Безопасность и защита данных B2B — Daisy Teams

Редакция от 19 октября 2026.

Daisy Teams — сервис ООО «НЕЙРАЛДИПТЕХ» для работы сотрудников компании с нейросетями в общем рабочем пространстве. Данные размещены в России, в облаке Timeweb Cloud (Санкт-Петербург). Обязательства сторон установлены офертой Daisy Teams: gptdaisy.com/policy_b2b.

Подробное описание мер защиты и ответы на опросный лист службы ИБ предоставляются по запросу на gptdaisy@neuraldeep.tech в течение 10 рабочих дней.

Описание отражает меры защиты на дату публикации. Меры могут быть усилены под требования клиента: дополнительные меры, выделенная инфраструктура и индивидуальные условия обсуждаются отдельно по запросу на gptdaisy@neuraldeep.tech.

Размещение и хранение данных

- **Размещение.** Переписка, файлы и базы данных хранятся в облаке Timeweb Cloud в Санкт-Петербурге, в дата-центрах уровня Tier III.
- **Срок хранения.** Данные рабочего пространства хранятся весь срок действия договора.
- **После окончания договора.** Если договор не продлён или прекращён, рабочее пространство 90 дней доступно только для чтения; о неоплате клиент получает предупреждения за 30, 7 и 1 день. В этот период данные выгружаются по запросу. Затем Правообладатель вправе удалить рабочее пространство и его содержимое, в том числе из резервных копий по мере их обновления.
- **Уход сотрудника.** Чаты и файлы сотрудника, исключённого из команды, остаются у компании. Если сотрудник удалил аккаунт и не восстановил его в течение 30 дней, его переписки удаляются, загруженные файлы сохраняются. В отчётах компании остаются сведения о его запросах без их текстов.
- **Журналы.** Журналы работы сервиса хранятся на сервере в ограниченном объёме, при текущей нагрузке — менее суток. Централизованного сбора журналов нет.
- **Финансовые документы** хранятся 5 лет в соответствии с 402-ФЗ.

Защита персональных данных

В режимах «Анонимизация» и «Деанонимизация» перед отправкой запроса в нейросеть персональные данные в тексте заменяются служебными метками, и нейросеть исходных значений не получает. В режиме «Деанонимизация» исходные значения восстанавливаются в ответе на стороне сервиса, в режиме «Анонимизация» не восстанавливаются. В режиме «Без защиты» текст передаётся в нейросеть как есть. Соответствие меток и значений хранится в России вместе с чатом и удаляется вместе с ним.

- **Распознаваемые данные.** 20 типов: ФИО, адрес, телефон, e-mail, ИНН, СНИЛС, полис ОМС, паспорт, водительское удостоверение, военный билет, свидетельство о рождении, номер банковской карты, номер счёта, БИК, почтовый индекс, имя пользователя Telegram, IP-адрес и порт, адрес веб-страницы, дата и время.
- **Область действия.** Тексты сообщений, документов и таблиц, инструкции проекта и сохранённые факты о пользователе.
- **Режимы.** «Без защиты» — данные передаются в нейросеть как есть, ответственность за это несёт клиент как оператор данных своих работников; «Анонимизация» — данные скрываются и в ответе не восстанавливаются; «Деанонимизация» — данные скрываются и восстанавливаются в ответе. По

умолчанию действует «Деанонимизация». Режим задают владелец и администраторы для каждого сотрудника и каждой нейросети, изменения фиксируются в журнале команды.

