УТВЕРЖДАЮ

Генеральный директор ООО «Азон»

_____ / Е.А. Гуцало

«17» августа 2026 г.



МП

Руководство администратора

программного обеспечения

«Чистый интернет»

МОСКВА, 2026

1. Общие сведения

1.1. Настоящий документ является руководством администратора программного обеспечения «Чистый интернет» (далее — Комплекс) и разработан в соответствии с п. 10.3 Технического задания на разработку программного обеспечения «Чистый интернет».

1.2. Документ предназначен для специалиста, выполняющего развёртывание, настройку, эксплуатацию и восстановление Комплекса.

1.3. Требуемая квалификация администратора: администрирование операционных систем семейства Linux, работа со средствами контейнеризации, администрирование системы управления базами данных PostgreSQL, базовые навыки настройки сетевых служб и средств криптографической защиты каналов связи.

1.4. Комплекс устанавливается в закрытом контуре информационной системы Заказчика. Передача обрабатываемых данных во внешние сервисы не выполняется.

1.5. Применяемые сокращения:

— МСЭ — межсетевой экран;

— NGFW — межсетевой экран нового поколения (МСЭ «Континент»);

— КСУ — узел централизованного управления МСЭ «Континент», источник журналов событий;

— КСФ — узел фильтрации МСЭ «Континент»;

— СУБД — система управления базами данных;

— ETL — подсистема извлечения, преобразования и загрузки данных;

— ML — нейросетевая классификация содержимого;

— SA, CA, CO — роли системного администратора, администратора узла и оператора соответственно.

2. Состав и архитектура Комплекса

2.1. Поток обработки данных

2.1.1. Обработка данных выполняется по следующей схеме:

МСЭ «Континент» → база данных КСУ (таблица `ids_log`) → служба ETL → база данных Комплекса → брокер сообщений → служба извлечения содержимого → служба нейросетевой классификации → служба ETL → служба аналитики → шлюз программного интерфейса → веб-интерфейс.

2.1.2. Обратный прокси-сервер является единственной точкой публикации Комплекса в сети Заказчика. Внутренние службы сетевых портов на узел не публикуют.

2.2. Перечень служб

Служба	Назначение	Внутренний порт
`nginx`	Обратный прокси-сервер, терминирование TLS, публикация Комплекса	80, 443 (публикуются)
`frontend`	Веб-интерфейс оператора	3001
`api-gw`	Шлюз программного интерфейса, проверка маркеров доступа, маршрутизация	8001
`tg-an`	Служба аналитики: показатели, сессии, выявления, отчёты, перечень блокировок	7000
`tg-etl`	Служба ETL: опрос базы данных КСУ, оркестрация обработки, приём результатов классификации	8005
`tg-usercontrol`	Управление учётными записями и ролями	8002
`tg-blog`	Журнал бизнес-событий (только чтение через программный интерфейс)	8004
`webscraper`	Извлечение содержимого ресурсов, определение геолокации	8010
`neuro`	Нейросетевая классификация содержимого и тональности	8071
`kafka`, `zookeeper`	Брокер сообщений и служба координации	9092, 2181
`kafka-ui`	Служебный интерфейс контроля очередей	8080
`configdb`	СУБД PostgreSQL Комплекса	5432
`keycloak`	Служба идентификации и выдачи маркеров доступа	8443
`grafana`	Служебные панели мониторинга	3000
`prometheus`, `node_exporter`	Сбор метрик служб и узла	9090, 9100

2.2.1. Все службы разворачиваются как контейнеры в единой сети контейнеризации `deploy_continent`.

2.2.2. База данных КСУ является внешней по отношению к Комплексу и относится к зоне ответственности эксплуатирующей организации МСЭ «Континент». Комплекс обращается к ней в режиме чтения.

