



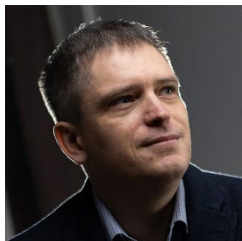
РусКрипто

XXVIII

НАУЧНО-ПРАКТИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Обзор проблематики обеспечения безопасности киберфизических систем.

От потребностей к требованиям, технологиям и нормативно-технической документации



**Владимир
Карантаев.** Доцент
Кафедры ИУ10 МГТУ
им. Баумана

Алексей Лазарев.

Руководитель департамента
защиты киберфизических
систем. Компания «Актив».





Ключевые тренды цифровой электроэнергетики

Smart Grid и интеллектуальные сети — двустороннее взаимодействие, интеграция распределённой генерации

Цифровые подстанции IEC 61850 — виртуализация РЗА, цифровые протоколы, встроенная кибербезопасность

ИИ и предиктивная аналитика — прогноз нагрузки и генерации ВИЭ, предиктивная диагностика оборудования

Киберфизические системы и цифровые двойники — совместное моделирование электро- и ИТ-инфраструктуры

Кибербезопасность by design — Zero Trust Architecture, микросегментация, непрерывный мониторинг

Интеграция ВИЭ и накопители энергии — виртуальная инерция, BESS/ГАЭС, балансировка режимов

Микросети и виртуальные электростанции (VPP) — островные режимы, мультиагентное управление

IoT/IIoT и граничные вычисления — интеллектуальные датчики, Edge-аналитика, безопасное управление устройствами

HVDC и супергриды — передача энергии на дальние расстояния, мультитерминальные системы

Цифровая трансформация энергосистем — облачные платформы, SDN/5G, фабрика ИИ-приложений



Примеры атак на киберфизические системы (АСУ ТП)

Stuxnet (2010)

Havex (2014)

BlackEnergy (2015)

TRITON (2017)

Industroyer (2017)

Атака на ВЭС в Германии (2022)

Industroyer 2 (2022)

Pipedream (2022)

Атака на энергосистему Дании (2023)

Атака на энергосистему Польши (2025)

Pipedream (2022)

Компьютерные атаки на АСУ ТП и РЗА (10)

Специально разработаны
для атак на АСУ ТП и РЗА (10)

Специально разработаны
для нарушения
технологического процесса (7)

Кросс-отраслевое ВПО, разработанное
для нарушения технологического
процесса (1)

Подходы к анализу:

- "Постанализ" произошедших атак.
- Анализ сценариев потенциальных последствий.
 - Экспертная оценка.
 - Подготовка и принятие решений по развитию систем.

Stuxnet (2010)

TRITON (2017)