- **Поведение при сбое.** Если обезличивание включено, но не выполнено, запрос блокируется и в нейросеть не передаётся.
- **Технология.** Собственный сервис на основе открытой разработки PII Guard (github.com/redmadrobot-rnd/pii-guard). Точность на тестовом наборе — 93,3% micro-F1, для имён и фамилий — 96,6%.
- **Ограничения.** Обезличивается только текст: изображения, аудио и сканы без текстового слоя передаются как есть. Специальные категории персональных данных и биометрия не распознаются, их загрузка запрещена офертой. Распознавание не гарантируется при намеренно искажённой записи. Запросы на генерацию изображений, видео и музыки не обезличиваются: их текст передаётся как есть в фильтр контента и в сервисы генерации, в том числе за пределами РФ. Без обезличивания текст также передаётся во внутренние классификатор аналитики и модуль памяти, размещённые в РФ. В памяти пользователя данные хранятся в исходном виде.

Нейросети и обучение

- **Обучение.** Правообладатель не обучает и не дообучает модели на данных клиентов и не передаёт данные третьим лицам для этих целей.
- **Маршрутизация.** Запросы к моделям сторонних поставщиков проходят через шлюз red_mad_router (ООО «РЭДМЭДРОБОТ ЛАБС», РФ). Шлюз хранит только метаданные запросов, без текстов.
- **Условия поставщиков.** OpenAI, Anthropic, Google (платный Gemini API) и xAI не используют данные API для обучения и хранят их от 30 до 55 дней для проверки на злоупотребления. Условия DeepSeek допускают использование данных для обучения, поэтому передавать в DeepSeek конфиденциальную информацию не рекомендуется.
- **Собственные модели.** Модели семейства Qwen размещены на инфраструктуре Правообладателя в РФ, модель gpt-oss-120b — за пределами РФ.
- **Состав моделей** определяется тарифом.

Доступ и роли

- **Роли.** Владелец — все права. Администратор — приглашения, роли, счета, настройки обезличивания. Биллинг — счета и отчёты об использовании. Участник — без административных прав.
- **Что видит компания.** Тексты запросов сотрудников без ответов модели, включая персональные данные: скрываются они только в режиме «Анонимизация», а в режимах «Деанонимизация» (по умолчанию) и «Без защиты» владелец, администраторы и биллинг видят их как есть; названия загруженных файлов, расход токенов, используемые модели и время активности. Данные выгружаются в CSV, каждая выгрузка фиксируется в журнале.
- **Что не видит компания.** Личные чаты сотрудника вне рабочего пространства и его личные покупки.
- **Уведомление сотрудников.** Обязанность работодателя: по оферте сотрудники знакомятся с локальным актом об использовании сервиса под подпись до получения доступа.
- **Доступ персонала Правообладателя.** Только для поддержки по обращению клиента и расследования инцидентов. Раскрытие полного текста запроса и ответа через административный интерфейс фиксируется в журнале доступа. Доступ к базам данных осуществляется под общей учётной записью без журнала запросов.

Изоляция данных

Данные рабочего пространства недоступны другим клиентам и пользователям вне команды. Каждый запрос к базе данных содержит идентификатор пространства. Исключения из этого правила ограничены перечнем и проверяются автоматическим тестом. Исключение — чаты, которыми участник сам поделился по публичной ссылке: такой чат открывается любому, у кого есть ссылка.

Шифрование и резервное копирование

- **При передаче.** HTTPS, TLS 1.2 и выше, HTTP перенаправляется на HTTPS. Трафик проходит через Cloudflare.
- **При хранении.** Шифрование данных при хранении не применяется.
- **Резервные копии.** Ежедневные копии базы данных хранятся 3 дня, ежемесячные — 100 дней. Загруженные файлы в копии не входят. Максимальная потеря данных при сбое — 24 часа. Копии хранятся в двух хранилищах в РФ: в отдельном бакете Timeweb Cloud и в immers.cloud (Москва).
- **Доступность.** Целевая доступность сервиса — 90% времени в месяц.

Аутентификация

Вход по e-mail и паролю, через Яндекс ID или VK ID. Корпоративный вход (SSO) и двухфакторная аутентификация не поддерживаются.