2.3. Базы данных

База данных	Размещение	Назначение
`etl`	СУБД Комплекса	Нормализованные события, сессии, домены, категории, решения по блокировке, контрольные точки
`ml`	СУБД Комплекса	Результаты нейросетевой

		классификации
`keycloak`	СУБД Комплекса	Учётные записи и роли
`blog`	СУБД Комплекса	Журнал бизнес-событий
`grafana`	СУБД Комплекса	Конфигурация панелей мониторинга
`web`	СУБД Комплекса	Служебные данные веб-интерфейса
`ksu` (таблица `ids_log`)	Внешняя СУБД КСУ	Источник журналов МСЭ (только чтение)
`ksu_mon` (таблица `stats_json`)	Внешняя СУБД КСУ	Показатели состояния узлов (только чтение)

3. Требования к техническим и программным средствам

3.1. Программные средства узла

3.1.1. Операционная система семейства Linux архитектуры x86-64. Проверенные варианты — Ubuntu Server 22.04 LTS и 24.04 LTS, а также отечественные дистрибутивы, поддерживающие среду контейнеризации.

3.1.2. Среда контейнеризации Docker Engine с подключаемым модулем Compose версии 2 (команда `docker compose`).

3.1.3. Дополнительно требуются пакеты `ca-certificates`, `curl`, `gnupg`, `openssl`, `make`, `git`.

3.1.4. Эксплуатация Комплекса выполняется от имени непривилегированной учётной записи, включённой в группу `docker`. Запуск от имени суперпользователя не требуется и не рекомендуется.

3.2. Аппаратные средства

3.2.1. Минимальная конфигурация узла для пилотной эксплуатации: не менее 4 вычислительных ядер, не менее 16 ГиБ оперативной памяти, не менее 100 ГиБ дискового пространства на твердотельном накопителе.

3.2.2. Рекомендуемая конфигурация при размещении нейросетевой классификации на том же узле: не менее 8 вычислительных ядер и не менее 32 ГиБ оперативной памяти.

3.2.3. При размещении нейросетевой классификации на выделенном узле с графическим ускорителем на этом узле дополнительно требуются драйвер NVIDIA и модуль `nvidia-container-toolkit`, не менее 16 ГБ видеопамяти и свободный порт TCP 8071.

3.3. Сетевое взаимодействие

Направление	Порт	Назначение
Рабочие места → узел Комплекса	TCP 443	Веб-интерфейс и программный интерфейс
Рабочие места → узел Комплекса	TCP 80	Перенаправление на защищённое соединение и подтверждение владения доменом
Узел Комплекса → СУБД КСУ	TCP 5432	Чтение журналов МСЭ
Узел с графическим ускорителем → узел Комплекса	TCP 9094, TCP 5433	Внешние точки подключения брокера сообщений и СУБД при выносе классификации

4. Установка и первичное развёртывание

4.1. Автоматизированная установка

4.1.1. Основным способом первичного развёртывания является установочный сценарий:

```
bash deploy/scripts/install.sh --domain <доменное имя или адрес> --le-email <адрес электронной почты>
```

4.1.2. Сценарий выполняет следующие действия:

— проверку наличия среды контейнеризации, требуемых утилит и свободных портов 80 и 443;

— создание сети контейнеризации `deploy_continent`;

— формирование файлов параметров среды из поставляемых образцов (корневой файл и файлы отдельных служб);

— генерацию стойких значений паролей и служебных ключей и согласованную их подстановку во все файлы параметров;

— настройку доменного имени, разрешённых источников межсайтовых запросов и выпуск внутренних сертификатов;

— создание каталогов постоянного хранения данных служб;

— сборку и запуск всех служб;

— контроль перехода служб в работоспособное состояние и вывод сводки с адресом веб-интерфейса и реквизитами первичной учётной записи.

4.1.3. Поддерживаемые параметры сценария:

Параметр	Назначение
`--domain`	Доменное имя или сетевой адрес публикации Комплекса
`--le-email`	Адрес электронной почты для выпуска публичного сертификата
`--ksu-host`, `--ksu-pass`	Реквизиты подключения к внешней СУБД КСУ
`--offline`	Установка без подключённого МСЭ; режим наблюдения переводится в демонстрационный
`--no-deploy`	Подготовка параметров и сертификатов без запуска служб
`--letsencrypt`	Выпуск и активация публичного сертификата
`--force`	Повторная генерация файлов параметров (требует очистки томов баз данных)
`--yes`	Работа без интерактивных запросов

4.1.4. Сценарий не перезаписывает существующие файлы параметров без указания `--force`, что позволяет выполнять его повторно.

