КОМПАНИЯ ФРАКТИВ

rapid »» foresight

Будущее безопасности киберфизических систем в России. Перспективы и векторы развития.

Обсуждаем с участниками рынка вызовы безопасности и образ будущего через 10–15 лет

март, 2025

площадка МТУСИ в рамках Международного фестиваля отраслевой науки «Festival of Communications and Informatics Science — ComInfFest 2025»

ПРОБЛЕМАТИЗАЦИЯ

Компания Актив

Киберфизические системы (КФС), объединяющие физические и информационные процессы, стали основой цифровизации промышленности, энергетики, транспорта, умных городов. Однако их стремительное развитие сталкивается с критическими проблемами безопасности, требующими системного подхода и долгосрочного планирования.

ТЕКУЩЕЕ СОСТОЯНИЕ И КЛЮЧЕВЫЕ ПРОБЛЕМЫ

КОМПАНИЯ ПРАКТИВ

Наследие традиционной инфраструктуры

Киберфизические системы часто строятся на базе устаревшей инфраструктуры, созданной порой до осознания проблематики киберугроз. Интеграция цифровых компонентов повысила эффективность (управляемость, прозрачность, экономия ресурсов), но привнесла уязвимости, свойственные ИТ-системам. Таким образом, вредоносное воздействие на кибернетическую составляющую дестабилизирует физическую составляющую, что значительно повышает масштаб возможных последствий.

Дефицит ресурсов у разработчиков киберфизических систем

Стартапы, разрабатывающие решения в области киберфизических систем, зачастую игнорируют вопросы обеспечения безопасности по следующим причинам: дефицит ресурсов на ранних стадиях проекта, необходимость скорейшего выхода на открытый рынок, дабы опередить конкурентов. Впоследствии значительная доля выпущенных решений применяется в различной инфраструктуре, включая критически важную.
Внедрение необходимых защитных механизмов на поздних стадиях оказывается на порядок дороже, чем защита, встроенная изначально по принципу Security-by-Design, и игнорируется до момента вмешательства регулятора.

Ограниченный подход к проектированию

Разработчики, как правило, фокусируются на главной функции создаваемой киберфизической системы, игнорируя «вредные факторы», связанные с деятельностью нарушителя, — кибератаки, саботаж, человеческие ошибки. Это напоминает проектирование традиционных механических систем без учёта трения или температурных деформаций, воздействия химических веществ. Отсутствует осознание того, что нарушитель в современном мире – такая же неотъемлемая часть системы, как и ее основные узлы и компоненты.

Устаревшие стандарты

Многие протоколы обмена данными, применяемые в промышленном интернете вещей, были разработаны еще в 80-е годы XX века. Они в принципе не предусматривают каких-либо механизмов защиты информации кроме примитивного контроля целостности посредством подсчета контрольной суммы.
При разработке решений для обеспечения безопасности в киберфизических системах используются технологии, взятые из смежных областей:
• смарт-карточные стандарты типа PKCS,
• инфраструктура PKI.
Это приемлемо на первых этапах развития технических систем, но эти стандарты плохо подходят к текущей области применения, и с большой вероятностью будут замещены по мере развития рынка средств защиты КФС.

Технологическое отставание технических систем, выполняющих функции обеспечения безопасности

Наблюдается прогрессирующее отставание развития систем, реализующих механизмы безопасности, от развития целевых систем, где эти механизмы должны применяться. Причем отставание идет как по объемам, так и по темпам. Отставание заметно по всему спектру существующих систем обеспечения безопасности, особенно тех, где используется криптография. Часто это связано с жестким регламентированием применения защитных механизмов, ресурсоемкостью создания новых перспективных систем защиты и необходимостью оценки соответствия решений требованиям регуляторов. Как следствие, возникает нежелание разработчиков связываться с вопросами обеспечения безопасности, взаимодействовать с регулятором и приобретать соответствующую компетенцию.
Подобные проблемы существуют не только в нашей стране, но и за рубежом. Однако, активность в области разработки новых решений, внедрения новых стандартов и их применения в целевых системах за рубежом гораздо выше.

ТЕКУЩЕЕ СОСТОЯНИЕ И КЛЮЧЕВЫЕ ПРОБЛЕМЫ

Ресурсные ограничения устройств

На сегодняшний день подавляющее количество устройств, используемых в киберфизических системах, можно отнести к маломощным. Дефицит оперативной и постоянной памяти, низкая пропускная способность каналов обмена информацией и жесткие требования к энергопотреблению автономных устройств затрудняют использование классической асимметричной криптографии и технологий, построенных на ее основе, таких как PKI.
Альтернативой сегодня является использование низкоресурсных шифров (ГОСТ Магма или аутентифицированное шифрование Ascon).

Возможные угрозы из будущего на горизонте 10-15 лет

Для криптографических систем, в особенности оперирующих асимметричными алгоритмами, опасность в будущем представляют квантовые вычисления. Способность квантовых компьютеров к мгновенному разложению на множители больших чисел и решению ряда других задач, вычислительно сложных для традиционных компьютеров, может в перспективе обесценить существующие криптографические механизмы.
Постквантовые алгоритмы, устойчивые к квантовым вычислениям, требуют значительных ресурсов и не адаптированы для применения в киберфизических системах из-за малой вычислительной мощности большинства устройств. Рост вычислительных мощностей по закону Мура может не покрыть потребности противостояния квантовой угрозе на обозримом горизонте в 10-15 лет, если на данном интервале времени случится «квантовый прорыв».
Увеличение количества устройств в киберфизических системах, рост скоростей обмена информацией за счет применения новых технологий связи (5G+), применение технологий искусственного интеллекта приведут к росту поверхности атак из-за создания новых точек уязвимости и появления новых векторов атаки.

ОПИСАНИЕ ПРОЦЕССА ПРОВЕДЕНИЯ МЕРОПРИЯТИЯ

КОМПАНИЯ ПРАКТИВ

При подготовке форсайт-сессии участникам была предложена тема — «Будущее безопасности киберфизических систем в России. Перспективы и векторы развития». Участники могли заранее сформулировать вопрос, который они желали бы разобрать на сессии. Из поступивших вопросов организаторами было отобрано три, которые распределили по трём тактам сессии.

Группа активных участников состояла из 30 человек и была разделена на 4 подгруппы:

Криптография

Маркетинг

Бизнес и управление

Регуляторика

Участники сессии представляли разные сферы деятельности: **разработчики и производители средств защиты информации, представители технических комитетов и регулирующих органов, представители научной среды, представители бизнеса и государственных институтов.** Распределение участников по подгруппам прошло с учетом их пожеланий.

Поскольку некоторые участники были погружены в тематику поверхностно и большинство ранее не принимало участие в мероприятиях формата форсайт, организаторы подготовили один приветственный и три вступительных доклада. На первом докладе длительностью 10 минут освещалась тема мероприятия и связанная с ней проблематика. Второй доклад на 10 минут был посвящен текущим проблемам криптографии в киберфизических системах. Третий доклад на 25 минут делал модератор встречи, который рассказывал о целях и принципах форсайта, построении и модерации текущей сессии, структуре программы сессии, вопросах для предстоящей работы.

Помещение для работы представляло собой аудиторию ВУЗа МТУСИ, где для каждой группы были предоставлены столы с круговой посадкой, письменные принадлежности и флип-чарт для фиксации результатов работы каждой группы. Проводилась частичная видеофиксация работы групп и полная видеофиксация отчетов групп по результатам.

