

ПОЛИТИКА ИСПОЛЬЗОВАНИЯ (AUP)

SakuraNet — Правила допустимого использования услуг

Дата последнего обновления: 2 июля 2026 г.

1. Назначение документа

Настоящая Политика использования (Acceptable Use Policy, AUP) определяет правила допустимого использования услуг SakuraNet (далее — «Сервис») и применяется ко всем Заказчикам/Пользователям.

AUP является неотъемлемой частью Договора-оферты SakuraNet. Продолжение использования услуг означает согласие с настоящей AUP.

2. Термины и определения

- **Исполнитель** — Индивидуальный предприниматель Федоров Илья Владимирович (ИП Федоров И.В.), ИНН 246011078628, ОГРНИП 326774600465994, предоставляющий услуги вычислительных мощностей и игрового хостинга.
- **Заказчик** — лицо, оформившее или оплатившее услуги SakuraNet.
- **Услуги** — виртуальные серверы (VPS/VDS), удалённые рабочие столы, игровые серверы и сопутствующие услуги поддержки.
- **Аккаунт** — учётная запись Заказчика в биллинге SakuraNet.
- **AUP / Политика** — настоящий документ.

3. Общие правила использования

Заказчик обязуется использовать Услуги только законным образом и не нарушать права третьих лиц. Заказчик самостоятельно отвечает за безопасность своего Аккаунта (логин, пароль, 2FA, API-ключи) и за действия всех лиц, которым он предоставил доступ к серверу или к Аккаунту.

- Заказчик обязан самостоятельно обеспечивать резервное копирование (backup) своих данных и конфигураций.

4. Запрещённые действия и контент

Заказчику запрещается использовать Услуги для:

4.1. Незаконной деятельности

- Любой деятельности, запрещённой законодательством Российской Федерации.
- Распространения наркотических средств, оружия, поддельных документов, а также иных запрещённых товаров или услуг.
- Организации незаконных азартных игр и мошеннических схем.

4.2. Мошенничества и вредоносной активности

- Фишинга, скама, социальной инженерии, подменных страниц оплаты.
- Размещения или распространения вредоносного ПО (вирусы, трояны, ботнеты, эксплойты).
- Сканирования портов или уязвимостей сторонних ресурсов без письменного разрешения владельца ресурса.

4.3. Сетевых атак, спама и злоупотреблений

- DDoS/DoS-атак, флуд-атак, сетевого «шума», направленного на третьих лиц.
- Массовых рассылок (spam), размещения спам-ботов, «почтовых пушек», а также любых рассылок без согласия получателей.
- Использования сервера как анонимайзера или прокси для сокрытия источника атак или противоправных действий.

4.4. Нарушения интеллектуальной собственности

- Размещения пиратского контента, нелицензионного ПО, взломанных версий программ («кряков»), генераторов ключей и т.п.
- Нарушения авторских прав, товарных знаков и иных прав правообладателей.

4.5. Запрещённого контента

- Детской порнографии и любого контента, связанного с сексуальной эксплуатацией несовершеннолетних.
- Контента, содержащего призывы к терроризму, экстремизму, насилию, разжиганию ненависти.

4.6. Перепродажи и «реселлинга»

- Перепродажи вычислительных мощностей третьим лицам без отдельного письменного согласования с Исполнителем.
- Использования Услуг для оказания услуг «хостинга от имени третьих лиц», если это прямо не согласовано.

4.7. Ограничения на организацию VPN и прокси-серверов

- **Разрешенное использование:** На тарифах виртуальных серверов (VPS) разрешается настройка частных VPN и Проxy-серверов исключительно для личных нужд Заказчика. Максимальное количество одновременно подключенных устройств или пользователей к одному серверу не должно превышать 5 единиц.
- **Запрещенная деятельность:** Категорически запрещено создание публичных, бесплатные или коммерческих VPN-сервисов, прокси-ферм, а также любая форма перепродажи или совместного (shared) предоставления VPN-доступа третьим лицам.
- **Запрет на P2P/Торренты:** На виртуальных серверах (VPS) запрещено использование P2P-протоколов (включая BitTorrent, Torrent-TV, DHT и их аналоги).
- **Критерии нарушений:** Характер использования VPN-трафика определяется Исполнителем на основе анализа сетевой активности. Основаниями для признания использования нецелевым являются: аномально высокий PPS (количество пакетов в секунду), генерация тысяч одновременных сетевых

сессий (conntrack), непрерывная 100% утилизация канала, попадание IP-адреса в международные или локальные блеклисты (Spamhaus, AbuseIPDB, Роскомнадзор и др.), либо поступление Abuse-жалоб.

