TRIZ SUMMIT 2022

TRIZ Developers SUMMIT

TRIZ BIOPHARMA

Innovation Management and Triz Institute

TRIZ MASTER

TRIZ SUMMIT 2022

ALEXEY LAZAREV

Компании «Актив»
Руководитель департамента
защиты кибер-физических систем

SERGEY KHOVANOV

СПАО «Ингосстрах»
Руководитель направления
методологии и проектов ТРИЗ

TRIZ BIOPHARMA

INNOVATION MANAGEMENT AND TRIZ INSTITUTE

TRIZ SUMMIT 2022

Применение инструментов ТРИЗ для анализа развития систем безопасности в умном городе

TRIZ BIOPHARMA

INNOVATION MANAGEMENT AND TRIZ INSTITUTE

Город как техническая система

Умный город – это глобальная рукотворная система, состоящая из массы подсистем с многоуровневой иерархией

Техника развивается закономерно

Эти закономерности можно учитывать и использовать

Техника развивается через устранение противоречий

Г.С. Альтшуллер

Цель существования системы – выполнение ее основной полезной функции

Технические системы развиваются неравномерно

Элементы систем могут порождать вредные воздействия, приводящие к нежелательным эффектам

Системы обеспечения безопасности, как и другие, подчиняются тем же законам

Основная полезная функция систем безопасности – борьба с нежелательными эффектами и вредными факторами

Чем сложнее система, тем больше вероятность появления нежелательных эффектов

Системы обеспечения безопасности испытывают дефицит ресурсов в большинстве случаев.

Они, как правило, отстают по темпам развития от надсистемы.

Умный - не значит продуманный

- Умный город использует традиционную инфраструктуру, как базовый фундамент
- Возможности для внедрения есть, но они ограничены уже созданной архитектурой
- Большая часть инфраструктуры создавалась до осознания проблем безопасности

Новые системы – старые ошибки

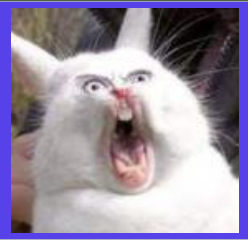
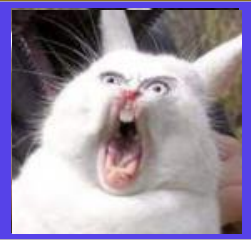
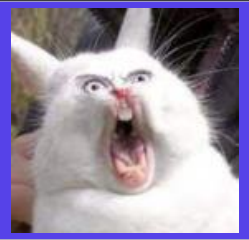
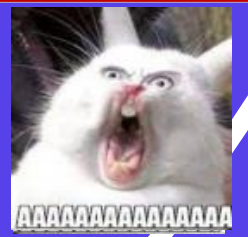
- Инерция мышления при создании новых продуктов:
  Сначала делаем продукт – потом пишем модель угроз.
- Защитим, когда будут: время, деньги, нормативка.
- На обеспечение безопасности нет времени на стадии стартапа и нет денег на момент внедрения в той области, где безопасность необходима.
- **Не все элементы, порождающие вредные эффекты рассматриваются как часть системы.**

  Злоумышленник – такая же часть информационной системы, как и ее основные компоненты.

