

УТВЕРЖДЕН

РДПИ.00888-04 91 01 - ЛУ

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

**ОБЩЕСИСТЕМНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**

**«Веста-В»**

**Руководство администратора**

**РДПИ.00888-04 91 01**

**(CD-R)**

**Страниц 33**

2021

Решение от 17.01.2022

Литера О О<sub>1</sub>



## АННОТАЦИЯ

Настоящий документ является руководством администратора общесистемного программного обеспечения «Веста-В» (далее по тексту ОСПО «Веста-В»), функционирующее под ОС Windows.

В документе приведены сведения об операциях по обеспечению порядка работы ОСПО «Веста-В», его настройке и отладке.

Документ состоит из восьми разделов.

В первом разделе приводятся сведения о назначении ОСПО, функциональных возможностях его компонентов.

Во втором разделе приводятся сведения о программных и технических средствах, необходимых для работы ОСПО.

В третьем разделе определен порядок действий должностного лица по настройке окружения, установке и удалению ОСПО.

В четвёртом разделе описана настройка доступа пользователя.

В пятом и шестом разделах описана работа с дополнительными утилитами для проверки правильности настроек мандатных прав и настройки сетевых маршрутов на ПЭВМ в случае необходимости.

В седьмом разделе описаны механизмы поиска причин сбоя в ходе работы ОСПО.

В восьмом разделе приводятся сведения и порядок работы с пакетом технологических процедур.

## СОДЕРЖАНИЕ

1. Назначение и функциональные возможности ОСПО.....	5
1.1. Состав и функции ОСПО.....	5
1.2. Функциональные возможности.....	5
2. Системные требования.....	7
2.1 Требования к аппаратному обеспечению.....	7
3. Установка и удаление ОСПО.....	8
3.1. Установка.....	8
3.2. Удаление.....	9
4. Настройка и проверка мандатного и дискреционного доступа.....	11
4.1. Настройка доступа.....	11
5. Утилита проверки доступа checkAccess.....	14
5.1. Общие сведения.....	14
5.2. Проверка доступа.....	14
6. Редактор сетевых маршрутов routeEditor.....	16
6.1. Общие сведения.....	16
6.2. Работа с программой routeEditor.....	16
7. Отладка ОСПО.....	18
7.1. Общие сведения.....	18
7.2. Уровни логирования.....	18
7.3. Экспорт логов.....	21
8. Детальная настройка.....	22
9. Проверка контрольной суммы ОСПО.....	31
Перечень сокращений.....	32

## 1. НАЗНАЧЕНИЕ И ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ОСПО

### 1.1. Состав и функции ОСПО

ОСПО «Веста-В» предназначено для организации автоматизированного обмена закрытыми данными, в том числе данными, содержащими сведения, составляющие государственную тайну до уровня совершенно секретно включительно, между типовыми (аналогичными) АРМ по IP-сетям, общегосударственным телефонным линиям связи и выделенным каналам связи с использованием специальных средств защиты информации от несанкционированного доступа.

### 1.2. Функциональные возможности

ОСПО «Веста-В» обеспечивает:

- отправку и прием сообщений, содержащих данные определенной категории секретности (открытые данные; конфиденциальные данные; данные содержащие сведения, составляющие государственную тайну до уровня совершенно секретно включительно), заголовок, текст сообщения, прикрепленные к сообщению файлы различных форматов и крайний срок доставки;
- отправку групповых сообщений;
- транзитную передачу сообщений;
- параллельную отправку сообщений нескольким получателям;
- отправку сообщений абоненту в соответствии с заданным пользователем приоритетом, соответствующим внутреннему алгоритму отправки сообщений;
- отправку и прием сообщений по различным каналам связи (IP-сети, общегосударственные телефонные линии связи и выделенные каналы связи);
- ведение журналов регистрации входящих, исходящих и транзитных сообщений, действий пользователя и статистики исходящих, входящих и транзитных сообщений ОСПО;

- автоматический контроль над сроками доведения отправленного сообщения в соответствии с крайним сроком доставки;
- отслеживание состояний созданных сообщений;
- автоматическое сжатие информации при создании сообщения;
- автоматическую досылку информации в случае прерывания передачи данных;
- сохранение и восстановление конфигурации ОСПО;
- звуковое уведомление при получении новых сообщений;
- отображение текущего состояния транспортной подсистемы и доступности абонентов;
- проверку доступа к файловой системе;
- редактирование таблицы маршрутизации операционной системы;
- совместную работу с СЗИ от НСД (ОСПО распределяет работу с сообщениями и журналами по различным каталогам в зависимости от их уровня секретности, что позволяет организовать совместную работу с большинством СЗИ от НСД).

## 2. СИСТЕМНЫЕ ТРЕБОВАНИЯ

### 2.1. Требования к аппаратному обеспечению

Для работы ОСПО «Веста-В» необходима ПЭВМ (с установленной операционной системой Microsoft Windows 10) с техническими характеристиками:

- 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой не менее 1.2 ГГц с поддержкой PAE, NX и SSE2;
- 4 ГБ (для 32-разрядного процессора) или 8 ГБ (для 64-разрядного процессора) ОЗУ;
- графическое устройство с поддержкой DirectX 9 и драйвера WDDM 1.0 или более поздней версии;
- ПЗУ – объемом не менее 120 Гбайт;
- сетевая карта со скоростью передачи данных не менее 100 Мбит/с;
- CD-ROM;
- COM-порт (RS-232) - для передачи данных по коммутируемому или выделенному каналу связи;
- средство защиты информации от несанкционированного доступа;
- операционная среда функционирования - Microsoft Windows 10.

Установка (инсталляция) и эксплуатация ОСПО «Веста-В» на объекте эксплуатации должна осуществляться в соответствии с требованиями руководства оператора РДПИ.00888-04 34 01 и руководства администратора РДПИ.00888-04 91 01, входящих в комплект поставки.

