

МАТЕРИАЛЫ VENDOCERTA

Безопасность и GDPR

Защита данных в VendoCerta распределена по всему продукту: в том, как записывается журнал, кто может увидеть какой документ, как шифруется банковский счёт и чего роль намеренно не может. Эта страница собирает всё в одном месте — включая части, где честный ответ звучит как «пока нет».

5

ролей с разделением полномочий

5

правил, которые нельзя обойти

AES-256

шифрование чувствительных данных

Шесть вопросов, которые задают первыми.

Могут ли данные остаться у нас?

Да. VendoCerta устанавливается на инфраструктуре, которую вы контролируете.

Как защищены чувствительные данные?

AES-256-GCM в состоянии покоя; раскрытие требует повторного ввода пароля и причины, записываемой в журнал.

У кого какой доступ?

Роли с реальным разделением обязанностей. Никто не может изменить свою роль.

Есть ли второй фактор при входе?

Да, обязателен для ролей с доступом к бизнес-данным.

Может ли один человек сменить банковский счёт поставщика?

Нет. Четыре этапа, разделённые роли, минимум два человека.

Можно ли исправить журнал аудита?

Нет. В интерфейсе нет функции правки или удаления, ни в одной роли, даже для владельца.

Запись нельзя изменить или удалить. Даже владельцу.

Каждое записанное действие становится записью: вход, смена статуса поставщика, решение по документу, отправленное приглашение, скачанный файл. В VendoCerta нигде нет функции правки или удаления записи, и она никогда не затирает существующее событие.

До и после, при каждом изменении данных

Каждая запись несёт: кто, что, когда — а при изменении ещё и то, как значения выглядели с обеих сторон.

Отказы тоже записываются

Если кто-то пытается открыть то, на что у него нет прав, эта попытка становится записью. Повторные попытки поэтому видны, а не бесшумны.

Отфильтрованный вид — это ссылка

Фильтры попадают в адрес страницы, поэтому конкретный срез журнала можно передать коллеге — или аудитору — адресом. Именно так работает ссылка на историю отдельного дела.

Собственный срок хранения — и мы об этом говорим

Число дней внизу экрана журнала аудита — не то же поле, что на экране настроек. Хранение журнала аудита — отдельная настройка, которую сейчас нельзя изменить из интерфейса, и правка того поля её не сдвинет.

Единственная операция, которую продукт отказывается делать удобной.

Смена банковского счёта поставщика — это четыре этапа и правило о том, кто может их завершить. Всё остальное в VendoCerta спроектировано так, чтобы убирать трение; это — так, чтобы его сохранить.

Шифруется с момента сохранения

Номер счёта никогда не лежит в базе открытым текстом — AES-256-GCM при хранении, с момента записи.

Раскрытие стоит трёх вещей

Право на чувствительные данные, повторный ввод пароля несмотря на активную сессию и указанная причина, попадающая в журнал. Причина записывается; номер — никогда. С экрана он исчезает через 45 секунд.

Дубли показываются, а не прячутся

Если такой же номер счёта уже числится за другим поставщиком, предупреждение нужно осознанно отклонить, прежде чем согласование вообще станет возможным.

Пять ролей, и удивительная из них — намеренная.

Системный администратор поддерживает инсталляцию — конфигурация, диагностика, резервные копии — и вообще не видит поставщиков, документы, дела и банковские счета. Полная противоположность бизнес-администратору, который ведёт сторону поставщиков и не может восстановить резервную копию.

