

Atlas OS

Встроенное программное обеспечение сетевых устройств ATLAS

ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК И ТЕХНИЧЕСКОЙ АРХИТЕКТУРЫ

Версия программного обеспечения 1.0.0

Редакция документа 1.0 от 24.09.2026

Правообладатель: ООО «СВЯЗЬ» (Российская Федерация).

Класс программного обеспечения по классификатору (приказ Минцифры России от 22.09.2020 № 486): 01.03
«Встроенные прикладные программы».

Документация размещена на сайте правообладателя: <https://atlastel.tech/atlas-os/>

Содержание

1. Общие сведения
2. Состав программного обеспечения
3. Функциональные характеристики
4. Техническая архитектура
5. Поддерживаемые аппаратные платформы
6. Требования к техническим средствам
7. Безопасность и независимость от иностранной инфраструктуры
8. Ограничения

1. Общие сведения

Наименование	Atlas OS (Атлас ОС)
Версия	1.0.0 (сборка 1.0.0+owrt24.10.8)
Правообладатель	ООО «СВЯЗЬ», ОГРН 1257800119422, ИНН 7805827854
Вид программного обеспечения	Встроенное программное обеспечение (микропрограмма), записываемое в энергонезависимую память сетевого устройства
Класс по классификатору № 486	01.03 «Встроенные прикладные программы»
Язык интерфейса	Русский

Назначение. Atlas OS обеспечивает выполнение сетевым устройством — точкой доступа Wi-Fi, маршрутизатором, шлюзом с модемом 4G/LTE — предопределённых задач: организацию беспроводного и проводного доступа к сети передачи данных, защиту беспроводной сети, построение защищённых туннелей, сбор телеметрии и мониторинг радиоэфира, локальное управление устройством через веб-интерфейс на русском языке и централизованное управление устройством из системы управления сетью Atlas Controller.

Область применения. Корпоративные и гостевые сети Wi-Fi организаций, сети филиалов и объектов торговли, сети операторов связи и государственных учреждений; оборудование линейки ATLAS (точки доступа, шлюзы) и совместимые устройства других производителей, для которых собран образ Atlas OS.

Режимы работы. Автономный — устройство настраивается локально через веб-интерфейс или командную строку. Управляемый — устройство регистрируется в Atlas Controller по ключу подключения организации и получает от контроллера конфигурацию, команды и обновления, передавая ему телеметрию и события. Переход между режимами выполняется без перепрошивки.

2. Состав программного обеспечения

Atlas OS состоит из собственных компонентов правообладателя и базовой платформы — свободного программного обеспечения проекта OpenWrt (выпуск 24.10.8), используемого на условиях открытых лицензий. Собственные компоненты не изменяют исходный текст свободных компонентов: они работают как самостоятельные программы в составе образа через штатные программные интерфейсы базовой платформы (шина ubus, хранилище конфигурации uc1, служба rpsd, служба управления сетью netifd, hostapd). Весь образ, включая свободные компоненты, собирается правообладателем из исходных текстов на собственном сборочном сервере на территории Российской Федерации.

