УТВЕРЖДЕН
643.СПЕТ.21092-01 97 01-ЛУ

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АГЕНТ СЕРВЕРА БЕЗОПАСНОСТИ»

Описание функциональных характеристик

643.СПЕТ.21092-01 97 01

Листов 11

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

2025

АННОТАЦИЯ

Документ содержит сведения о функциональных характеристиках специального программного обеспечения «Агент сервера безопасности».

Документ предназначен для пользователей программного обеспечения и сотрудников организации-разработчика.

Документ разработан с учетом основных положений следующих нормативных документов:

– ГОСТ 19.105–78 «Единая система программной документации. Общие требования к программным документам»;

– ГОСТ Р ИСО/МЭК 9126–93 «Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению».

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование программы

Полное наименование программы: «Агент сервера безопасности».

В рамках настоящего документа употребляется также обозначение «СПО».

Обозначение программы: 643.СПЕТ.21092-01.

1.2. Основные сведения

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

Сайт организации-разработчика: https://inseq.ru/.

Организация-правообладатель: Акционерное общество «ИНСЕК» (АО «ИНСЕК»).

Сведения о СПО не составляют государственную тайну. СПО не содержит сведения, составляющие государственную тайну. СПО может обрабатывать сведения, составляющие государственную тайну, имеющие степень секретности не выше «Совершенно секретно».

СПО не имеет принудительного обновления и управления из-за рубежа.

Лицензии используемых компонентов позволяют получить исключительные права на СПО.

СПО относится к классу 02.08 «Средства мониторинга и управления» по Классификатору программ для электронных вычислительных машин и баз данных в соответствии с приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 22.09.2020 № 486.

СПО «Агент сервера безопасности» представляет собой клиент-серверное решение на основе общей базы данных и состоит из следующих компонентов:

- модуль агента сервера безопасности (далее – МАСБ);
- модуль управления агентом сервера безопасности (далее – МУ АСБ);
- база данных СПО АСБ (далее – БД АСБ);
- модуль управления БД АСБ (далее – МУ БД АСБ);
- модуль комплексного отображения событий безопасности (далее – МКОСБ).

1.3. Назначение программы

1.3.1. 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.

1.3.2. Эксплуатационное назначение

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

1.4. Особенности применения

Эксплуатация выполняется конечными пользователями, которые должны обладать следующими знаниями и навыками:

– навыки работы на персональном компьютере;

– навыки работы с командной оболочкой ОС Linux;

– навыки работы с консольными приложениями.

2. ПЕРЕЧЕНЬ РЕАЛИЗУЕМЫХ ФУНКЦИЙ

СПО АСБ 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.

3. ОПИСАНИЕ ХАРАКТЕРИСТИК

3.1. Общие характеристики

3.1.1. 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 СПО.

3.1.2. 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).

3.1.3. Соответствие стандартам

СПО разрабатывается с применением ключевых принципов безопасной разработки программного обеспечения, с учетом положений ГОСТ 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Оценка разрабатываемой программной продукции осуществляется с учетом положений ГОСТ Р ИСО/МЭК 9126–93 «Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению».

Разработка и сопровождение СПО в рамках его жизненного цикла осуществляется с учетом положений документа ГОСТ Р ИСО/МЭК 12207–2010 «Системная и программная инженерия. Процессы жизненного цикла программных средств».

3.1.4. Средства разработки

Основные компоненты СПО АСБ разработаны на языке программирования C++ с использованием следующих инструментов и библиотек:

- Компилятор Clang (версия 6.0.0-3, лицензия University of Illinois/NCSA Open Source License, ссылка на компонент: releases.llvm.org/6.0.0/tools/clang/docs/ReleaseNotes.html);
- Компилятор GCC (версия 6.3, лицензия GNU General Public License version 3, ссылка на компонент: gcc.gnu.org/gcc-6/);
- Инструмент отладки GDB (версия 7.12, лицензия GNU General Public License, ссылка на компонент: ftp.gnu.org/gnu/gdb/);
- Фреймворк Qt (версия 5.11, лицензия GNU Lesser General Public License version 3, ссылка на компонент: wiki.qt.io/Qt_5.11_Release).