4.2. Установка в ручном режиме

4.2.1. Скопировать образцы файлов параметров: корневой файл параметров среды и файлы параметров каждой службы.

4.2.2. Создать сеть контейнеризации `deploy_continent`.

4.2.3. Выпустить внутренние сертификаты командой `make cert-gen`.

4.2.4. Выполнить развёртывание командой `make deploy`.

4.3. Целевые команды сборки

Команда	Действие

`make all`	Выпуск внутренних сертификатов и развёртывание
`make install`	Запуск установочного сценария
`make cert-gen`	Выпуск внутренних сертификатов
`make cert-letsencrypt`	Выпуск публичного сертификата
`make activate-public-ssl`	Активация публичного сертификата на обратном прокси-сервере
`make stand-domain-env`	Настройка доменного имени и разрешённых источников запросов
`make secret-scan`	Проверка отсутствия секретов в составе поставки
`make deploy`	Сборка и запуск служб
`make stop`	Останов служб
`make status`	Отображение состояния служб
`make clean`	Полное удаление служб, томов и локальных образов
`make nginx-reload`	Перезапуск обратного прокси-сервера после изменения параметров защищённого соединения

4.4. Сертификаты

4.4.1. Комплекс использует два независимых контура сертификатов.

4.4.2. **Внутренний контур** обслуживает взаимодействие служб между собой, а также службы идентификации и мониторинга. Сертификаты выпускаются командой `make cert-gen`; сертификат удостоверяющего центра размещается в каталоге данных транспортной защиты и используется службами для проверки подлинности партнёров.

4.4.3. **Публичный контур** обслуживает порт 443 обратного прокси-сервера. При наличии выхода к службе автоматического выпуска сертификатов применяются команды `make cert-letsencrypt` и `make activate-public-ssl`. В закрытом контуре применяется самоподписанный сертификат с указанием сетевого адреса узла в поле альтернативных имён и соответствующий файл параметров защищённого соединения.

5. Конфигурирование

5.1. Порядок применения параметров

5.1.1. Параметры служб задаются в файлах YAML в составе поставки и в файлах параметров среды каталога развёртывания. **Значения из среды имеют приоритет над значениями из файлов YAML.**

5.1.2. Корневой файл параметров среды содержит общие значения: версии образов, имена и порты служб, реквизиты пользователей и наименования баз данных, доменное имя, режим наблюдения и режим работы нейросетевого компонента.

5.1.3. Файлы параметров отдельных служб размещаются в каталогах соответствующих служб и содержат частные значения.

5.2. Ключевые группы параметров

Группа	Назначение	Примечание
`POSTGRES_*`	Реквизиты СУБД Комплекса и наименования баз данных	Задаются до первого запуска; изменение после инициализации требует очистки томов
`KC_*`, `KEYCLOAK_*`	Параметры службы идентификации, реквизиты администратора службы и первичной учётной записи Комплекса	Пароль администратора службы идентификации и пароль первичной учётной записи Комплекса — разные значения

