CLOUD networks

# Риск-ориентированная сервисная модель промышленной кибербезопасности

Инновации

Технологии

Отношения

# Актуальность и проблематика

## Цифровизация производства

- Повышение степени развитости управляющих функций АСУ ТП
- Длительный жизненный цикл систем управления
- Тесная интеграция в информационную инфраструктуру предприятия
- Необходимость наличия комбинированных компетенций (ИБ + АСУ ТП)

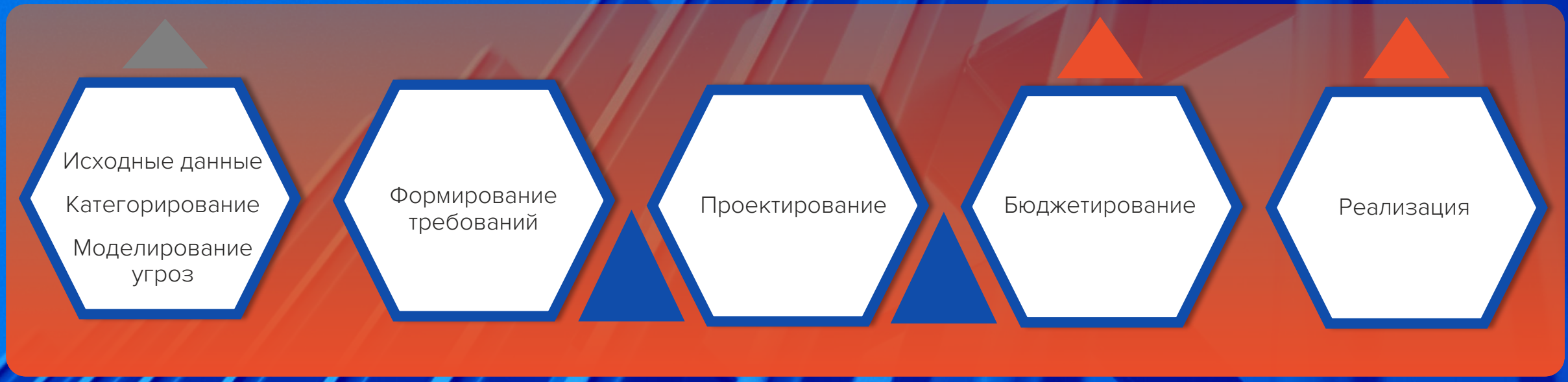
## При этом

- Направленность на ужесточение требований по обеспечению ИБ со стороны Регуляторов
- «Серые зоны» в нормативной документации Регуляторов
- Кадровый голод на местах
- Необходимость «отстаивать» бюджет ИБ
- Многие проекты «кладутся на полку» или сильно затянуты по срокам реализации

Промышленная кибербезопасность как сервис: риск-ориентированная модель

# «Классический» путь

- Отчет о сборе исходных данных
- Акт категорирования
- Модель угроз безопасности по методике ФСТЭК России
- Техническое задание
- Проектная и рабочая документация