### 3. УСТАНОВКА И УДАЛЕНИЕ ОСПО

#### 3.1. Установка

Для установки ОСПО «Веста-В» в операционной системе Windows необходимо произвести запуск установочного пакета с правами администратора.

В окне установки необходимо ознакомиться с лицензионным соглашением, принять его условия, выбрать каталог для установки и запустить процесс установки.

Установка должна производиться под администратором безопасности.

В случае установки новой версии ОСПО взамен старой необходимо удалить старую версию, затем установить новую версию, при этом предварительно можно сохранить все настройки в соответствии с пунктом 3.1.5.10 РДПИ.00888-04 34 01. Устанавливать новую версию поверх уже установленной нельзя.

После установки ОСПО на ОС Windows следует вручную настроить мандатный и дискреционный доступ в СЗИ для его каталогов. Настройка описана в разделе «Настройка и проверка мандатного и дискреционного доступа».

В целях исключения уязвимости «DLL Hijacking» необходимо внести изменения в ветку реестра `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs` в части добавления доверенных системных динамических библиотек, используемых ОСПО «Веста»: `USERENV.dll`, `MPR.DLL`, `NETAPI32.dll`, `VERSION.dll`, `WINMM.DLL`, `WINMMBASE.dll`, `DNSAPI.DLL`, `IPHLPAPI.DLL`, `COMCTL32.dll`, `WINSPOOL.DRV`, `bcrypt.dll`, `dwmapi.dll`, `UxTheme.dll`. После перезагрузки операционной системы применение данных системных динамических библиотек будет производиться из доверенного хранилища.



### 3.2. Удаление

Для удаления ОСПО «Веста-В» в операционной системе Windows необходимо произвести запуск командного файла **uninstall.bat** с правами администратора.

В случае использования средств защиты информации, удаление должно производиться под администратором безопасности (рис. 1).

## Запуск файла uninstall.bat от имени администратора

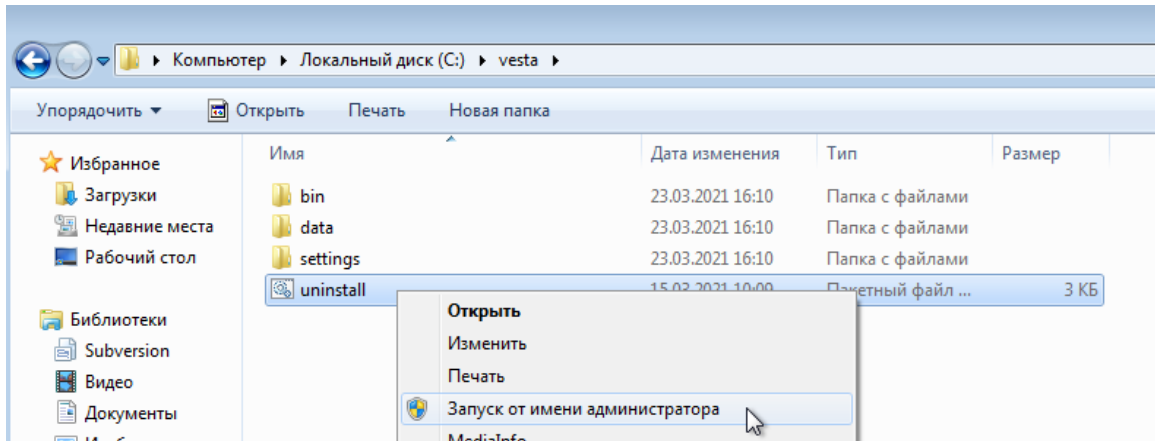


Рис. 1

После успешного удаления в командной строке отобразится соответствующая надпись (рис. 2).

## Результат выполнения uninstall.bat

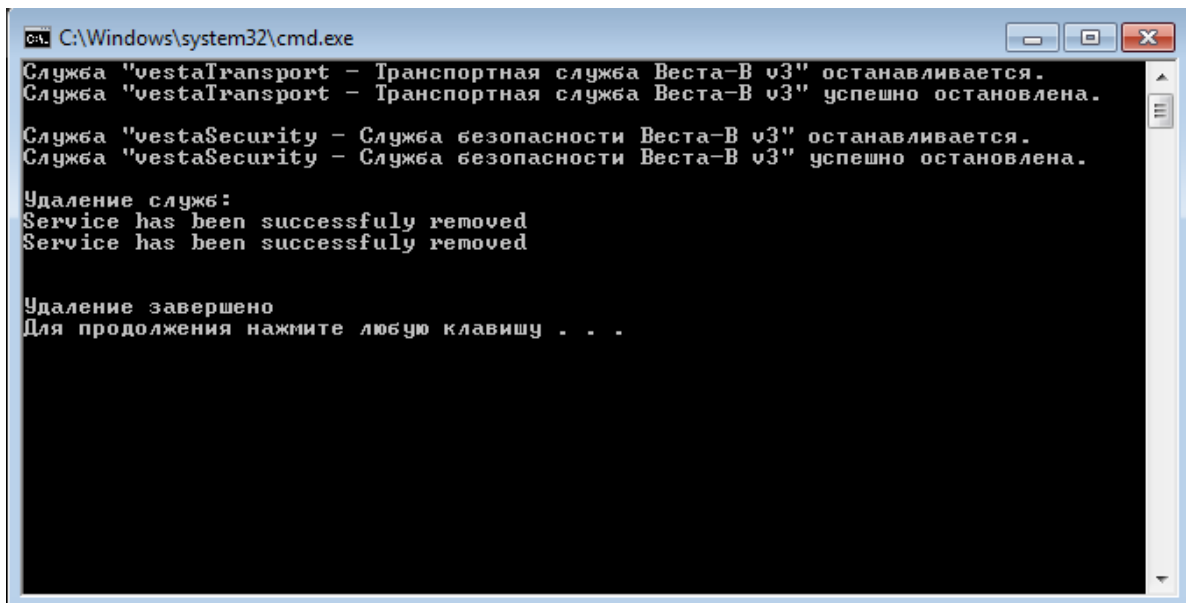


Рис. 2

## 4. НАСТРОЙКА И ПРОВЕРКА МАНДАТНОГО И ДИСКРЕЦИОННОГО ДОСТУПА

### 4.1. Настройка доступа

В операционной системе Windows рекомендуется создать группу *vesta* и добавить в нее пользователей, допущенных к работе с ОСПО для упрощения и централизации управления дискреционными и мандатными правами доступа.

