Политика допустимого использования

Дата вступления в силу: 28 июля 2026 г.

Настоящая Политика допустимого использования (далее — «Политика») устанавливает правила работы с услугами, предоставляемыми **UPHOST SOLUTIONS LIMITED** (Company number 17188833), далее — «Компания». Политика обязательна для всех клиентов (далее — «Клиент») и направлена на обеспечение законности, безопасности и стабильности инфраструктуры. Политика является неотъемлемой частью Пользовательского соглашения (публичной оферты) Компании. Используя услуги Компании, Клиент подтверждает своё согласие с настоящей Политикой.

1. Общие положения

1.1. Клиент обязан использовать услуги ответственно, не нарушая права и интересы других пользователей, а также не создавая угрозу стабильности и безопасности платформы.

1.2. Клиент обязан соблюдать применимые законы, нормативные акты и международные стандарты, включая законодательство Великобритании (в том числе Computer Misuse Act 1990, Fraud Act 2006, Online Safety Act 2023, Privacy and Electronic Communications Regulations 2003), а также законодательство страны своего местонахождения и страны размещения серверов.

1.3. Клиент самостоятельно отвечает за защиту своих данных, учётных записей и программного обеспечения, включая использование актуальных обновлений и надлежащих мер информационной безопасности.

1.4. Клиент несёт ответственность за весь контент и деятельность, осуществляемые с использованием его услуг, в том числе третьими лицами, получившими доступ к услугам Клиента (включая случаи компрометации).

1.5. В случае выявления инцидентов безопасности или подозрительной активности Клиент обязан незамедлительно уведомить службу поддержки Компании по адресу support@uphost.cloud.

2. Запрещённые действия

2.1. Использование услуг в целях, противоречащих законодательству и условиям обслуживания Компании, а также любые из перечисленных ниже действий.

2.2. Спам и злоупотребление рассылками

2.2.1. Массовая рассылка сообщений (e-mail, SMS, сообщения в мессенджерах и социальных сетях) без предварительного явного согласия получателей, рассылка спама любого вида.

2.2.2. Использование купленных, арендованных или автоматически собранных (harvested) списков контактов.

2.2.3. Рассылка сообщений с поддельными, скрытыми или вводящими в заблуждение заголовками, адресами отправителя и темами.

2.2.4. Размещение и эксплуатация открытых почтовых релеев (open relay), открытых прокси-серверов и сервисов анонимной массовой рассылки.

2.2.5. Реклама ресурсов, размещённых у Компании, посредством спама, рассылаемого с любой инфраструктуры (spamvertising).

2.3. Вредоносное программное обеспечение

2.3.1. Создание, хранение, распространение и запуск вредоносного ПО любого вида: вирусов, троянских программ, червей, программ-вымогателей (ransomware), шпионского ПО, руткитов, кейлоггеров.

2.3.2. Размещение и эксплуатация командных серверов ботнетов (C&C/C2), панелей управления вредоносным ПО и инфраструктуры его распространения; участие в ботнетах, в том числе вследствие непринятия Клиентом мер по устранению компрометации.

2.4. Фишинг и мошенничество

2.4.1. Фишинг — создание, размещение и распространение поддельных веб-страниц, форм и сообщений, имитирующих законные организации, с целью получения учётных данных, платёжной и иной конфиденциальной информации.

2.4.2. Подделка данных (spoofing) доменных имён, адресов электронной почты и иных идентификаторов; фарминг.

2.4.3. Мошенничество любого вида (включая деяния, подпадающие под Fraud Act 2006), кража личности (identity theft), операции с похищенными платёжными данными (carding), финансовые пирамиды.

2.4.4. Регистрация с использованием недостоверной информации.

2.5. Сетевые атаки и несанкционированный доступ

2.5.1. Проведение DDoS-атак любого типа и содействие их проведению, включая размещение инструментов для атак (стрессеры, бутеры).

2.5.2. Сканирование портов и сетей третьих лиц, подбор паролей (brute force), эксплуатация уязвимостей, несанкционированный доступ и попытки доступа к чужим системам и данным в нарушение Computer Misuse Act 1990.

2.5.3. Перехват, подмена и мониторинг чужого сетевого трафика; IP-спуфинг; подделка сетевых пакетов и маршрутной информации.

2.5.4. Тестирование на проникновение допускается исключительно в отношении собственных систем Клиента либо при наличии письменного согласия владельца тестируемой системы.

2.6. Незаконный и запрещённый контент

2.6.1. Размещение или распространение незаконного, нарушающего авторские права, обманчивого или клеветнического контента.