Активная работа участников была поделена на три такта. Во всех группах на каждом такте обсуждался один предварительно отобранный вопрос. Каждый такт предполагал 45-минутную работу над вопросом и фиксацию результатов в группах, после чего пятнадцать минут отводилось на доклады представителей групп. Таким образом, длительность каждого такта составляла один час, а продолжительность всего рабочего времени сессии составила 4 часа, включая вступительные доклады.

РАСПИСАНИЕ МЕРОПРИЯТИЯ

КОМПАНИЯ ПРАКТИВ

11:00–11:20	Приветствие и вводные доклады
11:20–11:35	Установочный доклад модератора
11:35–12:45	Работа в группах (такт 1) **Обсуждение итогов**
12:45–13:15	Обед
13:15–14:00	Работа в группах (такт 2) **Обсуждение итогов**
14:00–14:35	Работа в группах (такт 3) **Обсуждение итогов**
14:00–14:35	Финальное подведение итогов **Краткие выступления участников с предложениями по будущей совместной работе и закрытие форсайт-сессии**

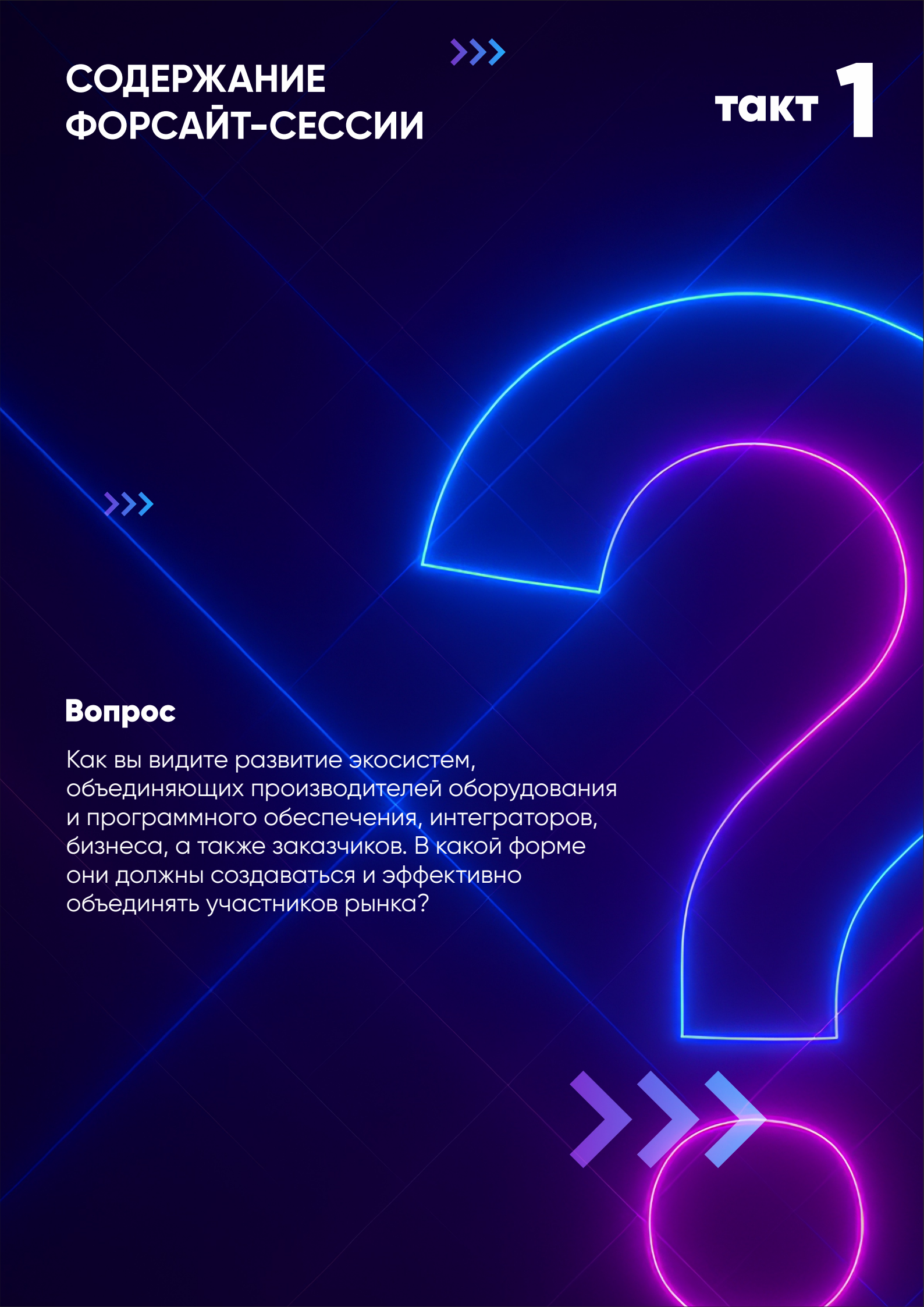
УЧАСТНИКИ ФОРСАЙТ-СЕССИИ

Модератором сессии выступил Вячеслав Марача — вице-президент Национальной Гильдии профессиональных консультантов.

Ступин Дмитрий	ведущий инженер-исследователь	НТУ «Сириус»
Шемякина Ольга	соруководитель рабочей группы «Криптографические механизмы для индустриальных систем» ТК26	ИнфоТеКС
Матреницкий Тимофей	директор по международным и специальным проектам	Компания «Актив»
Мытник Константин	начальник отдела разработки средств защиты информации и встроенного ПО	«НИИМЭ»
Дударев Дмитрий	исполнительный директор	Фирма «АНКАД»
Иванов Владимир	директор по развитию	Компания «Актив»
Исайкина Екатерина	директор по развитию и маркетингу	«С-Терра СиЭсПи»
Ищукова Евгения	доцент кафедры безопасности информационных технологий ИКТИБ ЮФУ	ИКТИБ ЮФУ
Карантаев Владимир	менеджер по анализу эффективного использования аппаратных средств Департамент перспективных технологий	Лаборатория Касперского
Кашаев Михаил	начальник отдела ИБ	Zelax
Колесников Андрей	директор	Ассоциация интернета вещей
Лазарев Алексей	руководитель департамента защиты киберфизических систем	Компания «Актив»
Лурье Мария	руководитель направления по работе с партнерами	«СпецИнт»
Манжура Юлия	начальник отдела отраслевого сотрудничества и взаимодействия с госсектором	«НИИМЭ»
Нагин Владимир	исполнительный директор	Майсимтех
Новоселов Александр	руководитель проектов по смарт-технологиям	«НИИМЭ»
Панасенко Сергей	директор по научной работе	Компания «Актив»
Парьев Сергей	руководитель группы разработки ПО	Лаборатория Касперского
Петренко Сергей	руководитель группы «Квантовая информатика и информационная безопасность»	НТУ «Сириус»
Попов Артем	руководитель проектов по развитию продаж	«НИИМЭ»
Правиков Дмитрий	директор	ЭнергоЦИБ Ассоциации «Цифровая энергетика»
Птуха Анастасия	председатель совета директоров	ГК Step by Step
Салманова Шахноз	начальник отдела маркетинга и внедрения	Фирма «АНКАД»
Степин Андрей	заместитель генерального директора по управлению	Компания «Актив»
Димитров Илия	исполнительный директор	Ассоциация Электронных Торговых Площадок: АЭТП
Марченко Марина	руководитель направления комплексных маркетинговых программ	Компания «Актив»
Короткова Наталья	руководитель направления маркетинга продукта Рутокен	Компания «Актив»
Сохадзе Кетеван	руководитель направления маркетинга Guardant	Компания «Актив»
Вершинина Екатерина	ведущий менеджер по связям с общественностью	Компания «Актив»

СОДЕРЖАНИЕ ФОРСАЙТ-СЕССИИ

такт 1



Вопрос

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?

