

Госкорпорации, ОПК и КИИ: почему данные и AI должны оставаться в локальном российском контуре

Юридические запреты, специальные требования и ответственность для государственного и военного сектора

Адресат: собственникам, органам управления, советам директоров и генеральным директорам госкорпораций, ОПК, предприятий с госучастием и субъектов КИИ

Дата подготовки: 7 июля 2026 г.

Назначение документа: краткое юридико-маркетинговое обращение к собственникам и руководителям предприятий о необходимости локального контура обработки данных и AI-инструментов.

Главный тезис: когда персональные данные граждан РФ, данные сотрудников, клиентские базы и корпоративные документы попадают в зарубежные облака или внешние AI-сервисы, собственник получает не технологическое ускорение, а юридический, регуляторный и репутационный риск.

1. Ключевой вывод для органов управления

Управленческий вывод

Для госкорпораций, предприятий ОПК, компаний с госучастием, субъектов 223-ФЗ и КИИ вопрос локального хранения данных шире, чем персональные данные. Речь идет о защите государственных информационных ресурсов, данных сотрудников, производственной документации, коммерческой тайны, информации ограниченного доступа, значимых объектов КИИ и возможных сведений, составляющих государственную тайну.

Использование зарубежных облачных сервисов, внешних AI-моделей, иностранных SaaS-платформ и неуправляемых подрядчиков в таком контуре может создать не только административный риск по персональным данным, но и риск нарушения специальных требований 149-ФЗ, 187-ФЗ, режима КИИ, режима государственной тайны и правил защиты информации.

2. Что прямо запрещено или недопустимо

Запрет / ограничение	Норма закона	Практический смысл для госсектора и ОПК
Не допускается выполнение ключевых операций с ПДн граждан РФ с использованием баз данных, находящихся за пределами РФ.	152-ФЗ, ст. 18 ч. 5; 149-ФЗ, ст. 16 ч. 4 п. 7	ПДн сотрудников, пропуска, анкеты, кадровые документы, медосмотры, зарплатные и контактные данные должны быть в российском контуре.
Нельзя начинать трансграничную передачу ПДн без уведомления Роскомнадзора; передача может быть запрещена или ограничена.	152-ФЗ, ст. 12; портал РКН	Передача ПДн сотрудников и контрагентов в иностранные сервисы или внешние AI-платформы требует предварительной процедуры и оценки рисков.
Технические средства информационных систем, используемых госорганами, МСУ, ГУП/МУП, государственными и муниципальными учреждениями, должны размещаться на территории РФ.	149-ФЗ, ст. 13 ч. 2.1	Для соответствующих организаций иностранная инфраструктура как техническая основа системы недопустима.
Операторы ГИС, МИС и информационных систем юридических лиц, работающих по 223-ФЗ, не должны использовать при эксплуатации размещенные за пределами РФ базы данных и технические средства, не входящие в состав таких систем.	149-ФЗ, ст. 13 ч. 2.1; 223-ФЗ, ст. 1	Для госкорпораций, госкомпаний и компаний с госучастием, подпадающих под 223-ФЗ, риск возникает при подключении внешних зарубежных SaaS/AI-компонентов.
При использовании хостинга для ряда государственных/муниципальных систем необходимо использовать вычислительные мощности провайдера из утверждаемого перечня; такой провайдер должен быть российским юрлицом и размещать технические средства в РФ.	149-ФЗ, ст. 13 ч. 2.1-1 и 2.1-2	Не любой "российскоязычный" или "удобный" хостинг подходит для государственных контуров; юридически важны статус провайдера и размещение оборудования.
Госорганы, ГУП, государственные учреждения и ряд муниципальных субъектов при создании/эксплуатации систем не вправе использовать принадлежащие иностранным лицам интернет-системы и программы, кроме случаев, установленных Правительством РФ.	149-ФЗ, ст. 13 ч. 2.4	Иностранные облачные AI-сервисы, SaaS и веб-приложения нельзя считать нейтральным инструментом без проверки прямого правового основания.
Не допускается передача информации из государственных информационных систем в иные информационные системы, не соответствующие требованиям о защите информации.	149-ФЗ, ст. 14 ч. 8.1	Передача данных из ГИС в внешние сервисы и AI-инструменты требует проверки соответствия требованиям защиты информации.

