**УТВЕРЖДЕН**
643.СПЕТ.21092-01 94 01-ЛУ

# СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АГЕНТ СЕРВЕРА БЕЗОПАСНОСТИ»

Инструкция по установке

643.СПЕТ.21092-01 94 01

Листов 8

| Инв. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата |
|---|---|---|---|---|
| | | | | |

2025

# АННОТАЦИЯ

Настоящий документ является инструкцией по установке (далее – Инструкция) для специального программного обеспечения «Агент сервера безопасности».

Инструкция содержит общие сведения о программном обеспечении, его характеристиках, а также о порядке выполнения действий по установке.

Документ разработан с учетом основных положений ГОСТ 19.105–78 «Единая система программной документации. Общие требования к программным документам» и ГОСТ 19.503–79 «Руководство системного программиста».

# СОДЕРЖАНИЕ

# 1. ОБЩИЕ СВЕДЕНИЯ

## 1.1. Наименование

Полное наименование программы: «Агент сервера безопасности».

Обозначение программы: 643.СПЕТ.21092-01.

В рамках настоящего документа употребляется также обозначение «СПО».

«Агент сервера безопасности» – российское специальное программное обеспечение. Правообладателем ПО является Акционерное общество «ИНСЕК» (АО «ИНСЕК»).

Сайт разработчика: https://inseq.ru/.

## 1.2. Назначение

### 1.2.1. Функциональное назначение

Специальное программное обеспечение «Агент сервера безопасности» предназначено для:

– осуществления функций централизованного контроля и управления модулями доверенной загрузки (далее – МДЗ);

– централизованного мониторинга, контроля и управления средствами защиты информации (далее – СЗИ);

– интеграции с различными СЗИ для автоматизации процессов администрирования и реагирования на угрозы.

### 1.2.2. Эксплуатационное назначение

СПО «Агент сервера безопасности» предназначено для обеспечения централизованного взаимодействия пользователя с модулями доверенной загрузки и средствами защиты информации.

## 1.3. Функции ПО

СПО «Агент сервера безопасности» реализует выполнение следующих функциональных возможностей:

– централизованный контроль и управление модулями доверенной загрузки;

– централизованный контроль и управление средствами защиты информации;

– отображение событий безопасности в едином интерфейсе;

– ведение журнала событий безопасности в отдельной базе данных;

– оповещение о событиях безопасности.

# 2. ОПИСАНИЕ ХАРАКТЕРИСТИК ПО

## 2.1. Технические средства, необходимые для функционирования

Для корректного функционирования СПО оборудование должно иметь характеристики не хуже:

- процессор с тактовой частотой не ниже 2 ГГц;
- ОЗУ – не менее 2 Гб;
- объем свободного дискового пространства на НЖМД – не менее 1 Гбайт;
- монитор с разрешением не менее 1024x768;
- наличие устройства для вывода звука.

Приведенные выше требования к техническим средствам являются минимально допустимыми. Применение более производительных технических средств улучшает эксплуатационные свойства ПО.

## 2.2. Программные средства, необходимые для функционирования

Для выполнения СПО на вычислительном оборудовании организации-заказчика должны быть установлены следующие программные средства:

- для функционирования МАСБ:
  - операционная система Astra Linux Special Edition РУСБ.10015-01 (версия 1.6 «Смоленск» и выше);
  - пакеты GStreamer: libgstreamer1.0-0, gstreamer1.0-plugins-base, gstreamer1.0-plugins-good, gstreamer1.0-plugins-bad, gstreamer1.0-plugins-ugly, gstreamer1.0-libav;
  - Python 3.
- для функционирования МУ АСБ:
  - операционная система Astra Linux Special Edition РУСБ.10015-01 (версия 1.6 «Смоленск» и выше);
  - система управления базами данных (далее – СУБД): PostgreSQL (версия 9.6).
- для функционирования МКОСБ:
  - операционная система Astra Linux Special Edition РУСБ.10015-01 (версия 1.6 «Смоленск» и выше;
- СУБД: PostgreSQL (версия 9.6).

