SaleVPS.net

ПОЛИТИКА ДОПУСТИМОГО ИСПОЛЬЗОВАНИЯ (AUP)

услуги хостинга и аренды виртуальных серверов SaleVPS.net

Дата публикации: «03» ноября 2026 г. Редакция № 1.

Политика вступает в силу с «03» ноября 2026 г. с момента публикации на Официальном сайте и является неотъемлемой частью Публичной оферты о предоставлении услуг хостинга и аренды виртуальных серверов SaleVPS.net.

1. Общие положения

1.1. Настоящая Политика допустимого использования («AUP») издана Обществом с ограниченной ответственностью «ИТБОТС» (ООО «ИТБОТС», ОГРН 1214700014275, ИНН 4703185659), оказывающим услуги под коммерческим обозначением SaleVPS.net (далее — «Исполнитель»), и определяет запрещённые и ограниченные способы использования Услуг, правила использования ресурсов и сети, меры реагирования и порядок рассмотрения сообщений о нарушениях.

1.2. Исполнитель вправе самостоятельно определять, является ли поведение Клиента нарушением настоящей AUP, на основании результатов собственного мониторинга, поступивших жалоб (abuse-обращений) и иной доступной информации. В зависимости от тяжести нарушения меры, предусмотренные разделом 11, применяются с предварительным уведомлением Клиента либо, при грубых нарушениях (раздел 3), незамедлительно и без предварительного уведомления — с последующим уведомлением Клиента о принятых мерах и причинах их применения в течение 24 (двадцати четырёх) часов.

1.3. Термины, используемые в настоящей AUP с заглавной буквы («Услуги», «Клиент», «Тариф», «Учётная запись», «Тикет-система», «Официальный сайт», «Личный кабинет»), имеют значения, установленные Публичной офертой о предоставлении услуг хостинга и аренды виртуальных серверов SaleVPS.net (далее — «Оферта»).

1.4. Для целей настоящей AUP нарушения подразделяются на грубые нарушения (категория A, раздел 3) и иные нарушения (категория B, раздел 4).

2. Общие принципы

2.1. Клиент обязан использовать Услуги ответственно — так, чтобы не ухудшать производительность, стабильность и безопасность инфраструктуры, используемой для оказания Услуг, и услуг, предоставляемых другим клиентам.

2.2. Клиент обязан соблюдать законодательство Российской Федерации, а также право места размещения сервера и право юрисдикции самого Клиента в части, применимой к Клиенту, размещаемому контенту и осуществляемой через Услуги деятельности.

2.3. Клиент обязан принимать разумные меры защиты собственных серверов и приложений, включая своевременную установку обновлений безопасности, надёжные пароли и контроль доступа, межсетевые экраны и отключение неиспользуемых сервисов.

2.4. Клиент обязан незамедлительно уведомлять Исполнителя через Тикет-систему о ставшей ему известной компрометации своего сервера или Учётной записи, а также об инцидентах безопасности, затрагивающих Услуги.

2.5. Клиент обязан обладать всеми правами, необходимыми для используемых на Услугах данных и программного обеспечения, и несёт единоличную ответственность за всю информацию, программное обеспечение и иные материалы, размещаемые на Услугах или передаваемые через них.

