УТВЕРЖДЕН

643.СПЕТ.21092-01 96 01-ЛУ

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АГЕНТ СЕРВЕРА БЕЗОПАСНОСТИ»

Руководство пользователя

643.СПЕТ.21092-01 96 01

Листов 17

2025

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

АННОТАЦИЯ

Настоящий документ является руководством пользователя (далее – Руководство) для специального программного обеспечения «Агент сервера безопасности».

Руководство содержит общие сведения о программном обеспечении, его характеристиках, а также порядке выполнения различных операций при эксплуатации программного обеспечения.

Руководство разработано с учетом основных положений ГОСТ 19.505–79 «Единая система программной документации. Руководство оператора. Требования к содержанию и оформлению».

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование

Полное наименование программы: «Агент сервера безопасности».

В рамках настоящего документа употребляется также обозначение «СПО».

Обозначение: 643.СПЕТ.21092-01.

«Агент сервера безопасности» – российское специальное программное обеспечение, организация-разработчик: Акционерное общество «ИНСЕК» (АО «ИНСЕК»).

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

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

1.2. Назначение программы

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 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.

1.4. Состав ПО

СПО АСБ 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.

2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1. Аппаратные требования

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. Требования к программным средствам

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): PostrgeSQL (версия 9.6).

для функционирования МКОСБ:

- операционная система Astra Linux Special Edition РУСБ.10015-01 (версия 1.6 «Смоленск» и выше;

СУБД: PostrgeSQL (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 И ПОДГОТОВКА К РАБОТЕ

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.

4. ВЫПОЛНЕНИЕ ПРОГРАММЫ

4.1. Запуск программы

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.

4.2. Работа с ПО

4.2.1. Общее описание интерфейса

После запуска МКОСБ открывается основное окно СПО АСБ, представленное на рисунке 1, со следующими элементами:

– главное меню: предназначено для навигации по программе;

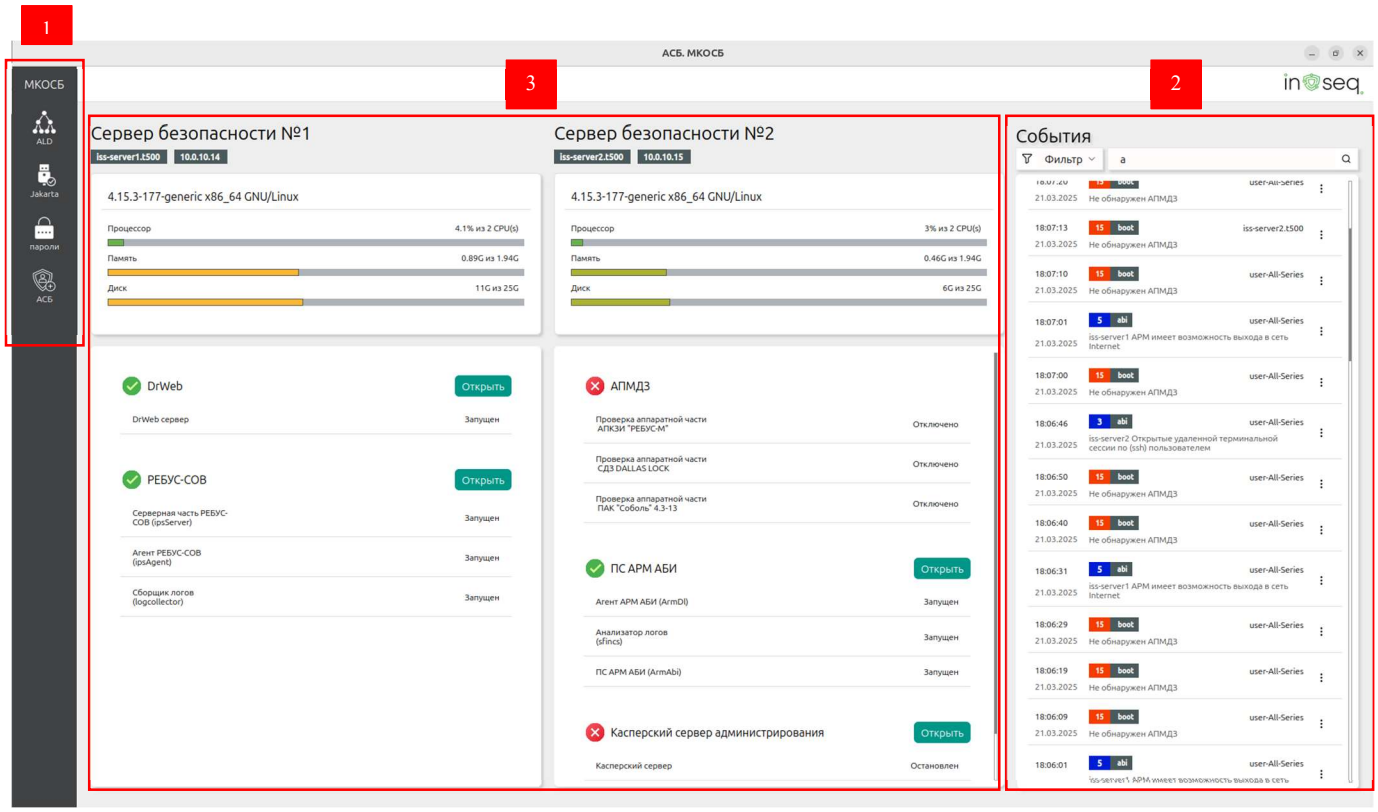
– панель для отображения событий: предназначена для навигации по МАСБ, установленным на контролируемых АРМ;