ВОЗМОЖНОСТЬ	ВЛАДЕЛЕЦ	БИЗНЕС-АДМИНИСТРАТОР	СИСТЕМНЫЙ АДМИНИСТРАТОР	ПРОВЕРЯЮЩИЙ	НАБЛЮДАТЕЛЬ
Видит поставщиков и документы	✓	✓	—	✓	✓
Добавляет и редактирует поставщиков	✓	✓	—	—	—
Проверяет документы и решает по согласованию	✓	✓	—	✓	—
Видит чувствительные документы (платёжные реквизиты)	✓	✓	—	—	—
Управляет пользователями и ролями	✓	✓	✓	—	—
Восстанавливает резервную копию	✓	—	—	—	—

Правила, которые роль не обойдёт

- Никто — включая владельца — не может изменить собственную роль.
- Администратор не может создать или понизить учётную запись с ролью владельца.
- Последнюю учётную запись владельца нельзя понизить или отключить, поэтому компания никогда не остаётся без человека с полными правами.
- Двухфакторная аутентификация обязательна и непропускаема для владельца, бизнес-администратора, системного администратора и проверяющего. Наблюдатель может её включить, но не обязан.

- Неудачный вход никогда не сообщает, что именно было неверным — адрес или пароль, — поэтому экран нельзя использовать, чтобы узнать, существует ли учётная запись.

Что хранится, кто может это достать и как долго.

Чувствительные документы требуют отдельного права

Обычные документы поставщика видит каждый, у кого есть доступ к его карточке. Документы, помеченные как чувствительные — в основном связанные с платежами, — требуют отдельного права сверх этого, что на практике означает только владельца и администратора. Попытка открыть без него заканчивается отказом, а отказ записывается.

У файлов никогда нет постоянного адреса

Скачивание идёт через подписанную ссылку, действующую несколько минут и привязанную к вашей компании. Открытие её из другого контекста ничего не даст. Каждое скачивание чувствительного файла аудируется отдельно.

Хранение: по умолчанию семь лет

Настройка документов и хранения по умолчанию равна 2555 дням, что соответствует типичным требованиям закупочного аудита, и её можно изменить в любой момент. Честно: сегодня она фиксирует вашу политику и будет управлять будущей уборкой — ничего не удаляется автоматически просто потому, что срок прошёл.

Приглашения истекают, а повторная отправка аннулирует

Ссылка-приглашение — одноразовый случайный токен с ограниченным сроком жизни, по умолчанию неделя. Отправка нового приглашения немедленно аннулирует предыдущее, даже если его открывали, — и это сейчас единственный способ отсечь ссылку; отдельной кнопки отзыва нет.

Банковские реквизиты шифруются при хранении

AES-256-GCM с момента сохранения. Указанная причина раскрытия номера попадает в журнал аудита; сам номер — никогда.

Отчёт для поддержки без данных

Вкладка диагностики в системном центре создаёт отчёт для технической поддержки: версии, счётчики и замаскированные строки логов — никогда содержимое документов, банковские реквизиты или персональные данные поставщиков.

Вопросы, которые оценщик присылает первыми.

VendoCerta — это облачный сервис, которому мы доверяем данные?

Нет. Он устанавливается на машину, которую контролируете вы. PostgreSQL, файловое хранилище и предпросмотр почты работают как переносимые бинарники внутри папки проекта — ничего не устанавливается в Windows, права администратора не нужны, Docker опционален. Интернет нужен при первом запуске, чтобы загрузить эти службы, а дальше инсталляция ваша.

Можем ли мы получить техническую документацию помимо этой страницы?

Да. Инсталляция поставляется с моделью безопасности и моделью угроз в виде документов в репозитории — тех же источников, из которых сделана эта страница. Спросите того, кто поддерживает вашу инсталляцию, или нас через форму демо, указав, что это для аудита безопасности.

К чему имеет доступ ИИ-ассистент?

Только к тому, что спрашивающий и так может видеть, и он никогда не выполняет действие без его явного подтверждения — права проверяются заново в момент нажатия, у того, кто нажимает. Он не может согласовать, отклонить или приостановить поставщика, не может изменить роль и не может ничего удалить.

Позволяет ли сброс пароля обойти двухфакторную аутентификацию?

Нет. Для ролей, где второй фактор обязателен, он обязателен на каждом пути к учётной записи, в том числе после сброса.

Куда уходит почта во время пилота?

В локальный почтовый ящик предпросмотра на самой инсталляции, а не реальным получателям, — поэтому пилот не может случайно написать поставщику. Вкладка инсталляции в системном центре показывает, какой почтовый ящик используется на самом деле.