Компонент	Назначение	Реализация
Веб-интерфейс Atlas OS	Локальное управление устройством на русском языке (также английский и китайский; тёмное и светлое оформление): обзор, Wi-Fi, клиенты, радиоэфир, безопасность, подключение к контроллеру, туннели, интеграции, система, мастер первичной настройки	HTML, CSS, JavaScript
Агент управления atlas-agent	Протокол ADP: регистрация в Atlas Controller, получение и применение конфигурации, отчёт о результате применения, телеметрия, события, команды, туннели, мониторинг эфира	ucode
Служба atlas-radar	Сбор probe-запросов устройств посетителей для аналитики присутствия (включается политикой контроллера; данные накапливаются только в оперативной памяти и передаются в контроллер по HTTPS)	ucode
Служба atlas-sta-tc	Ограничение скорости для каждого подключённого клиента по событиям hostapd	ucode
Ретранслятор NetFlow	Приём NetFlow v5 от стороннего оборудования площадки и доставка в контроллер по защищённому каналу HTTPS	POSIX sh, socat
Сценарии отчётов	Проводная топология (LLDP/CDP), радиоокружение (соседние сети), анализ трафика (DPI L7/L4)	POSIX sh
Модуль rpcd «atlas»	Загрузка радиоканала, состояние туннелей, создание и удаление локальных туннелей WireGuard (ключ создаётся на устройстве), управление службами из белого списка, сведения о выпуске ПО, смена пароля администратора	POSIX sh
Сценарии первичной настройки	Роль устройства (точка доступа / шлюз), сетевые умолчания для массового развёртывания без выезда (zero-touch), резервный канал LTE, закрытие пустого пароля, сведения о выпуске, серверы времени РФ	POSIX sh (uci-defaults)
Облегчённый агент atlas-agent-lite	Подключение к контроллеру для устройств с малым объёмом памяти (8–16 МБ)	POSIX sh
Сборочный конвейер Atlas OS	Воспроизводимая сборка образов из исходных текстов, подпись пакетов ключом правообладателя, спецификация состава (SBOM), контрольные суммы	bash, OpenWrt buildroot
Базовая платформа (свободное ПО)	Ядро Linux 6.6, драйверы (в том числе драйвер радиомодулей mt76), procd, netifd, ubus, uci, rpcd, uhttpd, hostapd/wpa_supplicant, strongSwan, WireGuard, nftables, opennnds, net-snmp, lldpd и др.	проект OpenWrt, свободные лицензии

Объём исходного текста собственных компонентов — около 4 700 строк (агент управления — около 2 750 строк), не считая сборочного конвейера и описаний аппаратных платформ. Перечень свободных компонентов с версиями и лицензиями приводится в спецификации состава (SBOM в формате CycloneDX), прилагаемой к каждому образу, и в документе «Состав программного обеспечения и свободные компоненты».

3. Функциональные характеристики

3.1. Беспроводной доступ Wi-Fi

- Несколько беспроводных сетей (SSID) на каждом радиомодуле, диапазоны 2,4 и 5 ГГц, стандарты IEEE 802.11b/g/n/ac/ax (в зависимости от радиомодуля устройства).
- Режимы защиты: открытая сеть, WPA2-PSK, WPA3-SAE, смешанный WPA2/WPA3, WPA2/WPA3-Enterprise (IEEE 802.1X, EAP) с внешним сервером RADIUS, учётом (accounting) и динамической авторизацией (CoA/DAE); защита служебных кадров (PMF, IEEE 802.11w).
- Быстрый роуминг IEEE 802.11r, помощь в роуминге IEEE 802.11k/v, перевод клиентов в диапазон 5 ГГц (band steering), кэширование PMK/OKC.
- Скрытые сети, изоляция клиентов, ограничение числа клиентов, фильтрация по MAC-адресам, минимальный уровень сигнала подключения, Hotspot 2.0 / Passpoint (IEEE 802.11u).
- Привязка сетей к VLAN, расписания работы сетей, ограничение скорости на сеть и на каждого клиента.
- Настройка радиомодулей: канал (в том числе автоматический выбор), ширина канала, мощность передатчика, код страны.
- Гостевой доступ через портал авторизации (captive portal) с внешним сервером авторизации, в том числе системы Wi-Fi.Click.

3.2. Сетевые функции

- Режимы сети точки доступа: прозрачный мост с проводной сетью или маршрутизируемый сегмент с NAT и DHCP; проверка пересечения адресных планов.
- VLAN на проводных портах и в мосту (IEEE 802.1Q), отдельный VLAN управления с автоматическим откатом при потере связи с контроллером.
- Резервирование канала: основной проводной WAN и резервный 4G/LTE (встроенный или подключаемый по USB модем) с автоматическим переключением.
- Проводные порты: скорость и дуплекс, аутентификация IEEE 802.1X на порту.
- Списки контроля доступа (ACL) по MAC- и IP-адресам на основе nftables, защита от посторонних DHCP-серверов.
- Приоритизация трафика (QoS, WMM).