– содержание вкладки: предназначено для отображения информации соответствующей вкладки, выбранной на панели главного меню.

В левой части окна располагается главное меню программы, которое служит для навигации по следующим разделам программы:

– раздел «ALD», «Jakarta», «Пароли»;

– раздел «АСБ» – предназначен для перехода в МУ АСБ.



1 – главное меню; 2 – панель для отображения событий; 3 – содержание вкладки

Рисунок 1 – Общий интерфейс СПО АСБ

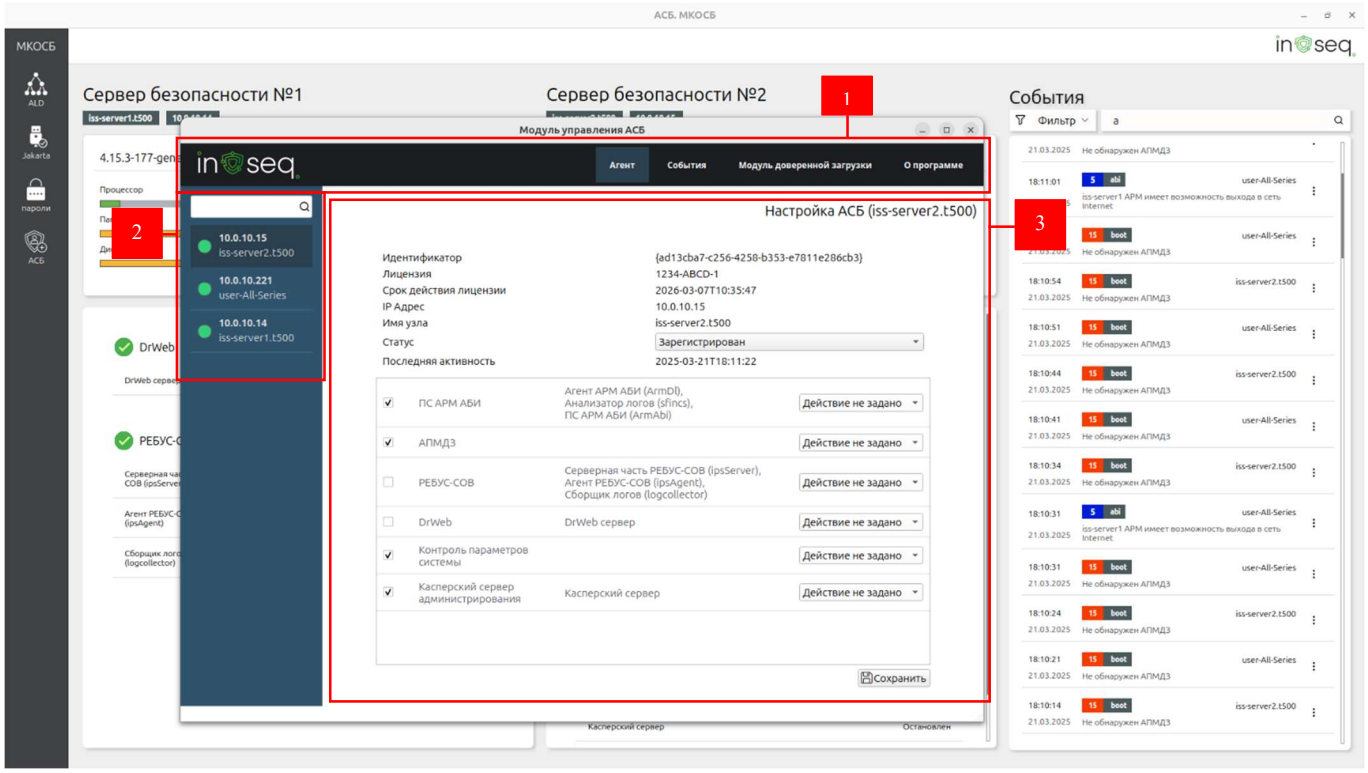
4.2.2. Общее описание интерфейса МУ АСБ

После запуска МУ АСБ открывается окно СПО АСБ, представленное на рисунке 2, со следующими элементами:

– главное меню – предназначено для навигации по программе;

– панель навигации по агентам – предназначена для навигации по МАСБ, которые установлены на контролируемых АРМ;

– содержание вкладки – предназначено для отображения информации соответствующей вкладки, выбранной на панели главного меню.



1 – главное меню; 2 – панель навигации по агентам; 3 – содержание вкладки

Рисунок 2 – Интерфейс СПО АСБ