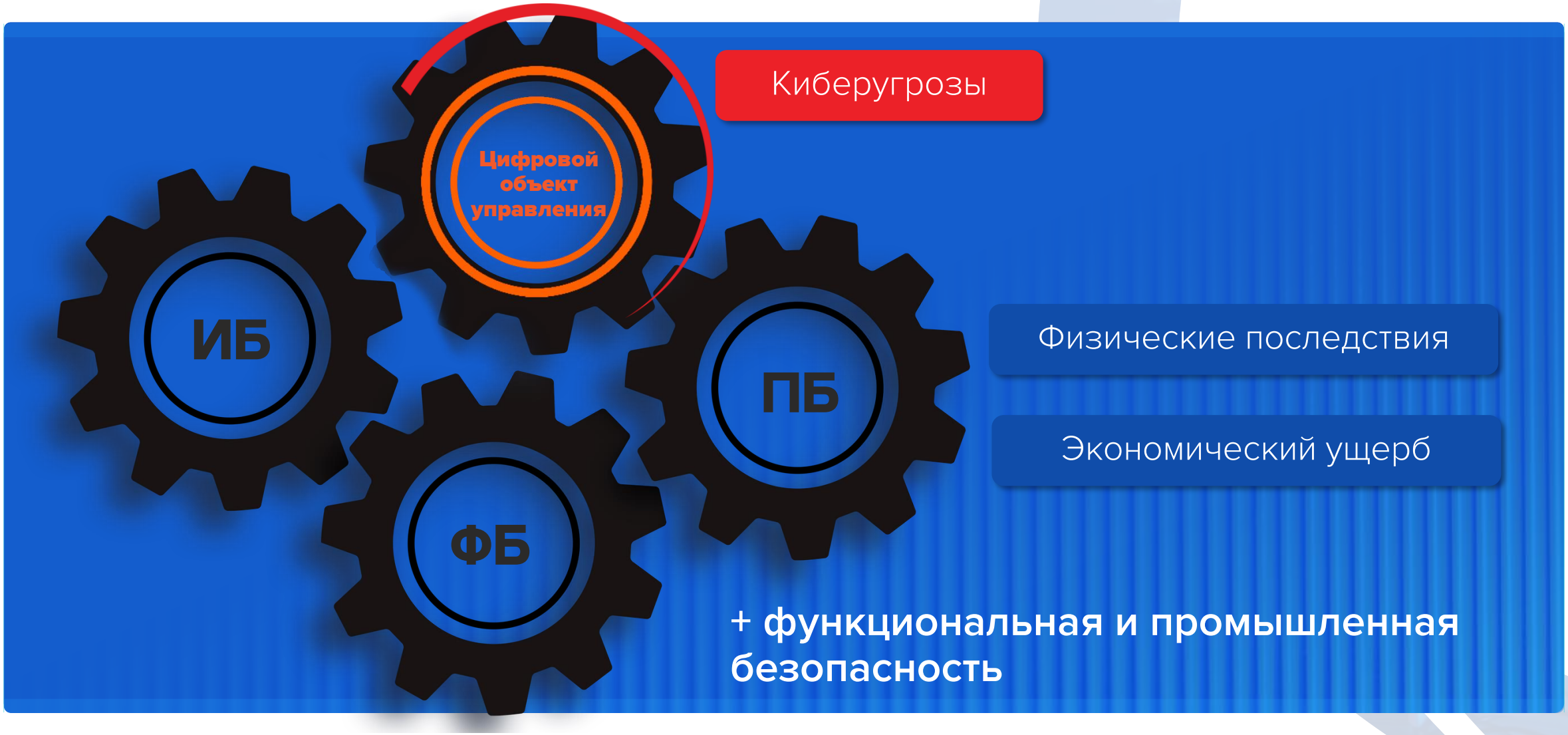
Новый подход

# Риск-ориентированная модель ИБ

Концепция

Отличия от «классической ИБ»

# АСУ ТП – это не просто объект КИИ



# Позиционирование

ИБ

- Законодательство по ИБ ОКИИ
- Документы Регуляторов
- Корпоративные стандарты ИБ

ФБ

- HAZOP-анализ
- Стандарты

ПБ

- Федеральный закон «О промышленной безопасности №116-ФЗ
- Федеральный закон «О безопасности объектов ТЭК» №256-ФЗ


- Однозначная взаимосвязь инцидентов ИБ, ФБ, ПБ
- Основа комплексной риск-ориентированной модели по обеспечению ИБ-объектов

# Анализ рисков

## Исходные данные

- Сведения о структурно-функциональных характеристиках ПТК АСУ ТП
- Карта технологического процесса
- Технологические объекты управления:
  - Схема автоматизации
  - Перечень контролируемых параметров
  - Факторы, нарушающие оптимальный ход тех. прогресса
- Декларация промышленной безопасности

## Методология

- Методика оценки рисков
- Шкала оценки тяжести последствий (ущерба)
- Методика моделирования угроз безопасности

## Результаты

- Перечень актуальных угроз ИБ
- Сценарий реализации
- Перечень негативных последствий
- Оценка потенциального ущерба
- Ранжирование рисков
- Перечень приоритетных мер по обеспечению ИБ

