CLOUD networks

Особенности реализации СОИБ в условиях импортозамещения компонентов АСУ ТП

О КОМПАНИИ

Cloud Networks — инновационный бизнес-партнер ведущих компаний России, использующий неординарные подходы к решению ИТ и ИБ-задач бизнеса

Наша миссия — создавать глобальную безопасную цифровую среду, развивать отраслевые тренды и объединять профессионалов в сообщества

Наша задача — непрерывное развитие экспертизы в области ИТ/ ИБ и сбор знаний на базе CN Academy, чтобы отвечать на вызовы глобальной цифровизации

СПЕЦИАЛИЗАЦИЯ

- **С 2015 года работаем в сфере информационной безопасности**, являясь бизнес-партнером крупнейших компаний России из сфер промышленности, энергетики и финансового сектора
- Используем инновационные подходы к решению ИТ и ИБ-задач бизнеса, формируя архитектуру системы информационной безопасности, внедряя ПО наших партнеров – ведущих российских поставщиков решений ИБ - Kaspersky, Positive Technologies, UserGate, Киберпротект и других (более 100 партнеров)
- **Начиная с 2021 года, совместно с Kaspersky Antidrone развиваем направление ПАК Антидрон**

КИБЕРБЕЗОПАСНОСТЬ

Защищаем инфраструктуру, данные и приложения

АУДИТ И КОНСАЛТИНГ

Оцениваем риски, подбираем оптимальные решения

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Знаем, как построить сетевую инфраструктуру с нуля и оптимизировать ее

ОСНОВА СТРАТЕГИИ: БЕЗОПАСНОСТЬ В НАШЕМ ДНК

1 Берем ответственность за **цифровое будущее Заказчика**, внедряя комплексные системы обеспечения ИБ в первую очередь **на объектах промышленности и энергетики**, обеспечивающих устойчивость и развитие экономики России. Реализуем проекты на принципах **комплексной информационной безопасности**

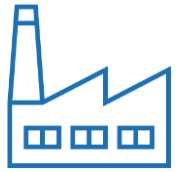
2 **Являемся авторизованным партнером** по всем проектируемым и внедряемым средствам защиты информации (СЗИ). Специалисты Cloud Networks регулярно проходят обучения и сдают сертификационные экзамены по проектируемым и внедряемым СЗИ, **постоянно внедряют инновационные методы и технологии**

3 **Специалисты Cloud Networks имеют богатый опыт проектирования**, установки и настройки всех актуальных классов средств и систем защиты: NGFW, EPP, NTA, СРК, SIEM, PAM, SWG, DLP, SandBox, VM и другие

Наш опыт и ключевые заказчики

НАШ ОПЫТ

Более **800** проектов реализовано в **29** регионах страны



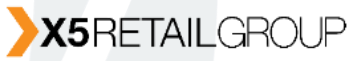
Нашими заказчиками являются **12** из **20** ТОП-компаний РФ

У нас работает более **40** профильных инженеров

Команды проектировщиков систем ИБ АСУ ТП и защиты конфиденциальных данных

КЛЮЧЕВЫЕ ЗАКАЗЧИКИ

CLOUD networks



КЛЮЧЕВЫЕ ПАРТНЕРЫ

CLOUD networks

positive technologies

R-Vision

INDEED ID

UserGate

КИБЕРПРОТЕКТ

kaspersky

phishman

Dr.WEB®

MULTIFACTOR

КОД безопасности

RST CLOUD
SIMPLE. SECURE. FLEXIBLE.