	2.6. Спам, фишинг и любая иная злоупотребительная активность запрещены (разделы 3 и 6). 2.7. Массовые e-mail-рассылки допускаются только с соблюдением раздела 6 настоящей AUP и законодательства о рекламе и связи.
3. Грубые нарушения (категория A)	3.1. Запрещается хранить, публиковать, распространять, передавать или иным образом использовать посредством Услуг материалы, программное обеспечение, данные или иную информацию, которые являются незаконными по применимому законодательству; нарушают авторские, смежные, патентные права, права на товарные знаки, коммерческую тайну либо иные права интеллектуальной собственности; содержат украденные, утёкшие либо незаконно полученные персональные данные, базы данных, учётные записи, токены доступа, API-ключи, пароли, файлы cookie, криптографические ключи либо иную конфиденциальную информацию; содержат материалы, полученные в результате несанкционированного доступа либо утечки информации; содержат вредоносное программное обеспечение, эксплойты, shell-коды, webshell, средства удалённого управления, C2-инфраструктуру, инструменты постэксплуатации либо иные средства, предназначенные преимущественно для совершения несанкционированных действий; предназначены для совершения компьютерных преступлений либо существенно облегчают их совершение; используются для мошенничества, фишинга, социальной инженерии, распространения ложной информации с целью обмана пользователей, реализации схем незаконного получения денежных средств либо иных мошеннических действий; связаны с незаконным оборотом товаров, услуг, контрафактной продукции либо иных объектов, оборот которых ограничен или запрещён законом; пропагандируют терроризм, экстремизм, насилие, разжигание ненависти либо содержат материалы организаций, деятельность которых запрещена законодательством; содержат материалы сексуальной эксплуатации детей, инструкции по изготовлению запрещённых предметов или иные материалы, распространение которых запрещено законодательством; нарушают право на неприкосновенность частной жизни, содержат персональные данные без законных оснований либо используются для преследования, шантажа, угроз или иных противоправных целей. 3.2. Запрещается использовать Услуги для массовой рассылки несогласованных сообщений (спама) по электронной почте, в мессенджерах, социальных сетях, SMS и иных каналах связи; организации, проведения или содействия сетевым атакам любого вида, включая DoS, DDoS, флуд, амплификацию, reflection-атаки, атаки уровня приложений (Layer 7), SYN flood, UDP flood, DNS amplification и иные аналогичные действия; несанкционированного сканирования сетей, портов, сервисов и информационных систем; поиска, эксплуатации либо автоматизированной проверки уязвимостей без согласия владельца соответствующих систем; подбора паролей (brute force), credential stuffing, password spraying, перебора кодов подтверждения и иных способов получения несанкционированного доступа; подмены IP-, ARP-, DNS-, MAC-адресов, BGP-маршрутов и иных сетевых идентификаторов; эксплуатации открытых DNS-, NTP-, SSDP-, Memcached-, прокси- и иных сервисов для усиления атак либо сокрытия их источника; создания, размещения, эксплуатации или управления ботнетами, C2-инфраструктурой, прокси-сетями либо иными средствами удалённого управления вредоносным программным обеспечением; создания, хранения, распространения или использования вирусов, троянов, червей, программ-вымогателей (ransomware), spyware, stealer-программ, rootkit, dropper, loader, backdoor, криптоджекеров, webshell и иных вредоносных программ или компонентов; проведения кардинга, проверки украденных банковских карт, похищенных учётных данных, обхода антифрод-систем либо иной деятельности, связанной с платёжным мошенничеством; организации фишинга, фарминга, социальной инженерии, создания поддельных страниц авторизации, сайтов-клонов, мошеннических интернет-магазинов, инвестиционных схем, финансовых пирамид и иных сервисов, направленных на введение пользователей в заблуждение; обхода технических средств защиты, механизмов лицензирования, DRM, античит-систем, средств аутентификации либо иных систем безопасности; массовой регистрации учётных записей, обхода ограничений сторонних

