|  |
| --- |
| Значок НИТА |
| ООО «Фирма «НИТА» |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| СПЕЦИАЛЬНОЕ (ПРИКЛАДНОЕ) ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ «СФЕРА»  Руководство оператора  НКПГ.10302 |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Санкт-Петербург  2021 |

Содержание

[1 Общие сведения 4](#_Toc87887105)

[1.1 Назначение средств защиты информации 4](#_Toc87887106)

[1.2 Состав средств защиты информации 4](#_Toc87887107)

[1.3 Принцип действия средств защиты информации 5](#_Toc87887108)

[2 Пользовательский интерфейс 6](#_Toc87887109)

[2.1 Главное окно, монитор диагностики СЗИ (АРМ АБИ) 6](#_Toc87887110)

[2.2 Регистрация пользователя 7](#_Toc87887111)

[2.3 Настройка подсистемы контроля целостности файлов 8](#_Toc87887112)

[2.4 Настройка подсистемы контроля целостности сети 9](#_Toc87887113)

[2.5 Окно «О программе» 11](#_Toc87887114)

Настоящее руководство оператора описывает основные правила работы со специальным (прикладным) программным обеспечением комплекса средств защиты информации «Сфера» (НКПГ.10302).

Полное руководство по эксплуатации поставляется в составе эксплуатационной документации вместе с поставляемым изделием на объект установки КСЗИ «Сфера».

# Общие сведения

## Назначение средств защиты информации

Специальное (прикладное) программное обеспечение выполняет функции по исключению несанкционированного доступа к информации, хранимой и обрабатываемой в системах и комплексах, например КСА УВД, КСА ПИВП, КДВИ, СКРС и СЕВ.

В состав СПО входит комплекс программ и компонент, обеспечивающих выполнение задач по назначению:

* программные средства подсистемы контроля доступом;
* программные средства подсистемы регистрации и учета;
* программные средства подсистемы обеспечения целостности;
* комплекс программ администратора безопасности информации (АБИ).

КСЗИ обеспечивает:

* управление доступом пользователей к конфиденциальной информации;
* оперативный контроль работы пользователей компьютера путем регистрации событий, связанных с безопасностью;
* средства просмотра и представления зарегистрированной информации на месте инженера (администратора безопасности);
* печать данных из журнала средств защиты информации (СЗИ);
* контроль целостности программ, защищаемых СЗИ;
* контроль целостности ЛВС.

Защите подлежит следующая информация:

* информационные ресурсы, содержащие сведения ограниченного доступа, общее, специальное и функциональное программное обеспечение, доступ к которым должен быть ограничен;
* основные технические средства, используемые для обработки, хранения и передачи служебной информации.

На всех рабочих местах комплекса постоянно запущены средства защиты информации, которые контролируют вторжения и регистрируют их на АРМ сменного инженера (администратора безопасности). КСЗИ обеспечивает управление доступом, регистрацию и учет, обеспечение целостности информации.

## Состав средств защиты информации

КСЗИ «Сфера» включает в себя следующие подсистемы:

* Подсистема контроля целостности сети;
* Подсистема контроля целостности файлов;
* Подсистема управления и настройки;
* Подсистема передачи данных;
* Подсистема печати;
* Подсистема работы с защищаемой информацией.

## Принцип действия средств защиты информации

Система защиты представляет собой набор программ и библиотек, которые автоматически запускаются или используются на защищаемом компьютере при его включении, и функционируют на протяжении всего времени работы компьютера.

В процессе работы КСЗИ выполняет следующие функции:

* обеспечивает обмен данными между компонентами системы и обработку команд, поступающих от этих компонент;
* обеспечивает доступ других компонент системы к информации, хранящейся в базе данных системы защиты;
* осуществляет сбор сведений о состоянии компьютера;
* контролирует доступ пользователя к ресурсам компьютера.

Подсистема управления и настройки предназначена для настройки компонентов СЗИ. Данный компонент системы настраивается поставщиком изделия при развертывании. В дальнейшем изменение конфигурации доступно администратору АБИ.