Настройка дискреционных и мандатных прав производится сертифицированными средствами защиты информации от несанкционированного доступа (СЗИ от НСД):

- каталог *vesta/bin/* содержит исполняемые файлы и его содержимое не меняется в процессе работы. Поэтому всем пользователям в группе *vesta* необходимо разрешить дискреционный доступ на чтение и исполнение, но рекомендуется запретить запись и удаление, чтобы пользователи не могли случайно удалить исполняемые файлы ОСПО. Этому каталогу необходимо установить мандатный доступ, соответствующий режиму работы с несекретными (открытыми) данными;

- каталог *vesta/data/* содержит подкаталоги с данными, которые могут иметь различный уровень секретности. На этот каталог и все его подкаталоги всем пользователям в группе *vesta* необходимо разрешить дискреционный доступ на чтение, запись и удаление;

- подкаталог *vesta/data/0/* содержит данные, соответствующие нулевому уровню секретности – «Не секретно». Этому каталогу необходимо установить мандатный доступ соответствующий режиму работы с несекретными (открытыми) данными;

- подкаталог *vesta/data/1/* содержит данные, соответствующие первому уровню секретности – «Конфиденциально». Этому каталогу необходимо установить мандатный доступ соответствующий режиму работы с конфиденциальными данными;

- подкаталог *vesta/data/2/* содержит данные, соответствующие второму

уровню секретности – «Секретно». Этому каталогу необходимо установить мандатный доступ соответствующий режиму работы с данными, содержащими сведения, составляющими государственную тайну и соответствующими уровню «Секретно»;

– подкаталог `vesta/data/3/` содержит данные, соответствующие третьему уровню секретности – «Сов. секретно». Этому каталогу необходимо установить мандатный доступ соответствующий режиму работы с данными, содержащими сведения, составляющими государственную тайну и соответствующими уровню «Сов. секретно»;

– каталог `vesta/settings/` содержит настройки ОСПО. Всем пользователям в группе `vesta` необходимо разрешить дискреционный доступ на чтение, запись и удаление. Этому каталогу необходимо установить мандатный доступ, соответствующий режиму работы с несекретными (открытыми) данными.

**Внимание! При неправильной настройке дискреционных и мандатных прав доступа в СЗИ существует угроза информационной безопасности.**

При формировании сообщения заданный уровень секретности записывается в файл сообщения. Данный уровень не может быть изменен не при каких обстоятельствах.

Сообщения с секретностью «Несекретно» сохраняются в каталоге данных `vesta/data/0/`, сообщения с секретностью «Конфиденциально» в каталоге данных `vesta/data/1/` и т.д.

При передаче сообщения через сеть, сообщение не меняет своего каталога.

Например, если сообщение имеет уровень секретности «Секретно», то оно всегда будет располагаться в каталоге данных `vesta/data/2/`, вне

зависимости от того, чей это компьютер: отправителя, транзитного узла или получателя.

**Таким образом, для исключения появления угроз информационной безопасности связанных с работой ОСПО необходимо, чтобы во всей сети настройки СЗИ в части взаимодействия с ОСПО были одинаковыми.**

## 5. УТИЛИТА ПРОВЕРКИ ДОСТУПА CHECKACCESS

### 5.1. Общие сведения

Данная утилита предназначена для проверки доступа к каталогам в условиях работы средств защиты информации (СЗИ). Таким образом, checkAccess позволяет проверить правильность настройки мандатного и дискреционного доступа в СЗИ. Главное окно программы checkAccess представлено на рис. 3.

Расположение программы checkAccess: **vesta/bin/checkAccess.exe**

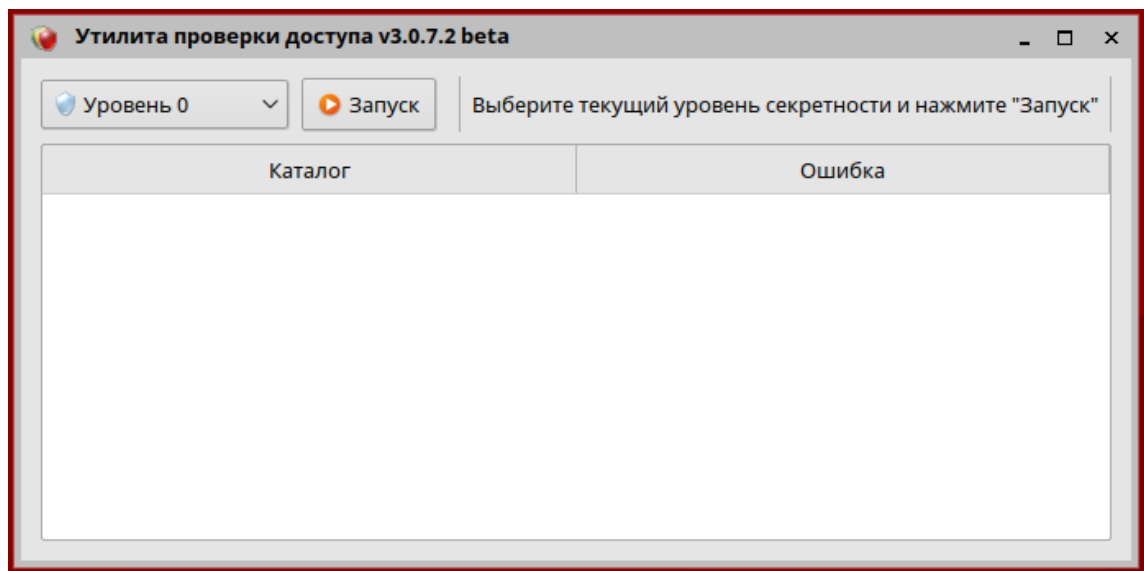


Рис. 3

### 5.2. Проверка доступа

Для проверки доступа необходимо выполнить следующие действия:

- поочередно войти под каждым уровнем секретности;
- запустить программу checkAccess;
- выбрать из выпадающего списка уровень секретности, под которым произведен вход (рис. 4);
- нажать кнопку «Запуск».