	сервисов, искусственной накрутки просмотров, подписчиков, лайков, голосований, отзывов, рейтингов и иных показателей; вмешательства в работу инфраструктуры, оборудования, сетей, программного обеспечения либо услуг других клиентов; создания чрезмерной нагрузки на инфраструктуру либо использования ресурсов способом, способным повлиять на стабильность или доступность Услуг для других клиентов; осуществления иной деятельности, нарушающей законодательство, права и законные интересы третьих лиц либо создающей угрозу безопасности информационных систем. 3.3. Запрещается также использовать Услуги для: работы нелицензированных финансовых сервисов (включая обработку платежей, обменные сервисы и сервисы перевода денежных средств) и нелицензированных азартных сервисов; размещения даркнет-площадок и сервисов, предназначенных для анонимного доступа к незаконному контенту; деятельности, направленной на обход санкционных режимов или поддержку лиц, находящихся под применимыми санкциями; доксинга, «сваттинга» и публикации частной информации в целях угроз, преследования или запугивания; а также для создания ложного впечатления об аффилированности с Исполнителем или об одобрении Исполнителем деятельности Клиента. 3.4. Нулевая терпимость: любые материалы сексуальной эксплуатации детей влекут немедленную блокировку доступа и прекращение всех Услуг без предварительного уведомления и без возврата средств (с последующим уведомлением, когда это требуется законодательством). Исполнитель сохраняет относящиеся к нарушению доказательства (журналы доступа, данные Учётной записи и платежей) в защищённом хранилище не менее 90 (девяноста) календарных дней либо в течение более длительного срока по требованию компетентного органа и передаёт сведения в компетентные правоохранительные органы. Клиент не уведомляется, если уведомление может помешать расследованию или запрещено законом. Такие сообщения рассматриваются с наивысшим приоритетом вне обычных сроков раздела 12 и могут подаваться анонимно. 3.5. Организация публичных (открытых) прокси-серверов, публичных VPN-сервисов, выходных узлов TOR и иных публичных сервисов анонимизации без предварительного письменного согласия Исполнителя признаётся грубым нарушением. Использование частного VPN для собственных нужд Клиента разрешено.
4. Иные нарушения (категория B)	4.1. Запрещаются и по общему правилу относятся к нарушениям категории B: хранение и распространение контента, нарушающего авторские и иные права интеллектуальной собственности (включая раздачу торрентов и файлообмен с нарушающими материалами); майнинг криптовалют, валидация («стейкинг» с использованием вычислительных ресурсов) и аналогичная вычислительная деятельность, если она прямо не разрешена описанием Тарифа либо предварительным письменным согласием Исполнителя, которое может быть обусловлено лимитами ресурсов и дополнительной платой; длительная аномальная нагрузка в значении раздела 5; автоматизированный сбор данных (парсинг) с нарушением условий сторонних сервисов; дипфейки и сгенерированный ИИ контент, нарушающий права третьих лиц; сервисы «пассивного дохода» с раздачей пропускной способности и аналогичные; размещение порнографических материалов и ссылок на них; рекламное и кликовое мошенничество, искусственная накрутка просмотров, подписчиков, рейтингов и иных показателей; эксплуатация открытых DNS-резолверов, открытых SMTP-релеев и иных некорректно настроенных сервисов, пригодных для атак усиления; сохранение контента, являющегося предметом обоснованной жалобы о нарушении прав, после истечения срока устранения. 4.2. При нарушении категории B Исполнитель направляет письменное предупреждение через Тикет-систему или по электронной почте с указанием срока устранения — не менее 24 (двадцати четырёх) часов и не более 5 (пяти) рабочих дней, если характер нарушения не требует иного. Если нарушение не устранено в срок, затронутые Услуги могут быть

	ограничены или приостановлены; повторные или неустранённые нарушения могут повлечь прекращение договора в порядке Оферты. 4.3. Исполнитель вправе квалифицировать нарушение категории B как грубое (категория A) с учётом его тяжести, умысла, повторности и последствий. И наоборот, при первом неумышленном нарушении (например, при компрометации сервера Клиента третьими лицами или ошибке конфигурации) Исполнитель может применить более мягкую меру — предупреждение или временное ограничение.
5. Ресурсы, трафик и IP-адреса	5.1. Клиент обязан соблюдать лимиты ресурсов Тарифа. На тарифах с разделяемыми ресурсами запрещена постоянная максимальная утилизация CPU, дисковых операций или сети, ухудшающая работу других клиентов («аномальная нагрузка»). 5.2. Для целей настоящей AUP «длительной аномальной нагрузкой» на тарифах с разделяемыми ресурсами по общему правилу признаётся использование более 90% выделенных ресурсов vCPU более 12 (двенадцати) часов непрерывно либо более 72 (семидесяти двух) часов суммарно в течение любых 7 (семи) дней. Кратковременные пики (как правило, до 4 (четырёх) часов в течение любых 24 часов) допустимы, если они не ухудшают работу услуг других клиентов. 5.3. При влиянии на стабильность инфраструктуры или качество услуг других клиентов Исполнитель вправе временно ограничить ресурсы, запросить оптимизацию нагрузки либо предложить переход на более подходящий Тариф. Клиент обязан разумно содействовать таким запросам. 5.4. Пропускная способность порта, burst-скорость, лимиты трафика и последствия их превышения (включая ограничение пропускной способности и перевод на Тариф с выделенным каналом и оплатой трафика) устанавливаются пунктами 5.11–5.14 Оферты и Тарифами. Такие ограничения, применённые в соответствии с Офертой, не являются Простоем по SLA (пункт 2.4 SLA). 5.5. Запрещается систематическое оформление и отмена Услуг (в том числе с требованиями возврата или перерасчёта) с целью перебора IP-адресов, получения новых IP-адресов либо обхода блокировок, наложенных на IP-адреса. Связанный лимит — не более 2 (двух) перерасчётов по Учётной записи в календарный месяц — установлен пунктом 10.12 Оферты. 5.6. IP-адреса предоставляются исключительно для использования совместно с Услугами и не переходят в собственность Клиента. Действия Клиента, повлекшие включение предоставленных IP-адресов в чёрные списки (спам-базы, государственные реестры, списки блокировок платёжных систем, интернет-платформ и иных организаций), признаются нарушением настоящей AUP. В таком случае Исполнитель вправе взыскать с Клиента фактически понесённые расходы на исключение IP-адресов из соответствующих списков либо заменить затронутые IP-адреса на платной основе. 5.7. В случае прекращения оказания Услуг вследствие нарушения, указанного в пункте 5.6, последствия для возврата денежных средств определяются Офертой и законодательством. Исполнитель вправе удержать из суммы, подлежащей возврату, документально подтверждённые расходы на исключение IP-адресов из списков блокировок, их замену и устранение последствий нарушения; если такие расходы равны сумме, подлежащей возврату, или превышают её, возврат не производится.
6. Электронная почта, антиспам и порты	6.1. На отдельных Тарифах порт 25 (SMTP) может быть закрыт по умолчанию.