Подсистема контроля целостности файлов осуществляет слежение за неизменностью контролируемых объектов с целью защиты их от модификации. Для этого определяется перечень контролируемых объектов. Для каждого из входящих в него объектов рассчитываются эталонные значения контролируемых параметров. Эталонные значения для проверяемых объектов, а также информация о размещении объектов хранятся в файлах конфигурации КСЗИ «Сфера».

При загрузке компьютера подсистема контроля целостности файлов проверяет целостность контролируемых файлов. Если целостность файлов не нарушена, подсистема контроля целостности передает управление подсистеме идентификации пользователя. В случае нарушения целостности файлов на АРМ АБИ отображается соответствующая сигнализация, при этом работоспособность остального ПО не останавливается, и доступ пользователя к АРМ не запрещается.

Подсистема контроля целостности сети осуществляет слежение за неизменностью сетевой конфигурации. Перечень разрешенных адресов системы (IP и MAC адресов в вычислительной сети) поступает в подсистему контроля целостности сети от АРМ АБИ. Фильтр доступных адресов создается при установке СЗИ и передается на все защищаемые РМ в сервис подсистемы контроля целостности сети. Перечень разрешенных адресов системы хранится в файлах конфигурации КСЗИ «Сфера».

Подсистема передачи данных предназначена для осуществления передачи данных о действиях, связанных с объектами СЗИ, на монитор АБИ. Подсистема передает на монитор АБИ общее состояние компонентов СЗИ, работающих на защищаемых РМ, и информацию о событиях, которые сгенерировали средства СЗИ.

# Пользовательский интерфейс

## Главное окно, монитор диагностики СЗИ (АРМ АБИ)

Для доступа к монитору диагностики СЗИ необходимо зарегистрироваться в окне регистрации пользователя (Рисунок 1). Для регистрации необходимо ввести имя пользователя «АдминГранит», пароль «1234567».

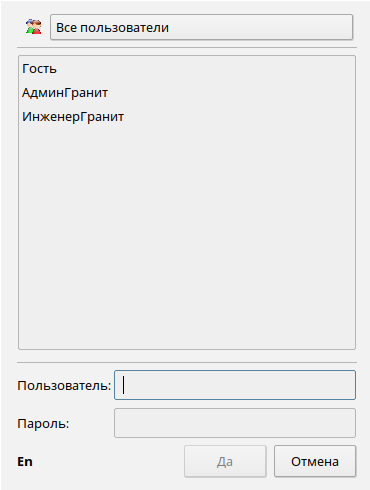


Рисунок 1 – Регистрация пользователя

Вся информация о состоянии СЗИ отображается в главном окне (Рисунок 2) – мониторе диагностики СЗИ. В этом окне информация о защищаемой системе группируется по объектам, которые отображаются в виде пиктограмм. Текущее состояние диагностируемого объекта отображается цветом пиктограммы:

* зеленый – нормальная работа;
* желтый – предупреждение;
* красный – отказ, вторжение, нарушена целостность файлов.

При выборе объекта на карте монитора диагностики СЗИ в нижней части окна отображаются его составные компоненты. Например, на рисунке ниже выбран объект «АВI», для выбранного объекта в нижней части окна отображаются входящие в его состав компоненты СЗИ: контроль целостности файлов, контроль целостности сети и агент СЗИ.