ETL_KSU_*	Адрес, порт, наименование базы данных и реквизиты доступа к внешней СУБД КСУ	Учётная запись должна обладать правом чтения
ETL_PG_*	Реквизиты базы данных Комплекса для службы ETL	
ETL_RUN_MIGRATIONS	Применение миграций схемы при запуске службы ETL	Штатное значение — включено
ETL_REFRESH	Интервал опроса источника в секундах	Штатное значение — 10
ETL_MAX_COUNT	Размер пакета обрабатываемых записей	Штатное значение — 100
ETL_CACHE_TTL	Срок жизни внутреннего кеша	
ETL_KAFKA_*	Адрес брокера сообщений и наименование очереди необработанных сообщений	
ETL_AUTO_DECISION_*	Режим автоматического принятия решения и пороговые значения	Штатное значение режима — выключено
AN_ETL_*, AN_METRICS_*	Источники данных службы аналитики	
AN_NEG_DETECTION_THRESHOLD	Порог отнесения выявления к негативным	Штатное значение — 0,5
AN_CORS_ORIGINS, API_GW_CORS_ORIGINS, USER_CTRL_CORS_ORIGINS	Перечень разрешённых источников межсайтовых запросов	Заполняется сценарием настройки домена
API_GW_KEYCLOAK_PEM, AN_KEYCLOAK_PEM	Путь к открытому ключу проверки маркеров доступа	Формируется служебным сценарием
API_GW_AUTH_RATE_LIMIT	Ограничение частоты попыток входа с одного адреса в минуту	Штатное значение — 20
WEBSCRAPER_WORKERS_MAX	Предельное число потоков извлечения содержимого	Штатное значение — 32
WEBSCRAPER_API_KEY	Служебный ключ синхронного извлечения содержимого	При пустом значении метод недоступен
NEURO_MODELS_DIR	Каталог размещения нейросетевых моделей	Подключается к службе классификации в режиме только для чтения
NEURO_MODE	Режим нейросетевого компонента: локальный или на выделенном узле	
CONTENTGUARD_MONITORING_MODE	Режим наблюдения: рабочий, обслуживание, демонстрационный	Демонстрационный режим подавляет оповещения об отсутствии потока данных
*_TLS_INSECURE_SKIP_VERIFY	Отключение проверки сертификата партнёра	В промышленной эксплуатации должно быть выключено

5.2.1. Изменение параметров вступает в силу после пересоздания соответствующей службы.

6. Базы данных и миграции

6.1. Схема базы данных Комплекса создаётся и обновляется версионируемыми миграциями. Файлы миграций входят в состав поставки службы ETL.

6.2. При включённом параметре применения миграций служба ETL применяет непринятые миграции автоматически при запуске. Порядок применения определяется нумерацией файлов, сведения о применённых миграциях хранятся в служебной таблице.

6.3. Состав миграций и вносимые изменения:

Миграция	Содержание
Базовая	Таблицы узлов, источников, категорий, доменов, действий, связей доменов с категориями, перечней контроля, адресов ресурсов, сессий и контрольных точек
Идентификатор исходной записи	Поле связи сессии с записью журнала МСЭ и частичный уникальный индекс
Оповещения о трафике	Поле категории МСЭ у домена и таблица оповещений
Системные настройки	Таблица параметров, изменяемых из интерфейса
Полный уникальный индекс	Полный уникальный индекс по идентификатору исходной записи

6.4. Таблица результатов нейросетевой классификации создаётся отдельным служебным сценарием инициализации базы данных классификации.

6.5. Откат миграции выполняется вручную по согласованию с разработчиком. Автоматизированная процедура отката схемы не предусмотрена; штатным способом восстановления состояния является восстановление из резервной копии по разделу 12.

6.6. Перед применением миграций при обновлении Комплекса обязательно создание резервной копии.

7. Служба идентификации и управление доступом

7.1. Настройка службы идентификации

7.1.1. Служба идентификации разворачивается в составе Комплекса, использует выделенную базу данных и не публикует сетевых портов за пределы сети контейнеризации.

7.1.2. При первом запуске выполняется импорт области безопасности из файла, входящего в состав поставки. В области безопасности создаются клиент приложения, группы и роли.

7.1.3. Открытый ключ проверки маркеров доступа выгружается служебным сценарием и указывается в параметрах шлюза программного интерфейса и службы аналитики. При смене ключей службы идентификации выгрузку необходимо повторить и пересоздать указанные службы.

7.2. Первичная учётная запись

7.2.1. При установке создаётся учётная запись `admin` с ролью системного администратора. Пароль формируется установочным сценарием и указывается в файле параметров службы идентификации.

7.2.2. Пароль администратора консоли службы идентификации и пароль первичной учётной записи Комплекса — различные значения; их не следует смешивать.

7.2.3. После первого входа пароль первичной учётной записи подлежит смене средствами веб-интерфейса.

