Nevel

БЕЗОПАСНОСТЬ

Меры защиты и требования РФ

Как связать 152-ФЗ, ПП № 1119, ФСТЭК № 21 и № 117, обезличивание и уничтожение с технической архитектурой Nevel.

Облако / В контуре

https://docs.nevel.sh/security/rf-controls/

Для российского внедрения сначала определяется правовой и технический режим самой информационной системы, затем выбираются меры. Нельзя назначить уровень защищённости по названию продукта, числу масок или фразе «сервер находится в России». Nevel предоставляет механизмы, которые включаются в систему защиты заказчика; итоговая оценка относится к конкретным данным, инфраструктуре, участникам и процедурам.

Технические меры включаются в систему защиты с учётом применимых нормативных требований. Таблица соответствия механизмов сама по себе не является сертификатом, актом аттестации или заключением регулятора. Правовые основания, поручение и внешняя передача раскрыты в разделе о 152-ФЗ.

Сначала определить область системы

Описание внедрения должно отвечать на пять вопросов: какие данные обрабатываются, для какой цели, кто определяет эту цель, кто фактически получает данные и где находятся все компоненты. В перечень входят не только приложение и модель, но и OCR, embeddings, инструменты, журналы, поддержка и резервные копии.

On-prem обозначает размещение платформы у заказчика. Разрешённые маршруты моделей определяются отдельно: локальная модель, российский провайдер, self-hosted Nevel на серверах РФ или глобальный провайдер. Изолированный профиль — частный случай с обработчиками внутри инфраструктуры заказчика. Передача российскому облачному получателю выходит за её границу, но этот факт сам по себе не устанавливает трансграничную передачу. Политика различает ограничение периметром, требование к территории обработки и список разрешённых получателей; см. матрицу вариантов и оценку передачи.

Если система обрабатывает персональные данные, учитываются применимые требования 152-ФЗ и подзаконных актов. Государственная информационная система, иной контур государственного органа, учреждение или значимый объект критической инфраструктуры требуют отдельного определения применимости специальных требований. Сам факт покупки корпоративного ИИ не присваивает системе такой статус и не отменяет уже установленный режим.

Категории сведений фиксируются предметно: данные работников, клиентов и представителей контрагентов; содержание кадровых или медицинских документов; финансовая информация; коммерческая тайна. Технический детектор INN или MEDICAL_POLICY не является юридическим классификатором всех этих режимов. Для каждого процесса задаются допустимые операции и получатели.

Основные документы

Документ	Что он регулирует в рассматриваемом вопросе	Как используется при внедрении
152-ФЗ	Основания, принципы, обязанности участников и защита персональных данных	Реестр процессов, поручение, права субъектов, локализация и передача
Постановление Правительства № 1119 от 01.11.2012	Требования к защите персональных данных в информационных системах и уровни защищённости	Определение уровня для конкретной системы и исходных условий выбора мер
Приказ ФСТЭК № 21 от 18.02.2013	Состав организационных и технических мер защиты персональных данных	Выбор и адаптация мер с учётом актуальных угроз и используемых технологий

Документ	Что он регулирует в рассматриваемом вопросе	Как используется при внедрении
Приказ ФСТЭК № 117 от 11.04.2025	Защита информации в перечисленных государственных и иных системах	Отдельная проверка применимости к системе заказчика
Приказ Роскомнадзора № 140 от 19.06.2025	Требования и методы обезличивания вне указанного в нём специального случая	Оценка выбранного метода и организационного порядка
Приказ Роскомнадзора № 179 от 28.10.2022	Подтверждение уничтожения персональных данных	Акт, выгрузка и хранение подтверждений

Постановление № 1119 устанавливает четыре уровня защищённости; требуемый уровень определяется по условиям обработки, а не выбирается поставщиком как универсальное свойство платформы. Официальное сообщение и документ размещены на сайте Правительства РФ.

На портале Минздрава размещена копия приказа № 21 в редакции от 14.05.2020. При выборе мер учитывайте последующие изменения и действующую редакцию на дату внедрения. Нормативные документы Минздрава, приказ № 21.

Что изменилось для государственных систем

Приказ ФСТЭК № 117 вступил в силу 1 марта 2026 года и признал утратившим силу приказ № 17 от 11.02.2013 и перечисленные изменения к нему. В пункте 3 отдельно сохранена действительность аттестатов, выданных до вступления нового приказа. Поэтому ссылка только на № 17 в новом проекте требует пересмотра применимости; наличие старого аттестата не следует автоматически считать его аннулированием. Публикация приказа № 117, официальный PDF.

Область № 117 включает государственные информационные системы и указанные в названии и требованиях иные системы государственных органов, государственных унитарных предприятий и государственных учреждений. Его нельзя механически распространить на любую частную B2B-компанию. Конкретное применение определяется статусом системы и обрабатываемой информации.

Как технические меры собираются в систему защиты

Ниже приведено сопоставление задач защиты с механизмами Nevel и инфраструктуры. Это рабочая карта реализации; она не воспроизводит полный обязательный набор для каждого уровня и не подменяет выбор мер по актуальным угрозам.