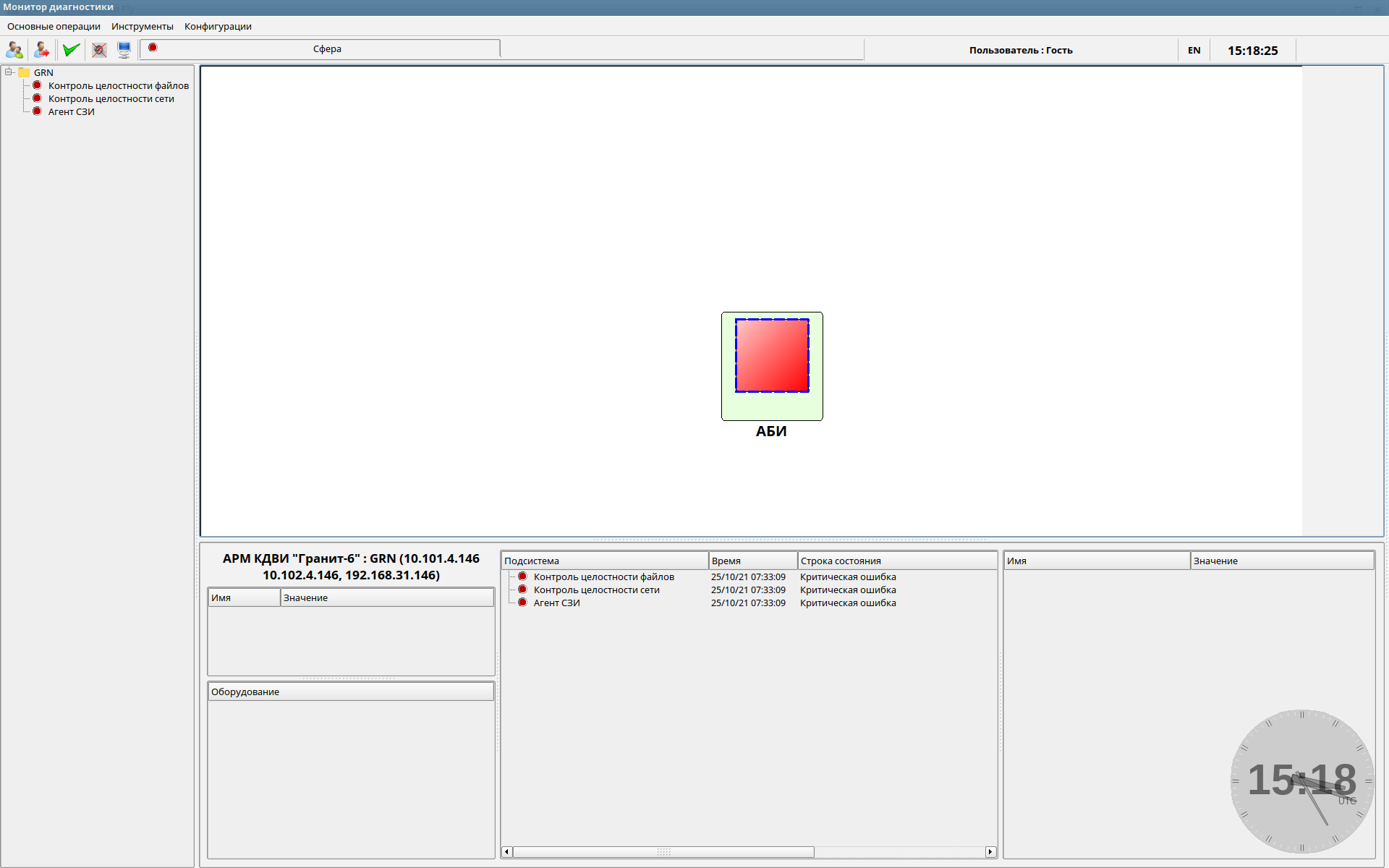


Рисунок 2 – Общий вид главного окна монитора диагностики СЗИ

В главном окне монитора диагностики СЗИ оператору предоставляется возможность:

* просмотреть журнал событий о действиях, связанных с объектами защищаемой системы;
* просмотреть текущее состояние объектов СЗИ;
* выполнить настройку следующих подсистем:

1. подсистемы целостности файлов;
2. подсистемы целостности сети.

## Регистрация пользователя

Смена пользователя выполняется в окне регистрации пользователя (Рисунок 3).

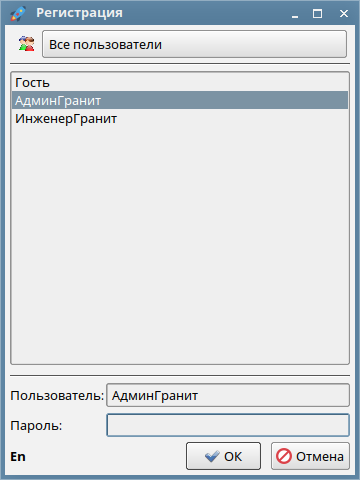


Рисунок 3 – Окно регистрации пользователя

Для вызова окна регистрации пользователя необходимо нажать на кнопку  на панели инструментов в основном окне монитора диагностики СЗИ. Для регистрации пользователя выбрать в списке пользователей имя, ввести пароль и нажать кнопку «OK».