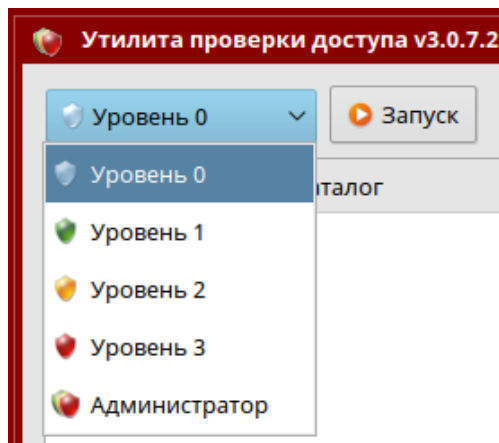


Рис. 4

В случае неправильной настройки мандатного и дискреционного доступа в СЗИ в информационном поле программы checkAccess отобразятся соответствующие ошибки.

В поле «Каталог» отобразится место ошибки, а в поле «Ошибка» описание ошибки, которую необходимо устранить (рис. 5). Например, если указано, что произведено чтение из каталога, то это означает, что в выбранном уровне секретности данный каталог не должен быть доступен для чтения.

После устранения ошибок необходимо произвести проверку повторно.

#### Пример результата проверки доступа

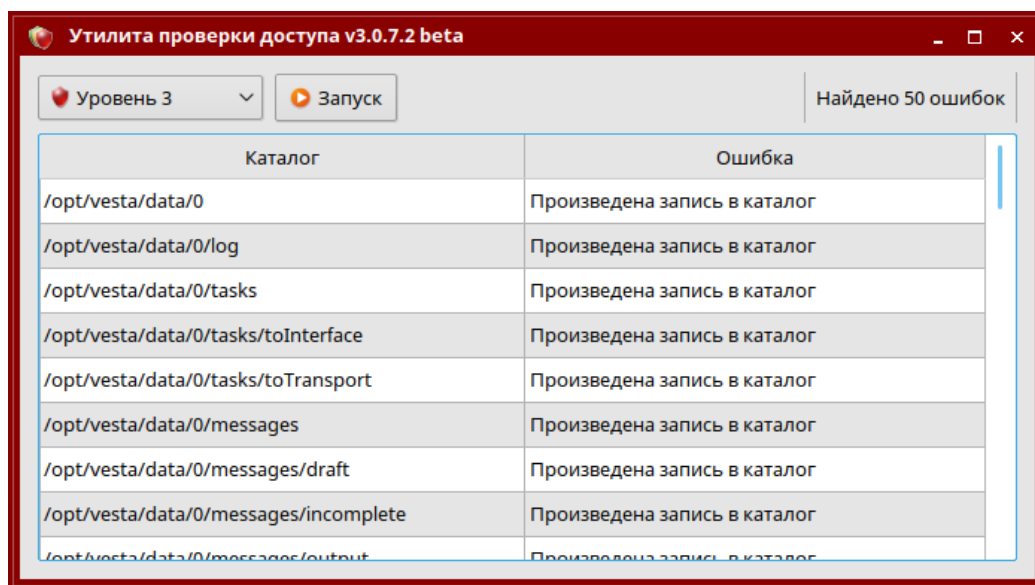


Рис. 5

Если проверка завершена без ошибок, это означает, что настройка СЗИ выполнена правильно.

## 6. РЕДАКТОР СЕТЕВЫХ МАРШРУТОВ ROUTEEDITOR

### 6.1. Общие сведения

Данная утилита предназначена для настройки сетевых маршрутов в операционной системе компьютера. Верная настройка сетевых маршрутов обеспечивает правильный выбор сетевого маршрута в IP сетях для доставки информации удаленному абоненту.

Изменение сетевых маршрутов необходимо только при наличии нескольких физических сетевых карт в компьютере, при условии их одновременного использования.

В случае наличия или использования только одной сетевой карты настройка **не требуется**.

Расположение программы routeEditor: **vesta/bin/routeEditor.exe**.

### 6.2. Работа с программой routeEditor

Главное окно программы routeEditor имеет вид таблицы, столбцы которого представлены значениями «Ip-адрес», «Маска», «Адрес шлюза» (рис.6).

