kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Дмитрий Правиков

Директор Научно-образовательного центра новых информационно-аналитических технологий (НОЦ НИАТ), РГУ нефти и газа (НИУ) им. И. М. Губкина

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

Kaspersky Industrial Cybersecurity Conference 2021

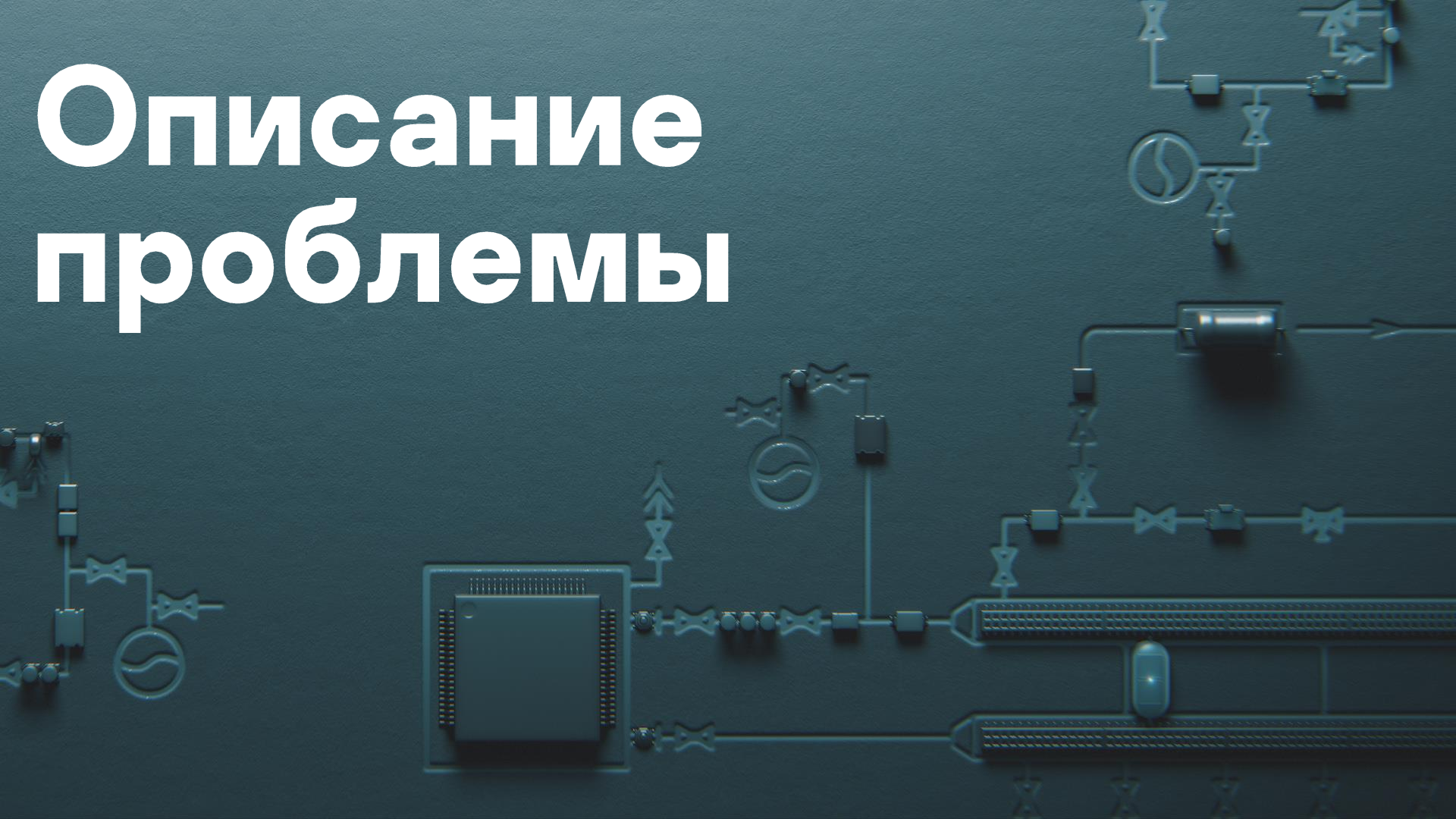
Концепция информационной безопасности «роя» киберфизических систем