## Настройка подсистемы контроля целостности файлов

Настройка подсистемы контроля целостности файлов выполняется в окне «Контроль целостности файлов» (Рисунок 4).

Для вызова этого окна необходимо выполнить следующие действия:

1. На карте монитора диагностики СЗИ выбрать объект.

2. В панелях дополнительной информации выбрать службу «Контроль целостности файлов». Вызвать контекстное меню нажатием ПКМ.

3. Выбрать пункт меню «Настройки».

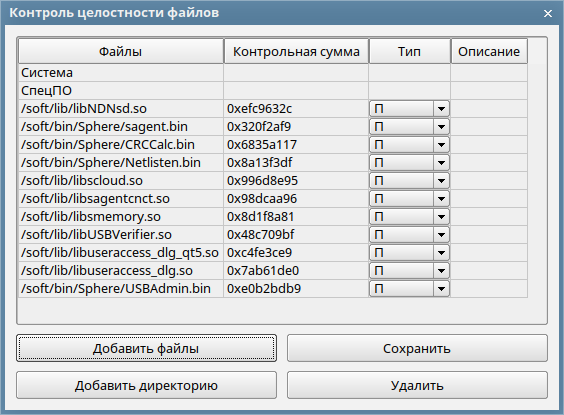


Рисунок 4 – Окно «Контроль целостности файлов»

Все контролируемые файлы в этом окне разбиты на две части:

* «Система» – это файлы, которые принадлежат ОС;
* «СпецПО» – это файлы, которые не входят в состав ОС.

Описание параметров файлов представлено в таблице (Таблица 1).

Таблица 1 – Информация в окне целостности файлов

|  |  |
| --- | --- |
| Наименование | Назначение |
| Файлы | Описание местоположения контролируемого объекта с указанием тома, каталога, имени файла. |
| Контрольная сумма | Результат расчета алгоритмом контрольной суммы данного объекта. |
| Тип | Указывается тип контроля файла: периодический (П) или при старте (С). При первом типе контроль целостности выполняется периодически с заданным интервалом. Во втором – проверка объекта производится только при старте системы. |
| Описание | Назначение контролируемого объекта. |

Для выполнения операций по редактированию (создание, удаление, сохранение) списка контролируемых файлов используются кнопки, расположенные в нижней части окна.

## Настройка подсистемы контроля целостности сети

Настройка подсистемы контроля целостности сети выполняется в окне «Служба контроля целостности сети» (Рисунок 5). Данное окно вызывается из контекстного меню службы «Контроль целостности сети».