Главное окно редактора сетевых маршрутов routeEditor

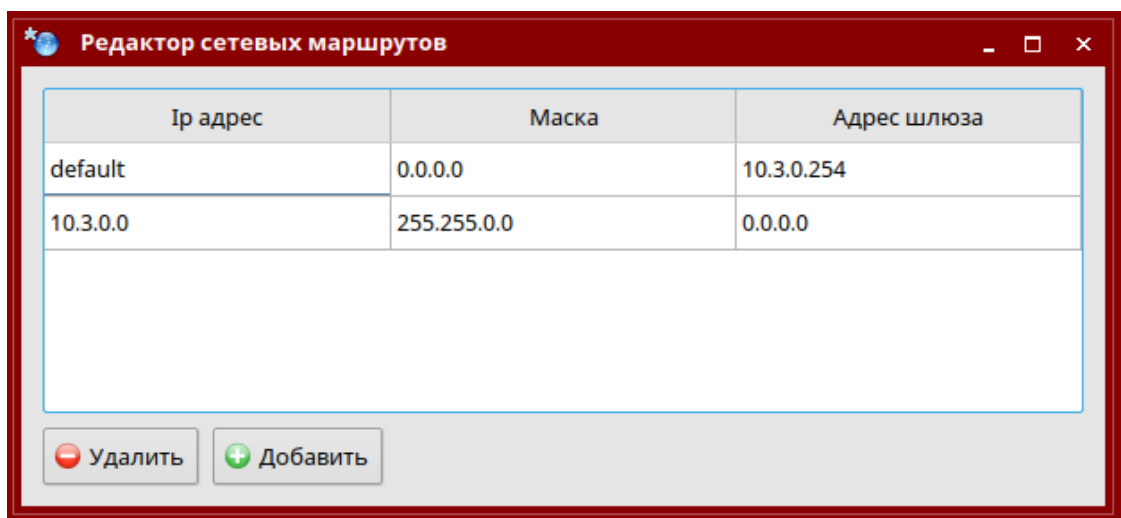


Рис. 6



Если после запуска программы routeEditor в нижней части окна отображается сообщение «Недостаточно прав доступа для редактирования» (рис. 7), то необходимо нажать на кнопку «Перезапуск», которая перезапустит программу routeEditor с правами суперпользователя.

В случае если ошибка останется, то необходимо зайти под учетной записью суперпользователя и произвести настройку под ним.

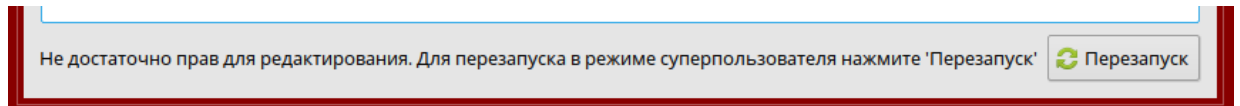


Рис. 7

Для редактирования сетевых маршрутов в нижней части окна имеются кнопки «Удалить», «Добавить». Изменить имеющиеся маршруты нельзя.

При добавлении нового маршрута открывается окно добавления, где необходимо заполнить поля: «Ip-адрес», «Маска», «Адрес шлюза» (рис. 8).

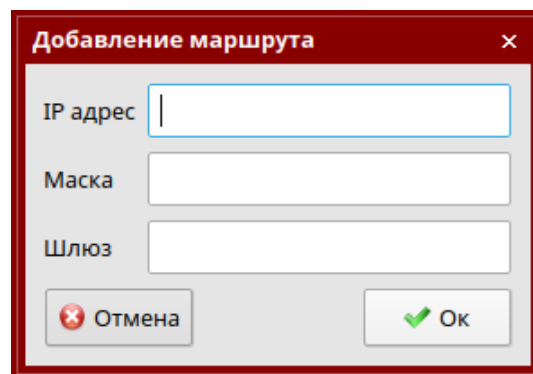


Рис. 8

Для удаления выбранного маршрута нажмите кнопку «Удалить».

## 7. ОТЛАДКА ОСПО

### 7.1. Общие сведения

В данном разделе описываются механизмы поиска причины сбоя в ходе работы ОСПО.

Отладка ОСПО осуществляется через анализ файлов системных журналов – логов. Файлы логов представляют собой внутренний журнал работы ОСПО и не имеют ничего общего с журналами в ОСПО.

Логи располагаются в каталогах с данными в соответствующей папке, например **vesta/data/0/log/**, **vesta/data/1/log/**, ...

Имя файла лога включает название исполняемого файла, пользователя под которым он запущен и дату запуска ОСПО:

- **checkAccess\_ПОЛЬЗОВАТЕЛЬ\_ДАТА.log** – лог утилиты проверки доступа;
- **vesta\_ПОЛЬЗОВАТЕЛЬ\_ДАТА.log** – лог интерфейса приложения;
- **vestaSecurity\_ПОЛЬЗОВАТЕЛЬ\_ДАТА.log** – лог подсистемы безопасности;
- **vestaTransport\_ПОЛЬЗОВАТЕЛЬ\_ДАТА.log** – лог транспортной подсистемы;
- **workingProtocol\_ДАТА.log** – лог рабочего протокола транспортной подсистемы.

Логи содержат расширенную информацию о ходе внутренней работы ОСПО. Логи, по большей части, предназначаются разработчику, нежели пользователю ОСПО, однако, с помощью них пользователь может самостоятельно выявить причину сбоя в ОСПО.

### 7.2. Уровни логирования

Степень детализации информации в логах определяется параметрами в секции **[Debug]** файла **vesta/settings/settings.ini** (рис. 9).

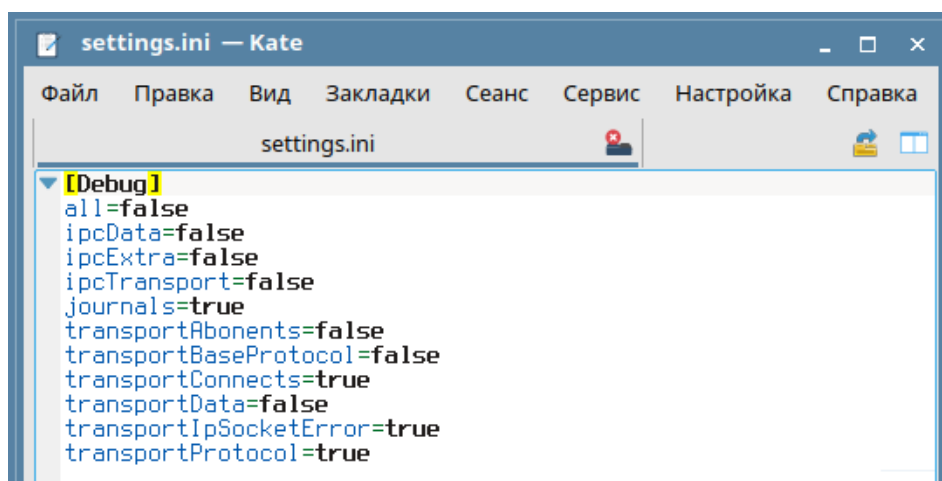


Рис. 9

Для включения того или иного уровня логирования следует открыть данный файл в текстовом редакторе и изменить необходимый параметр. В большинстве случаев перезапуск ОСПО не требуется.

