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

Дата актуализации: 07.09.2026 ИНН: [УКАЗАТЬ до публикации]

БЕЗОПАСНОСТЬ НА TAIGA TAVERN

Мы серьёзно относимся к защите вашего аккаунта и данных. На этой странице описано, что мы делаем и что можете сделать вы.

1. КАК МЫ ЗАЩИЩАЕМ ВАШИ ДАННЫЕ

Шифрование передачи данных. Соединения с Платформой должны использовать актуальные версии TLS; фактическая минимальная версия и настройки шифров фиксируются в техническом стандарте и проверяются мониторингом. Данные не передаются в открытом виде.

Хранение паролей. Ваш пароль никогда не хранится в исходном виде. Мы используем современный алгоритм хеширования Argon2id — даже при гипотетической утечке базы данных восстановить ваш пароль по хешу практически невозможно.

Production-инфраструктура Taiga Tavern, используемая для хранения и обработки данных, включая базы данных, объектное хранилище и резервные копии, размещается на серверах в Российской Федерации. При сборе персональных данных граждан РФ первичная запись, систематизация, накопление, хранение, уточнение и извлечение выполняются через базы данных в РФ в соответствии с ч. 5 ст. 18 ФЗ № 152-ФЗ. Передача отдельных данных внешнему подрядчику возможна только в описанном законом порядке и не изменяет место основного хранения данных.

Резервные копии. Ежедневно создаются резервные копии. Они хранятся 30 дней и зашифрованы.

Ограниченный доступ сотрудников. Команда платформы имеет доступ только к тем данным, которые нужны для выполнения конкретных задач. Все действия в административной панели логируются.

2. ВАША УЧЁТНАЯ ЗАПИСЬ

Используйте надёжный пароль. Минимум 12 символов, смешивайте буквы, цифры и символы. Не используйте один пароль на разных сайтах.

Включите двухфакторную аутентификацию (2FA). Это наиболее эффективная защита аккаунта. Рекомендуем приложение-аутентификатор (Google Authenticator, Яндекс.Ключ, Aegis). Включить: «Настройки» → «Безопасность» → «Двухфакторная аутентификация».

Проверяйте активные сессии. В настройках можно посмотреть список активных сессий и завершить те, которые вам незнакомы: «Настройки» → «Безопасность» → «Активные сессии».

Не передавайте данные для входа. Сотрудники Taiga Tavern никогда не просят пароль или коды 2FA в чате, email или по телефону.

3. УВЕДОМЛЕНИЯ БЕЗОПАСНОСТИ

Мы отправляем на ваш email уведомление, если:

— в аккаунт совершён вход с нового устройства или из другой страны;

— изменён пароль;

— изменён адрес электронной почты;

— привязан или отвязан способ входа.

Если вы получили такое уведомление, но не совершали этих действий — немедленно смените пароль и напишите нам на security@taigatavern.ru.

4. ЧТО ДЕЛАТЬ, ЕСЛИ АККАУНТ ВЗЛОМАН

1. Перейдите на страницу «Сброс пароля» и установите новый пароль.

2. Завершите все активные сессии: «Настройки» → «Безопасность» → «Завершить все сессии».

3. Напишите на security@taigatavern.ru — мы поможем разобраться.

5. СООБЩИТЬ ОБ УЯЗВИМОСТИ

Если вы обнаружили уязвимость в безопасности платформы, просим сообщить нам по программе ответственного раскрытия:

Email: security@taigatavern.ru Тема: [Security Report]

Пожалуйста:

— Опишите уязвимость с конкретными шагами для воспроизведения.

— Не публикуйте данные о найденной уязвимости до её устранения.

— Не используйте уязвимость для получения доступа к чужим данным.

Мы рассматриваем отчёты в течение 5 рабочих дней и благодарим исследователей за помощь.

6. ИНЦИДЕНТЫ С ДАННЫМИ

Если произойдёт инцидент, затрагивающий ваши данные, мы:

— уведомим вас по email в разумные сроки;

— сообщим, какие данные могли быть затронуты;

— расскажем, что мы сделали и что вам следует предпринять.

Серьёзные инциденты также сообщаются в Роскомнадзор в установленные законом сроки.

По вопросам безопасности: security@taigatavern.ru