ЦОДы и облака для КИИ

Кто за что отвечает?

Николай Носов
обозреватель-эксперт ИКС-Медиа

КИИ

Критическая информационная инфраструктура — это цифровой «каркас» экономики: системы, от которых зависит здоровье граждан, энергетика, транспорт и оборона.

Распределение ответственности

- Государство
- Субъекты КИИ
- Облачные провайдеры
- ЦОДы.

Кто за что

Оператор дата-центра отвечает за физическую инфраструктуру:

- контроль доступа;
- системы видеонаблюдения;
- электропитание и охлаждение;
- устойчивость инженерных систем.

Облачный провайдер отвечает за инфраструктурный уровень:

- платформу виртуализации;
- сетевую безопасность;
- базовые средства мониторинга;
- защиту от сетевых атак.

Субъект КИИ отвечает за уровень информационной системы:

- операционные системы и приложения;
- управление доступом пользователей;
- защиту данных;
- выполнение требований регуляторов.

Регулирование размещения КИИ в облаках

Параметр	Россия	США	ЕС	Китай
Основной подход	Единая система регулирования КИИ	Отраслевой подход	Экосистемный подход	Централизованный государственный контроль
Основные нормативы	187-ФЗ, приказы ФСТЭК	NIST, FedRAMP, NERC CIP, FFIEC	NIS2, GDPR, нац-е законы ЕС	Cybersecurity Law, Data Security Law, PIPL
Регуляторы	ФСТЭК, ФСБ, Минцифры	CISA, NERC, FFIEC, NIST	ENISA, национальные регуляторы	CAC (Cyberspace Administration of China)
Требования к облакам	Возможна аттестация инфраструктуры	Сертификация (FedRAMP) и аттестация	Управление рисками и аудит	Государственная сертификация облаков
Импортозамещение	Требуется отечественное ПО	Не регулируется	Не регулируется напрямую	Стимулируются национальные технологии
Локализация данных	Обязательна	Обычно не требуется	Для персональных данных	Обязательная
Публичные облака	Допускаются при соблюдении требований	Широко используются	Допускаются при управлении рисками	Сильно контролируются

Регуляторика КИИ

Документ	Что регулирует
187-ФЗ «О безопасности КИИ»	Определяет понятие КИИ, вводит обязанности субъектов КИИ, закрепляет ответственность за инциденты
Постановление Правительства №127	Устанавливает порядок категорирования объектов КИИ и критерии значимости
Приказ ФСТЭК №239	Определяет требования к защите значимых объектов КИИ (организационные и технические меры ИБ)
Нормативные документы ФСБ (СКЗИ)	Требования к криптографической защите информации и защищённым каналам связи
Указы Президента №250, №166	Требования к обеспечению кибербезопасности и переходу на отечественные решения
58-ФЗ (2025, изменения к 187-ФЗ)	Усиливает требования к КИИ, включая запрет на иностранное ПО для значимых объектов
Распоряжение Правительства РФ № 360-р от 26.02.2026	Перечень типовых отраслевых объектов КИИ

Что такое КИИ

Согласно Федеральному закону №187-ФЗ, объекты критической информационной инфраструктуры (КИИ) — это системы, которые играют важную роль в работе критических отраслей экономики. К ним относятся:

Информационные системы (ИС) — наборы данных и технологии, которые помогают обрабатывать эти данные.

Информационно-технологические системы (ИТС) — системы, которые передают информацию через линии связи.