3.3. Туннели и защищённые каналы

- Туннели управления и сервисные туннели уровней L2 и L3: WireGuard, VXLAN, GRE-TAP, L2TPv3, IPsec (IKEv2).
- Закрытые ключи туннелей генерируются на устройстве и не покидают его; наружу передаётся только открытый ключ.
- Контроль состояния туннелей, повторное установление, отчёт о доступности удалённой стороны.
- Локальные туннели WireGuard создаются и удаляются в веб-интерфейсе (раздел «Туннели»): закрытый ключ создаётся на устройстве, публичный ключ показывается для настройки удалённой стороны, маршрут по умолчанию через туннель не устанавливается. Туннели, заданные политикой контроллера, веб-интерфейс отображает, но не изменяет.

3.4. Мониторинг, телеметрия и безопасность эфира

- Телеметрия: загрузка процессора и памяти, время работы, состояние радиомодулей и загрузка радиоканала, подключённые клиенты и качество их сигнала, состояние проводных портов,

задержка до контроллера.

- События и пороговые значения (перегрузка, потеря канала, ошибки применения конфигурации), локальные правила реакции (в том числе ограниченная плановая перезагрузка).
- Обнаружение угроз беспроводной сети (WIDS): поиск «двойников» собственной сети (evil twin) и посторонних точек доступа, передача событий в контроллер.
- Сбор probe-запросов устройств посетителей (аналитика присутствия), отчёты о радиоокружении, проводной топологии (LLDP/CDP) и составе трафика (DPI).
- Выдача телеметрии во внешние системы по MQTT (в том числе TLS) и SNMP v2c/v3, журналирование на внешний сервер syslog.

3.5. Централизованное управление (протокол ADP)

- Регистрация устройства в Atlas Controller по ключу подключения организации без ручной настройки (zero-touch); резервные адреса контроллера с автоматическим переключением.
- Получение конфигурации и её атомарное применение с отчётом о результате (применено / применено частично / ошибка) и версией конфигурации.
- Команды контроллера: перезагрузка, индикация (поиск устройства), применение конфигурации, сброс туннелей, сброс к заводским настройкам, открытие и закрытие сервисного доступа, обновление ПО.
- Обновление ПО по сети с проверкой контрольной суммы SHA-256 и совместимости образа до записи; на устройствах с двумя разделами ПО — запись в неактивный раздел.
- Централизованная смена пароля администратора, серверов времени, журналирования, индикации.

3.6. Локальное управление (веб-интерфейс)

- Язык интерфейса — русский (основной), английский или китайский; оформление — тёмное (Eclipse, основное) или светлое (Signature). Переключатели — в шапке и на экране входа, выбор сохраняется в браузере.
- «Обзор» — модель, версия ПО, время работы, память, адрес, график трафика в реальном времени.
- «Wi-Fi» — радиомодули и сети, защита от двойников (PMF/WPA3), быстрый роуминг.
- «Клиенты» — подключённые устройства, сигнал, скорость, принудительное отключение клиента.
- «РЧ и нагрузка» — канал, загрузка канала, шум, число клиентов в реальном времени.
- «Безопасность» — сканирование эфира, поиск двойников собственной сети, соседние сети.
- «Контроллер» — подключение к Atlas Controller и отключение от него, WIDS, туннели, заданные контроллером.
- «Туннели» — все туннели устройства: тип, удалённая сторона, состояние, источник (контроллер или локальный); публичный ключ WireGuard устройства; создание и удаление локального туннеля WireGuard.
- «Интеграции» — MQTT и SNMP-агент.
- «Система» — имя устройства, сведения о ПО, смена пароля администратора, язык и оформление, перезагрузка.
- «Мастер» — первичная настройка в три шага (имя, страна, сеть Wi-Fi с паролем).

