  - Сертификация ≠ аттестация
  - Оценка соответствия > сертификации
  - …
- Оценивать реальные риски и способы их уменьшения (не только технологиями)
  - Риски информационной безопасности – это часть операционных рисков компании
  - …

В большинстве случаев решение есть

Есть ли окно на пересечении технологий, реалий и безопасности? Пример 1.

Конференция ФСТЭК: критическая инфраструктура: формы оценки соответс



17

Оценка соответствия средств защиты:

- Средство защиты ≠ любое оборудование/софт
- Обязательная сертификация:
  - В случаях, установленных зак-вом (например, если объект КИИ = ГИС).
  - По решению субъекта КИИ
- В остальных случаях оценка соответствия средств защиты осуществляется в форме испытаний или приемки.
  - Документов, регламентирующих испытания и приемку средств защиты, разрабатывать не предполагается

Оценка соответствия значимого объекта КИИ

- Значимый объект КИИ ≠ любой объект КИИ
- В форме аттестации, если:
  - объект КИИ является ГИС или
  - гос. тайна или
  - если субъект КИИ принял такое решение.
- В остальных случаях осуществляется в форме приемочных испытаний (никак не регулируется)

Есть ли окно в пересечении технологий, реалий и безопасности? Пример 2.

Практические способы оценки и минимизации рисков:

- Модель угроз:
  - Будьте реалистами
  - Вовлекайтесь при работе с вендором/интегратором
- Сегментирование:
  - Разделяйте зоны с разными требованиями по безопасности
- Если нужно (или хочется) использовать сертифицированные средства защиты:
  - Наложенные средства защиты (IPSec на ГОСТ, сертифицированные МЭ)

Спасибо!

Алмаз Хисамов, CISSP, GICSP

Директор по информационной безопасности, GE Россия/СНГ

Almaz.Khisamov@ge.com