Nevel

БЕЗОПАСНОСТЬ

Шифрование и управление ключами

TLS, защита хранилищ и резервных копий, секреты подключений, ротация и границы доступа к открытому тексту.

Облако / В контуре

https://docs.nevel.sh/security/encryption/

Шифрование в Nevel защищает данные при передаче и хранении. Оно применяется вместе с разграничением доступа, контролем маршрута и ограничением сроков. Для оценки защиты нужно различать три объекта: ключи шифрования данных, ключи доступа к API и соответствия масок. Они решают разные задачи и не заменяют друг друга.

API-ключ даёт право выполнить запрос. Ключ шифрования позволяет расшифровать защищённое представление. Таблица соответствий связывает заменитель с исходным значением; сама по себе такая замена не является криптографическим шифрованием. Утечка любого из этих объектов имеет собственные последствия и требует отдельного отзыва или удаления.

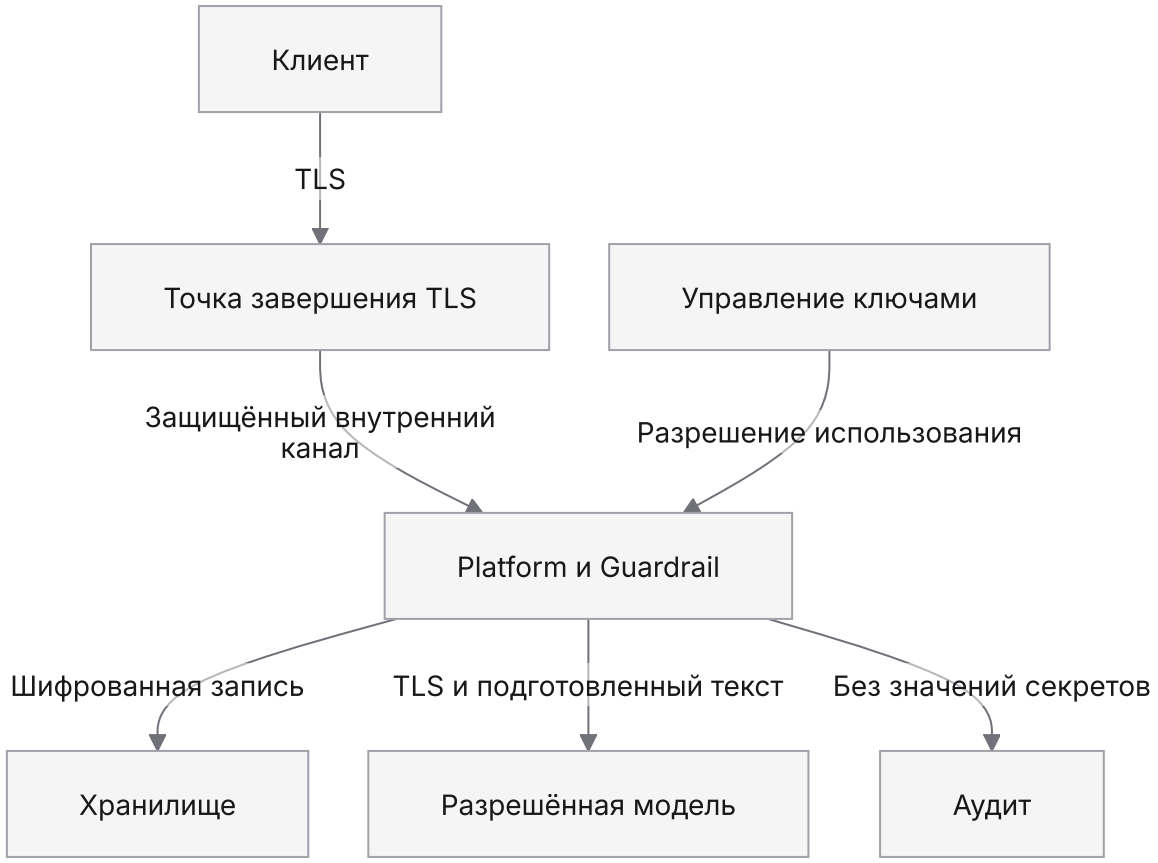
Защита каналов

Базовое требование транспортной защиты — TLS 1.2 или выше. Оно относится к пользовательскому входу, API, соединениям между компонентами, хранилищам и разрешённым внешним получателям. При проверке оцениваются не только версия протокола, но и доверие к сертификату, соответствие имени узла, срок действия и отсутствие автоматического понижения до незащищённого канала.

