



Как аттестовать информационную систему с помощью защищенного облака Astra Cloud



Максим Куртин

Директор департамента информационной безопасности «Группы Астра»



Наиль Енаев

Менеджер по развитию бизнеса, Astra Cloud



Почитать статью
на сайте

Приказ N°117 ФСТЭК России: что изменилось

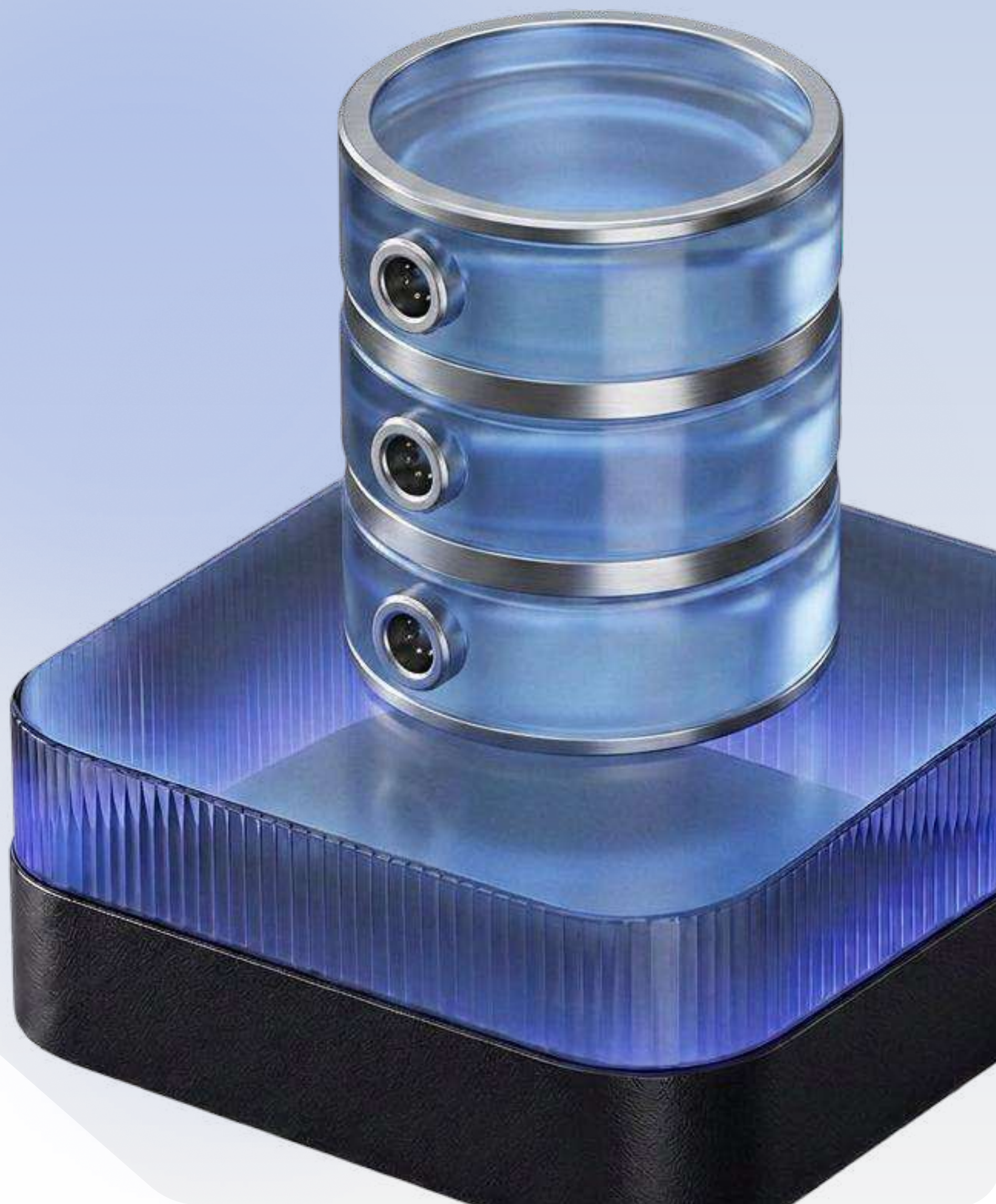
Вступил в силу в марте 2026, заменил приказ о защите государственных информационных систем.