В верхней части окна располагается главное меню программы, которое служит для навигации по следующим разделам программы:

– раздел «Агент» – предназначен для отображения данных и настройки АСБ;

– раздел «События» – предназначен для отображения журнала событий;

– раздел «Модуль доверенной загрузки» – предназначен для отображения информации об АПМДЗ;

– раздел «О программе» – предназначен для отображения данных о программе.

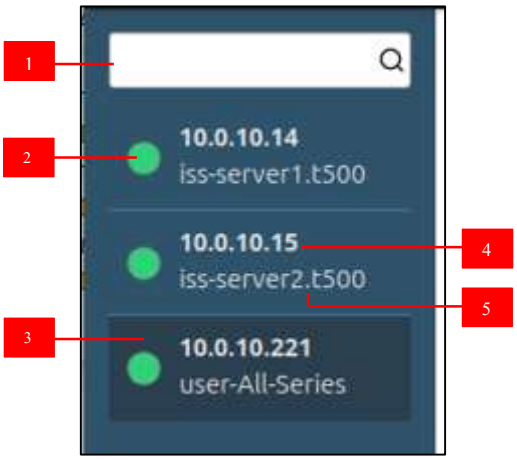
В левой части окна располагается панель навигации по агентам, которая служит для навигации по МАСБ, расположенным на контролируемых устройствах. Панель навигации по агентам содержит следующие элементы, представленные на рисунке 3:

– поле поиска по агентам: предназначено для быстрого поиска агента в списке;

– индикатор активности агента: предназначен для отображения информации о состоянии агента (зеленый цвет – агент активен, красный цвет – агент находится в неактивном состоянии);

– выделение цветом выбранного агента, для которого будет отображаться информация в области «содержание вкладки»;

– IP-адрес агента и доменное имя: предназначены для идентификации агента в сети.