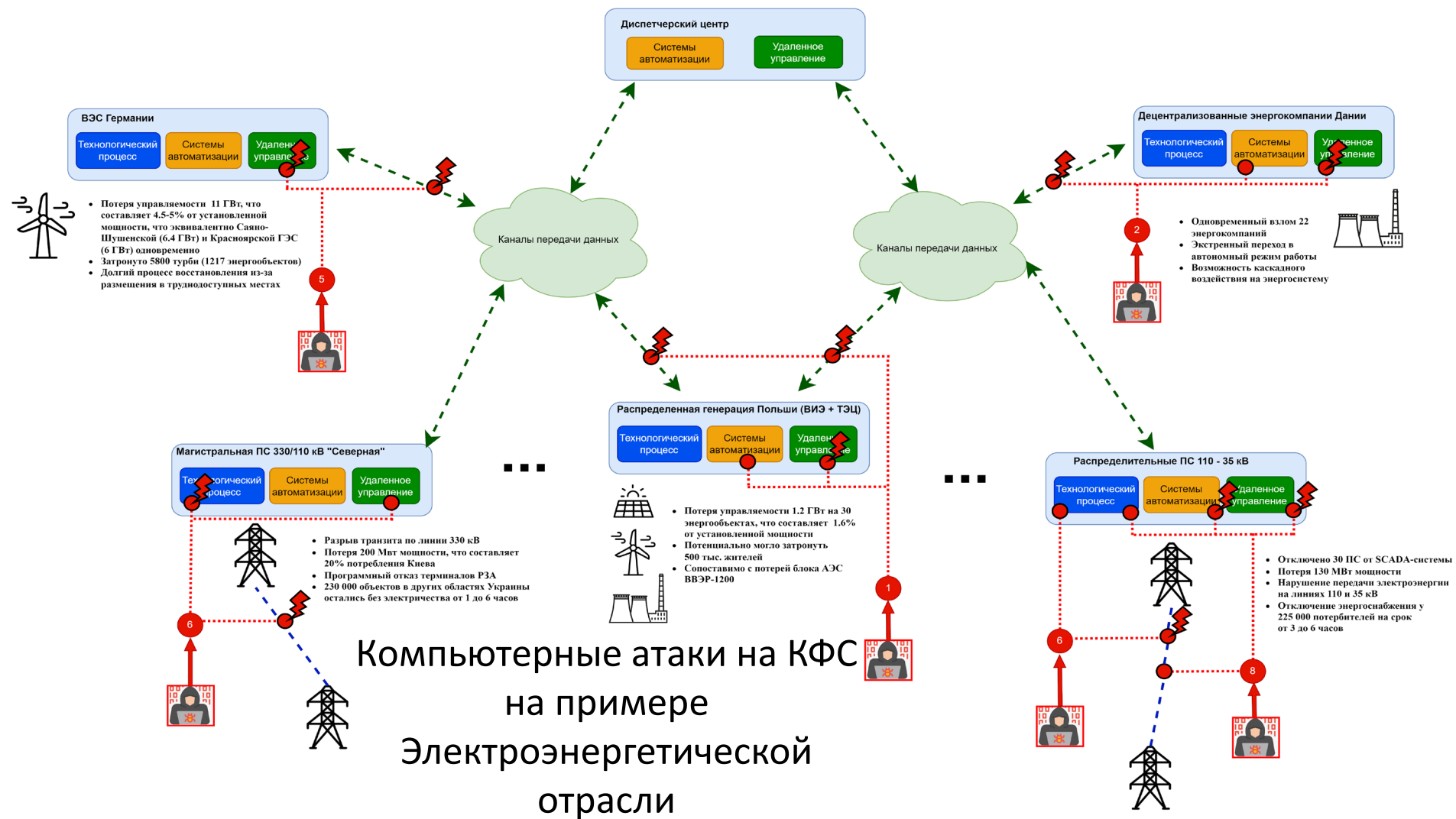
Industroyer (2017)

Industroyer 2 (2022)

Pipedream (2022)

Атака на энергосистему Дании (2023)

Атака на энергосистему Польши (2025)