Что нового:

- аттестация для любых информационных систем гос. органов, не только ГИС
- аттестация систем подрядчиков
- новые типы мер для: контейнеризации, защиты от DDoS-атак, защиты почтовых серверов
- сроки устранения уязвимостей
- коэффициенты защищенности:
показатель уровня зрелости (Пзи)
показатель защищенности (Кзи)

Опрос в чате

**Какие системы вам
нужно аттестовать?**



Что осталось без изменений

- требования к разработке модели угроз
- требования к архитектуре защищаемых систем и процессам обработки информации
- классификация систем: К1, К2, К3
- требования к используемым средствам защиты: все они должны быть сертифицированы

K1

высший класс

K2

средний класс

K3

базовый класс

Классы защищенности простым языком

Государственные информационные системы (ГИС)
Регулируется Приказом ФСТЭК №117

Какие бывают

Класс 1 (K1)

Высший класс. Применяется, если сбой грозит ущербом жизни людей, остановкой критических процессов или утечкой гостайны.

Класс 2 (K2)

Средний класс. Устанавливается при риске крупных финансовых потерь или сбоев в работе органов власти.

Класс 3 (K3)

Низкий класс. Назначается системам с минимальным потенциальным ущербом от нарушения безопасности.



Приказ N°21 ФСТЭК России: пока всё как прежде

В июле 2026 года на публичное рассмотрение опубликован проект приказа по обеспечению безопасности персональных данных.

Что нового:

- коэффициент защищенности:
показатель уровня зрелости (Пзи)
- новые типы мер для: контейнеризации,
защиты от DDoS-атак, защиты
почтовых серверов
- требования РБПО
- взаимодействие с ГосСОПКА

УЗ-1
максимальный

УЗ-2
высокий

УЗ-3
средний

УЗ-4
базовый

Уровни защищенности простым языком

Информационные системы персональных данных (ИСПДн)
Постановление Правительства РФ №1119

Какие бывают

УЗ-1

максимальный уровень требуется при обработке биометрических/специальных данных или угрозах 1-го типа.

УЗ-2

высокий уровень для крупных баз данных (от 100 тыс. человек) или угроз 1–2 типов.

УЗ-3

средний уровень при работе со стандартными данными до 100 тыс. человек и угрозах 3-го типа.

УЗ-4

базовый уровень для небольших баз данных (до 1 тыс. человек) при минимальных угрозах.

Опрос в чате

**Знаете ли вы какой
класс защищенности
нужен вашей системе?**



Защищённое аттестованное облако Astra Cloud

К моменту вступления в силу приказа №117
система защиты Astra Cloud была создана
и внедрена согласно новым требованиям



телефоны: (495) 363-01-33, 775-31-20
адрес электронной почты: info@step.ru

Лицензия ФСТЭК России рег. № 268 от 1 октября 2004 года

УТВЕРЖДАЮ
Коммерческий директор,
действующий на основании
доверенности № 2024-105 от 13.11.2024 г.
ООО «СТЭП ЛОДЖИК»


Д. А. Юшин
«15» июля 2026 г.

АТТЕСТАТ СООТВЕТСТВИЯ
ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ИНФОРМАЦИИ
Информационная система «Коммунальное облако»
№ 0268/00011/2026

Выдан: 15 июля 2026 г.

Действует бессрочно

Аттестат соответствия требованиям по защите информации

Настоящим АТТЕСТАТОМ СООТВЕТСТВИЯ удостоверяется, что объект информатизации «Информационная система «Коммунальное облако», принадлежащий ООО «Астра Облако», соответствует требованиям по защите информации, предъявляемым к информационным системам 1-го класса защищенности и информационным системам персональных данных 1-го уровня защищенности.



