X2PROXY

Политика допустимого использования

Дата вступления в силу: 1 августа 2026 г.

Настоящий документ является переводом официальной версии на английском языке и предоставлен для удобства пользователей. Соотношение языковых версий определяется в порядке, предусмотренном разделом 22 Пользовательского соглашения; Провайдер вправе определить приоритетную языковую версию в отдельном официальном уведомлении.

Оператор сервиса: бренд x2proxy и лицо (лица), фактически осуществляющее администрирование, поддержку, комплаенс-контроль и предоставление доступа к сервису x2proxy, до возможной регистрации юридического лица и/или публикации иных официальных идентификационных данных («Провайдер»).

Контакты: privacy@x2proxy.com — вопросы конфиденциальности и юридически значимые уведомления; support@x2proxy.com — поддержка, включая вопросы оплаты, возврата средств и злоупотреблений; чат поддержки — https://t.me/x2proxysupport; официальный канал — https://t.me/x2proxynews.

Пользователь: физическое лицо, индивидуальный предприниматель, юридическое лицо или иное лицо, использующее сервис x2proxy («Пользователь»).

Настоящая Политика допустимого использования (AUP) определяет допустимые и запрещённые способы использования сервиса x2proxy, включая использование через интерфейс, API, субаккаунты, внутренние команды и иные интеграции.

Использование Сервиса означает согласие Пользователя соблюдать настоящую Политику совместно с Пользовательским соглашением, Политикой конфиденциальности и Политикой возврата средств.

Провайдер вправе обновлять настоящую Политику. Обновлённая версия вступает в силу с даты, указанной в ней, либо с момента публикации в Сервисе, если иное не предусмотрено императивными нормами права.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цель и статус Политики

1.1.1. Настоящая Политика допустимого использования (AUP) устанавливает обязательные правила и ограничения на использование сервиса x2proxy.

1.1.2. Политика применяется ко всем способам использования Сервиса, включая личный кабинет, API, субаккаунты, внутренние команды, автоматизированные инструменты и иные интеграции.

1.1.3. Настоящая Политика является неотъемлемой частью Пользовательского соглашения и применяется совместно с Политикой конфиденциальности и Политикой возврата средств.

1.2. Принятие Политики

1.2.1. Регистрация аккаунта, пополнение баланса, создание конфигураций прокси, использование API или фактическое использование трафика означает принятие настоящей Политики.

1.2.2. Если Пользователь не согласен с настоящей Политикой, он обязан воздержаться от использования Сервиса.

1.3. Общая модель мер реагирования

1.3.1. При выявлении риска или нарушения Провайдер вправе применить временную приостановку, заморозку, ограничение функций либо отзыв доступа к отдельным доменам, портам, локациям или иным возможностям Сервиса.

1.3.2. Окончательное прекращение доступа регулируется Пользовательским соглашением и может применяться в случаях существенных или повторных нарушений.

1.3.3. В случаях, связанных с безопасностью, злоупотреблениями, жалобами или платёжными/комплаенс-рисками, меры могут применяться без предварительного уведомления.

2. ОБЩИЕ ПРИНЦИПЫ ИСПОЛЬЗОВАНИЯ

2.1. Законность и добросовестность

2.1.1. Пользователь обязан использовать Сервис только в законных целях и с учётом применимого права, правил целевых ресурсов и обязательств перед третьими лицами.

2.1.2. Пользователь самостоятельно оценивает правомерность своего сценария использования, законность доступа к данным и допустимость автоматизации в отношении конкретных ресурсов.

2.1.3. Использование Сервиса не должно причинять финансовый, технический, юридический или репутационный вред Провайдеру, другим пользователям или третьим лицам.

2.2. Динамический характер допустимых сценариев

2.2.1. Перечень допустимых сценариев, указанных в настоящей Политике, является иллюстративным, неисчерпывающим и может дополняться, уточняться или ограничиваться с учётом развития Сервиса, рисков и требований применимого права.

2.2.2. То обстоятельство, что конкретный сценарий использования прямо не указан среди примеров допустимого использования, само по себе не делает его автоматически запрещённым; однако такой сценарий должен соответствовать настоящей Политике, Пользовательскому соглашению и применимому праву.

2.3. Право на оценку риска

2.3.1. Провайдер вправе оценивать характер использования Сервиса, применяемые инструменты, профиль нагрузки, целевые ресурсы и иные значимые обстоятельства в целях противодействия злоупотреблениям, обеспечения безопасности и комплаенса.

2.3.2. Формальное соответствие одному из допустимых сценариев не исключает ограничения доступа, если конкретная реализация сценария использования создаёт риск злоупотребления, блокировки инфраструктуры, нарушения закона или нарушения прав третьих лиц.