### 2.3. Уровень квалификации пользователя

Эксплуатация выполняется конечными пользователями, которые должны обладать знаниями о функциональных возможностях ПО в рамках технической документации («Руководство пользователя»), а также навыками администрирования операционных систем семейства Linux.

# 3. УСТАНОВКА

БД АСБ использует систему управления базами данных PostgreSQL 9.6, устанавливается и настраивается с помощью пакета ssa-control.deb. Для установки пакета необходимо перейти в каталог с дистрибутивом и выполнить команду:

sudo dpkg -i ./ssa-control.deb.

В результате будет установлена консольная утилита ssa-control, предназначенная для управления БД АСБ. Далее необходимо выполнить команду:

/opt/ssa/install_server.sh

Перед выполнением скрипта у пользователя будет запрашиваться ввод следующих параметров:

– PG_PORT: порт для подключения к PostgreSQL (по умолчанию 5446);

– NEW_DB_NAME: имя новой базы данных для создания (по умолчанию ssadb);

– NEW_DB_USER: имя пользователя базы данных (по умолчанию ssauser);

– SERVER_IP: IP-адрес сервера, на котором будет запущена база данных (по умолчанию берется автоматически).

Для того, чтобы выполнить скрипт, необходимо выполнить следующее:

– проверка прав пользователя: скрипт проверяет, что он запущен с правами суперпользователя (root). Если права недостаточны, скрипт завершится с ошибкой;

– установка PostgreSQL: скрипт выполняет установку PostgreSQL версии, указанной в переменной PG_VERSION, а также пакетов openssl и acl;

– создание системного пользователя для базы данных: создается системный пользователь для работы с базой данных, если он еще не существует;

– генерируется корневой сертификат (SSA-ROOT);

– генерируется серверный сертификат для PostgreSQL с использованием Subject Alternative Name (SAN), включающего IP-адрес сервера;

– генерируется клиентский сертификат для пользователя базы данных;

– настройка PostgreSQL для работы с SSL и локальной сетью;

– настройка файла pg_hba.conf: добавляется строка для разрешения подключения к базе данных по сертификатам (метод hostssl);

– перезапуск PostgreSQL: после внесения изменений в конфигурацию скрипт перезапускает службу PostgreSQL для применения новых настроек;

– проверка существования базы данных: скрипт проверяет, существует ли база данных с указанным именем (NEW_DB_NAME). Если база данных уже существует, она не будет создана заново;

– создание роли пользователя: создается роль пользователя для подключения к базе данных, предоставляется роль суперпользователя с правами на создание и управление объектами в БД;

– выполнение SQL-скрипта: скрипт выполняет SQL-скрипт (database.sql), если файл существует, для создания и настройки базы данных;

– генерация клиентского сертификата: генерируется клиентский сертификат для пользователя базы данных, который используется для подключения по защищенному каналу (SSL);

– настройка прав доступа: скрипт настраивает права доступа к файлам /etc/parsec/macdb и /etc/parsec/capdb, для пользователя postgres;

– конфигурация подключения: скрипт использует утилиту ssa-control для инициализации подключения к базе данных и обновления конфигурации для системы мониторинга.

МАСБ функционирует как сервис (служба) в операционной системе Linux. Он предназначен для выполнения функций мониторинга СЗИ, контроля и централизованного управления МДЗ. Для установки МАСБ необходимо перейти в каталог с дистрибутивом и выполнить команду:

sudo dpkg -i ./ssa-client.deb.

Модуль комплексного отображения событий безопасности (МКОСБ) — выполняет функции отображения событий, полученных от МАСБ в графическом интерфейсе. Модуль управления агентом сервера безопасности (МУ АСБ) — выполняет функции настройки МАСБ в графическом интерфейсе. МКОСБ и МУ АСБ устанавливаются с помощью пакета ssa-manager.deb. Для установки модулей МКОСБ и МУ АСБ необходимо перейти в каталог с дистрибутивом и выполнить команду:

sudo dpkg -i ./ssa-manager.deb

После чего ПО запустится и будет готово к работе.