3.7. Массовое развёртывание и обслуживание

- Роли устройства (точка доступа / шлюз) определяются по модели платы; точка доступа после установки получает адрес по DHCP и не раздаёт адреса в сеть оператора, шлюз поднимает резервный канал LTE — устройство само выходит на контроллер.
- Пустой пароль администратора при первой загрузке заменяется случайным; далее пароль задаёт политика контроллера или администратор.
- Сохранение и восстановление настроек, сброс к заводским настройкам, аварийный режим восстановления (failsafe).

4. Техническая архитектура

Atlas OS построена по уровням. Каждый уровень взаимодействует с соседним только через документированные интерфейсы, поэтому один и тот же собственный слой (пакет atlas-ui) без изменений работает на всех поддерживаемых аппаратных платформах, а для новой модели устройства добавляется только описание платы (DTS) и профиль образа.

Уровень	Состав и функции
Аппаратный	Процессор (SoC MediaTek, Qualcomm Atheros, x86-64), радиомодули Wi-Fi, коммутатор и порты Ethernet, модем 4G/LTE, энергонезависимая память (NOR/NAND/eMMC/диск)
Ядро и драйверы	Ядро Linux 6.6 с драйверами платы; драйвер радиомодулей mac80211/mt76 (свободный исходный текст); сетевой стек, nftables, туннели
Системные службы базовой платформы	procd — запуск и контроль служб; netifd — сетевые интерфейсы; hostapd/wpa_supplicant — Wi-Fi; ubus — шина межпроцессного взаимодействия; uci — единое хранилище конфигурации (/etc/config); rpcd — удалённый вызов процедур с разграничением доступа; uhttpd — веб-сервер
Собственный слой Atlas OS	Агент atlas-agent (служба procd) — протокол ADP с контроллером; веб-интерфейс (выполняется в браузере, обращается к устройству по JSON-RPC через uhttpd/ubus); модуль rpcd «atlas» и правила доступа (ACL) веб-интерфейса; службы atlas-radar, atlas-sta-tc, ретранслятор NetFlow; сценарии отчётов и первичной настройки
Внешние системы	Atlas Controller (HTTPS, протокол ADP), серверы RADIUS и порталы авторизации, системы мониторинга (SNMP, MQTT, syslog), серверы времени

4.1. Протокол управления ADP

ADP (Atlas Device Protocol) — собственный протокол взаимодействия устройства с контроллером поверх HTTPS (REST, JSON). Устройство всегда выступает клиентом и работает за NAT без открытия входящих портов. Последовательность: регистрация (/adp/v1/register, ключ подключения организации, MAC-адрес и модель) → выдача контроллером идентификатора и токена устройства → периодический опрос конфигурации (/device/{id}/config) и её применение с отчётом (/config-result) → телеметрия (/telemetry), события (/events), команды (/commands, /command-result), состояние туннелей и данные мониторинга эфира. Все запросы после регистрации подписываются токеном устройства (заголовок Authorization: Bearer).

4.2. Хранение данных

Конфигурация хранится в хранилище uci (/etc/config) в разделе энергонезависимой памяти, доступном для записи (overlay); неизменяемая часть ПО — в сжатой файловой системе squashfs. Параметры подключения к контроллеру — в /etc/config/atlas, сведения о выпуске — в /etc/atlas-release. Сведения о клиентах (MAC-адреса, уровень сигнала) устройство в энергонезависимой памяти не хранит: они накапливаются в оперативной памяти и передаются только в контроллер по защищённому каналу HTTPS; сбор аналитики присутствия включается политикой контроллера, адреса, помеченные как случайные (privacy), по умолчанию исключаются.

