УТВЕРЖДАЮ

Генеральный директор ООО «Азон»

_____ /Е.А. Гуцало

«17» августа 2026 г.

МП

Описание функциональных характеристик

программного обеспечения

«Чистый интернет»

МОСКВА, 2026

1. Общие сведения

1.1. Настоящий документ содержит описание назначения, архитектуры и функциональных характеристик программного обеспечения «Чистый интернет» (далее — ПО, Комплекс) в соответствии с подпунктом «д» пункта 11 Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных, утверждённых постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236.

1.2. Правообладателем и разработчиком ПО является Общество с ограниченной ответственностью «Азон» (ИНН 7723340837, КПП 771301001, ОГРН 1037723029570).

1.3. Сведения о государственной регистрации программы для ЭВМ в Федеральной службе по интеллектуальной собственности (Роспатент):

Показатель	Значение
Название программы для ЭВМ	Чистый интернет
Правообладатель	Общество с ограниченной ответственностью «Азон» (RU)
Номер свидетельства о государственной регистрации	2026686084
Дата государственной регистрации	27.08.2026
Номер и дата поступления заявки	2026686151 от 27.08.2026
Дата публикации и номер бюллетеня	27.08.2026, бюл. № 9
Тип ЭВМ	IBM PC-совместимый персональный компьютер
Операционная система	Семейство Linux
Языки программирования	Go, Python, TypeScript
Объём программы	2,0 МБ
Контактные реквизиты правообладателя	+7 (495) 902-66-36, info@azone-it.ru

2. Назначение и область применения

2.1. ПО «Чистый интернет» предназначено для централизованного сбора и анализа журналов событий межсетевых экранов нового поколения (МСЭ «Континент»), автоматической категоризации посещаемых сетевых ресурсов на основе анализа их текстового содержимого с применением нейросетевых

алгоритмов (технологий искусственного интеллекта), формирования рекомендаций по блокировке нежелательного и запрещённого контента и предоставления единой операторской веб-консоли мониторинга и отчётности.

2.2. ПО разворачивается в локальном (on-premise) контуре организации и не требует передачи обрабатываемых данных во внешние облачные сервисы.

2.3. ПО не заменяет средства межсетевого экранирования и не выполняет функции средства криптографической защиты информации: оно надстраивается над существующей инфраструктурой фильтрации, повышая полноту и точность категоризации веб-ресурсов и снижая долю ложных срабатываний штатных списков категорий межсетевого экрана.

3. Функциональная структура и подсистемы

3.1. Комплекс построен по микросервисной архитектуре и включает пять функциональных подсистем:

— **Подсистема сбора и нормализации событий (`tg-etl`)** — чтение журналов событий межсетевых экранов из базы данных управления в режиме реального времени, нормализация записей, идемпотентная загрузка без дублирования по уникальному идентификатору события (`ids_log_id`), ведение контрольной точки опроса и построение сессий сетевой активности.

— **Подсистема извлечения содержимого и нейросетевой классификации (`webscraper`, `neuro`)** — извлечение основного текста веб-страниц по обнаруженным адресам, определение геолокации узлов по локальной базе, классификация текста и оценка эмоциональной тональности с помощью дообученных нейросетевых моделей формата ONNX, сопоставление результата с категорией межсетевого экрана.

— **Подсистема аналитики, выявлений и отчётности (`tg-analytics`, `frontend`)** — расчёт оперативных показателей, карточек выявлений, графиков трафика и тепловых карт активности, фильтрация сессий и формирование аналитических отчётов в форматах PDF, XLSX, JSON, DOCX и PPTX.

— **Подсистема формирования рекомендаций по блокировке** — ведение решений оператора по выявленным доменам («Разрешено» / «Заблокировано»), опциональное автоматическое принятие решений по настраиваемому порогу классификатора (`system:auto-policy`) и выгрузка машиночитаемого перечня ресурсов для блокировки (`block-list`) в форматах CSV и JSON со схемой версии `1.0`.

— **Подсистема администрирования, идентификации и аудита (`api-gw`, `userctrl`, `blog`, `keycloak`)** — единая точка входа REST API, аутентификация по токенам JWT (RS256), ролевая модель доступа и неизменяемый журнал действий пользователей.

4. Основные функциональные характеристики

4.1. Категоризация контента с применением искусственного интеллекта

4.1.1. Нейросетевой классификатор относит текстовое содержимое исследуемых ресурсов к категориям контролируемого контента (агрессия и экстремизм, наркотические средства, алкоголь и табак, азартные игры, компьютерные игры, социальные сети, реклама, вредоносное ПО, порнография, безопасный контент, неопределённый контент) с расчётом числовой оценки уверенности классификатора.