TLS завершается на конкретном компоненте: балансировщике, reverse proxy, Gateway или средстве защиты. В этой точке запрос становится доступен в открытом виде для разрешённой обработки. Если после завершения TLS есть следующий сетевой участок, он проверяется отдельно. Зелёный значок в браузере подтверждает только участок до выбранной точки завершения, а не всю цепочку до модели.

СХЕМА 1

Где данные расшифровываются



В on-prem внутренние сервисы используют доверенные сертификаты инфраструктуры заказчика, а соединения с разрешёнными модельными провайдерами отдельно проверяют сертификат и имя внешнего endpoint. Подмена доверия ради удобства — например, отключение проверки сертификата у модельного клиента — создаёт обход транспортной защиты. При подключении собственного AI firewall его точка расшифрования включается в схему доступа к открытому тексту; см. сетевую архитектуру.

Защита хранилищ

Шифрованное хранение охватывает служебные данные и секреты в пределах выбранной поставки. Для резервных копий в базовом профиле Guardrail версии 1.2 указан AES-256. Это точное указание относится к профилю резервирования; его нельзя автоматически переносить на алгоритм каждой базы, файла или поля приложения без паспорта установленной конфигурации.

У шифрования несколько уровней. Шифрование диска защищает носитель вне работающей системы. Шифрование объекта защищает сохранённое представление в файловом хранилище. Шифрование отдельных секретов отделяет их от обычных записей приложения. Эти уровни могут сочетаться, но доступ приложения к рабочему ключу позволяет ему обрабатывать данные в открытом виде.

Данные	Что проверяется	Какой риск остаётся
История и файлы	Шифрование тома или хранилища, сервисные права, защита экспорта	Авторизованный процесс приложения может читать разрешённое содержимое
Соответствия масок	Отдельная область, шифрованное хранение, ограниченный доступ	Компрометация процесса восстановления может раскрыть доступные ему значения
Токены интеграций	Шифрованное хранение и выдача только нужному исполнителю	Избыточные права самого токена позволяют действие во внешней системе

Данные	Что проверяется	Какой риск остаётся
Резервные копии	Защита копии, отдельное хранение ключа, проверка восстановления	Доступ к копии вместе с рабочим ключом позволяет восстановить сведения
Журналы	Минимизация содержания, доступ и защита экспорта	Даже без тел запросов метаданные могут раскрывать активность людей
Временные файлы	Изоляция рабочего каталога и очистка	Аварийный процесс или дамп памяти может сохранить фрагмент данных

Шифрование не исправляет открытый бакет, чрезмерные полномочия или публикацию расшифрованного экспорта. Поэтому проверка зашифрованного носителя дополняется попыткой неавторизованного чтения через прикладной API.

Реестр ключей и секретов

У каждого секрета фиксируются назначение, владелец, среда, область действия, потребители и порядок отзыва. Разделяются производственная среда, тестирование и разработка. Ключ модели не передаётся в браузер; пользователь обращается к Platform или Gateway под своей идентичностью. Секрет подключения доступен исполнителю только для разрешённой операции.

Объект	Назначение	Действие при компрометации
Сертификат и закрытый ключ TLS	Подлинность узла и защищённый канал	Замена ключевой пары и сертификата, проверка доверия клиентов
Ключ шифрования хранилища	Защита сохранённых данных	Ограничение доступа, ротация или повторное шифрование по механизму хранилища
Секрет подписи сессий	Проверка подлинности пользовательской сессии	Замена и прекращение доверия к затронутым сессиям
Ключ доступа к Nevel API	Доступ приложения к разрешённым моделям и операциям	Немедленный отзыв ключа, новый ключ с минимальными правами
Ключ провайдера модели	Оплата и доступ к модельному обработчику	Отзыв у провайдера, замена в защищённой конфигурации, проверка расходов
OAuth-токен подключения	Действия в подключённой системе	Отзыв подключения и токена у источника, повторная авторизация
Доступ к хранилищу соответствий	Восстановление масок	Отзыв сервисного доступа и оценка раскрытых областей запросов

Отзыв ключа Nevel не отзывает автоматически уже скомпрометированный ключ внешнего провайдера. Удаление подключения из интерфейса также проверяется на стороне источника: отдельный внешний токен может иметь свой срок действия и механизм отзыва.