Инновации

Технологии

Отношения

# Отчетная документация

## Отчет по анализу рисков ИБ АСУ ТП

- Результаты моделирования угроз
- Методика оценки рисков
- Ценность информационных активов
- Последствия реализации угроз ИБ
- Шкала оценки ущерба от последствий реализации УБИ

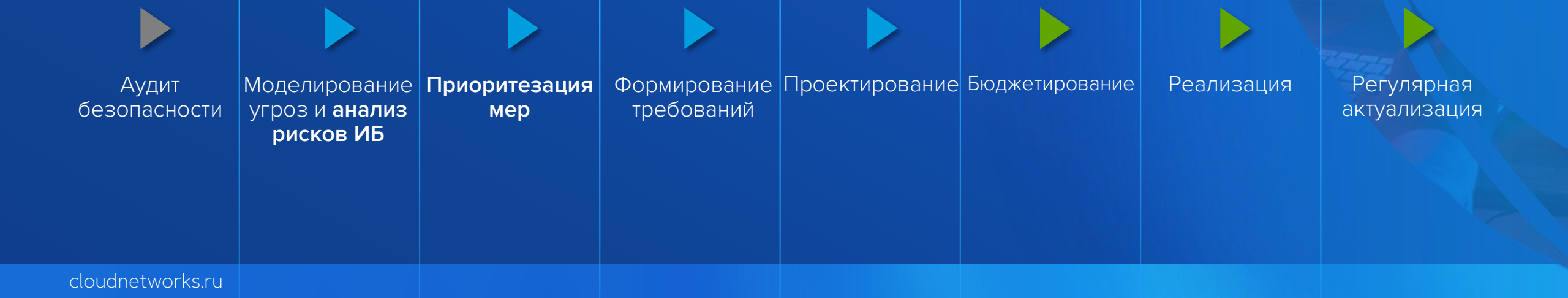
## Реестр рисков ИБ АСУ ТП

- Реестр угроз ИБ и сопутствующих рисков
- Ранжирование рисков на приемлемые и неприемлемые
- Размер потенциального ущерба
- Перечень приоритетных мер
- Выводы и рекомендации

Промышленная кибербезопасность как сервис: риск-ориентированная модель

# Создание СОИБ

- Отчет о сборе исходных данных (результаты аудита)
- Акт категорирования
- Модель угроз безопасности по методике ФСТЭК (+ тактики и техники MITRE)
- Отчет по анализу рисков ИБ
- Реестр рисков ИБ
- Техническое задание
- Проектная и рабочая документация



Промышленная кибербезопасность как сервис: риск-ориентированная модель

# Что меняется?

- Угрозы ИБ
- Требования регуляторов
- Особенности функционирования


Выявление проблемных областей

Приоритет выполнения мер

Прогнозируемость выполнения

Обоснование затрат на ИБ

Информационная безопасность как процесс

Сравнение подходов

# Методология

| Сценарный подход | Работа с недопустимыми событиями |
| --- | --- |
| ✗ Сценарий 1 | |
| ✓ Сценарий 2 | |
| ✓ Сценарий 3 | |
| ✓ Сценарий 4 | |
| ✗ Сценарий ... | Недопустимое событие |
| ✗ Сценарий N | |

**Исключение сценариев реализации**

**Исключение факта наступления события как такового**

# Экосистема сервиса

# Примеры: сценарии

| Сценарий | | |
|---|---|---|
| **Нарушители** | Преступные группы (криминальные структуры)<br>Группа сговора (Преступные группы (криминальные структуры)<br>Внутренние пользователи объекта защиты | |
| **Вектор атаки** | Получение НСД путем компрометации учетных данных | |
| **Результат** | Несанкционированная модификация установок технологического процесса с последующим аварийным остановом | |
| **Цепочка атак** | Корпоративный АРМ → Сервер контроллера домена → АРМ инженера (SCADA) → OPC-сервер → ПЛК | |
| Негативные последствия после наступления сценария | Аварийное завершение технологического процесса с потерей промежуточного продукта<br>Повреждение или утрата критически важных производственных данных<br>Затраты на устранение последствий атаки и восстановление систем<br>Риск аварийных ситуаций на производстве<br>Нарушение работоспособности АСУ ТП<br>Потеря визуального контроля за технологическим процессом, отсутствие возможности повлиять на его ход средствами автоматизации | |
| **Паттерн нарушителя** | **Точка входа** | **Целевой объект** |
| Получение НСД путем компрометации данных | Корпоративный АРМ | Сервер контроллера домена<br>АРМ инженера (SCADA) |
| **Шаг 1** | **Способы реализации** | |
| Получение НСД путем фишинга в корпоративный сегмент связи | СП.2.3 Использование недостатков, связанных с отсутствием проверки достоверности отправителя и/или получателя<br>СП.13.4 Почтовый фишинг | |

