tech

Октябрь 2026

Размещение ГИС и ЗОКИИ в облаке

Что требуют регуляторы, как делится ответственность с облачной площадкой и что выяснить до подписания договора.

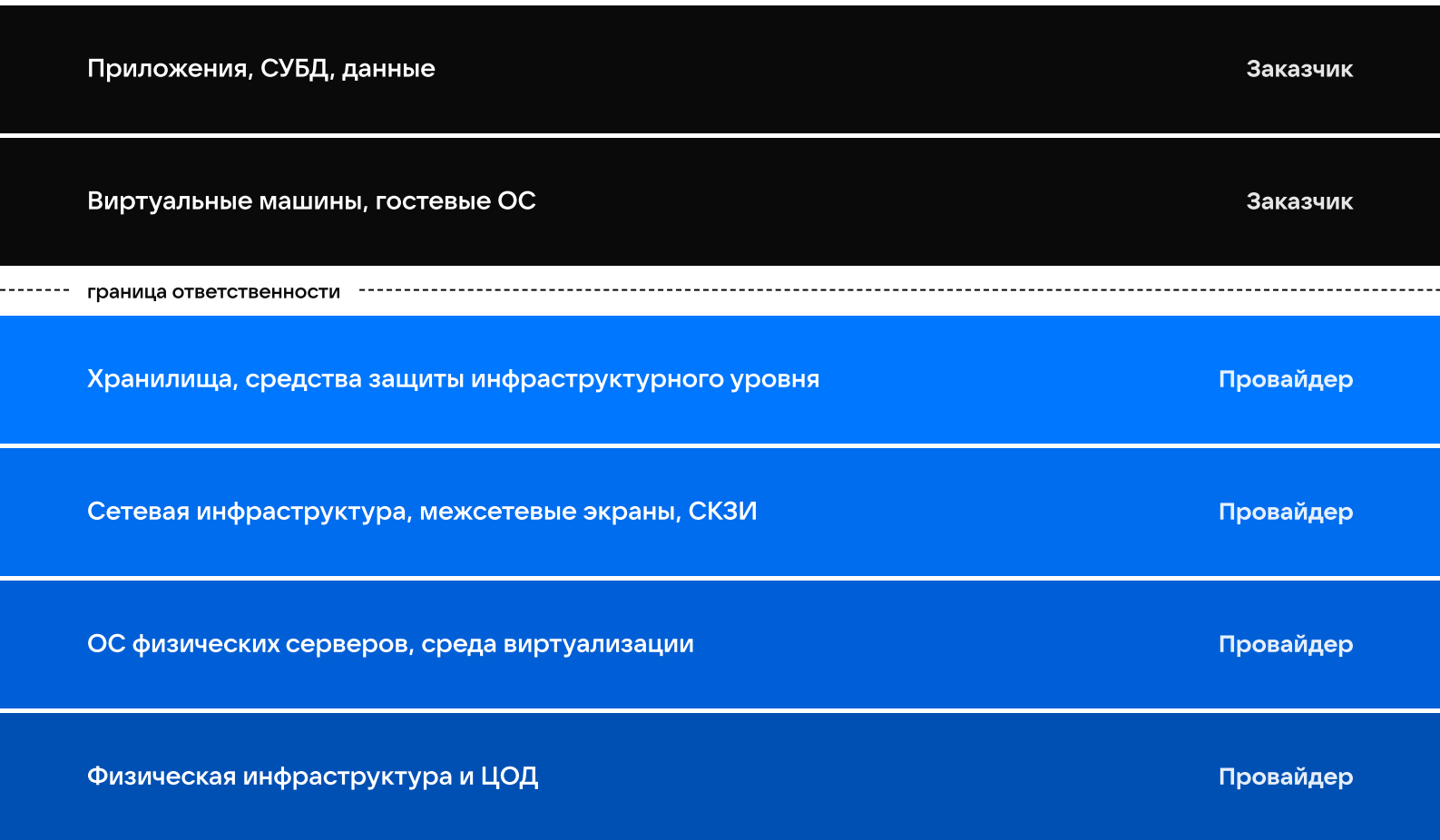
Справочник для руководителя ИТ или ИБ, который впервые ведёт такой проект или сверяет начатый с правилами 2026 года. Нормы приведены по состоянию на октябрь 2026 года.