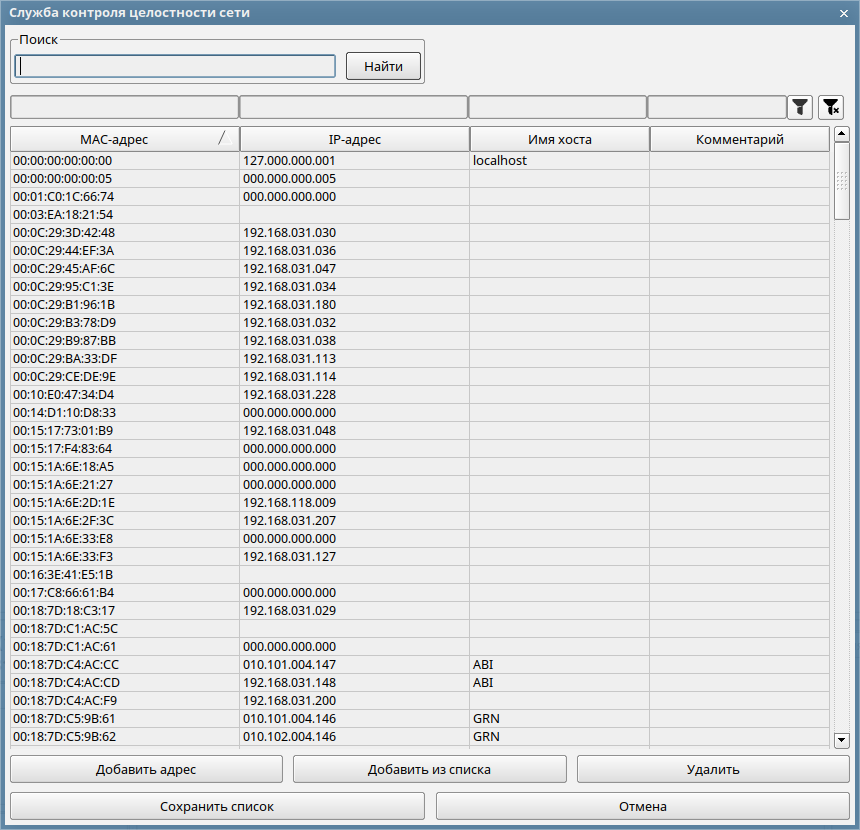


Рисунок 5 – Окно настройки службы контроля целостности сети

В данном окне доступна фильтрация по MAC-адресам, IP-адресам и именам хоста (Рисунок 7).

Для включения фильтров необходимо нажать на кнопку .

Для сбрасывания фильтров необходимо нажать на кнопку .

Также в окне настроек доступен общий поиск по тексту. Для осуществления поиска необходимо ввести текст, по которому будет производиться поиск, в поле и нажать на кнопку «Найти» (Рисунок 6).



Рисунок 6 – Текстовое поле с поиском

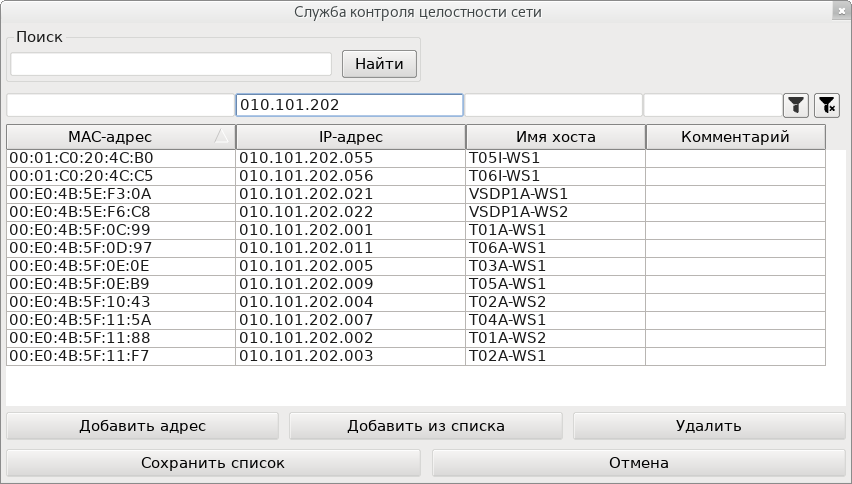


Рисунок 7 – Фильтрация в окне настройки

Информация в этом окне представлена в табличном виде. В таблице (Таблица 2) представлено описание колонок.

Таблица 2 – Информация в окне сервиса прослушивания сети

|  |  |
| --- | --- |
| Наименование | Назначение |
| IP адрес | IP адрес объектов, разрешенных для защищаемой АС, (для IP v4, это четыре числа от 0-255, на которые наложены некоторые ограничения). В случае, если на разрешенном объекте контроля отсутствует семейство протоколов TCP/IP, значение выставляется в 0. |
| MAC адрес | MAC адрес объектов, разрешенных для защищаемой автоматизированной системы (шесть чисел от 0-255). Представляется в шестнадцатеричной системе исчисления. |

Для выполнения операций по редактированию (добавление, создание, удаление, сохранение) списка контролируемых сетевых адресов используются кнопки, расположенные в нижней части окна.

## Окно «О программе»

В окне «О программе» указывается Правообладатель специального (прикладного) программного обеспечения комплекса средств защиты информации «Сфера» (НКПГ.10302).

Для открытия окна «О программе» необходимо нажать на кнопку  в правом верхнем углу на экране регистрации (Рисунок 8).



Рисунок 8 – Окно «О программе»