

Mask Gate – обработка персональных данных и границы 152-ФЗ

Mask Gate · trust pack · версия 1.1 · дата 25.10.2026 · проект документа, публикация — после подтверждения владельца

Версия: 1.1 · **Дата:** 25.10.2026 · **Статус:** проект документа, публикация — после подтверждения владельца.
Документ: trust pack, файл 2 из 4. Соседние: «Архитектура безопасности», «Поручение и субпроцессоры», «Качество детекции».

Что это. Описание того, **какие** персональные данные (ПДн) обрабатывает сервис, в каких режимах, какими мерами защищает и что из требований 152-ФЗ реализовано, а что — нет. Документ не является юридическим заключением: он описывает факты и честно называет границы. Каждое утверждение о праве снабжено ссылкой на текст нормы; каждое утверждение о продукте — ссылкой на код или артефакт.

1. Кто и в какой роли

Роль	Кто	Комментарий
Оператор ПДн (SaaS)	ИП Цымбалюк Андрей Вадимович, ИНН 503123539105, запись в реестре операторов № 77-25-184814	определяет цели и состав обработки, отвечает перед субъектами
Обработчик по поручению (B2B)	ИП Цымбалюк А.В. — когда клиент-оператор поручает обработку по договору (шаблон — в документе 3)	действует по поручению клиента, ответственность перед клиентом; перед субъектом отвечает оператор (ч. 5 ст. 6 152-ФЗ)
Оператор (self-hosted)	сам клиент	сервис развёрнут в контуре клиента, вендор данные не получает

Основания обработки (SaaS), в терминах ст. 6 152-ФЗ: **согласие субъекта** (п. 1 ч. 1) — для регистрации и использования сервиса; **исполнение договора** (п. 5 ч. 1) — для оплаты и оказания услуги. Правовые основания и перечень данных зафиксированы в политике конфиденциальности `/privacy` и в уведомлении оператора; конкретная формулировка согласия — в интерфейсе при регистрации.

2. Какие данные обрабатываются

2.1. Данные, которые вводит пользователь

Это содержимое проверяемых текстов и документов: ФИО, паспортные данные, СНИЛС, ИНН, банковские карты, телефоны, email, адреса, даты рождения и иные категории, предусмотренные политикой детекции.
Перечень категорий — производный от политики сервиса: на 25.10.2026 в `config/policy.yaml` **48 категорий** (46 со стратегией `mask`, 2 — `redact`). Актуальный перечень для клиента публикуется на странице `/kakie-dannye-nahodim` и не дублируется здесь, чтобы не расходиться с политикой.

2.2. Технические и учётные данные

Данные	Зачем	Где и сколько
email, пароль (хеш), коды входа (хеш + соль)	регистрация, вход	БД, пока жив аккаунт
платежные метаданные (сумма, статус, идентификатор платежа)	оплата, сверка	БД; реквизиты карт не хранятся
IP-адрес, user-agent, время запроса	безопасность, лимиты, расследование инцидентов	access-логи ≥ 30 суток; счётчики квот
технические события (категории находок, счётчики, origin)	аудит, статистика, отчёт о находках	журнал аудита 180 суток, без содержимого
cookie/аналитика	только после согласия на cookie-баннере	Яндекс.Метрика; Webvisor отключён

2.3. Что сервис НЕ обрабатывает

- **специальные категории (ст. 10 152-ФЗ)** — сведения о здоровье, национальности, политических взглядах, религиозных убеждениях, интимной жизни: облачный сервис их **не принимает**. В облачном профиле включён предохранитель: при находке такой категории запрос отклоняется с сообщением об отказе, содержимое отказа не сохраняется и никуда не передаётся. Технически предохранитель включается переменной `MG_REFUSED_CATEGORIES` (`core/special_categories.py`); в SaaS-конфигурации он включён, но эффективное значение — параметр эксплуатации, а не свойство кода;
- **биометрические ПДн (ст. 11 152-ФЗ)** — детектор их **не выявляет**; маскирование такие данные не защитит. Документы с биометрией загружать нельзя (запрещено офертой);
- **данные банковских карт** — обрабатываются платёжным провайдером (ЮKassa), через сервис не проходят.

3. Режимы обработки

Режим	Что видит клиент	Обратимость	Где настраивается
<code>block</code>	запрос отклоняется, наружу ничего не уходит	—	политика (<code>config/policy.yaml</code>), админка
<code>redact</code>	<code>[REMOVED:КАТЕГОРИЯ]</code> вместо значения	необратимо	политика, личная политика пользователя
<code>mask</code>	<code>[VAULT:...]</code> — токен; значение можно вернуть по ключу	обратимо, пока жив vault (TTL 30 суток)	политика; пользователь включает/выключает в запросе (<code>use_vault</code>)

Личная политика пользователя (сценарии `api/files/ui`) накладывается поверх глобальной. Если обратимое хранение выключено, `mask` деградирует до необратимого `[REMOVED:...]` — и в ответе, и в аудите это отражается отдельным полем (`mask_downgraded`), чтобы «тихого» изменения поведения не было.