К-1

высший класс ГИС

УЗ-1

максимальный уровень ИСПДн

Классы аттестации Astra Cloud

Аттестовано по максимальному уровню требований:

- К-1 - высший класс защищённости для государственных информационных систем (ГИС)
Приказ ФСТЭК №117
- УЗ-1 - высший уровень защищённости для информационных систем, обрабатывающих персональные данные (ИСПДн)
Приказ ФСТЭК №21

К-1 и УЗ-1 - это потолок требований

Можно размещать информационные системы любого класса — от самых чувствительных до менее критичных



Используем сертифицированные КОМПОНЕНТЫ

Из ОС и других продуктов «Группы Астра»
по требованиям приказа №117



**Заказчику не нужно тестировать
СОВМЕСТИМОСТЬ** — все компоненты уже
протестированы и совместимы

Компоненты Защищенного аттестованного облака

Задействованные СЗИ



Межсетевые
экраны



Средства
антивирусной
защиты



Системы
обнаружения и
предотвращения
вторжений



Средства
доверенной
загрузки



Средства
криптографической
защиты



Система обработки
событий
безопасности



Система ключевой
инфраструктуры

Состав облачной платформы ASTRA CLOUD | Platform

Служба
каталога

ALD Pro

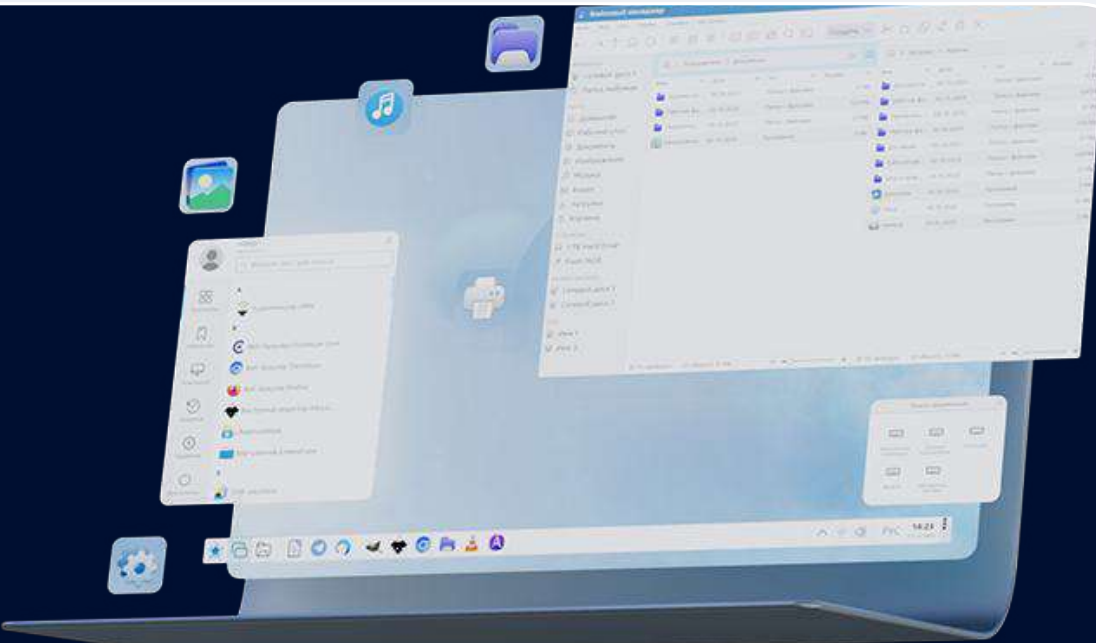
Средства виртуализации
ПК СВ «Брест»

Создание и управление виртуальными
машинами и инфраструктурой



Операционная система
Astra Linux Special Edition

Сертифицированная ОС со встроенными
средствами защиты информации (СЗИ)



Путь в Astra Cloud: от оценки до аттестации



1 Оценка и планирование

Определите класс защищённости ИС.
Проведите инвентаризацию ресурсов.
Рассчитайте необходимые мощности.
Сформируйте проектную команду.