Компонент интеграции с БД «Ребус-СОВ» разработан на языке Python. Для хранения и управления данными использовалась СУБД PostgreSQL (версия 9.6, лицензия PostgreSQL License, ссылка на компонент: www.postgresql.org/docs/9.6/).

3.2. Функциональные характеристики

3.2.1. Режим функционирования

СПО «Агент сервера безопасности» функционирует на локальном вычислительном оборудовании организации-заказчика.

МАСБ из состава СПО АСБ является системной службой (*ssa-client*) операционной системы и запускается автоматически при старте операционной системы.

МУ АСБ из состава СПО АСБ запускается двойным кликом по ярлыку «АСБ» в главном меню СПО АСБ.

МУ БД АСБ из состава СПО АСБ является консольной утилитой и запускается путем выполнения команды:

ssa-control --<option>

Полное описание поддерживаемых опций представлено в Руководстве администратора СПО АСБ.

МКОСБ из состава СПО АСБ запускается двойным кликом по ярлыку «Модуль управления АСБ» на рабочем столе.

3.2.2. Пользователи и роли

СПО не реализует собственную систему аутентификации пользователей. Ролевая модель предполагает одну роль – «Пользователь».

3.2.3. Сетевое взаимодействие

Сетевое взаимодействие клиентской и серверной частей ПО осуществляется в рамках локальной сети.

3.2.4. Сбор и хранение данных

СПО не осуществляет сбор и передачу данных о пользователях во внешние сети. Хранению подлежат следующие данные (Таблица 1):

Таблица 1 – Перечень таблиц служебной базы данных и их назначение

Наименование таблицы	Назначение
agent	Информация об АСБ
alert	Информация о событиях безопасности
control	Данные о выполненных операциях контроля
event	Описание событий
hardware	Данные об АПМДЗ
metrics_config	Данные об отслеживаемых СЗИ
rule	Данные о правилах
services	Информация об отслеживаемых сервисах

Наименование таблицы	Назначение
services_template	Информация о шаблонах отслеживания СЗИ
settings	Информация о настройках МУ БД АСБ

Логи работы СПО хранятся в файловой системе. Для хранения служебной информации используется база данных PostgreSQL (версия 9.6), которая входит в состав СПО и разворачивается автоматически при его установке.

3.3. Прочие характеристики качества программного обеспечения

3.3.1. Надежность

СПО разработано с использованием современных технологий, модульной архитектуры, распространенного языка программирования и ориентировано на длительный срок эксплуатации.

СПО ориентировано на работу в режиме сеансов, начинаемых и останавливаемых сообразно потребностям пользователя.

Надежность СПО обеспечивается реализацией необходимых процедур контроля качества при разработке, в том числе проведение тестирования.

3.3.2. Расширяемость

СПО построено с применением принципов модульной открытой архитектуры и позволяет расширять перечень реализуемых функций путем добавления новых сервисов.

3.3.3. Защищенность

СПО разрабатывается с применением ключевых принципов безопасной разработки программного обеспечения.

СПО поддерживает механизмы защиты, предоставляемые операционной системой.

3.3.4. Эргономичность

СПО содержит интуитивно понятный веб-интерфейс на русском языке.

3.3.5. Сопровождаемость

Эксплуатация ПО не требует специальных знаний от пользователей, кроме общих навыков работы с серверным оборудованием под управлением ОС Linux, а также знаний функциональных возможностей ПО в рамках эксплуатационной документации.

Сопровождение эксплуатации СПО выполняется силами службы технической поддержки организации-разработчика посредством регистрации и обработки обращений пользователей.

Обратиться в службу технической поддержки организации-разработчика можно по электронной почте mail@inseq.ru.

Режим работы службы технической поддержки организации-разработчика: по будням с 10:00 до 19:00 (по московскому времени).