такт 1

Вопрос

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?

КОМПАНИЯ ПРАКТИВ

ГРУППА КРИПТОГРАФИЯ

Для эффективного развития экосистем, объединяющих производителей оборудования, ПО, интеграторов, бизнес и заказчиков, необходимо учитывать следующие принципы:

1. **Классификация.**
   Киберфизические системы требуют четкой классификации из-за их разнообразия. Классификация возможна по отраслям, по принципу построения архитектуры, по необходимому уровню защиты.

2. **Упор на сотрудничество.**
   Участникам рынка важно осознавать взаимозависимость и активно создавать коллаборации. Успешным примером служит взаимодействие в рамках технических комитетов по стандартизации.

3. **Интеграция заказчиков в общий процесс.**
   Заказчики часто остаются вне общей экосистемы, так как их запросы разнонаправлены и не способствуют унификации. Это усугубляется наличием «зоопарка» аппаратных и программных решений, что осложняет разработку. Необходима тесная кооперация с заказчиками при разработке стандартов и решений на их основе.

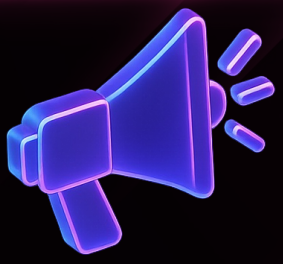
4. **Стимулирующая роль стандартизации и регуляторики.**
   Стандарты и регуляторные нормы отстают от рыночных и технологических реалий, хотя должны задавать вектор развития. Решением может стать гибкая стандартизация, ориентированная на перспективные технологии.

5. **Open source VS проприетарные решения.**
   Поддержка открытых решений (open source) способствует формированию коллабораций и развитию рынка, тогда как избыточное патентование и проприетарные решения создают барьеры. Нужно стараться на начальных этапах обеспечить доступ заинтересованным участникам. Это обеспечит необходимые для развития систем и рынка горизонтальные связи. Данное мнение выражено большинством участников группы, но не является консенсусным.

6. **Целевая сертификация и экспертиза.**
   Требовать полной сертификации всех компонентов следует только в случаях, когда это прямо предусмотрено законом. При этом критически важна отраслевая экспертиза применения криптографических средств, чтобы избежать ошибок в их внедрении.

7. **Ориентация на успешные модели.**
   Отраслевые экосистемы (банки, телекоммуникации) демонстрируют эффективные подходы, которые стоит адаптировать для киберфизических систем.

8. **Разумное импортозамещение.**
   Необходимо избегать тотального замещения зарубежных решений, выбирая лучшие мировые практики и интегрируя их в локальные разработки. Таким образом, развитие экосистем требует баланса между стандартизацией, открытыми технологиями, гибким регулированием и ориентацией на проверенные отраслевые модели.



такт **1**

Вопрос

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?

КОМПАНИЯ ФРАКТИВ

ГРУППА МАРКЕТИНГ

Для создания эффективных экосистем, объединяющих производителей оборудования и ПО, интеграторов, бизнес, заказчиков, регуляторов и технологических лидеров, группа маркетинга предлагает следующую стратегию:

1. Определение экосистемы.
Экосистема рассматривается как сообщество участников, связанных общей технологической идеей или результатом. Ключевые элементы включают не только базовых игроков (производителей, интеграторов), но и регуляторов, крупных технологических лидеров, а также заказчиков, которые выступают как «поле» для внедрения решений и драйвер развития через понимание их потребностей.

2. Роль регулятора.
В условиях зарегулированного рынка криптосистем регулятор становится центральным звеном, инициирующим объединение участников. Предлагается модель «полурегулируемого рынка», где регулирование сочетается с гибкостью, позволяя адаптироваться к быстро меняющимся технологическим реалиям.

3. Использование маркетинговых инструментов:

- **Кросс-маркетинг.**
  Участники экосистемы совместно продвигают свои решения, усиливая взаимную ценность.
- **Популяризация технологий.**
  Формирование комьюнити с лидерами мнений для демистификации киберфизических систем, устранения стереотипов («теорий заговора») и повышения доверия.
- **Развитие регуляторики.**
  Активное участие в создании норм, которые не ограничивают, а стимулируют рыночный рост.

4. Создание сообщества.

- **Формирование ядра из экспертов**, технологических лидеров и регуляторов для координации развития.
- **Вовлечение заказчиков** через решение их конкретных проблем, что превращает их из пассивных в активных участников экосистемы.
- **Использование образовательных и информационных кампаний** для расширения аудитории за пределы узкого рынка информационной безопасности.

5. Расширение границ.
Киберфизические системы должны выйти за рамки текущего рынка, что требует продвижения их ценности для смежных отраслей. Лидеры мнений и эксперты играют ключевую роль в этом процессе, переводя сложные технологии в понятные и востребованные решения.

Успешная экосистема строится на балансе регулирования, кросс-коллабораций, активного маркетинга и сильного сообщества. Её цель — не только объединить участников, но и создать устойчивую среду, где технологии воспринимаются как надежный инструмент, а не как «закрытая» или пугающая инновация.

такт 1

Вопрос

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?

КОМПАНИЯ ПРАКТИВ

БИЗНЕС И УПРАВЛЕНИЕ

Группа бизнеса выделяет следующие ключевые аспекты формирования экосистем, объединяющих производителей оборудования, интеграторов, заказчиков и регуляторов:

ОСНОВНЫЕ УЧАСТНИКИ И ИХ ВЗАИМОДЕЙСТВИЕ

1. Ядро экосистемы:

- Производители ИБ (информационной безопасности), интеграторы, регуляторы (например, ФСБ, Роскомнадзор) и операторы киберфизических систем (коммунальные компании, управляющие сети и др.).
- Технический комитет 194 — пример успешной площадки, где эксперты рынка и регуляторы совместно разрабатывают стандарты для киберфизических систем.

2. Драйверы развития:

- Взаимодействие рынка и регулятора — ключевой механизм, обеспечивающий гармонизацию требований и стимулирующий инновации.
- Бизнес-интересы: возможность монетизации решений через создание стандартов и внедрение защищенных технологий.

ПРОБЛЕМЫ ТЕКУЩЕЙ МОДЕЛИ

1. Выпадение заказчиков и операторов:

- Потребители (операторы) часто остаются вне экосистемы, так как текущие решения не всегда помогают им экономить ресурсы или решать конкретные задачи (например, защита от хищений данных).
- Производители оборудования (например, для инфраструктуры: кабели, датчики) также не всегда интегрированы в процессы стандартизации.

2. Неоднозначность состава рынка ИБ:
Кто входит в рынок ИБ? Только производители и интеграторы или также заказчики и операторы? Необходимо включить в экосистему все звенья цепочки: от разработчиков «железа» до конечных пользователей.

