

Geodema Network — Политика безопасности и ответственного раскрытия

Дата вступления в силу: **27.02.2026 (МСК)**

1) Цель

1.1. Мы приветствуем ответственное раскрытие уязвимостей, которые могут повлиять на безопасность сервиса **Geodema Network** (далее — **Сервис**) и данных пользователей.

1.2. Цель политики — дать понятный и безопасный способ сообщить о проблеме без вреда для пользователей и инфраструктуры.

2) Куда отправлять отчёты

2.1. Отчёты о безопасности направляйте на **security@geodema.net** с темой письма: **[SECURITY] Geodema Network**.

2.2. Специальные требования к шифрованию/PGP не устанавливаются. Если вы хотите — можете использовать собственные средства шифрования на своей стороне, но это не является обязательным условием.

3) Что включить в отчёт

3.1. Желательно указать:

- описание уязвимости и предполагаемый вектор атаки;
- шаги воспроизведения;
- затронутые компоненты (бот, сайт, API, панель управления и т.п.);
- потенциальное влияние (что можно сделать злоумышленнику);
- доказательства (логи, скриншоты) — без лишних персональных данных;
- контакт для обратной связи.

4) Правила тестирования (важно)

4.1. Разрешено: аккуратная проверка, направленная на подтверждение проблемы при минимальном воздействии.

4.2. Запрещено:

- DDoS/нагрузочное тестирование без письменного согласования;
- сканирование и массовый перебор;
- эксплуатация уязвимости для доступа к данным пользователей;

- изменение/удаление данных;
- социальная инженерия сотрудников/пользователей;
- публикация деталей до предоставления нам разумного времени на исправление.

4.3. Просим ограничиваться тестированием собственных аккаунтов/данных и не затрагивать третьих лиц.

5) Как мы реагируем

5.1. Мы стараемся:

- подтвердить получение отчёта в разумный срок;
- запросить уточнения при необходимости;
- принять меры по исправлению/смягчению последствий.

5.2. Сроки исправления зависят от критичности и сложности. Мы можем временно ограничить функциональность ради безопасности.

6) Публичное раскрытие

6.1. Просим не публиковать детали уязвимости до её устранения или до согласованной даты раскрытия.

6.2. Если требуется публичный отчёт (например, в исследовательских целях), согласуйте это заранее через **security@geodema.net**.

7) Награды

7.1. На данный момент Сервис обещает вознаграждение (bug bounty), если прямо не заявлено отдельно.

Geodema Network — Security & Responsible Disclosure Policy

Effective date: **27 Feb 2026 (Moscow time)**

Send security reports to **security@geodema.net** with subject **[SECURITY] Geodema Network**. No PGP requirement. Include description, reproduction steps, affected components, impact, and safe evidence. Do not run DDoS/stress tests, mass scanning, or access/modify user data. Please allow reasonable time to fix before public disclosure.