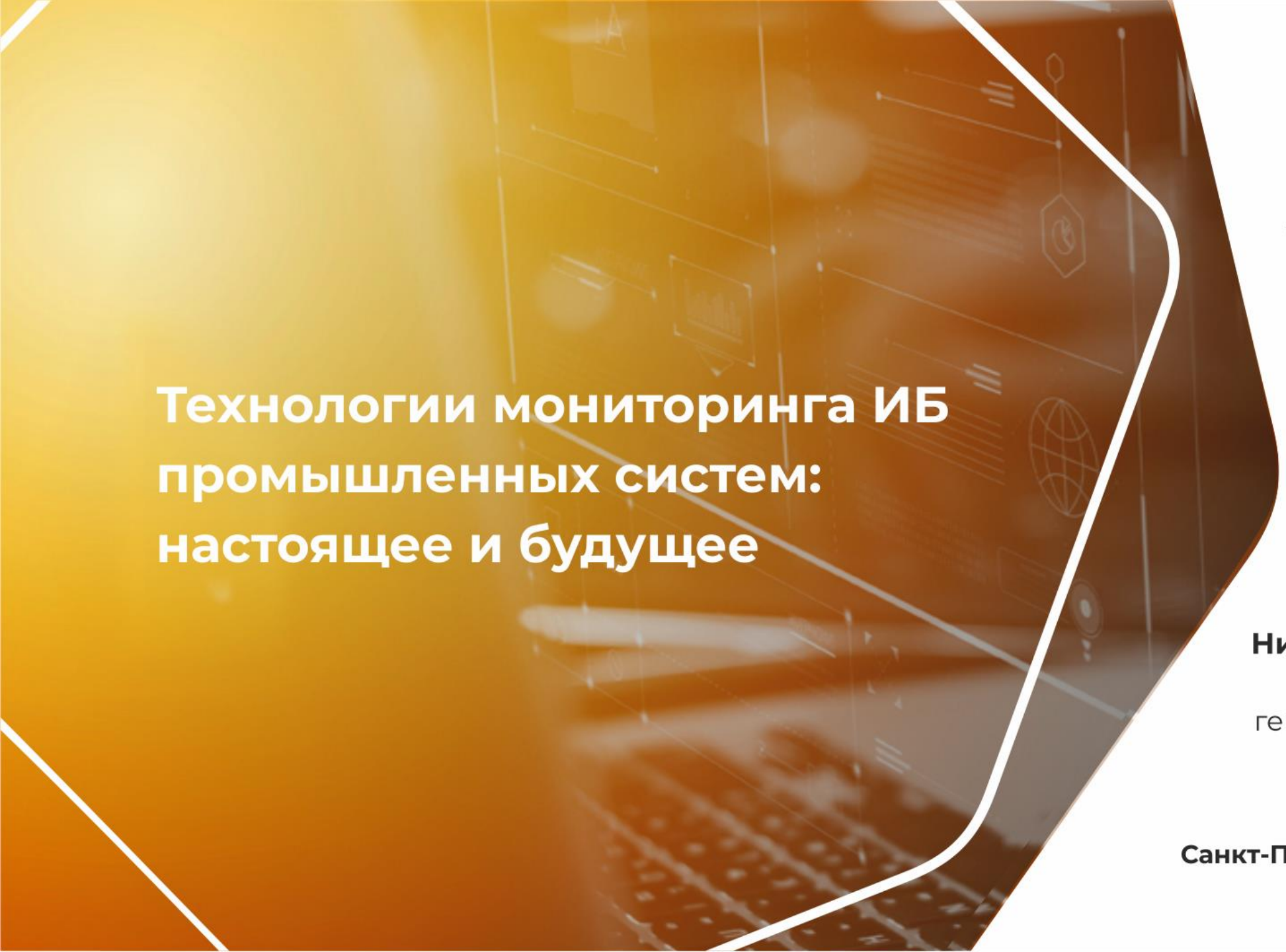


# Технологии мониторинга ИБ промышленных систем: настоящее и будущее

УЦСБ

**Николай Домуховский**

Заместитель
генерального директора

**Санкт-Петербург, GIS Days, 2020**

# Система анализа и мониторинга ИБ как часть СОИБ

# Создание САМСИБ (по мотивам проекта ГОСТ Р «Мониторинг ИБ. Общие положения»)

| Обследование объекта мониторинга | Выбор и внедрение средств сбора данных мониторинга | Разработка правил обработки данных мониторинга | Выстраивание процессов СОИБ на основе данных мониторинга |
|---|---|---|---|
| • Инвентаризация объекта<br>• Подготовка справочников (протоколов, событий, конфигураций и пр.) | • Подбор, установка и настройка средств сбора данных мониторинг<br>• Первичная нормализация данных мониторинга (на основе справочников) | • Разработка правил корреляции данных мониторинга (событий, сведений об изменениях и пр.)<br>• Разработка экранных форм оператора системы мониторинга | • Определение порядка действий при выявлении признака инцидента ИБ (квалификация, классификация)<br>• Определение порядка реагирования на инцидент ИБ и устранения последствий инцидента ИБ |

# Облик системы мониторинга ИБ с элементами СОИБ

# Почему не так просто создать систему мониторинга ИБ?

## Разнообразные системы автоматизации

### Наследие старых систем

- Время жизни систем 15-25 лет
- Самый распространенный протокол ПАСиУ – Modbus, созданный в 1979 г.