infotecs®

CHECK POINT™

Avanpost

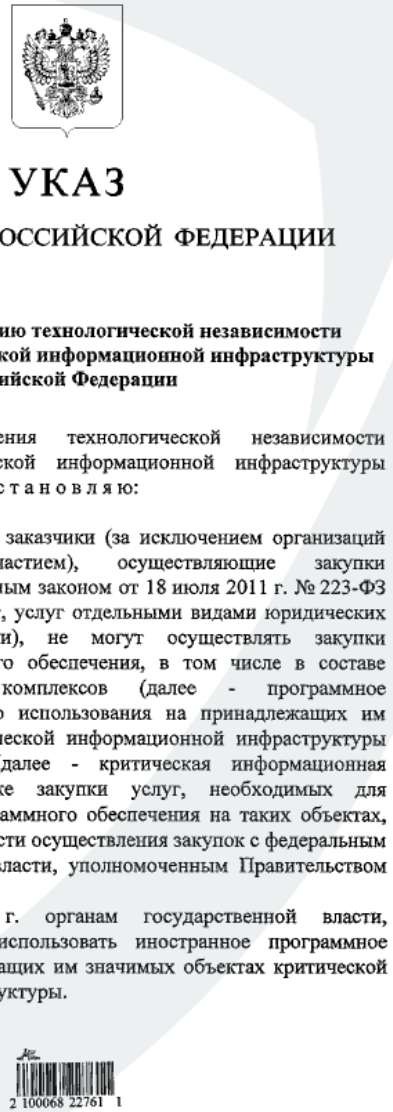
ГАРДА ТЕХНОЛОГИИ

Аладдин

В числе партнеров Cloud Networks – мировые лидеры, специализирующиеся на разработке и поставке средств информационной безопасности и информационных технологий

Особенности реализации СОИБ в условиях импортозамещения компонентов АСУ ТП

ПРАВОВЫЕ ТРЕБОВАНИЯ



УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации

В целях обеспечения технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации п о с т а н о в л я ю:

1. Установить, что:

а) с 31 марта 2022 г. заказчики (за исключением организаций с муниципальным участием), осуществляющие закупки в соответствии с Федеральным законом от 18 июля 2011 г. № 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" (далее - заказчики), не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов (далее - программное обеспечение), в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура), а также закупки услуг, необходимых для использования этого программного обеспечения на таких объектах, без согласования возможности осуществления закупок с федеральным органом исполнительной власти, уполномоченным Правительством Российской Федерации;

б) с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры.

2 100068 22761 1

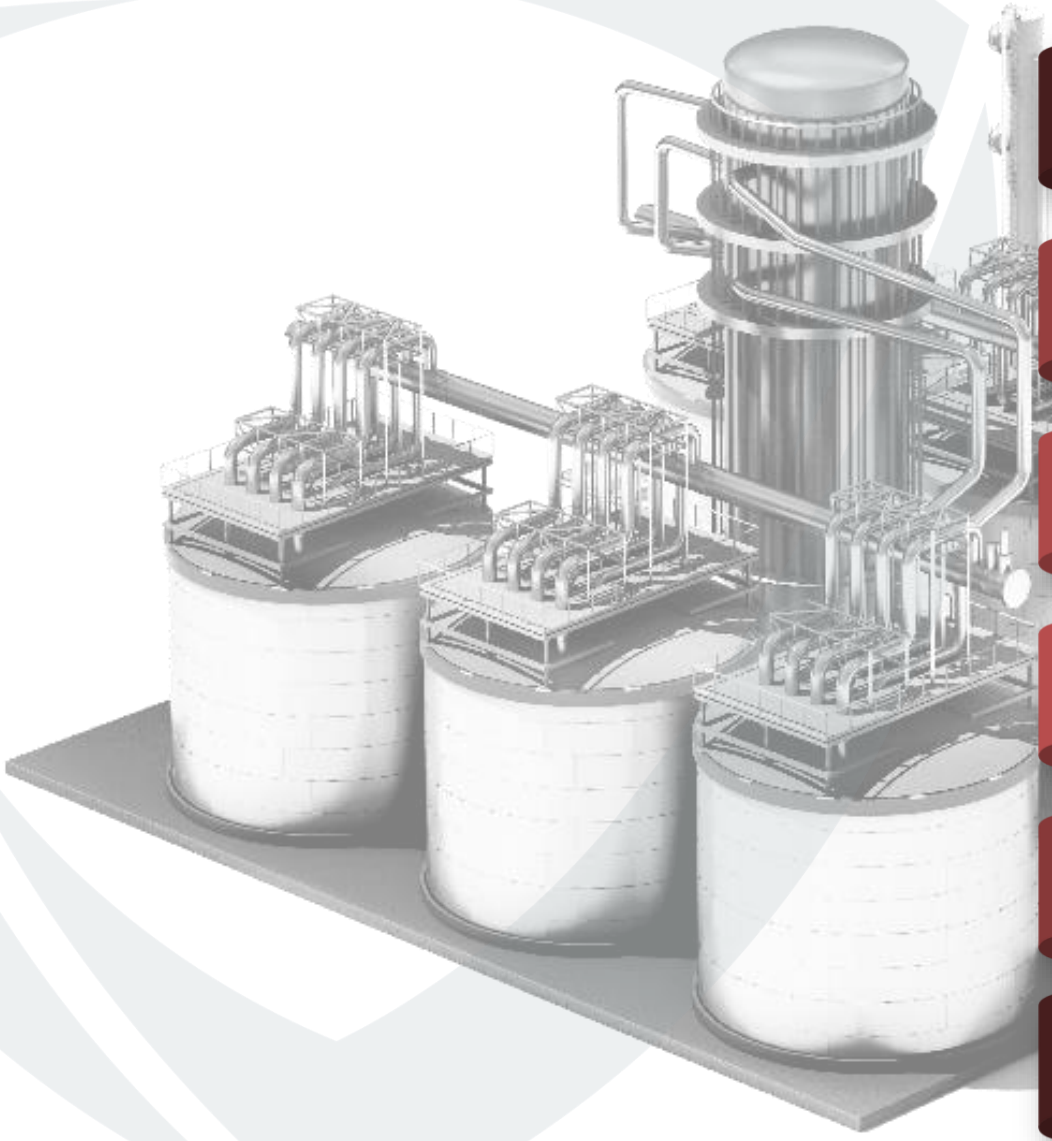
Указ президента Российской Федерации от 30 марта 2022 года № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»