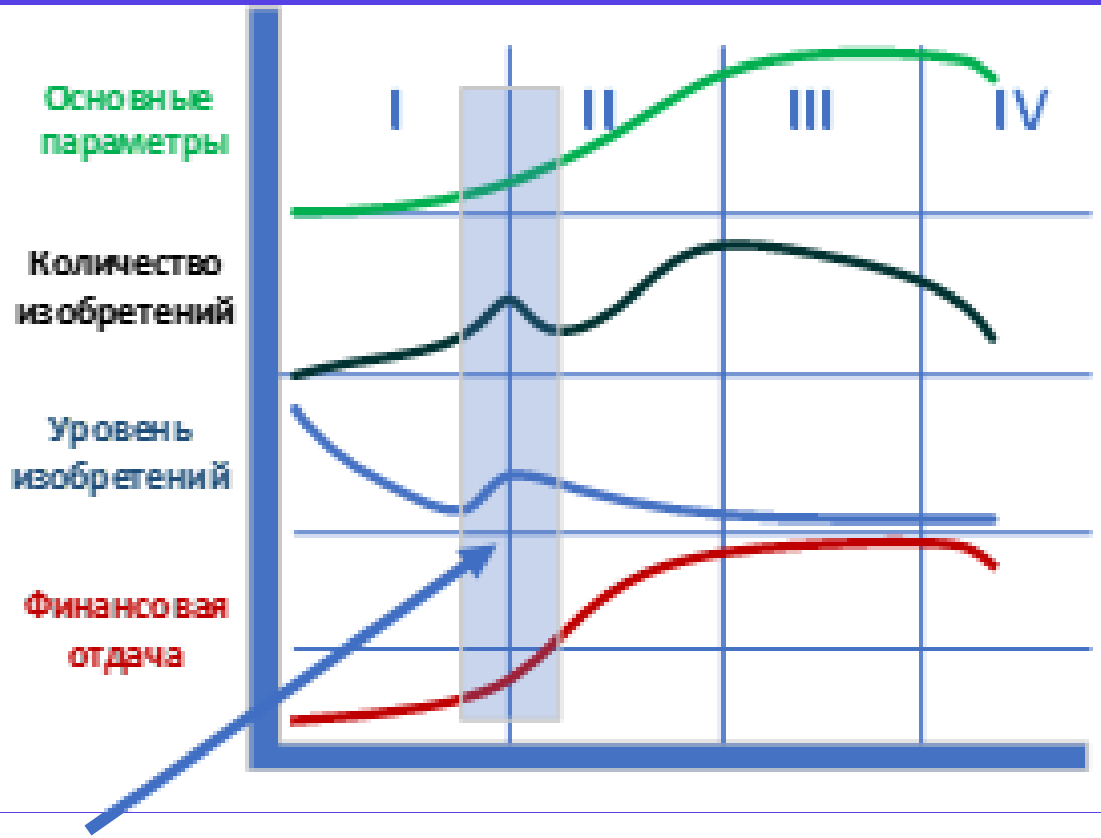
Безопасники постоянно в роли догоняющих. Как правило, они должны встроиться в уже готовые работающие системы.

Краткая история времени

Стоимость внедрения защитных механизмов

2012 IoT-Стартап	2014 Изначально планируемое применение	2018 Продукт в новых сферах применения	2020 Продукт в критических сферах применения
			
- Ресурсов мало!	- Защита не требуется, ведь продукт в закрытом контуре	- Прикручивать защиту дорого, прокатит и так.	- Доделывать за сто тыщ мильЁнов!
- Нет денег на защиту!	- Защита обеспечивается протоколом обмена!	- Никто атаковать не будет. Никому это не нужно!	- ОЙ ВСЁ!
- Некогда защищать, надо внедрять, пока мы первые!	- У нас Антивирус!	- Нормативка не требует применения защиты!	- Сертификат не дают!
- Конкуренты копаются со своей защитой) Дураки!	- Не было ни одной атаки!	- Цифровизация! Надо выйти за защищенный периметр!	- Конкурентов купили, они по нормативке проходят!

Развитие технических систем



(с) А. Любомирский, С. Литвин

Первый этап

с момента создания системы до выхода на рынок

- Нехватка ресурсов (кадровых, материальных)
- Наличие узких мест (скорость выполнения криптографических операций, автономность устройства)
- Потребление ресурсов других систем (чипы, система команд, технологии)

Переходный этап

- Увеличение темпов роста главных показателей
- Достижение уровня первоначальных требований
- Попытки внедрения в разных областях
- Растет количество инноваций

Второй этап

- Рост главных показателей системы
- В систему начинают интенсивно инвестировать
- Появляются дополнительные функции
- Система начинает потреблять ресурсы, предназначенные конкретно для нее

Системы информационной безопасности

На переходном этапе побеждают не самые перспективные, а самые приспособленные к текущей инфраструктуре системы

Первый этап

с момента создания системы до выхода на рынок

1. **Нехватка ресурсов**
   - Не хватает квалифицированных кадров, знакомых со спецификой IoT
   - Не хватает специализированных микросхем. Используются чипы общего назначения
   - В стартапах ресурсы на обеспечение безопасного обмена данными выделяются в недостаточном объеме либо не выделяются вовсе

2. **Наличие узких мест**
   - Невозможно обработать объемы данных на чипе криптографического устройства
   - Применение криптографических преобразований в разы снижает время автономной работы от батареи. А таких устройств большинство

3. **Потребление ресурсов других систем** (системы криптографии и ЭЦП)
   - Широко используется стек стандартов ISO-7816, разработанный для контактных смарт-карт в 90-х годах.
   - Используемые аппаратные технические средства взяты из области электронного документооборота, наиболее распространенной на данный момент.