1 – поисковая строка для поиска по агентам; 2 – индикатор активности агента; 3 – выбранный агент; 4 – IP-адрес агента; 5 – доменное имя

Рисунок 3 – Панель навигации по агентам

Раздел «События» из главного меню программы представлен на рисунке 4.

Для перехода в раздел «События» необходимо выбрать соответствующий пункт в главном меню программы, после чего в области «Содержание вкладки» отобразится информация о событиях в МАСБ, которая содержит «Журнал событий».

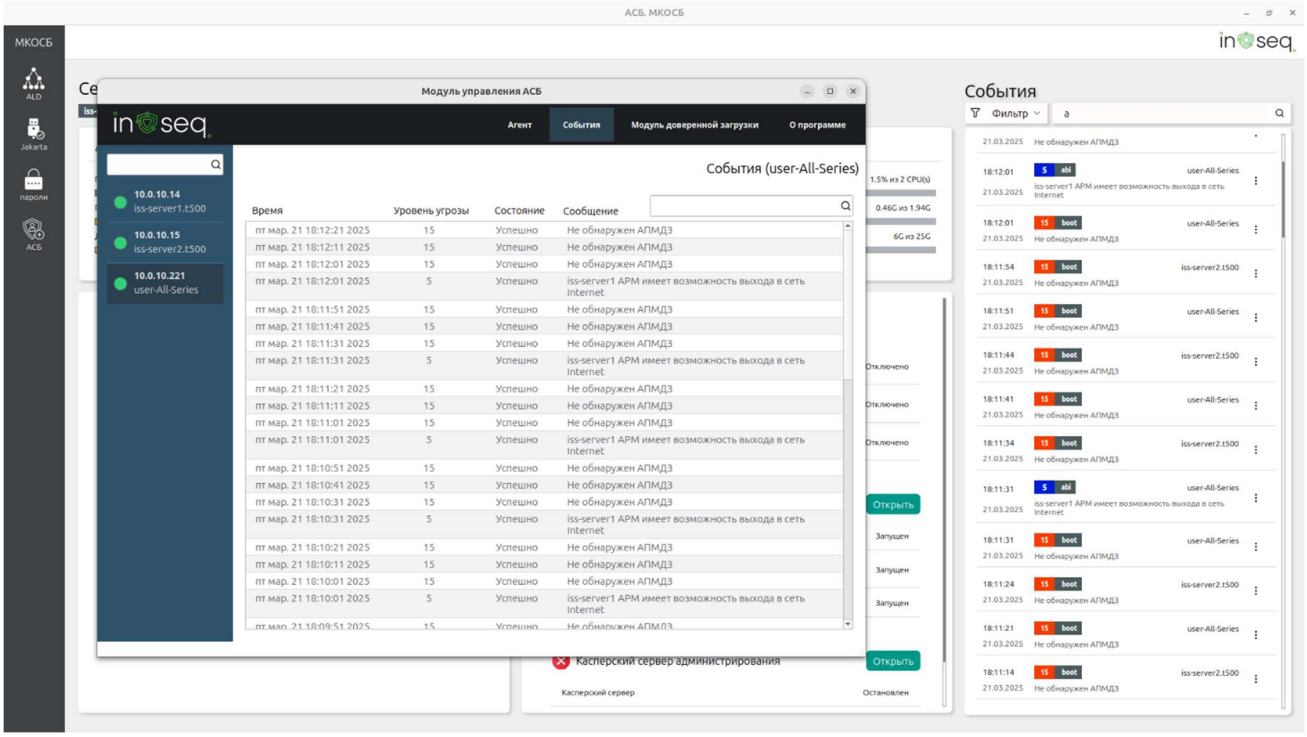


Рисунок 4 – Раздел «События» МУ АСБ

4.2.3. Раздел «Модуль доверенной загрузки»

Для перехода в раздел «Модуль доверенной загрузки», представленный на рисунке 5, необходимо выбрать соответствующий пункт в главном меню программы, после чего в области «Содержание вкладки» отобразится информация об АПМДЗ.