| Тактики MITRE Att&CK | Техники MITRE Att&CK | Техники методики ФСТЭК России | Угрозы (новый раздел БДУ ФСТЭК России) | Угрозы |
|---|---|---|---|---|
| Reconnaissance | T1598 – Phishing for Information | T1.11 Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга | УБИ.2 – Угроза несанкционированного доступа | УБИ.175 – Угроза «фишинга»<br>УБИ.015 – Угроза доступа к защищаемым файлам с использованием обходного пути |
| Initial Access | T1566 – Phishing | | | |
| **Шаг 2** | | **Способы реализации** | | |
| Получение учетных данных SCADA-пользователя | | СП.2.2 Использование недостатков связанных с управлением учетными данными<br>СП.8.5 Идентификация пользователей<br>СП.17.1 Перебор паролей к учетной записи | | |
| **Тактики MITRE Att&CK** | **Техники MITRE Att&CK** | **Техники методики ФСТЭК России** | **Угрозы (новый раздел БДУ ФСТЭК России)** | **Угрозы** |
| Resource Development | T1586 – Compromise Accounts | T2.11 Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля | УБИ.2 – Угроза несанкционированного доступа | УБИ.008 – Угроза восстановления и/или повторного использования аутентификационной информации<br>УБИ.074 – Угроза несанкционированного доступа к аутентификационной информации |
| Persistence | T1078 – Valid Accounts | | | |

# Промышленная кибербезопасность как сервис

| **Паттерн нарушителя** | | **Точка входа** | | **Целевой объект** |
|---|---|---|---|---|
| Закрепление доступа с помощью повышения привилегий | | APM инженера (SCADA) | | OPC-сервер |
| **Шаг 3** | | **Способы реализации** | | |
| Превышение привилегий путем использования уязвимостей SCADA | | СП.2.2 Использование недостатков связанных с управлением учетными данными<br>СП.19.4 Изменение (подмена, удаление) системных файлов операционной системы | | |
| **Тактики MITRE Att&CK** | **Техники MITRE Att&CK** | **Техники методики ФСТЭК России** | **Угрозы (новый раздел БДУ ФСТЭК России)** | **Угрозы** |
| Privilege Escalation | T1068 – Exploitation for Privilege Escalation<br>T1098 – Account Manipulation | T6.3 Эксплуатация уязвимостей ПО к повышению привилегий | УБИ.3 – Угроза несанкционированной модификации (искажения) | УБИ.007 – Угроза воздействия на программы с высокими привилегиями<br>УБИ.025 – Угроза изменения системных и глобальных переменных<br>УБИ.031 – Угроза использования механизмов авторизации для повышения привилегий<br>УБИ.122 – Угроза повышения привилегий |

| **Паттерн нарушителя** | | | **Точка входа** | **Целевой объект** |
|---|---|---|---|---|
| Несанкционированная модификация уставок технологического процесса с последующим аварийным остановом | | | OPC-сервер | ПЛК |
| **Шаг 4** | | **Способы реализации** | | |
| Несанкционированная модификация прошивки | | СП.21.3 Искажение данных<br>СП.23.2 Модификация прошивки (микропрограммы) | | |
| **Тактики MITRE Att&CK** | **Техники MITRE Att&CK** | **Техники методики ФСТЭК России** | **Угрозы (новый раздел БДУ ФСТЭК России)** | **Угрозы** |
| Impair Process Control | T0836 – Modify Parameter | T10.6 Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства<br><br>T10.12 Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления | УБИ.3 – Угроза несанкционированной модификации (искажения) | УБИ.179 – Угроза несанкционированной модификации защищаемой информации<br><br>УБИ.027 – Угроза искажения вводимой и выводимой на периферийные устройства информации<br><br>УБИ.183 – Угроза перехвата управления автоматизированной системы управления технологическими процессами |
| | T0831 – Manipulation of Control<br><br>T0827 – Loss of Control | | | |
| Impact | T0813 – Denial of Control | | | |

