РусКрипто

КОМПАНИЯ АКТИВ

МТУСИ
МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ

Развитие рынка защиты киберфизических систем. Взгляд из будущего.

Алексей Лазарев,

Руководитель департамента защиты киберфизических систем,
Компания «Актив»

Андрей Колесников,

Директор «Ассоциации участников рынка Интернета Вещей»

iotas
НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ АССОЦИАЦИЯ УЧАСТНИКОВ РЫНКА ИНТЕРНЕТА ВЕЩЕЙ

Развитие глобальной инфраструктуры

1 Давние корни проблемы

- Традиционная инфраструктура в качестве базового фундамента
- Не было осознания проблем кибербезопасности
- Ограничения инфраструктуры, созданной десятки лет назад

2 Новые системы — старые ошибки

- Не все вредные факторы рассматриваются как часть системы. Сначала продукт — потом модель угроз
- Инерция мышления при создании новых продуктов
- Защитим, когда будут время, деньги, нормативка

Развитие решений

Этап 1
Стадия стартапа

Нехватка ресурсов, защита — не главная функция системы

Этап 2
Выход за пределы контролируемых контуров

Уязвимости известны, решения по защите от них нет

Этап 3
Попытки применения на значимых объектах

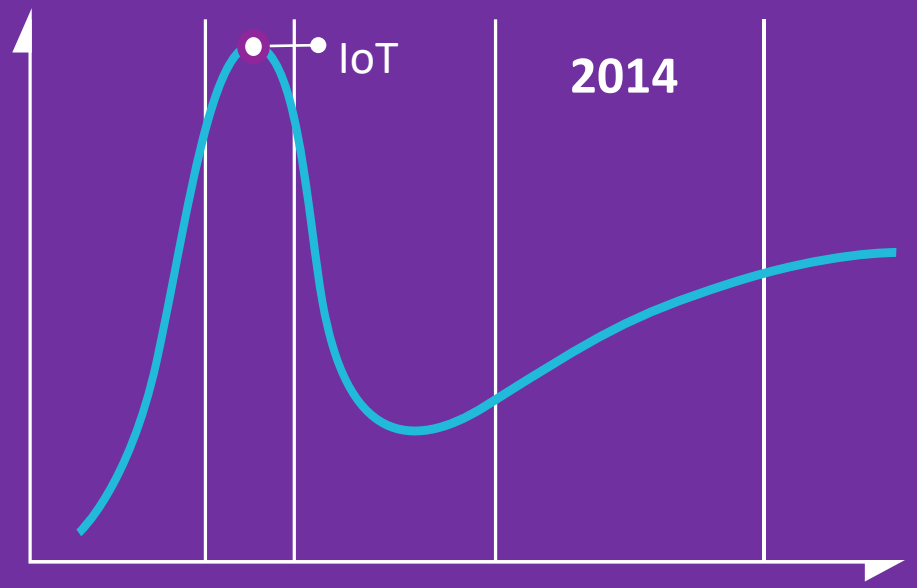
- Есть нормативка по защите, но дорого защищать
- Нет нормативки, применяются готовые решения с уязвимостями

Развитие систем защиты

1

Диалектика цифровизации

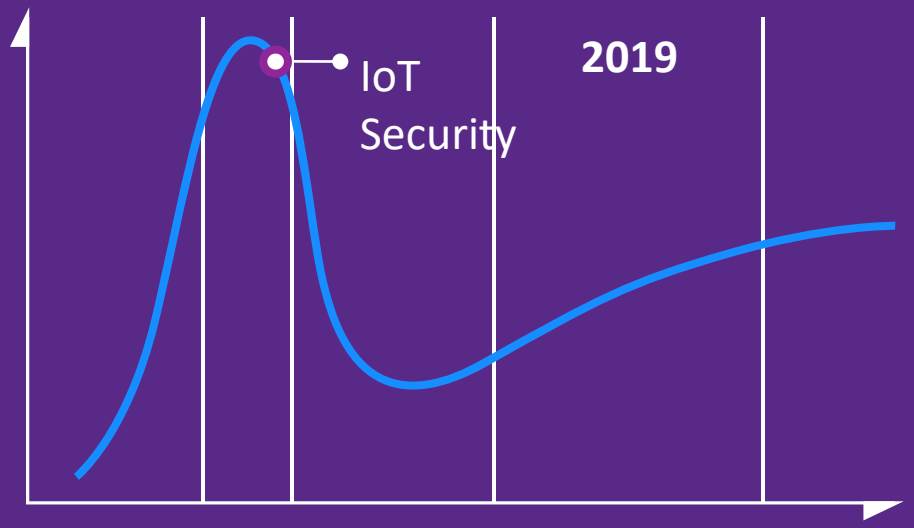
Новые возможности приносят пользу,
но порождают новые угрозы



2

Отставание в развитии систем защиты:

- во времени реакции на проблему
- по возможностям систем
- по темпам развития



Проблема — ограниченность ресурсов

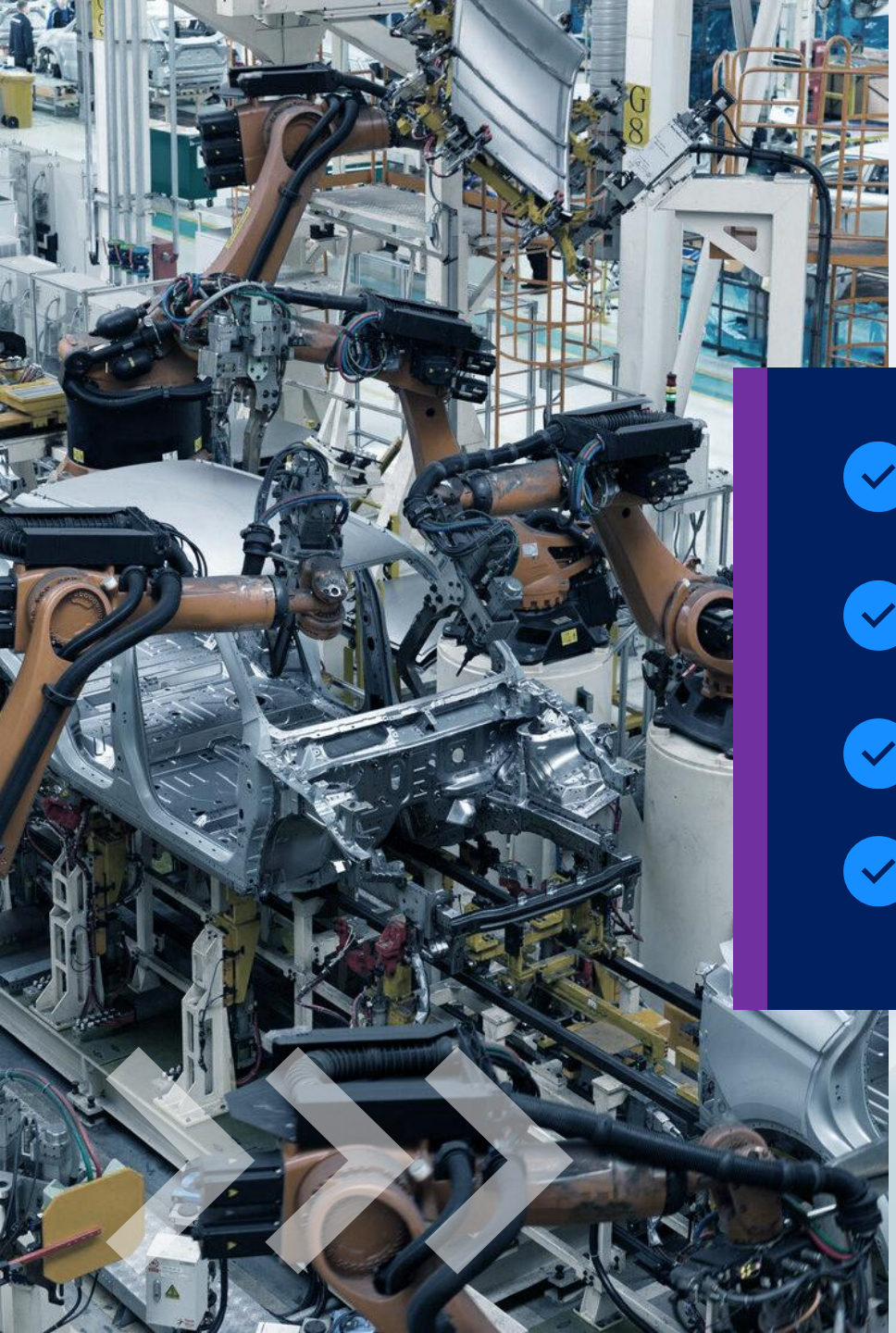
Киберфизические системы ⟷ **…ного устройств с ограниченными ресурсами:**