1 Правовое поле 2026 года — с. 3

2 Категорирование КИИ и требования после него — с. 5

3 Модели размещения и границы ответственности — с. 7

4 Выбор площадки и план перехода — с. 9



Главное за 2026 год

1 сентября

У облака для ГИС появилась правовая основа

С 1 сентября 568-ФЗ разрешил использовать облачные сервисы для государственных систем, а ПП № 1024 задало условия: все компоненты в России, защита не ниже класса системы, требования к восстановлению и передаче данных прописаны в контракте.

№ 321

Криптотребования ФСБ дошли до облака

Приказ № 321 распространил их на внешние сервисы и оборудование, на которых работает ГИС.

1 марта 2027

Провайдера проверяют как подрядчика

Методика ФСТЭК от 7 августа задаёт целевые уровни зрелости, а с 1 марта 2027 года подрядчик с доступом к значимому объекту КИИ обязан рассчитать свой уровень ещё до получения доступа.

раз в полгода

Защищённость меряют раз в полгода

В ГИС с 1 марта 2026 года, на значимых объектах КИИ с 1 марта 2027 года.

3 часа

Счёт идёт на часы

Об инциденте на значимом объекте КИИ сообщают в НКЦКИ не позднее 3 часов, критическую уязвимость в ГИС закрывают за 24 часа, о сбое облачного сервиса для ГИС поставщик извещает заказчика не позднее 3 часов.

Как читать справочник

ГИС

Оператору ГИС пригодятся строки с пометкой «ГИС» в разделе 1, колонка «ГИС» в разделе 2 и план перехода на приказ № 117 в разделе 4.

КИИ

Субъекту КИИ: строки с пометкой «КИИ», шаги категорирования и колонка «Значимые объекты КИИ».

ГИС КИИ

Разделы 3 и 4 про модели размещения и выбор площадки общие для всех.

1 Правовое поле 2026 года

Основные документы для государственных информационных систем (ГИС) и значимых объектов критической информационной инфраструктуры (ЗОКИИ). Они сгруппированы по статусу: что действует с прошлых лет, что заработало в 2026 году и что вступит в силу позже.

Документ и срок	Кого касается и что устанавливает
Действуют с 2025 года или раньше	
действуют **Приказы ФСТЭК № 235 от 21.12.2017 и № 239 от 25.12.2017**	■ **КИИ: владельцы значимых объектов** № 239: требования к защите значимых объектов. № 235: требования к системе безопасности значимых объектов
с 01.09.2025 **Федеральный закон № 58-ФЗ от 07.04.2025** (поправки в 187-ФЗ)	■ **КИИ: владельцы значимых объектов** На значимых объектах применяется российское ПО при наличии аналога в реестре. Порядок и сроки перехода определяет Правительство
с ноября 2025 **ПП № 1762 от 07.11.2025** (изменения в ПП № 127)	■ **КИИ: все субъекты** Новые правила категорирования: объекты выявляют по перечню типовых отраслевых объектов, в сведения для ФСТЭК добавлены доменные имена и сетевые адреса объекта
Новое в 2026 году	
с 30.01.2026 **Приказ ФСБ № 547 от 25.12.2025**	■ **КИИ: все субъекты** Порядок информирования НКЦКИ. Об инциденте на значимом объекте сообщают не позднее 3 часов с момента обнаружения, на ином объекте КИИ и о компьютерной атаке не позднее 24 часов. Заменил приказ ФСБ № 282
с 26.02.2026 **Распоряжение № 360-р от 26.02.2026**	■ **КИИ: все субъекты** Перечень типовых отраслевых объектов КИИ: 397 позиций в 14 разделах. С него начинается категорирование
с 01.03.2026 **Приказ ФСТЭК № 117 от 11.04.2025**	■ **ГИС: операторы ГИС, иных ИС госорганов, ГУП и госучреждений** Новые требования к защите взамен приказа № 17. Ввёл показатель защищённости Кзи и показатель уровня зрелости Узи (до сентября 2026 года назывался Пзи), сроки устранения уязвимостей и долю профильных специалистов в подразделении защиты информации не ниже 30%. Аттестаты, выданные до 01.03.2026, сохраняют силу
с 12.03.2026 **Информационное сообщение ФСТЭК от 12.03.2026 № 240/22/1492**	■ **ГИС: операторы ГИС и иных систем госсектора** Разъясняет переход на № 117: для действующих систем нужно спланировать приведение в соответствие. Работы по договорам, заключённым до 01.03.2026, допускается вести по приказу № 17
с 07.08.2026 **Методика оценки уровня зрелости ФСТЭК от 07.08.2026**	**Операторы ГИС и ИСПДн, субъекты КИИ, их подрядчики** Пять уровней зрелости, оценка по 21 направлению. Целевой Узи: не ниже 1 для III категории, К3, УЗ-3 и УЗ-4; не ниже 2 для II категории, К2, УЗ-2; не ниже 3 для I категории, К1, УЗ-1. Требуемый уровень подрядчика закрепляют в договоре