Для включения определенного уровня логирования необходимо изменить значение нужного уровня в данном файле на **true**, для выключения на **false**.

**Внимание:** не рекомендуется изменять параметры в данном файле без четкого осознания последствий.

Уровни логирования:

- all – включает логирование всех остальных уровней, а так же логирование каждой используемой функции в ОСПО. Размер логов увеличивается до астрономических размеров, но данный режим позволяет с наибольшей точностью выявить причину сбоя. Настоятельно не рекомендуется включать данный уровень логирования, т.к. он предназначен исключительно для разработчиков;

- ipcData – включает логирование всех передаваемых данных через межпроцессное взаимодействие. Настоятельно не рекомендуется включать данный уровень логирования;

- ipcExtra – включает логирование особенно частых событий межпроцессного взаимодействия;

- ipcSecurityDaemon – включает логирование базового межпроцессного взаимодействия между интерфейсом ОСПО и подсистемой безопасности;
- ipcTransport – включает логирование базового межпроцессного взаимодействия между интерфейсом ОСПО и транспортной подсистемой;
- journals – включает логирование записей в журналы;
- messagesAutodelete – включает логирование автоудаления сообщения;
- messagesLock – включает логирование блокировки сообщений;
- transportAbonents – включает логирование отслеживания приоритета вызова абонентов в транспортной подсистеме;
- transportConnects – включает логирование всех соединений с абонентами в транспортной подсистеме;
- transportData – включает логирование всех передаваемых данных в транспортной подсистеме. Настоятельно не рекомендуется включать данный уровень логирования;
- transportBaseProtocol – включает логирование базового транспортного протокола;
- transportProtocol – включает логирование транспортного протокола. Наиболее важный уровень логирования для выявления ошибок при передаче данных другому абоненту;
- transportProtocolAttaches – включает логирование передачи вложений в сообщении в транспортном протоколе;
- transportIpSocketError – включает логирование всех ошибок сокета в IP-канале;
- transportComPortError – включает логирование ошибок СОМ-порта в коммутируемом канале;
- transportComAtCommands – включает логирование АТ команд в коммутируемом канале;
- transportComPackets – включает логирование принимаемых и передаваемых пакетов в коммутируемом канале;

– transportComData – включает логирование всех передаваемых данных через коммутируемый канал. Настоятельно не рекомендуется включать данный уровень логирования;

– transportTasks – включает логирование задач в транспортной подсистеме.

### 7.3. Экспорт логов

При появлении внештатной работы ОСПО необходимо сформировать список файлов с логами ОСПО через режим «Экспорт логов» или ручным способом и отправить в АО «НПП «Рубин» для анализа.

Для сбора логов необходимо зайти в настройки в раздел «Разное» и нажать кнопку экспорта логов. При этом в один файл будут собраны и сжаты все необходимые логи. Получившийся в результате файл необходимо отправить разработчику для анализа.

При неисправности ОСПО, которая не позволяет ему запускаться, необходимо вручную собрать все логи из всех каталогов логов с разной секретностью, заархивировать и передать разработчику для анализа.

Возможно, что уровня логирования по умолчанию может быть недостаточно для выявления проблемы, в данном случае разработчик может попросить Вас временно включить те или иные уровни логирования, воспроизвести ошибку в ОСПО и еще раз собрать и передать логи, но на этот раз уже более детальные.

## 8. ДЕТАЛЬНАЯ НАСТРОЙКА

В данном разделе описывается детальная настройка ОСПО.

Детальная настройка ОСПО производится путем редактирования параметров в файле **vesta/settings/settings.ini** с помощью текстового редактора. Если требуется вернуть значение по умолчанию - необходимо удалить строку с параметром или весь файл. При перезапуске ОСПО значения восстановятся по умолчанию.

Секция **[Debug]** позволяет включать и отключать отладку (логирование) на определенных уровнях. Данная процедура более подробно описана в разделе «ОТЛАДКА».

Параметры секции **[Permissions]**:

- filePermissions - права доступа для всех файлов (в десятичном виде), создаваемых ОСПО;
- dirPermissions - права доступа для всех каталогов (в десятичном виде), создаваемых ОСПО.

Параметры секции **[Ports]**:

- securityDaemonIpc - TCP-порт, используемый интерфейсом ОСПО для связи с подсистемой безопасности;
- transportIpc - TCP-порт, используемый интерфейсом ОСПО для связи с транспортной подсистемой;
- singleAppIpcPort - TCP-порт, используемый интерфейсом ОСПО для связи с сервером защиты от повторного запуска.

Параметры секции **[Details]**:

- journalUpdateTime - интервал обновления данных в журналах в миллисекундах;

- `messagesDeadlineCheckInterval` - интервал проверки истечения крайнего срока у сообщений в миллисекундах;
- `messagesAutodeleteCheckInterval` - интервал проверки для автоудаления сообщений;
- `freeSpaceCheckMb` - порог проверки свободного места на диске в мегабайтах;
- `freeSpaceCheckInterval` - интервал проверки свободного места на диске в миллисекундах;
- `secrecyChangeCheckInterval` - интервал проверки изменения текущего уровня секретности в миллисекундах;
- `copyBlockSizeKb` - размер блока данных при копировании вложений в килобайтах;
- `copySleep` - задержка между копированием блоков данных в миллисекундах;
- `maxWritingTime` - максимальное время ожидания записи блока данных в файл в миллисекундах;
- `transportRestart` - флаг, отвечающий за автоматический перезапуск транспортной подсистемы;
- `transportChannelsStartDelay` - задержка в миллисекундах перед запуском каналов при запуске транспортной подсистемы;
- `transportServerThreadStartTimeout` - время ожидания инициализации потока сервера в плагине канала в транспортной подсистеме в миллисекундах;
- `transportServerThreadStopTimeout` - время ожидания завершения потока сервера в плагине канала в транспортной подсистеме в миллисекундах;
- `transportProtocolInterval` - задержка между тиками транспортного протокола в миллисекундах;
- `transportProtocolHashCheckCount` - количество пакетов данных после которого необходимо произвести проверку надежности протокола;
- `transportProtocolSilentTimeout` - таймаут в секундах до разъединения в

