

Безопасность данных

Редакция: 2026-10-10. Применяется с момента публикации этой редакции на сайте Operium.

Документ описывает подход к защите Operium и пределы технических заявлений. Дополнительные требования, аудит и SLA согласуются отдельно. Сообщить об инциденте или уязвимости: support@operium.ru. Поставщик Operium и оператор персональных данных для собственных целей платформы: Романов Михаил Мурманович, самозанятый (НПД), ИНН 504314464974.

1. Разделение ответственности

Operium отвечает за меры защиты предоставляемой платформы в пределах своей инфраструктуры и договора. Организация отвечает за состав загружаемых материалов, назначение администраторов, права участников, разрешённые интеграции и требования своей деятельности. Пользователь защищает устройство и средства доступа.

Размещение на сервере не делает любое содержание допустимым для любого класса защиты. Для регулируемых данных и систем со специальными требованиями необходима отдельная оценка до использования. Универсальная пригодность для государственных систем, банковских, медицинских или иных специальных режимов не заявляется.

2. Идентичность и права

Доступ строится вокруг аккаунта Operium ID и членства в организациях, командах и проектах. Разрешение проверяется для запрашиваемой операции и соответствующих материалов. Приглашение, публичная ссылка и интеграция могут расширять круг получателей; их настройка требует внимания администратора.

Пароли хранятся в виде хешей. Сессии и токены имеют условия срока и отзыва; используйте доступные средства завершения чужой сессии и защиты аккаунта. Двухфакторная защита, если доступна и включена, дополняет пароль, но не исключает компрометацию устройства или разрешённой интеграции.

3. Передача и секреты

Публичное взаимодействие с сервисом должно выполняться по HTTPS. TLS защищает канал до соответствующего получателя; это не означает сквозное шифрование любого документа или запрет законного служебного доступа. Наличие HTTPS не подтверждает шифрование каждого файла и резервной копии при хранении.

OAuth-разрешения подключения почты на серверном посреднике хранятся зашифрованными и привязываются к аккаунту и контексту подключения. Краткоживущие попытки авторизации ограничены сроком, проверками возврата и подтверждением клиента. Секреты провайдера не должны включаться в публичную сборку или журнал. Подробности, увеличивающие угрозу инфраструктуре, не публикуются.

4. Инфраструктура и резервирование

Основные арендуемые серверы Operium размещены у FirstVDS в Москве; резервные копии - в РФ. Дата-центр обеспечивает свои инфраструктурные меры, а защита операционной системы, приложения, прав и содержания требует самостоятельных мер Operium. Уровень конкретной площадки не равнозначен сертификации всей платформы.

Собственное резервирование охватывает PostgreSQL Core, базу Messenger/Matrix и серверные файловые хранилища с необходимой конфигурацией. Новые наборы шифруются до передачи в отдельное хранилище FirstVDS в РФ; ключ восстановления хранится отдельно от резервируемого сервера. Это не образ всей виртуальной машины и не подтверждение сквозного шифрования рабочих материалов.

Для новых полных наборов настроена ротация 7 суток; для временных проверочных и незавершённых наборов - 1 сутки при очередном проходе. Старые ручные выгрузки и отдельные архивы провайдера требуют самостоятельной проверки. Проверены получение зашифрованного набора из внешнего хранилища и восстановление обеих баз в изолированной среде. Проверка одного набора не доказывает непрерывное выполнение расписания или восстановление всей платформы.

Резервирование служит восстановлению после сбоя и не заменяет экспорт и исполнение удаления. До открытия восстановленной системы для пользователей ответственный должен повторно применить зарегистрированные удаления и проверить доступ. Универсальная автоматическая защита от возврата удалённых данных не заявляется. Гарантированные RPO, RTO и срок доступности определяются только прямо согласованными условиями; данный документ не устанавливает числовой SLA.

5. Служебный доступ и наблюдение

Доступ к данным предоставляется уполномоченным лицам для конкретной необходимой задачи. Применяются ограничения прав, конфиденциальность и контроль операций в предусмотренном объёме. Запрос поддержки не означает разрешение читать произвольные документы или письма. Для просмотра данных Google действуют дополнительные ограничения Limited Use.

Технические события используются для безопасности и устранения сбоев с ограничением состава и срока. Секреты, пароли, токены и полный пользовательский контент не должны включаться в обычные журналы. Журналы и отчёты об ошибках сами могут содержать персональные сведения и требуют защиты.

6. AI и локальные клиенты

Разрешения файлов, терминала, браузера, почты и MCP определяют возможные действия агента. Изолируйте рабочую папку, ограничивайте права и проверяйте подтверждения значимых операций. Ответ внешнего инструмента может содержать вредоносную инструкцию; вывод модели не считается достоверным средством управления доступом.

Локальная модель уменьшает необходимость передачи запроса провайдеру модели, но не делает сетевой инструмент локальным. Безопасность локального файла зависит также от ОС, дискового шифрования, других приложений, системных резервных копий и разрешений. Облачная синхронизация и подключение AI проверяются отдельно от локального хранения.

7. Инциденты и уязвимости

При сообщении укажите затронутый сервис, время, версию клиента и безопасные шаги воспроизведения. Не отправляйте пароль, приватный ключ или выгрузку чужих данных. При расследовании ограничивается ущерб, сохраняются необходимые доказательства и проверяется состав затронутых сведений. Уведомления выполняются по применимым обязанностям и договору.

При подтверждённом инциденте персональных данных учитываются обязательные сроки уведомления уполномоченного органа; сообщение заказчику не заменяет такого уведомления. Исследование уязвимостей допускается только в согласованных границах. Программа вознаграждений и разрешение на активное тестирование не возникают только из этой страницы.

8. Пределы заявлений

Этот документ не заявляет SOC 2, ISO 27001, сертификацию ФСТЭК, универсальное сквозное шифрование, нулевое хранение у всех AI-провайдеров, абсолютную защищённость или гарантированное мгновенное уничтожение во всех системах. Для специальных требований запросите подтверждённые сведения и отдельные условия до заключения договора.

Изменение архитектуры, значимого получателя или функций защиты оценивается до выпуска и отражается в актуальных документах. Договорные меры защиты должны соответствовать выполняемым процессам. У пользователя сохраняются обязательные права и возможность обращения по персональным данным независимо от ограничения доступа.