РТК-ЦОД

Облако КИИ

Особенности размещения ЗО КИИ

2012 — Ростелеком — DATALINE — РТК-ЦОД — 13 лет на рынке облачных сервисов → 2025

Единый партнёр по всем сервисам и решениям для построения надежной ИТ-инфраструктуры

25
дата-центров

Крупнейшая геораспределенная сеть дата-центров Tier III с отказоустойчивой инфраструктурой

300 000
физических ядер

27 000
стоек

260 МВт
мощность

190 ПБ
объем хранения

Безопасное и надёжное хранение данных

РТК-ЦОД

Облачные сервисы РТК-ЦОД базируются
в дата-центрах Tier III с отказоустойчивой инфраструктурой

Физическая безопасность размещения в собственных ЦОД

- Контроль и управление доступом с физически огражденным периметром безопасности
- Отказоустойчивость платформы: все узлы и компоненты продублированы
- Охранно-пожарная сигнализация
- Автоматическое пожаротушение
- Круглосуточная охрана и видеонаблюдение

Сертификаты международного образца соответствия требованиям ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019

Сертификат PCI DSS v4.0.1

Информационная безопасность (ИБ)

- Регистрация и учет действий администраторов
- Криптографическая защита каналов
- Межсетевое экранирование
- Антивирусная защита
- Защита от DDoS-атак
- Применение сертифицированных ФСТЭК и ФСБ средств защиты информации

Инфраструктура аттестована в соответствие требованиям 17-го и 21-го приказа ФСТЭК по защите персональных данных согласно 152-ФЗ