Переходный этап

1. **Увеличение темпов роста главных показателей**

2. **Достижение уровня первоначальных требований**
   - В ряде систем существующих средств достаточно, но порой их функционал избыточен, в плане технологического стека
   - Используются компоненты из другой отрасли

   Умные счетчики электроэнергии. Передаваемых данных мало и их легко обработать, но для этого применяются СКЗИ, используемые, например, в ЭЦП.

   Так было в первых моделях

3. **Попытки внедрения в разных областях**

   Транспорт, СКУД, электронные пломбы, видеонаблюдение, сбор показаний, управление исполнительными механизмами.

4. **Растет количество инноваций**
   - Появляются специализированные протоколы

   Протокол обмена короткими сообщениями CRISP от ТК 26, чипы от Элвис, Миландр

Проблемы переходного периода

в криптографических системах защиты для умного города

- Очень многое перенесено из других систем, но полной адаптации компонентов пока нет
- Стоимость внедрения механизмов защиты может быть сопоставимой со стоимостью конечного устройства
- Нормативная база находится на стадии формирования, множество постановлений пересматривается. Это отпугивает как разработчиков, так и инвесторов
- Конкурирующие системы есть, но они достаточно дороги

TRIZ BIOPHARMA

INNOVATION MANAGEMENT AND TRIZ INSTITUTE

Факторы, сдерживающие переход на второй этап

- Микроконтроллеры с аппаратной поддержкой ГОСТ-шифрования только начинают появляться. Реализация на уровне плагинов или микропрограммы медленнее в разы.
- Для криптографической обработки большого объема данных нужны большие вычислительные мощности, а их нет за приемлемую цену.
- События последних месяцев отбросили нас назад в плане технического обеспечения, но значительно продвинули в плане понимания проблематики в широких кругах.

Состояние дел на 2021-й год (переходный этап)

Что происходит:

1. Зоопарк применяемых технологий постепенно упорядочивается и сужается
2. Идет работа по согласованию и гармонизации стандартов
3. В России взят курс на импортозамещение в регулируемых сферах
4. Первые решения в сфере защиты КФС выходят на рынок

Нет универсальной таблетки для обеспечения безопасного IoT, но попытки ее создания делаются крупными игроками

Действия на переходном этапе

Умеренная адаптивная стратегия развития

1. Необходимо максимально ускорить внедрение.
Лучшее — враг хорошего.

2. Нужно достичь минимально приемлемого
значения основных параметров и резкого
опережения как минимум
по одному из них.

