[ФИО/наименование Оператора], [статус: самозанятый/ИП/ООО]

Дата актуализации: 07.09.2026 ИНН: [УКАЗАТЬ до публикации]

УСЛОВИЯ ИСПОЛЬЗОВАНИЯ API TAIGA TAVERN

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящие Условия регулируют доступ разработчиков (физических лиц и организаций) к программному интерфейсу (API) Платформы Taiga Tavern для создания сторонних приложений, ботов, интеграций и инструментов.

Использование API означает полное принятие Условий. Для юридических лиц — принятие уполномоченным представителем.

2. ПОЛУЧЕНИЕ ДОСТУПА К API

2.1. Доступ к API предоставляется через Developer Console: https://taigatavern.ru/developer.

2.2. Для получения доступа необходимо:

— Иметь верифицированный Аккаунт Taiga Tavern.

— Зарегистрировать приложение с указанием: наименования, описания, callback URL, типа (public/confidential client).

— Принять настоящие Условия.

2.3. Для коммерческих или высоконагруженных интеграций может потребоваться дополнительное соглашение с Оператором.

3. API-КЛЮЧИ И ТОКЕНЫ

3.1. При регистрации приложения выдаётся пара client_id / client_secret (для confidential clients).

3.2. API-ключи и токены являются конфиденциальными:

— Не публикуйте их в репозиториях (в т.ч. публичных).

— Не передавайте третьим лицам.

— Используйте переменные окружения или секретные хранилища (Vault, Secrets Manager).

3.3. При подозрении на компрометацию — немедленно ротировать ключ через Developer Console.

3.4. Каждое приложение должно использовать отдельный набор ключей. Запрещено использовать один ключ для нескольких несвязанных приложений.

4. АВТОРИЗАЦИЯ

4.1. API поддерживает:

— OAuth 2.0 Authorization Code Flow (для приложений, действующих от имени пользователя).

— OAuth 2.0 Client Credentials (для серверных интеграций).

— API Key (для простых интеграций с ограниченными правами).

4.2. Запрашивайте только те scopes (разрешения), которые реально необходимы приложению.

4.3. Callback URL приложения должен использовать HTTPS (исключение: localhost в dev-среде).

5. ОГРАНИЧЕНИЯ ЗАПРОСОВ (RATE LIMITS)

Тариф	Лимит запросов
Free	100 запросов/минута
Developer	500 запросов/минута
Pro	2 000 запросов/минута
Enterprise	По индивидуальному договору

При превышении лимита: HTTP 429 Too Many Requests + заголовок Retry-After.

Оператор вправе снизить лимиты при выявлении злоупотреблений без предупреждения.

6. РАЗРЕШЁННОЕ ИСПОЛЬЗОВАНИЕ

API разрешено использовать для:

— Синхронизации данных персонажей и игровых материалов между Платформой и сторонними приложениями.

— Создания Discord / Telegram / VK-ботов для уведомлений о сессиях.

— Миграции данных из других VTT-систем (с явного согласия пользователя).

— Аналитики собственных игровых сессий.

— Создания инструментов для Ведущих (генераторы NPC, инструменты планирования и т.п.).

— Академических исследований (при уведомлении Оператора).

7. ЗАПРЕЩЁННОЕ ИСПОЛЬЗОВАНИЕ

Использование API запрещено для:

— Scraping: массовый сбор данных сверх лимитов и без явного согласия пользователей.

— Обход защиты: обход paywall, модерации, rate limits, MFA.

— Reverse engineering: попытки восстановить логику внутренних endpoint по ответам API.

— DDoS / нагрузочные атаки: намеренное создание избыточной нагрузки.

— Credential stuffing: перебор учётных данных.

— Перепродажа доступа: предоставление API-доступа третьим лицам за вознаграждение.

— Автоматическая регистрация аккаунтов: создание аккаунтов без участия реальных пользователей.

— Сбор данных несовершеннолетних: без явного согласия родителей, противоречащий AGE.md.

8. ЛИЦЕНЗИЯ НА ДАННЫЕ

8.1. API предоставляет данные только в объёме, разрешённом пользователем через OAuth scopes.

8.2. Разработчик получает ограниченную, неисключительную, отзывную лицензию на использование данных, полученных через API, исключительно для функционирования своего приложения.

8.3. Запрещено хранить данные пользователей Платформы дольше, чем необходимо для функционирования приложения, или передавать их третьим лицам без согласия.

8.4. При обработке персональных данных через API Разработчик выступает самостоятельным оператором или обработчиком (в зависимости от архитектуры) и несёт ответственность за

соблюдение ФЗ № 152-ФЗ в части своей обработки.

9. ВЕРСИОНИРОВАНИЕ И ИЗМЕНЕНИЯ API

9.1. API имеет версионирование: v1, v2 и т.д. Версия указывается в пути запроса (/api/v1/...).

9.2. Breaking changes (изменения, нарушающие обратную совместимость):

— Уведомление за 90 дней до вступления в силу.

— Поддержка старой версии — минимум 2 мажорных версии (deprecation period).

9.3. Deprecation-период для endpoint: минимум 6 месяцев с момента объявления.

9.4. Не-breaking изменения (добавление полей, новых endpoint) могут вноситься без предупреждения.

10. БЕЗОПАСНОСТЬ

10.1. Разработчик обязан:

— Использовать HTTPS для всех взаимодействий с API.

— Хранить токены и ключи безопасно (переменные окружения, vault).

— Немедленно уведомлять Оператора при выявлении уязвимостей: security@taigatavern.ru.

— Не логировать тела запросов, содержащих персональные данные пользователей.

10.2. Оператор реализует для API:

— Обязательный HTTPS.

— Контроль scopes для OAuth.

— Детектирование аномального использования.

— Автоматическое ограничение при выявлении атак.

11. ОТЗЫВ ДОСТУПА

11.1. Оператор вправе отозвать API-ключ:

— С уведомлением за 7 дней — при систематическом нарушении лимитов или Условий.

— Немедленно — при угрозе безопасности, компрометации ключа, злоупотреблении данными.

11.2. Пользователь вправе отозвать разрешения своего аккаунта приложению через: «Настройки» → «Безопасность» → «Подключённые приложения».

12. ПРИМЕНИМОЕ ПРАВО

Настоящие Условия являются дополнением к Пользовательскому соглашению. Применяется законодательство РФ.