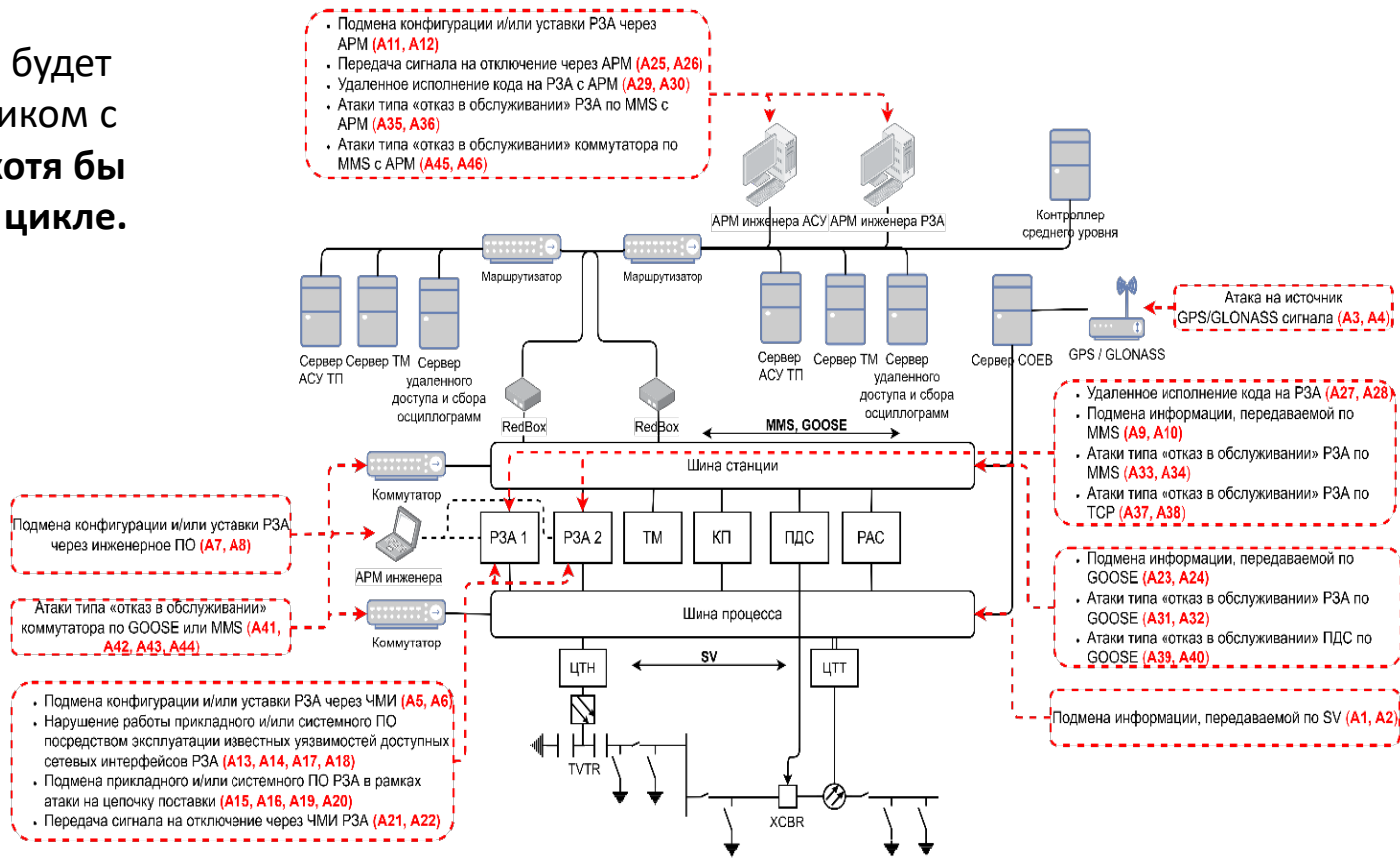


Потенциальный ущерб от компьютерных атак на подстанции

КФС, являющаяся ЗОКИИ будет атакована злоумышленником с **высоким потенциалом хотя бы один раз на жизненном цикле.**

Потенциальный ущерб может быть выражен количественно:

- Метод основан на деревьях отказов.
- Расчет вероятностей методом экспертного оценивания.
- Расчет электр.





Потенциальный ущерб от компьютерных атак на подстанции

Объект	Математическое ожидание недоотпуска электроэнергии, МВтч			Математическое ожидание экономического ущерба от недоотпуска электроэнергии, млн. рублей			Математическое ожидание увеличения стоимости ремонтов оборудования, млн. рублей		
	Сумма	Не связанные с комп. атаками	Комп. атаки	Сумма	Не связанные с комп. атаками	Комп. атаки	Сумма	Не связанные с комп. атаками	Комп. атаки
Подстанция 110/35/10 кВ	5877,535	1976,245	3901,290	581,876	195,648	386,228	63,808	61,546	2,262
Подстанция 220/110/35/10 кВ	8829,119	3228,658	5600,461	1087,269	397,609	689,660	174,981	162,990	11,991

- **Суммарная трансформаторная мощность:**

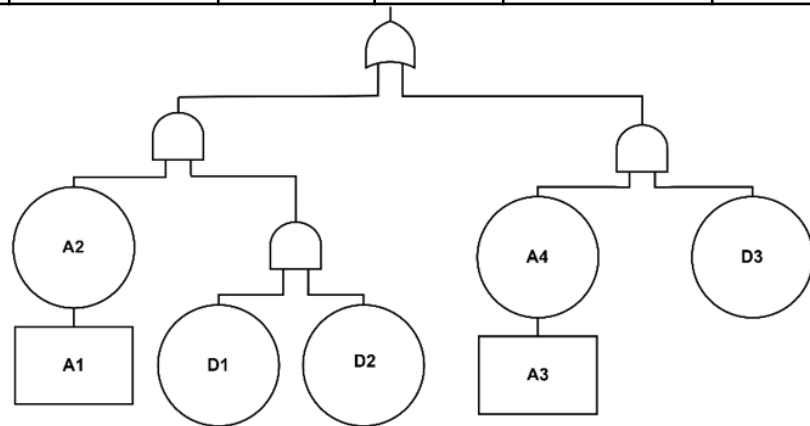
110 кВ — 160 МВА;
220 кВ — 412,6 МВА.

