security.ru

Заявление о безопасности и защите данных

Сервис: AINet (https://ainet.bytestrike.dev)

Редакция: 2026-05-13.

Контакт по безопасности: security@bytestrike.dev

---

1. Назначение документа

Этот документ описывает публичные принципы безопасности AINet. Он не является техническим runbook, схемой инфраструктуры или перечнем внутренних механизмов защиты. Детали реализации, которые могут облегчить атаку на Сервис, намеренно не раскрываются.

2. Основные принципы

2.1. **Минимизация данных.** Сервис собирает и хранит только данные, необходимые для аккаунта, API-доступа, биллинга, ограничения злоупотреблений, безопасности и поддержки.

2.2. **Stateless по содержимому.** AINet не сохраняет на своей стороне тексты запросов к моделям и тексты ответов моделей.

2.3. **Разделение секретов.** Пользовательские API-ключи, session tokens, 2FA-данные и ключи upstream-провайдеров обрабатываются как секреты и не хранятся в открытом виде.

2.4. **Ограничение рискованных функций.** Сервис ограничивает функции, которые могут приводить к provider-side хранению файлов, состоянию беседы или обходу stateless-модели.

2.5. **Правовые и risk-ограничения.** Доступ для отдельных категорий пользователей или сценариев использования может ограничиваться на сетевом и прикладном уровнях. Такие ограничения основаны на технических сигналах сети и risk-политике и не являются проверкой гражданства, паспорта или налогового резидентства.

3. Передача и хранение данных

3.1. Передача данных между пользователем, инфраструктурой Сервиса и upstream-провайдерами выполняется через защищённые каналы связи.

3.2. Содержимое запросов передаётся Anthropic или OpenAI для выполнения запроса. У Оператора нет Zero Data Retention-соглашения с этими провайдерами, поэтому их собственные политики хранения остаются применимыми.

3.3. На стороне AINet не сохраняются:

- тексты prompts, сообщений и инструкций;
- тексты ответов моделей;
- raw API-ключи Пользователей;
- plaintext ключи upstream-провайдеров;
- банковские реквизиты.

3.4. Для работы Сервиса могут сохраняться технические и биллинговые метаданные: идентификаторы аккаунта и запросов, выбранный провайдер/модель, статус обработки, счётчики потребления, суммы начислений/списаний, идентификаторы платежей и записи аудита.

4. Аккаунты и доступ

4.1. Доступ к API выполняется по API-ключам. Пользователь отвечает за хранение ключей в защищённой среде и обязан немедленно отозвать ключ при подозрении на компрометацию.

4.2. Сервис применяет технические ограничения потребления и антиабуз-контроли для защиты пользователей, балансов и инфраструктуры.

4.3. Административные действия ограничены привилегированным доступом и журналируются. Журналы аудита не предназначены для хранения пользовательских prompts или outputs.

5. Платежи

5.1. Сервис принимает криптовалютные платежи через подключенных платёжных провайдеров. В AINet сохраняются технические идентификаторы платежей и записи баланса, необходимые для зачисления, списания, возврата и разрешения споров.

5.2. AINet не обрабатывает и не хранит данные банковских карт, банковских счетов или фиатных платёжных реквизитов.

6. Ограничения и честное раскрытие

6.1. Ни одна система не может гарантировать абсолютную безопасность. AINet применяет разумные технические и организационные меры, но риск инцидентов не может быть исключён полностью.

6.2. AINet не контролирует внутреннюю безопасность, доступность и политики хранения Anthropic, OpenAI, Cloudflare, хостинг-провайдера и платёжных провайдеров.

6.3. Пользователь не должен отправлять в prompts чужие персональные данные, пароли, токены, приватные ключи, seed-фразы, коммерческую тайну, NDA-материалы, банковские данные или иные чувствительные сведения без законного основания и понимания рисков передачи upstream-провайдерам.

7. Уязвимости

Если вы обнаружили уязвимость, сообщите на security@bytestrike.dev до публичного раскрытия.

Добросовестное исследование не должно включать:

- доступ к чужим аккаунтам, данным, ключам или сессиям;
- перебор API-ключей или credential stuffing;
- DoS/DDoS, нагрузочное тестирование без разрешения;
- обход биллинга, лимитов или ограничений доступа;
- публикацию exploit details до устранения проблемы.

8. Связанные документы

- Пользовательское соглашение — `/legal/terms.ru.md`
- Политика конфиденциальности — `/legal/privacy.ru.md`
- Политика допустимого использования — `/legal/aup.ru.md`

Редакция от 2026-05-13.