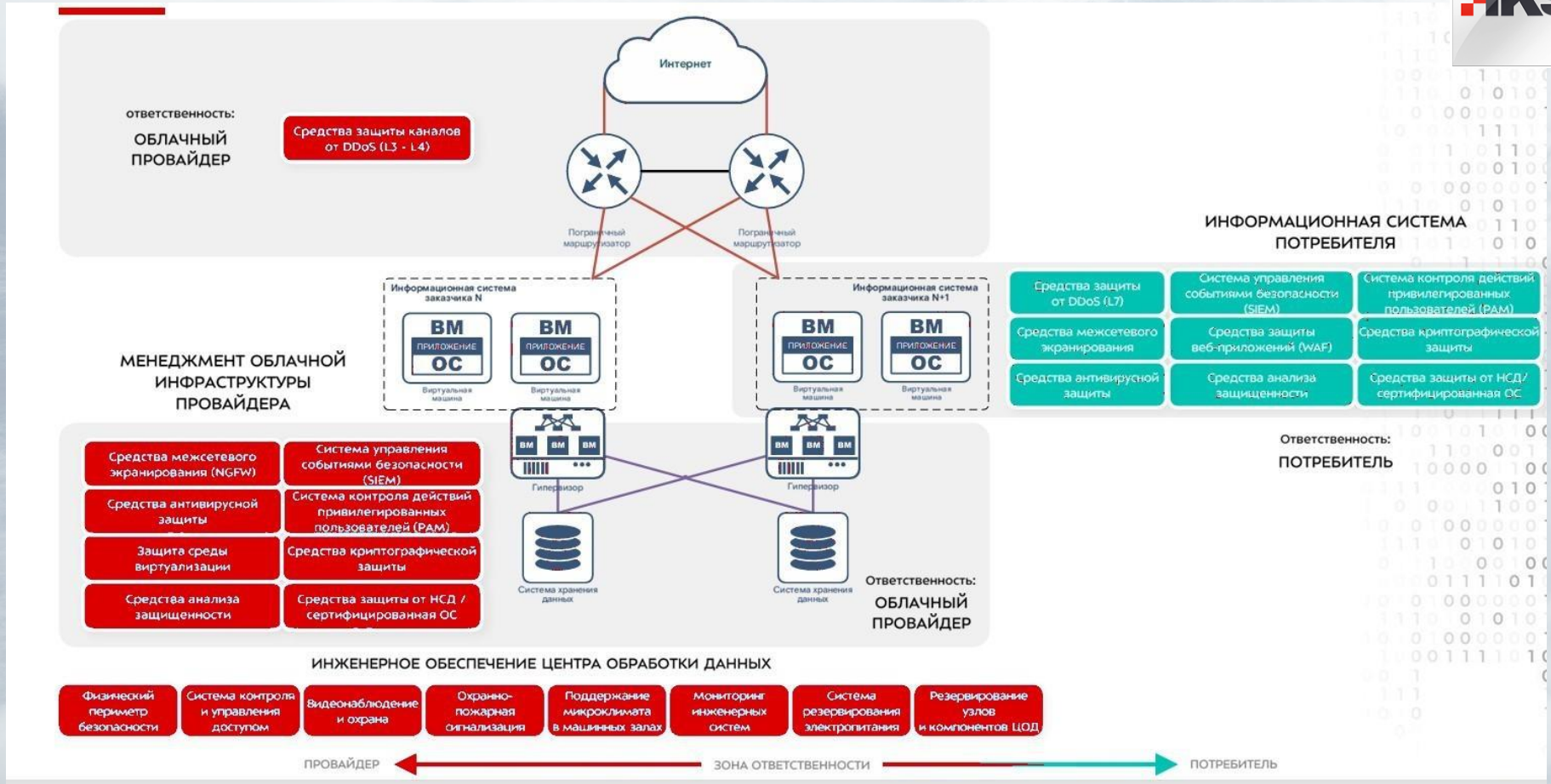
Автоматизированные системы управления технологическими процессами (АСУ ТП) — программы и устройства, которые контролируют работу производственного оборудования и управляют процессами.