4.1.2. При расхождении между категорией, присвоенной межсетевым экраном, и категорией, определённой нейросетевой моделью, формируется признак расхождения (`ml_ngfw_mismatch`), позволяющий выявлять пропуски запрещённых ресурсов и ложные срабатывания.

4.1.3. Перечень категорий хранится в справочнике базы данных и расширяется средствами конфигурации без изменения исходного текста ПО.

4.2. Операторский веб-интерфейс (на русском языке)

4.2.1. Графический веб-интерфейс полностью реализован на русском языке, поддерживает светлую и тёмную темы оформления и включает следующие разделы:

Раздел интерфейса	Выполняемые функции
Обзор (`/dashboard`)	Сводные показатели за выбранный период, график входящего и исходящего трафика, карточки разрешённых, заблокированных и ожидающих запросов, рейтинг запрещённых категорий, топ нерешённых выявлений, распределение аномалий, тепловая карта запрещённой активности и состояние подключённых узлов межсетевых экранов
Выявления (`/detections`)	Сводка по общему числу выявлений, нерешённым, разрешённым, заблокированным ресурсам и расхождениям NGFW/ML; карточки ресурсов с описанием, геолокацией, числом обращений и кнопками принятия решения («Подтвердить», «Отклонить», «Отменить решение»)
Сессии (`/sessions`)	Таблица сетевых сессий со статусами («Разрешен», «Запрещен», «Ожидает», «Аномалия»), фильтрацией по периоду, узлу, категории, типу и поиском по URL
Отчёты (`/reports`)	Генератор аналитических отчётов за неделю, месяц, квартал, год или произвольный период по всем либо выбранному узлу с выгрузкой в форматах PDF, XLSX, JSON, DOCX, PPTX; выгрузка машиночитаемого списка блокировок (CSV, JSON); архив ранее сформированных отчётов
Пользователи (`/users`)	Создание, редактирование, блокировка и удаление учётных записей, назначение ролей и сброс временных паролей
Логи (`/logs`)	Просмотр журнала действий пользователей (создание, изменение, удаление объектов) с поиском и фильтрацией
Настройки и Профиль (`/settings`, `/profile/edit`)	Переключение темы оформления, управление режимом автоматического принятия решений по выявлениям, переход к панелям технического мониторинга, редактирование профиля и смена пароля

4.3. Ролевая модель доступа

Роль	Обозначение	Полномочия
Системный администратор	`SA`	Доступ ко всем подключённым узлам, работа с разделом выявлений, принятие решений по блокировке, выгрузка перечня блокировок, управление пользователями и настройками
Администратор узла	`CA-<узел>`	Доступ к аналитике, сессиям, отчётам, пользователям и журналу событий строго в пределах закреплённого узла межсетевого экрана
Оператор	`CO-<узел>`	Просмотр обзора, сессий и

		формирование отчётов в пределах закреплённого узла

4.4. Программный интерфейс и форматы обмена данными

4.4.1. Комплекс предоставляет документированный REST API по протоколу HTTPS с префиксом `/api/v1` и интерактивной спецификацией OpenAPI (`/swagger/`).

4.4.2. Для интеграции со смежными системами предусмотрены машиночитаемые выгрузки с явным указанием версии схемы данных (`schema_version: "1.0"`):

— аналитический отчёт в формате JSON (`GET /api/v1/reports`, `GET /api/v1/reports/{hostname}`);

— перечень заблокированных ресурсов в форматах JSON и CSV (`GET /api/v1/block-list?format=json|csv`).

5. Требования к программно-аппаратной среде и сведения об установке и эксплуатации

5.1. Комплекс функционирует на серверных платформах архитектуры x86-64 под управлением операционных систем семейства Linux (включая отечественные дистрибутивы Astra Linux Special Edition, РЕД ОС, Альт Сервер, а также Ubuntu Server 22.04 / 24.04 LTS) со средой контейнеризации Docker Engine и модулем Docker Compose v2.

5.2. Минимальные аппаратные требования для развёртывания на одном узле: не менее 4 вычислительных ядер CPU (8 ядер при локальном выполнении нейросетевой классификации на CPU), не менее 16 ГиБ оперативной памяти (32 ГиБ при локальном ML), не менее 100 ГиБ на твердотельном накопителе SSD. При выносе нейросетевой классификации на выделенный сервер с графическим ускорителем поддерживаются ускорители NVIDIA с объёмом видеопамяти не менее 16 ГБ.

5.3. Подробные инструкции по установке, конфигурированию, резервному копированию, мониторингу и обновлению приведены в документе **«Руководство администратора программного обеспечения «Чистый интернет»**, инструкции по работе пользователя в веб-интерфейсе — в документе **«Руководство оператора программного обеспечения «Чистый интернет»**.