Использование текущей материальной базы

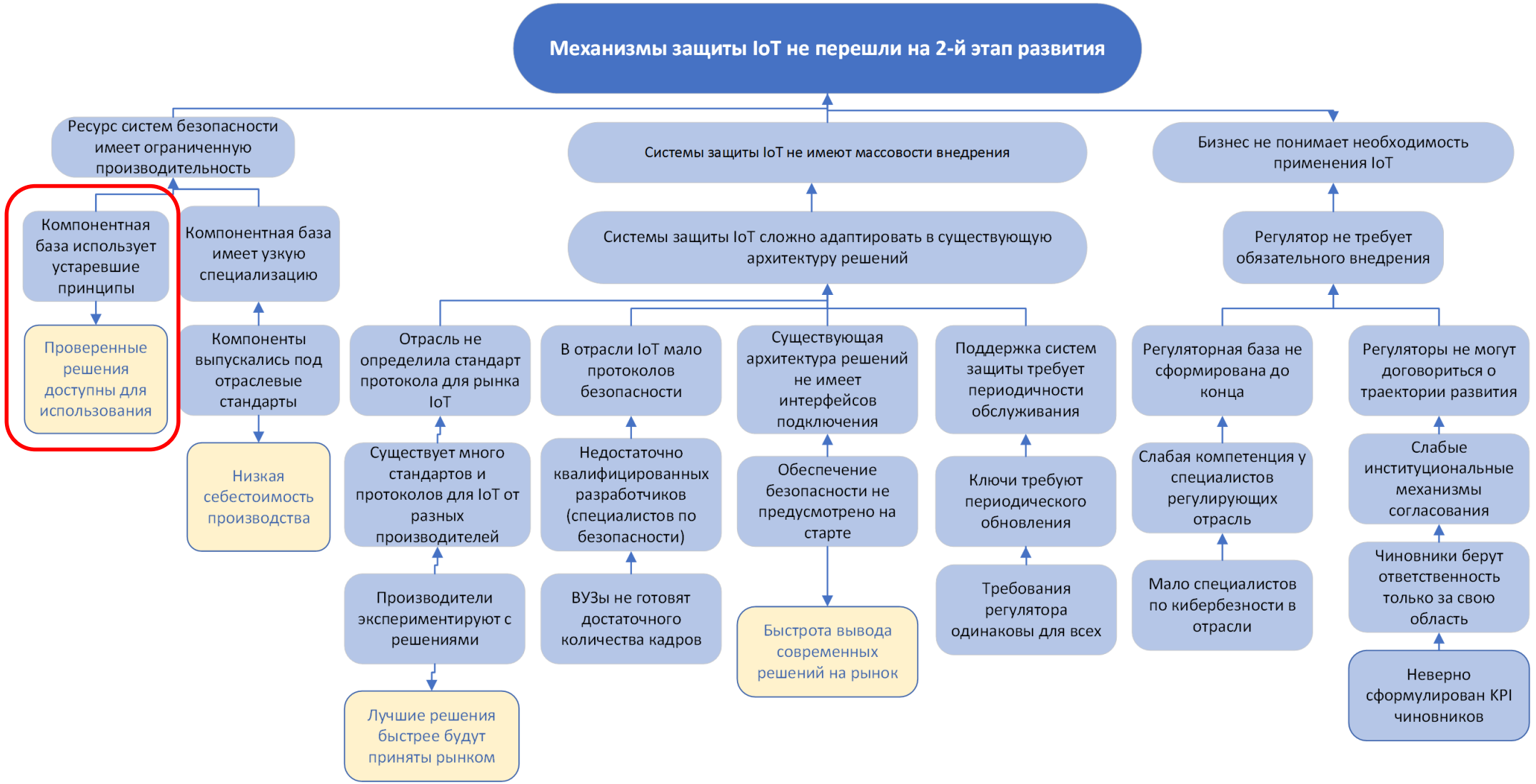
3. Нужно внедрять ТС в одной конкретной области где наиболее приемлемо соотношение достоинств и недостатков системы, а параметр – «чемпион» имеет важное значение.

4. Систему нужно приспособить
к существующим инфраструктуре
и источникам ресурсов.

Второй этап. Типовые признаки

1. Если рост главных показателей сопровождается ростом факторов расплаты, то относительно равномерным
2. Нарастают количество разновидностей системы и областей ее применения
3. Нарастает глубина различий между разновидностями ТС
4. Относительная глубина различий между поколениями системы существенно уменьшается к концу этапа
5. Система приобретает дополнительные функции, относительно тесно связанные с выполнением главной
6. Система начинает потреблять ресурсы, предназначенные специально для нее
7. При объединении системы с элементами надсистемы они начинают приспосабливаться к ней

Причинно-конфликтный анализ (RCA+)