Задача	Механизм в архитектуре	Проверяемое доказательство
Идентификация и доступ	SSO, личные пользователи, сервисные ключи, роли и права объектов	Отказ чужому пользователю и отозванному ключу
Разделение организаций	Контекст пространства на сервере, фильтрация хранилищ и RAG	Отсутствие чужой контрольной фразы в ответе, поиске и экспорте
Ограничение программной среды	Изолированные обработчики файлов и ограниченные инструменты	Документ не исполняет встроенную команду и не получает произвольную сеть
Защита носителей и данных	Шифрованное хранение, отдельные права, учёт копий	Недоступность копии обычному пользователю и восстановление уполномоченным
Регистрация событий	Связанные события доступа, политики, маршрута и удаления	Воспроизводимая цепочка одного запроса
Защита от вредоносного содержимого	Безопасный разбор, ограничения ресурсов, подключённые средства защиты	Отказ опасного файла без обхода обязательной проверки
Контроль защищённости	Негативные проверки и повторные испытания после изменений	Протокол с версией продукта и фактическим результатом

Задача	Механизм в архитектуре	Проверяемое доказательство
Целостность	Контроль источников знаний, версий политики и артефактов	Обнаружение изменения и проверка происхождения результата
Доступность	Резервирование в пределах допустимого маршрута и восстановление	Испытание отказа без выхода в запрещённую модель
Защита сети	Сегментация, TLS, разрешённые получатели, свой AI firewall	Сетевой след и блокировка прямого обхода
Реагирование	Мониторинг, ограничение маршрута, расследование	Карточка инцидента и подтверждённое устранение причины
Управление конфигурацией	Версии правил, отдельные полномочия, контроль обновлений	История изменения и повторный тест затронутого сценария

Физическая защита площадок, виртуализация, защита рабочих станций и организационные процедуры реализуются на уровне соответствующей инфраструктуры. В облаке за часть этих мер отвечает эксплуатация поставки; в on-prem за установленную у заказчика часть — заказчик или его исполнитель. При разрешённом внешнем модельном маршруте инфраструктура получателя рассматривается отдельно. Границы закрепляются в матрице ответственности, чтобы один и тот же контроль не оказался предположительно выполненным обеими сторонами без доказательства.

Обезличивание и обратимые маски

Приказ Роскомнадзора № 140 действует с 1 сентября 2025 года. Он предусматривает, в частности, метод введения идентификаторов и отдельное хранение ключа сопоставления оператором без передачи третьим лицам. Требования включают оценку достаточности метода, защиту обработки, раздельное хранение соответствующих массивов и учёт действий. Поэтому обратимость сама по себе не означает отсутствия предусмотренного нормативным актом метода, но одной замены ФИО недостаточно для вывода о соблюдении всех требований. Официальный приказ № 140, приложения 1–2.

Для облачной схемы отдельно оцениваются роли оператора и исполнителя, расположение и доступ к соответствиям, состав передаваемого текста и получатели. Нельзя из факта существования метода вывести универсальное разрешение отправлять любой результат иностранной модели. В Nevel чувствительная категория может иметь обязательный российский или внутренний маршрут независимо от наличия масок.

Постановление Правительства № 1154 от 01.08.2025 регулирует специальный процесс обезличивания, связанный с предоставлением данных по требованиям в рамках статьи 13.1 152-ФЗ. Его не следует автоматически использовать как общий режим для любого корпоративного чата. Публикация постановления № 1154.

Подтверждение уничтожения

При автоматизированной обработке приказ № 179 предусматривает акт об уничтожении и выгрузку из журнала. Пункты 3 и 5 определяют сведения о субъектах или идентифицирующей информации, категориях данных, системе, причине и дате; акт дополнительно описывает участников и способ. Недостающие в выгрузке сведения включаются в акт по пункту 6. Подтверждения хранятся три года с момента уничтожения по пункту 8. Официальный приказ № 179, пункты 2–8.

Техническая реализация описана в хранении и удалении. Акт должен отражать фактическую область уничтожения, включая ограничения резервных копий, а не объявлять удалённым то, что продолжает выдаваться поиском или восстанавливается в рабочую систему. Сам акт содержит защищаемые сведения и имеет отдельный режим доступа.

Проектная и эксплуатационная документация

Для оформления проекта могут использоваться ГОСТ Р 59793-2021 о стадиях создания автоматизированных систем и ГОСТ Р 59795-2021 о содержании документов. Их карточки Росстандарта подтверждают предмет стандартов и статус действия; конкретный состав документации закрепляется в требованиях проекта. Ссылка на стандарт оформления не подтверждает автоматически выполнение всех мер защиты. ГОСТ Р 59793-2021, ГОСТ Р 59795-2021.

Практический пакет включает описание системы и потоков, модель угроз, матрицу прав, политику категорий и маршрутов, реестр получателей, правила хранения, процедуры управления секретами, программу испытаний, регламент обновлений и реагирования. Каждый документ содержит владельца, версию и область действия. Протокол испытаний ссылается на установленную конфигурацию, а не только на публичное описание возможностей.

Сертификаты и обязательные свойства

Если для системы требуется применение конкретных средств защиты, прошедших оценку соответствия, проверяются средство, версия, область действия и условия эксплуатации. Название алгоритма TLS или AES не является сертификатом. Российское расположение серверов не является аттестацией. Наличие DLP не присваивает системе определённый уровень защищённости.

В анкете ИБ указываются только реквизиты реально предоставленных документов. При отсутствии подтверждения соответствующее утверждение не заменяется общим обещанием. Техническая возможность интеграции с корпоративным средством также требует проверки выбранной версии и конфигурации; см. сетевую защиту.

Нормативная база и область применения

Дата нормативной справки: 8 сентября 2026 года. Для приказа № 21 ссылка ведёт на редакцию от 14.05.2020; для № 117, № 140, № 179 и № 1154 — на официальные публикации актов. Разбор № 117 и № 1154 охватывает перечисленные вводные положения, а не полный набор требований. При проектировании применяются действующие редакции с последующими изменениями и требования, относящиеся к отрасли и статусу системы.

Состояние нормативной базы 152-ФЗ и изменение статьи 12 законом № 265-ФЗ от 26.07.2026 описаны в юридическом разделе. Для конкретной системы нужны оценка применимости норм и согласованный состав мер.