ПРЕДЛОЖЕНИЯ ПО ОПТИМИЗАЦИИ

1. Расширение взаимодействия:

- Активное вовлечение операторов и заказчиков в работу технических комитетов (например, ТК 194) для учета их потребностей.
- Гармонизация интересов. Создание решений, которые не только соответствуют регуляторным нормам, но и приносят экономическую выгоду операторам.

2. Четкое определение ролей:

- Уточнение состава участников рынка ИБ, включая производителей инфраструктурного оборудования (датчики, кабели и др.).
- Разделение зон ответственности между регуляторами для избежания дублирования требований.

3. Фокус на практическую ценность:

- Разработка технологий, которые напрямую решают проблемы операторов (например, защита от утечек данных, оптимизация затрат).
- Продвижение успешных кейсов, демонстрирующих выгоду внедрения киберфизических систем.

Успешная экосистема должна:

- **Объединять всех участников цепочки (производителей «железа», интеграторов, регуляторов, операторов).**
- **Базироваться на практико-ориентированных стандартах (через площадки типа ТК 194).**
- **Обеспечивать экономическую выгоду для заказчиков, мотивируя их к участию.**

Это позволит достичь баланса между регуляторными требованиями, бизнес-интересами и реальными потребностями рынка.

такт **1**

Вопрос

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?

КОМПАНИЯ АКТИВ

ГРУППА РЕГУЛЯТОРИКА

Развитие экосистем: регуляторные аспекты и стандартизация. Для создания эффективных экосистем, объединяющих производителей, интеграторов, бизнес и заказчиков, группа регуляторики выделяет следующие ключевые проблемы и пути их решения:

1. **Регулирование в критических областях.** Многие направления, такие как системы видеонаблюдения, практически не регулируются. Например, существующие нормы ограничиваются лишь запретом на нарушение приватности, но не регламентируют использование технологий (например, камеры у критических объектов без четких правил их использования). Необходимо выявлять и своевременно закрывать «регуляторные дыры».
2. **Снижение неопределенности требований и страха перед регулятором.** Заказчики не инвестируют в защиту из-за неопределенности требований, а производители избегают инноваций из-за страха перед регуляторами. Популяризация успешных кейсов, связанных со взаимодействием с регулятором, могла бы «прокачать обе стороны». Отказ от избыточных требований регуляторики в конкретных отраслях, кроме случаев, прямо указанных в законе. Фокус на «разумное регулирование», где нормы стимулируют, а не тормозят развитие.
3. **Уход от устаревших стандартов.** Даже при наличии стандартов (например, криптографических) продукты разных производителей остаются несовместимыми. Действующие нормы регуляторики разрабатывались для других условий применения, нежели киберфизические системы, где существует ряд очевидных потребностей, которые текущая регуляторная база не позволяет реализовать. Создание межотраслевых стандартов (например, для совместимости криптомодулей в киберфизических системах) с учетом опыта успешных кейсов (например, стандарт CRISP от ИнфоТеКС, объединивший разработчиков микрочипов). Нужно стараться использовать международный опыт из аналогичных областей (например, систем учета энергоресурсов по модели ИСУЭ). Пересмотр устаревших норм и адаптация их под текущие технологические реалии.
4. **Устранение расхождения в базовых принципах и понятиях регуляторов и институций.** Регуляторы, действуя в рамках своих полномочий и соблюдая границы своей ответственности, часто работают обособленно. Это может приводить к противоречивым требованиям, особенно в условиях постоянно растущей нагрузки. Возникает необходимость создания институции, гармонизирующей нормативную базу, начиная с терминологии, заканчивая классификацией объектов, угроз, принимаемых мер. Хороший пример гармонизации — ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения» - результат совместной работы Технических комитетов по стандартизации № 362 и № 26 фактически устранивший разногласия в терминологическом плане.
5. **Повышение эффективности экспертных площадок.** Экспертные площадки и технические комитеты (например, по стандартизации) недостаточно эффективны из-за отсутствия запросов от рынка. Нужна активизация экспертных площадок в направлении стимулирования взаимодействия между техническими комитетами, производителями и интеграторами через запросы от рынка.
6. **Уход от «бумажной безопасности» в сторону решения реальных задач.** Соблюдение формальных норм часто не позволяет выпускать конкурентоспособные продукты, удовлетворяющие реальным потребностям стейкхолдеров. Создание гибкой нормативной базы под массовое внедрение криптографии, включая правила интеграции, отчетности и сертификации. Создание направления «гражданской криптографии» там, где кроме интересов бизнеса нет других уязвимых сущностей.

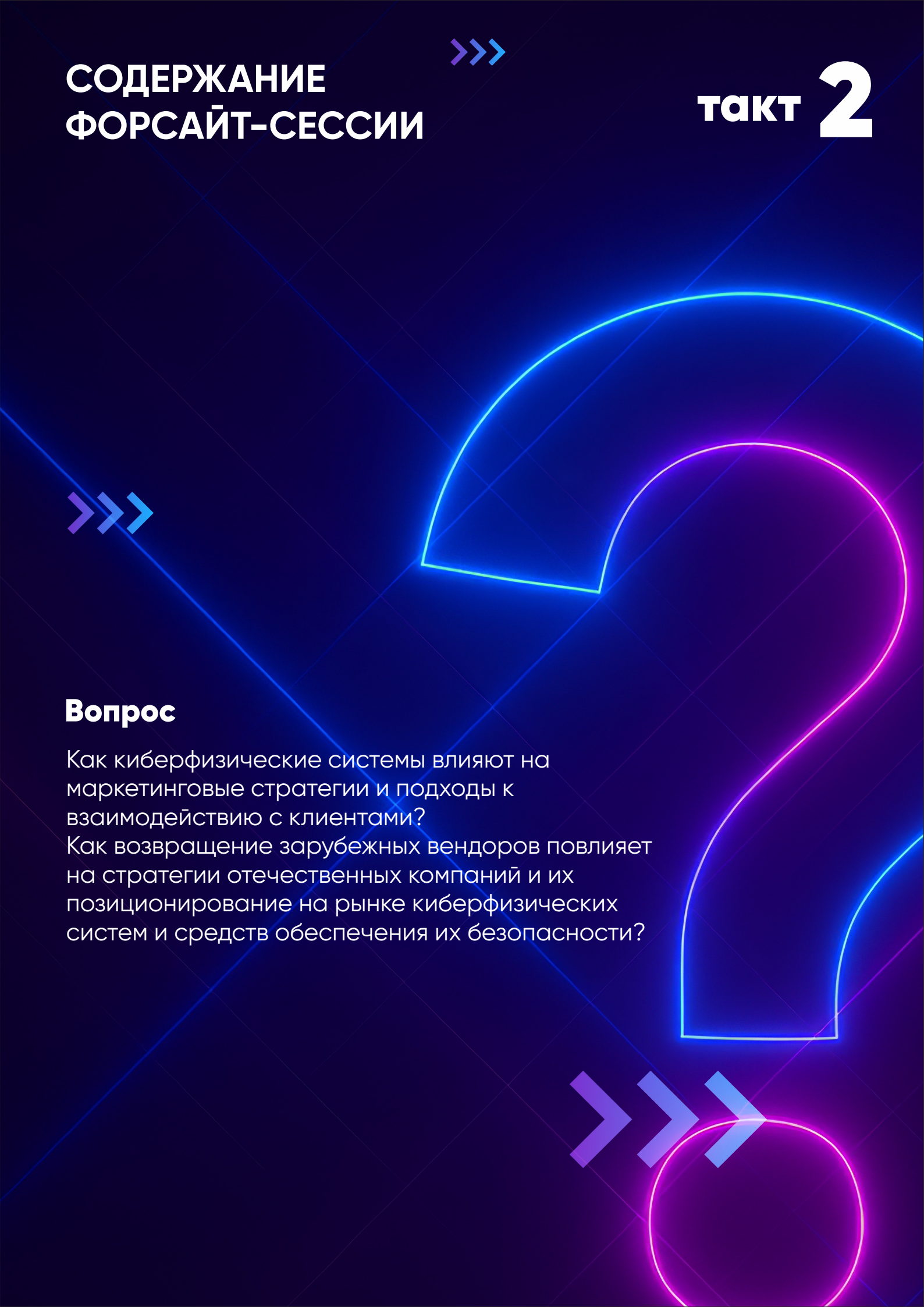
Успешная экосистема требует:

- **Единых гармонизированных стандартов для совместимости решений.**
- **Скоординированной работы регуляторов и участников рынка.**
- **Гибкой нормативной базы, обновляемой с учетом технологических трендов.**
- **Практико-ориентированных норм на смену «бумажной безопасности».**

Это позволит в обозримом горизонте в 5-10 лет создать среду, где регуляторика становится не барьером, а драйвером для развития защищенных и конкурентоспособных решений. Для этого необходима решительность к активным действиям всех участников рынка.

СОДЕРЖАНИЕ ФОРСАЙТ-СЕССИИ

такт 2



Вопрос

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?

такт **2**

Вопрос

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?

КОМПАНИЯ ФРАКТИВ

ГРУППА МАРКЕТИНГ

ВЛИЯНИЕ КИБЕРФИЗИЧЕСКИХ СИСТЕМ НА МАРКЕТИНГОВЫЕ СТРАТЕГИИ И ВЗАИМОДЕЙСТВИЕ С КЛИЕНТАМИ

1. Адаптация маркетинга к реалиям киберфизических систем

- **Киберфизические системы** же стали неотъемлемой частью промышленности, логистики, энергетики и других отраслей. Их повсеместное распространение требует пересмотра маркетинговых подходов.
- **Диверсификация** продуктов из-за большого разнообразия решений на рынке клиентам сложно ориентироваться в предложениях. Компаниям необходимо четко дифференцировать свои продукты, подчеркивая уникальные преимущества (например, интеграция с криптографией, безопасность, совместимость).
- **Переход от продажи технологий к решению проблем.** Акцент в маркетинге смещается на демонстрацию практической ценности КФС для конкретных задач клиентов (оптимизация процессов, снижение издержек, защита данных).

2. Возвращение зарубежных вендоров, риски и возможности для российских компаний

- **Текущая ситуация:** Зарубежные вендоры формально ушли с рынка, но их решения остаются в эксплуатации. Поддержка осуществляется через интеграторов и третьи страны (обновление лицензий, неофициальные каналы).
- **Последствия возвращения:**
  - **Рост конкуренции.** Крупные иностранные компании обладают ресурсами для агрессивного маркетинга и продвижения.
  - **Давление на отечественные решения.** Потребители могут отдать предпочтение проверенным зарубежным брендам.

3. Стратегии для российских производителей

- **Патриотическое позиционирование:** Упор на поддержку локальной экономики («покупая наш продукт, вы кормите российских инженеров»).
- **Регуляторные преимущества:** Использование требований законодательства (например, обязательное применение отечественных решений в госзакупках).
- **Акцент на безопасность:** Продвижение КФС с «защитой от санкционных рисков» и полным контролем над цепочкой поставок.

КЛЮЧЕВЫЕ ВЫВОДЫ

ДЛЯ МАРКЕТИНГА КИБЕРФИЗИЧЕСКИХ СИСТЕМ:

- **Сфокусироваться на образовании клиентов:** объяснять сложные технологии через понятные кейсы.
- **Создавать нишевые предложения** для разных отраслей: логистика, энергетика, промышленность.

ДЛЯ КОНКУРЕНЦИИ С ЗАРУБЕЖНЫМИ ВЕНДОРАМИ:

- **Усилить PR-кампании,** подчеркивающие технологический суверенитет («патриотическое позиционирование»).
- **Развивать сервисную поддержку** и долгосрочные партнерства с клиентами.
- **Инвестировать в R&D**, чтобы закрыть функциональные разрывы между российскими и иностранными решениями.

Киберфизические системы меняют правила игры, требуя от компаний гибкости и клиентоориентированности. Возвращение зарубежных игроков — это не только вызов, но и возможность для отечественных производителей укрепить позиции через уникальное позиционирование и регуляторную поддержку.

такт 2

Вопрос

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?

КОМПАНИЯ ПРАКТИВ

БИЗНЕС И УПРАВЛЕНИЕ

КЛЮЧЕВЫЕ АСПЕКТЫ СТРАТЕГИИ ДЛЯ ЗАПУСКА «ОБЯЗАТЕЛЬНОГО» ПРОДУКТА

1. Фокус на будущие потребности:

- Продукт создается под будущие регуляторные требования, а не текущий спрос. Задача маркетинга — формировать потребность у клиентов, объясняя, почему решение станет необходимым (например, через прогнозы законодательных изменений, риски несоответствия).
- Акцент на долгосрочное видение (10+ лет), включая переход от закрытых систем к открытым экосистемам.

2. Оптимизация маркетингового бюджета:

- Перераспределение ресурсов на анализ конкурентов и рынка. Даже при «обязательности» продукта сохраняется риск конкуренции с аналогами.
- Усиление позиций через превентивное изучение слабых сторон конкурентов и нишевых возможностей.

3. Партнерские стратегии:

- Co-branding и партнерский маркетинг. Создание альянсов с производителями, интеграторами и другими участниками цепочки для продвижения продукта как части экосистемы.
- Совместные предложения. Упаковка решения в комплексы с дополнительными услугами (например, обучение, интеграция, поддержка).

4. Стимулирование спроса:

- Финансовые инструменты. Введение баллов для клиентов, которые приобретают продукт заранее.
- Прагматичный подход к патриотизму. Акцент не на эмоциональные лозунги, а на экономическую выгоду — например, «покупая наш продукт, вы получаете гарантию соответствия будущим стандартам и избегаете штрафов».

РИСКИ И ВОЗМОЖНОСТИ ПРИ ВОЗВРАЩЕНИИ ЗАРУБЕЖНЫХ ВЕНДОРОВ

Угрозы:

- Конкуренция с технологическими гигантами, обладающими ресурсами для агрессивного продвижения.
- Риск устаревания отечественных решений, если не будет инвестиций в R&D.

Преимущества:

- Укрепление позиций через регуляторную поддержку (например, обязательное использование локальных решений в госсекторе).
- Возможность занять нишу «безопасных» решений с полным контролем над цепочкой поставок.

РЕКОМЕНДАЦИИ

- Инвестиции в образование рынка: вебинары, кейсы, прогнозы — материалы, которые готовят клиентов к будущим изменениям.
- Формирование стандартов. Участие в разработке регуляторных норм для закрепления преимуществ отечественных продуктов.
- Гибкость маркетинга. Готовность адаптировать коммуникации под меняющиеся условия (например, возврат зарубежных игроков).