случае молчания собеседника;

– transportProtocolNothingToSendTimeout - таймаут в миллисекундах до разъединения если нечего передавать;

– transportProtocolKeepAliveTimeout - таймаут в секундах до разъединения если нечего передавать, но установлен флаг удержания соединения;

– transportProtocolNewMessagesCheckInterval - интервал в миллисекундах проверки поступления новых сообщений для передачи, если нам нечего было передавать;

– transportProtocolMaxErrorCount - максимальное число ошибок в транспортном протоколе до разъединения;

– transportProtocolFreeSpaceBuffer - минимальный размер свободного места на диске в мегабайтах для приема сообщения;

– transportProgressUpdateTimeout - таймаут в миллисекундах между обновлениями прогресса сообщения;

– transportMessageCopyProgressLogTimeout - таймаут в секундах между логированием прогресса копирования сообщения;

– transportRandomReconnectTimeout - максимальный случайный таймаут в секундах для переподключения к абоненту;

– transportUselessReconnectTimeout - максимальный дополнительный случайный таймаут в секундах для переподключения к абоненту, если последнее соединение с ним было бесполезным;

– transportConnectionTickInterval - интервал в миллисекундах между проверками необходимости вызова абонентов;

– transportAutoDeleteTickInterval - интервал в миллисекундах между проверками возможности автоматического удаления исходящих сообщений;

– transportTaskMaxHops - максимальное число транзитных узлов через которые может быть передана задача;

– transportIpThreadStartTimeout - таймаут в миллисекундах ожидания



запуска потока канала из транспортного сервера;

- `transportIpConnectTimeout` - таймаут в миллисекундах ожидания соединения по IP-каналу;

- `transportIpMaxReconnectTimeout` - максимальное время в секундах между попытками вызова недоступного абонента по IP-каналу;

- `transportComConnectTimeout` - таймаут в миллисекундах ожидания соединения по коммутируемому каналу;

- `transportComOpenInterval` - интервал в миллисекундах между попытками открытия СОМ порта в коммутируемом канале;

- `transportComDsrCheckInterval` - интервал в миллисекундах между проверками DSR сигнала;

- `transportComAtOkTimeout` - таймаут в миллисекундах ожидания ответа 'OK' на команду 'AT' в коммутируемом канале;

- `transportComAtReadyCheckTimeout` - таймаут в миллисекундах между перепроверками доступности СОМ порта в коммутируемом канале;

- `transportComResetTimeout` - время ожидания сброса соединения модема в миллисекундах в коммутируемом канале;

- `transportComMaxBytesToWrite` - максимальное количество байт, стоящих в очереди на записи внутри СОМ порта в коммутируемом канале;

- `transportComResendInterval` - интервал между перепосылкой пакетов в коммутируемом канале;

- `transportComConfirmationInterval` - интервал между отправками подтверждений получения пакетов в коммутируемом канале;

- `transportComMaxBytesInQueue` - максимальное количество байт, стоящих в очереди на записи в канале;

- `transportComControlSymbol` – символ переноса строки для AT-команд;

- `transportDedicatedOpenInterval` - интервал в миллисекундах между попытками открытия СОМ порта в выделенном канале;

- `transportDedicatedDsrCheckInterval` - интервал в миллисекундах между

проверками DSR сигнала в COM порте в выделенном канале;

- `transportDedicatedDcdCheckInterval` - интервал в миллисекундах между проверками DCD сигнала в COM порте в выделенном канале;

- `transportDedicatedMaxBytesToWrite` - максимальное количество байт, стоящих в очереди на записи внутри COM порта в выделенном канале;

- `transportDedicatedResendInterval` - интервал между перепосылкой пакетов в выделенном канале;

- `transportDedicatedConfirmationInterval` - интервал между отправками подтверждений получения пакетов в выделенном канале;

- `transportDedicatedMaxBytesInQueue` - максимальное количество байт, стоящих в очереди на записи в канале;

- `transportDedicatedKeepAliveTimeout` - таймаут в секундах до разъединения если нечего передавать, но установлен флаг удержания соединения в выделенном канале;

- `transportDedicatedUseOnePortForSeveralAbonents` - флаг позволяющий использовать один выделенный COM порт у нескольких абонентов;

- `applicationStyle` - стиль приложения;

- `toolbarStyle` - стиль кнопок панели инструментов;

- `abonentsModelTooltipMinLength` - минимальная длина имени абонента для которого необходимо отобразить тултип;

- `maxTooltipRowCount` - максимальное количество строк в тултипе;

- `CNewMessageDialog_attachFilters` - фильтр вложений;

- `CNewMessageDialog_maxContextMenuAbonents` - максимальное число избранных абонентов, отображаемых в контекстном меню быстрого выбора получателей;

- `CNewMessageDialog_maxContextMenuAttaches` - максимальное число файлов, отображаемых в контекстном меню быстрого выбора вложений;

- `abonentsDetailedSettingsCheck` - флаг детальной проверки настроек у абонентов (рекомендуется выключать при большом количестве абонентов на

слабых ЭВМ);

– CViewMessageDialog\_saveLastNames - флаг сохранения недавних ФИО операторов при обработке сообщений;

– CViewMessageDialog\_maxLastNames - максимальное количество сохраненных недавних ФИО операторов;

– messagesFontSizeModifier - модификатор размера шрифта в сообщениях;

– soundRepeatTimeout - таймаут между повторениями мелодии в уведомлениях;

– journalColor\_0 - цвет подсветки 0 уровня секретности;

– journalColor\_1 - цвет подсветки 1 уровня секретности;

– journalColor\_2 - цвет подсветки 2 уровня секретности;