2 Подготовка и миграция

Подготовка инфраструктуры со стороны ИТ и ИБ.
Перенос системы в защищённое аттестованное облако
Astra Cloud.

3 Аттестация

Подготовка к аттестации перенесенных ИС экспертами
Astra Cloud.
Проведение аттестационных испытаний.
Выдача аттестата соответствия.

4 Промышленная эксплуатация

Переход системы в рабочий режим в аттестованном
контуре (облако + ваша инфраструктура)

Опрос в чате

**Когда вы планируете
переход в облако?**



Защищенное аттестованное облако



Наиль Енаев

Менеджер по развитию бизнеса, Astra Cloud

Почему выгоднее аттестовать ИС в облаке

Потому что это способ подготовить инфраструктуру к аттестации без крупных вложений

Готовность к аттестации

- Контур уже аттестован К-1 и УЗ-1
- СЗИ входят в состав сервиса
- Не нужно с нуля строить систему защиты
- Не нужно поддерживать её под меняющиеся требования регуляторов



Железо дорожает

- Стоимость серверного оборудования и СХД продолжает расти
- Для аттестации нужны сертифицированные средства защиты



Ограничение бюджетов

- CAPEX-проекты сокращают в первую очередь
- Модель OPEX защищённого аттестованного облака снимает эту проблему
- Оплата за использование



Когда аттестованное облако необходимо



Нужна аттестация для тендера

Тендер требует аттестации, а ее еще нет, поэтому к конкурсу компанию не допускают

Нехватка кадров

В штате нет сертифицированного специалиста который может сопровождать аттестационные мероприятия

Предписание регулятора

Регулятор выдал предписание на несколько пунктов, и закрыть его точно не получается

Долгий перенос в аттестованный контур

DevOps-пайплайны не работают в аттестованной среде, перенос новой версии системы занимает 3-6 месяцев

Чувствительные данные для ИИ

ИИ работает с чувствительными данными, а с 1 марта 2026 года такие сервисы нельзя размещать в публичном облаке

Аттестованный контур переполнен

Собственный аттестованный контур заполнен, очередь на ресурсы для новых проектов и подрядчиков растет

Изменение требований регулятора

Требования регуляторов меняются ежегодно, и компания каждый раз настраивает инфраструктуру заново

Свой ЦОД не окупается

Всего 1-3 системы требуют высокого уровня защиты, но строить ради них отдельный ЦОД экономически невыгодно

Проверки ФСТЭК России

Подготовка к очередной проверке ФСТЭК занимает недели на сбор документов и сверку настроек

Опрос в чате

**С какой проблемой вы
сталкиваетесь при эксплуатации
защищенных информационных
систем?**



причин перейти
в защищённое
аттестованное
облако Astra Cloud

1 ОРЕХ вместо CAPEX

Не нужно вкладываться в оборудование заранее — платите за фактически используемые ресурсы

2 Экономия на аттестации

Инфраструктура облака уже аттестована по УЗ-1/К-1 — аттестовать нужно только саму информационную систему.

3 Дефицит ИБ-кадров

Обслуживание инфраструктуры и поддержку средств защиты берёт на себя команда Astra Cloud.

4 Устаревание оборудования

Собственный ЦОД требует регулярной модернизации. В облаке об актуальности «железа» и уровня защиты заботится провайдер.