п.п.	Причина	Постановка задач (Оператор отрицания)	Идея решения
1	**Механизмы защиты IoT не перешли на 2-й этап развития**	-	
1.1	**Ресурс систем безопасности имеет ограниченную производительность**	Как при ограниченной производительности ресурса систем безопасности обеспечить переход механизмов защиты на 2-й этап	
1.1.1	Компонентная база использует устаревшие принципы	Как на компонентой базе, использующей устаревшие принципы обеспечить достаточную ресурсную производительность систем безопасности	
1.1.2	Компонентная база имеет узкую специализацию	Как на компонентой базе узкой специализации обеспечить достаточную ресурсную производительность систем безопасности	
	Компоненты выпускались под отраслевые стандарты	Как на компонентной базе, которая выпускалась под отраслевые стандарты, компонентная база не имела узкой специализации	
2.1	**Бизнес не понимает необходимость применения IoT**	Как при отсутствии понимания у бизнеса необходимости применения IoT обеспечить переход механизмов защиты на 2-й этап	
2.1.1	**Регулятор не требует обязательного внедрения**	Как при отсутствии требования со стороны регулятора о необходимости внедрения IoT бизнес понимал необходимость применения IoT	
2.1.1.1	Регуляторная база не сформирована до конца	Как при несформированной до конца регуляторной базе регулятору обеспечить обязательное внедрение IoT	
	Слабая компетенция у специалистов регулирующих отрасль	Как при слабой компетенции у специалистов, регулирующих отрасль, сформировать полноценную регуляторную базу	
	Мало специалистов по кибербезности в отрасли	Как при малом количестве специалистов по кибербезопасности в отрасли обеспечить высокий уровень компетенций у специалистов, регулирующих отрасль	
2.1.1.2	Регуляторы не могут договориться о траектории развития	Как при отсуствии договоренностей у регуляторов по траекториям развития IoT регуляторы требовали обязательного внедрения	
	Слабые институциональные механизмы согласования	Как при слабых институциональных механизмах согласования регуляторы могли догвооритьсяо о траекториях развития IoT	
	Чиновники берут ответственность только за свою область	Как при ответственности чиновников только в своей области укрепить институциональные механизмы согласования	
	Неверно сформулирован KPI чиновников	Как при неверно сформулированных KPI чиновников сделать так, чтобы они брали ответственность не только за свою область	

п.п.	Причина	Постановка задач (Оператор отрицания)	Идея решения
3.1	**Системы защиты IoT не имеют массовости внедрения**	Как при отсутствии массовости внедрения систем защиты IoT обеспечить переход механизмов защиты на 2-й этап	
3.1.1	**Системы защиты IoT сложно адаптировать в существующую архитектуру решений**	Как при сложностях адаптации систем защиты IoT в существующую архитектуру решений они получили массовость внедрения	
3.1.1.1	Отрасль не определила стандарт протокола для рынка IoT	Как при отсутствии в отрасли стандарта протокола для рынка IoT системы защиты легко адаптировались в существующие архитектуры решений	
	Существует много стандартов и протоколов для IoT от разных производителей	Как при большом количестве стандартов и протоколов для рынка IoT от разных производителей отрасль смогла определить стандарт протокола для рынка IoT	
	Производители экспериментируют с решениями	Как при экспримментах производетелей с решениями IoT не было большого количества стандартов и протоколов IoT от разных производителей	
3.1.1.2	В отрасли IoT мало протоколов безопасности	Как при малом количестве в отрасли IoT протоколов безопасности можно было легко адаптировать системы защиты IoT в существующую архитектуру решений	
	Недостаточно квалифицированных разработчиков (специалистов по безопасности)	Как при недостаточном количестве квалифицированных разработчиков (специалистов пр безопасности) сформировать достаточное количество протоколов безопасности	
	ВУЗы не готовят достаточного количества кадров	Как при недосточном количестве подготавливаемых специалистов (в ВУЗах)обеспечить достаточное количество квалифицированныхх разработчиков	
3.1.1.3	Существующая архитектура решений не имеет интерфейсов подключения	Как при отсутствующих интерфейсах подключения у существующей архитектуре решений к ней было легко адаптировать системы защиты IoT	
	Обеспечение безопасности не предусмотрено на старте	Как при отсутствии систем безопасности у существующих решений обеспечить их интерфейсами подключения систем безопасности IoT	
3.1.1.4	Поддержка систем защиты требует периодичности обслуживания	Как при необходимости периодического обслуживания систем защиты IoT обеспечить их поддержку при адаптации к существующей архитектуре решений	
	Ключи требуют периодического обновления	Как при необходимости периодического обновления ключей защиты не возникала потребность периодического обслуживания	
	Требования регулятора одинаковы для всех	Как при одинаковых для всех требованиях регулятора можно было не обновлять ключи	