- **Нормативное время восстановления:**

110 кВ и ниже — 9,4 часов;
220 кВ — 12,7 часов.

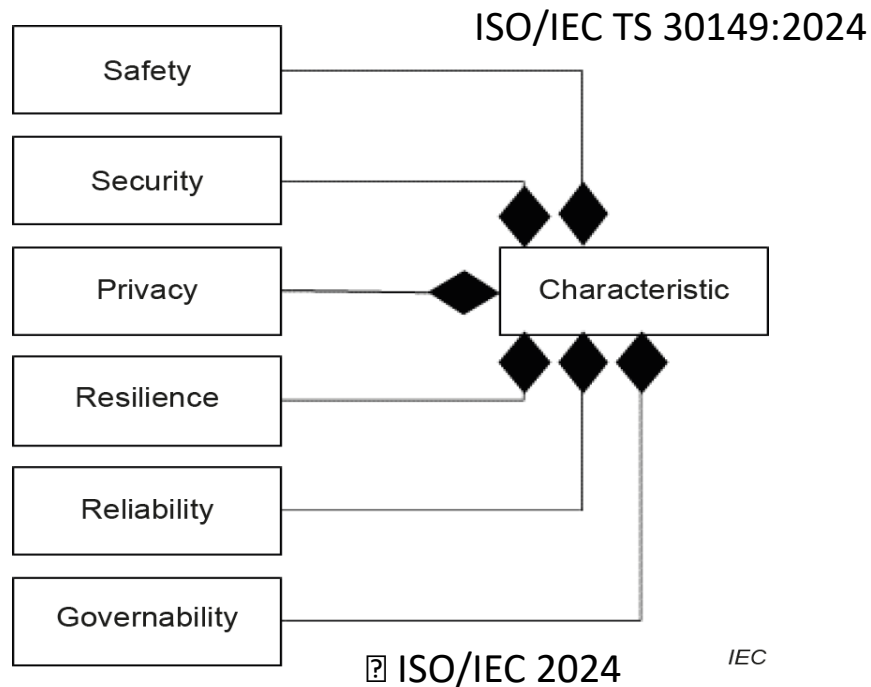
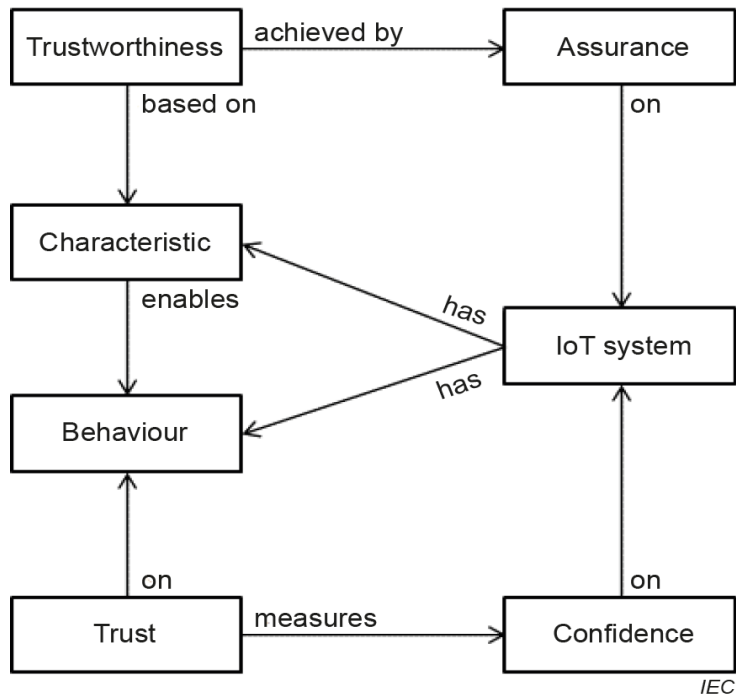
- **Удельный ущерб:**

110 кВ — 99 рублей/кВтч;
220 кВ — 175 рублей/кВтч.