Модерация контента

Запросы на генерацию и редактирование изображений, видео и музыки проверяются фильтром на модели Claude Haiku (Anthropic). Такие запросы не обезличиваются. Проверяется запрос: его текст, а для удаления фона и улучшения качества — описание загруженного изображения. Сгенерированные изображения, видео и музыка фильтр не проходят. Запросы, нарушающие закон, права третьих лиц или Политику допустимого использования, отклоняются. Текстовый чат отдельной модерации не проходит.

Персональные данные и 152-ФЗ

- Клиент — оператор персональных данных своих работников. Правообладатель обрабатывает их по поручению клиента (ч. 3 ст. 6 152-ФЗ).
- Для данных учётных записей, представителей клиента и платёжных данных Правообладатель — самостоятельный оператор.
- Базы данных с персональными данными находятся в РФ (ч. 5 ст. 18 152-ФЗ).

Инциденты и запросы

- **Уничтожение данных.** По требованию клиента персональные данные, обрабатываемые по его поручению, уничтожаются, в том числе в резервных копиях, не позднее 30 дней. Уничтожение подтверждается письменно.
- **Документы для ИБ.** Подробное описание мер защиты и ответы на опросный лист — в течение 10 рабочих дней по запросу. Выездные проверки — по отдельному соглашению.
- **Контакт.** gptdaisy@neuraldeep.tech — для запросов службы ИБ и сообщений об инцидентах.

Перечень обработчиков

Назначение	Поставщик	Страна
Инфраструктура	Timeweb Cloud (ООО «ТАЙМВЭБ.КЛАУД»)	РФ
Резервные копии базы данных	immers.cloud (Москва)	РФ
Сеть и защита трафика	Cloudflare	США
Шлюз к моделям	ООО «РЭДМЭДРОБОТ ЛАБС» (red_mad_router)	РФ
Текстовые модели	OpenAI	США
Текстовые модели	Anthropic	США
Текстовые модели	Google (Gemini API)	США
Текстовые модели	xAI	США
Текстовые модели	DeepSeek	КНР
Модерация запросов на генерацию медиа	Anthropic (Claude Haiku)	США
Генерация видео	Runway AI, Inc.	США
Генерация видео	Google (Vertex AI, Veo)	США
Генерация музыки	Suno через посредника sunoapi.org (MIRA MUSE LLC)	США
Почта	Unisender; Яндекс 360	РФ
Платежи	ООО НКО «ЮMoney» (ЮKassa)	РФ
Вход в аккаунт	Яндекс ID, VK ID	РФ
Аналитика сервиса	Яндекс Метрика, Яндекс AdFox	РФ
Аналитика сайта	VK-пиксель, Tilda	РФ
Шрифты и значки сайтов	Google	США

Обезличивание, собственные модели, распознавание и озвучка голоса, веб-поиск и генерация изображений выполняются собственными сервисами Правообладателя в РФ, кроме модели gpt-oss-120b.

Частые вопросы

Обучаются ли нейросети на наших данных?

Правообладатель не обучает модели на данных клиентов. OpenAI, Anthropic, Google и xAI по условиям API также не используют их для обучения. Условия DeepSeek это допускают.

Где хранятся данные?

В России, в облаке Timeweb Cloud в Санкт-Петербурге. Для ответа поставщикам моделей, в том числе за пределами РФ, передаются тексты запросов. В режимах «Анонимизация» и «Деанонимизация» персональные данные в них заменены метками. Запросы на генерацию изображений, видео и музыки не обезличиваются.

Видят ли сотрудники Правообладателя нашу переписку?

Только при обращении клиента в поддержку или при расследовании инцидента. Раскрытие полного текста запроса и ответа через административный интерфейс фиксируется в журнале доступа.

Шифруются ли данные?

При передаче — да, TLS 1.2 и выше. При хранении — нет.

Есть ли SSO и двухфакторная аутентификация?

Нет.

Что происходит с данными после расторжения договора?

Рабочее пространство 90 дней доступно только для чтения, данные выгружаются по запросу. Затем Правообладатель вправе удалить данные, в том числе из резервных копий по мере их обновления.