# Примеры: описание негативных последствий

| Факторы, нарушающие оптимальный технологический режим | Возможный сценарий развития событий | Негативные последствия |
|---|---|---|
| Несанкционированное изменение положения регулирующих клапанов подачи греющей или нагреваемой среды | ○ Повышение давления в трубопроводе или емкостях с нагревающей (греющей) средой ➔ разрушение стенок трубопровода или емкости ➔ разлив нефти и выброс газов ➔ пожар разлива<br><br>○ Повышение давления в трубопроводе или емкостях с нагреваемой (греющей) средой ➔ разрушение стенок трубопровода или емкости ➔ разгерметизация трубопровода или емкости ➔ разлив нефти и выброс газов ➔ образование облака газовоздушной смеси ➔ взрыв | ○ Ущерб жизни и здоровью персонала<br>○ Разрушение оборудования |
| Отказ датчиков или некорректные значения, получаемые с датчиков | ○ Несвоевременное срабатывание (несрабатывание) противоаварийной защиты ➔ избыточное давление или нагрев среды ➔ разрушение стенок трубопровода или емкости, запорно-регулирующей арматуры ➔ разгерметизация трубопровода или емкости, запорно-регулирующей арматуры ➔ разлив нефти и выброс газов ➔ пожар разлива | ○ Ущерб жизни и здоровью персонала<br>○ Разрушение оборудования |

# Конкурентные преимущества для Заказчика

## Преемственность

- Использование результатов аудита, моделирования угроз ИБ, категорирования
- «Бесшовное» встраивание в систему управления рисками

## Адаптивность

- Универсальность и масштабируемость
- Оперативность актуализации ландшафта угроз и принимаемых мер

## Комплексность

- Учет всех аспектов и нюансов
- АСУ ТП + технологический процесс + бизнес-процесс
- Вовлеченность всех служб (ИБ и АСУ ТП)

## Завершенность

- Разработка дорожной карты реализации мер **с доказанной эффективностью**
- Доведение задачи «до числа»: бюджетирование и реализация

# Путь промышленной кибербезопасности как сервиса

- Объект КИИ – это не только информационная инфраструктура
- Обеспечение ИБ – от процесса к системной деятельности
- Анализ рисков – как инструмент оперативного реагирования
- Дополнение регулярной составляющей для повышения эффективности принимаемых мер

# Коротко о главном

## Единый знаменатель

Результат, понятный всем, – представление в денежном выражении последствий от реализации угроз

## Доказательная база

Обоснованные затраты на реализацию мер по обеспечению ИБ

## Точно в цель

Присвоение приоритетов мероприятиям по защите информации

Целенаправленный выбор внедряемых средств защиты информации

Инновации

Технологии

Отношения

# Реализация

Разработка базовой методологии и методик моделирования и анализа

Наработка базы типовых сценариев, цепочек событий, реестров рисков

Адаптация методик и моделей под отраслевую специфику

Автоматизация расчетов и рутинных операций

Разработка платформы предоставления сервисов

Предоставление услуг по риск-ориентированной модели **как сервиса ИБ**

# Контакты


## Айрат Мухаметшин

Начальник отдела
методологии и комплексной
экспертизы, Cloud Networks

моб. +7 (927) 673 – 56 – 33
a.mukhametshin@cloudnetworks.ru

CLOUD networks

# СОЗДАЕМ БЕЗОПАСНОЕ ЦИФРОВОЕ БУДУЩЕЕ НАШИХ ЗАКАЗЧИКОВ

Инновации

Технологии

Отношения