- Методы системной инженерии
- Разработка КФС на основе принципов конструктивной информационной безопасности





КФС с какими характеристиками необходимо развивать?

Надежность:

Структурная надежность

Функциональная надежность

Обеспечивающие устойчивость функционирования

Функциональная безопасность (Safety)

Кибербезопасность

Конструктивная информационная безопасность (Secure by Design).

Барьеры:

- Регуляторные
- Мотивационные

Комплексное улучшение характеристики при разработке КФС приведут к

- Увеличению времени разработки и вывода на рынок продуктов
- Повышению затрат на разработку

- Компетентные



Матрица влияния стейкхолдеров и противоречия

Стейкхолдеры системы:

Граждане (Физические лица)

Владелец системы

Заказчик системы

Разработчик системы:

Разработчики подсистем.

Аппаратно-программных
платформ

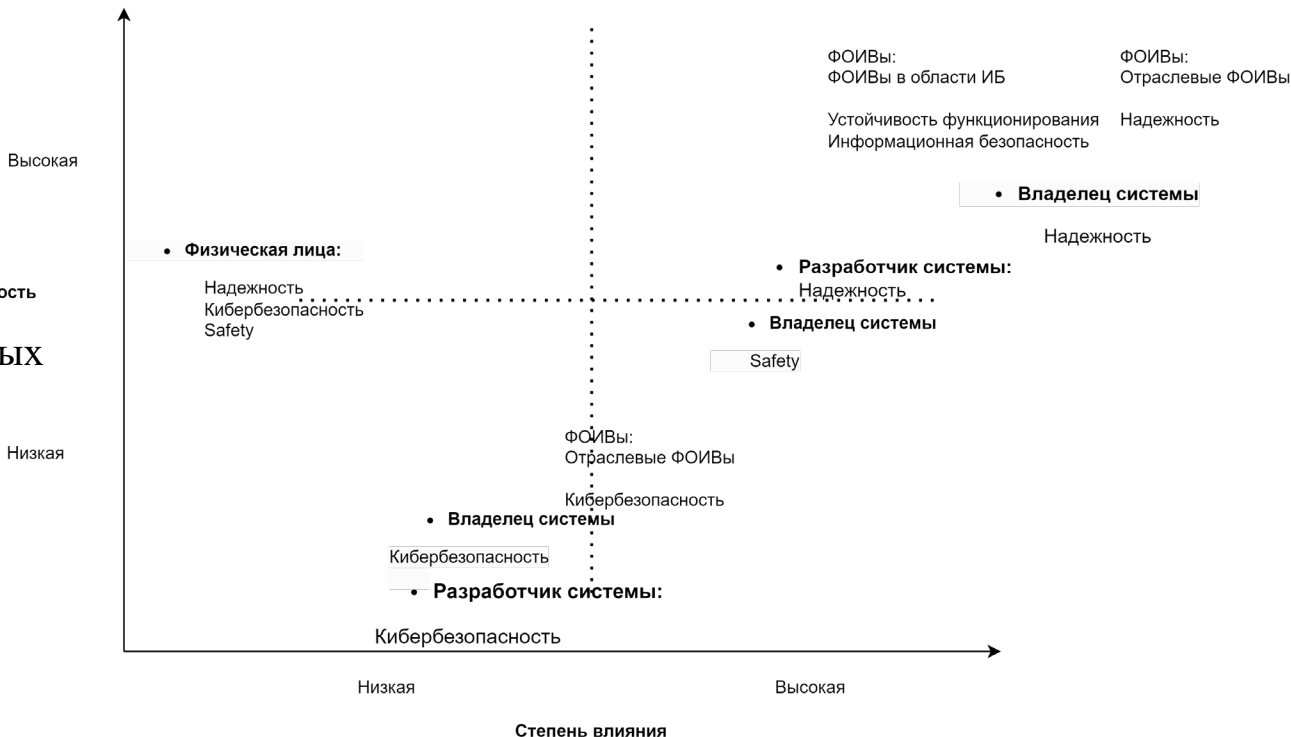
Цифровых микросхем

Разработчики СЗИ и СКЗИ

ФОИВЫ в области ИБ

Отраслевые ФОИВЫ

Злоумышленник





Матрица влияния стейкхолдеров и противоречия

Защищенная аппаратно-программная платформа должна:

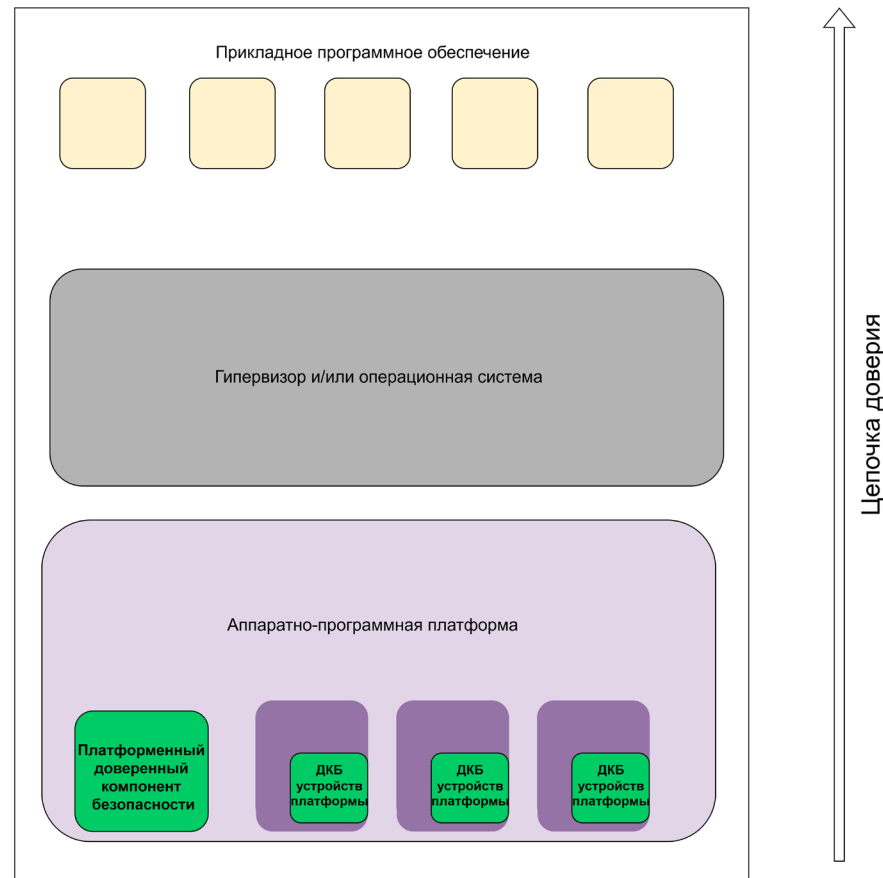
- Должна включать доверенный компонент - RoT for Update.
- При обновлении критического встроенного ПО должны быть:
 - Реализованы механизмы обеспечения целостности и аутентичности
 - Обновление аутентифицированным субъектом.
 - Модификация критических данных только аутентифицированным субъектом.
 - Механизмы обеспечения целостности критичного встроенного ПО и данных при хранении в ПЗУ и обработке в ОЗУ.

Восстанавливаемая АПП должна содержать - RoT for Detection and Recovery:

- Механизмы для обнаружения нарушения состояния целостности критического встроенного программного обеспечения и данных.
- Механизмы восстановления состояния целостности критического встроенного ПО и данных через санкционированный механизм

Отказоустойчивая АПП должна:

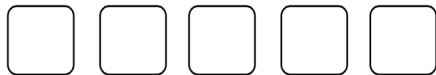
- Поддерживать как требования к защищенной, так и к восстанавливаемой платформе.





Как реализовать

Объект оценки 3:
Доверенный компонент безопасности
Тип: 2



Объект оценки 2:
Защищенная (специальная) встраиваемая
операционная система

Объект оценки 1:
Защищенная Цифровая МС с фирменным
ПО производителя

Основной упор делается на защиту
аппаратной платформы и сопутствующего
фирменного ПО производителя микросхемы.

Нормативно-технические требования
ГОСТ Р "ЗИ Доверенный компонент безопасности.
Общие положения. 1 редакция ноябрь 2026.

Доверенный компонент безопасности:

- Подсистема (доверенная подсистема) АПП
- Неотъемлемая часть АПП
- Программный или аппаратно-программный, аппаратный компонент
- Реализует одну или несколько функций безопасности.
- В отношении ДКБ должен быть сформирован перечень идентифицированных угроз безопасности информации.