Документ и срок	Кого касается и что устанавливает
Новое в 2026 году продолжение	
с 01.09.2026 **Приказ ФСТЭК № 60 от 27.02.2026** (изменения в порядок аттестации по приказу № 77)	**ГИС и муниципальные ИС. КИИ, если владелец значимого объекта выбрал аттестацию** Методы контроля защищённости: анализ уязвимостей и тестирование на проникновение. Пентест обязателен для систем К1 и К2 с выходом в интернет или связью с другими системами. Отчёт о контроле направляют во ФСТЭК не реже раза в три года, в течение пяти рабочих дней после его завершения
с 01.09.2026 **Федеральный закон № 568-ФЗ от 29.12.2025**	**ГИС: операторы ГИС и иных ИС госорганов** Делит ГИС на федеральные и региональные, разрешает использовать для них облачные сервисы в порядке, который задаёт Правительство, и обязывает операторов взаимодействовать с ГосСОПКА
с 01.09.2026 **ПП № 1024 от 18.08.2026**	**ГИС: операторы и поставщики сервисов** Правила использования облачных и других внешних сервисов для ГИС. Все компоненты сервиса находятся в России, его защита не ниже класса системы. В закупку и контракт включают требования к защите, резервному копированию, сроку восстановления и передаче данных заказчику. О сбое или нарушении защиты поставщик сообщает не позднее трёх часов, о привлечении соисполнителя за три рабочих дня
с 01.09.2026, часть норм с 01.03.2027 **Приказ ФСТЭК № 137 от 08.05.2026** (изменения в № 117)	**ГИС: операторы и их подрядчики** Пзи переименован в Узи. С 01.03.2027 во ФСТЭК направляют только показатель защищённости Кзи. Оператор может установить подрядчику требуемый уровень зрелости
с 01.09.2026 **Приказ ФСБ № 297 от 06.08.2026**	**ГИС: операторы ГИС и иных систем госсектора** Порядок взаимодействия с ГосСОПКА по 568-ФЗ. Об инциденте сообщают в НКЦКИ не позднее 24 часов. Личный кабинет открывают только после заключения регламента взаимодействия
с сентября 2026 **Приказ ФСБ № 321 от 22.08.2026**	**ГИС: операторы ГИС и иных систем госсектора** Требования к криптографической защите ГИС распространены на внешние облачные сервисы и оборудование, на которых работает система. Криптографическую часть модели угроз согласуют с ФСБ. Заменил прежние требования ФСБ от 18.03.2025
Впереди	
с 01.03.2027 **Приказ ФСТЭК № 220 от 16.07.2026** (изменения в № 235)	**КИИ: владельцы значимых объектов и их подрядчики** Для значимых объектов: Кзи не реже раза в полгода, Узи не реже раза в три года. Если Кзи ниже нормы, руководителя уведомляют в течение трёх календарных дней. Подрядчик с доступом к объекту рассчитывает Узи до получения доступа и не реже раза в три года
срок до 01.01.2030 **ПП № 1912 от 14.11.2023**	**КИИ: владельцы значимых объектов** Переход значимых объектов на доверенные программно-аппаратные комплексы