### ...в новых тоже нет стандартизации

- Более 20 ОС в IoT – лишь верхушка айсберга
- Большинство IoT слишком сложны, так как используют множество разных протоколов и технологий

## Нуждаются в эффективных средствах защиты

### Число атак растет

- В 2019 году зафиксирован рост числа атак на 19%
- Построение защиты, которую нельзя сломать, — утопично по своей сути

### ...и число объектов тоже

- Рынок автоматизации вырастет до $269.5 млрд. к 2024 г.
- Основным сдерживающим фактором роста являются вопросы обеспечения ИБ

## Но их некому настраивать и эксплуатировать

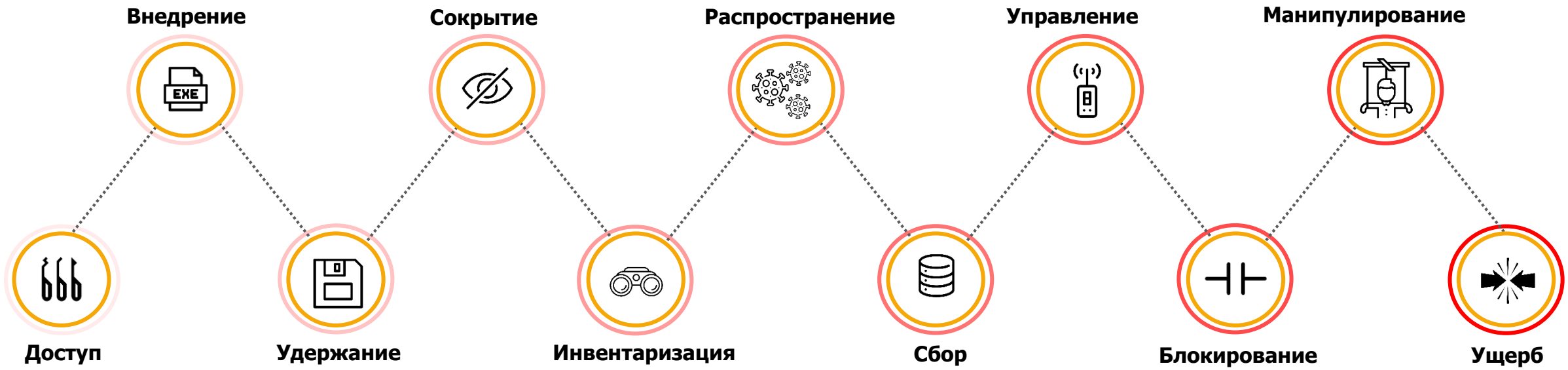
### Не хватает квалифицированных кадров для защиты

- Мировая нехватка специалистов по ИБ составляет около 4 млн. человек
- Для удовлетворения всех вакансий число специалистов по ИБ должно вырасти в 2.5 раза

### ...но при этом растет сложность защищаемых систем

- Третий кризис сложности компьютерных систем
- Основной сдерживающий фактор развития информационных технологий – неспособность обойти растущую сложность

# Проблемы управления инцидентами ИБ в «классической» СОИБ




Жизненный цикл инцидента ИБ в соответствии с MITRE ATT&CK® for Industrial Control Systems

**77%** Компаний подвергаются успешной атаке в течение одного года

**77%** На столько уменьшиться ущерб, если инцидент будет выявлен в течение недели

**10k** Оповещений получают более половины корпоративных центров управления безопасностью каждый день

**101** День в среднем уходит на обнаружение инцидента

**96%** На столько уменьшиться ущерб, если инцидент будет выявлен в течение дня

**30** Минут в среднем уходит у аналитика на обработку оповещения

# Будущее обнаружения признаков инцидентов ИБ

### Получение входных данных

- Что является входными данными (сетевой трафик, события ИБ)?
- Технология их получения (агент, пассивное прослушивание, удаленный доступ)

### Обработка входных данных

- Алгоритм обработки (глубокая инспекция, вычисление метаданных)
- Правила обработки (правила разбора данных, правила вычисления метаданных)
- Механизм адаптации