ДКБ, как объект оценки может включать минимум два предсертифицированных компонента:

- Защищенную цифровую микросхему
- Защищенную (специальную) операционную систему



Технологические:

От требований к ISA к
верификации аппаратных
средств и верификации ПО.

Для ответственных
применений возможна
«сквозная» формальная
верификация аппаратного и
программного обеспечения

• Система момент (ISA)

Ограничения в реализации:

- Технологические нормы
- Методы верификации на поздних этапах ЖЦ.
- Необходимость разработки шкалы «уровней доверия» для аппаратных средств.



Регуляторные

- Разработать систему национальных стандартов с требованиями к АПП и ДКБ, включая защищенные цифровые интегральные микросхемы.
- Адаптировать систему оценки соответствия для достижения «обоснованного доверия» к разработанным Цифровым ИМС.
- Обеспечить их применение на нормативно-правовом уровне регулирования.

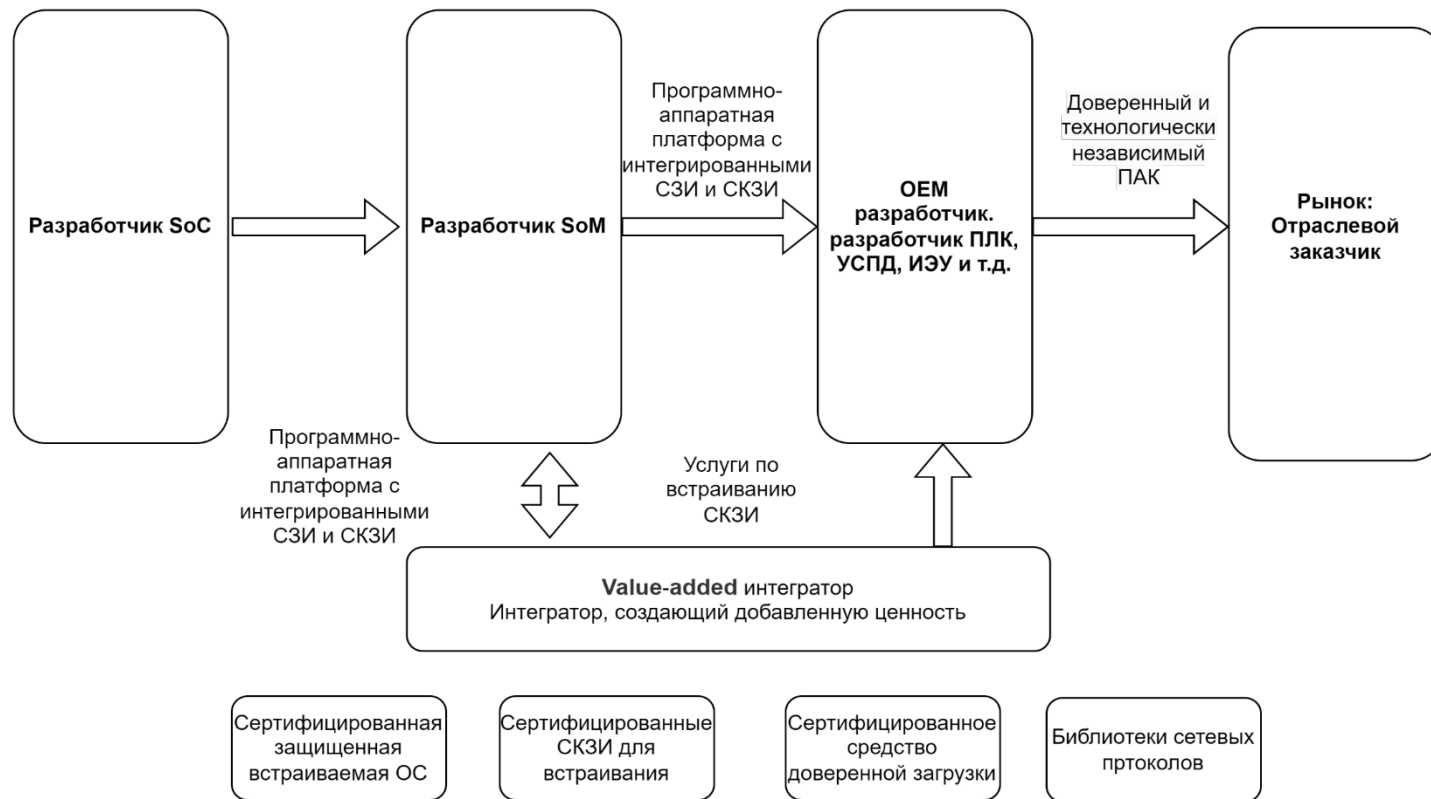
Мотивационные и технологические

- Инициировать и профинансировать выполнение следующих целевых НИОКР.
 - Разработка научно-обоснованных архитектур и решений по использованию корней доверия для построения АСУ ТП с открытой модульной архитектурой, РЗА и ПА нового поколения. Исследования должны учитывать отраслевую специфику для энергетики и промышленности.
 - Создание технологий доверенных программно-аппаратных комплексов с интегрированными корнями доверия для запуска и защиты технологий искусственного интеллекта.
 - Исследование устойчивых архитектур программно-аппаратных комплексов на основе корней доверия в контексте постквантовых угроз. Данное направление носит опережающий характер и имеет стратегическое значение для национальной безопасности. Необходимо разработать научно-обоснованные подходы к интеграции постквантовых криптографических алгоритмов в аппаратные корни доверия и архитектуру доверенных АСУ ТП.



Компетентностные

- Разработать руководства по применению системы стандартов.
- Разработать практико-ориентированные учебно-методические комплексы, ориентированные на реализацию требований НТД.
- В рамках программы «Приоритет 2030» для вузов технического и энергетического профиля рекомендовать включить показатели по созданию таких лабораторий и разработке соответствующих учебно-методических комплексов (УМК) в систему критериев эффективности. Это обеспечит дополнительную мотивацию вузов к развитию данного критически важного направления.