2 Категорирование КИИ и требования после него

Пять шагов категорирования КИИ

1 **Инвентаризация** информационных систем, АСУ и сетей.

2 **Сверка систем** с перечнем типовых объектов своей отрасли по распоряжению № 360-р.

3 **Оценка объектов** по критериям значимости: социальной, политической, экономической, экологической, а также значимости для обороны страны, безопасности государства и правопорядка. Показатели и их значения задаёт ПП № 127.

4 **Присвоение категории значимости** (I, II, III) или решение о её отсутствии. Решение принимает комиссия, которую создают приказом по организации.

5 **Направление сведений во ФСТЭК** в течение 10 рабочих дней после утверждения акта. ФСТЭК проверяет их до 30 дней и может вернуть, если сочтёт категорию присвоенной неверно, поэтому инвентаризация на первом шаге должна быть подробной.

Сроки

10
рабочих дней
на отправку сведений во ФСТЭК после утверждения акта

до 30
дней
ФСТЭК проверяет сведения и может вернуть их

20
рабочих дней
на отправку обновлённых сведений, если данные об объекте изменились

5
лет
категории пересматривают не реже раза в пять лет

Категории пересматривают не реже раза в пять лет, а также при изменении показателей значимости или отраслевых особенностей. Если сведения об объекте изменились, обновлённые направляют во ФСТЭК не позднее 20 рабочих дней.

Что требуется после категорирования или классификации

Требование	Значимые объекты КИИ	ГИС	ИСПДн
Основной документ	Приказы ФСТЭК № 239 и № 235, с 01.03.2027 в редакции № 220	Приказ ФСТЭК № 117 в редакции № 137	ПП № 1119, приказ ФСТЭК № 21. ФСТЭК готовит ему замену, проект опубликован в июле 2026 года
Градация	Категории I, II, III	Классы К1, К2, К3	Уровни защищённости УЗ-1 … УЗ-4
Регулярная оценка	С 01.03.2027: Кзи не реже раза в полгода, Узи не реже раза в три года. Если Кзи ниже нормы, руководителя уведомляют в течение трёх календарных дней	Кзи не реже раза в полгода, результаты во ФСТЭК в течение пяти рабочих дней. Узи не реже раза в два года. Отчёт о контроле защищённости во ФСТЭК не реже раза в три года	Оценка эффективности мер не реже раза в три года
Уязвимости	По требованиям приказа № 239	Критические: 24 часа. Высокого уровня: 7 календарных дней. Закрывают обновлением или компенсирующими мерами	По требованиям приказа № 21
Подтверждение соответствия	Оценка соответствия или аттестация, испытания проводит лицензиат ФСТЭК	Аттестация обязательна, проводит лицензиат ФСТЭК. С 01.09.2026 для К1 и К2 с выходом в интернет или связью с другими системами включает тестирование на проникновение	Аттестация по решению оператора
Инциденты	НКЦКИ: не позднее 3 часов с момента обнаружения инцидента, о компьютерной атаке не позднее 24 часов (приказ ФСБ № 547)	НКЦКИ: не позднее 24 часов (приказ ФСБ № 297). Сначала заключают регламент взаимодействия	Уведомление Роскомнадзора: 24 часа о факте, 72 часа о результатах расследования
Подрядчики с доступом	С 01.03.2027: подрядчик рассчитывает Узи до получения доступа и не реже раза в три года, владелец объекта закрепляет это в договоре	Обязательства по безопасности в договоре. Оператор может установить подрядчику требуемый уровень зрелости (приказ № 137)	Поручение обработки по 152-ФЗ

3 Модели размещения и границы ответственности

Где бы ни работала система, перед регулятором за неё отвечает её владелец.