7.3. Ролевая модель

Роль	Обозначение	Область видимости и полномочия
Системный администратор	`SA`	Весь контур: все узлы, работа с выявлениями, выгрузка перечня блокировок, управление учётными записями и параметрами
Администратор узла	`CA-<идентификатор узла>`	Данные закреплённого узла, управление учётными записями своего узла

Оператор	СО-<идентификатор узла>	Просмотр показателей, сессий и отчётов в пределах закреплённого узла

7.3.1. Роли администратора узла и оператора создаются парой при регистрации нового узла средствами службы управления пользователями.

7.3.2. Ограничение области видимости для роли администратора узла применяется на стороне службы аналитики: запросы автоматически ограничиваются идентификатором закреплённого узла независимо от параметров запроса.

7.3.3. Доступ к работе с нейросетевыми выявлениями, к изменению решения по ресурсу и к выгрузке перечня блокировок предоставляется только роли системного администратора.

7.3.4. В форме создания учётной записи веб-интерфейса доступны роли системного администратора и администратора узла. Учётные записи с ролью оператора создаются администратором средствами службы управления пользователями.

8. Подключение к МСЭ «Континент»

8.1. Комплекс получает журналы событий из внешней СУБД КСУ в режиме чтения. Реквизиты подключения задаются группой параметров службы ETL.

8.2. Учётной записи Комплекса в СУБД КСУ достаточно права подключения к базе данных и права чтения таблицы журнала событий и таблицы показателей состояния узлов. Права на изменение данных не требуются и не должны предоставляться.

8.3. Корректность подключения проверяется служебным сценарием контроля доступа к СУБД КСУ: проверяются сетевая доступность, подлинность реквизитов, наличие прав чтения и положение контрольной точки службы ETL.

8.4. Служба ETL ведёт контрольную точку обработки. Повторный запуск службы продолжает обработку с последней зафиксированной позиции; повторная загрузка одной и той же записи журнала не приводит к появлению дубликата сессии за счёт уникального индекса по идентификатору исходной записи.

8.5. Сброс контрольной точки для повторной обработки выполняется служебным сценарием настройки подключения с соответствующим параметром. Операция выполняется по согласованию, так как приводит к повторной обработке ранее принятых записей.

8.6. При развёртывании до подключения МСЭ режим наблюдения переводится в демонстрационный, что исключает ложные оповещения об отсутствии потока данных.

9. Нейросетевой компонент

9.1. Локальное размещение

9.1.1. В штатной поставке служба классификации разворачивается на узле Комплекса и использует вычисления на центральном процессоре.

9.1.2. Файлы моделей размещаются в каталоге, указанном параметром каталога моделей, и подключаются к службе в режиме только для чтения. Пути к модели классификации содержимого, модели определения тональности и каталогу разбиения текста задаются отдельными параметрами.

9.1.3. Перед первым запуском необходимо разместить файлы моделей в указанном каталоге и выполнить инициализацию базы данных классификации.

9.1.4. Состояние службы контролируется методом проверки работоспособности, который возвращает признаки доступности базы данных, брокера сообщений и загруженных моделей. Следует учитывать, что штатная проверка среды контейнеризации подтверждает только факт ответа службы; содержательное состояние необходимо контролировать по телу ответа.

9.2. Размещение на выделенном узле с графическим ускорителем

9.2.1. Для повышения производительности классификация может быть вынесена на выделенный узел. В этом случае режим нейросетевого компонента переводится в соответствующее значение и применяется дополнительный файл описания служб, открывающий внешние точки подключения брокера сообщений и базы данных классификации.

9.2.2. Комплект для выделенного узла включает файл описания службы, образец файла параметров, образ контейнера, архив моделей, сценарии проверки и инструкцию для администратора узла.

9.2.3. Возврат к локальному размещению выполняется служебным сценарием восстановления локальной классификации.

9.3. Проверка прохождения данных

9.3.1. Сквозная проверка нейросетевой обработки выполняется служебным сценарием и считается успешной при одновременном выполнении условий: служба классификации сообщает о работоспособном состоянии; позиция чтения очереди результатов классификации увеличилась; в базе данных классификации появилась запись с идентификатором проверочного запроса.