Соответствие «банковскому» ГОСТ Р 57580.1-2017

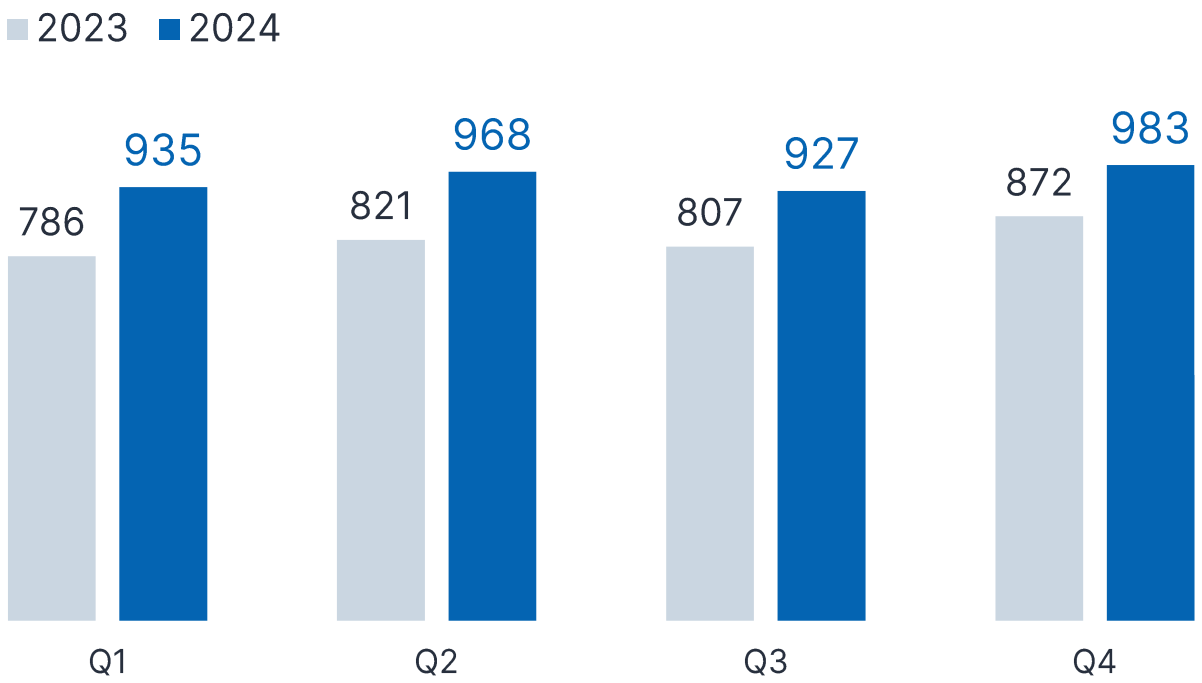
Лицензии, сертификаты и аттестаты

Актуальность защиты ЗО КИИ

РТК-ЦОД

1 января 2018 года вступил в силу №187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры РФ»

Сохраняется тренд на постоянный рост количества инцидентов



+16%

рост количества инцидентов по итогам 2024 года

64%

инцидентов по итогам 2024 года связано с организациями из отраслей КИИ

По данным Positive Technologies и RED Security.

Тенденции в сфере защиты КИИ

Ужесточение требований к объектам КИИ

Усиление контроля за категорированием объектов КИИ и выполнением мер защиты

Изменения в законодательстве

Предпосылки к отмене заявительного принципа отнесения информационных систем (ИС) к объектам КИИ РФ, что позволит однозначно сформировать перечень объектов

Требование по импортозамещению

Необходимо обеспечить все значимые объекты КИИ российским ПО с 1 января 2025 года согласно требованиям указа Президента РФ от 30.03.2022 № 166

Федеральный закон № 187-ФЗ

Основной нормативный правовой документ, регулирующий взаимодействие различных субъектов в сфере КИИ, — Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Нормативная правовая база по защите КИИ постоянно актуализируется и ужесточается

РТК-ЦОД

Федеральный закон № 187

Содержит основные требования
к мерам безопасности ЗО КИИ

Постановление правительства № 1912

Утверждает порядок перехода на отечественные доверенные программно-аппаратные комплексы

Указ Президента РФ № 166

Утверждает меры по обеспечению технологической независимости и безопасности ЗО КИИ

Приказ ФСТЭК № 239

Утверждает требования
по обеспечению безопасности ЗО КИИ

… и ещё более 30 НПА

Федеральные законы

Указы Президента РФ

Постановления Правительства РФ

Приказы ФСТЭК России

Список мер защиты ЗО КИИ согласно правовой базе

РТК-ЦОД

VM	Анализ защищенности
AV1	Антивирусная защита
СРК	Резервное копирование
ФИЗ	Физическая защита
UPD	Управление обновлениями
СОВ	Обнаружение вторжений
FW	Межсетевое экранирование
WAF	Защита веб-приложений
ОРД	Комплекс организационных мер
TEST	Тестовая среда

PAM	Контроль действий привилегированных пользователей
СЗИ от НСД	Защита от НСД
ЗСВ	Защита среды виртуализации
SIEM	Мониторинг событий ИБ
СКЗИ	Криптографическая защита информации
NTA	Анализ сетевого трафика
SandBox	Эмуляция вредоносной активности
AV2	Антивирусная защита отразличных производителей
ППО	Механизмы защиты прикладного ПО
ИДЧОР	Исключение доступа через общие ресурсы

ГЕОРЕЗЕРВИРОВАНИЕ

On-premise: проектирование, создание архитектуры и внедрение может занять 12–15 месяцев

РТК-ЦОД

1. Определение требований к защите
   1 месяц
2. Разработка концепции защиты
   1 месяц
3. Проектирование архитектуры
   1–2 месяца
4. Реализация и тестирование
   2–6 месяцев
5. Аттестация, доработки и ввод в эксплуатацию
   3–4 месяца
6. Отправка сведений о категорировании во ФСТЭК

Сокращение затрат времени на разных этапах за счёт использования Облака КИИ

РТК-ЦОД

Концепция защиты

Не придется прорабатывать инфраструктурную часть при разработке концепции защиты

Архитектура

Архитектура на уровне инфраструктуры уже проработана и закрывается аттестатом соответствия Облака КИИ