Дмитрий Правиков

Теоретик информационной безопасности 2 поколения

kaspersky

Описание проблемы



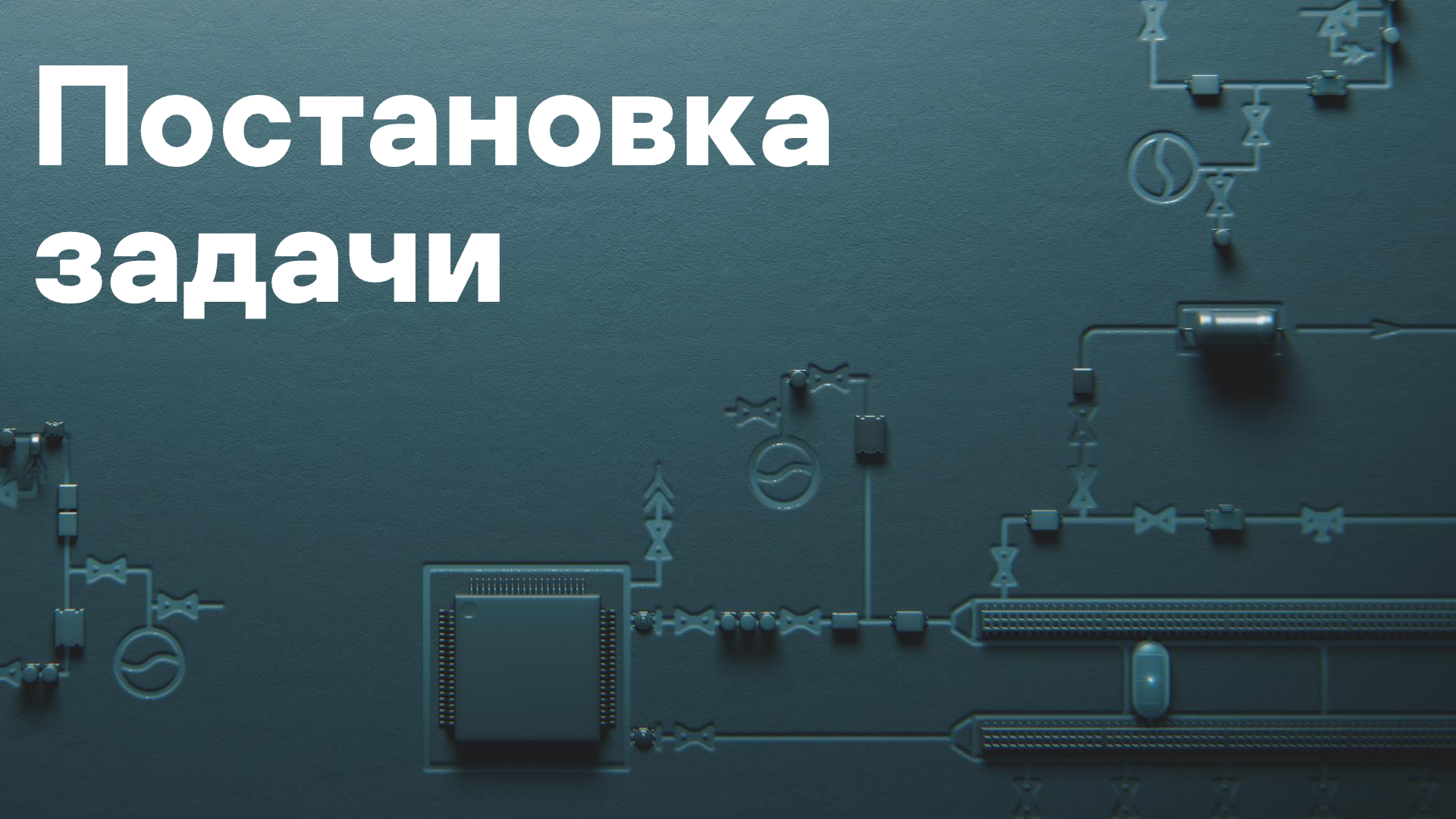
Периметра нет – изменение подходов к безопасности