Успех зависит от способности сочетать формирование регуляторной среды с учетом текущих трендов, партнерские коллаборации и клиентоориентированный подход, превращая «обязательность» использования продукта в конкурентное преимущество.

такт 2

Вопрос

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?

КОМПАНИЯ ПРАКТИВ

ГРУППА РЕГУЛЯТОРИКА

УСЛОВИЯ ВОЗВРАЩЕНИЯ ЗАРУБЕЖНЫХ ВЕНДОРОВ

1. Локализация производства:

- Возвращение иностранных компаний должно сопровождаться обязательной локализацией критических компонентов (например, криптографических модулей) на территории России.
- Даже формальное требование к локализации («на бумаге») может стать барьером для недобросовестных игроков.

2. Экономические механизмы регулирования:

- Введение налоговых стимулов для отечественных производителей:
- Ускоренная амортизация российских решений (сокращение сроков списания с 5 до 1 года).
- Субсидии или компенсации из госбюджета для компаний, выбирающих локальные продукты.
- Увеличение стоимости ввоза зарубежных решений через таможенные пошлины или административные барьеры.

3. Экспертные оценки рисков:

- Создание системы оценки «уровня недоверия» к иностранным вендорам, основанной на анализе их прошлых действий (например, внезапный уход с рынка в «трудные моменты»).
- Регуляторный контроль за соблюдением требований к безопасности и прозрачности цепочек поставок.

РИСКИ ДЛЯ ОТЕЧЕСТВЕННОГО РЫНКА

1. Давление на локальных производителей:

- Зарубежные компании (например, Cisco) могут вернуться с агрессивной ценовой политикой, что угрожает конкурентоспособности российских решений.
- Пример из прошлого: неконтролируемый ввоз мобильных телефонов, которые не соответствовали нормативным требованиям, но заполонили рынок из-за отсутствия своевременного регулирования.

2. Технологическая зависимость:

- Некоторые критически важные технологии (например, компоненты для КФС) пока не могут быть замещены отечественными аналогами.

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ РЫНКА

1. Баланс между открытостью и защитой:

- Не допускать полного закрытия рынка, но создать условия, при которых иностранные компании будут вынуждены инвестировать в локальную экосистему (например, через совместные предприятия).

2. Долгосрочное регулирование:

- Учесть уроки прошлых ошибок (например, с мобильными телефонами) и заранее разработать стандарты для новых технологий.
- Внедрить «умные» регуляторные рамки, которые адаптируются к изменению рыночных условий.

3. Поддержка отечественных разработок:

- Стимулировать НИОКР через гранты, налоговые льготы и госзаказы.
- Продвигать российские решения как «страховку» от санкционных рисков и гарантию стабильности.

Возвращение зарубежных вендоров требует:

• Прецизионных регуляторных мер (локализация, налоги, экспертиза рисков).

• Системной поддержки отечественных производителей через экономические инструменты и долгосрочное планирование.

• Упреждающих мер для предотвращения повторения сценариев, когда рынок захлестывают нерегулируемые иностранные продукты.

Главная цель — создать среду, где киберфизические системы развиваются без ущерба для технологического суверенитета, а регуляторика становится инструментом защиты, а не бюрократическим барьером.

такт **2**

Вопрос

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?

КОМПАНИЯ АКТИВ

ГРУППА КРИПТОГРАФИЯ

РОЛЬ ОБРАЗОВАНИЯ И КАДРОВОЙ ПОДГОТОВКИ В РАЗВИТИИ ЭКОСИСТЕМ

Примечание. Группа решила вместо поставленного вопроса продолжить обсуждение развития экосистем в части образования и подготовки кадров, поскольку в первом такте им не было уделено внимание.

Киберфизические системы, объединяющие вычислительные и физические компоненты, требуют специалистов, способных работать с IoT, AI, Big Data и другими инновационными технологиями. Однако система образования отстает от динамики технологического развития:

• **Проблемы образования.** Отсутствие актуальных профстандартов и программ, учитывающих специфику КФС. Например, подготовка специалистов по безопасной разработке продуктов или исследованию киберфизической безопасности остается ограниченной.

• **Сотрудничество с вузами:**

• Создание **совместных программ** с компаниями для обучения студентов на реальных задачах (например, проектирование умных производственных линий или оптимизация энергосетей).

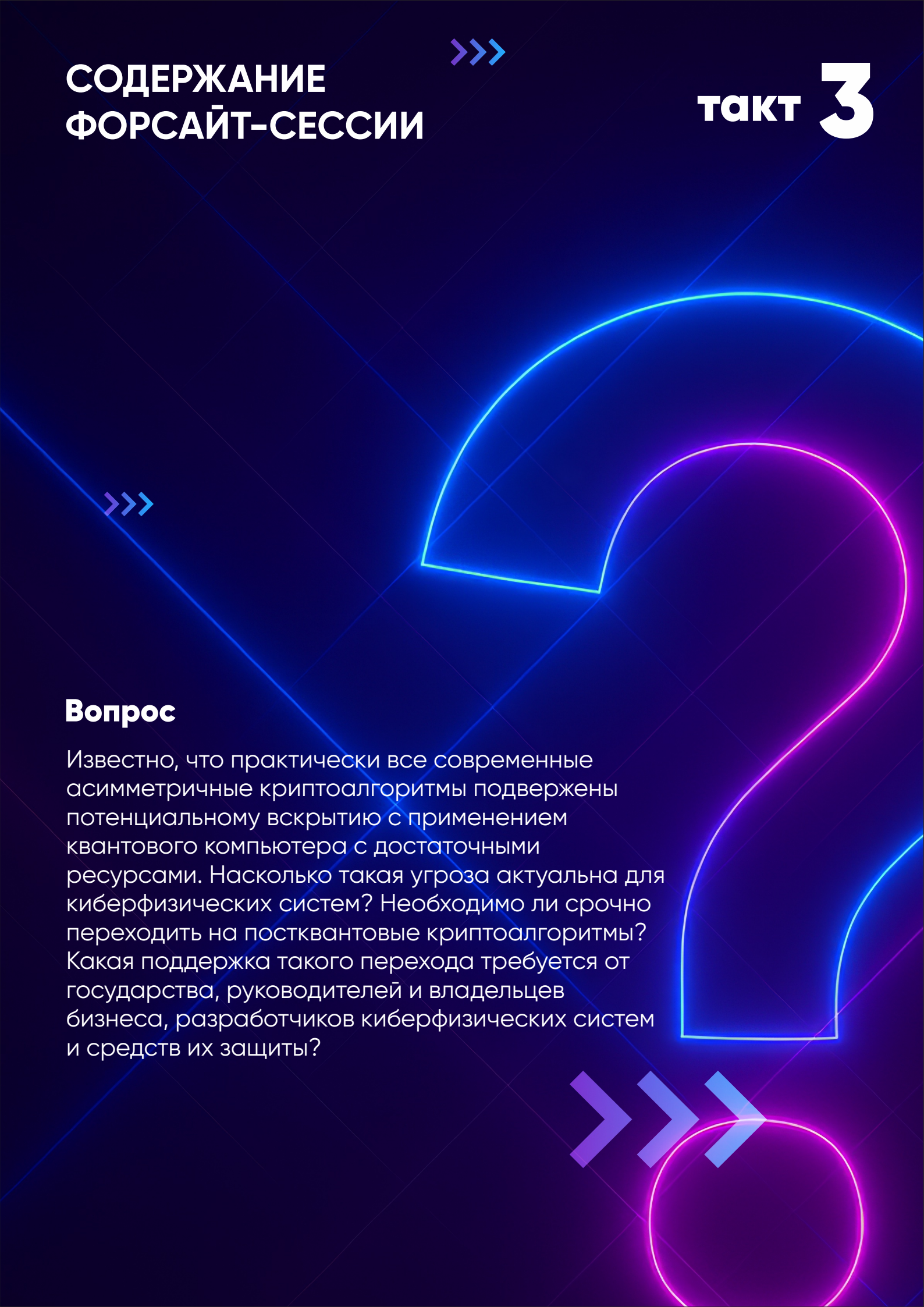
• **Практики на предприятиях:** Погружение студентов в работу с оборудованием и ПО, используемым в КФС (датчики, системы управления, облачные платформы).