Провайдер берёт на себя часть работ, и какую именно, зависит от модели размещения. Границу закрепляют в договоре матрицей ответственности. Для ГИС часть этой границы задаёт регулятор: условия ПП № 1024 включают в закупку и контракт, а криптографическую часть модели угроз владелец согласует с ФСБ по приказу № 321.

Три модели

заказчик · провайдер · вендор и заказчик



Модель

Аттестованное облако провайдера

Когда подходит

Нужен быстрый старт без строительства собственного защищённого контура

За заказчиком

Приложения, СУБД, виртуальные машины, аттестация своей системы

За провайдером

Всё ниже виртуальной машины, аттестат на инфраструктуру, комплект документов для аттестации заказчика

Затраты

Операционные: регулярная оплата ресурсов по договору



Модель

Частное облако на своей площадке

Когда подходит

Данные должны оставаться в собственном периметре

За заказчиком

Площадка, средства защиты, эксплуатация, аттестация систем

За провайдером

Сертифицированная платформа, её обновления и поддержка

Затраты

Капитальные или подписка



Модель

Гибрид

Когда подходит

Чувствительные контуры у себя, разработка и пиковые нагрузки в облаке

За заказчиком · За провайдером

По каждому контуру действует своя модель. Связность через сертифицированные СКЗИ

Затраты

Смешанные

Матрица ответственности по слоям

заказчик провайдер вендор и заказчик

Слой	Модель **Аттестованное облако провайдера**	Модель **Частное облако на своей площадке**
Физическая инфраструктура и ЦОД	**Провайдер**	**Заказчик**
ОС физических серверов, среда виртуализации	**Провайдер**	Платформа и обновления: вендор. Эксплуатация: заказчик
Сетевая инфраструктура, межсетевые экраны, СКЗИ	**Провайдер** Для ГИС криптографическую часть модели угроз согласует с ФСБ владелец системы	**Заказчик**
Хранилища, средства защиты инфраструктурного уровня	**Провайдер**	**Заказчик** на сертифицированных компонентах платформы
	граница ответственности ----------	
Виртуальные машины, гостевые ОС	**Заказчик**	**Заказчик**
Приложения, СУБД, данные	**Заказчик**	**Заказчик**
Аттестация системы	**Заказчик** на базе аттестата и документов инфраструктуры	**Заказчик** на базе сертификата платформы

4 Выбор площадки и план перехода

Восемь вопросов провайдеру до подписания договора

Разделы о соответствии требованиям на сайтах провайдеров почти неотличимы. Разница видна в ответах на вопросы ниже, поэтому задавайте их письменно. Для ГИС условия из вопросов 6 и 8 с 1 сентября 2026 года обязательно входят в контракт по ПП № 1024.

1 На какие классы систем аттестована инфраструктура?

Провайдер должен назвать классы ГИС, уровни ИСПДн и категории ЗОКИИ, реквизиты аттестата и акт классификации. Если вместо реквизитов звучат «сертифицированные СЗИ», перед вами другой продукт: облако со средствами защиты, но без аттестата инфраструктуры.

2 Что входит в границы аттестата?

Нужны технический паспорт, перечень площадок и сегментов, модель изоляции заказчиков и список соисполнителей с доступом к инфраструктуре.

3 Какие документы провайдер передаст для аттестации вашей системы?

Минимальный комплект: копия аттестата с приложениями, технический паспорт, модели угроз, формуляры, сертификаты средств защиты с уровнями доверия и схема разграничения ответственности. Перечень лучше согласовать до сделки.

4 Как устроена криптографическая защита?

Провайдер называет СКЗИ, их классы и сертификаты ФСБ и показывает, на каких участках шифруется трафик, в том числе внутри ЦОД, если этого требует модель угроз. Для ГИС это требование приказа ФСБ № 321.