Субъект КИИ обязан создавать систему безопасности значимого объекта КИИ и обеспечивать предотвращение неправомерного доступа, копирования, предоставления и распространения информации.	187-ФЗ, ст. 10	Значимый объект КИИ не может быть “подключен к AI” без анализа угроз, доступа, журналирования, резервирования и требований безопасности.
Субъекты КИИ со значимыми объектами обязаны соблюдать требования безопасности и использовать допустимое ПО: российское ПО из реестра либо ПО, применяемое в защищенных государственных системах.	187-ФЗ, ст. 9 ч. 3 п. 5; 149-ФЗ, ст. 12.1	На значимых объектах КИИ иностранные или неучтенные программные компоненты могут быть неприемлемы без специального правового и технического обоснования.
Сведения, составляющие государственную тайну, не могут передаваться в открытые облака, внешние AI-сервисы и неконтролируемые информационные системы; разглашение влечет уголовную ответственность.	Закон РФ «О государственной тайне», ст. 5; УК РФ, ст. 283	В ОПК часть производственных, мобилизационных, военных, научно-технических и иных сведений может требовать закрытого сертифицированного контура.

3. Отдельный блок: кто попадает под 223-ФЗ и почему это важно

223-ФЗ прямо относит к заказчикам государственные корпорации, государственные компании, публично-правовые компании, субъекты естественных монополий, организации регулируемых видов деятельности, автономные учреждения, а также хозяйственные общества с совокупной долей участия РФ, субъекта РФ или муниципального образования более 50%. Поэтому для таких организаций ограничения 149-ФЗ по информационным системам и использованию зарубежных баз/технических средств должны рассматриваться как существенный комплаенс-риск.

Смысл для собственника и совета директоров

Если закупочная, кадровая, производственная, договорная, проектная или AI-система фактически использует зарубежную базу данных, иностранную облачную инфраструктуру или внешний AI-сервис, это нужно оценивать не как обычный IT-аутсорсинг, а как потенциальное нарушение режима эксплуатации информационной системы и защиты информации.

4. КИИ и оборонный сектор: почему внешний AI особенно опасен

Зона риска	Почему это критично	Безопасная модель ABS
АСУ ТП, производственные системы, инженерные базы, КБ и испытательные данные	Могут относиться к объектам КИИ или содержать сведения ограниченного доступа; внешняя обработка создает риск неправомерного доступа, копирования и раскрытия.	Изолированный локальный контур, доступ по ролям, журналирование, запрет внешней отправки, интеграция только с утвержденными системами.
Кадровый контур ОПК и госкорпорации	ФИО, должности, подразделения, допуски, контакты, командировки, зарплаты и медданные сотрудников являются ПДн и могут быть чувствительны для безопасности.	Локальная обработка ПДн сотрудников в российской инфраструктуре с разграничением прав и контролем выгрузок.
Документооборот с ГОЗ, подрядчиками и закрытыми проектами	Документы могут содержать коммерческую тайну, служебную информацию, данные по ГОЗ и потенциально сведения гостайны.	Раздельные контуры: открытый, внутренний, конфиденциальный, КИИ/закрытый; запрет на отправку секретных данных во внешние AI.
Внешние AI-сервисы и SaaS-платформы	Сервис может сохранять промпты, документы, метаданные, логи доступа и использовать иностранную инфраструктуру.	Локальные модели, локальная база знаний, контролируемый RAG, запрет передачи данных в зарубежные LLM по умолчанию.

5. Ответственность и последствия

Нарушение	Норма	Штраф / последствия
Нарушение локализации баз ПДн граждан РФ	КоАП РФ, ст. 13.11 ч. 8	Юрлица: 1-6 млн ₽; должностные лица: 100-200 тыс. ₽.
Повторное нарушение локализации	КоАП РФ, ст. 13.11 ч. 9	Юрлица: 6-18 млн ₽; должностные лица: 500-800 тыс. ₽.
Крупная утечка/неправомерная передача ПДн	КоАП РФ, ст. 13.11 ч. 12-14	Юрлица: от 3 до 15 млн ₽ в зависимости от масштаба.
Повторная крупная утечка/неправомерная передача ПДн	КоАП РФ, ст. 13.11 ч. 15	Юрлица: 1-3% выручки/капитала, но не менее 20 млн ₽ и не более 500 млн ₽.
Утечка специальных или биометрических ПДн	КоАП РФ, ст. 13.11 ч. 16-18	Юрлица: 10-20 млн ₽; повторно - 1-3% выручки/капитала, но не менее 25 млн ₽ и не более 500 млн ₽.
Нарушение требований в области безопасности КИИ	КоАП РФ, ст. 13.12.1	Юрлица: до 500 тыс. ₽; должностные лица: до 50 тыс. ₽, если нет признаков уголовного деяния.
Нарушение правил эксплуатации объектов КИИ	КоАП РФ, ст. 13.12.2	Юрлица: 100-500 тыс. ₽; должностные лица: 10-50 тыс. ₽; граждане: 5-10 тыс. ₽, если нет признаков уголовного деяния.
Разглашение государственной тайны	УК РФ, ст. 283	До 4 лет лишения свободы; при тяжких последствиях - от 3 до 7 лет лишения свободы.
Неправомерное воздействие на КИИ РФ	УК РФ, ст. 274.1	В зависимости от состава - принудительные работы/лишение свободы; при тяжких последствиях - до 10 лет лишения свободы.