4.3. Процессы

Процесс (служба)	Назначение
------------------	------------

atlas-agent (procd, приоритет 95)	Цикл опроса контроллера; при отсутствии адреса контроллера — автономный режим (поддерживает только локальные ограничения скорости)
atlas-radar (procd, 96)	Сбор probe-запросов при включённой политике
atlas-netflow-relay (procd)	Ретрансляция NetFlow v5 со стороннего оборудования
atlas-sta-tc	Ограничения скорости на клиента по событиям подключения
cron: отчёты топологии, эфира, DPI	Периодическая отправка отчётов в контроллер (каждые 5–15 минут)
uhttpd + rpcd	Веб-интерфейс и программный интерфейс JSON-RPC устройства

5. Поддерживаемые аппаратные платформы

Платформа	Устройства	Образы выпуска 1.0.0
Эталонная платформа x86-64	Виртуальная машина (QEMU/KVM, VirtualBox, VMware) и компьютеры x86-64; радиомодули эмулируются (mac80211_hwsim) — для ознакомления, проверки и автоматических испытаний	Да (BIOS, UEFI, OVA, QCOW2)
MediaTek Filogic (MT7981, Wi-Fi 6)	Точки доступа ATLAS на платформе MT7981; Comfast CF-E393AX, Cudy AP3000 Outdoor (энергонезависимая память NAND). Устройства MT7981 с флеш-памятью 16 МБ (например, Yuncore AX835) — облегчённый профиль образа	Да (CF-E393AX, AP3000 Outdoor)
Qualcomm Atheros (ath79), MediaTek MT7620/MT7621/MT7628 (ramips)	Ubiquiti UniFi AC-Lite/AC-Pro, Comfast CF-E375AC и CF-E355AC v2, ZBT WE1026-5G, Yuncore AX820, Teltonika RUT240/RUT200/RUT950, Kroks KNdRt41R1, LigoWave NFT-2ac, Horedtech W618AP	По заказу (тот же сборочный конвейер)

Новая модель устройства на поддерживаемой архитектуре добавляется описанием платы (DTS) и профилем образа; собственные компоненты Atlas OS от модели не зависят.

6. Требования к техническим средствам

Параметр	Значение
Процессор	Архитектуры MIPS, ARM, AArch64 или x86-64, поддерживаемые базовой платформой
Оперативная память	Не менее 128 МБ (рекомендуется 256 МБ и более)
Энергонезависимая память	Не менее 32 МБ для полного набора функций; 8–16 МБ — облегчённый вариант с агентом atlas-agent-lite
Виртуальная машина (эталонная платформа)	1 виртуальный процессор, 256 МБ ОЗУ, диск от 128 МБ, один сетевой адаптер (Intel E1000 или virtio)
Рабочее место администратора	Любой современный веб-браузер (Яндекс Браузер, Chromium, Firefox и др.) с поддержкой JavaScript

7. Безопасность и независимость от иностранной инфраструктуры

- Устройство само не обращается к зарубежным серверам: внешние репозитории пакетов отключены, обновления предоставляет правообладатель (через Atlas Controller или сайт правообладателя); принудительного обновления и управления из-за рубежа нет.
- Точное время — от серверов Государственной службы времени (ФГУП «ВНИИФТРИ»).
- Пакеты ПО подписываются ключом правообладателя; образ собирается из исходных текстов на сервере правообладателя в Российской Федерации.
- Доступ к веб-интерфейсу — по паролю администратора через сеансы gresd с ограничением прав (ACL); при первом входе без пароля веб-интерфейс требует задать пароль администратора; в образах для управляемого развёртывания пустой пароль при первой загрузке заменяется случайным, далее пароль задаёт политика контроллера.

- Взаимодействие с контроллером — только по HTTPS с аутентификацией устройства токеном; закрытые ключи туннелей не покидают устройство.

8. Ограничения

- Набор доступных функций Wi-Fi (диапазоны, стандарты 802.11ax, число сетей) определяется радиомодулем и драйвером конкретного устройства.
- Функции централизованного управления (раздел 3.5) требуют подключения к системе управления Atlas Controller.
- На устройствах с малым объёмом памяти (8–16 МБ) используется облегчённый агент без веб-интерфейса и части сетевых функций.

Президент ООО «УК «МАКС» —
управляющей организации ООО «СВЯЗЬ»

_____ М. А. Клевцов