5. DDoS-защита, L3-L4, L7 и blackhole

- **5.1. Общие положения:** SakuraNet применяет меры сетевой защиты от DDoS-атак на уровнях L3-L4 (сетевой и транспортный уровни), а также встроенную фильтрацию трафика на уровне приложений (L7) для фиксированного перечня сервисов.
- **5.2. Защита от L7:** Исполнитель предоставляет встроенную защиту уровня L7 на свои сервисы и протоколы исключительно для следующих направлений: FiveM, Arma, Minecraft, San Andreas SAMP, CS2, 7 Days to Die, Rust, SQUAD, Garry's Mod, OpenVPN, WireGuard, TeamSpeak, SCP: SL, RDP, SSH. Для любых иных видов приложений и сервисов, не входящих в данный перечень, защита от атак уровня L7 обеспечивается Заказчиком самостоятельно (на уровне приложения/веб-сервера/WAF), если иное не согласовано отдельно.
- **5.3. Blackhole/RTBH (временная недоступность):** При критических сетевых атаках на IP-адрес или ресурс Заказчика Исполнитель имеет техническую возможность применения blackhole/RTBH (маршрутизация в «чёрную дыру», при которой входящий трафик к цели принудительно сбрасывается) для защиты инфраструктуры и других клиентов. Настоящим прямо подчеркивается, что Исполнитель оставляет за собой право и имеет возможность применить blackhole при атаке мощностью выше 200 Гбит/с, однако данное действие является исключительным правом, но не обязанностью Исполнителя (Исполнитель имеет возможность включения меры, но не факт, что будет её использовать). На период действия blackhole доступность ресурса может отсутствовать.
- **5.4. Компенсации:** Недоступность, вызванная DDoS-атаками и/или применением blackhole (RTBH), может не являться основанием для компенсации по SLA, если иное не предусмотрено Договором-офертой или тарифом.

6. Жалобы и abuse-обращения

Обращения по нарушениям и жалобы принимаются через тикет-систему в личном кабинете биллинга или по электронной почте: support@sakuranet.cloud. При поступлении обоснованной жалобы Исполнитель вправе запросить у Заказчика пояснения и/или принять меры, предусмотренные разделом 7.

7. Меры при нарушениях

При нарушении настоящей AUP Исполнитель вправе по своему усмотрению и с учётом характера нарушения:

- Выдать предупреждение и установить срок на устранение нарушения;
- Временно приостановить оказание Услуг;
- Ограничить сетевую доступность ресурса (в т.ч. blackhole/RTBH при DDoS);
- Заблокировать Аккаунт/Услугу без предварительного уведомления и без возврата денежных средств в случаях грубых нарушений (включая размещение вредоносного ПО, сетевые атаки, фишинг, нарушение правил организации VPN/Proxu и т.п.);
- Передать информацию в компетентные органы при наличии законных оснований.

8. Изменение политики

Исполнитель вправе обновлять настоящую AUP, публикуя актуальную редакцию на сайте SakuraNet. Продолжение использования Услуг после публикации изменений означает согласие Заказчика с новой редакцией.

9. Контакты

- **Поддержка:** тикет-система в личном кабинете биллинга
- **Email:** support@sakuranet.cloud
- **Discord:** официальный сервер сообщества
- **Телефон (рабочее время 10:00-22:00 МСК):** +7 (916) 838-71-79
- **Адрес для корреспонденции:** Москва, Черемушки, ул. Гарибальди

Версия: 2.2. Дата актуализации: 2 июля 2026 г.