ASTRA CLOUD

АКТУАЛЬНО НА 2026 ГОД

ЧЕК-ЛИСТ

10 шагов для выполнения требований КИИ

Практический маршрут от первичного анализа до готовности к проверке регулятора

Статус субъекта КИИ влияет не только на ИБ-процессы, но и на требования к инфраструктуре, импортозамещению, взаимодействию с регуляторами и персональной ответственности руководства компании.

01 Определите, являетесь ли вы субъектом КИИ

Проверьте, работает ли организация в одной из 13 отраслей, перечисленных в 187-ФЗ:

- здравоохранение
- транспорт
- энергетика
- топливно-энергетический комплекс
- оборонная и ракетно-космическая промышленность
- сфера государственной регистрации прав на недвижимое имущество
- наука
- связь
- банковская сфера и финансовые рынки
- атомная энергетика
- горнодобывающая, металлургическая и химическая отрасли

⚠ ВАЖНО

Субъектом КИИ может оказаться и ИТ-компания, если она обеспечивает взаимодействие систем организаций из этих отраслей — интеграторы, провайдеры, разработчики корпоративного ПО для критических секторов.

Основание: 187-ФЗ, ст. 2

02 Создайте комиссию по категорированию

Сформируйте рабочую группу — она должна включать технических специалистов, представителей бизнес-подразделений и юридической службы. Комиссия будет принимать решения о присвоении категорий значимости объектам.

✦ ВАЖНОЕ НОВОВВЕДЕНИЕ

Теперь организациям не нужно самостоятельно доказывать критичность каждого процесса «с нуля». С ноября 2025 года порядок категорирования регулируется обновленным ПП №1762. Документ переводит категорирование на отраслевую модель: объекты КИИ определяются через типовые отраслевые перечни — утвержденные государством списки информационных систем, сетей и АСУ, подлежащих категорированию в конкретной отрасли. Перечни формируются профильными ведомствами и используются как базовый ориентир для идентификации объектов КИИ.

Основание: ПП №1762 от 18.11.2025

03 Проведите инвентаризацию и категоризируйте объекты

Зафиксируйте все информационные системы (ERP, CRM, медицинские ИС), сети передачи данных и АСУ ТП. Для каждого объекта оцените последствия потенциальной атаки и присвойте категорию:

1-я	Катастрофические последствия для страны или отрасли
2-я	Значительный ущерб в масштабе региона
3-я	Локальные последствия

Объект без существенных последствий признается незначимым — требования к нему минимальны.

Основание: ПП №127 (в ред. ПП №1762)

04 Направьте сведения о категорировании во ФСТЭК

После завершения категорирования передайте результаты в ФСТЭК России. Ведомство ведет реестр значимых объектов КИИ и вправе запросить актуализацию сведений при изменении инфраструктуры. Если по итогам проверки типового перечня состав ваших объектов изменился — необходимо пересмотреть прежние результаты и направить обновленные данные.

НЮАНС

Подать заявку или сведения о результатах категорирования объектов КИИ во ФСТЭК России можно только путем официальной отправки пакета документов почтой или курьером в территориальный орган регулятора по месту нахождения субъекта КИИ. Электронная подача документации напрямую на портале ведомства невозможна.

Основание: 187-ФЗ, ст. 7; Приказ ФСТЭК №236

05 Назначьте заместителя по ИБ или CISO

С 1 мая 2022 года назначение ответственного за информационную безопасность обязательно для всех субъектов КИИ. Это должен быть конкретный человек с полномочиями и ресурсами — фиктивное назначение фиксируется при проверках и квалифицируется как нарушение. Руководитель организации несет личную ответственность за ИБ-процессы.

Основание: Указ Президента №250 от 01.05.2022

06 Подключитесь к ГосСОПКА

Все субъекты КИИ обязаны информировать Национальный координационный центр по компьютерным инцидентам (НКЦКИ) об атаках и инцидентах.

ЗНАЧИМЫЕ ОБЪЕКТЫ	НЕЗНАЧИМЫЕ ОБЪЕКТЫ
не позднее 3 часов с момента обнаружения	**в течение 24 часов**

✦ С ЯНВАРЯ 2026 ГОДА

Действует Приказ ФСБ №548, закрепляющий порядок непрерывного взаимодействия: подключение через личный кабинет НКЦКИ и круглосуточный обмен данными. Подробнее — в регламенте взаимодействия с НКЦКИ.

Основание: 187-ФЗ, ст. 9; Приказ ФСБ №548 от 25.12.2025

07 Разработайте и внедрите систему защиты значимых объектов

Для каждого значимого объекта необходимо создать систему безопасности и внедрить технические меры защиты согласно Приказу ФСТЭК России №239. Требования сгруппированы в 14 функциональных группах:

ИАФ	Идентификация и аутентификация	УПД	Управление доступом
ОПС	Ограничение программной среды	ЗНИ	Защита машинных носителей информации
АУД	Аудит безопасности	АВЗ	Антивирусная защита
СОВ	Предотвращение вторжений	ОЦЛ	Обеспечение целостности
ОДТ	Обеспечение доступности	РКН	Регистрация событий в системе безопасности
АНЗ	Анализ защищенности	ОНВ	Безопасность облачных вычислений
ОТС	Безопасность персональной вычислительной техники	СИИ	Безопасность среды виртуализации

Все применяемые средства защиты должны пройти оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

Основание: Приказ ФСТЭК №239 от 25.12.2017 (ред. 28.08.2024)

08 Составьте дорожную карту импортозамещения

С июня 2026 года дорожная карта перехода на отечественное ПО обязательна для субъектов КИИ. Зафиксируйте в ней: текущий состав иностранного ПО и оборудования, российские альтернативы с оценкой функциональной совместимости, этапы и сроки замены. Документ потребуется при проверках и при заявке на продление сроков.

НЮАНС

Отраслевые планы импортозамещения утверждаются уполномоченными органами (в зависимости от отрасли). После этого организация обязана разработать собственный план перехода в течение 1 месяца и согласовать его с этим ведомством. Финально утвержденный план и сведения о текущем состоянии инфраструктуры направляются во ФСТЭК России — в бумажном (заказным письмом) и электронном виде на носителе.

Основание: Указ №166; методические рекомендации Минцифры

09 Перейдите на российское ПО и оборудование

1 января 2028	Основной дедлайн для значимых объектов КИИ
До 2031 года	При наличии контракта на разработку российского ПО, заключенного до 1 сентября 2027 года
До 2036 года	Для организаций из приоритетных правительственных программ

Значимые объекты КИИ должны работать исключительно на отечественном ПО. Переход затрагивает не только программное обеспечение, но и аппаратную платформу, включая серверное оборудование и процессорную архитектуру.

Оставить заявку на тестирование облака Astra Cloud на Baikal-S

Основание: Указ №166; ПП о дифференцированных сроках

10 Обеспечьте готовность к проверкам ФСТЭК России

ФСТЭК России проводит плановые и внеплановые проверки значимых объектов КИИ. Поддерживайте актуальность: модели угроз, организационно-распорядительной документации по ИБ, сведений о составе средств защиты и результатов категорирования. Проводите внутренние аудиты и фиксируйте инциденты — «не знали» перестало работать как аргумент при наличии прямых регуляторных требований.

Основание: 187-ФЗ, ст. 13; Приказ ФСТЭК №239