3.1. Ключевая честная граница: обратимое маскирование — не «обезличивание» по закону

152-ФЗ определяет **обезличивание** как действия, после которых **без использования дополнительной информации невозможно** определить принадлежность данных субъекту (п. 9 ст. 3 152-ФЗ; текст нормы: ГАРАНТ, ст. 3). У нас при включённом vault «дополнительная информация» есть — ключ и хранилище, и именно ей пользуется клиент, когда возвращает значения. Значит:

- **обратимое маскирование (mask с vault) не является обезличиванием по 152-ФЗ** — это псевдонимизация:

для получателя-третьего лица токен бесполезен, но для оператора субъект восстановим;

- к обезличиванию ближе **необратимое удаление** (`redact` / `mask` без vault): значение удалено

безвозвратно, восстановить его нельзя.

Поэтому в документах и на сайте мы **не пишем** «данные обезличиваются» без уточнения режима. Честная формулировка: «значения маскируются; в режиме без восстановления — удаляются безвозвратно».

4. Сроки хранения и удаление

Что	Срок	Как удаляется
Тексты запросов	не хранятся	обработка в памяти
Загруженные файлы	минуты (на время разбора)	удаление временного файла в коде
Пары «токен–значение» vault	30 суток по умолчанию (<code>MG_VAULT_TTL_DAYS</code>)	фильтрация на чтении + janitor <code>python -m core.purge</code>
Журнал аудита	180 суток по умолчанию (<code>MG_AUDIT_RETENTION_DAYS</code>)	ротация по возрасту; содержимого в нём нет
Журнал списаний <code>usage_ledger</code>	365 суток (<code>USAGE_LEDGER_RETENTION_DAYS</code>)	<code>python -m core.purge</code>
Резервные копии БД	30 суток (<code>BACKUP_RETENTION_DAYS</code>)	удаление старых копий
Access-логи nginx	не менее 30 суток	logrotate
Платёжные записи	по требованиям фискального учёта	не удаляются по запросу об удалении аккаунта

4.1. Удаление аккаунта и данных субъекта

- **Удаление аккаунта:** `DELETE /auth/me` (описано в политике конфиденциальности и доступно в интерфейсе). Запись пользователя удаляется; операция журналируется в аудиторском журнале (без содержимого данных).
- **Каскад:** вместе с аккаунтом удаляются связанные записи (refresh-токены, личные политики, API-ключи); пары vault удаляются по TTL и janitor-процессом.
- **Резервные копии:** из базы данные удаляются сразу, из резервных копий — в течение 30 суток (окно ротации бэкапов). Это ограничение названо в политике конфиденциальности.
- **Остаётся:** аудит (HMAC-метки, без содержимого), платёжные записи (фискальные требования) и обезличенные счётчики. Это не позволяет восстановить содержимое.
- **Права субъекта:** доступ, уточнение, удаление, отзыв согласия — запрос на security@maskgate.ru; порядок и сроки — в политике конфиденциальности `/privacy`.

5. Что реализовано для снижения рисков по 152-ФЗ

Мера	Факт	Проверка
Минимизация	тексты не накапливаются; файлы не сохраняются	<code>api/processing.py</code> , <code>api/files_routes.py</code>
Шифрование при хранении	vault: AES-256-GCM, ключ вне БД	<code>core/vault.py</code>
Шифрование при передаче	TLS 1.2/1.3	<code>nginx/default.conf</code>
Целостность журнала	HMAC-SHA256-цепочка + межфайловые якоря	<code>core/audit.py</code> , <code>python -m core.audit_verify</code>
Разграничение доступа	JWT + роли; API-ключи только хешами	<code>core/jwt.py</code> , <code>api/deps.py</code>
Сроки хранения	TTL vault, ротация аудита/логов/бэкапов	см. раздел 4
Удаление данных	удаление аккаунта, janitor, окно бэкапов	<code>core/purge.py</code> , <code>docs/privacy</code>
Поручение обработки	шаблон договора по ч. 3 ст. 6 152-ФЗ	документ 3 trust pack
Специальные категории	отказ до обработки (облачный профиль)	<code>core/special_categories.py</code>
Уведомление оператора	запись в реестре № 77-25-184814 – данные оператора	публичные страницы; реестр РКН

6. Чего мы не утверждаем и чего нет

- **«Соответствует 152-ФЗ»** – такого утверждения нет и быть не может без юридического заключения.