Перечень типовых отраслевых объектов КИИ

	Наименование типового объекта критической информационной инфраструктуры Российской Федерации	Признаки значимости типового объекта критической информационной инфраструктуры Российской Федерации	
		типовые процессы (функции), выполняемые типовым объектом критической информационной инфраструктуры Российской Федерации	виды деятельности субъекта критической информационной инфраструктуры Российской Федерации*
93.	Информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, размещенные в центре обработки данных и обеспечивающие предоставление информационных, вычислительных и телекоммуникационных ресурсов, возможностей и услуг для функционирования значимых объектов критической информационной инфраструктуры в сфере связи	реализация процессов на всех стадиях (этапах) жизненного цикла значимых объектов критической информационной инфраструктуры с использованием цифровых продуктов, обеспечивающих создание, развитие и эксплуатацию значимых объектов критической информационной инфраструктуры; предоставление виртуальных ресурсов для размещения значимых объектов критической информационной инфраструктуры и хранения данных	63 Деятельность в области информационных технологий

Утверждено распоряжением Правительства РФ № 360-р от 26.02.2026

Архитектура облака КИИ



Источник: РТК-ЦОД

Требований ФСТЭК к облаку

Требование ФСТЭК	Как реализуется в облаке
Идентификация и аутентификация	IAM, MFA, ролевые аккаунты, интеграция с каталогами
Управление доступом	RBAC, сегментация, принцип минимальных привилегий
Регистрация событий	Централизованный сбор логов, SIEM/SOC
Антивирусная защита	Антивирус на ВМ и инфраструктуре, контроль образов
Обнаружение вторжений	IDS/IPS, WAF, анализ трафика
Сегментация	VLAN/VXLAN, микросегментация, изолированные контуры
Защита каналов	VPN, СКЗИ, шифрование по ГОСТ
Целостность	Контроль изменений, доверенные образы
Уязвимости	Сканирование, патч-менеджмент
Резервирование	Backup, DR, георезервирование
Защита виртуализации	Контроль гипервизора, изоляция ВМ
Физическая защита	Охрана ЦОД, контроль доступа, резервирование
Мониторинг	SOC 24/7, реагирование на инциденты
Оргмеры	Регламенты, SLA, разделение ответственности
СЗИ	Использование сертифицированных средств защиты

Требования ФСТЭК к инженерной инфраструктуре

Основные требования ФСТЭК (Приказ №239) по защите инженерной инфраструктуры:

Защита технических средств и систем: Обеспечение безопасности помещений, где размещается ИТ-оборудование (серверные, ЦОД), контроль доступа, защита от краж и физического вмешательства.

Обеспечение доступности: Создание условий для бесперебойной работы систем электропитания, кондиционирования, вентиляции, пожаротушения.

Контроль физической среды: Реализация мер по предотвращению воздействий на компоненты ИТ-системы через инженерные сети (например, электромагнитное воздействие, аварии в инженерных сетях).

Организационные меры: Планирование мероприятий по безопасности, реагирование на инциденты, обучение персонала по вопросам физической защиты.

Требования варьируются в зависимости от категории значимости объекта КИИ (1, 2 или 3 категория)

Риски клиента облака (1)

Риск	Суть проблемы	Что необходимо учитывать субъекту КИИ
Потеря прозрачности инфраструктуры	Часть инфраструктуры управляется облачным провайдером, а не владельцем системы	Необходимо прописывать механизмы аудита, мониторинга и доступа к журналам событий
Зависимость от одного провайдера	Использование одного облака может привести к риску отказа целого региона	Желательно проектировать архитектуру с резервированием по регионам или провайдерам
Ошибки конфигурации облака	Неправильные настройки доступа и сетевой политики могут привести к утечкам данных	Требуется строгая политика управления доступом и регулярные проверки конфигураций
Разграничение ответственности	Не всегда четко понятно, кто отвечает за безопасность конкретного уровня инфраструктуры	В договорах должны быть прописаны зоны ответственности и процедуры реагирования на инциденты
Риски внешних атак	Облачные инфраструктуры могут становиться целью DDoS-атак или атак на гипервизор	Необходимо использовать защиту от DDoS, системы IDS/IPS и мониторинг безопасности

Риски клиента облака (2)

