

Политика информационной безопасности

Версия 1.0 · Действует с 1 ноября 2026 · Владелец: Александр Сенкевич, katelabs, Белград, Сербия · katelabs.io

1. Цель и область применения

Настоящая политика определяет, как katelabs защищает системы, которые собирают, оценивают, хранят и поставляют её датасет, а также информацию, которую передают ей клиенты. Она охватывает конвейер сбора, базу данных, веб-сайт и API, каналы поставки, а также каждое устройство и каждую учётную запись, используемые для их эксплуатации. katelabs управляется одним инженером; приведённые ниже меры контроля соразмерны этой реальности и сформулированы так, чтобы читатель мог их проверить.

2. Классификация информации

- **Публичная:** исследовательские заметки, открытый фрагмент датасета, веб-сайт.
- **Лицензируемая:** полный датасет, индекс, ответы API. Предоставляется только аутентифицированным лицензиатам.
- **Конфиденциальная:** контактные данные клиентов, договоры, журналы использования, отзывы клиентов, всё, что клиент помечает как конфиденциальное.
- **Секретная:** учётные данные, API-ключи, ключи подписи, строки подключения к базе данных, ключи бирж.

Конфиденциальная и секретная информация никогда не помещается в исследовательские заметки, в журналы, передаваемые за пределы katelabs, или в сторонние ИИ-инструменты.

3. Управление доступом

1. Для каждой учётной записи, используемой для эксплуатации katelabs (облако, база данных, хостинг кода, домен, электронная почта, биржа), включена многофакторная аутентификация.
2. Производственные учётные данные существуют только в хранилище секретов хостинг-платформы и в менеджере паролей; они не хранятся в исходном коде, истории чатов или документах. Перед каждым релизом репозиторий проверяется на наличие закоммиченных секретов.
3. Доступ предоставляется по принципу минимальных привилегий: процесс сбора может записывать заголовки; веб-сайт может только читать; ключи поставки могут читать только те данные, которые охватывает соответствующая лицензия.
4. Каждый лицензиат получает индивидуальный API-ключ или учётные данные для поставки. Ключи отзываются по окончании договора или по запросу в течение одного рабочего дня и могут быть ротированы лицензиатом в любое время.

5. Любой подрядчик или будущий сотрудник получает доступ только к тем системам, которые требуются для его задачи, на основании письменного обязательства о конфиденциальности, и этот доступ отзывается по завершении задачи.

katelabs · Политика информационной безопасности · v1.0

katelabs.io

4. Шифрование

Весь трафик к веб-сайту, API и базе данных шифруется при передаче с помощью TLS. База данных и резервные копии шифруются при хранении управляемым провайдером. Файлы, предоставляемые лицензиатам, передаются по аутентифицированному HTTPS или по каналу, указанному лицензиатом; данные не отправляются по незашифрованной электронной почте.

5. Инфраструктура и управление изменениями

1. Сервисы работают на управляемых облачных платформах с операционными системами, обслуживаемыми провайдером; katelabs не эксплуатирует собственных серверов.
2. Изменения кода проходят через систему контроля версий с доступной для проверки историей. Зависимости зафиксированы по версиям и обновляются по регулярному графику; бюллетени безопасности по зависимостям проверяются не реже одного раза в месяц, а критические исправления применяются в течение семи дней.
3. Для производственной среды и среды разработки используются отдельные базы данных и учётные данные. Производственные данные не копируются на личные устройства, за исключением зашифрованных снимков с контролем доступа, используемых для анализа и удаляемых по его завершении.

6. Журналирование и мониторинг

Сбор, оценка и поставка формируют журналы, в которых фиксируется, что было запущено, когда и с каким результатом. Журналы не содержат учётных данных и конфиденциальных данных клиентов. Доступ к API журналируется по каждому ключу. Сбои сбора обнаруживаются автоматически и доводятся до сведения оператора; пробел в сборе продолжительностью более одного часа влечёт расследование.

7. Резервное копирование и непрерывность

База данных непрерывно резервируется управляемым провайдером с возможностью восстановления point-in-time (на момент времени), а полный экспорт выполняется не реже одного раза в неделю во второе, независимое хранилище. Восстановление тестируется не реже двух раз в год. Поскольку датасет только пополняется (append-only) и каждая запись содержит собственные временные метки, восстановленную базу данных можно сверить с поставленными файлами. Целевое время восстановления сервисов поставки — один рабочий день.

8. Реагирование на инциденты

1. Инцидентом безопасности является любой подтверждённый или предполагаемый несанкционированный доступ к системам, учётным данным или информации клиентов, а также любое повреждение датасета.
2. При обнаружении оператор локализует инцидент (отзывает учётные данные, изолирует сервис), сохраняет журналы и фиксирует хронологию.
3. Затронутые лицензиаты уведомляются в течение 72 часов с момента подтверждения с указанием того, что произошло, какие данные были затронуты и что им следует предпринять. Если законодательство юрисдикции клиента требует более быстрого уведомления, применяется это требование.
4. Письменный разбор инцидента готовится в течение двух недель, а вытекающие из него изменения отслеживаются до полного внедрения.

9. Провайдеры

katelabs полагается на небольшое число провайдеров: облачный хостинг, управляемая база данных, хостинг кода, провайдер языковой модели для оценки и провайдер электронной почты. Каждый из них — крупный провайдер с опубликованными сертификатами безопасности. Провайдеры получают только те данные, которые необходимы для их функции; провайдер языковой модели получает текст заголовков и не получает никакой информации о клиентах. Список провайдеров предоставляется лицензиатам по запросу.

10. Обязанности клиентов и пересмотр

Лицензиаты отвечают за защиту выданных им ключей и за доступ внутри своей организации. Настоящая политика пересматривается не реже одного раза в год, а также после любого инцидента. Вопросы и сообщения о проблемах безопасности:

aler.senkevich3301@gmail.com; получение сообщений подтверждается в течение двух рабочих дней.