Ротация без потери управляемости

Ротация начинается с выпуска нового секрета в той же или более узкой области. Разрешённые потребители переводятся на новую версию, выполняется контрольный запрос, затем старый секрет отзывается. Переходный период ограничен и отражён в журнале. Если источник не позволяет безопасное одновременное действие двух ключей, переключение выполняется как управляемая операция с проверкой доступности.

Ключи шифрования требуют отдельного внимания к старым данным и резервным копиям. Простая замена значения переменной окружения не гарантирует доступность ранее зашифрованного содержимого. Механизм хранения должен связывать данные с версией ключа или выполнять предусмотренное повторное шифрование. Проверяется чтение текущих данных и восстановление контрольной копии после ротации.

Удаление последнего ключа может сделать данные невосстановимыми, но такой результат не объявляется универсальным способом исполнения любого запроса на уничтожение. Нужно знать, какие копии использовали этот ключ, существовали ли расшифрованные экспорты и сохранились ли другие версии. Порядок удаления описан в жизненном цикле данных.

Облако и ключи заказчика

В облаке эксплуатационная команда управляет инфраструктурными ключами в пределах поставки. Корпоративный API-ключ, персональный токен подключения и ключ провайдера с оплатой заказчика сохраняют отдельного владельца и область ответственности. Использование собственного ключа модели меняет учёт и полномочия обращения к провайдеру, но не переносит автоматически обработку внутрь компании.

В on-prem источники секретов установленной платформы находятся под управлением заказчика в рамках выбранной конфигурации. Это включает ключи разрешённых внешних моделей: российский провайдер, self-hosted Nevel в РФ или глобальная цепочка API не становятся внутренними сервисами из-за локального хранения их ключа. В изолированном профиле секреты и все рабочие потребители остаются внутри контура. Заказчик контролирует выдачу, ротацию, резервирование и аварийное восстановление своей части системы. Необходимость HSM, сертифицированного СКЗИ или конкретного корпоративного KMS определяется требованиями к установленной системе и интеграцией; совместимость проверяется для выбранных средства, версии и конфигурации.

Диагностика и защита от случайного раскрытия

В журнал попадает идентификатор ключа или его безопасный отпечаток, но не значение. Заголовки авторизации, cookie, строки подключения и исходные соответствия масок исключаются из сообщений об ошибках, трассировок и экспортов поддержки. Скриншоты настроек и диагностические архивы рассматриваются как отдельные передаваемые объекты.

Воспроизводимая проверка использует специальный тестовый секрет и поиск его точного значения в логах, ответах, сохранённых артефактах и диагностических выгрузках. Настоящие производственные ключи для такого теста не нужны. Дамп памяти работающего процесса способен содержать расшифрованные данные, поэтому доступ к дампам и их срок хранения ограничиваются так же, как доступ к самим данным.

Приёмка

Проверьте отказ при недоверенном сертификате, невозможность незашифрованного соединения и отсутствие понижения протокола. Затем отзовите тестовый API-ключ и токен интеграции, убедитесь в прекращении новых операций и сохранении события. После ротации ключа хранения проверьте чтение данных и восстановление копии; после отказа источника секретов защищённый маршрут не должен продолжать работу с неразрешённым запасным секретом.

Для регуляторной оценки важно различать применение современных алгоритмов и применение конкретных средств, прошедших требуемую оценку соответствия. TLS и AES сами по себе не являются сертификатом СКЗИ или заключением о выполнении требований ФСТЭК. Применимость таких требований рассмотрена в мерах защиты РФ.