3. ЗАПРЕЩЁННОЕ ИСПОЛЬЗОВАНИЕ

3.1. Общий запрет

3.1.1. Пользователю запрещается использовать Сервис для неправомерной, злонамеренной, недобросовестной, вводящей в заблуждение или иным образом недопустимой деятельности.

3.1.2. Запрещается любое использование, направленное на сокрытие неправомерной деятельности, обход императивных ограничений или создание существенного риска для Провайдера или третьих лиц.

3.2. Сетевые атаки и несанкционированный доступ

3.2.1. Запрещаются DDoS-атаки, стресс-тестирование без надлежащей авторизации, подбор паролей методом перебора (brute force), credential stuffing, угадывание паролей, эксплуатация уязвимостей, обход аутентификации, обход антифрод-механизмов и иные формы несанкционированного доступа.

3.3. Вредоносная и обманная деятельность

3.3.1. Запрещаются вредоносное ПО, ботнеты, фишинг, выдача себя за другое лицо (impersonation), социальная инженерия, рекламное мошенничество, накрутка кликов, фиктивные показы, платёжное мошенничество, создание или поддержка мошеннических схем и иные формы обманного поведения.

3.4. Неправомерный сбор данных

3.4.1. Запрещаются сбор персональных данных без надлежащего правового основания, скрапинг непубличных данных, обход авторизации, сбор учётных данных (harvesting), массовый сбор адресов электронной почты и номеров телефонов, а также сбор специальных категорий или иных чувствительных данных без законных полномочий.

3.5. Спам и нежелательные коммуникации

3.5.1. Запрещается использование Сервиса для массовых рассылок, спама, несанкционированных сообщений, спама в комментариях, спама в личных сообщениях и иных несанкционированных коммуникаций.

3.6. Обход ограничений и злоупотребление платформами

3.6.1. Запрещается обход лимитов частоты запросов, лимитов API, платных ограничений (paywalls), лицензий, обязательных географических ограничений, средств защиты от ботов и иных технических или договорных ограничений, если такие действия запрещены применимым правом, правилами целевого сервиса или настоящей Политикой.

3.6.2. Запрещаются создание или использование фиктивных профилей, сетей фиктивных аккаунтов, схем искусственного создания спроса, недобросовестной автоматизации социальных платформ, манипулирования маркетплейсами, скупки билетов (scalping), ботов для скупки товаров (sneaker bots) и аналогичных схем.

3.7. Сферы повышенного риска и чувствительные области

3.7.1. Запрещается использование Сервиса для неправомерного воздействия на государственные ресурсы, образовательные учреждения, финансовые услуги, финтех-платформы и медицинские системы или для злоупотребления ими, а также для операций политического влияния или иных чувствительных областей, если это нарушает закон, права третьих лиц или создаёт неприемлемый риск.

3.8. Санкции и экспортный контроль

3.8.1. Запрещается использование Сервиса для обхода санкций, экспортных ограничений или запретов на предоставление услуг определённым лицам, территориям или категориям деятельности, если такие ограничения применимы.

3.9. Существенно аналогичные нарушения

3.9.1. Также запрещается любая деятельность, по существу аналогичная перечисленным выше действиям и создающая сопоставимый риск злоупотребления, блокировки, юридических претензий или причинения вреда.

4. ДОПУСТИМОЕ ИСПОЛЬЗОВАНИЕ

4.1. Примеры допустимых сценариев

4.1.1. При условии соблюдения настоящей Политики допускаются, в частности: законный сбор общедоступных веб-данных, SEO-мониторинг, маркетинговые исследования, мониторинг цен, QA/тестирование, проверка рекламы, защита бренда, исследовательские и аналитические задачи, разработка программного обеспечения и иные добросовестные сценарии.

4.1.2. Допускается использование Сервиса через API, субаккаунты, автоматизированные инструменты и внутренние рабочие процессы Пользователя при условии, что такое использование остаётся контролируемым, законным и не нарушает настоящую Политику.

4.2. Внутреннее использование и команда

4.2.1. Пользователь вправе использовать Сервис для собственных целей и предоставлять доступ сотрудникам, подрядчикам и членам своей команды при условии, что такой доступ осуществляется от имени Пользователя и под его контролем.

4.2.2. Пользователь несёт ответственность за действия лиц, которым он предоставил доступ к аккаунту, субаккаунтам, API-ключам или иным учётным данным.

4.3. Условия допустимости

4.3.1. Любой формально допустимый сценарий перестаёт считаться допустимым, если он нарушает закон или условия целевых сервисов, нарушает требования о защите данных, создаёт аномальную нагрузку, направлен на обход ограничений либо иным образом подпадает под запрещённые действия.