5 Какой уровень зрелости подтвердит провайдер?

Значение Узи по методике ФСТЭК от 07.08.2026 должно быть не ниже целевого для вашей системы. Сам уровень стоит закрепить в договоре. Для значимых объектов КИИ с 1 марта 2027 года подрядчик с доступом обязан рассчитать Узи до получения доступа и затем пересчитывать не реже раза в три года.

6 Что будет с аттестатом в середине контракта?

ПП № 1024

В договоре должны быть порядок уведомления об изменениях платформы и о приостановке аттестата, контроль защищённости раз в три года, дополнительные испытания при изменениях, срок оповещения о сбоях и инцидентах и действия сторон. Для ГИС на оповещение о сбое ПП № 1024 отводит не больше трёх часов.

7 В каких реестрах числятся ПО и оборудование и кто их разработчик?

Ответ подкрепляют номерами записей в реестрах Минцифры и Минпромторга и записью в реестре ЦОД. Отдельно стоит узнать разработчика виртуализации и хранилища, а если стек сторонний, то в какие сроки провайдер обязуется ставить обновления.

8 Как устроен выход?

ПП № 1024

Форматы и сроки выгрузки, передача документации и журналов, помощь в миграции и подтверждение, что данные уничтожены после переноса. Для ГИС порядок передачи данных заказчику обязательно прописывают в контракте.

План перехода на приказ № 117

1. ☐ Составить перечень систем и действующих аттестатов со сроками их окончания.
2. ☐ Классифицировать системы по приказу № 117 и проверить, какие из них попадают в область его применения.
3. ☐ Подготовить план приведения систем в соответствие с перечнем мер и сроками. Необходимость такого плана ФСТЭК подчеркнула в информационном сообщении от 12.03.2026 № 240/22/1492.
4. ☐ Наладить расчёт Кзи раз в полгода с отправкой результатов во ФСТЭК в течение пяти рабочих дней и оценку Узи по методике от 07.08.2026.
5. ☐ Утвердить регламент устранения уязвимостей: критических за 24 часа, высокого уровня за 7 календарных дней.
6. ☐ Запланировать контроль защищённости раз в три года. Для систем К1 и К2 с выходом в интернет или связью с другими системами он включает тестирование на проникновение.
7. ☐ Довести долю профильных специалистов в подразделении защиты информации как минимум до 30%.
8. ☐ Заключить регламент взаимодействия с НКЦКИ по приказу ФСБ № 297: без него не откроют личный кабинет для передачи сведений об инцидентах.
9. ☐ При переезде в облако проверить область аттестации провайдера, согласовать матрицу ответственности и внести в контракт условия ПП № 1024.

Решения VK Tech

VK Secure Cloud

Аттестованное облако в дата-центре VK Tech

ГИС К1 | ИСПДн УЗ-1 | ЗОКИИ до I категории

- Аттестованная инфраструктура на отечественном оборудовании для ГИС К1, ИСПДн УЗ-1 и ЗОКИИ до первой категории.
- Изолированный аппаратный контур под каждого заказчика, компоненты собственной разработки, ПО и оборудование из реестров.
- Заказчик получает модели угроз, формуляры инфраструктуры и копию аттестата.
- Порядок обновления аттестата и регламент выхода входят в договор.
- Оплата за фактически заказанные ресурсы.



On-Premise

VK Private Cloud

Модульное частное облако на площадке заказчика

Сертификат ФСТЭК № 4857 | Реестр ПО № 6092 | ПО или ПАК

- Сертификат ФСТЭК № 4857: ГИС, ЗОКИИ, ИСПДн и АСУ ТП до первого класса, уровня или категории.
- Реестр российского ПО, запись № 6092.
- Поставка как ПО или готовый ПАК.
- Платформа разворачивается в контуре заказчика и остаётся в его эксплуатации.
- VK Tech отвечает за сертифицированные версии, обновления и поддержку.



Справочник подготовлен VK Tech

Материалы о размещении КИИ в облаке: cloud.vk.ru/kii-v-oblake