- Вычислительные ресурсы микроконтроллера или ASIC
- Энергонезависимая и (особенно) оперативная память
- Энергопитание
- Время/задержка выполнения операций
- Полоса пропускания канала связи

Криптографические алгоритмы (особенно асимметричные) ⟷
высокие требования к ресурсам (в общем случае)

Проблемы регуляторики

- Нормативка не покрывает все отрасли, которые следовало бы
- Высокий порог входа для вендоров в плане обеспечения безопасности, соответствующей текущим нормативным актам
- Ограниченные ресурсы регулятора при стремительном росте запросов рынка
- Слабая адаптивность регуляторов (где-то требования ниже, где-то выше, чем нужно)
- У каждого регулятора свой взгляд на безопасность
- Новые стандарты. Проблема актуальности на обозримом горизонте

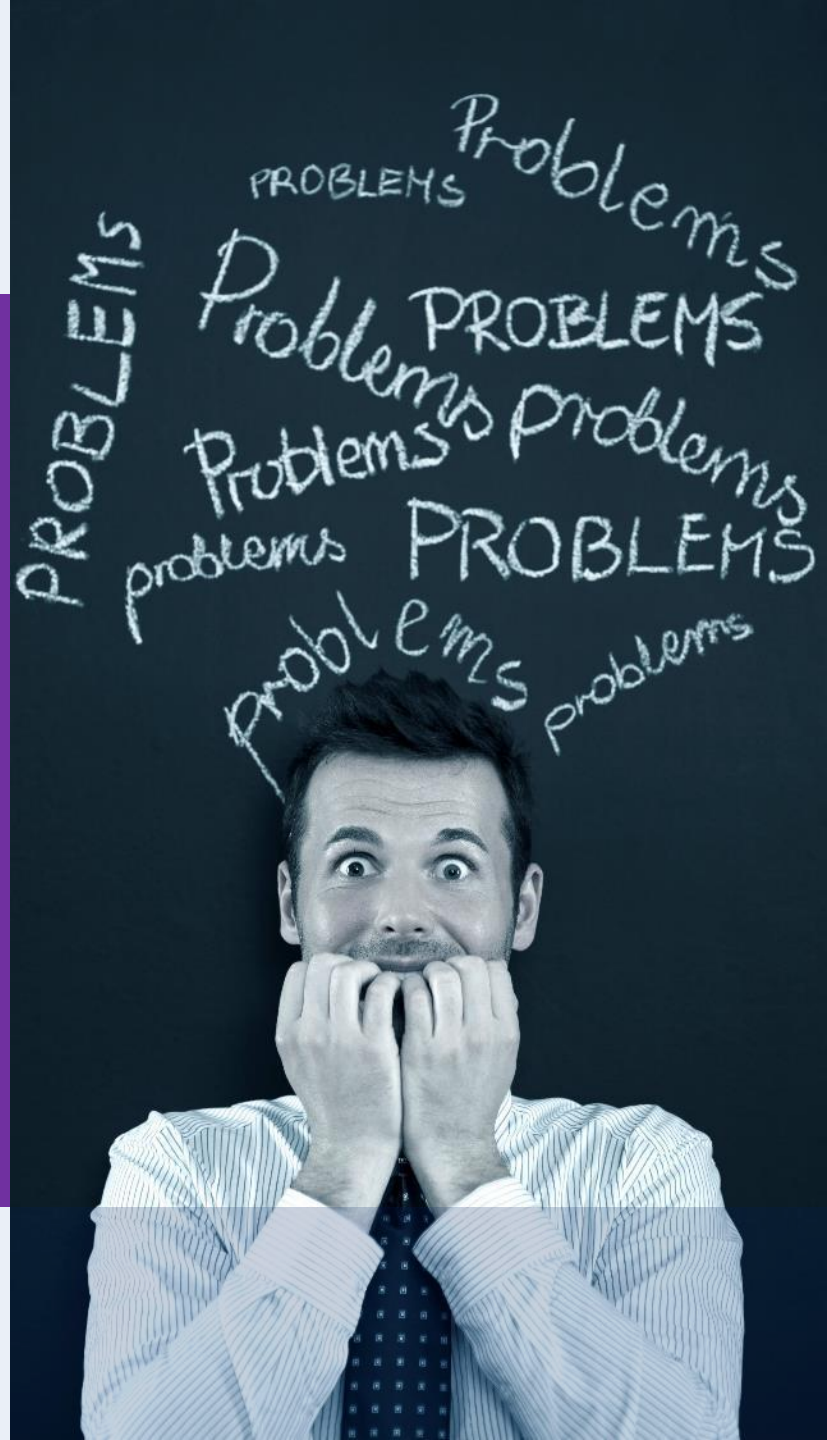


Производство компонентов

- Импортозамещение по компонентам
- Зарубежная криптография на отечественных решениях
- Производство чипов в России
- Отечественная криптография в кремнии

Проблемы интеграторов

- Перевес в сторону наложенных средств
- Криптографические средства требуют учета и контроля. Это существенно усложняет логистические процессы
- Устройство с СКЗИ проще заменить, чем отремонтировать
- Строгая позиция регулятора
- Зоопарк технологий



Коммуникационная инфраструктура

- Рост количества подключаемых устройств
- Рост скоростей передачи данных
- Зоопарк конкурирующих технологий и систем
- Работают ли прогнозы?
- «Бутылочные горлышки» сейчас, через 10 лет, через 20 лет

Знакомая ситуация?

Форсайт: что это такое и для чего нужно?

Форсайт (от английского *foresight* – предвидение) зародился в конце 1950-х в военно-промышленном комплексе США. Поначалу этот метод применялся для предсказания последствий долгосрочных решений и согласования приоритетов в области оборонных исследований и безопасности. Постепенно форсайт распространился на всю научно-техническую сферу, а затем и на более общие задачи социально-экономического развития.

В **методе форсайта** можно выделить два ключевых аспекта:

1) содержательный: форсайт – это сценарное прогнозирование научно-технологического и социально-экономического развития, определяющее возможные варианты развития экономики, промышленности, общества в 10-20 летней перспективе;
цель форсайта – определение возможного будущего, создание желаемого образа будущего и формирование стратегий его достижения.

2) организационно-деятельностный и процедурный: форсайт – это процесс, вовлекающий всех «стейкхолдеров»: промышленные предприятия, исследовательские центры, неправительственные фонды, общественные организации и т.д. и позволяющий согласовать и скоординировать действия по достижению желаемого будущего.

Кто участники и в чем их общий интерес?