2.6.2. Размещение материалов сексуальной эксплуатации детей (CSAM) и любых материалов сексуального характера с участием несовершеннолетних — влечёт немедленное прекращение услуг и передачу сведений в правоохранительные органы.

2.6.3. Размещение порнографии, в том числе ссылок и рекламы, содержащей порнографические сцены.

2.6.4. Размещение контента, пропагандирующего терроризм и экстремизм, содержащего призывы к насилию, разжигающего ненависть; доксинг и нарушение неприкосновенности частной жизни третьих лиц.

2.6.5. Размещение нелицензионного ПО, пиратских копий произведений и средств обхода технической защиты в нарушение Copyright, Designs and Patents Act 1988.

2.6.6. Незаконная торговля: наркотическими средствами, оружием, похищенными данными, поддельными документами и иными предметами, оборот которых запрещён или ограничен законом; организация незаконных азартных игр.

2.7. Прочие запрещённые действия

2.7.1. Длительное использование выделенных ресурсов (CPU, RAM, I/O) на уровне, создающем угрозу нормальной работе других клиентов.

2.7.2. Майнинг криптовалют без предварительного письменного согласия Компании.

2.7.3. Размещение сетевых сканеров, прокси-чекеров и подобного ПО, а также сервисов (в том числе с платным или приватным доступом), которые могут служить вспомогательными средствами для противоправных действий в сети Интернет.

2.7.4. Использование услуг для создания, предоставления или продажи коммерческих VPN-сервисов, включая платный, публичный или массовый доступ третьих лиц; использование VPN для личных, некоммерческих целей Клиента допускается.

2.7.5. Действия, способные нанести ущерб репутации или инфраструктуре Компании, включая действия, влекущие попадание IP-адресов Компании в чёрные списки (RBL/DNSBL).

2.7.6. Использование услуг лицами и организациями, включёнными в санкционные списки (Великобритания/OFSI, OFAC, ЕС, ООН и др.), а также в интересах таких лиц.

2.7.7. Перепродажа услуг Компании без её письменного согласия; при наличии согласия Клиент отвечает за соблюдение настоящей Политики своими конечными пользователями.

3. Использование ресурсов

3.1. Виртуальные серверы используют общие вычислительные мощности, распределяемые между клиентами. Кратковременные пики нагрузки допускаются, однако постоянная загрузка всех vCPU на уровне 100% не допускается.

3.2. Превышение лимитов: если нагрузка Клиента систематически превышает установленные тарифом нормы, Компания вправе ограничить ресурсы, предложить переход на более высокий тариф или принять иные меры для восстановления стабильной работы.

3.3. Отсутствие реакции: если Клиент игнорирует запросы Компании по снижению нагрузки, Компания может в одностороннем порядке ограничить или заблокировать сервер до устранения нарушений.

3.4. Использование дисковых и сетевых ресурсов должно находиться в разумных пределах. Для приложений с высокой нагрузкой рекомендуется внедрение кэширования и оптимизации.

4. Сетевой трафик

4.1. Чрезмерное использование трафика, негативно влияющее на работу сети и других клиентов, запрещается. С целью обеспечения комфортной работы всех клиентов Компания применяет политику честного использования (Fair Use Policy).

4.2. В случае превышения допустимых норм пропускная способность может быть ограничена (shaping) до уровня 10–100 Мбит/с в зависимости от тарифа до конца расчётного периода.

4.3. Компания оставляет за собой право мониторить сетевую активность (объём, интенсивность и направления трафика, без систематического просмотра содержимого данных Клиента) для обеспечения соблюдения настоящей Политики.

5. Электронная почта и антиспам

5.1. Для защиты от злоупотреблений исходящие SMTP-порты (25, 465) по умолчанию закрыты.

5.2. Открытие портов возможно по запросу в службу поддержки после дополнительной проверки.

5.3. Клиент обязан поддерживать корректные SPF-, DKIM- и DMARC-записи и соблюдать законодательство в области рассылок (наличие согласия получателей, работоспособный механизм отказа от рассылки),

включая Privacy and Electronic Communications Regulations 2003 (PECR).

5.4. Попадание IP-адресов Компании в чёрные списки (RBL/DNSBL) по вине Клиента признаётся существенным нарушением настоящей Политики.

6. Контактные данные

6.1. Клиент обязан указывать достоверные и актуальные контактные данные при регистрации и использовать их для связи.

6.2. Использование временных или одноразовых адресов электронной почты запрещено.