Пример противоречия

Устаревшая технология

Доступность

Электронные компоненты

Производительность

Современная технология

Устройства с автономным питанием

10 MHz – 40 MHz
(Энергосбережение)

Время автономной работы

Микроконтроллер
(Режим работы)

Количество обработанных запросов

100 MHz
(Поточное шифрование)

Устройства с автономным питанием

Прием	Рекомендация	Идея
35. ИЗМЕНЕНИЕ ФИЗИКО-ХИМИЧЕСКИХ ПАРАМЕТРОВ ОБЪЕКТА **20-26 и 16-26**	изменить концентрацию или консистенцию изменить температуру	Увеличить легкость вычисления криптографии за счет понижения ее стойкости (изменить длину ключа, уменьшить количество проходов).
	изменить агрегатное состояние объекта	Использовать ПЛИС для криптографии
10. ПРЕДВАРИТЕЛЬНОГО ДЕЙСТВИЯ **16-39**	Заранее выполнить требуемое действие (полностью или хотя бы частично) Заранее расставить объекты так, чтобы они могли вступить в действие без затрат времени на доставку и с наиболее удобного места	Не генерировать ключи каждый раз, а записать их все на производстве и потом менять по мере надобности. (Для СКЗИ нужен регулятор) Договориться с регулятором о продлении срока действия ключей для определенных применений
27. ДЕШЕВАЯ НЕДОЛГОВЕЧНОСТЬ ВЗАМЕН ДОРОГОЙ ДОЛГОВЕЧНОСТИ **20-23**	Заменить дорогой объект набором дешевых объектов, поступившись при этом некоторым качеством (например, долговечностью)	Менять все устройство в процессе поверки

Первые шаги ко 2-му этапу

1. Провести более глубокий анализ (RCA+), выявить ключевые НЭ и устранить их
2. Определить конфликты и разрешить их через устранение противоречий
3. Сформулировать задачи и подумать над идеями решений

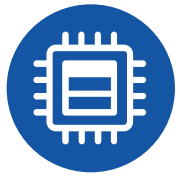
Наши действия?

1. Выявление проблемных сфер применения
2. Анализ у корректировка текущей нормативной базы совместно с регуляторами
3. Разработка, обкатка и демонстрация прототипа решения
4. Отстройка от конкурентов

Какие перспективы?

Выход на 2-й этап S-образной кривой

1. Адаптация текущих решений к новым областям применения
2. Использование специально адаптированных для нашей области ресурсов (чип)
3. Использование новых утвержденных стандартов (CRISP TK26)
4. Разработка собственного стандарта для модуля защиты



Одним из компонентов универсальной таблетки может быть массовый чип с российского производства с российской криптографией, реализованной на уровне транзисторной логики

TRIZ BIOPHARMA

INNOVATION MANAGEMENT AND TRIZ INSTITUTE

Роль регуляторов

- В дело включились регуляторы
- Безопасность кибер-физических систем перестала быть заботой только специалистов по безопасности
- Возникли новые потребительские ценности на рынке IoT и IIoT

- Соответствие требованиям регуляторов по линии защиты информации (152-ФЗ, 187-ФЗ)
- Наличие необходимых сертификатов
- Вхождение продукции в реестры (ЕРРП, ЕРПО)

Минкомсвязь России

МИНПРОМТОРГ РОССИИ

TRIZ BIOPHARMA

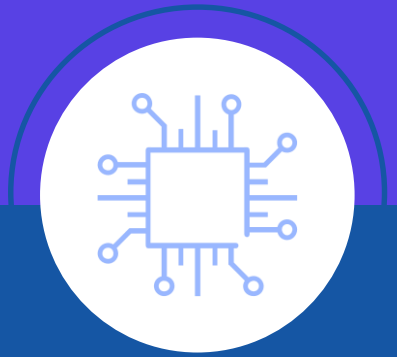
Innovation Management and Triz Institute

Основные тренды на ближайшие годы

Усиление и усовершенствование законодательства и требований регуляторов

Рост импортозамещения в плане софта и аппаратуры

Увеличение масштаба применения кибер-физических систем



Увеличение производительности и уменьшение энергопотребления электронных компонентов

TRIZ SUMMIT 2022

THANK YOU!

TRIZ BIOPHARMA

INNOVATION MANAGEMENT AND TRIZ INSTITUTE