Кто участники:

- исследователи, инженеры и другие специалисты разных профилей (все позиции инновационного цикла);
- стратеги, идеологи новых продуктов и услуг;
- руководители (лица, принимающие решения).

В чем их общий интерес (гипотеза):

- понять тренды развития киберфизических систем и систем их безопасности;
- совместно определить будущее рынка;
- координация конкурентов (coopetition): улучшать и продвигать рынок в целом.

Категории участников и рабочие группы

Специализации участников:

- маркетологи
  (включая руководителей и стратегов);
- технические специалисты (включая идеологов новых продуктов и услуг);
- «люди науки».

Рабочие группы:

- Бизнес и управление
- Позиционирование на рынке и маркетинг
- Регуляторика
- Криптография

Организация работы и некоторые правила коммуникации

- свобода самоопределения;
- полицелевой и «экосистемный» характер;
- чередование тактов групповой работы и пленара;
- использование специального «реквизита» (стикеры и доска для фиксации трендов).
- полидисциплинарный и полипрофессиональный характер (нет единой системы понятий и «правильных» определений);
- уважение к чужому мнению и стремление к взаимопониманию;
- работа на «общую доску»;
- не бывает глупых вопросов (ценность постановки проблем);
- уважение регламента.

Вопросы к тактам групповой работы

1. **Как вы видите развитие экосистем,** объединяющих производителей оборудования и программного обеспечения, интеграторов, бизнеса, а также заказчиков, в какой форме они должны создаваться и эффективно объединять участников рынка?

2. **Как киберфизические системы влияют на маркетинговые стратегии и подходы к взаимодействию с клиентами?** Как возвращение зарубежных вендоров повлияет на стратегии отечественных компаний и их позиционирование на рынке киберфизических систем и средств обеспечения их безопасности?

3. Известно, что практически все современные асимметричные криптоалгоритмы подвержены **потенциальному вскрытию с применением квантового компьютера с достаточными ресурсами.** Насколько такая угроза актуальна для киберфизических систем? Необходимо ли срочно переходить на постквантовые криптоалгоритмы? **Какая поддержка такого перехода требуется от государства, руководителей и владельцев бизнеса, разработчиков киберфизических систем и средств их защиты?**

Выводы по столу «регуляторика»

Тренд на разделение по сферам применения. Единый подход для всех вреден в ряде аспектов.

Тренд на облегченную нормативку для массового рынка. Гражданская криптография.

Тренд на повышение загрузки экспертных площадок и технических комитетов.

Тренд на создание экосистемы вокруг центров компетенций. Упор на производителя.

Прямой подход: формирование институциональной прослойки между регуляторами и участниками рынка. Отдельное направление бизнеса.

Обратный подход: разрешить всем все в разумных пределах, а затем постепенно закручивать регуляторные гайки.

Метарегулятор с нужными набором компетенций и полномочий.

Тренд на повышение стандартизации между вендорами на уровне протоколов, процессов, API.

Тренд на раздемонизацию регулятора.

Что получилось?

- Коммуникация на высоком уровне.
- Быстрое вовлечение в проблематику представителей других областей.
- Повышение осведомленности и компетенции участников
- Быстрое разрешение профессиональных споров
- Общий взгляд на проблему из формируемого образа будущего

А что дальше?

- Подготовка комплексного детализированного отчета с выводами
- Карта образа будущего по полученным результатам
- Набор команды на следующую сессию
- Верификация выводов и прогнозов предыдущей сессии
- Внесение новой проблематики
- Корректировка образа будущего и мер по его достижению

РусКрипто

Компания Актив

МТУСИ
Московский технический университет связи и информатики

Спасибо за внимание!

iotas
НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
АССОЦИАЦИЯ УЧАСТНИКОВ
РЫНКА ИНТЕРНЕТА ВЕЩЕЙ

Алексей Лазарев

Руководитель департамента защиты киберфизических систем, Компания «Актив»

Андрей Колесников

Директор Ассоциации участников рынка Интернета Вещей