5 Компетенции и инфраструктура под ключ

Готовая архитектура, сертифицированные СЗИ, ЦОД уровня Tier IV и команда экспертов ИБ

Что мы предлагаем

	Защищённое аттестованное облако	Выделенное облако
Формат	Защищённый аттестованный контур в облаке (изолированный)	Физически выделено, «без соседей»
Аттестация	Уже аттестовано: К-1, УЗ-1	Готово под аттестацию, но проходит её заказчик
Запуск	Дни, pay as you go	Проектный срок, от 10+ серверов
Кому	ИСПДн, чувствительные данные	Повышенные требования к ИБ, изоляция



ЦОД

Единственный в России ЦОД с полной сертификацией Tier IV по всем категориям



АТОМ DATA



- › Полная избыточность всех систем
- › Автономная система энергообеспечения
- › Независимые пути распределения
- › Минимальное время простоя
- › Устойчивость к отказам
- › Повышенные меры физической безопасности



Забота о клиентах

1 Помощь в подготовке к аттестации ИС

Предоставляем полный пакет документов на платформу, консультируем по вопросам прохождения проверок, помогаем взаимодействовать с аттестующей организацией.

2 Прозрачное разделение ответственности

Закрепляем в документах за что отвечает Astra Cloud, а за что Заказчик. Никаких зон риска.

3 Оперативная техническая поддержка

Круглосуточный мониторинг инфраструктуры и реагирование на инциденты в соответствии с заявленным SLA

4 Индивидуальный подход к сопровождению

Ресурсы VDC масштабируются по вашей заявке, дополнительные сервисы защиты (WAF, SIEM, DLP) подключаются по запросу с учетом ваших требований

5 Простота и предсказуемость

Оплата по OPEX, отсутствие скрытых платежей, фиксированная стоимость ресурсов и работ по индивидуальным проектам

Бизнес сценарии

Перенос ИТ-систем в Astra Cloud

Быстрый запуск систем соответствующих требованиям регуляторов (№117, №378, №21)

- > Госструктуры, финсектор, операторы ПДн
- > Готовая аттестованная IaaS (УЗ-1/К-1) без необходимости строить свою инфраструктуру
- > Готовый защищённый VDC за дни - быстрый запуск без CAPEX и аттестации инфраструктуры



Ускоренная аттестация новых ИС

- > Гос.сектор, медицинские организации, банковский и финансовый сектор
- > Готовая среда (УЗ-1/К-1) для быстрого запуска и упрощённой аттестации ИС
- > Сокращение сроков запуска в 3–5 раз - аттестовать нужно только ИС, инфраструктура уже аттестована



Переход на отечественную защищённую инфраструктуру

- > Переход с VMware / Hyper-V и др. зарубежных решений
- > Готовое импортозамещенное решение
- > На 100% состоит из российского ПО в реестре отечественного ПО имеет все необходимые сертификаты





Почему в облаке Astra Cloud
безопасность часто выше,
чем в своём ЦОД



Запросите
демонстрацию
на сайте

Свои продукты + решения лидеров

Экосистема «Группы Астра» и лучшие партнёрские СЗИ в едином защищённом контуре

ЦОД Tier IV без единой точки отказа

Atom Data – единственный в России ЦОД с полной сертификацией Tier IV по всем категориям

Устойчивость и доступность

Работа продолжается без сбоев при отказе любого компонента

Физическая защита

Многоуровневый контроль доступа, видеонаблюдение, обнаружение вторжений, шифрование данных



Будущее защищённого аттестованного облака Astra Cloud

- Создание облака для КИИ – приказ №239
- Защищённая контейнеризация в облаке – платформа «Боцман»
- Защищенные ИИ-решения в облаке
- Сервисы ИБ для заказчиков: мониторинг событий безопасности, анализ уязвимостей, антивирусная защита и др.
- Аттестация ИС заказчика в Astra Cloud «под ключ»

Опрос в чате

Что вам было бы полезно
получить после вебинара?

Готовы обсудить ваши задачи



**Алёна
Еникеева**

Коммерческий директор



+7 (985) 350-60-95



eenikeeva@astralinux.ru



**Юрий
Толстых**

Менеджер по работе
с партнерами



+7 (916) 684-36-43



itolstykh@astralinux.ru



Публично о продуктах Astra Cloud



astracloud.ru

Подробнее о продукте
и заказ демонстрации



ТГ-канал

Читать новости и блог