- Запрет на закупку иностранного программного обеспечения на значимые объекты критической информационной инфраструктуры
- Поэтапный переход к использованию доверенных программно-аппаратных комплексов
- **Срок выполнения с 1 января 2025 года**

ПЛЮСЫ АРХИТЕКТУРЫ АСУ ТП, ПОСТРОЕННЫХ НА БАЗЕ ОТЕЧЕСТВЕННЫХ КОМПОНЕНТОВ

- Развитие внутреннего рынка и как следствие независимость от западных решений
- Снижение уровня рисков потери поддержки и обновлений
- Уход на отечественные ОС, которые обладают более высоким уровнем защиты
- Использование проприетарных либо специфических протоколов

МИНУСЫ АРХИТЕКТУРЫ АСУ ТП, ПОСТРОЕННЫХ НА БАЗЕ ОТЕЧЕСТВЕННЫХ КОМПОНЕНТОВ



- Отсутствие на рынке решений соответствующих высоким классам западных вендоров
- Сложность средств разработки
- Снижение уровня сервиса
- Отсутствие полноценной и актуальной документации
- Проприетарность вендорский решений
- Слабость встроенных средств защиты информации

СОСТЫКОВКА ОТЕЧЕСТВЕННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ С ОТЕЧЕСТВЕННЫМИ КОМПОНЕНТАМИ АСУ ТП

ПЛЮСЫ

- Совместимость компонентов АСУ ТП зачастую официально подтверждена разработчиком СЗИ
- Большинство отечественные вендоров в своих СЗИ осуществляют анализ множества проприетарных протоколов, используемых в отечественных АСУ ТП
- Отечественные вендоры СЗИ могут оперативно помочь в адаптации своих систем с АСУ ТП

МИНУСЫ

- **Неготовность работы СЗИ с отечественными ОС**
- **Не все модули в подсистемах готовы обеспечить тот же функционал** при защите серверов и АРМ под ОС Linux, который реализован в данных продуктах для линейки ОС Windows

СЛОЖНОСТИ ИНТЕГРАЦИИ С УЖЕ ВНЕДРЕННЫМИ В ПРЕДПРИЯТИИ СИСТЕМАМИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- **Отсутствие совместимости** компонентов АСУ ТП с используемыми в СОИБ подсистемах