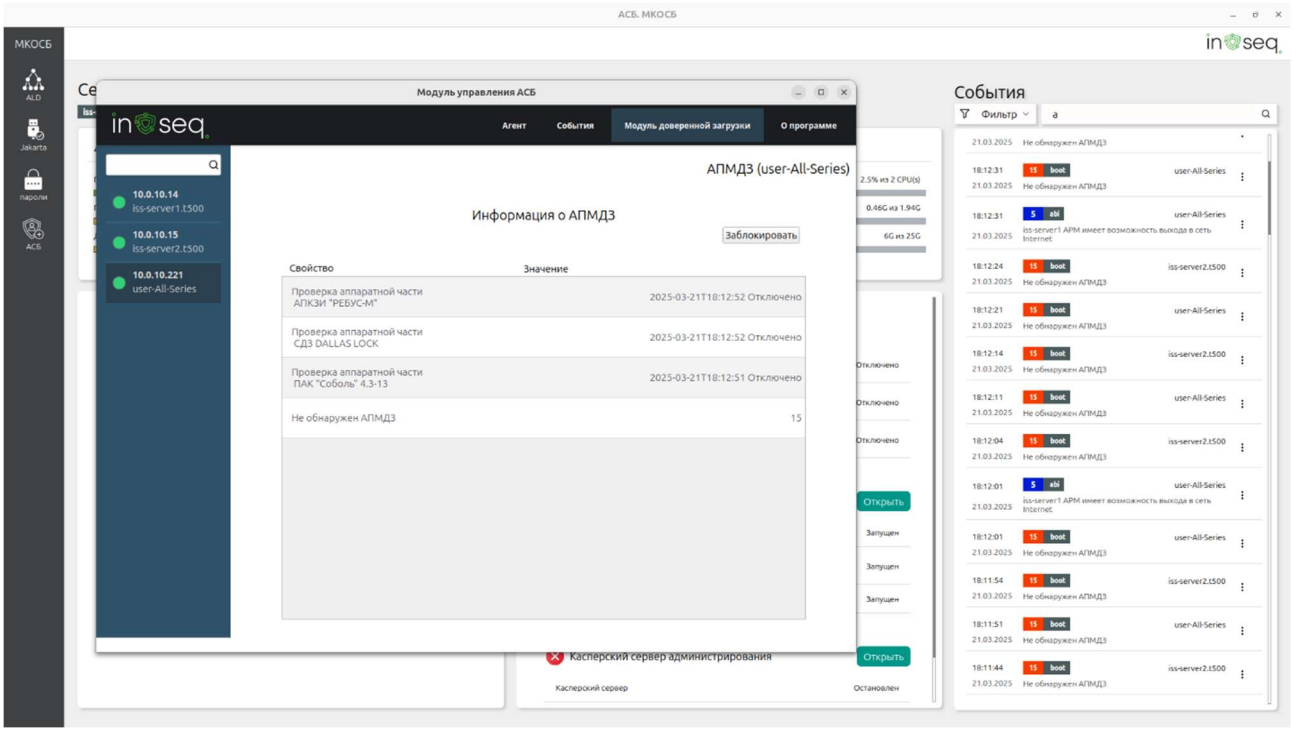


Рисунок 5 – Раздел «Модуль доверенной загрузки»

В разделе располагается журнал событий агента, содержащий следующие элементы:

– свойство: название параметра АПМДЗ;

– значение свойства: значение параметра АПМДЗ;

– кнопка «заблокировать»: предназначена для блокировки пользователей через *umode -l.*

4.2.4. Раздел «О программе»

Для перехода в раздел «О программе», представленный на рисунке 6, необходимо выбрать соответствующий пункт в главном меню программы, после чего в области «Содержание вкладки» отобразится информация о программе, где указана информация об организации-разработчике и годе разработки СПО.