	6.2. Клиент может запросить открытие порта 25 через Тикет-систему. Открытие осуществляется по усмотрению Исполнителя, может требовать проверки предполагаемого использования и соблюдения антиспам-требований, может быть обусловлено дополнительной платой и не гарантируется; отказ в открытии порта 25 не является основанием для возврата денежных средств. 6.3. Массовые e-mail-рассылки допускаются только при соблюдении законодательства, включая предварительное согласие получателей, работающий механизм отписки и достоверную идентификацию отправителя, и в пределах технических лимитов Тарифа. Исполнитель вправе запросить доказательства согласия получателей и учитывать уровень жалоб. 6.4. Клиент обязан поддерживать корректные записи SPF, DKIM и DMARC для доменов, используемых для отправки почты через Услуги. 6.5. Исполнитель вправе отслеживать агрегированные показатели рассылок и ограничивать почтовый трафик, когда это необходимо для предотвращения злоупотреблений и защиты репутации сети.
7. Лицензирование программного обеспечения	7.1. Исполнитель не продаёт и не сублицензирует стороннее программное обеспечение, если иное прямо не указано в Тарифе или счёте. Применяется модель «bring your own licence»: Клиент самостоятельно приобретает необходимые ему лицензии. 7.2. Клиент гарантирует наличие действительных лицензий на всё программное обеспечение, установленное или используемое на Услугах. 7.3. Неактивированные образы операционных систем и установочные носители могут предоставляться исключительно для удобства и тестирования; ответственность за их активацию действительными лицензионными ключами несёт Клиент. 7.4. Клиент возмещает документально подтверждённые убытки, требования и расходы Исполнителя (включая расходы на аудит и штрафы), возникшие вследствие нарушения Клиентом условий лицензирования программного обеспечения, в порядке Оферты.
8. Критические системы	8.1. Услуги не предназначены для использования в составе систем, отказ или нарушение функционирования которых может повлечь угрозу жизни, здоровью людей, причинение вреда окружающей среде, значительный материальный ущерб либо иные тяжкие последствия, включая медицинские, авиационные, промышленные и иные критически важные системы. Также Услуги не предназначены для использования в объектах критической информационной инфраструктуры в случаях, предусмотренных Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Клиент подтверждает, что не использует Услуги для указанных целей, и самостоятельно несёт ответственность за последствия такого использования, если оно имело место.
9. Достоверность данных Учётной записи	9.1. Клиент обязан предоставлять точные и полные контактные данные при регистрации и поддерживать их актуальность в соответствии с Офертой. 9.2. Одноразовые и временные адреса электронной почты не могут использоваться в качестве контактного адреса Учётной записи. Ориентированные на конфиденциальность почтовые сервисы с постоянными ящиками одноразовыми не считаются.