6.3. Обновление контактной информации должно производиться в течение 7 (семи) дней с момента её изменения.

6.4. Сообщения Компании, направленные на указанный Клиентом адрес электронной почты, считаются надлежащим уведомлением Клиента.

7. Безопасность и реагирование на инциденты

7.1. В случае компрометации услуг или их участия в нарушениях Компания вправе приостановить или ограничить их работу с уведомлением Клиента (при возможности).

7.2. Клиент обязан своевременно устранять уязвимости, удалять вредоносное ПО и запрещённый контент, проводить переустановку программного обеспечения и смену учётных данных по запросу Компании.

7.3. Клиент обязан сотрудничать при расследованиях инцидентов и предоставлять необходимые данные в пределах, установленных законом.

7.4. Компания вправе передавать информацию о нарушениях правоохранительным и иным уполномоченным органам в случаях, предусмотренных законом.

8. Применение и санкции

8.1. В зависимости от характера нарушения Компания вправе:

8.1.1. вынести предупреждение с требованием устранить нарушение;

8.1.2. временно ограничить ресурсы или отдельные функции услуги (включая блокировку портов и фильтрацию трафика);

8.1.3. приостановить услуги;

8.1.4. расторгнуть договор обслуживания без возврата уплаченных средств.

8.2. В экстренных случаях (угроза сети, безопасности или третьим лицам — DDoS-атаки, фишинг, вредоносное ПО, CSAM) меры применяются немедленно, без предварительного уведомления.

8.3. Повторные или грубые нарушения ведут к окончательному прекращению обслуживания.

8.4. При приостановке услуги вследствие нарушения данные Клиента хранятся в порядке, предусмотренном Пользовательским соглашением: в течение 2 (двух) календарных дней с момента приостановки, после чего могут быть безвозвратно удалены без возможности восстановления.

8.5. Применение мер по настоящей Политике не освобождает Клиента от обязанности возместить причинённые Компании убытки.

9. Сообщения об абузах

9.1. Жалобы на нарушения настоящей Политики направляются на адрес **abuse@uphost.cloud** с указанием времени инцидента (предпочтительно в UTC), логов и затронутых IP-адресов/доменов.

9.2. Для эффективного рассмотрения жалоба должна содержать:

9.2.1. описание нарушения и его характер;

9.2.2. дату и время инцидента с указанием часового пояса;

9.2.3. затронутые IP-адреса, доменные имена и/или URL;

9.2.4. подтверждающие материалы: журналы (логи), заголовки электронных писем, скриншоты, образцы трафика;

9.2.5. контактные данные заявителя для обратной связи.

9.3. Компания рассматривает все обращения и взаимодействует с клиентами для устранения нарушений в следующем порядке:

9.3.1. каждая жалоба регистрируется; получение подтверждается заявителю, как правило, в течение 1 (одного) рабочего дня;

9.3.2. при подтверждении признаков нарушения Клиенту направляется уведомление с требованием устранить нарушение, как правило, в течение 24 (двадцати четырёх) часов; при критических нарушениях (фишинг, вредоносное ПО, атаки, CSAM) услуга приостанавливается немедленно;

9.3.3. при неустранении нарушения в установленный срок услуга приостанавливается без дополнительного уведомления;

9.3.4. по итогам рассмотрения Компания информирует заявителя о принятых мерах в объёме, допустимом с учётом требований законодательства о защите данных;

9.3.5. жалобы на нарушения авторских прав рассматриваются при указании конкретных материалов, подтверждении прав заявителя и предоставлении заверения о добросовестности требования.

9.4. Умышленные ложные жалобы рассматриваются как злоупотребление и могут привести к приостановке учётной записи заявителя и/или отказу в рассмотрении его последующих обращений.

10. Изменения политики

10.1. Компания оставляет за собой право изменять настоящую Политику в связи с изменениями законодательства, технологий или условий предоставления услуг.

10.2. Обновлённая версия публикуется на официальном сайте. Продолжение использования услуг после вступления изменений в силу означает согласие Клиента с новой редакцией.

10.3. Настоящая Политика регулируется правом Англии и Уэльса.

Информация о компании

UPHOST SOLUTIONS LIMITED

Company number: 17188833

128 City Road, London EC1V 2NX, United Kingdom

E-mail: support@uphost.cloud

Жалобы и злоупотребления (abuse): **abuse@uphost.cloud**

Официальный сайт: https://uphost.cloud

Личный кабинет: https://my.uphost.cloud