Риск	Суть проблемы	Что необходимо учитывать субъекту КИИ
Требования регуляторов	Несоответствие инфраструктуры требованиям ФСТЭК или ФСБ может привести к запрету эксплуатации	Нужно выбирать облака с аттестованной инфраструктурой и сертифицированными СЗИ
Локализация данных	Данные КИИ должны храниться и обрабатываться на территории РФ	Провайдер должен гарантировать размещение данных в российских дата-центрах
Сложность миграции	Перенос критических систем в облако может быть технологически сложным и длительным	Требуется план миграции, тестирование и подготовка резервных сценариев
Риск отказа облачного региона	Инциденты в дата-центрах могут привести к остановке сервисов	Нужно реализовать георезервирование и планы аварийного восстановления (DR)
Контроль подрядчиков	Доступ к инфраструктуре могут иметь сотрудники провайдера и подрядчики	Требуются процедуры контроля доступа, логирование действий и соглашения о конфиденциальности

Преимущества облака КИИ

Преимущество	Суть	Практическая польза для субъекта КИИ
Быстрое развертывание инфраструктуры	Облачная модель позволяет развернуть вычислительные ресурсы и сервисы за часы или дни	Сокращение времени внедрения новых систем и модернизации инфраструктуры
Снижение капитальных затрат	Не требуется строить собственный дата-центр и закупать оборудование	Переход от капитальных инвестиций (CAPEX) к операционным расходам (OPEX)
Масштабируемость ресурсов	Возможность быстро увеличивать или уменьшать вычислительные мощности	Удобно для систем с переменной нагрузкой (банковские сервисы, порталы госуслуг и т.п.)
Повышенная отказоустойчивость	Использование нескольких дата-центров, зон доступности и резервирования	Снижение риска остановки критических сервисов
Готовая инфраструктура безопасности	Провайдеры внедряют сертифицированные средства защиты информации	Упрощается выполнение требований регуляторов (ФСТЭК, ФСБ)

Преимущества облака КИИ (2)

Преимущество	Суть	Практическая польза для субъекта КИИ
Экспертиза провайдера	У облачных операторов есть специализированные команды ИБ и эксплуатации	Повышается общий уровень защиты и мониторинга инфраструктуры
Геораспределенность	Возможность размещения систем в нескольких дата-центрах	Улучшение сценариев аварийного восстановления (DR)
Поддержка импортозамещения	По из ЕРРП	Упрощается соответствие требованиям регуляторов
Централизованный мониторинг и SOC	Облачные платформы интегрируют системы мониторинга безопасности	Быстрое обнаружение и реагирование на инциденты
Упрощение аттестации систем	Аттестованная облачная инфраструктура ускоряет сертификацию ИС заказчика	Снижение времени и затрат на соответствие требованиям КИИ

Сравнение облаков КИИ

Параметр	РТК-ЦОД	Cloud.ru	Т1 Облако	Туча
Соответствие регуляторике	187-ФЗ, ФСТЭК №239	187-ФЗ, ФСТЭК №239	187-ФЗ, ФСТЭК №239	187-ФЗ, ФСТЭК №239
Аттестация платформы	Аттестована	Аттестована	Категорировано как ЗОКИИ К1	Аттестована
Категория КИИ	До 2 категории	До 1 категории	1 категория	До 1 категории
Архитектура	Облако сообщества	Частные облака	Публичное облако	Публичное облако с проверкой контрагентов
Облачная платформа	Базис	Cloud.ru Evolution Stack	Т1 Cloud	СВ Брест (Astra Infrastructure Cloud)
Аппаратная платформа	Доверенные ПАК	Соответствует текущим требованиям	Соответствует текущим требованиям	Соответствует текущим требованиям

Рынок КИИ

20 отраслей отнесены к КИИ. На их долю приходится порядка 51% всех ИТ-бюджетов.

Удельный вес КИИ в совокупных ИТ-бюджетах российских заказчиков, 2024 г.

Доля затрат на КИИ в структуре ИТ-бюджетах российских предприятий, подпадающих под импортозамещение, % от общих ИТ-затрат

Источник: оценки iKS-Consulting

Облако — КИИ, ЦОД - нет

В договорах между сторонами должны быть подробно прописаны зоны ответственности, порядок реагирования на инциденты, требования к доступности сервисов и процедуры аудита.

Спасибо за внимание