Кризис подходов к обеспечению информационной безопасности

Классическая «субъектно-объектная» модель становится не применимой

- Размытая граница защищаемых систем
- Динамическое формирование защищаемой системы
- Нельзя перечислить все субъекты и объекты
- Для произвольной пары «субъект – объект» нет верифицированных прав доступа
- Концепция ZTA
- Отсутствие каких-либо теоретических подходов

Постановка задачи



Безопасность «роя» систем

Состав «роя» не фиксирован

Нет «центра» принятия решений

Состояние безопасности элемента не критично для безопасности «роя»

Анализ

Подходы к решению

Требуется ответить на ряд основополагающих вопросов

— В чем будет заключаться безопасность «роя» киберфизических систем?

— Можно ли формализовать описание безопасности?

— Как обеспечить распределенный центр безопасности «роя»?

— Как это можно будет реализовать?

Безопасность «роя» определяется как устойчивое функционирование совокупности прикладных программ «роя» киберфизических систем

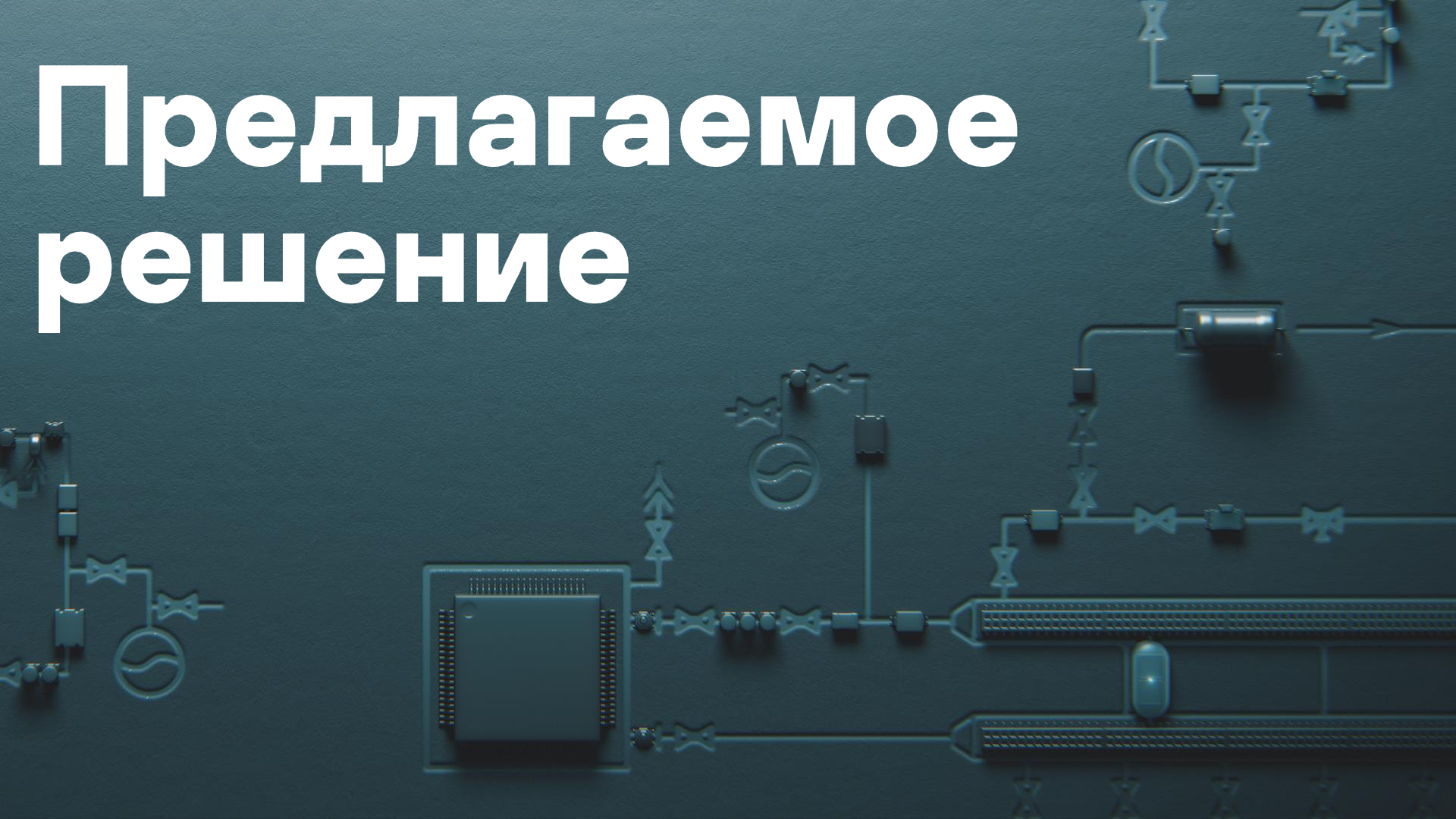
> Модель описывает сетевую инфраструктуру промышленной системы (ПС) в виде ориентированного графа G, множество вершин $V = \{v_1, \dots, v_N\}$ которого характеризует все компоненты ПС, способные к сетевому взаимодействию. Множество дуг $E = \{e_1, \dots, e_M\}$ графа отражает все возможные межкомпонентные связи, проявляющиеся как обмен данными между устройствами. Каждый компонент ПС, моделируемый вершиной v_i, характеризуется набором функций, которые он способен реализовывать.