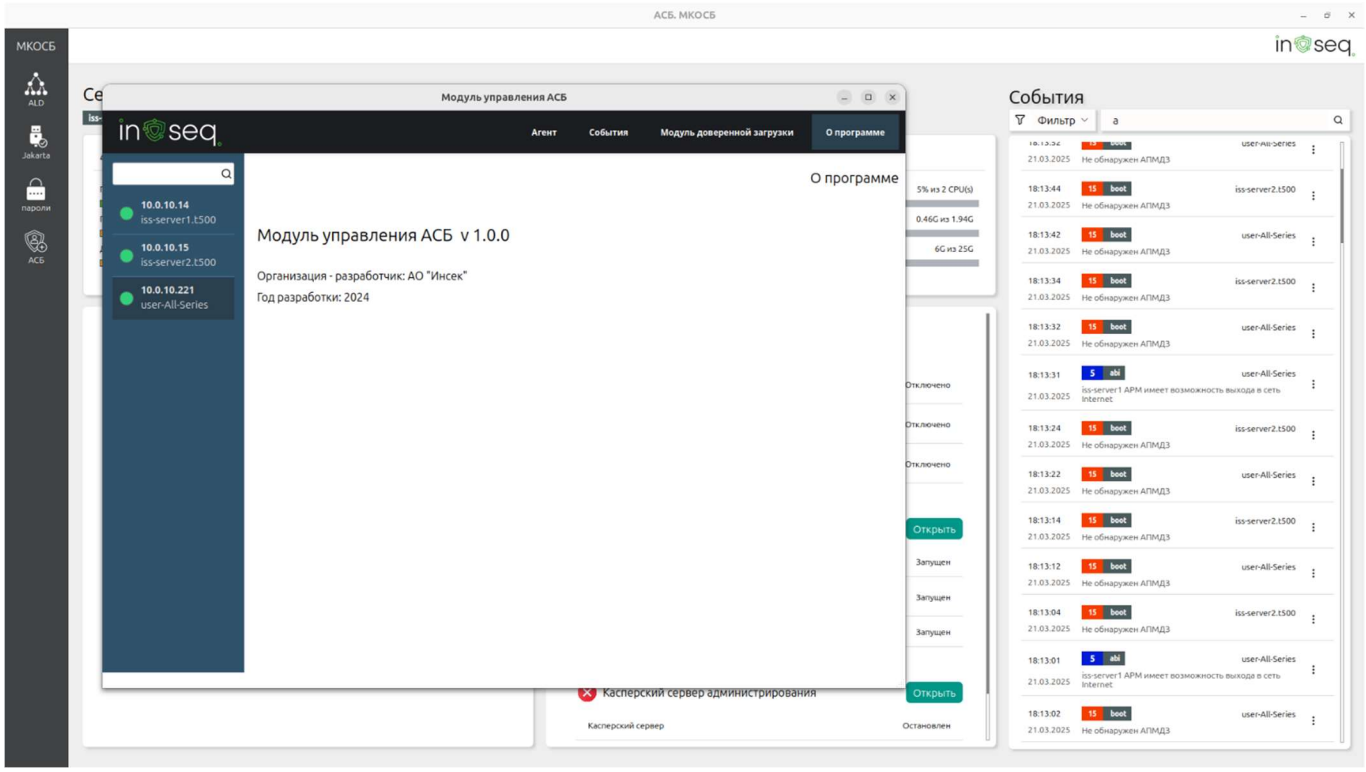


Рисунок 6 – Раздел «О программе»

4.3. Завершение работы с ПО

Для завершения работы МУ АСБ необходимо нажать кнопку закрытия в правом верхнем углу основного окна программы.

5. СООБЩЕНИЯ ОПЕРАТОРУ

В процессе эксплуатации СПО АСБ информация о работе АПМДЗ выводится в разделе программы «Модуль доверенной загрузки» в виде списка.

Сообщения о событиях, связанных с работой контролируемого АРМ выводятся в разделе программы «События» в виде списка.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ОС	Операционная система
ПО	Программное обеспечение