6. Рекомендуемая позиция для внедрения ABS

Формулировка для обращения к госкорпорациям и ОПК

ABS - локальный AI-контур для предприятий с повышенными требованиями к защите данных. Персональные данные сотрудников, документы, производственная информация, сведения ограниченного доступа, контуры 223-ФЗ и КИИ обрабатываются внутри российской инфраструктуры заказчика, без вывода в зарубежные облака и внешние AI-сервисы.

Для госсектора и военного сектора ABS должен предлагаться не как “облачный AI-сервис”, а как локальная архитектура с возможностью развертывания в инфраструктуре заказчика, сегментацией контуров, управлением доступом, журналированием, контролем выгрузок и интеграцией с действующими системами предприятия.

- **Локальность.** Данные остаются в инфраструктуре заказчика или в российском контуре, соответствующем применимым требованиям.
- **Разделение контуров.** Открытые данные, ПДн, коммерческая тайна, КИИ и закрытые/секретные данные не смешиваются.
- **Управляемость.** Собственник и служба безопасности видят, какие агенты и сотрудники имеют доступ к каким данным.
- **Снижение зависимости.** Предприятие не зависит от иностранных облаков, санкционных ограничений, внешних LLM и скрытых политик обработки данных.
- **Комплаенс.** ABS создает техническую основу для соблюдения 152-ФЗ, 149-ФЗ, 187-ФЗ и внутренних режимов защиты информации; окончательная юридическая модель определяется проектным аудитом.

Нормативные ссылки

Ссылки ниже кликабельны в электронной версии PDF. Основной источник сводных редакций - КонсультантПлюс; для процедур трансграничной передачи дополнительно указан официальный портал Роскомнадзора.

1. [152-ФЗ, ст. 18 ч. 5 - локализация баз персональных данных](#) — источник: consultant.ru
2. [152-ФЗ, ст. 12 - трансграничная передача персональных данных](#) — источник: consultant.ru
3. [Роскомнадзор - уведомление о намерении осуществлять трансграничную передачу ПДн](#) — источник: pd.rkn.gov.ru
4. [149-ФЗ, ст. 16 - защита информации и локализация баз ПДн](#) — источник: consultant.ru
5. [149-ФЗ, ст. 13 - информационные системы, размещение техсредств, 223-ФЗ, хостинг](#) — источник: consultant.ru
6. [149-ФЗ, ст. 14 - государственные информационные системы](#) — источник: consultant.ru
7. [223-ФЗ, ст. 1 - круг заказчиков: госкорпорации, госкомпании, компании с госучастием](#) — источник: consultant.ru
8. [187-ФЗ, ст. 2 - субъекты и объекты критической информационной инфраструктуры](#) — источник: consultant.ru
9. [187-ФЗ, ст. 9 - обязанности субъектов КИИ и требования к ПО](#) — источник: consultant.ru
10. [187-ФЗ, ст. 10 - система безопасности значимого объекта КИИ](#) — источник: consultant.ru
11. [187-ФЗ, ст. 11 - требования по обеспечению безопасности значимых объектов КИИ](#) — источник: consultant.ru
12. [КоАП РФ, ст. 13.11 - ответственность за нарушения в области персональных данных](#) — источник: consultant.ru
13. [КоАП РФ, ст. 13.12.1 - ответственность за нарушения требований безопасности КИИ](#) — источник: consultant.ru
14. [КоАП РФ, ст. 13.12.2 - нарушение правил эксплуатации объектов КИИ](#) — источник: consultant.ru
15. [Закон РФ «О государственной тайне», ст. 5 - перечень сведений, составляющих гостайну](#) — источник: consultant.ru
16. [УК РФ, ст. 283 - разглашение государственной тайны](#) — источник: consultant.ru
17. [УК РФ, ст. 274.1 - неправомерное воздействие на КИИ РФ](#) — источник: consultant.ru

Оговорка: документ является информационно-аналитическим и маркетинговым материалом для обсуждения внедрения локального AI-контура ABS. Он не заменяет индивидуальное юридическое заключение, аудит ИСПДн, КИИ, режима коммерческой тайны, гостайны и требований ФСТЭК/ФСБ для конкретного предприятия.