5. АВТОМАТИЗАЦИЯ И НАГРУЗКА

5.1. Контролируемая автоматизация

5.1.1. Использование скриптов, ботов, автоматизированных клиентов и иных средств автоматизации допускается только при контролируемом профиле нагрузки, соблюдении правил целевых сервисов и отсутствии запрещённых действий.

5.1.2. Пользователь обязан самостоятельно ограничивать частоту запросов, избегать резких всплесков активности и корректировать поведение своей автоматизации с учётом технических и договорных ограничений целевых платформ.

5.2. Ограничение права на безусловную автоматизацию

5.2.1. Наличие в описании Сервиса утверждений о высокой производительности, параллелизме или иных технических возможностях не означает, что Пользователь обладает безусловным правом использовать любой профиль нагрузки в любом объёме и для любой цели.

5.2.2. Провайдер вправе ограничивать параллелизм, частоту запросов, географические комбинации, доступ к доменам, портам и иным параметрам использования, если это необходимо для противодействия злоупотреблениям, защиты инфраструктуры, соблюдения закона или выполнения требований третьих лиц.

5.3. Автоматизация повышенного риска

5.3.1. Провайдер вправе в любое время ограничить или запретить определённый шаблон автоматизации, если он создаёт повышенную нагрузку, увеличивает риск блокировки инфраструктуры, используется для обхода защитных механизмов или иным образом становится несовместимым с настоящей Политикой.

6. ЛОКАЦИИ, ПОРТЫ И ИНЫЕ ТЕХНИЧЕСКИЕ ОГРАНИЧЕНИЯ

6.1. Общие положения

6.1.1. Провайдер вправе динамически вводить ограничения на локации, порты, категории соединений, типы конфигураций прокси, способы доступа и иные технические параметры Сервиса.

6.1.2. Такие ограничения могут вводиться по соображениям безопасности, комплаенса, предотвращения злоупотреблений, технической устойчивости, управления рисками или по иным операционным причинам.

6.2. Динамический характер ограничений

6.2.1. Доступность конкретных стран, регионов, городов, доменов, портов и иных технических параметров не гарантируется и может изменяться в любое время.

6.2.2. Пользователю запрещается обходить такие ограничения путём манипулирования настройками, использования нескольких аккаунтов, сокрытия информации о сценарии использования или иными аналогичными способами.

7. ОГРАНИЧЕННЫЕ РЕСУРСЫ, ПОРТЫ И ПРОВЕРКА СЦЕНАРИЯ ИСПОЛЬЗОВАНИЯ

7.1. Доступ по умолчанию и специальные ограничения

7.1.1. Базовая модель Сервиса предусматривает стандартный набор доступных функций и пунктов назначения. Отдельные домены, ресурсы, категории ресурсов, порты или иные возможности могут быть ограничены по умолчанию.

7.1.2. Наличие аккаунта и оплаченного пакета трафика не влечёт автоматического права доступа ко всем доменам, портам и конфигурациям.

7.2. Запрос на открытие доступа

7.2.1. Если Пользователю необходим доступ к ограниченному ресурсу, домену или порту, он вправе направить Провайдеру соответствующий запрос.

7.2.2. Рассмотрение запроса может включать прохождение KYC через стороннюю службу, описание предполагаемого сценария использования, указание конкретных доменов или портов и предоставление дополнительных пояснений по запросу Провайдера.

7.3. Отказ от прохождения верификации

7.3.1. Отказ пройти KYC или предоставить информацию о сценарии использования сам по себе не делает Пользователя нарушителем настоящей Политики.

7.3.2. Однако в этом случае Провайдер вправе отказать в открытии доступа к соответствующим ограниченным ресурсам, портам или функциям.

7.4. Решение и отзыв доступа

7.4.1. Решение о предоставлении, частичном предоставлении, ограничении или отзыве доступа к ограниченным ресурсам принимается Провайдером по результатам оценки риска и проверки сценария использования.

7.4.2. Предоставленный доступ впоследствии может быть пересмотрен, ограничен или отозван при изменении уровня риска, выявлении нарушений, поступлении жалоб, изменении комплаенс-требований или по иным обоснованным причинам.

8. ПЕРЕПРОДАЖА, ВНЕШНИЕ КЛИЕНТЫ И ВНУТРЕННИЕ СУБАККАУНТЫ

8.1. Общее правило

8.1.1. Пользователю запрещается перепродавать Сервис, предоставлять к нему доступ внешним клиентам, использовать Сервис по модели white-label или иным образом предоставлять его третьим лицам в качестве самостоятельного сервиса без предварительного письменного разрешения Провайдера.