Документ описывает реализованные меры, а не выдаёт сертификат соответствия.

- **Сертификатов, аудитов, аттестаций нет** (ни ISO 27001, ни SOC 2, ни ФСТЭК) – см. документ 1.
- **Полного шифрования базы нет**: шифруется только vault; остальные поля БД – в открытом виде.
- **Обезличивания по 152-ФЗ при обратимом режиме нет** – см. раздел 3.1.
- **Гарантии 100 % обнаружения нет**: recall на нашем корпусе – 99,81 %, остаточный риск пропуска

есть; на незнакомых форматах он может быть выше (документ 4).

- **Локализация зависит от инфраструктуры**: «серверы в РФ (Санкт-Петербург, Beget)» – утверждение

оператора, код его не подтверждает.

- **Внешняя LLM есть только в двух сценариях, и в обоих наружу уходит только замаскированный текст**:

(1) **чат** – наш серверный ключ `MG_CHAT_LLM_KEY`, провайдер DeepSeek (`api/chat_routes.py`, `core/llm_client.py`); бэкенд реализован, публичный запуск – по решению владельца, передача возможна только при заданном ключе; (2) **ВУОК-шлюз** `/proxy/chat` – ключ приносит клиент, он не сохраняется и не логируется; выбор провайдера и ответственность за трансграничную передачу (ст. 12 152-ФЗ) – на клиенте (оферта, раздел «Ответственность»). **В сценарии проверки документов внешняя LLM не вызывается вообще.**

- **Операционные лимиты и цены** (квоты, число бесплатных операций) в этом документе числами не

фиксируются: они меняются по решению владельца сервиса, актуальные значения – на `/pricing`.

- **Оценка вреда по ч. 1 ст. 18.1** проведена оператором; документ оценки в репозитории **не хранится**

и предоставляется по запросу. Это заявление оператора, а не артефакт, проверяемый в этом репозитории.

7. Процедура инцидента (порядок действий)

Статус: **описанный порядок действий**, а не утверждённый внутренний регламент. Формальный регламент и приказ о назначении ответственных — на стороне оператора; документ не является юридической консультацией. Сроки уведомлений — из закона, см. ниже.

1. **Обнаружение.** Мониторинг доступности, проверка целостности аудита

(`python -m core.audit_verify`), контроль журналов, проверка ротации логов

(`scripts/check_log_retention.py --live`), сообщения на `security@maskgate.ru`.

1. **Сдерживание.** Изоляция затронутого контура, ротация скомпрометированных секретов

(`JWT_SECRET`, `AUDIT_HMAC_KEY`, `VAULT_KEY`, `SMTP_*`, `YOOKASSA_SECRET_KEY`), отзыв сессий и API-ключей, при необходимости — остановка сервиса.

1. **Оценка объёма.** Что затронуто: БД (хеши/шифрованный vault), журнал аудита, резервные копии, access-логи. Важно: **исходных текстов на диске нет**, поэтому «утечка содержимого» ограничена расшифровкой vault при компрометации `VAULT_KEY` (окно — 30 суток).

1. **Сохранение доказательств.** Копия журнала аудита с проверенной цепочкой, копии логов, фиксация времени и действий — до восстановительных работ.

1. **Уведомления (152-ФЗ).**

- о РКН — об инциденте утечки: **24 часа**; о результатах внутреннего расследования — **72 часа**

(ч. 3.1 ст. 21 152-ФЗ; текст нормы: ГАРАНТ, ст. 21). Уведомление направляет оператор.

- Субъекты — если инцидент привёл или может привести к нарушению их прав (по оценке оператора).
- Устранение и проверка.** Исправление причины, повторная проверка целостности, обновление мер.
- Разбор.** Внутренний постмортем: причина, окно, затронутые данные, действия, изменения.

Контакт для сообщений об инцидентах и уязвимостях: `security@maskgate.ru` (указан на `/security`, в оферте и политике конфиденциальности). Публичной программы bug bounty у сервиса нет.

8. Правовые оговорки

- Документ описывает **технические и организационные факты**, а не даёт юридическую квалификацию конкретной ситуации клиента.

- Нормы приведены по текстам 152-ФЗ (ред. от 26.07.2026): ст. 3, ст. 6, ст. 10, ст. 11, ст. 12, ст. 18.1, ст. 21, ст. 22. Ссылки на текст: [ст. 3](#), [ст. 6](#), [ст. 12](#), [ст. 21](#).

- Перед использованием документа во внешней коммуникации рекомендуем юридическую проверку: документ

подготовлен как инженерное описание, а не как заключение юриста.

Документ не является юридическим заключением. Сертификатов, независимого аудита и SLA у сервиса нет — это прямо указано в тексте. Вопросы: `security@maskgate.ru`