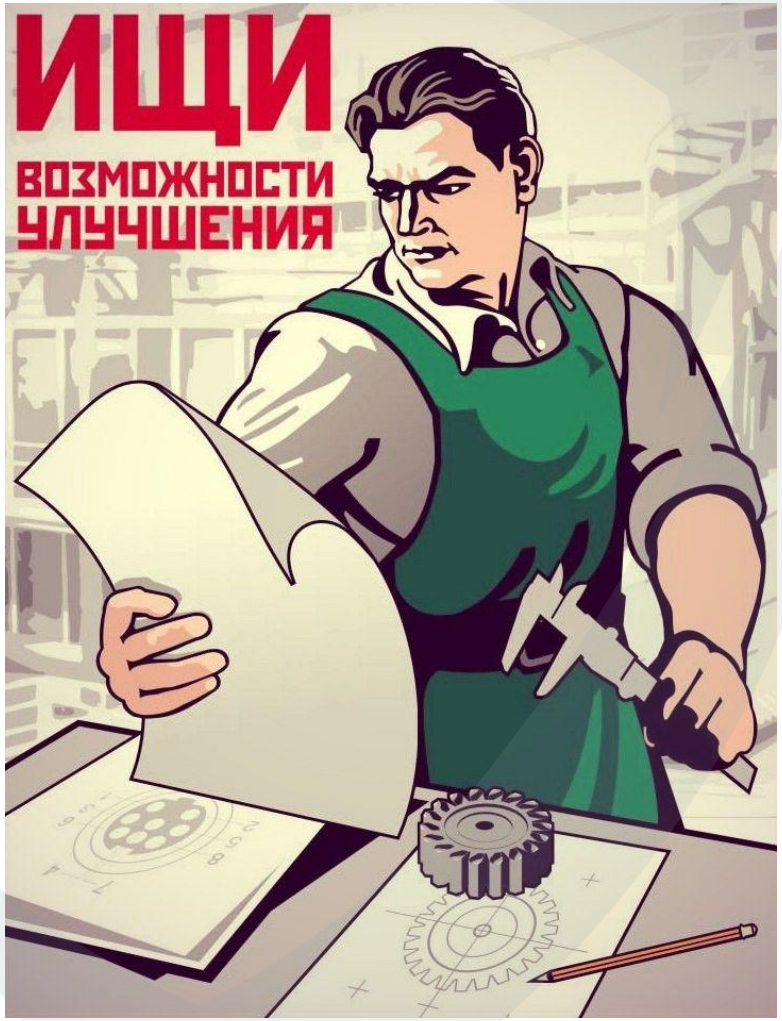
- **Отсутствие компетенций сотрудников ИБ** подразделений в настройке и управлении отечественными средствами защиты информации

ВЫБОР КОМПЕТЕНТНОГО ИСПОЛНИТЕЛЯ

На что обратить внимание:

- Разрешения на работы по ИБ на отечественном рынке (наличие лицензий ФСТЭК и ФСБ)
- Репутация и результаты работ исполнителя
- Ресурсы - кадровые и финансовые
- Сертификации от отечественных вендоров СЗИ
- **Опыт внедрения СЗИ в субъектах с импортозамещенными АСУ ТП**

ГРАМОТНЫЙ ПОДХОД К ЭТАПУ ПРОЕКТИРОВАНИЯ



Необходимо учесть:

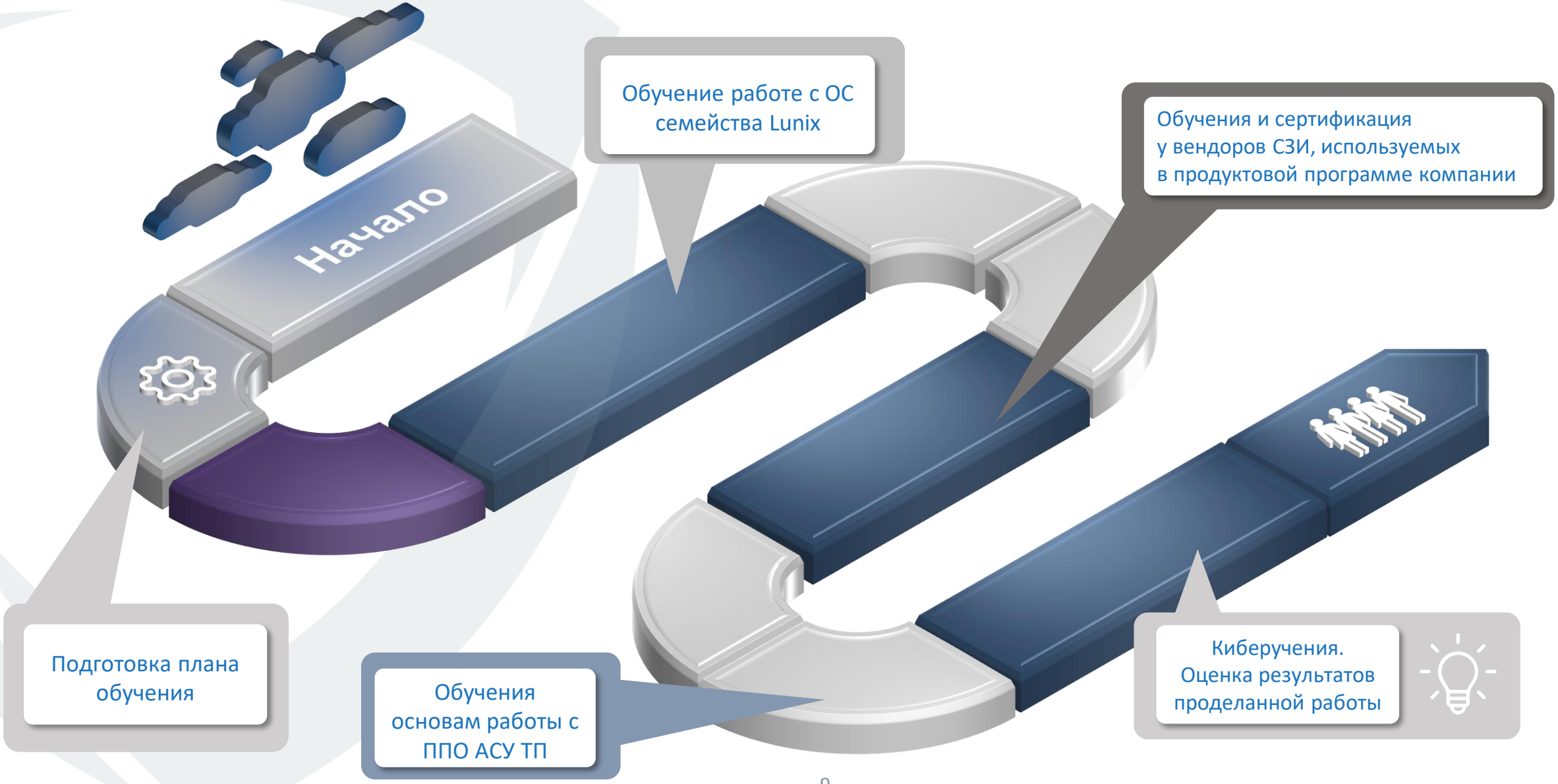
- Требования законодательства РФ в области защиты информации
- Архитектуру АСУ ТП
- Используемые средства защиты информации в корпоративном и технологическом сегменте сети
- Существующие в предприятие инженерные сети (коммуникации)

ОСТРОТА КАДРОВОГО ВОПРОСА В РАМКАХ ИМПОРТОЗАМЕЩЕНИЯ

Истоки проблемы:

- Сложность хантинга опытного ИБ-персонала для работы на территориально удаленных объектах
- Отток компетентных кадров зарубеж
- Исполнители имеют опыт работы только с западными ИБ-решениями
- Малый опыт использования и администрирования операционных систем семейства Linux
- Отсутствие у персонала опыта работы с решениями отечественных вендоров в области АСУ ТП

ПОДГОТОВКА КОМПЕТЕНТНЫХ КАДРОВ ДЛЯ ОБСЛУЖИВАНИЮ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



КОНТАКТЫ ДЛЯ ОТВЕТОВ НА ВОПРОСЫ

Проведение аудита ИБ АСУ ТП

https://cloudnetworks.ru/

https://cloudnetworks.ru/ib-asu-tp/

Начальник управления ИБ АСУ ТП

Дмитрий Кузин

+7 (495) 255-06-30

d.kuzin@cloudnetworks.ru