— Лаврова Д.С. Методология предотвращения компьютерных атак на промышленные системы на основе адаптивного прогнозирования и саморегуляции. Автореферат диссертации на соискание ученой степени доктора технических наук. СПбТУ – 2019.

1. Удалить информационный обмен между двумя прикладными программами (где он был).
2. Создать информационный обмен между двумя прикладными программами (где его не было).
3. Добавить новую прикладную программу (без информационного обмена).
4. Удалить существующую прикладную программу (вне зависимости от ее участия в информационном обмене).
5. Добавить новую прикладную программу и организовать ее информационный обмен с двумя другими существующими прикладными программами (комбинация действий 1, 2 и 3).

— Лаврова Д.С., Зегжда Д.П., Зайцева Е.А. Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. 2019. № 2 (30). С. 13–20

Предлагаемое решение



Распределение центра безопасности

Что, опять блокчейн?

- Это не блокчейн
- Это не криптовалюта
- Это распределенный реестр

- Необходимо обеспечить штатную работу
- Необходимо выявить попытку атаки

- Know-how в алгоритме консенсуса

Доработка операционной системы, управляющей киберфизическим устройством

Что такое «безопасность роя»

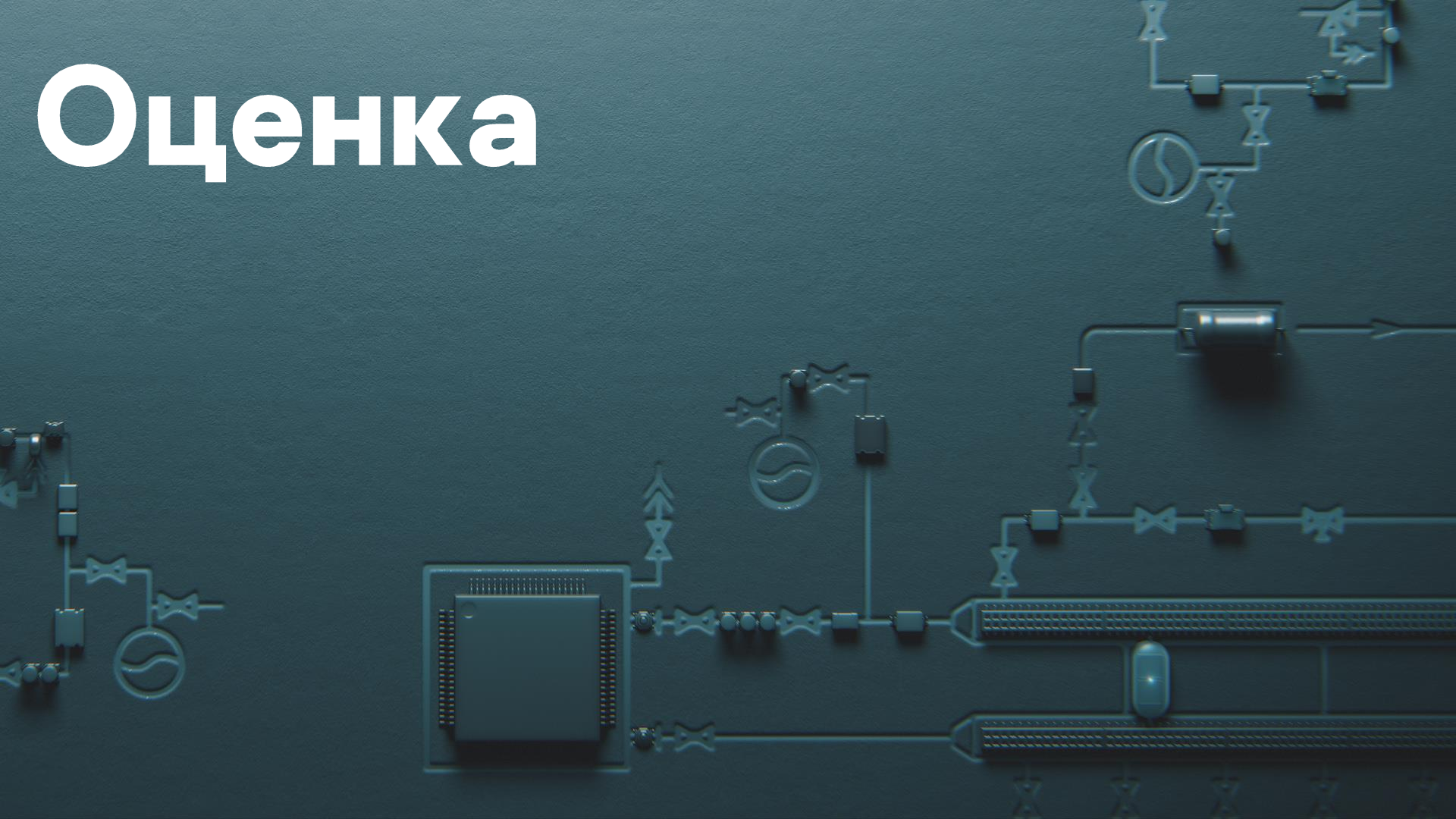
Основные элементы предлагаемого подхода

Сведения вопросов информационной безопасностик вопросам безопасного взаимодействия и модификации набора прикладного программного обеспечения, функционирующего в комплексе киберфизических устройств.

Вынесение описания прав и порядка взаимодействия прикладного программного обеспечения (аналога таблицы разграничения прав доступа) в распределенный реестр

Администрирование распределенного реестра на основании алгоритма консенсуса (фактически децентрализованное администрирование и управление безопасностью)

Оценка



Оценка предложенного подхода

Критерии:
- использование в основе не «субъектно-объектной» модели;
- возможность формализации;
- возможность технической реализации.

Удовлетворяет требованиям динамического изменения состава «роя» и децентрализации принятия решений по безопасности

Может быть формально описан и (при необходимой проработке) формально верифицирован

Может быть реализован путем доработки ОС для киберфизических систем

Благодарю за внимание!

Д.И.Правиков

kaspersky