Оборудование

Не требуется тратить время на закупку оборудования, нет необходимости проводить его тестирование

Необходимо реализовать только то, что лежит выше слоя виртуализации

Обучение персонала

Заказчику не нужно организовывать дополнительное обучение и планировать дополнительный ФОТ на новых специалистов

На каждом этапе необходимы глубокая экспертиза и наличие компетенций у команды

РТК-ЦОД

Размещение ресурсов в Облаке КИИ может значительно сократить издержки заказчика

1

Определение требований к защите информации

- Анализ нормативных требований
- Классификация информации по степени конфиденциальности и критичности
- Оценка угроз и рисков безопасности

2

Разработка концепции защиты

- Формирование политик безопасности
- Выбор методов защиты
- Определение архитектуры безопасности

3

Проектирование защищенной архитектуры

- Разделение компонентов ИС по уровням защищенности
- Реализация механизмов контроля доступа
- Внедрение средств криптозащиты: ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012

4

Реализация и тестирование

- Выбор и закупка оборудования и ПО
- Разработка кода с учётом безопасного программирования
- Динамическое тестирование кода
- Проведение проверок на соответствие требованиям ФСТЭК

5

Аттестация / доработки и ввод в эксплуатацию

- Проведение ПНР и ПСИ
- Обучение персонала
- Подготовка нормативной документации
- Оценка соответствия ИС
- Отправка сведений во ФСТЭК

∞

Эксплуатация и мониторинг

- Организация контроля безопасности
- Реагирование на инциденты
- Постоянный аудит и обновление систем защиты

Сравнение вариантов размещения КИИ

РТК-ЦОД

On-premise

- ⊕ Полный контроль над ресурсами
- ⊖ Высокие капитальные затраты
- ⊖ Сложность масштабирования
- ⊖ Сложность проектирования архитектуры и ИС с учётом требований к ЗО КИИ
- ⊖ Сложность обслуживания оборудования
- ⊖ Длительные сроки реализации и проблемы аттестации

Облако КИИ

- ⊖ Внешняя инфраструктура
- ⊕ Сервисная модель затрат
- ⊕ Гибкое масштабирование
- ⊕ Сокращение затрат на проработку концепции защиты и проектирование архитектуры
- ⊕ Обслуживание оборудования на стороне провайдера
- ⊕ Оперативная реализация и аттестованная инфраструктура

Преимущества Облака КИИ

РТК-ЦОД

Обеспечение возможности аттестации ИС заказчика	Заказчик получает инфраструктуру, аттестованную по 187-ФЗ и соответствующую требованиям ГИС К1 и У3-1 ИСПД, что облегчает дальнейшую аттестацию его информационной системы
Импортозамещение оборудования и ПО	Облако построено только на отечественных решениях в части инфраструктуры и ПО и соответствует требованиям приказа ФСТЭК № 239 на уровне инфраструктуры, с которой заказчик сможет пройти проверку регуляторов
Ресурсы и масштабируемость	Легко изменять состав и количество ресурсов для ИС заказчика без дополнительных усилий на переаттестацию системы и не закладывая дополнительный CAPEX
Георезервирование	Облако реализовано на базе геораспределенных площадок