• **Продвижение продукции через образование:** Предоставление вузам технологий для обучения (например, ПО для моделирования производственных процессов) формирует лояльность будущих специалистов и усиливает бренд компании.

Пример:
Проведение хакатонов или соревнований (региональных/международных) с использованием продуктов компании. Это не только стимулирует инновации, но и служит инструментом маркетинга, демонстрируя преимущества решений.

СОДЕРЖАНИЕ ФОРСАЙТ-СЕССИИ

такт 3



Вопрос

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?

такт 3

Вопрос

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?

КОМПАНИЯ АКТИВ

ГРУППА КРИПТОГРАФИЯ

Угроза вскрытия асимметричных криптоалгоритмов с использованием квантовых компьютеров для киберфизических систем на горизонте 5–10 лет оценивается как слабо актуальная. Однако переход на постквантовую криптографию и квантовое распределение ключей требует поэтапного подхода:

1. Верхние уровни систем (серверы, ЦОДы, где сосредоточены большие объемы данных и вычислительные ресурсы):

- Переход на постквантовые алгоритмы и квантовое распределение ключей необходимо начинать уже сейчас.
- Рекомендуется комбинировать квантовое распределение ключей с симметричной криптографией, так как это обеспечивает защиту в условиях квантовых угроз.

2. Низкоресурсные устройства (открытые компоненты киберфизических систем):

- Переход можно отложить на 10 лет (и осуществлять его постепенно) из-за длительного цикла внедрения и текущих ограничений по вычислительной мощности.
- Для таких устройств актуальна постквантовая криптография, которая постепенно станет менее ресурсоемкой по мере развития технологий. С другой стороны, возможно увеличение ресурсов устройств КФС с течением времени в рамках действия «закона Мура» и ЗРТС (законы развития технических систем).

КЛЮЧЕВЫЕ ПРИНЦИПЫ ПЕРЕХОДА:

1. Риск-ориентированный подход:

- Анализ стоимости данных и потенциальных атак для определения целесообразности перехода.
- Оценка актуальности угроз через 10 лет с учетом динамики развития систем и данных.

2. Исторический контекст:

- Аналогия с развитием традиционной асимметричной криптографии, которая 30 лет назад также считалась ресурсоемкой, но стала массово применяться по мере роста вычислительных мощностей.

3. Стандартизация:

- Активная разработка и совершенствование стандартов постквантовой криптографии, включая оптимизацию их ресурсоемкости.

РЕКОМЕНДАЦИИ ДЛЯ УЧАСТНИКОВ РЫНКА:

1. Государство:

- Поддержка разработки и внедрения стандартов через финансирование исследований и регуляторные инициативы.

2. Бизнес и руководители:

- Планирование долгосрочной стратегии перехода, начиная с критически важных систем.

3. Разработчики:

- Интеграция постквантовых алгоритмов в продукты с учетом их эволюции и снижения ресурсопотребления.

Переход на постквантовую криптографию для киберфизических систем требует поэтапного, взвешенного подхода с фокусом на верхние уровни инфраструктуры. Угрозы носят долгосрочный характер, но подготовка должна начинаться уже сейчас.

такт 3

Вопрос

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?

ГРУППА РЕГУЛЯТОРИКА

Угроза вскрытия асимметричных криптоалгоритмов квантовыми компьютерами для киберфизических систем на текущий момент носит скорее **хайповый характер**, однако риск технологического скачка, при котором квантовые компьютеры смогут быстро взламывать ключи, **существует**. Вероятность реализации такой угрозы в ближайшие 10 лет оценивается как **малая, но не нулевая**, особенно для систем с длительным сроком эксплуатации.

Для смягчения рисков предлагаются следующие меры:

1. Временные решения:

- Увеличение размера ключей в существующих алгоритмах для повышения их устойчивости.
- Постепенная замена алгоритмов в работающих системах по мере развития технологий и стандартов.

2. Crypto Agility:

- Внедрение архитектурной гибкости (Crypto Agility) в киберфизические системы, позволяющей быстро заменять криптографические модули (например, алгоритмы или ключи) без перепроектирования всей системы.
- Пример: Возможность «вытащить» текущий криптомодуль и заменить его новым (включающим постквантовые алгоритмы) через обновление ПО.

3. Регуляторные требования:

- Закрепление принципа Crypto Agility в нормативных документах для критически важных объектов (КИИ первой категории, особо опасных производств).
- Создание стандартов, обязывающих разработчиков предусматривать гибкость криптографических решений на этапе проектирования систем.

Переход на постквантовые алгоритмы не требует срочных мер для большинства систем, но критически важные объекты должны быть готовы к быстрой адаптации. Основная задача — заложить гибкость в архитектуру и регуляторику, чтобы минимизировать отрицательные последствия при будущих изменениях.

такт 3

Вопрос

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?

ГРУППА МАРКЕТИНГ

Угроза взлома асимметричных криптоалгоритмов квантовыми компьютерами для киберфизических систем на горизонте 10+ лет оценивается как малоактуальная, но риск технологического скачка, способного изменить ситуацию, исключать нельзя.

КЛЮЧЕВЫЕ АСПЕКТЫ:

1. Текущая оценка угрозы:

- Большинство экспертов считают, что угроза носит **хайповый характер**, а её реализация маловероятна в ближайшие 10 лет.
- Однако долгосрочные системы (срок эксплуатации 20–30 лет) требуют учета потенциальных рисков.

2. Меры по смягчению рисков:

- **Временные решения**: Увеличение длины ключей в существующих алгоритмах.
- **Crypto Agility:** Внедрение архитектурной гибкости для быстрой замены криптомодулей (алгоритмов, ключей) без перепроектирования системы.
- Пример: Возможность удаленной аттестации состояния системы (целостность, аутентичность компонентов).

3. Регуляторные и методические пробелы:

- Отсутствие общедоступных стандартов, позволяющее разработчикам оценить качество реализации криптографии и сопутствующих механизмов (безопасное хранение ключей, соответствие реализации в плане корректности, допустимость оптимизации под типовые платформы).
- Необходимость сертификации или иных форм проверки, особенно для критически важных объектов (энергосистемы, агропромышленные комплексы).

4. Поддержка перехода:

- **Финансирование:** Отсутствие венчурных программ и субсидий для разработки постквантовых решений.
- **Прогнозирование:** Требуется сценарный анализ последствий кибератак на физические процессы (точность энергосистем, функциональность автоматики).