8.1.2. Использование Сервиса в рамках собственной организации Пользователя, включая сотрудников, подрядчиков и внутренние субаккаунты, не считается перепродажей при условии, что такой доступ не превращается в отдельный внешний сервис для третьих лиц.

8.2. Разрешённая перепродажа

8.2.1. Провайдер вправе по своему усмотрению предоставить письменное разрешение на отдельные модели перепродажи или партнёрского использования.

8.2.2. При предоставлении такого разрешения Пользователь обязуется контролировать конечных пользователей, обеспечивать соблюдение настоящей Политики и оперативно реагировать на сообщения о нарушениях.

8.3. Отзыв разрешения

8.3.1. Провайдер вправе отозвать ранее предоставленное разрешение на перепродажу или партнёрское использование при выявлении нарушения условий, повышенного риска, неэтичного использования или несоблюдения согласованных ограничений Пользователем или его клиентами.

9. МОНИТОРИНГ, ЖАЛОБЫ И РАССЛЕДОВАНИЯ

9.1. Мониторинг использования

9.1.1. Провайдер вправе осуществлять мониторинг использования Сервиса в объёме, необходимом для обеспечения безопасности, противодействия злоупотреблениям, комплаенса, стабильности инфраструктуры и защиты законных интересов Провайдера.

9.1.2. Такой мониторинг может основываться на технических журналах, аномалиях биллинга/использования, риск-сигналах, результатах KYC/проверок, обращениях в поддержку, жалобах, платёжных/комплаенс-сигналах и иных значимых источниках.

9.1.3. Настоящая Политика не означает, что Провайдер хранит содержимое пользовательского трафика; мониторинг ограничен техническими и операционными данными в объёме, необходимом для функционирования Сервиса и защиты инфраструктуры.

9.2. Жалобы и внешние сигналы

9.2.1. Провайдер вправе учитывать жалобы и сигналы от пострадавших лиц, целевых сервисов, правообладателей, платёжных, комплаенс-, сетевых поставщиков, поставщиков услуг безопасности и иных значимых поставщиков, а также от компетентных органов.

9.3. Содействие Пользователя

9.3.1. Пользователь обязан добросовестно содействовать расследованию, в том числе предоставляя разумные пояснения о сценарии использования, подтверждая владение аккаунтом, отвечая на запросы по вопросам безопасности и инцидентов, а также предоставляя иную необходимую информацию в разумный срок.

10. МЕРЫ ВОЗДЕЙСТВИЯ И АВТОМАТИЗИРОВАННЫЕ СИГНАЛЫ

10.1. Перечень возможных мер

10.1.1. В ответ на риск или нарушение Провайдер вправе применить предупреждение, временную заморозку аккаунта, ограничение отдельных функций, блокировку определённых локаций, доменов или портов, требование о дополнительной верификации, отзыв ранее открытого доступа или иные соразмерные меры.

10.1.2. Меры, предусмотренные пунктом 10.1.1, могут также применяться по обоснованному требованию поставщика платёжных услуг, банка-эквайера или платёжной системы, а также если использование Сервиса создаёт повышенный риск для поставщиков платёжных услуг Провайдера.

10.2. Автоматизированные сигналы

10.2.1. Провайдер вправе использовать автоматизированные сигналы, риск-скоринг и обнаружение аномалий для первичного выявления нарушений или рисков.

10.2.2. Если характер ситуации или применимое право требует дополнительных гарантий, существенные ограничения подлежат последующей проверке человеком или иной дополнительной оценке.

10.3. Последствия нарушений

10.3.1. Нарушение настоящей Политики может повлечь применение мер без компенсации Пользователю убытков, утраты трафика или иных последствий, возникших в связи с собственным нарушением Пользователя, а также может повлиять на право на возврат средств по Политике возврата средств.

11. ОБНОВЛЕНИЕ ПОЛИТИКИ И ПОРЯДОК ПРИОРИТЕТА ПРАВИЛ

11.1. Обновления

11.1.1. Провайдер вправе обновлять настоящую Политику с учётом развития Сервиса, изменения рисков, требований законодательства, жалоб и иной значимой практики.

11.1.2. Обновлённая версия вступает в силу с даты, указанной в ней, либо с момента публикации в Сервисе, если иное не предусмотрено императивными нормами права.

11.2. Приоритет запретов

11.2.1. При толковании настоящей Политики положения о запрещённых действиях и ограничениях имеют приоритет перед примерами допустимого использования, если из текста прямо не следует иное.

11.3. Императивные нормы права

11.3.1. Ничто в настоящей Политике не ограничивает императивные права Пользователя, которые не могут быть ограничены применимым правом.