Зона ответственности провайдера
→ уровень инфраструктуры

РТК-ЦОД

Облачная инфраструктура
для размещения объектов КИИ

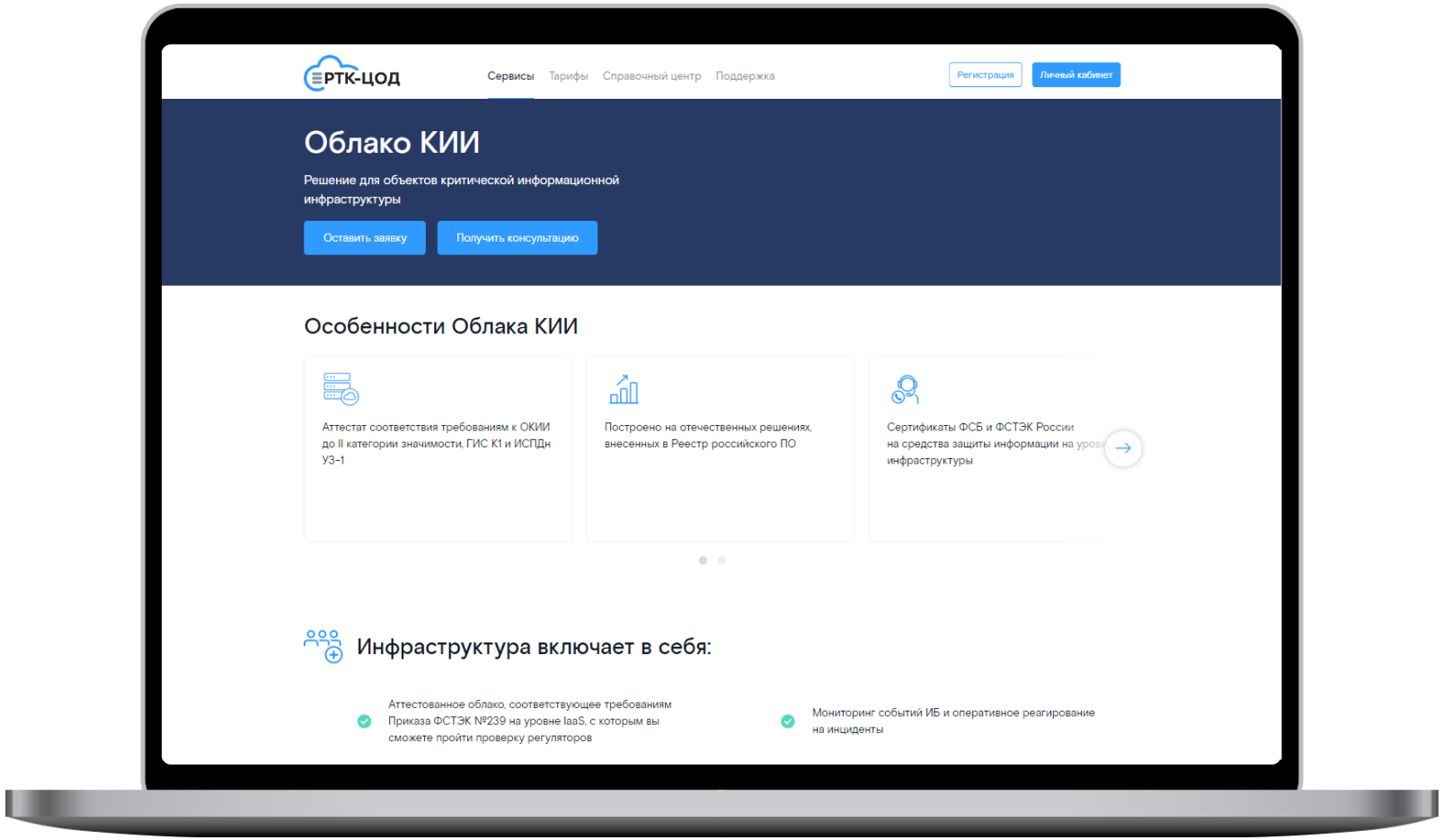
- Комплексная защита, включая аттестацию и обеспечение информационной безопасности
- Подключение к ГосСОПКА, взаимодействие с НКЦКИ по обмену информацией об инцидентах ИБ и проведение расследований

Заказчик

Ресурсы компании: информационные системы, виртуальные машины (ВМ)

- Определение категории значимости своих объектов КИИ
- Использование средств ИБ для защиты пула ресурсов компании
- Аттестация и подключение ИС компании к ГосСОПКА

РТК-ЦОД



cloud.rt.ru

РТК-ЦОД

Алексей Богачёв