- Кроме того, предлагается инициировать совместный проект с ведущими производителями аппаратного и программного обеспечения (чипов, АСУ ТП с открытой архитектурой) по разработке типовых учебно-исследовательских стендов для оснащения профильных вузов.
- На базе этих стендов создать сеть отраслевых научно-учебных лабораторий «Доверенные программно-аппаратные комплексы в электроэнергетике и промышленности»:
- обучать студентов и специалистов по дополнительным профессиональным программам работе с доверенными «паками», корнями доверия и открытыми АСУ ТП;
- давать практические навыки сборки отраслевых решений, написания прикладного и системного программного обеспечения для них;
- проводить прикладные исследования в области кибербезопасности и ИИ для энергетики и промышленности.
- В рамках программы «Приоритет 2030» для вузов технического и энергетического профиля рекомендовать включить показатели по созданию таких лабораторий и разработке соответствующих учебно-методических комплексов (УМК) в систему критериев эффективности. Это обеспечит дополнительную мотивацию вузов к развитию данного критически важного направления.





- **Доверенный компонент безопасности (ДКБ)** — ключевой элемент обеспечения фундаментальных свойств киберфизических систем КИИ за счёт гарантий целостности, аутентичности и конфиденциальности в условиях преднамеренных воздействий.
- **Конструктивная информационная безопасность** — основной принцип проектирования КФС, при котором требования безопасности закладываются на ранних этапах и последовательно проводятся через весь жизненный цикл.
- **Верифицируемые технологии** — основа разработки ДКБ: от системы команд и архитектуры (ISA, микроархитектура), через процессы производства (дизайн, топология, тестирование), к формализованным методам верификации и независимой проверке корректности реализации.
- **Стратегический императив:** технологический суверенитет в области КФС КИИ на основе конструктивной ИБ, ДКБ и верифицируемых технологий микроэлектроники для обеспечения контролируемости доверия от аппаратуры до прикладного ПО.
- **Необходимое условие:** создание отечественных защищённых и верифицируемых ДКБ, стандартов проектирования КФС и их внедрение в устройства автоматики и элементы КИИ для долгосрочной устойчивости и управляемой безопасности.



РусКрипто
XXVIII НАУЧНО-ПРАКТИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Спасибо за внимание!

Владимир Карантаев

Доцент Кафедры ИУ10 МГТУ
им. Баумана

+7(915) 221 15 96

expert@vkarantaev.ru

Алексей Лазарев

Руководитель департамента
защиты КФС

+7(905) 729 34 26

al@rutoken.ru