– journalColor\_3 - цвет подсветки 3 уровня секретности;

– PrintingRenderBackgroundColor - цвет заливки чередующихся строк в журналах и при печати;

– previewStateChangeTimeout - таймаут в миллисекундах перед изменением состояния входящего сообщения, отображаемого в предпросмотре, на прочитаное;

– transportCheckInterval - интервал в миллисекундах между проверками ответа от транспортной подсистемы;

– transportRestartMaxAttempts - максимальное количество попыток перезапуска транспортной подсистемы в случае его падения;

– transportRestartTimeout - таймаут в миллисекундах перед перезапуском транспортной подсистемы;

– transportControlTimeout - таймаут в миллисекундах запрещающий повторное управление состоянием транспортной подсистемы;

– transportStateOff - цвет текста состояния выключенной транспортной подсистемы;

– transportStateOn - цвет текста состояния работающей транспортной

подсистемы;

– transportStateNotRespond - цвет текста состояния зависшей транспортной подсистемы;

– messagePauseColor - цвет подсветки сообщений на паузе;

– messageReceivingColor - цвет подсветки получаемого сообщения;

– messageSendingColor - цвет подсветки передающегося сообщения;

– protocolWarningColor - цвет подсветки предупреждений в протоколе работы;

– protocolErrorColor - цвет подсветки ошибок в протоколе работы;

– protocolLimit - ограничение числа записей в протоколе работы;

– protocolUpdateInterval - таймаут в миллисекундах между обновлениями протокола работы;

– defaultNotificationColor1 - цвет заливки окна уведомления по умолчанию;

– defaultNotificationColor2 - второй цвет заливки окна уведомления по умолчанию;

– defaultNotificationBlinkInterval - время перехода между цветами в окне уведомления по умолчанию в миллисекундах;

– smartNotificationMoveCheckInterval - время в миллисекундах между проверками на движение мыши для определения находится ли пользователь за компьютером;

– smartNotificationMoveTimeout - время в миллисекундах между движениями мыши после которого считается, что пользователь находится не за компьютером;

– ipcSocketMaxWriteTime - максимальное время записи данных в миллисекундах в сокет межпроцессного взаимодействия;

– ipcProtocolMaxStopTime - максимальное время ожидания в миллисекундах завершения межпроцессного протокола;

– singleProtectConnectTimeout - время ожидания в миллисекундах

соединения с сервером защиты от повторного запуска интерфейса;

- `singleProtectReconnectTimeout` - таймаут в миллисекундах между попытками подключения к серверу защиты от повторного запуска интерфейса;

- `securityDaemonClientThreadStartTimeout` - время ожидания в миллисекундах запуска потока клиентского протокола подсистемы безопасности;

- `securityDaemonClientThreadStopTimeout` - время ожидания в миллисекундах остановки потока клиентского протокола подсистемы безопасности;

- `securityDaemonClientProtocolConnectTimeout` - время ожидания в миллисекундах соединения клиента с подсистемой безопасности;

- `securityDaemonClientProtocolResponseTimeout` - время ожидания в миллисекундах ответа от подсистемы безопасности;

- `securityDaemonLogsExportResponseTimeout` - время ожидания в миллисекундах ответа от подсистемы безопасности при экспорте логов;

- `ipcConnectTimeout` - время ожидания в миллисекундах соединения интерфейса с транспортной подсистемой;

- `ipcClientThreadStopTimeout` - время ожидания в миллисекундах завершения потока клиентского протокола межпроцессного взаимодействия с транспортной подсистемой;

- `ipcServerThreadStopTimeout` - время ожидания в миллисекундах завершения серверного потока межпроцессного взаимодействия в транспортной подсистеме;

- `transportMaxResponseTimeout` - максимальное время в секундах неполучения ответа от транспортной подсистемы после которого он будет считаться зависшим;

- `transportSpeedUpdateTimeout` - таймаут в миллисекундах между обновлением состояний каналов;

- `transportChannelStateUpdateTimeout` - интервал в миллисекундах

обновления общей скорости транспортной подсистемы;

– transportAbonentSmallSize - размер данных в байтах, который считается небольшим при подсчёте приоритета сообщения;

– transportAbonentOnlineActualTime - время в секундах, в течение которого онлайн статус абонента считается актуальным;

– transportAbonentOnlineSaveInterval - интервал в миллисекундах сохранения файла с доступностью абонентов;

– transportAbonentPrioritySmall - изменение приоритета абонента, если ему отправляется небольшой объем данных;

– transportAbonentPriorityHigh - изменение приоритета абонента, если ему отправляется сообщение с высоким приоритетом;

– transportAbonentPriorityNormal - изменение приоритета абонента, если ему отправляется сообщение с нормальным приоритетом;

– transportAbonentPriorityLow - изменение приоритета абонента, если ему отправляется сообщение с низким приоритетом;

– transportAbonentPriorityAvailable - изменение приоритета абонента при его недавней доступности;

– transportAbonentPriorityNotAvailable - изменение приоритета абонента при его недоступности.

## 9. ПРОВЕРКА КОНТРОЛЬНОЙ СУММЫ ОСПО

Проверка контрольной суммы ОСПО проводится с помощью «Программы фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.2). Расчет контрольной суммы файлов, находящихся на диске необходимо проводить по алгоритму «Уровень-1, программно».

Если фактическая (подсчитанная) КС совпадает с КС, приведенной в формуляре, то диск считается правильным.

Если фактическая КС не совпадает с КС, приведенной в формуляре, то диск считается испорченным.

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ДСП – для служебного пользования

КС – контрольная сумма

НСД – несанкционированный доступ

ОС – операционная система

ОСПО – общесистемное программное обеспечение

ПО – программное обеспечение

СЗИ – средство защиты информации

ЭВМ – электронно-вычислительная машина



Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
Изм	измененных	замененных	новых	аннулированных					
2		все			33	РДПИ.221-2022		Давыдова	14.07.2022