9.4. Очереди обработки

Очередь	Отправитель	Получатель
Запросы на обработку адресов	Служба ETL	Служба извлечения содержимого
Результаты по метаданным адресов	Служба извлечения содержимого	Служба ETL
Содержимое для анализа	Служба извлечения содержимого	Служба классификации
Результаты классификации	Служба классификации	Служба ETL
Очередь необработанных сообщений	Служба ETL	—

10. Штатная эксплуатация

10.1. Управление службами

Операция	Команда
Запуск и обновление служб	`make deploy`
Останов служб	`make stop`
Состояние служб	`make status`
Перезапуск обратного прокси-сервера	`make nginx-reload`
Пересоздание отдельной службы	Пересоздание средствами модуля Compose с указанием имени службы

10.2. Контроль работоспособности

10.2.1. Каждая служба предоставляет метод проверки работоспособности, опрашиваемый средой контейнеризации. Публично доступны проверка работоспособности шлюза программного интерфейса, стартовая страница веб-интерфейса и раздел панелей мониторинга.

10.2.2. Комплексная проверка узла выполняется служебным сценарием контроля состояния, который проверяет состояние контейнеров, доступность методов по защищённому соединению, срок действия сертификатов, состояние очередей, подключение к СУБД КСУ и состояние нейросетевого компонента.

10.3. Журналы работы

10.3.1. Службы ведут структурированные журналы в формате JSON и выводят их в стандартный поток вывода контейнера. Просмотр выполняется штатными средствами среды контейнеризации.

10.3.2. Для сквозной трассировки применяются идентификатор запроса в журналах программного интерфейса, идентификатор исходной записи журнала МСЭ при загрузке данных и идентификатор запроса в очередях нейросетевой обработки.

10.3.3. Централизованный сбор журналов Комплексом не выполняется; при необходимости он организуется средствами Заказчика на уровне среды контейнеризации.

11. Мониторинг

11.1. Службы шлюза программного интерфейса, аналитики, ETL и извлечения содержимого публикуют метрики в формате системы сбора метрик по отдельному методу. Дополнительно собираются метрики узла.

11.2. Панели мониторинга поставляются в составе конфигурации службы визуализации и включают панели производительности программного интерфейса, состояния журнала МСЭ, состояния приёма событий и состояния системы сбора метрик.

11.3. Правила оповещения поставляются в составе конфигурации и включают контроль свежести данных по метрике отметки времени последнего принятого события в разрезе потоков.

11.4. Доставка оповещений настраивается через веб-перехватчик или электронную почту заданием соответствующих параметров службы визуализации.

11.5. Вход в службу визуализации выполняется через единую службу идентификации; роль администратора визуализации назначается при наличии в маркере доступа роли системного администратора.

12. Резервное копирование и восстановление

12.1. Резервное копирование базы данных Комплекса выполняется служебным сценарием создания резервной копии. Копия сохраняется в каталог резервных копий в сжатом виде с сопровождающим файлом контрольной суммы.

12.2. Срок хранения резервных копий задаётся параметром и по умолчанию составляет 14 суток.

12.3. Периодическое выполнение резервного копирования настраивается модулем системного менеджера служб, входящим в состав поставки, либо, при его недоступности, планировщиком заданий через соответствующий сценарий установки.

12.4. Проверка пригодности резервной копии выполняется служебным сценарием проверки, который восстанавливает копию во временное окружение и не затрагивает рабочую базу данных. Проверку следует выполнять регулярно.

12.5. Резервное копирование внешней СУБД КСУ Комплексом не выполняется и относится к зоне ответственности эксплуатирующей организации МСЭ.

12.6. Восстановление выполняется на остановленных службах приложений: разворачивается резервная копия базы данных, после чего службы запускаются и выполняется контроль работоспособности по разделу 10.2.