	9.3. При обоснованном подозрении, что контактный адрес является одноразовым либо данные Учётной записи недостоверны, Исполнитель уведомляет Клиента и предоставляет не менее 48 (сорока восьми) часов на обновление данных до применения ограничений. 9.4. Изменения контактных данных должны быть отражены в Учётной записи в течение 7 (семи) календарных дней. Все данные Учётной записи должны быть подлинными, принадлежать Клиенту и не выдавать его за другое лицо.
10. Безопасность и реагирование на инциденты	10.1. При компрометации сервера Клиента или его вовлечении в злоупотребительную активность Исполнитель уведомляет Клиента, когда это практически возможно, и вправе применить меры, предусмотренные разделом 11. 10.2. По мотивированному запросу Исполнителя Клиент обязан оперативно устранить уязвимости, удалить вредоносное программное обеспечение, при необходимости переустановить операционную систему и сменить скомпрометированные учётные данные. 10.3. Клиент обязан добросовестно содействовать расследованию инцидентов и abuse-обращений и предоставлять относящиеся к делу журналы и сведения в пределах, допускаемых законодательством. 10.4. Исполнитель исполняет обязательные запросы компетентных государственных, регуляторных и судебных органов.
11. Меры реагирования	11.1. В случае нарушения настоящей AUP Исполнитель вправе с учётом характера, продолжительности, тяжести и последствий нарушения применить одну или несколько мер: направление предупреждения с требованием устранить нарушение в установленный срок (не менее 24 часов и не более 5 рабочих дней, если характер нарушения не требует иного); полное или частичное ограничение либо приостановление предоставления Услуг; блокировку отдельных ресурсов, IP-адресов, портов, сетевых соединений или отдельных видов трафика; прекращение действия договора в порядке, предусмотренном Офертой. При грубых нарушениях (раздел 3) либо при наличии обязательных требований компетентных органов меры могут применяться незамедлительно и без предварительного уведомления — с последующим уведомлением Клиента о принятых мерах и причинах их применения в течение 24 часов. 11.2. Исполнитель ведёт внутренний учёт подтверждённых нарушений по каждой Учётной записи, отражающий их количество и тяжесть. Повторные и систематические нарушения влекут нарастающие меры вплоть до прекращения договора; одно достаточно серьёзное нарушение (в частности, нарушение категории A) может повлечь немедленное прекращение. Отозванные, успешно оспоренные или ошибочно зафиксированные жалобы не учитываются. 11.3. Клиент обязан отвечать на abuse-уведомления в течение 24 (двадцати четырёх) часов с момента направления уведомления через Тикет-систему или по электронной почте. Отсутствие ответа в срок — самостоятельное основание для приостановления. 11.4. Клиент вправе направить мотивированное возражение против применённой меры через Тикет-систему с приложением подтверждающих сведений. Меры, применённые ошибочно, отменяются без необоснованной задержки. 11.5. Приостановление или прекращение Услуг вследствие нарушения настоящей AUP не компенсируется; последствия для возвратов определяются Офертой и законодательством. Системные записи Исполнителя являются основным доказательством факта и времени нарушения.

	11.6. Клиент возмещает документально подтверждённые убытки Исполнителя, причинённые нарушением (включая штрафы реестров и платёжных систем и расходы на обработку abuse-жалоб), в порядке, предусмотренном Офертой.
12. Сообщения о нарушениях	12.1. Сообщения о нарушениях принимаются через Тикет-систему в Личном кабинете (https://my.salevps.net/billing.php?do=tickets) или по адресу электронной почты support@salevps.net. Исполнитель не осуществляет предварительную модерацию контента клиентов и действует на основании поступивших сообщений и собственного мониторинга. 12.2. Сообщение о нарушении должно содержать: достаточно обоснованное объяснение, почему контент или деятельность считаются незаконными либо нарушающими настоящую AUP; точное расположение материала (URL, IP-адрес и иные идентификаторы); имя (наименование) и адрес электронной почты заявителя (для сообщений о материалах сексуальной эксплуатации детей — по желанию); заявление о добросовестности и достоверности изложенных сведений. Подача сообщений бесплатна. 12.3. Исполнитель подтверждает получение сообщения и приступает к его рассмотрению, как правило, в течение 24 (двадцати четырёх) часов (48 (сорока восьми) часов — для случаев, требующих углублённого анализа), рассматривает сообщения добросовестно и объективно, не использует исключительно автоматизированные средства для принятия решений и, если заявитель указал контактные данные, уведомляет его о принятом решении. 12.4. Если по результатам рассмотрения к контенту или Услугам Клиента применены меры, Клиенту предоставляется изложение причин, и он вправе возразить в порядке пункта 11.4, за исключением случаев, когда уведомление запрещено законом либо может помешать расследованию (включая случаи по пункту 3.4). 12.5. Заведомо ложные и недобросовестные жалобы запрещены; Исполнитель вправе отказать в рассмотрении дальнейших сообщений их отправителей. Исполнитель рассматривает все сообщения, но не обязан раскрывать детали и результаты своих расследований.
13. Изменение AUP	13.1. Настоящая AUP может изменяться в порядке, установленном Офертой. Актуальная версия AUP публикуется на Официальном сайте.