5. Проблемы реализации:

- **Недостаток исследований:** Зарубежные коллеги фокусируются на анализе последствий атак, а не на вероятности их реализации.
- **Качество криптографии:** Использование западных решений с непрозрачной реализацией (например, единые ключи для тысяч устройств).

РЕКОМЕНДАЦИИ:

- Разработать долгосрочные прогнозы (20–30 лет) для технологий киберфизических систем.
- Закрепить регуляторные требования к Crypto Agility для критической инфраструктуры.
- Создать механизмы финансирования R&D, включая венчурные программы и субсидии.

Срочный переход на постквантовые алгоритмы не требуется, но критически важно заложить основу для будущей адаптации через гибкие архитектуры, регуляторные стандарты и поддержку разработчиков.

такт 3

Вопрос

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?

БИЗНЕС И УПРАВЛЕНИЕ

Угроза взлома асимметричных криптоалгоритмов квантовыми компьютерами для киберфизических систем на горизонте 10+ лет оценивается как малоактуальная, однако долгосрочные риски требуют стратегического планирования.

КЛЮЧЕВЫЕ АСПЕКТЫ:

1. Текущая оценка угрозы:

- Реализация квантовой угрозы в ближайшее время маловероятна, но исключать её полностью нельзя.
- Примеры из истории (например, кризис 2008 года) показывают, что непредсказуемые события («чёрные лебеди») могут кардинально изменить правила игры.

2. Технологические вызовы:

- Квантовые компьютеры: Серийные технологии (например, фотонные сопроцессоры) уже демонстрируют превосходство в вычислительной мощности (на 8 порядков) при меньшем энергопотреблении.
- Альтернативные подходы: Возвращение к троичной логике (вместо бинарной) или другим нестандартным решениям может открыть новые возможности, но требует тщательного анализа рисков и ограничений.

3. Проблемы текущих IT-систем:

- Статичность. 98% информационных систем — это системы учёта (1С, ERP), что противоречит динамической природе реальных процессов.
- Энергозатратность. Рост потребления энергии (например, для Big Data и нейросетей) ставит под вопрос устойчивость развития.
- Устаревшие парадигмы. Текстоцентричные интерфейсы и линейная логика не соответствуют человеческому восприятию (образы, звуки, эмоции).

4. Стратегии адаптации:

- Шокоустойчивость (resilience). Необходимость создания систем, способных адаптироваться к непредсказуемым изменениям (например, санкции, уход зарубежных вендоров).
- Crypto Agility. Внедрение гибких архитектур для быстрой замены криптоалгоритмов.
- Оригинальные разработки. Акцент на создание принципиально новых технологий (например, динамических систем управления), а не копирование западных решений.

5. Поддержка перехода

Государство

- Снижение регуляторного давления на бизнес.
- Финансирование фундаментальных исследований (например, фотонных процессоров, альтернативных логик).

Бизнес

- Переход от систем учёта к динамическим моделям.
- Инвестиции в R&D с фокусом на энергоэффективность.

РЕКОМЕНДАЦИИ:

Для разработчиков

- Изучать опыт прошлого (например, троичные системы 80-х) для поиска альтернатив.
- Внедрять принципы «шокоустойчивости» в архитектуру систем.

Для государства

- Создать условия для венчурного финансирования инновационных проектов.
- Поддержать разработку отечественных стандартов, не зависящих от западных технологий.

Переход на постквантовые алгоритмы не требует срочных мер, но критически важно заложить основу для будущего через гибкие архитектуры, оригинальные разработки и адаптацию к неопределённости. Россия может занять нишу в создании принципиально новых решений, если сосредоточится на динамических, энергоэффективных и человекоориентированных системах.

ОБЩИЕ ИТОГИ ВСТРЕЧИ. СТРАТЕГИИ ДОСТИЖЕНИЯ БЕЗОПАСНОГО БУДУЩЕГО

КОМПАНИЯ АКТИВ

1 **Security-by-Design как норма:**
Интеграция защиты на этапе проектирования, а не постфактум.

2 **Формирование и развитие стандартов**
на базе технических комитетов в коллаборации с производителями и заказчиками.

3 **Международная кооперация в стандартизации.**
Зарубежный пример успешного взаимодействия - конкурсы NIST.

4 **Создание экспертного сообщества**
с привлечением представителей ключевых стейкхолдеров (производители, регуляторы, заказчики).

5 **Развитие гибкой, адаптивной, наращиваемой экосистемы**
с непротиворечащими интересам участников правилами и инструментами взаимодействия.

6 **Низкоресурсная и постквантовая криптография:**
Инвестиции в разработку алгоритмов, совместимых с ограничениями КФС (например, легковесные шифры, гибридные схемы).

7 **Аппаратная безопасность на основе аппаратных корней доверия.**
Массовое внедрение чипов с криптографическими модулями на уровне кремния и защитой от физического взлома.

8 **Регуляторные меры и образование:**

a. Жесткие требования к сертификации КФС для критической инфраструктуры.

b. Послабления для отдельных областей гражданской инфраструктуры и некритичных объектов. Гражданская отечественная криптография на замену зарубежной криптографии.

c. Подготовка специалистов на стыке кибербезопасности, инженерии и Data Science.

9 **ИИ и автоматизация защиты.**
Использование машинного обучения для прогнозирования атак и анализа аномалий в режиме реального времени.

Будущее КФС зависит от способности преодолеть разрыв между инновациями и обеспечением безопасности. Успех потребует не только технологических прорывов, но и изменения культуры проектирования, где защита станет неотъемлемой частью системы, а не запоздалым дополнением. Это позволит создать устойчивые к угрозам киберфизические экосистемы, способные обеспечить прогресс без компромиссов.

ОСНОВНЫЕ ТРЕНДЫ И ВОЗМОЖНЫЕ СОБЫТИЯ ДЛЯ ПРОРАБОТКИ НА КАРТЕ БУДУЩЕГО

КОМПАНИЯ ФРАКТИВ

ТРЕНДЫ

СИСТЕМНЫЕ:

- Рост поверхности атак.
- Увеличение количества устройств, требующих защиты.
- Рост дефицита специалистов по безопасности (разработка, интеграция). Особенно, специалистов на стыке знаний ИБ и целевой технологии.

ТЕХНОЛОГИЧЕСКИЕ:

- Увеличение скорости обработки информации в целевых системах.
- Технологическое отставание в развитии средств защиты от целевых систем.
- Отставание по темпам развития средств защиты от целевых систем.
- Рост сферы применения ИИ для прогнозирования атак и анализа аномалий в реальном времени.

РЕГУЛЯТОРНЫЕ:

- Увеличение количества обращений производителей целевых систем на сертификацию к регулятору.
- Снижение строгости требований регулятора для отдельных применений.
- Увеличение активности регулятора на критически важных и перспективных направлениях.

ДИКИЕ КАРТЫ

- «Квантовый прорыв».
- Возврат иностранных компаний на правах до СВО.
- Возрождение в России массового производства чипов по полному циклу.
- Война.
- Новая пандемия.
- Экономические дефолты крупных государств.
- Государственные перевороты и революции.
- Исчерпание или появление острого дефицита критически-важных сырьевых ресурсов.

КОМПАНИЯ АКТИВ

По вопросам сотрудничества в области киберфизических систем и участия в форсайт-сессиях обращайтесь к

Наталье Коротковой,

руководителю направления маркетинга продукта Рутокен, Компания «Актив»

korotkova@aktiv-company.ru

+7 929 674 3323