13. Обновление и откат

13.1. Обновление выполняется в следующем порядке:

— создать резервную копию базы данных согласно разделу 12;

— получить обновлённую версию исходных материалов и привести рабочую копию к целевому состоянию;

— выполнить развёртывание командой `make deploy`;

— при изменении параметров защищённого соединения перезапустить обратный прокси-сервер;

— выполнить контроль работоспособности согласно разделу 10.2.

13.2. Для ускорения обновления отдельных служб применяются служебные сценарии частичной пересборки веб-интерфейса, шлюза программного интерфейса, службы ETL и службы аналитики.

13.3. Откат выполняется приведением рабочей копии к предыдущему состоянию и повторным развёртыванием. Откат исходных материалов не выполняет обратного преобразования схемы базы данных: при необходимости выполняется восстановление из резервной копии, созданной до обновления.

13.4. Откат образа нейросетевой службы не изменяет ранее сохранённые результаты классификации.

14. Диагностика и устранение неисправностей

14.1. Средства диагностики

Средство	Назначение
Сценарий контроля состояния узла	Комплексная проверка контейнеров, соединений, сертификатов, очередей и внешних источников
Сценарий контроля доступа к СУБД КСУ	Проверка сетевой доступности, реквизитов, прав чтения и контрольной точки
Сценарий диагностики приёма событий	Проверка поступления записей журнала МСЭ и работы службы ETL
Сценарий проверки нейросетевой обработки	Сквозная проверка цепочки классификации
Сценарий проверки состава поставки	Контроль отсутствия секретов в поставляемых файлах

14.2. Типовые неисправности

Признак	Вероятная причина и порядок действий
Веб-интерфейс отображается, данные отсутствуют	Отсутствуют записи в журнале МСЭ либо не настроено подключение к СУБД КСУ. Выполнить сценарий контроля доступа к СУБД КСУ, проверить журнал службы ETL
Служба ETL сообщает об отсутствии новых записей	Штатное состояние при пустом источнике либо при достижении конца журнала. Проверить наличие новых записей в источнике
Ошибки проверки маркеров доступа	Не соответствует открытый ключ проверки. Повторно выгрузить ключ службы идентификации и пересоздать шлюз программного интерфейса и службу аналитики
Запросы веб-интерфейса отклоняются политикой межсайтовых запросов	Не задано доменное имя в перечне разрешённых источников. Выполнить сценарий настройки домена и пересобрать веб-интерфейс
Обратный прокси-сервер циклически перезапускается	Заданы параметры публичного сертификата при его

	отсутствии. Временно перевести на самоподписанный сертификат
Нейросетевая классификация не выполняется	Отсутствуют файлы моделей либо не инициализирована база данных классификации. Проверить каталог моделей, журнал службы, выполнить сквозную проверку
Кратковременные ошибки разрешения имён при запуске	Штатное состояние гонки запуска служб; при переходе служб в работоспособное состояние не требует вмешательства

15. Требования безопасности при эксплуатации

15.1. Обмен с рабочими местами выполняется по защищённому соединению. Порт незащищённого соединения используется только для перенаправления и подтверждения владения доменным именем.

15.2. Прямой доступ к базе данных, брокеру сообщений, службе идентификации и внутренним службам за пределы сети контейнеризации не публикуется. Публикуются только порты обратного прокси-сервера.

15.3. Параметры доступа хранятся в файлах параметров среды, не входящих в состав передаваемых исходных материалов. Перед передачей поставки выполняется проверка сценарием контроля состава.

15.4. Смена параметров доступа выполняется правкой соответствующих файлов параметров с последующим пересозданием служб и, при смене реквизитов баз данных, синхронным изменением на стороне СУБД. Изменение исходного кода при этом не требуется.

15.5. Отключение проверки подлинности сертификатов партнёров допускается только на этапе отладки во внутреннем контуре и должно быть выключено в промышленной эксплуатации.

15.6. Ограничение частоты попыток входа задаётся параметром шлюза программного интерфейса и по умолчанию составляет 20 попыток в минуту с одного сетевого адреса.

15.7. Обработка данных выполняется внутри контура Комплекса. Обращения к внешним сервисам обработки данных не производятся.

Разработчик:	
ООО «Азон»	_____/ _____