### Анализ данных

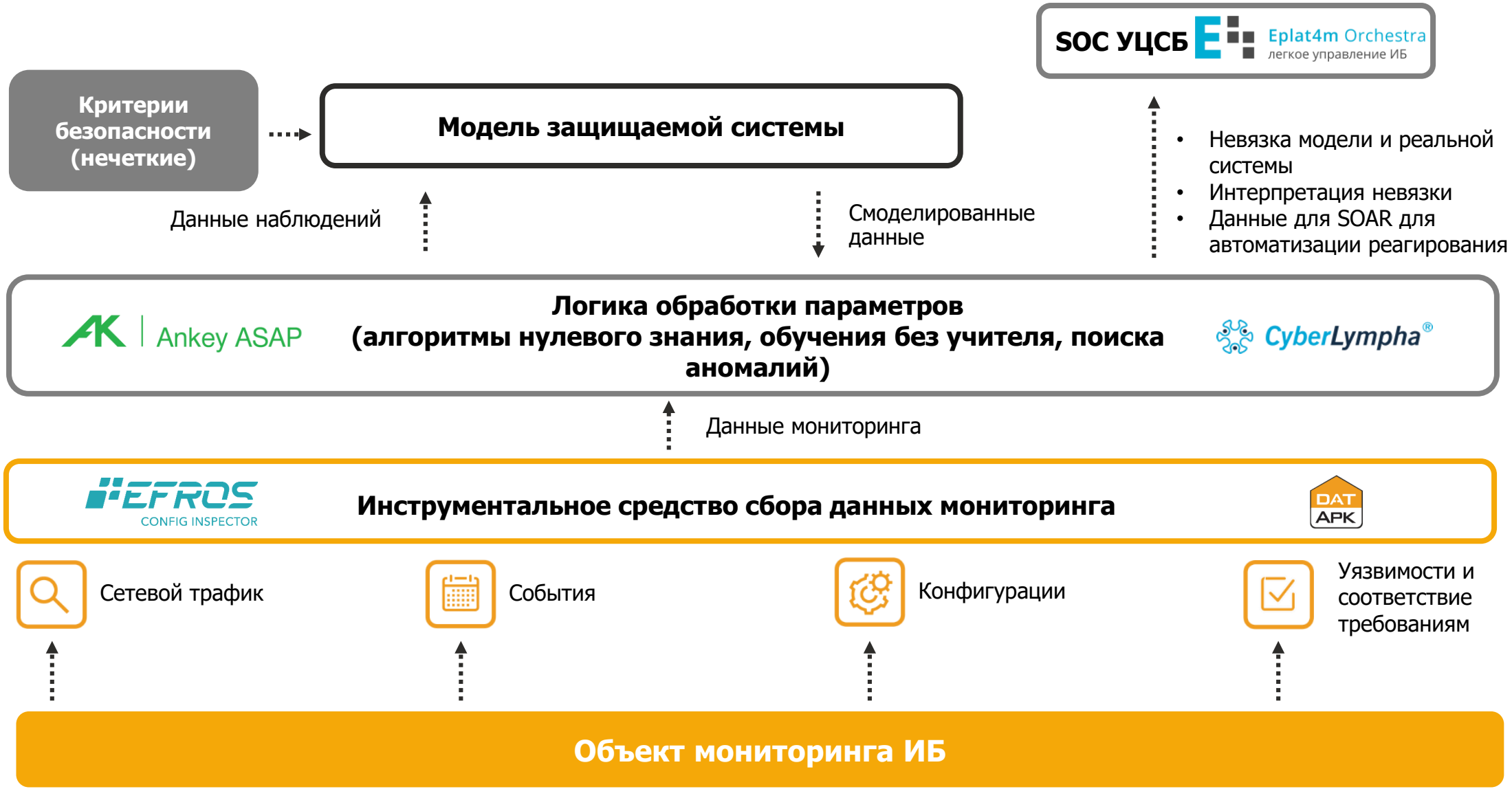
- Алгоритм анализа (классификация, моделирование)
- Правила анализа (сигнатуры)
- Глубина анализа (только текущий блок данных, механизмы памяти, детальное моделирование системы в целом)
- Степень автоматизации (автоматическая обработка, привлечение эксперта)
- Способность к обучению

### Оценка результата

- Способ выявления аномалии (количественная или качественная оценка)
- Возможность «объяснения» решения алгоритма
- Возможность локализации аномалии в реальной системе

| Вариант реализации | Скорость обнаружения | Точность обнаружения | Гибкость | Сложность реализации |
|---|---|---|---|---|
| Сигнатурные средства обнаружения | | | | |
| Обнаружение аномалий на основе метаданных и классификации | | | | |
| Обнаружение на базе модели ИБ | | | | |

# Облик системы мониторинга ИБ будущего



УЦСБ

**СПАСИБО ЗА ВНИМАНИЕ!**

**ВОПРОСЫ?**


**Николай Домуховский**
Заместитель генерального директора

ndomukhovsky@ussc.ru
**Тел.: +7 (343) 379-98-34 доб. +1103**

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU