Программно-аппаратный комплекс «Горизонт-ВС»

Руководство администратора

Часть 1

Описание и работа
Модуля идентификации и контроля доверенной среды
(МИиКДС) «Шина»

МБРЦ.468313.001.Д2.1

Листов: 101

Москва 2023

ГОРИЗОНТ-ВС

ЦИФРОВОЕ БУДУЩЕЕ
НАЧИНАЕТСЯ СЕГОДНЯ

Почтовый адрес:	123022, г. Москва, ул. 2-ая Звенигородская, дом 13, строение 43, офис 73
Телефон:	+7 (495) 120-15-37
E-mail:	info@gorizont-vs.ru
Web:	https://gorizont-vs.ru/about-us.html

Аннотация

Настоящее руководство является основным документом, описывающим порядок действий администратора при работе с модулем «Шина. В руководстве приведены сведения, необходимые администратору для установки изделия в вычислительную технику на базе персональных электронных вычислительных машин (ПЭВМ), а также для настройки и эксплуатации изделия.

Содержание

1 Введение

1.1 Область применения

ПАК «Горизонт-ВС» предназначен для организации взаимодействия пользователей *терминалов*[1] с ресурсами *серверов виртуализации*, объединенных в IP-сеть с использованием технологии «клиент-сервер».

Программно-аппаратный комплекс «Горизонт-ВС» МБРЦ.468313.001 (далее по тексту – ПАК «Горизонт-ВС») включает две составные части:

- модуль идентификации и контроля доверенной среды (МИиКДС) «Шина» МБРЦ.468264.001 (далее по тексту – МИиКДС «Шина»);
- комплекс программ «Терминал-Сервер» RU.МБРЦ.501130.01-01 (далее – комплекс программ (КП) «Терминал-Сервер»).

Руководство администратора МБРЦ.468313.001.И3.02 состоит из двух частей:

- МБРЦ.468313.001.И3.02-01 ПАК «Горизонт-ВС». Руководство администратора. Часть 1. Описание и работа модуля идентификации и контроля доверенной среды (МИиКДС) «Шина»;
- МБРЦ.468313.001.И3.02-02 ПАК «Горизонт-ВС». Руководство администратора. Часть 2. Описание и работа комплекса программ «Терминал-Сервер».

1.2 Краткое описание возможностей

Изделие работает в трех режимах:

- режим ***Терминал*** – изделие устанавливается на *терминале*;
- режим ***Сервер*** – изделие устанавливается на *сервере виртуализации;*
- режим **АРМ Администратора** – изделие устанавливается на АРМ Администратора.

Примечание *– Режим работы изделия определяет сервисный код, который вводится при инсталляции платы изделия (см. п. 4.1.3.1).*

МИиКДС «Шина» обеспечивает выполнение следующих основных функций:

[1] *Терминал* – аппаратное устройство, предназначенное для удаленного подключения к виртуальной машине, исполняемой на *сервере виртуализации.*

- при работе в режиме ***Терминал***:
  - идентификацию и аутентификацию администраторов/пользователей;
  - доверенную загрузку специального программного обеспечения (СПО);
- контроль целостности СПО;
- блокировку работы *терминала* в случае неудачной идентификации и аутентификации администратора/пользователя;
- ведение журнала регистрации событий, регистрирующего события имеющие отношение к безопасности системы;
- блокировку входа в систему зарегистрированного пользователя при:
  - нарушении целостности контролируемой информации СПО;
  - превышении предельного числа неудачных попыток входа и истечении срока действия пароля;
- блокировании администратором входа пользователя;
- самотестирование (проверка технического состояния);
- при работе изделия в режиме ***Сервер*** основные функции изделия аналогичны режиму ***Терминал****;*
- при работе изделия в режиме ***АРМ Администратора*** функции режима ***Терминал*** дополняются механизмом удаленного администрирования, обеспечивающего следующие основные функции:
  - регистрацию/удаление пользователей в изделии, установленном на удаленном *терминале/сервере виртуализации*;
  - блокировку/разблокировку пользователей в изделии, установленном на удаленном *терминале/сервере виртуализации*;
  - работу с журналом регистрации событий изделия, установленного на удаленном *терминале/сервере виртуализации;*
  - мониторинг состояния изделия в АГ;
- подключение шлюзов АГ[2] и установку связи между АГ, входящими в одну серию[3];

[2] Шлюз АГ – это *АРМ Администратора* другой АГ, входящий в состав текущей АГ, обеспечивающий связь с *серверами* своей группы.

- генерацию ключей маскирования;
- рассылку ключей маскирования;
- смену ключей маскирования;
- смену паролей администраторов и пользователей;
- создание инсталляционного ключа, транспортного ключа и электронных ключей (ЭК) аутентификации пользователей и администраторов.

1.3 Уровень подготовки персонала

Администраторы СГУ «Горизонт-ВС» должны иметь опыт работы с:

- персональным компьютером на уровне квалифицированного пользователя;
- стандартными приложениями на уровне свободного выполнения базовых операций;
- операционными системами:
  - Windows;
  - Unix-подобными ОС.

1.4 Перечень эксплуатационной документации, с которой необходимо ознакомиться администратору

Администратору СГУ «Горизонт» необходимо ознакомиться со следующими документами:

- Руководство пользователя. МБРЦ.468313.001.ИЗ.01.
- Руководство администратора. Часть 1. Описание и работа модуля идентификации и контроля доверенной среды (МИиКДС) «Шина». МБРЦ.468313.001.ИЗ.02-01;
- Руководство администратора. Часть 2. Описание и работа комплекса программ «Терминал-сервер». МБРЦ.468313.001.ИЗ.02-02.

[3] Серия – это совокупность изделий, входящих в состав нескольких АГ (максимум – 21 административная группа), объединенных одной поставкой на объект эксплуатации.

2 Назначение и условия применения

2.1 Назначение МИиКДС «Шина»

МИиКДС «Шина» предназначен для использования в клиент-серверных системах и предназначен для защиты АРМ, являющихся *терминалами*, *серверами виртуализации* и *АРМ администратора* от несанкционированного доступа (НСД).

2.2 Условия применения

Группа *серверов виртуализации* и *терминалов*, в которой работают пользователи, объединены в административную группу (далее по тексту – АГ). Администрирование в рамках АГ выполняют администраторы, используя автоматизированное рабочее место администратора безопасности – *АРМ Администратора*. В том числе при помощи АРМ Администратора могут производиться настроечные работы в АГ, после чего сервера виртуализации и терминалы будут работать в локальном режиме.

2.2.1 Минимальные системные требования

Изделие устанавливается на аппаратной платформе со следующими характеристиками:

- наличие шины PCI-Express;
- наличие интерфейса USB 2.0;
- оперативная память не менее 4 Гб для сервера и не менее 256 Мб для терминала;
- процессор класса x86 не ниже Pentium 4 для терминала и с поддержкой технологии Intel-VT или AMD-V для сервера;
- жесткий диск не менее 100 Гб для сервера;
- BIOS должен обеспечивать соответствие спецификации Plug and Play BIOS версии 1.0A;
- наличие разъема SATA на материнской плате.

Перед созданием автоматизированной системы в защищенном исполнении с использованием изделия в обязательном порядке должна быть проведена работа по проверке совместимости изделия и средств вычислительной техники, в составе которых предполагается его

использование. Технические средства ПЭВМ, в которую устанавливается изделие, не должны содержать аппаратно-программных механизмов, ориентированных на целенаправленное нарушение правильности его функционирования.

В изделии на одном *терминале* может быть зарегистрирован только один пользователь. В свою очередь каждый *терминал* конфигурируется на доступ только к одной виртуальной машине. Таким образом, пользователь может получить доступ только к одной виртуальной машине.

Администратором СДЗ должны быть выполнены процедуры по развертыванию АГ в соответствии с настоящим руководством администратора. Все действия по обслуживанию АГ администратор СДЗ выполняет с помощью программы «Администратор МИиКДС».

Крепление платы МИиКДС в корпусе ПЭВМ должно исключать возможность извлечения данной платы без вскрытия корпуса. После установки и настройки изделия в обязательном порядке должна быть исключена возможность бесконтрольного доступа к техническим средствам изделия, размещенным внутри системного блока ПЭВМ. Системный блок ПЭВМ должен быть опломбирован.

В изделии должны поддерживаться две роли безопасности: *пользователи* и *администраторы СДЗ*.

Администратор СДЗ должен после каждого выпуска обновлений изделия проводить тестирование функций безопасности согласно документу «МБРЦ.468313.001.ПМ. «Программа и методика испытаний. ПАК «Горизонт-ВС».

Для эксплуатации изделия в составе ГИС 1 класса защищенности должны быть проведены исследования технических средств ПЭВМ (в том числе исследования системной программы BIOS) на предмет отсутствия в их реализации аппаратно-программных механизмов, которые могут привести к нарушению правильности функционирования ПЭВМ и изделия или к утечке защищаемой информации. Исследования должны проводиться специализированной организацией с последующей экспертизой в установленном порядке.

Для эксплуатации изделия в составе ГИС 1 класса защищенности должны быть проведены исследования технических средств ПЭВМ (в том числе исследования системной программы BIOS) на предмет отсутствия в их реализации аппаратно-программных механизмов, которые могут привести к нарушению правильности функционирования ПЭВМ и изделия или к утечке защищаемой информации. Исследования должны проводиться специализированной организацией с последующей экспертизой в установленном порядке.

Администратор СДЗ перед началом работы должен установить пароль на BIOS. Пароль должен состоять минимум из 8 символов, и содержать строчные и прописные буквы латинского алфавита, как минимум одну цифру и один специальный символ. Пароль не должен иметь смысловой нагрузки. В случае выхода из строя батареи питания CMOS требуется ее замена и повторная установка пароля, а также повторное опечатывание корпуса. Плановая смена батареи питания CMOS – один раз в 5 лет.

Для сохранения бинарной целостности сертифицированного продукта запрещается устанавливать обновления программных и/или аппаратных компонентов, не прошедшие инспекционный контроль. Прошедшие инспекционный контроль обновления компонентов необходимо получать путем обращения в ООО «Инновационный Центр «БАРРИКАДЫ» по телефону +7(495)120-15-37, e-mail info@gorizont-vs.ru или в письменном виде по адресу: 123022, г. Москва, ул. 2-я Звенигородская, д.13, стр.43 оф. Информацию об обновлениях следует запрашивать не реже, чем один раз в полгода.

В ПАК «Горизонт-ВС» использование режимов «гибернация», «сон» или аналогичных им запрещено.

Для корректной работы АГ необходимо выполнить тестирование всех узлов АГ.

Для штатной работы АГ, необходимо, чтобы все подключенные изделия были в рабочем режиме.

Для поддержания АГ в рабочем состоянии администратор СДЗ должен выполнять следующие действия:

- мониторинг состояния АГ и оперативное реагирование на сбойные ситуации (раздел 5);
- оперативное выполнение функции администрирования пользователей (смена паролей пользователей, блокирование, удаление и регистрация, расчет векторов ИН);
- выполнение генерации и рассылки сменных ключей маскирования согласно регламенту безопасности (не реже одного раза в 90 дней) (см. п. 5);
- выполнение генерации и рассылки ключей аутентификации (не реже одного раза в три года) (см. п. 5);
- оперативное реагирование на факты компрометации носителей ключевой информации, *терминалов, серверов виртуализации* и *АРМ Администратора*.

На каждом *сервере виртуализации* работает специальное программно-аппаратное обеспечение, предназначенное для создания и исполнения виртуальных машин[4] (ВМ), с которыми удаленно через *терминалы* работают пользователи.

Значения максимальные параметров АГ представлены в таблице ниже (Таблица 1).

Таблица 1 – Максимальные параметры АГ (количество):

№, п/п	Группа	Количество
1.	терминалы	100;
2.	серверы	7;
3.	АРМ Администратора	1;
4.	администраторы	3;
5.	пользователи	125;
6.	шлюзы	20.

[4] Виртуальная машина – эмуляция аппаратной среды, сформированной программным способом.

В составе ПАК «Горизонт-ВС» может работать несколько АГ объединенных в «Сеть ПАК «Горизонт-ВС». *Терминалы и серверы виртуализации* из разных АГ взаимодействуют между собой через шлюзы, однако все функции, связанные с администрированием (настройкой параметров) пользователей, осуществляются только в той АГ, в которой данный пользователь зарегистрирован. В качестве шлюзов выступают *АРМ Администратора* других административных групп (Рисунок 1).

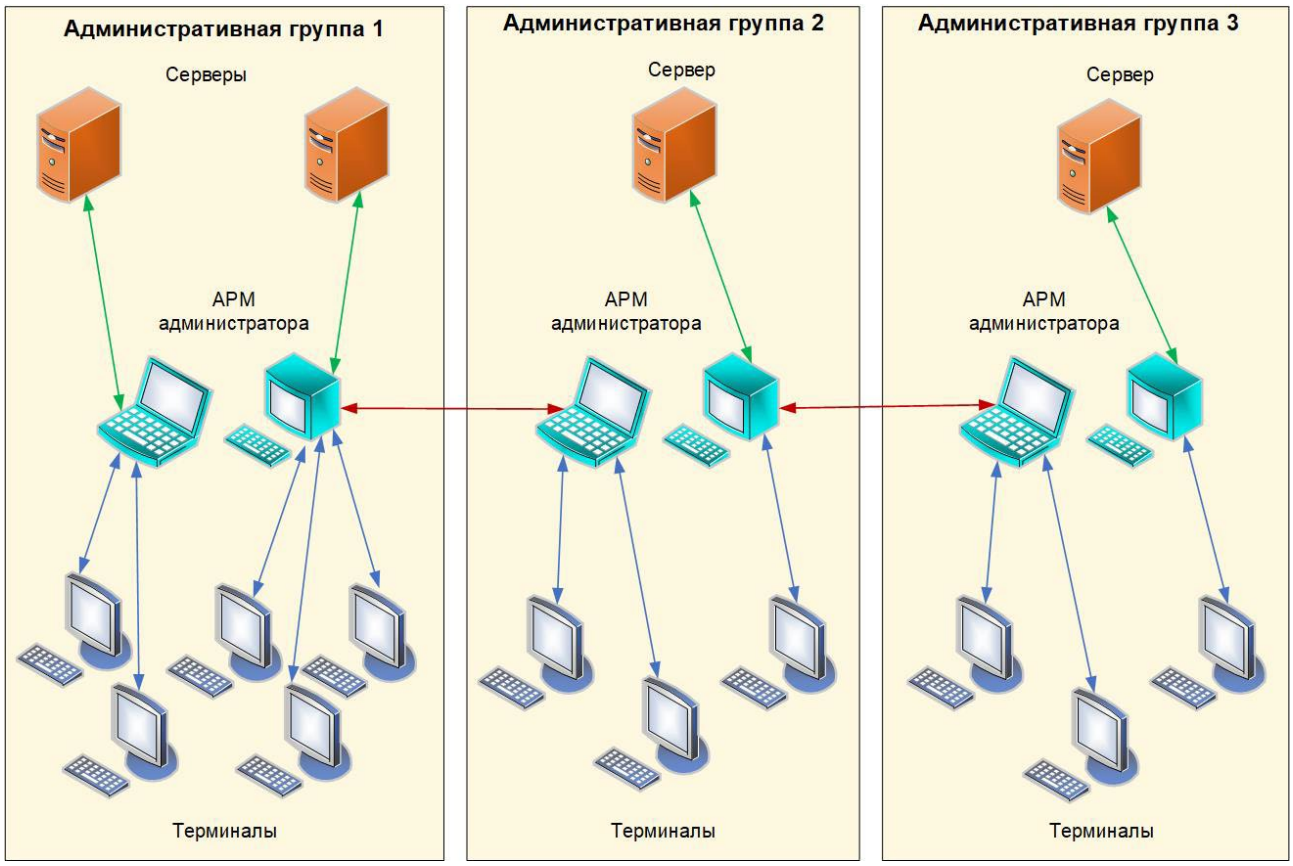

Рисунок 1 – Структура «Сети ПАК «Горизонт-ВС»

Значения максимальных параметров «Сети ПАК «Горизонт-ВС» (количество):

Таблица 2 – Максимальные параметры «Сети ПАК «Горизонт-ВС (количество):

№, п/п	Группа	Количество
1.	административные группы	21
2.	терминалы	2100 (100x21)
3.	серверы	147 (7x21)

4.	пользователи	2625 (125x21)

Функции, связанные с взаимодействием *терминалов* и *серверов виртуализации,* реализованы в комплексе программ «Терминал-Сервер». КП «Терминал-Сервер» является гипервизором, устанавливаемым непосредственно на аппаратное обеспечение в качестве системного программного обеспечения.

Аппаратная поддержка организации защищенного взаимодействия в «Сети ПАК «Горизонт-ВС» реализована с помощью МИиКДС «Шина». МИиКДС «Шина» имеет собственный интерфейс для подключения к локальной вычислительной сети (ЛВС) Ethernet 10/100, что дает возможность организации отдельной IP-сети для выполнения критически важных с точки зрения защищенности операций.

Для защиты данных передаваемых IP-пакетов применяется обратимое, основанное на ключе, маскирование. Этот метод преобразует исходные данные в замаскированное собственное представление, используя основанную на ключе безопасную обратимую функцию маскирования. На приеме данные IP-пакетов преобразуются к исходному значению с использованием того же самого ключа маскирования.

Изделие может использоваться в государственных информационных системах (ГИС) до 1 класса защищенности и для обеспечения защищенности персональных данных в информационных системах персональных данных (ИСПДн) до 1 уровня включительно.

Для пользователя ГИС, в состав которой входит ПАК «Горизонт-ВС», автоматизированным рабочим местом (АРМ) является виртуальная машина. ПАК «Горизонт-ВС» может линейно масштабироваться и поддерживать более 30 000 пользователей VDI в одной инсталляции. Работа пользователя с *терминалом*, через который происходит отображение виртуальной машины, описана в руководстве пользователя МБРЦ.468313.001 Д1. Администратор ГИС осуществляет настройку *сервера виртуализации* и *АРМ администратора*. Через *сервер виртуализации* предоставляется доступ к

виртуальным машинам. Настройка *сервера виртуализации* описана в руководстве администратора МБРЦ.468313.001.ИЗ.02-02.

В ПАК «Горизонт-ВС» отсутствуют механизмы, направленные на ограничение, мониторинг, полное или частичное устранение идентифицированных скрытых каналов. Наличие изолированной среды и полного аудита всех событий в системе исключает возможность создания пользователями каналов, скрытых от систем наблюдения и контроля, обоснование чего приведено в документе «ПАК «Горизонт-ВС». Анализ скрытых каналов МБРЦ.468313.001Д14».

2.2.2 Соответствие политике безопасности организации (ПБО)

Изделие выполняет приведенные ниже правила политики безопасности:

Политика безопасности-1. Изделие должно быть защищено от несанкционированного доступа и нарушений в отношении функций и данных.

Защита от НСД обеспечивается проверкой подлинности предъявленного ЭК аутентификации, пароля пользователя, вводимого с клавиатуры, и ИН. Доступ будет разрешен только владельцам тех ЭК, которые зарегистрированы на данном узле и при условии неизменности контролируемых секторов/файлов на индивидуальном USB-носителе.

Политика безопасности-2. Должно осуществляться управление со стороны администраторов средства доверенной загрузки (СДЗ) режимами выполнения функций безопасности СДЗ.

Для обслуживания АГ используется программа «Администратор МИиКДС» (описание работы программы приведено в п. 4.2). Программа функционирует на *АРМ Администратора* и предназначена для конфигурирования АГ (регистрация и удаление узлов), поддержки списков пользователей в актуальном состоянии (регистрация, удаление и блокировка пользователей) на всех *терминалах* и *серверах виртуализации* (узлах) АГ, генерации ключей маскирования, выполнения операций рассылки и смены ключей, мониторинга АГ, чтения журналов регистрации событий со всех *терминалов* и *серверов виртуализации,* входящих в АГ, подключения шлюзов АГ и установки связи между АГ, входящими в одну серию.

Политика безопасности-3. Управление параметрами СДЗ, которые влияют на выполнение функций безопасности СДЗ, должно осуществляться только администраторами СДЗ.

Управление параметрами СДЗ осуществляется в программе «Администратор МИиКДС», которая функционирует только на *АРМ Администратора*, доступ к которому предоставляется только администратору СДЗ.

Политика безопасности-4. Изделие должно осуществлять проверку (самотестирование) корректности работы механизмов СДЗ и контроль целостности параметров.

Перед загрузкой СДЗ производится самотестирование работы МИиКДС (п. 5.3.2.2). Контроль целостности осуществляется перед каждой загрузкой ПО на *АРМ Администратора, сервере виртуализации* и *терминале* (подробнее о контроле целостности см. п. 5.3.2.3, п.7).

Политика безопасности-5. Должна быть обеспечена невозможность несанкционированной загрузки ОС с нештатных носителей. Также изделие должно быть защищено от несанкционированного доступа и нарушений в отношении функций безопасности.

Изделие осуществляет блокировку загрузки ОС при обнаружении попыток обхода механизмов защиты, при нарушении целостности информации на носителе пользователя запрещается загрузка СПО.

Штатной ОС является операционная система, входящая в состав КП «Терминал-Сервер».

Политика безопасности-6. Должны быть обеспечены надлежащие механизмы регистрации и предупреждения (сигнализации) о любых событиях, относящихся к возможным нарушениям безопасности. Механизмы регистрации должны предоставлять уполномоченным на это администраторам безопасности возможность выборочного ознакомления с информацией о произошедших событиях.

При возникновении событий, относящихся к возможным нарушениям безопасности, осуществляется вывод предупреждающих сообщений на экран, а также регистрация их в журнале регистрации событий.

Журнал регистрации событий предназначен для хранения записей о событиях, регистрируемых изделием, а также предоставления администратору доступа к этим записям. Журнал регистрации событий платы функционирует только на *АРМ Администратора*, доступ к которому предоставляется только администратору СДЗ (подробнее о журнале регистрации событий см. п. 4.2.5). Кроме того, в КП «Терминал-Сервер» работает подсистема аудита, регистрирующая события, связанные с работой виртуальных машин.

Политика безопасности-7. Должна осуществляться проверка (обеспечение) целостности данных СВТ.

Контроль целостности осуществляется перед каждой загрузкой СПО на АРМ Администратора, сервере и терминале (подробнее о контроле целостности п. 4.3).

2.2.3 Соответствие требованиям безопасности для среды информационной технологии

Соответствие изделия требованиям безопасности для среды информационной технологии (ИТ) приведено в таблице ниже (Таблица 3).

Таблица 3 – Соответствие изделия требованиям безопасности для среды ИТ

Идентификатор компонента требований	Название компонента требований	Описание в документации
FAU_SAA.1	Анализ потенциального нарушения	Изделие осуществляет мониторинг всех событий, приведенных в Приложении Д. Накопление событий происходит в Журнале регистрации событий платы МИиКДС «Шина», подробная работа с которым описана в п. 4.2.5. Также события регистрируются подсистемой регистрации событий КП «Терминал-Сервер», команды для работы с которой описаны в части 2 руководстве администратора МБРЦ.468313.001.ИЗ.02-02
FPT_AMT.1	Тестирование абстрактной машины	В состав СПО МИиКДС «Шина» входят три программы тестирования функций безопасности изделия, описанные в приложении И. Также перед загрузкой СДЗ производится самотестирование

Идентификатор компонента требований	Название компонента требований	Описание в документации
		работы МИиКДС (п. 5.3.2.2).
FPT_STM.1	Надежные метки времени	Для получения реального времени в изделии используется микросхема часов реального времени (RTC) − DS1340U-33, работа которой приведена в описании алгоритма функционирования МИиКДС «Шина» МБРЦ.468313.001 Д3. При развертывании и расширении АГ расхождение значений системного времени на ПЭВМ, входящих в АГ, не должно превышать одного часа.

2.2.4 Соответствие предположениям относительно среды

Предположение-1. Должны быть обеспечены условия совместимости изделия с СВТ для реализации своих функциональных возможностей.

Для реализации своих функциональных возможностей изделие должно устанавливаться на ПЭВМ, обладающую характеристиками, приведенными в п. 2.2.1.

Предположение-2. Должны быть обеспечены установка, конфигурирование и управление изделием в соответствии с эксплуатационной документацией.

Изделие должно эксплуатироваться в соответствии с руководством администратора МБРЦ.468313.001 Д2, МБРЦ.468313.001.ИЗ.02-02 и руководством пользователя МБРЦ.468313.001.ИЗ.01. Администратором должны быть выполнены процедуры по развертыванию «Административной группы» в соответствии с МБРЦ.468313.001.ИЗ.02-01.

Предположение-3. Должен быть обеспечен доверенный канал при удаленном управлении изделием и взаимодействии с другими средствами защиты информации и доверенный маршрут при взаимодействии с уполномоченными субъектами.

Описание взаимодействия составных частей изделия приведено в п. 3.2.

Предположение-4. Должна быть обеспечена невозможность осуществления действий, направленных на нарушение физической целостности СВТ, доступ к которым контролируется с применением СДЗ.

Крепление платы МИиКДС в корпусе ПЭВМ должно исключать возможность извлечения данной платы без вскрытия корпуса. Порядок установки платы МИиКДС приведен в приложении к данному документу (ПРИЛОЖЕНИЕ А).

После установки и настройки изделия в обязательном порядке должна быть исключена возможность бесконтрольного доступа к техническим средствам изделия, размещенным внутри системного блока ПЭВМ.

Предположение-5. Должен быть обеспечен надежный источник меток времени для записи событий аудита безопасности СДЗ.

Для получения времени в изделии используется микросхема часов реального времени (RTC) − DS1340U-33. Микросхема DS1340U-33 имеет автономное питание от литиевой батареи CR2032-1GU.

Предположение-6. Должна быть обеспечена ассоциация пользователей с соответствующими атрибутами безопасности (идентификаторы, группы, роли и др.).

В изделии поддерживаются две роли безопасности: пользователи и администраторы СДЗ.

Предположение-7. Должна быть обеспечена синхронизация по времени между компонентами изделия, а также между изделием и средой его функционирования.

При развертывании и расширении АГ расхождение значений системного времени на ПЭВМ, входящих в АГ, не должно превышать одного часа.

Предположение-8. Должна быть обеспечена невозможность отключения (обхода) компонентов изделия.

Изделие осуществляет блокировку загрузки ОС при обнаружении попыток обхода механизмов защиты.

Предположение-9. Персонал, ответственный за функционирование изделия, должен обеспечивать функционирование изделия в соответствии с эксплуатационной документацией.

Изделие должно эксплуатироваться в соответствии с руководством администратора МБРЦ.468313.001.ИЗ.02-01, МБРЦ.468313.001.ИЗ.02-02,

руководством администратора безопасности МБРЦ.468313.001.ИЗ.02-04 и руководством пользователя МБРЦ.468313.001.ИЗ.01.

3 Принципы функционирования МИиКДС «Шина»

3.1 Общие положения

Изделие выполнено в виде платы расширения для IBM PC совместимого компьютера.

В состав изделия входят:

- плата МИиКДС МБРЦ.468243.001 (далее по тексту – плата МИиКДС) и программное обеспечение, которое прошивается в микросхемы платы изделия на этапе изготовления;
- носители ключевой информации - электронные ключи аутентификации администраторов и пользователей, инсталляционный ключ и транспортный ключ;
- устройство для считывания электронных ключей аутентификации - контактное устройство RDS-13 (далее по тексту – считыватель);
- шлейф для гарантированной блокировки работы ПЭВМ со стороны изделия - шлейф блокировки ПЭВМ МБРЦ.685611.001 (далее по тексту - шлейф блокировки ПЭВМ);
- специальное программное обеспечение (СПО) - комплекс программ «Администрирование МИиКДС» RU.МБРЦ.501410.01-01 (далее по тексту – СПО или СПО МИиКДС «Шина»), функционирующий в среде комплекса программ «Терминал-Сервер», который устанавливается на ПЭВМ, выполняющие функции АРМ администратора (компонент 3 согласно формуляру МБРЦ.468313.001 ФО). СПО МИиКДС «Шина» предназначено для работы на *АРМ Администратора.* В состав СПО входят:
  - драйвер. Предназначен для обеспечения взаимодействия СПО с платой изделия;
  - программа администратора. Предназначена для конфигурирования АГ и выполнения операций удаленного администрирования через сетевые интерфейсы, установленные на платах изделия;
  - три программы тестирования функций безопасности изделия.

СПО МИиКДС «Шина» поставляется на индивидуальном USB-носителе (далее по тексту − индивидуальный USB-носитель или ИН).

Изделие взаимодействует с комплексом программ «Терминал-Сервер» из состава ПАК «Горизонт-ВС». Комплекс программ поставляется на индивидуальном
USB-носителе. Работа КП «Терминал-Сервер» подробно описана во второй части руководства администратора МБРЦ.468313.001.ИЗ.02-02.

Примечания:

1 В качестве электронного ключа аутентификации (далее по тексту – электронный ключ или ЭК или ЭК аутентификации) администратора, инсталляционного ключа (далее по тексту – инсталляционный ключ или ИК) и транспортного ключа (далее по тексту – транспортный ключ или ТК) используется устройство DS1977 семейства iButton. В качестве ЭК аутентификации пользователя может использоваться устройство DS1995 семейства iButton. Правила работы с ЭК DS1977 и DS1995 описаны в приложении к настоящему документу (ПРИЛОЖЕНИЕ Б).

2 Индивидуальный USB-носитель с установленным СПО «Терминал-Сервер» должен иметь каждый пользователь, работающий в клиент-серверной системе. СПО загружается с ИН на терминале/сервере при входе пользователя в систему.

3 Индивидуальные USB-носители с установленным СПО МИиКДС «Шина» выдаются только администраторам и предназначены для работы на АРМ Администратора.

3.2 Принципы функционирования

В административной группе, в состав которой входят *терминалы/серверы виртуализации* с установленным изделием, подключенным к отдельной IP-сети, реализована возможность выполнения удаленного администрирования с *АРМ Администратора* всех *терминалов* и *серверов виртуализации*.

Схема обмена управляющими пакетами в рамках АГ представлена на рисунке ниже (Рисунок 2).

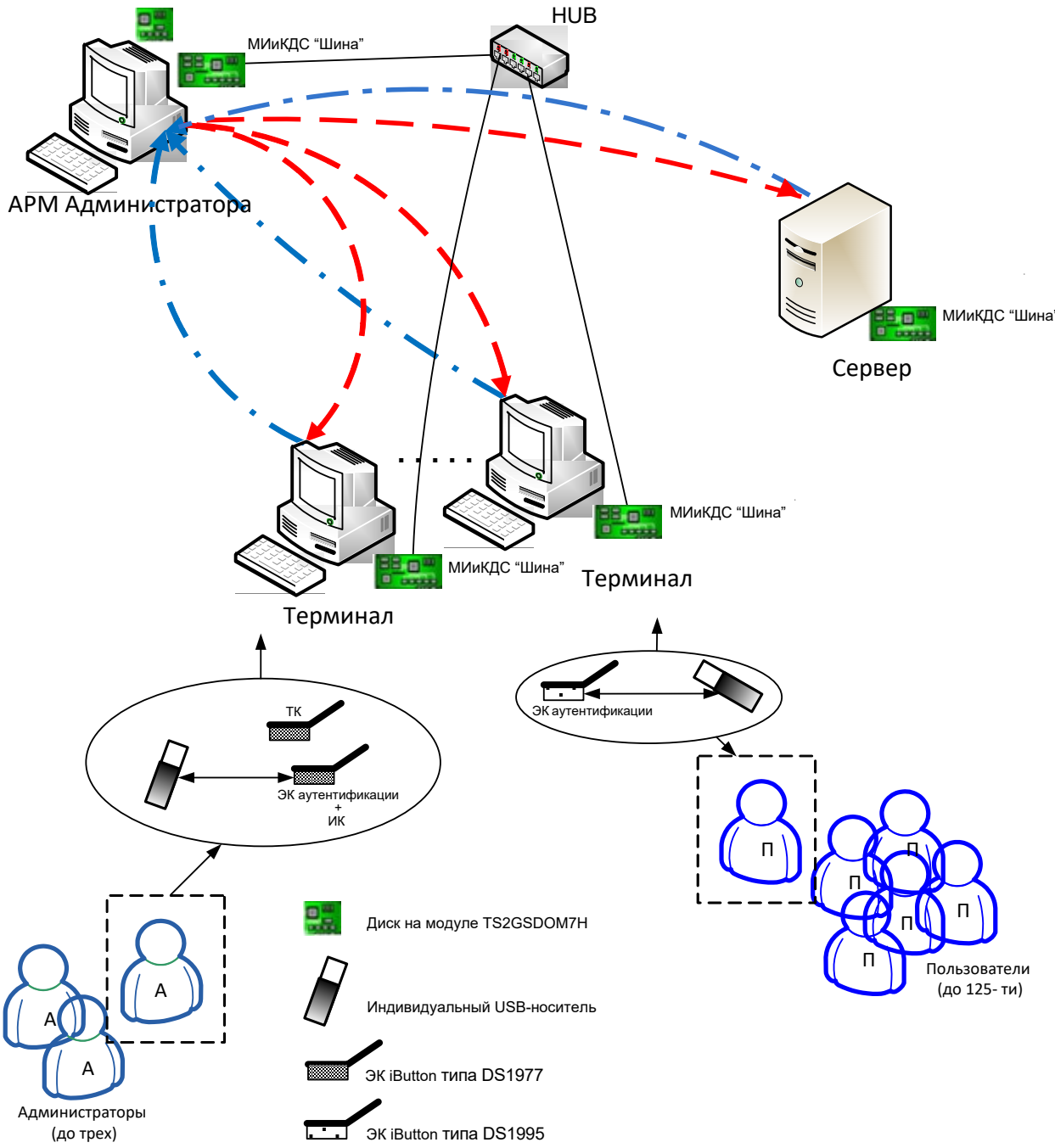

Рисунок 2 – Схема обмена управляющими пакетами в рамках одной АГ

АРМ Администратора, терминал и сервер с установленной платой изделия, подключенной к IP-сети, является узлом сети (далее по тексту – узел).

Каждый узел в составе АГ имеет свой порядковый номер. Максимальное число узлов в АГ **128** (номера от **001** до **128**). Узлом **№ 001** является АРМ Администратора. Остальные номера распределяются между терминалами и серверами, входящими в АГ:

- максимальное количество *серверов* – **7**;
- максимальное количество *терминалов* – **100**;
- максимальное количество зарезервированных шлюзов АГ – **20**.

Каждый узел имеет свой IP-адрес. Обмен данными между изделиями одной АГ осуществляется с помощью маскированных IP-пакетов (управляющих пакетов). Инициатором обмена всегда является АРМ Администратора.

3.3 Работа администратора с установленным МИиКДС «Шина»

Изделие обслуживает администратор средства доверенной загрузки (СДЗ).

На АРМ Администратора может быть создано и зарегистрировано три администратора СДЗ - имена фиксированы (**ADMIN_1**, **ADMIN_2** и **ADMIN_3)** и присваиваются автоматически при создании ЭК и регистрации на АРМ Администратора.

Развертывание административной группы начинается с АРМ Администратора. Первый администратор (**ADMIN_1)** создается при инсталляции изделия на АРМ Администратора (инсталляция выполняется в соответствии с 4.1.3.1 и 4.1.3.2*)*, данный администратор СДЗ является главным - создает и регистрирует еще двух администраторов: **ADMIN_2** и **ADMIN_3**. Первому администратору СДЗ, и только ему, дано право создавать, удалять и блокировать двух других администраторов.

Право выполнять инсталляцию изделий на *терминалах* и *серверах виртуализации*, входящих в АГ, дано всем трем администраторам СДЗ (инсталляция выполняется в соответствии с 4.1.3.1, 4.1.3.3 и 4.1.3.4).

На *АРМ Администратора* администраторы выполняют следующие функции:

- создание ЭК аутентификации, регистрацию пользователей и администраторов (создание второго и третьего администраторов может выполнить только первый администратор);
- работа со списками пользователей, входящих в АГ;
- установка контрольных векторов на индивидуальные USB-носители пользователей/администраторов СДЗ;

- работа с журналом регистрации событий (ЖРС);
- удаленный контроль функционирования изделий, входящих в АГ;
- оперативное управление изделиями в случае возникновения нештатных ситуаций;
- чтение информации о пользователях;
- смена паролей пользователей и администраторов СДЗ;
- администрирование ключей маскирования;
- инициализация изделий.

Для обслуживания АГ и выполнения вышеперечисленных функций используется программа «Администратор МИиКДС». Работа программы подробно описана в разделе 4.2.

4 Подготовка к работе

4.1 Развертывание административной группы

4.1.1 Подготовительная работа

Подготовительная работа для развертывания одной АГ заключается в следующем:

- создание списка *терминалов* и *серверов виртуализации* с «привязкой» их к номерам узлов;
- создание списка пользователей с «привязкой» к узлам (каждый пользователь имеет доступ только к одному узлу);
- определение количества ЭК:
- количество электронных ключей типа DS1995, предназначенных для ЭК аутентификации пользователей;
- количество электронных ключей типа DS1977, предназначенных для ЭК аутентификации администраторов и ЭК транспортного ключа;
- определение количества индивидуальных USB-носителей.

Примечание *– Инсталляционный ключ создается на ЭК аутентификации администратора СДЗ.*

4.1.2 Общая схема развертывания АГ

4.1.2.1 Последовательность действий при развертывании АГ

1) АРМ Администратора:
   а) установка аппаратной части изделия на *АРМ Администратора* (ПРИЛОЖЕНИЕ А);
   б) инсталляция изделия и создание ЭК **ADMIN_1** (см. п 4.1.3.2);
   в) установка даты и времени (см. п 4.2.2.1 и 4.2.2.2);
   г) создание ЭК аутентификации и регистрация **ADMIN_2** и **ADMIN_3** (см. п 4.2.4);
   д) создание ЭК аутентификации пользователей (см. п 4.2.4);
   е) создание ИК на ЭК аутентификации администратора СДЗ, необходимого для выполнения процедуры инсталляции изделий на *серверах виртуализации* и *терминалах* (см. п 4.1.3.2.4, 4.2.2.1).

ж) если необходима связь с другими АГ одной серии – создание ТК (см. п 4.2.2.1);

з) подсчет контрольных сумм (установка векторов) на ИН администраторов СДЗ и пользователей;

2) Серверы виртуализации и терминалы:

а) установка аппаратной части изделия на *терминалах* и *серверах виртуализации* (ПРИЛОЖЕНИЕ А);

б) инсталляция платы изделия на *терминалах* и *серверах виртуализации* и перевод их в режим **Удаленное управление**.

3) АРМ Администратора:

а) проверка связи между *АРМ Администратора* и проинсталлированными *терминалами* и *серверами виртуализации* (см. п 4.2.2.3);

б) установка даты и времени на терминалах и серверах виртуализации (см. п 4.2.2.2);

в) выполнение сетевых настроек плат МИиКДС, установленных на *терминалах*, *серверах виртуализации* и *АРМ Администратора* (см. п 4.2.3);

г) назначение каждому пользователю доступного ему *терминала* (узла) из сформированного списка (см. п 4.2.4).

Внимание: *при развертывании и расширении АГ расхождение значений системного времени на ПЭВМ, входящих в АГ, не должно превышать одного часа.*

4.1.2.2 Поддержка списков пользователей в актуальном состоянии

Список пользователей АГ формируется на *АРМ Администратора* при выполнении операции создания ЭК аутентификации (см. п 4.2.4). Позиция в списке пользователей соответствует идентификационному номеру пользователя/администратора в АГ.

В том случае, если происходит корректировка списка на *АРМ Администратора* (пользователя/администратора СДЗ удалили из списка), то данный пользователь/администратор СДЗ автоматически удаляется (блокируется) на *терминале*/всех узлах, на которых он был зарегистрирован.

Контроль ЭК аутентификации происходит по имени пользователя/администратора СДЗ, серийному номеру ЭК, идентификационному номеру в АГ и уникальной идентификационной информации.

4.1.3 Инсталляция МИиКДС «Шина»

4.1.3.1 Общие положения

Инсталляция МИиКДС «Шина» заключается в инсталляции платы МИиКДС.

Изделие работает в трех режимах: **АРМ Администратора**, **Терминал**, **Сервер**. Установка режима выполняется на этапе инсталляции путем ввода *сервисного кода*. *Сервисные коды* поставляются на объект эксплуатации установленным порядком отдельно от изделий.

Процедура инсталляции выполняется при первом включении ПЭВМ после установки платы изделия в соответствии с приложением А.

Примечание *– Так как СПО поставляется на USB-носителе, то, при необходимости, перед началом работы с платой изделия выполнить настройку системного BIOS, в части представления USB-носителя в качестве загрузочного жесткого магнитного диска (ЖМД) (пример настройки BIOS дан в приложении А(А.4)).*

Внимание: *перед включением ПЭВМ USB-носитель с СПО необходимо установить в USB-порт.*

Включить ПЭВМ – на экран выводится диалоговое окно (Рисунок 3).

Рисунок 3 – Диалоговое окно изделия

В данное окно необходимо ввести сервисный код, который определяет режим, в котором будет работать плата (**AADMIN** – АРМ Администратора**,** **SERVER** – сервер виртуализации**,** **TERMIN** – терминал), и нажать клавишу **Enter**.

После ввода сервисного кода в изделии устанавливается соответствующий режим работы и продолжается инсталляция.

На экран монитора в статусную строку выдается следующие сообщения:

1. **Введите номер группы.** Необходимо ввести номер АГ и нажать клавишу **Enter**.
2. **Введите номер узла**. Необходимо ввести номер узла в АГ и нажать клавишу **Enter**. Введенный номер узла должен соответствовать введенному сервисному коду:

   Нумерация изделий в АГ (или группе) – **SS-GG-NNN**,

   где

   SS – номер серии (от **001** до **099**) (задается при прошивке);

   GG – номер группы (от **001** до **021**) (задается при инсталляции);

   NNN – номер узла внутри группы (от **001** до **128**):

   001 – номер узла *АРМ Администратора* (задается на предприятии-изготовителе);

   002 – **021** – шлюзы групп – зарезервированные узлы для шлюзов, через которые выполняется подключение к другим АГ в рамках одной серии (в качестве шлюза АГ используется *АРМ Администратора* подключаемой АГ).

   022 – **028** – диапазон номеров узлов *серверов виртуализации* (номер задается при инсталляции платы МИиКДС);

   029 – **128** – диапазон номеров узлов *терминалов* (номер задается при инсталляции платы МИиКДС).

   В том случае, если информация на этом этапе введена правильно, то выполняется переход, в соответствии с *сервисным кодом*, к инсталляции *АРМ Администратора* или *терминала* или *сервера виртуализации*.

Сообщения о возможных ошибках:

При неправильном вводе сервисного кода выдаются сообщения:

1. **Неправильный сервисный код**. Данное сообщение выдается при неправильном вводе сервисного кода.
2. **Некорректный номер группы.** Данное сообщение появляется при вводе номера группы, не входящего в диапазон выделенных номеров.
3. **Некорректный номер узла.** Данное сообщение появляется при несоответствии сервисного кода и номеру узла из диапазона выделенных номеров.

На данные сообщения необходимо нажать клавишу **Enter** и повторить ввод информации. Полный список сообщений, выдаваемых в статусной строке при инсталляции и аутентификации, приведен в приложении к настоящему документу (ПРИЛОЖЕНИЕ В).

4.1.3.2 АРМ Администратора

4.1.3.2.1 Инсталляция платы изделия на АРМ Администратора

Если при инсталляции платы, предназначенной для работы на *АРМ Администратора,* введен сервисный код, соответствующие режиму работы *АРМ Администратора* (4.1.3.1), то выполняется переход ко второму этапу процесса инсталляции платы и на экран выводится диалоговое окно изделия (Рисунок 4).

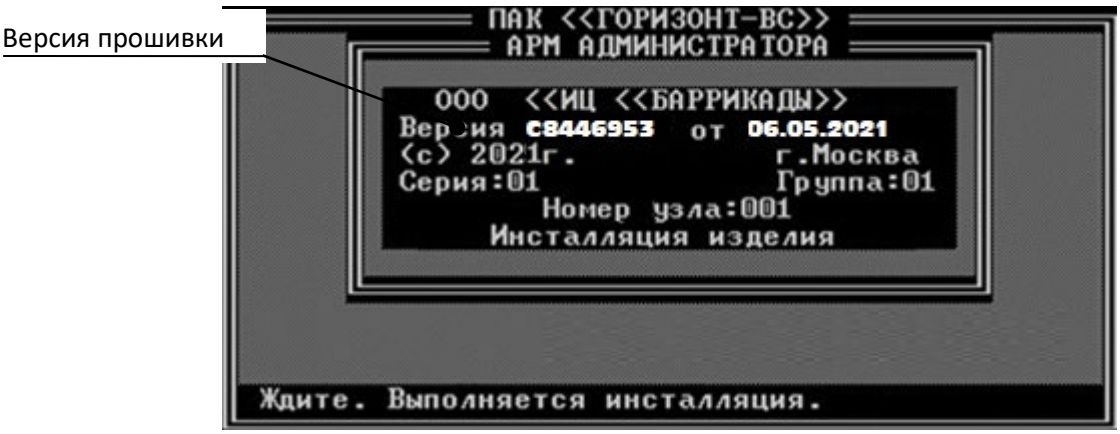

Рисунок 4 – Окно АРМ Администратора – инсталляция

Примечание *– В данном окне текущая версия прошивки должна совпадать с контрольной суммой версии прошивки, приведенной в паспорте на изделие*

МИиКДС «Шина» МБРЦ.468264.001 ПС. Данные контрольные суммы должны совпадать.

Через некоторое время в статусную строку выдаются сообщения:

1. **Установите ЭК и нажмите Enter**. Необходимо установить ЭК DS1977 в считыватель и нажать клавишу **Enter**.
2. **ЭК не установлен**. Данное сообщение выводится в статусную строку в том случае, если не удалось прочитать ЭК или ЭК не является DS1977

Если ЭК установлен правильно, то в строку ввода сообщения:

3. **Введите пароль:……..** Необходимо ввести пароль, а затем, для подтверждения пароля, еще раз ввести его в строку ввода сообщения:
4. **Повторите пароль:……..**

Пароль должен соответствовать следующим характеристикам:

- длина пароля – **8** символов;
- в пароле обязательно должны присутствовать символы из следующих категорий:
  - прописные буквы английского алфавита от A до Z;
  - строчные буквы английского алфавита от a до z;
  - десятичные цифры от 0 до 9;
  - специальные символы, не принадлежащие алфавитно-цифровому набору (например, *_@);
- в пароле должны отсутствовать повторяющиеся символы;
- пароль не должен иметь смысловой нагрузки.

Если какой-либо символ введен неверно, то его можно стереть (клавиша **BackSpace**) и повторить ввод.

5. **Ждите. Выполняется регистрация.** Данное сообщение появляется после ввода пароля.
6. **Успешная инсталляция.** Данное сообщение появляется после совпадения пароля. На это сообщение необходимо нажать клавишу **Enter** – будет выполнен переход к процедуре аутентификации (см. п. 4.1.3.2.2).

При успешной инсталляции платы на *АРМ Администратора* создается ЭК аутентификации первого администратора СДЗ (**ADMIN_1**). Введенный

пароль связан с установленным ЭК (ЭК аутентификации) и в дальнейшем будет использоваться администратором СДЗ при прохождении процедуры аутентификации при входе в систему.

Для дальнейшей работы первому администратору СДЗ необходимо пройти процедуру аутентификации, выполнить установку векторов на СПО, создать второго и третьего администратора СДЗ и инсталляционный ключ, который необходим при инсталляции изделий на *терминалах* и *серверах виртуализации*, входящих в АГ.

4.1.3.2.2 Процедура аутентификации на АРМ Администратора

Процедура аутентификации на *АРМ Администратора* начинается с тестирования платы и при успешном завершении процесса тестирования на экран выводится диалоговое окно изделия (Рисунок 5).

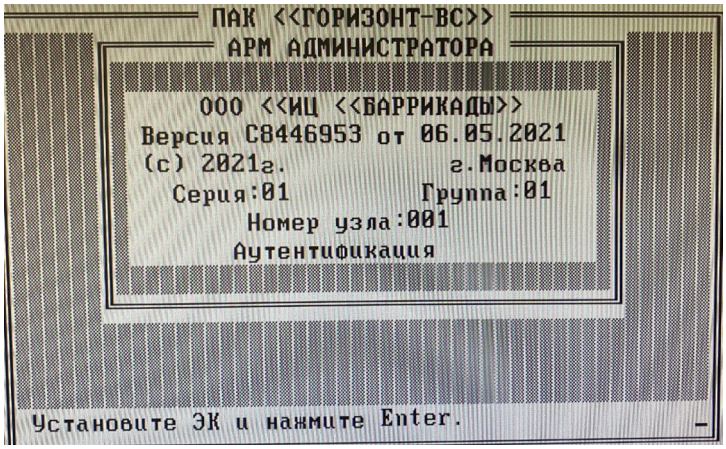

Рисунок 5 – Окно АРМ Администратора – аутентификация

В статусную строку выдается сообщения:

1. **Установите ЭК и нажмите Enter.** Необходимо установить в считыватель (если не установлен) ЭК аутентификации **ADMIN_1** и нажать клавишу **Enter** - выдается сообщение:
2. **Введите пароль:……..**На данное сообщение необходимо ввести пароль администратора СДЗ.
3. **Ждите. Идет аутентификация.**
4. **Успешная аутентификация.** Данное сообщение появляется при успешной аутентификации. Нажать клавишу **Enter.**
5. **Уберите ЭК из считывателя и нажмите Enter.** Необходимо извлечь ЭК аутентификации из считывателя, нажать клавишу **Enter** - далее

произойдет возврат управления системному BIOS, который через некоторое время (на экране стирается окно ПАК «Горизонт-ВС») вызовет процедуру установки векторов (расчет эталонных значений контрольных сумм) СПО на установленном носителе (индивидуальном USB-носителе) (см. п. 4.1.3.2.3, Рисунок 6).

4.1.3.2.3 Процедура установки контрольных векторов на АРМ Администратора

Контроль целостности осуществляется перед каждой загрузкой СПО на *АРМ Администратора, сервере виртуализации* и *терминале.* Для успешного выполнения данного требования на *АРМ Администратора* необходимо выполнить расчет эталонных значений контрольных сумм всех используемых в АГ носителей СПО.

Во время инсталляции платы изделия на *АРМ Администратора* рекомендуется выполнить установку векторов для носителя СПО **ADMIN_1** (носитель СПО должен быть установлен перед включением ПЭВМ).

Процедура расчета эталонных значений контрольных сумм начинается после успешной аутентификации с вывода на экран в окно **Контроль целостности** запроса на выполнение установки векторов после успешной аутентификации (Рисунок 6).

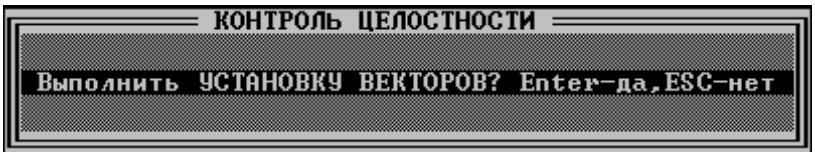

Рисунок 6 – Окно Контроль целостности

Для выполнения процедуры установки векторов необходимо нажать клавишу **Enter**, для отказа от установки векторов и для перехода к процедуре контроля целостности носителя СПО необходимо нажать клавишу **Esc**.

Установка векторов

В окне **Контроль целостности** (Рисунок 6) нажать клавишу **Enter** - на экран выдается сообщение:

1. **Установите ЭК и нажмите Enter.** Необходимо установить ЭК аутентификации администратора СДЗ/пользователя (в данном случае,

ЭК аутентификации **ADMIN_1**), для носителя СПО, который был установлен в ПЭВМ перед включение питания, и нажать клавишу **Enter**.

Внимание:

1 на этапе изготовления плат изделия на предприятии-изготовителе устанавливается режим контроля целостности: посекторный или файловый. Режим контроля на плате изделия, установленной на арм администратора должен распространяться на все платы, входящие в аг. При разных режимах на платах контроль целостности будет выполняться с ошибками.

2 администратор СДЗ должен выполнить установку векторов для всех ин, задействованных в АГ.

В том случае, если на плате изделия установлен режим – **посекторный** контроль - активизируется посекторный подсчет контрольных сумм информации на носителе и в окно **КОНТРОЛЬ ЦЕЛОСТНОСТИ** выдается сообщение:

2. **УСТАНОВКА ВЕКТОРОВ XXXXXX**, где **XXXXXX** – текущее значение сектора.
3. **<имя файла> YYYYYY**. Выдается сообщение в том случае, если на плате изделия установлен режим – файловый контроль, где

   <имя файла> – имя проверяемого файла;

   YYYYYY – текущее значение кластера данных.

В режиме **файловый** контролируется пять системных файлов: LDLINUX.C32, KERNEL, LDLINUX.SYS, SYSLINUX.CFG, ROOTFS.

4. **Выполните перезагрузку.** Данное сообщение выдается по окончании процесса. При успешном завершении процедуры установки векторов результат сохраняется в энергонезависимой памяти (ЭНП) платы изделия.

Контроль векторов

После перезагрузки и успешной аутентификации, при выводе на экран окна **КОНТРОЛЬ ЦЕЛОСТНОСТИ** (рисунок 6), необходимо нажать клавишу **Esc** – произойдет переход к процедуре контроля целостности информации на установленном носителе, и на экран выдается сообщение:

5. **КОНТРОЛЬ ВЕКТОРОВ XXXXXX** или **<ИМЯ ФАЙЛА> YYYYYY**

В том случае, если целостность носителя не нарушена, то выполняется загрузка СПО.

6. **Ошибка при КОНТРОЛЕ ВЕКТОРОВ** или **<имя файла> ERR.** Данное сообщение выдается, если целостность носителя нарушена. Необходимо нажать клавишу **Enter**
7. **Ошибка при КОНТРОЛЕ ВЕКТОРОВ.** Для продолжения процесса нажать клавишу **Enter** - произойдет переход к загрузке СПО.

Примечание *– Подсистема контроля целостности работает в* ***жестком*** *режиме, т.е. при нарушении целостности информации на носителе пользователя запрещается загрузка СПО. При нарушении целостности информации на носителе администратора СДЗ загрузка СПО разрешена. Сообщения о нарушении целостности носителя заносятся в ЖРС.*

4.1.3.2.4 Создание инсталляционного ключа

ИК используется при конфигурировании АГ. С помощью данного ключа выполняется инсталляция плат МИиКДС на *терминалах и серверах виртуализации* в соответствии с п. 4.1.3.1, 4.1.3.3 и 4.1.3.4.

Право выполнять инсталляцию изделий на *терминалах* и *серверах виртуализации*, входящих в АГ, дано всем трем администраторам СДЗ.

Примечание *– Инсталляционный ключ при создании записывается на ЭК аутентификации администратора СДЗ.*

Создание администраторов СДЗ (второго и третьего) и инсталляционного ключа выполняется с помощью программы «Администратор МИиКДС» в среде КП «Терминал-Сервер». Программа предназначена для обслуживания подсистемы администрирования АГ. Подробное описание работы и функций программы дано в разделе 4.2. В данном разделе описана только последовательность процедуры создания ИК на ЭК аутентификации первого администратора (**ADMIN_1)**.

После успешной аутентификации, контроля целостности и загрузки ОС необходимо запустить программу «Администратор МИиКДС». Для ее запуска необходимо на рабочем столе выбрать пункт главного меню **Средство администрирования АПМДЗ**, нажать левую клавишу манипулятора типа «мышь» (далее по тексту - «мышь») и выполнить следующие действия:

1. Открыть вкладку программы **Администрирование группы** и установить дату и время (кнопка **Установить дату и время** в поле **Локальные операции**) в соответствии с 4.2.2. Дата и время устанавливается на узле **№001**.
2. Открыть вкладку программы **Сетевые настройки** и откорректировать таблицу **Сетевые интерфейсы плат** в соответствии с конфигурацией АГ (см. п. 4.2.3).
3. Вкладка программы **Администрирование группы** – создать ИК (кнопка **Создать инсталляционный ЭК**) (см. п. 4.2.2).

После создания ИК можно перейти к процедуре инсталляции *терминалов* и *серверов виртуализации*.

4.1.3.3 Инсталляция платы изделия на *терминале*

В том случае, если при инсталляции введены сервисный код, соответствующий режиму **Терминал** (см. п. 4.1.3.1), то выполняется переход ко второму этапу процесса инсталляции платы, и на экран выводится диалоговое окно изделия (Рисунок 7).

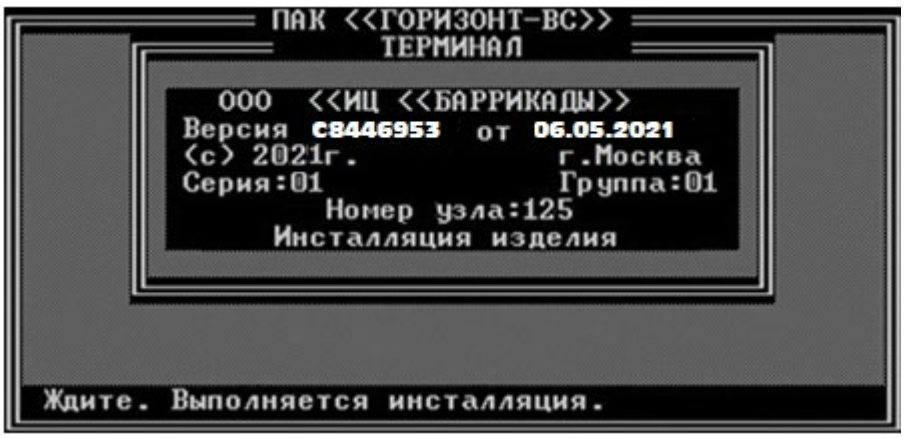

Рисунок 7 – Окно *терминала* - инсталляция

Через некоторое время в статусную строку будут появляться сообщения:

1. **Установите ИК и нажмите Enter.** Нужно установить ЭК аутентификации администратора, на котором был создан инсталляционный ключ, и нажать клавишу **Enter**.
2. **Неправильный формат ИК.** Данное сообщение появляется в том случае, если не удалось прочитать ИК (неправильный формат или не

был записан ИК). Необходимо установить правильный ЭК и нажать клавишу **Enter**.

3. **Введите пароль:……..**Данное сообщение выдается, если введен правильный формат ИК. Нужно ввести пароль аутентификации администратора СДЗ, соответствующий установленному ЭК.
4. **Неправильный пароль или ЭК.** Данное сообщение появляется в статусной строке том случае, если при вводе пароля допущена ошибка (неудачная попытка входа).

В ответ на это сообщение нажать клавишу Enter и повторить процедуру ввода пароля.

После успешного ввода пароля в статусную строку выдается сообщение:

5. **Ждите. Выполняется регистрация**. Данное сообщение появляется в статусной строке после успешного ввода пароля.
6. **Успешная инсталляция.** Данное сообщение выдается через некоторое время в статусную строку, если пароль введен правильно.
7. **Уберите ЭК из считывателя и нажмите Enter**. Данное сообщение появляется в статусной строке при нажатии клавиши **Enter.** Необходимо извлечь ЭК аутентификации из считывателя и нажать клавишу **Enter** - далее произойдет переход к выбору режима (Рисунок 8):

– по клавише **Esc** – переход к установке или контролю векторов СПО на установленном носителе, действия аналогичны описанным в 4.1.3.2.3;
– по клавише **Enter** – переход в режим удаленного управления (Рисунок 9).

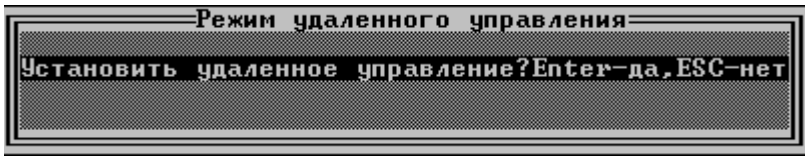

Рисунок 8 – Окно выбора режима

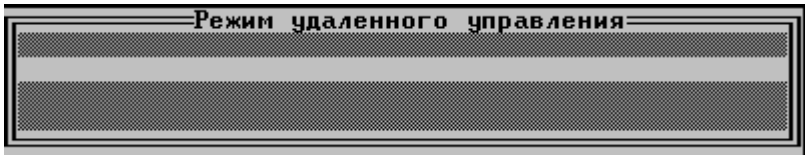

Рисунок 9 – Окно режима удаленного управления

При развертывании АГ рекомендуется в режим *удаленного управления* перевести все *терминалы* и *серверы виртуализации* – это необходимо для активации узлов в списке АГ на *АРМ Администратора* (см. п. 4.1.4).

В режим *удаленного управления терминалы* и *серверы виртуализации* могут быть переведены:

- при выполнении процедуры инсталляции изделия;
- после успешной аутентификации администратора СДЗ на *терминале/сервере виртуализации*.

4.1.3.4 Инсталляция платы изделия на *сервере виртуализации*

В том случае, если при инсталляции введены сервисный код, соответствующий режиму **Сервер**, номер группы и узла (см. п. 4.1.3.1), то выполняется переход ко второй стадии процесса инсталляции платы и на экран выводится диалоговое окно изделия (Рисунок 10).

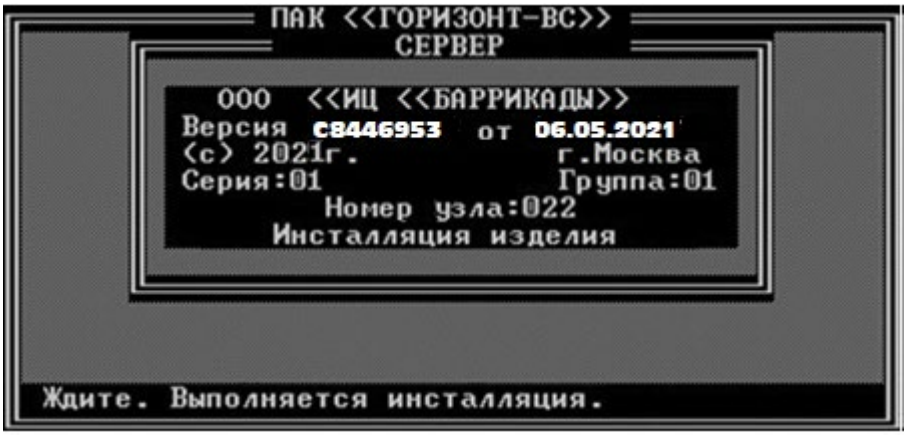

Рисунок 10 – Окно *сервера виртуализации* - инсталляция

Инсталляция аналогична инсталляции платы на *терминале* (4.1.3.3).

Серверы виртуализации также как и *терминалы* необходимо перевести в режим *удаленного управления*.

4.1.4 Активация узлов

Для выполнения процедуры активации узлов (включение в список текущей АГ *терминалов* и *серверов*) необходимо на *АРМ Администратора* запустить программу «Администратор МИиКДС». Описание программы дано в разделе 4.2.

Внимание: *на терминале/сервере виртуализации, для которого будет выполняться процедура включения в список АГ, должна успешно завершиться процедура аутентификации администратора СДЗ, и плата изделия должна быть переведена в режим* ***удаленного управления*** *или, после прохождения процедуры контроля векторов, выполнена загрузка ос (режим работы ОС).*

В окне программы выбрать вкладку **Администрирование группы** (Рисунок 11), в списке узлов (Рисунок 12) выбрать необходимые для активации узлы, в области окна **Удаленные операции** нажать кнопку **Добавить в административную группу** и дождаться успешного завершения операции.

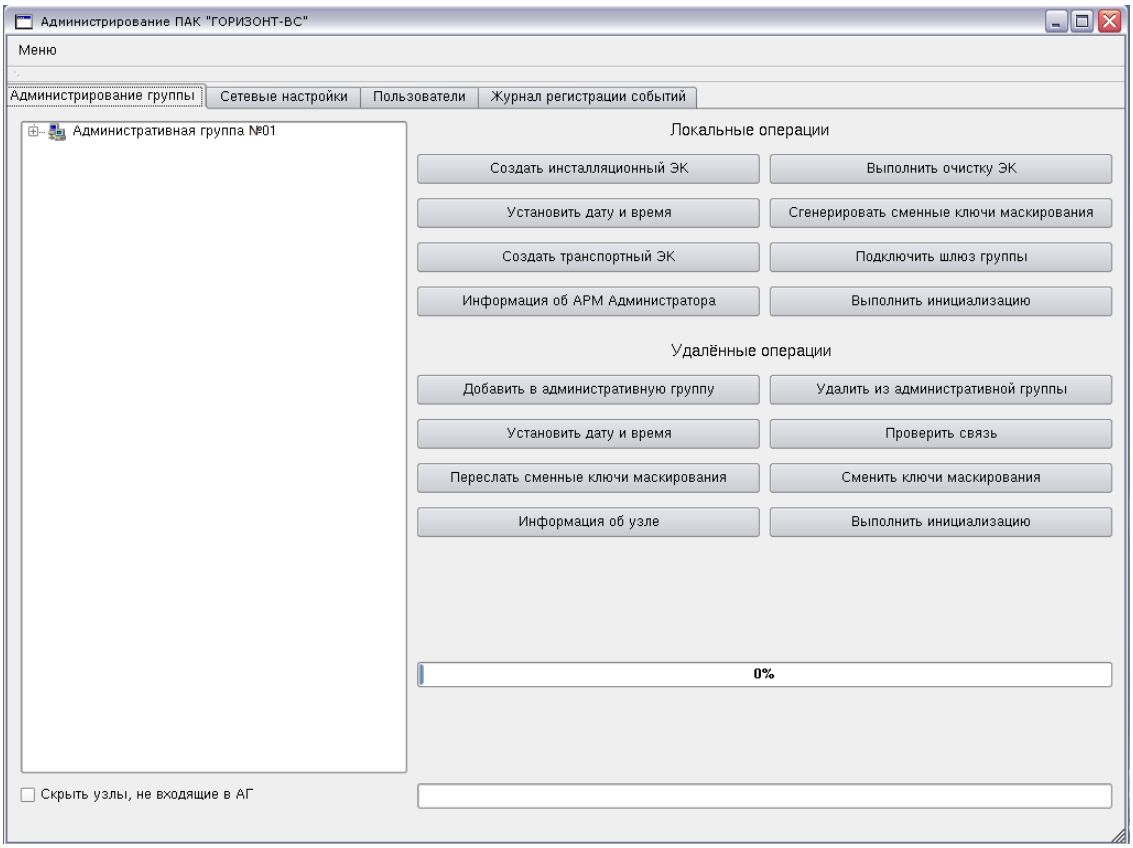

Рисунок 11 – Вкладка Администрирование группы

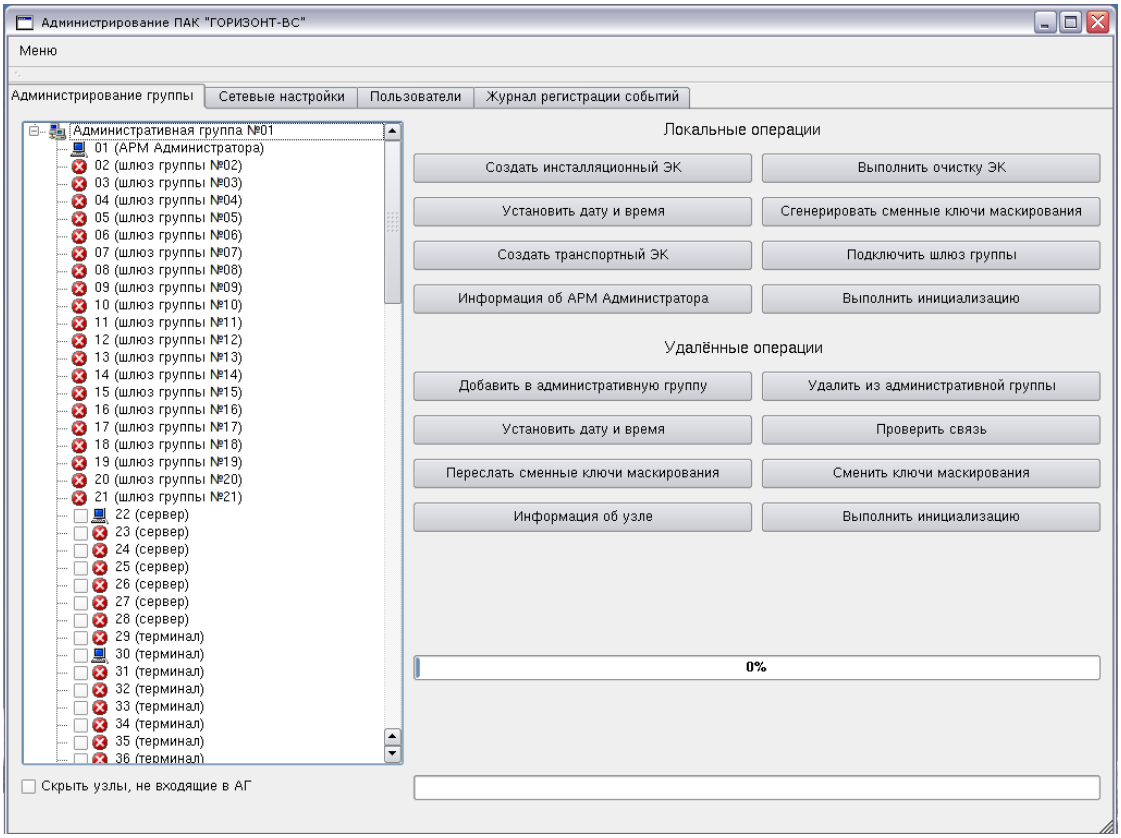

Рисунок 12 – Список узлов административной группы

При успешном добавлении узла в АГ его пиктограмма изменится с  на  .

4.2 Программа администратора

Для обслуживания АГ используется программа «Администратор МИиКДС».

Программа функционирует на *АРМ Администратора* (узел **№001**) и предназначена для конфигурирования АГ (регистрация и удаление узлов), поддержки списков пользователей в актуальном состоянии (регистрация, удаление и блокировка пользователей) на всех *терминалах* и *серверах виртуализации* (узлах) АГ, генерации ключей маскирования, выполнения операций рассылки и смены ключей, мониторинга АГ, чтения журналов регистрации событий со всех *терминалов* и *серверов виртуализации,* входящих в АГ, подключения шлюзов АГ и установки связи между АГ, входящими в одну серию.

Управление АГ выполняется через сетевые интерфейсы, установленные на платах изделия.

4.2.1 Основное окно программы

После включения *АРМ Администратора*, успешной аутентификации и загрузки ОС необходимо запустить программу «Администратор МИиКДС» (далее по тексту – программа или программа администратора). Программа функционирует в среде КП «Терминал-Сервер». Для ее запуска необходимо на рабочем столе выбрать пункт главного меню **Средство администрирования АПМДЗ** и нажать левую клавишу «мыши».

При запуске программы на экран выводится основное окно программы (Рисунок 13).

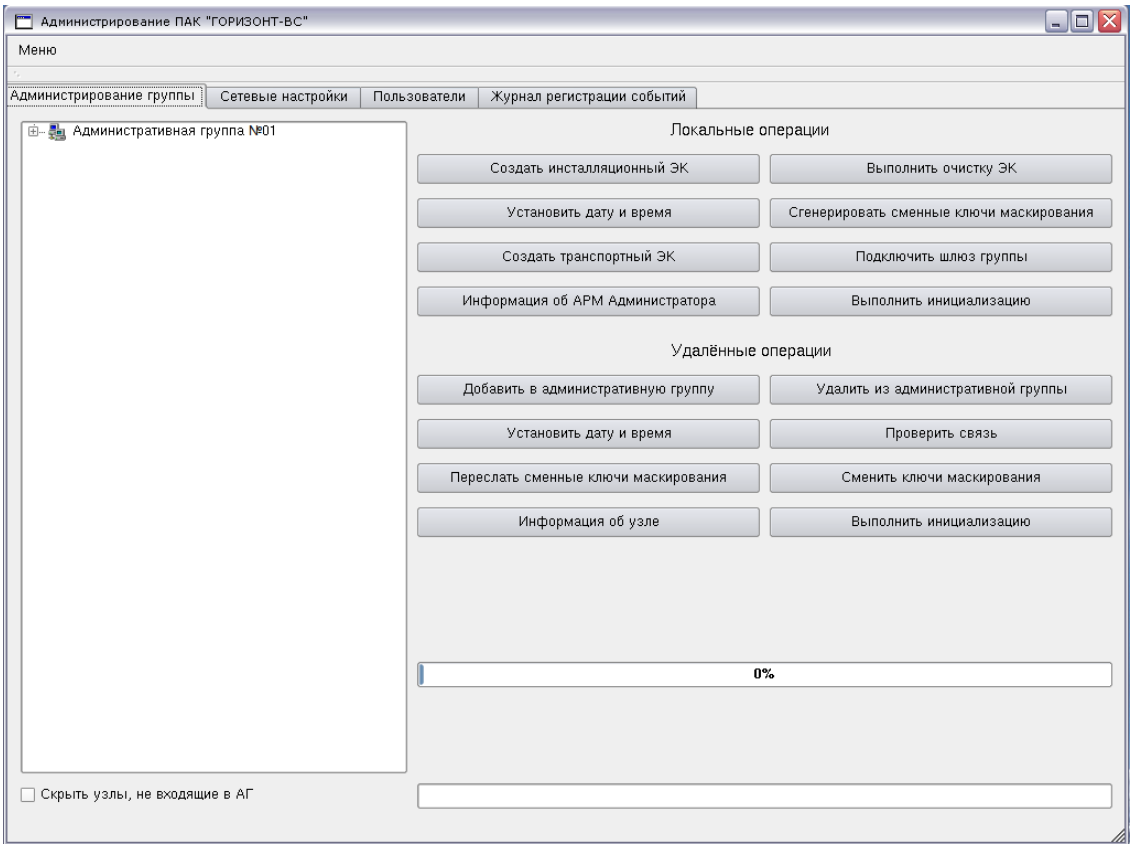

Рисунок 13 – Основное окно программы

В данном окне, используя различные вкладки, администратор СДЗ выполняет операции администрирования АГ.

Вкладка **Администрирование группы** предназначена для работы со списком узлов, входящих в АГ. Данная вкладка позволяет: добавлять/удалять узлы в АГ, генерировать, рассылать и выполнять смену ключей маскирования, выполнять процедуру инициализации изделий (см. п. 4.2.2).

Вкладка **Сетевые настройки** предназначена для управления сетевыми настройками узлов АГ (см. п. 4.2.3).

Вкладка **Пользователи** предназначена для работы со списком пользователей: вводить новых пользователей и администраторов СДЗ. Данная вкладка позволяет: удалять из списка, выполнять блокировку и разблокировку пользователей на узлах, выполнять смену их паролей (см. п. 4.2.4).

Вкладка **Журнал регистрации событий** предназначена для работы с журналом регистрации событий. Данная вкладка позволяет: просматривать журнал регистрации событий каждого узла, входящего в АГ, очищать его и сохранять в файле (см. п. 4.2.5).

С помощью программы выполняются операции, как для отдельного узла, так и групповые операции для всех зарегистрированных узлов.

К групповым операциям относятся:

- рассылка сменных ключей маскирования в узлы АГ (вкладка **Администрирование группы**);
- смена ключей маскирования на всех узлах АГ (во вкладке **Администрирование группы**);
- смена пароля пользователя (во вкладке **Пользователи**);
- исключение пользователя из списка пользователей АГ.

Информация о выполнении групповых операций хранится в журнале групповых операций (файл ***group_log.txt*** в каталоге ***/root***). Структура журнала приведена в приложении к настоящему документу приложении (ПРИЛОЖЕНИЕ Е).

***Примечания**:*

1. При выполнении групповых операций с узлами изменяется статус узла только в том случае, если операция на узле выполнена успешно (пиктограмма *в списке узлов АГ, изменяется на пиктограмму*  *). Результат выполнения групповых операций после закрытия программы стирается, но автоматически сохраняется в журнале групповых операций.*

2. При выполнении операций с отдельными узлами пиктограмма  *изменяется в соответствии с выполненной операцией и только в том случае,*

если данная операция на узле выполнена успешно. Результат выполнения операций после закрытия программы стирается.

Список сообщений, выдаваемых программой, приведен в приложении к настоящему документу (ПРИЛОЖЕНИЕ Г).

4.2.2 Администрирование группы

Для управления АГ используется вкладка **Администрирование группы** (Рисунок 14).

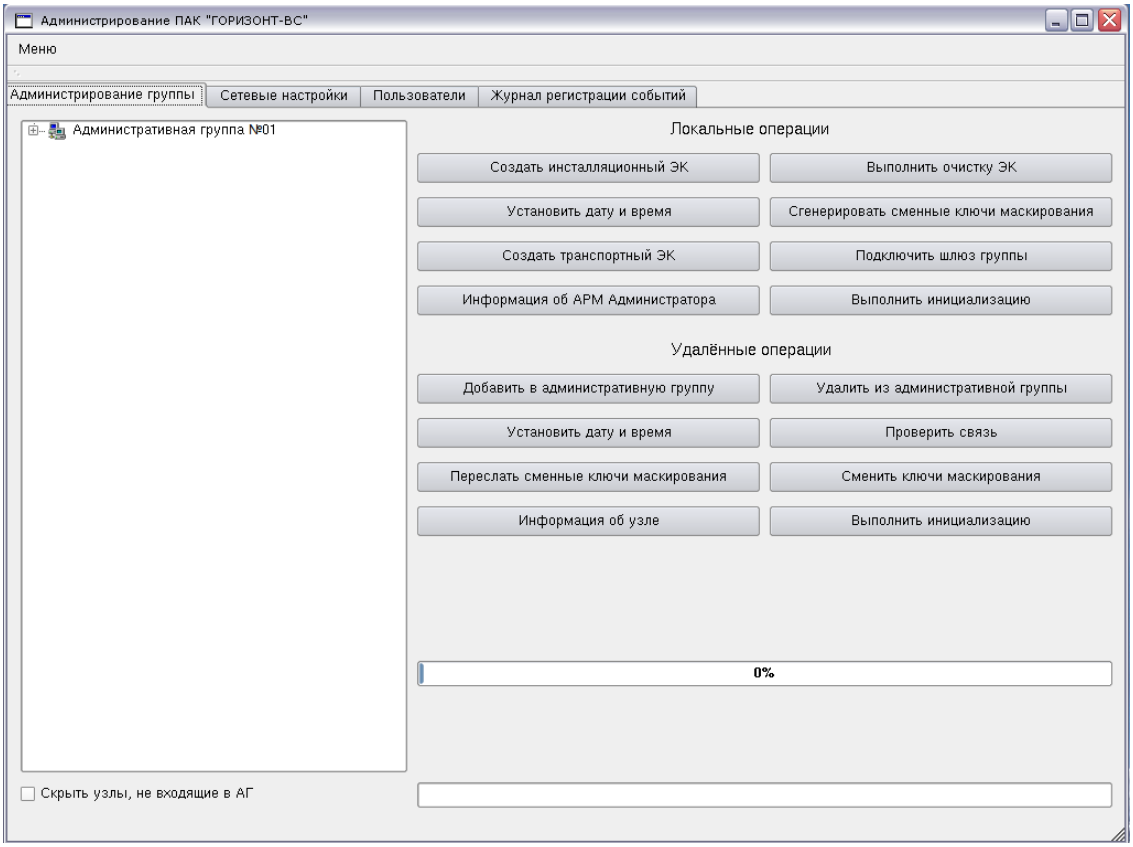

Рисунок 14 – Вкладка «Администрирование группы»

В левой части окна выводится список узлов, входящих в АГ, в виде дерева объектов. Для просмотра списка узлов АГ, необходимо щелкнуть левой клавишей «мыши», наведя курсор на значок ⊞, расположенный слева от объекта (Рисунок 14). В окне появится список узлов с пиктограммами, показывающими их статус (Рисунок 15).

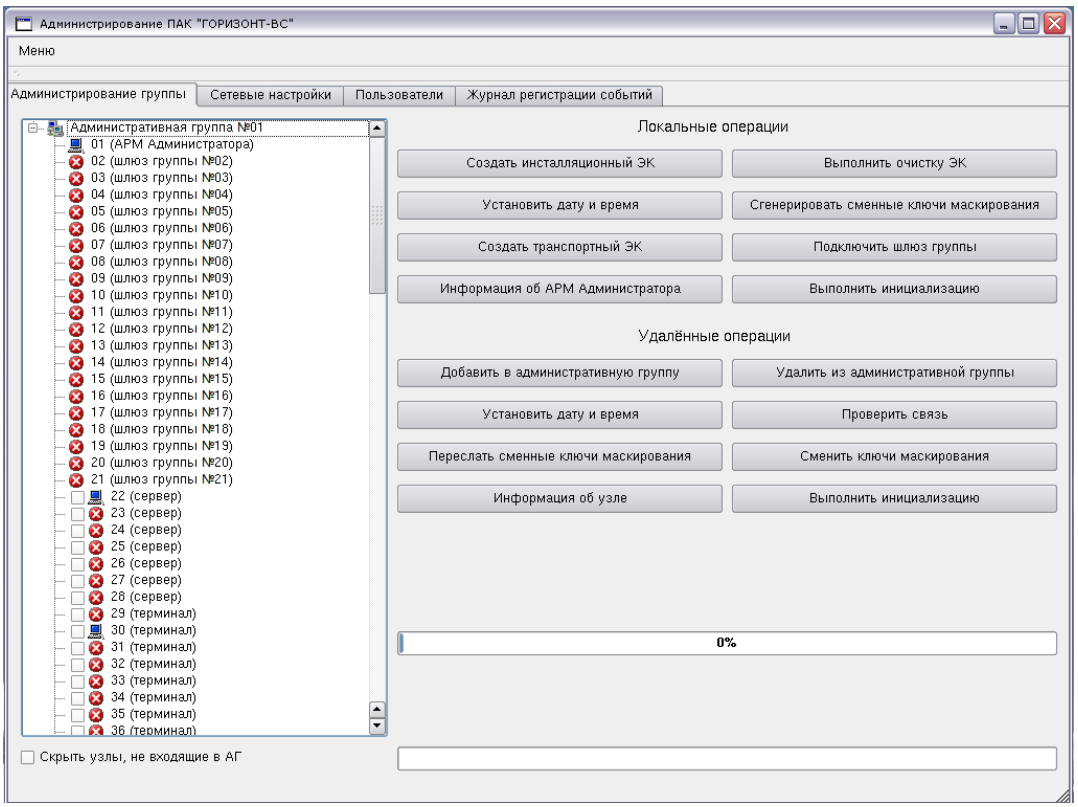

Рисунок 15 – Список узлов административной группы

Для свертывания ветви, необходимо щелкнуть левой клавишей «мыши», наведя указатель на значок 

Пиктограмма  означает, что узел зарегистрирован в АГ, а пиктограмма  – что узел не зарегистрирован в АГ. В том случае, если в параметре **Скрыть узлы, не входящие в АГ** (находится внизу окна списка узлов) установить «флажок», то на экран не будут выводиться незарегистрированные в АГ узлы.

В правой части окна расположены основные элементы управления узлами – кнопки вызова команд, прогресс-индикатор и статусная строка.

Для получения информации об узле **№ 001** можно воспользоваться кнопкой **Информация об АРМ Администратора.** Для получения информации о конкретном узле его необходимо выделить и нажать левую кнопку мыши два раза. В ответ на экран выводится окно **Информация об узле** (Рисунок 16).

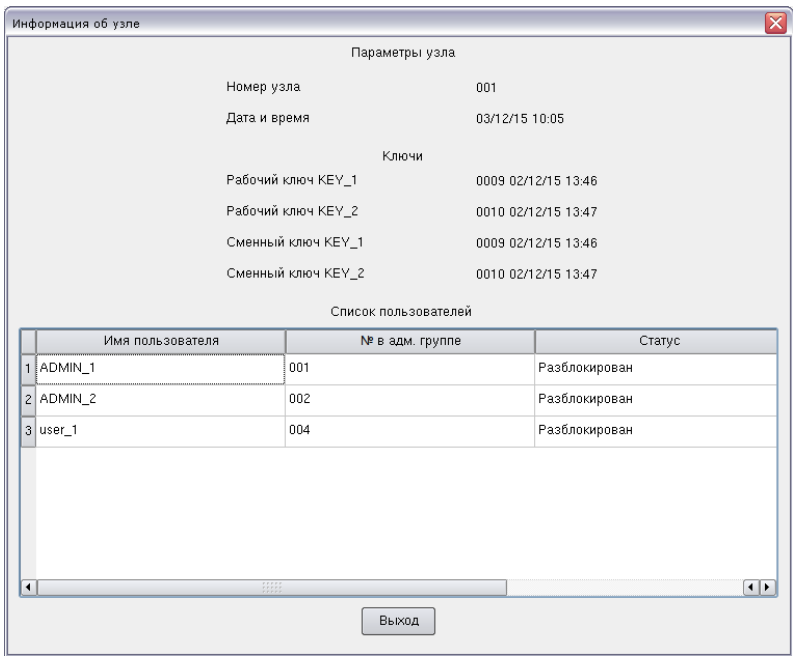

Рисунок 16 – Окно «Информация об узле»

В окне показаны номера и даты генерации ключей маскирования (рабочих и сменных ключей **KEY_1** и **KEY_2**), а также список зарегистрированных на узле администраторов СДЗ и пользователя, с их номерами в группе и статусом (*разблокирован* или *заблокирован*).

Для получения информации об узле **№ 001** также можно воспользоваться кнопкой **Информация об АРМ Администратора**.

Для возврата в список узлов АГ необходимо нажать кнопку **Выход**.

***Примечание**. Если даты соответствующих текущих и сменных ключей одинаковые, то необходимо подготовить новые сменные ключи (4.2.2.1). Смена ключей выполняется не реже одного раза в 90 дней.*

4.2.2.1 Основные элементы управления узлами

В области окна **Локальные операции** (Рисунок 14) представлены операции, выполняемые на *АРМ Администратора*.

В области окна **Удаленные операции** представлены операции, выполняемые на *терминалах* и *серверах виртуализации* через сетевой интерфейс. Добавление узлов в АГ, исключение узлов из АГ, проверка связи, установка даты и времени, пересылка ключей маскирования выполняется только для выбранных узлов списка. Смена ключей маскирования выполняется для всех узлов, входящих в АГ.

Для выбора узла в списке необходимо установить «флажок» рядом с пиктограммой узла с помощью левой клавиши «мыши».

Все операции, содержащиеся в области окна **Локальные операции** и области окна **Удаленные операции** дублируются в контекстном меню. Для вызова контекстного меню необходимо нажать правую клавишу «мыши» на выбранном узле в списке.

4.2.2.2 Локальные операции

1. Установка даты и времени на узле №001 – кнопка Установить дату и время.
2. Нажать кнопку **Установить дату и время** - на экране появится диалоговое окно (Рисунок 17).

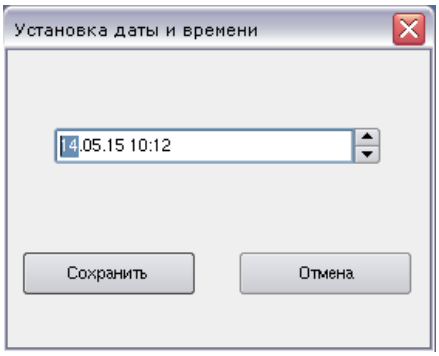

Рисунок 17 – Установка даты и времени

В данном диалоговом окне необходимо ввести дату и время в формате: **ДД.ММ.ГГ ЧЧ:ММ** и нажать кнопку **Сохранить**. При успешной установке даты и времени пиктограмма узла **№001** *АРМ Администратора* изменится на .

3. *Создание инсталляционного ключа* – кнопка **Создать инсталляционный ЭК**.

Выполняется создание ИК - формируется информация необходимая для инсталляции плат изделия на *терминалах/серверах*. При создании ИК информация, необходимая для инсталляции, записывается на ЭК аутентификации администратора.

Примечание *– Вызов данной функции доступен только первому администратору. Создание ИК и его хранение допускается на ЭК аутентификации всех трех администраторов.*

Нажать кнопку **Создать инсталляционный ЭК.**

На предложение установить ЭК (Рисунок 18) установить в считыватель ЭК аутентификации одного из созданных администраторов и нажать кнопку **Да**.

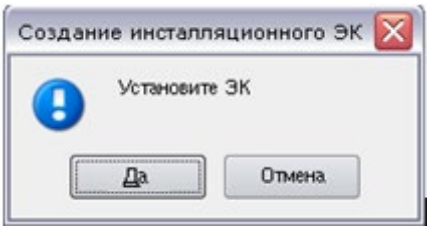

Рисунок 18 – Создание инсталляционного ЭК

Если не удалось прочитать ЭК или ЭК не является DS1977, то на экран выводится сообщение об ошибке (Рисунок 19).

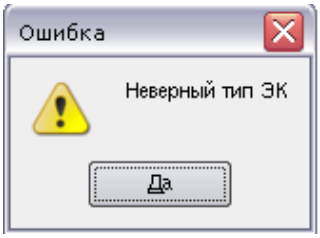

Рисунок 19 – Сообщение о неверном типе ЭК

В данном окне нажать кнопку **Да** – выполняется переход в окно со списком узлов. Инсталляционный ключ не был создан.

При успешном выполнении операции на экран выводится информационное сообщение (Рисунок 20).

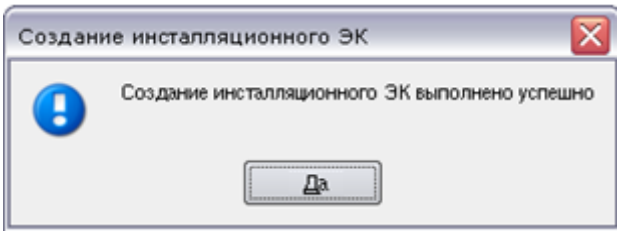

Рисунок 20 – ЭК создан

4. **Создание транспортного ключа** – кнопка **Создать транспортный ЭК.** Выполняется создание транспортного ЭК (ТК), на котором формируется информация, необходимая для доступа к серверам виртуализации текущей АГ из других административных групп, входящих в одну серию.

Нажать кнопку **Создать транспортный ЭК** – на предложение установить ЭК (Рисунок 21) необходимо установить в считыватель ЭК DS1977 и нажать кнопку **Да**.

На ЭК будет создан транспортный ключ – ТК. При успешном выполнении операции на экран выводится информационное сообщение (Рисунок 21).

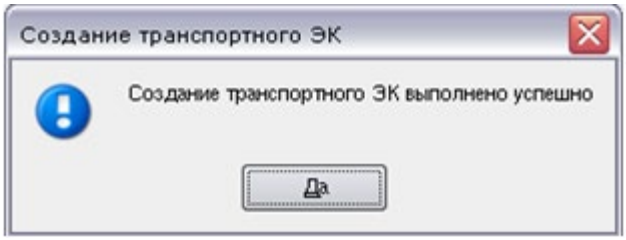

Рисунок 21 – Информационное сообщение

В том случае, если не удалось прочитать ЭК или ЭК не является DS1977, то на экран выводится сообщение об ошибке (рисунок 16).

5. **Очистка содержимого ЭК** – кнопка **Выполнить очистку ЭК**. Выполняется очистка секторов установленного в считыватель ЭК.

   Нажать кнопку **Выполнить очистку ЭК** – на экран выводится диалоговое окно (Рисунок 22).

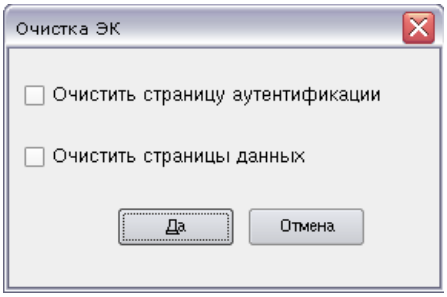

Рисунок 22 – Очистка ЭК

В данном окне необходимо установить опцию очистки ЭК.

- опция **Очистить страницу аутентификации** – выполняется очистка аутентифицирующей информации о пользователе;
- опция **Очистить страницы данных** – выполняется очистка страниц данных (данные страницы используются в ИК и ТК).

После выбора опции необходимо нажать кнопку **Да** - на предложение установить ЭК (Рисунок 18) необходимо установить ЭК в считыватель и нажать кнопку **Да**.

При успешном выполнении операции очистки на экран выводится информационное сообщение (Рисунок 23).

***Примечание**. Процедуру очистки ЭК рекомендуется выполнять перед созданием ТК.*

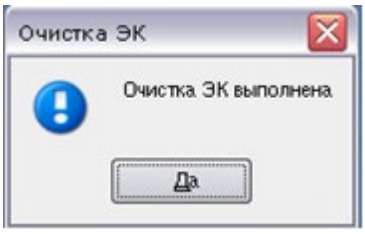

Рисунок 23 – Очистка ЭК выполнена

6. **Генерация сменных ключей маскирования** – кнопка **Сгенерировать сменные ключи маскирования**. Выполняется генерация сменных ключей маскирования для всех узлов АГ (создается матрица ключей). Эта процедура выполняется не реже одного раза в 90 дней.

   Нажать кнопку **Сгенерировать сменные ключи маскирования.**

   При успешной генерации ключей, в статусной строке выводится сообщение:

   Генерация сменных ключей – успешно.

   Пиктограмма узла **№001** изменится на .

7. **Подключение шлюза АГ** – кнопка **Подключить шлюз группы**. Выполняется включение *АРМ Администратора* другой АГ в состав текущей АГ (должны входить в одну серию).

   Нажать кнопку **Подключить шлюз группы** – на экран выводится сообщение (Рисунок 24):

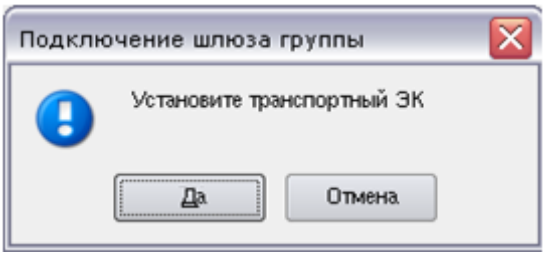

Рисунок 24 – Сообщение о необходимости установить транспортный ЭК

Необходимо установить в считыватель ТК *подключаемой* АГ и нажать кнопку **Да**. При успешном подключении шлюза группы на экран выводится сообщение (Рисунок 25).

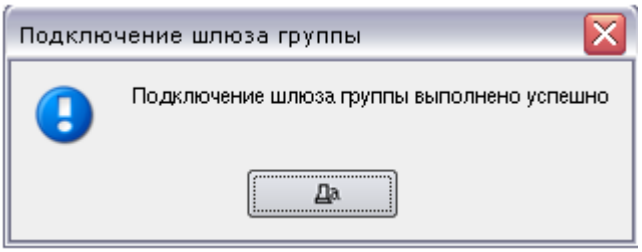

Рисунок 25 – Шлюз группы подключен

При успешном включении шлюза в состав АГ его пиктограмма в списке АГ изменится с  на  .

Процедура установки связи между двумя АГ

Терминалы каждой группы изначально имеют доступ только к *серверам виртуализации* своей группы. Для того, чтобы *терминалы* группы **А** имели доступ к *серверам виртуализации* группы **Б**, а *терминалы* группы **Б** – к *серверам виртуализации* группы **А**, необходимо выполнить следующие операции:

- на *АРМ Администратора* группы **А** выполнить создание транспортного ЭК;
- на *АРМ Администратора* группы **Б** выполнить создание транспортного ЭК;
- на *АРМ Администратора* группы **А** выполнить подключение шлюза группы **Б** – для этого воспользоваться транспортным ЭК группы **Б**;
- на *АРМ Администратора* группы **Б** выполнить подключение шлюза группы **А** – для этого воспользоваться транспортным ЭК группы **А**;

8. Инициализация изделия на АРМ Администратора.

   Процедура инициализации дает возможность администратору СДЗ перевести изделие, установленное на *АРМ Администратора*, в исходное состояние. В процессе инициализации происходит очистка ЖРС, списка пользователей, всех настроек и служебных данных, которые хранятся в памяти изделия. Инициализация изделия выполняется двумя способами:

- из программы, вкладка **Администрирование группы**;
- с помощью аппаратных средств.

Для выполнения программной инициализации изделия, установленного на *АРМ Администратора,* необходимо в области окна **Локальные операции** нажать кнопку **Выполнить инициализацию** – начнется процесс инициализации узла **№001**. По окончании процесса на экран выводится сообщение:

Инициализация выполнена.

При появлении данного сообщения – завершить работу программы.

Для выполнения аппаратной инициализации необходимо:

- выключить ПЭВМ, открыть корпус системного блока и установить на плате изделия перемычку на вилку XP17 (ПРИЛОЖЕНИЕ А, Рисунок 61);
- включить ПЭВМ - начнется процесс инициализации, признаком завершения является начало процедуры инсталляции (при аппаратной инициализации после завершения процедуры инициализации выполняется автоматический переход к процедуре инсталляции (Рисунок 26):

Рисунок 26 – Инсталляция ПАК «Горизонт-ВС»

- если необходимо оставить плату в состоянии готовности к инсталляции, то следует выключить ПЭВМ и убрать на плате перемычку, установленную на вилку XP17, и закрыть корпус системного блока;
- если после инициализации был выполнен переход к инсталляции, то после ее завершения следует выключить ПЭВМ и убрать на плате перемычку, установленную на вилку XP17.

Внимание! *После выполнения инициализации платы, установленной на АРМ администратора, плата изделия переводится в состояние инсталляции. Дальнейшее функционирование АГ без АРМ администратора невозможно.*

4.2.2.3 Удаленные операции

1. **Установка даты и времени_**– кнопка **Установить дату и время**. Выполняется установка даты и времени на выбранных узлах.

Для установки даты и времени необходимо установить слева от выбранных узлов «флажок» и нажать кнопку **Установить дату и время.** На экране появится диалоговое окно (Рисунок 17), в котором необходимо выставить дату, время в формате: **ДД.ММ.ГГ ЧЧ:ММ** и нажать кнопку **Сохранить**. Результат выполнения операции для каждого следующего узла отображается в статусной строке и в списке узлов. Если установка даты и времени на узле была произведена успешно, в статусную строку выдается сообщение:

Установка даты и времени в узле ххх – успешно,

где

ххх – номер узла, пиктограмма данного узла изменится на .

2. **Включение узла в состав АГ** - кнопка **Добавить в административную группу**.

Выполняется добавление в АГ выбранных из списка узлов.

Внимание! *На терминале/сервере виртуализации, для которого будет выполняться процедура включения в список АГ, должна успешно завершиться процедура аутентификации администратора СДЗ и плата изделия должна быть переведена в режим* ***удаленного управления*** *или, после прохождения процедуры контроля векторов, выполнена загрузка ОС (режим работы ОС).*

В окне программы выбрать вкладку **Администрирование группы** (Рисунок 14), в списке узлов (Рисунок 15) выбрать необходимые для активации узлы, в области окна **Удаленные операции** нажать кнопку **Добавить в административную группу** и дождаться успешного завершения операции.

При успешном добавлении узла в АГ его пиктограмма изменится с на .

3. **Исключение узла из состава АГ** – кнопка **Удалить из административной группы**.

   Выполняется удаление в АГ выбранных из списка узлов.

   При успешном удалении узла из АГ его пиктограмма изменится на .

4. **Проверка связи между узлами** - кнопка **Проверить связь**.

   Выполняется проверка связи между узлом **№001** (*АРМ Администратора*) и выбранными в списке узлами.

   Для проверки связи необходимо установить слева от выбранных узлов «флажок» и нажать кнопку **Проверить связь**. Далее строка прогресс-индикатор покажет процесс выполнения команды. Результат проверки связи с каждым следующим узлом отображается в статусной строке и в списке узлов. Если проверка связи с узлом была выполнена успешно, то в статусную строку выводится сообщение:

   Проверка связи с узлом xxx – успешно,

   где:

   xxx – номер узла, пиктограмма данного узла изменится на .

5. **Рассылка сменных ключей маскирования в узлы АГ** – кнопка **Переслать сменные ключи маскирования**.

   Групповая операция. Выполняется рассылка в *выбранные* в списке узлы сгенерированных ранее сменных ключей маскирования (**локальная операция**). Предварительно необходимо активировать данные узлы.

   Для выполнения рассылки сменных ключей необходимо установить слева от выбранных узлов «флажок» и нажать кнопку **Переслать сменные ключи**. Далее строка прогресс-индикатор покажет процесс выполнения команды. Результат пересылки ключей в каждый следующий узел отображается в статусной строке и в списке узлов. При успешной пересылке ключей в узел, в статусную строку выводится сообщение:

   Пересылка сменных ключей в узел xxx - успешно,

   где:

   xxx – номер узла, пиктограмма данного узла изменится на .

Примечание. *Результат выполнения групповой операции для конкретных узлов выводится в файл групповых операций – **group_log.txt** в каталоге **/root**. На*

основании данных в этом файле администратор СДЗ получает информацию о тех узлах, для которых данная операция закончилась с ошибкой. В случае ошибочного завершения операции администратор СДЗ должен выяснить причину ошибки и устранить ее (как правило причиной ошибки является то, что узел не находится в активном состоянии), а затем повторить групповую операцию.

Групповую команду смены ключа маскирования можно выдавать только после того как будет успешно выполнена рассылка для всех задействованных узлов АГ. Узлы, в которые по каким-либо причинам не удалось успешно выполнить пересылку ключа, необходимо исключить из административной группы (удалить). Их необходимо удалить до процедуры смены ключей маскирования. В дальнейшем эти узлы могут быть введены в состав АГ путем повторной инсталляции (после выполнения процедуры инициализации изделия). Если невозможно активировать одновременно все зарегистрированные в АГ узлы, то групповая команда смены ключа маскирования может выдаваться повторно, но, при этом, необходимо вводить одну и ту же дату смены ключа – это необходимо для того, чтобы смена была выполнена одновременно на всех узлах.

6. **Смена ключей маскирования на всех узлах АГ** - кнопка **Сменить ключи маскирования.**

   Групповая операция. Выполняется одновременная смена ключей маскирования на всех зарегистрированных узлах АГ, включая узел **№001**.

   Для смены ключей маскирования во всей группе необходимо нажать кнопку **Сменить ключи маскирования**. В ответ на экран выводится диалоговое окно **Установка даты и времени** (рисунок 14), в котором необходимо выставить дату и время смены ключей и нажать кнопку **Сохранить.** Дата смены ключей определяется периодом действия ключей (90 дней). Далее строка прогресс-индикатор покажет процесс выполнения команды. Результат операции для каждого следующего узла отображается в статусной строке и в списке узлов. При успешной пересылке команды смены ключа в узел в статусную строку выводятся сообщения:

   Пересылка команды смены ключа в узел xxx - успешно

   где:

   xxx – номер узла, пиктограмма  данного узла изменится на  .

В том случае, если какой-либо узел не был активен, то статусную строку выводится сообщение:

7. **Нет связи с узлом.**

При появлении данного сообщения хотя бы по одному узлу необходимо повторить команду смены предварительно активировав все зарегистрированные узлы.

Инициализация изделия на терминале и сервере виртуализации

Инициализация изделий, установленных на *терминалах* и *серверах виртуализации*, выполняется аналогично инициализации изделия, установленного на *АРМ Администратора*:

- из программы, вкладка **Администрирование группы**;
- с помощью аппаратных средств.

Отличие только в том, что при программной инициализации необходимо выбрать требуемый узел в списке и нажать кнопку **Выполнить инициализацию** в области окна **Глобальные операции** – начнется процесс инициализации выбранного узла.

После выполнения инициализации *терминал/сервер виртуализации* выводится из состава АГ. Плата изделия переводится в состояние инсталляции.

4.2.3 Сетевые настройки

Для управления сетевыми настройками плат МИиКДС используется вкладка **Сетевые настройки** (Рисунок 27). Вкладка состоит из трех информационных окон, в которые выводятся таблицы:

- **Сетевые интерфейсы плат;**
- **IP-адреса серверов группы;**
- **IP-адреса серверов других групп**.

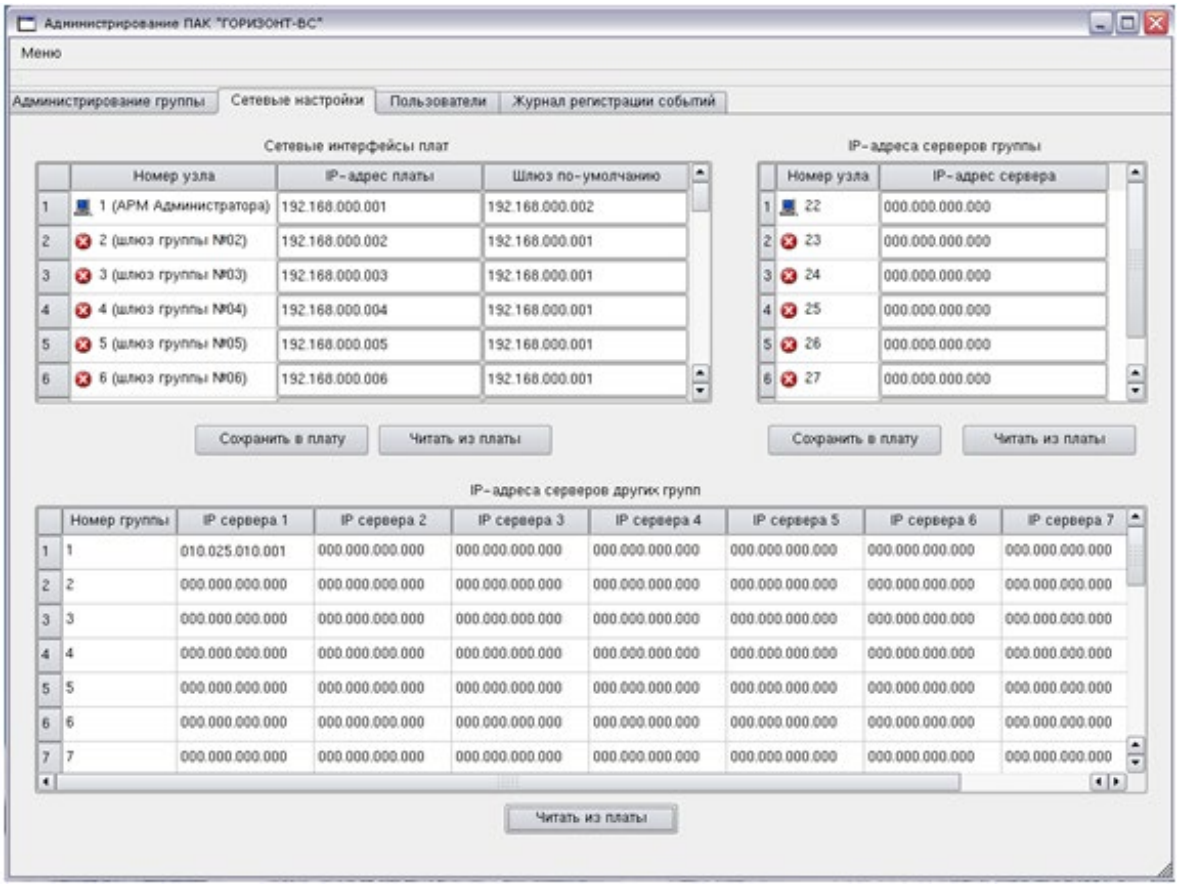

Рисунок 27 – Вкладка **Сетевые настройки**

Таблица **Сетевые интерфейсы плат** содержит сетевые настройки плат изделий, входящих в состав текущей АГ.

Для активизации таблицы нажать кнопку **Читать из платы**. В таблицу будут выведены данные из ЭНП платы изделия.

В строки таблицы выводится сетевая информация по узлам:

- первый столбец (**Номер узла)** – номер узла, присвоенный конкретному изделию при инсталляции;
- второй столбец (**IP-адрес платы)** – IP-адрес платы изделия;
- третий столбец (**Шлюз по умолчанию)** – выводится IP-адрес сетевой платы последнего использованного на данном узле шлюза.

***Примечание**. На этапе изготовления по каждому узлу, по умолчанию, введена сетевая информация. Данная информация (IP-адрес платы изделия и IP-адрес шлюза) может быть изменена в соответствии с требованиями текущей АГ.*

Для корректировки информации в таблице Сетевые интерфейсы плат:

1. Установить курсор в нужное поле строки.
2. Дважды нажать на левую клавишу «мыши».

   Поле станет активным.
3. Ввести новое значение.
4. Нажать кнопку **Сохранить в плату**.

Таблица **IP-адреса серверов группы** содержит сетевые настройки сетевых плат серверов, входящих в состав ЛВС текущей АГ.

Для активизации таблицы нажать кнопку **Читать из платы**. В таблицу будут выведены данные из ЭНП платы изделия.

В строки таблицы выводится сетевая информация по *серверам виртуализации*:

- первый столбец (**Номер узла)** – номер узла, присвоенный конкретному изделию, выполняющему функции сервера виртуализации;
- второй столбец (**IP-адрес сервера)** – IP-адрес платы изделия на сервере виртуализации.

Действия при работе с таблицей **IP-адреса серверов группы** аналогичны действиям при работе с таблицей **Сетевые интерфейсы плат**.

Таблица **IP-адреса серверов других групп** содержит сетевые настройки *сетевых плат серверов виртуализации*, входящих в состав других АГ.

В строки таблицы выводится сетевая информация по определенной АГ: в *первом столбце* показан номер другой АГ, а в остальных *семи столбцах* - IP-адреса *серверов виртуализации,* принадлежащих данной АГ.

Таблица носит ознакомительный характер, так как изменения в IP-адрес *сервера виртуализации* можно внести только непосредственно с *АРМ Администратора* группы, в которую он входит. При помощи этой таблицы администратор проверяет актуальность информации о *серверах виртуализации* других АГ для дальнейшей работы с ними.

В АГ может быть максимально **7** серверов виртуализации, а количество АГ может быть не более **21** (входят в одну серию).

4.2.4 Пользователи

Для управления списком пользователей АГ используется вкладка Пользователи (Рисунок 28).

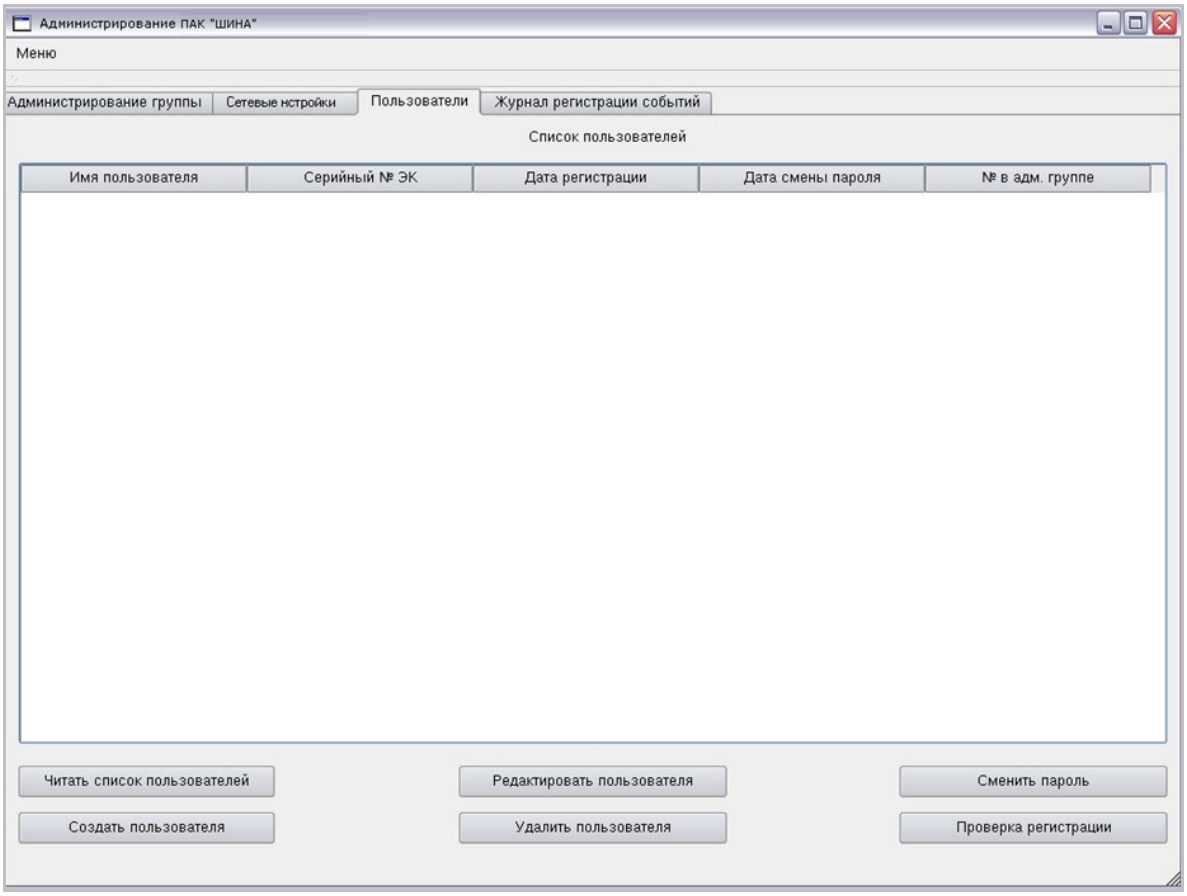

Рисунок 28 – Вкладка «Список пользователей»

4.2.4.1 Чтение списка пользователей.

Для чтения списка пользователей необходимо нажать кнопку **Читать список пользователей**. В информационном окне будет выведен список созданных и зарегистрированных в АГ пользователей и администраторов СДЗ (Рисунок 29).

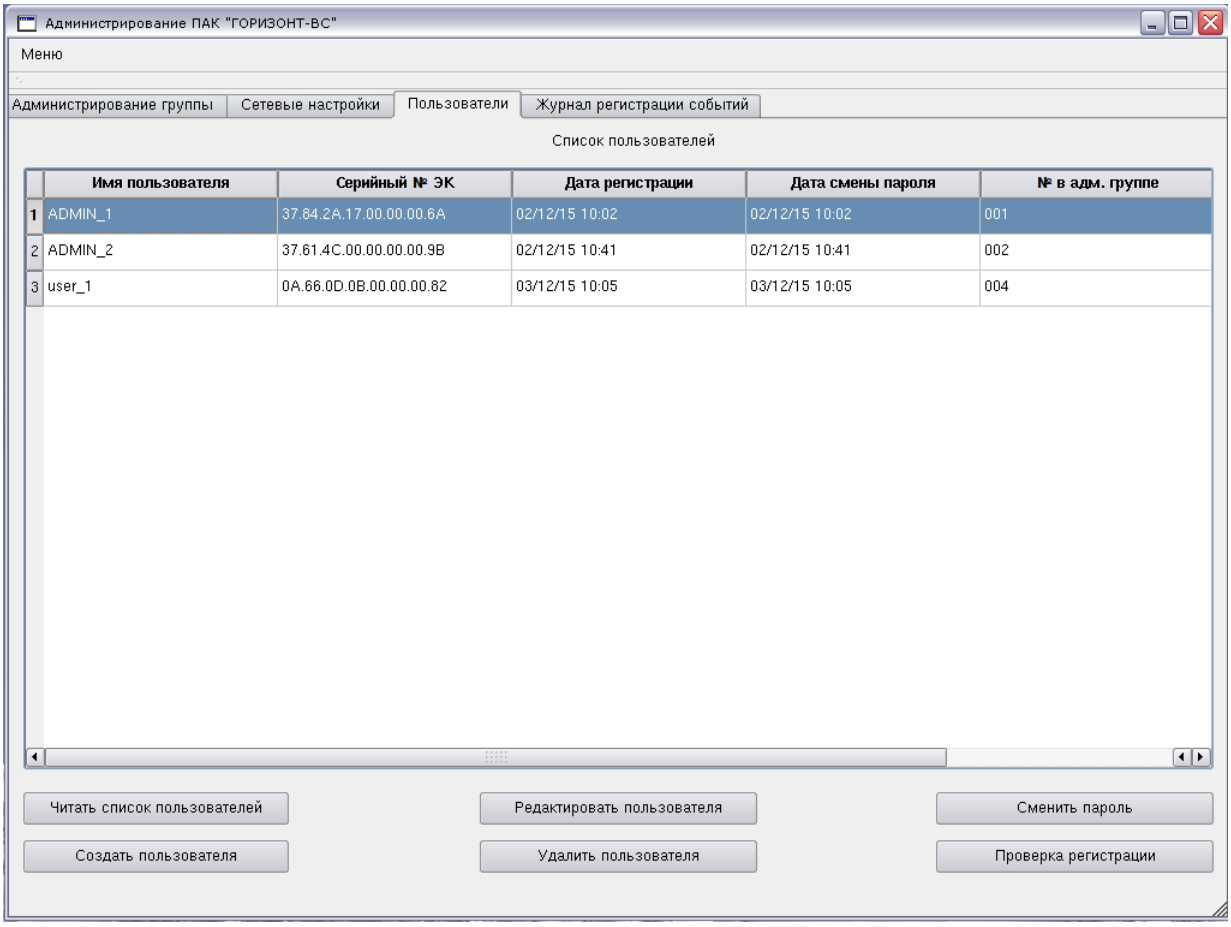

Рисунок 29 – Список пользователей

В АГ может быть зарегистрировано не более трех администраторов и не более 125-ти пользователей. Создание и регистрация первого администратора СДЗ (**ADMIN_1**) выполняется при инсталляции платы изделия на *АРМ Администратора*. По каждому пользователю выводится следующая информация:

- имя пользователя;
- серийный номер ЭК аутентификации пользователя;
- дата регистрации (создания) пользователя;
- дата последней смены пароля;
- номер пользователя в административной группе: для администраторов СДЗ зарезервированы номера с **1** по **3**, для пользователей: с **4** по **128**

4.2.4.2 Создание и регистрация администраторов и пользователей

Для создания и регистрации нового администратора СДЗ или пользователя:

1. Нажать кнопку **Создать пользователя**.

На экран будет выведено диалоговое окно **Создание пользователя** (Рисунок 30).

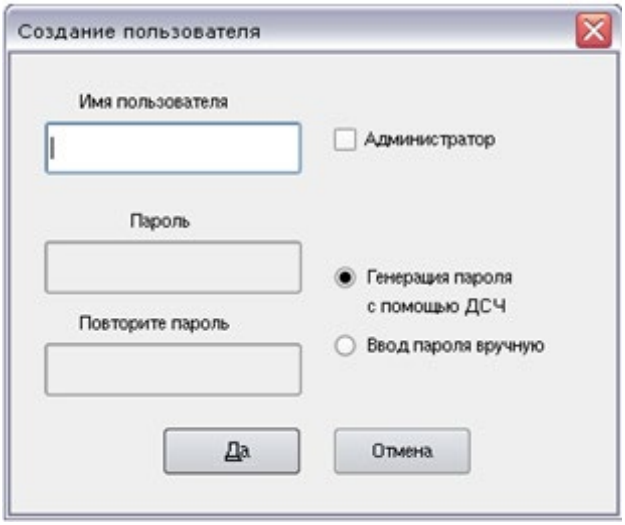

Рисунок 30 – Окно «Создание пользователя»

2. В строке **Имя пользователя** ввести имя пользователя. Минимальная длина имени пользователя – три символа (в имени не должны присутствовать пробелы).
3. Для создания администратора СДЗ установить флаг в поле **Администратор**.

Изделие автоматически назначает имена администраторам (**ADMIN_2** и **ADMIN_3**).

4. Пароль аутентификации формируется либо с помощью датчика случайных чисел (ДСЧ) (по умолчанию), либо вводится вручную с клавиатуры.

Для ввода пароля вручную выбрать опцию **Ввод пароля вручную** и ввести пароль два раза в строку ввода **Пароль** и **Повторите пароль**. Все введенные символы отображаются знаком ‘*’. Если какой-либо символ введен неверно, то его можно стереть (клавиша **BackSpace)** и повторить ввод.

Пароль должен удовлетворять следующим требованиям:

- длина пароля – **8** символов;
- в пароле обязательно должны присутствовать символы из следующих категорий:
  - прописные буквы английского алфавита от A до Z;

- строчные буквы английского алфавита от a до z;
- десятичные цифры от 0 до 9;
- специальные символы, не принадлежащие алфавитно-цифровому набору (например, *_@);

– в пароле должны отсутствовать повторяющиеся символы;

– пароль не должен иметь смысловой нагрузки.

5. Нажать кнопку **Да**. В процессе создания, будут представлены следующие сообщения:

– **Минимальная длина имени пользователя – 3 символа.** Данное сообщение появляется в том случае, если было введено недостаточно длинное имя пользователя.

Если был введен недостаточно длинный пароль, на экран выводится сообщение об ошибке:

– **Требуемая длина пароля – 8 символов**. Данное сообщение выводится, если был введен недостаточно длинный пароль.

Если в строку ввода **Пароль** и строку ввода **Повторите пароль** были введены разные пароли, на экран выводится сообщение об ошибке:

– **Пароли не совпадают**. Данное сообщение появляется в том случае, если в строку ввода и строку ввода **Повторите пароль** были введены разные пароли.

6. На предложение установить ЭК (Рисунок 31) установить ЭК в считыватель и нажать кнопку **Да**.

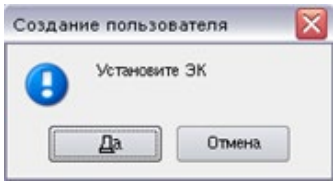

Рисунок 31 – Предложение установить ЭК

Запустится процедура создания пользователя/администратора. При успешном ее выполнении на экран выводится сообщение (Рисунок 32).

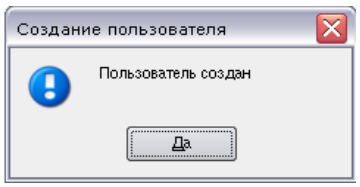

Рисунок 32 – Сообщение о создании пользователя

7. Нажать кнопку **Да.** и в

В списке пользователей появится новый пользователь (Рисунок 29).

Если ЭК не установлен – на экран выводится сообщение об ошибке (Рисунок 33).

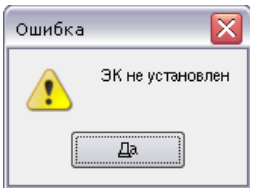

Рисунок 33 – Сообщение об ошибке

Необходимо установить ЭК, нажать кнопку **Да** и повторить процедуру создания пользователя.

***Примечание**. При эксплуатации системы пользователь должен сохранять свой пароль в тайне.*

Если процедура создания пользователя выполнена с ошибкой, на экран выводится соответствующее сообщение об ошибке. Возможны следующие ошибочные ситуации:

- зарегистрированы три администратора – попытка зарегистрировать четвертого администратора;
- попытка регистрации двух пользователей с одинаковым именем.

Созданный пользователь/администратор СДЗ автоматически регистрируется на *АРМ Администратора*.

4.2.4.3 Просмотр и редактирование информации о пользователе

Для просмотра и редактирования информации о пользователе/администраторе, а также для блокировки и разблокировки его на *терминале/сервере виртуализации*, необходимо открыть окно **Информация о пользователе** (Рисунок 34). Для этого следует выделить

нужного пользователя в списке и дважды нажать левую клавишу «мыши», либо нажать кнопку **Редактировать пользователя**.

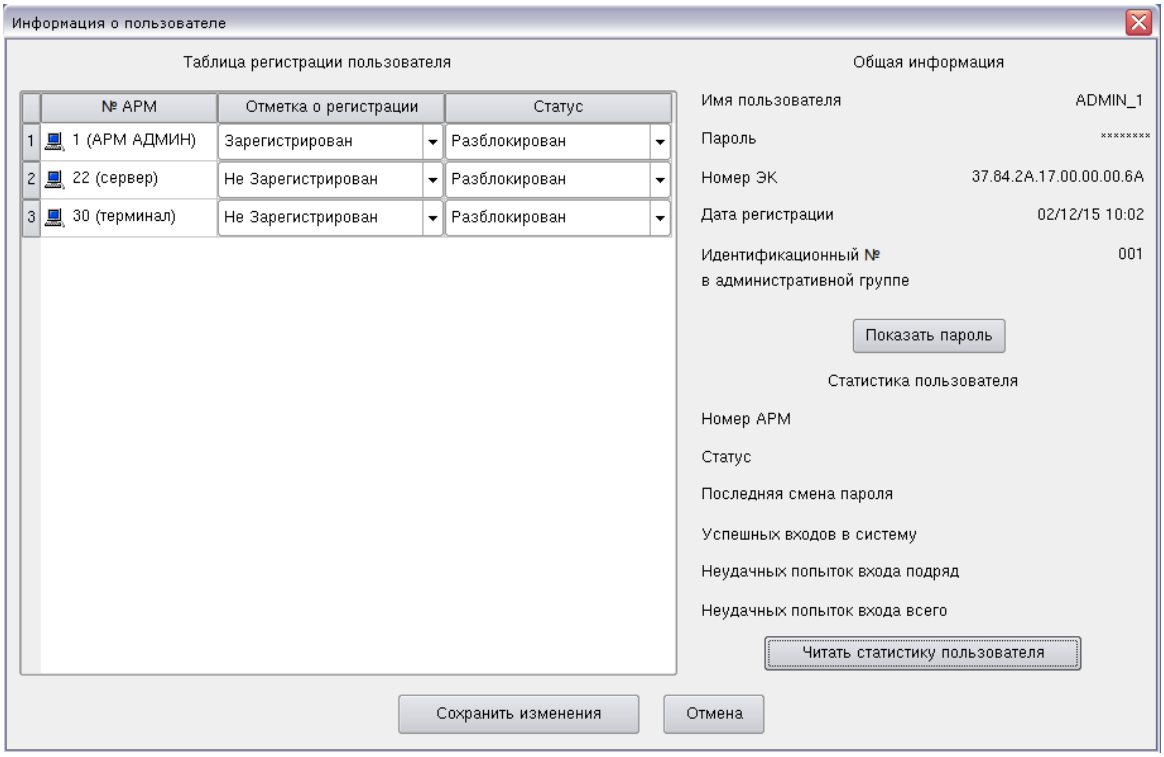

Рисунок 34 – Окно информации о пользователе

В левой части окна расположена Таблица регистрации пользователя.

В строки таблицы выводится информация по всем АРМ (узлам), входящим в АГ.

Каждая строка соответствует одному АРМ (узлу) в АГ.

- первый столбец **(№ АРМ**) – номер узла в АГ;
- второй столбец (**Отметка о регистрации**) – информация о регистрации - зарегистрирован или не зарегистрирован пользователь на данном АРМ (узле);
- третий столбец (**Статус**) – статус пользователя, указывающий есть ли у пользователя доступ на вход в систему на данном АРМ (узле) (имеет смысл только для зарегистрированного на данном узле пользователя).

В правой части окна расположены информационные поля, содержащие основные данные пользователя. При нажатии кнопки **Показать пароль** вместо символов ******** будет отображаться пароль выбранного пользователя, заводской номер ЭК, номер АГ, дата создания (регистрации) пользователя на *АРМ Администратора* (Рисунок 35).

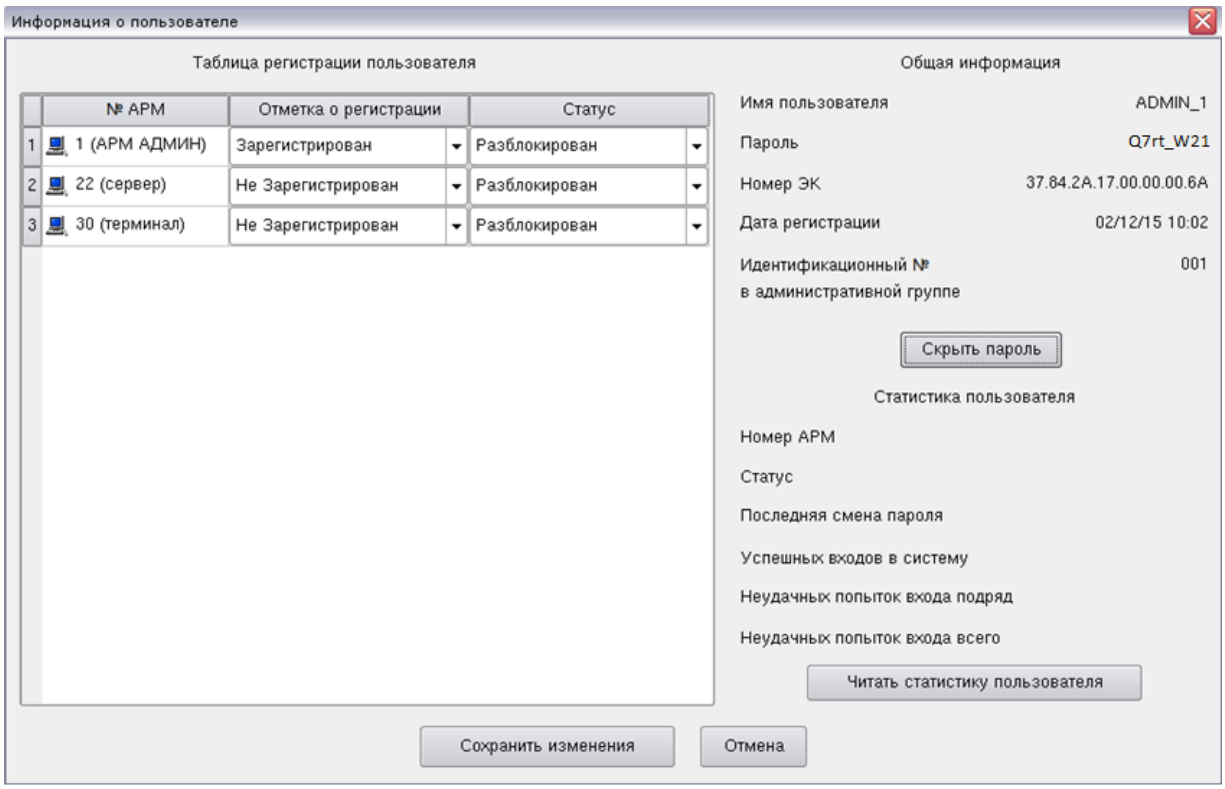

Рисунок 35 – Отображение пароля пользователя

4.2.4.4 Просмотр статистики пользователя

Для просмотра статистики пользователя необходимо выделить в таблице регистрации конкретный узел и нажать кнопку **Читать статистику пользователя**. В области окна **Таблица регистрации пользователя** выводится статистика пользователя по выбранному узлу (Рисунок 36).

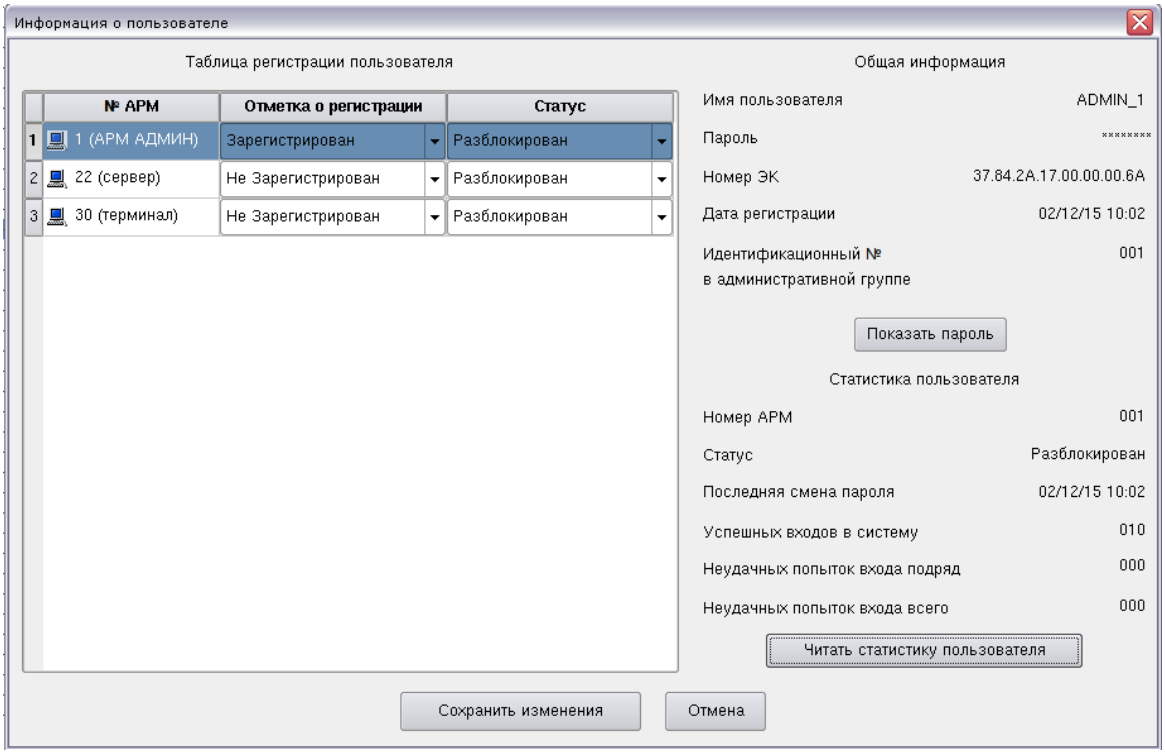

Рисунок 36 – Статистика пользователя

Если узел в таблице не был выбран, на экран выводится сообщение об ошибке (Рисунок 37), необходимо нажать кнопку **Да** и повторить описанные ранее действия.

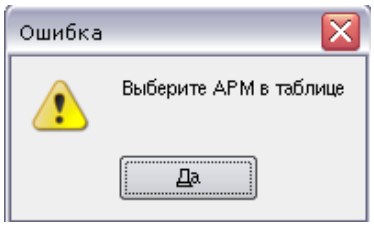

Рисунок 37 – Сообщение об ошибке. Не выбран узел

Чтение статистики пользователя возможно только для того узла, на котором он зарегистрирован. При попытке прочитать статистику пользователя на узле, на котором он не зарегистрирован, выводится сообщение об ошибке (Рисунок 38).

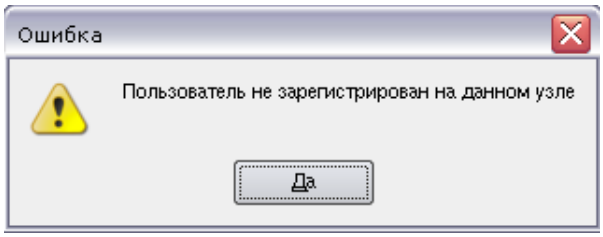

Рисунок 38 – Сообщение об ошибке. Пользователь не зарегистрирован на данном узле

4.2.4.5 Регистрация пользователя на терминале/сервере

Внимание! *1. На одном терминале, согласно указаниям по эксплуатации (Формуляр МБРЦ.468313.001ФО, п. 6.4), разрешается регистрировать только одного пользователя.*

2. На сервере виртуализации, согласно условиям по безопасности, разрешается регистрировать только администраторов СДЗ.

Для регистрации пользователя на узле АГ необходимо в **Таблице регистрации пользователя** в выпадающем меню во *втором столбце* выбрать пункт **Зарегистрирован** для соответствующего узла, после чего нажать кнопку **Сохранить изменения** в нижней части окна (Рисунок 39).

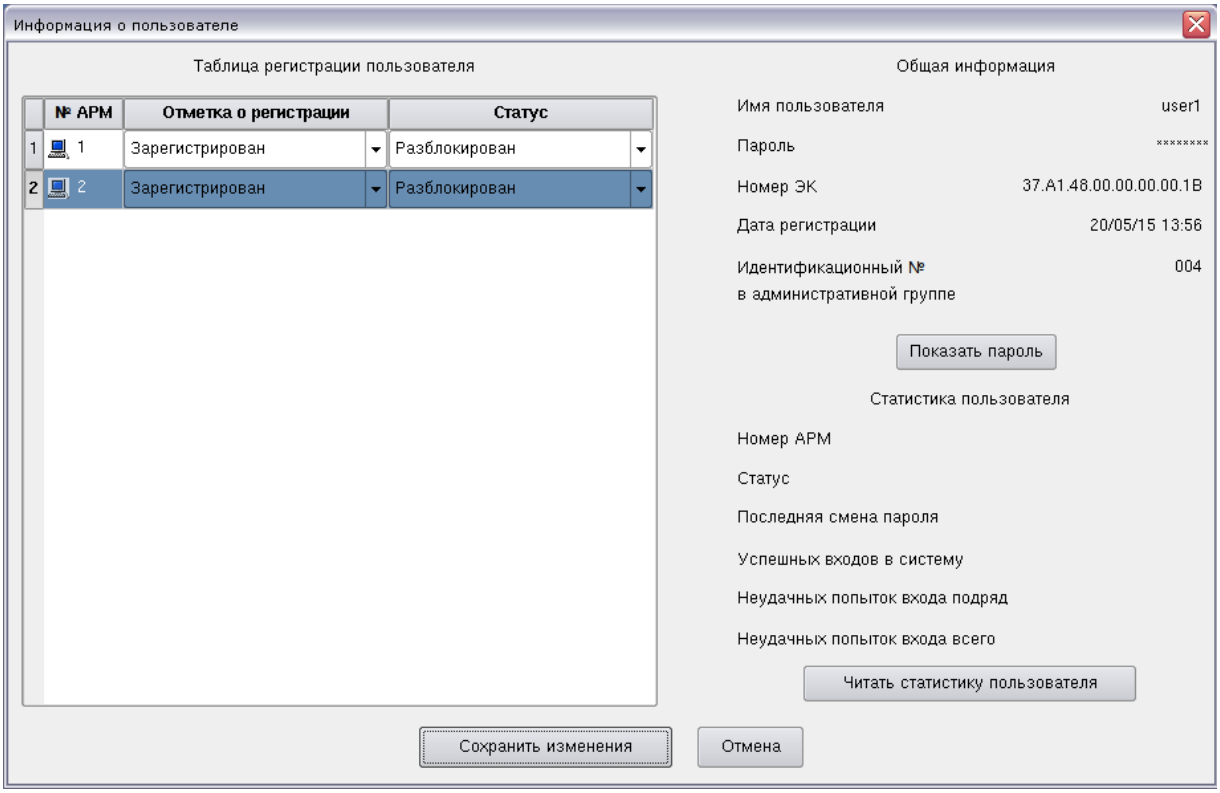

Рисунок 39 – Регистрация пользователя на узле

Для блокировки/разблокировки пользователя на узле АГ в **Таблице регистрации пользователя** в соответствующей нужному узлу строке в выпадающем меню в третьем столбце выбрать пункт **Заблокирован/Разблокирован**, затем нажать кнопку **Сохранить изменения**.

При успешном сохранении изменений на экране появится сообщение (Рисунок 40).

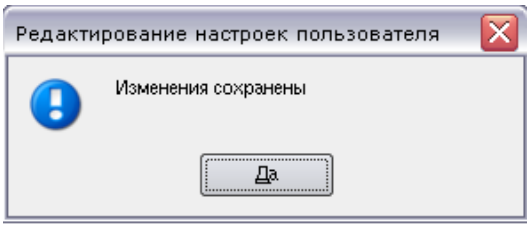

Рисунок 40 – Сообщение о сохранении изменений настроек

Внимание! *На АРМ администратора (узел №001) необходимо заблокировать пользователя после его создания (регистрации), изменив в таблице регистрации пользователей его статус на узле* ***№001****.*

4.2.4.6 Смена пароля пользователя

Групповая операция.

Примечание. *Смену пароля второго и третьего администраторов СДЗ может выполнить только первый администратор СДЗ или администратор СДЗ сам себе.*

Для изменения пароля пользователя необходимо выделить соответствующую ему строку в списке пользователей и нажать кнопку **Сменить пароль**. На экран будет выведено диалоговое окно смены пароля пользователя (Рисунок 41).

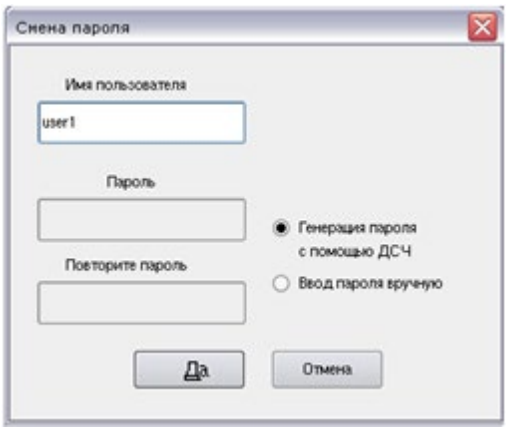

Рисунок 41 – Смена пароля

Последовательность действий при выполнении смены пароля аналогична последовательности действий при создании пользователя за исключением того, что в строке ввода **Имя пользователя** выведено имя пользователя.

Процесс выполнения смены пароля отображается в отдельном диалоге выполнения операции (Рисунок 42).

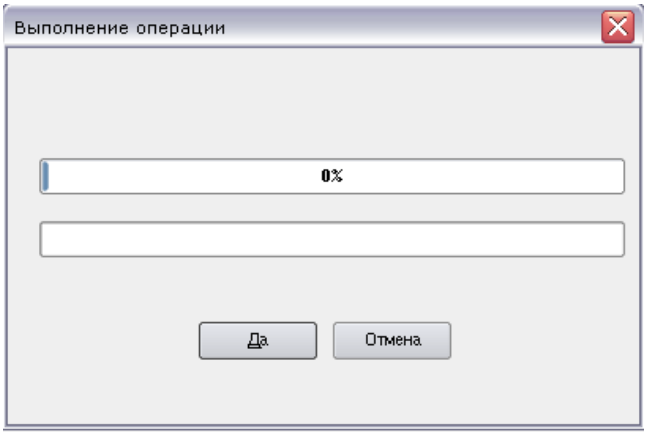

Рисунок 42 – Процесс выполнения смены пароля

При успешном выполнении процедуры смены пароля выдается информационное сообщение (Рисунок 43).

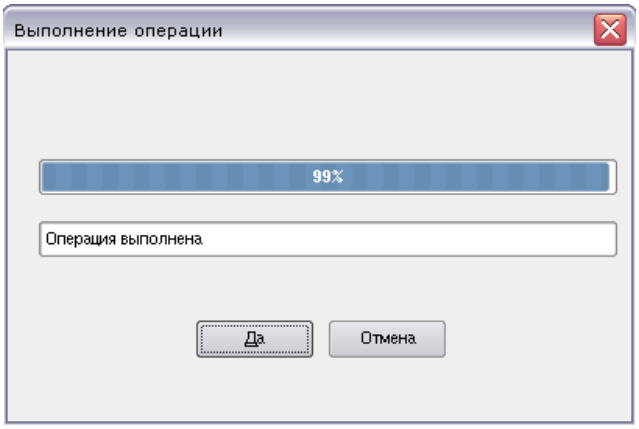

Рисунок 43 – Пароль изменен

Внимание! *Смена паролей на ЭК аутентификации всех администраторов СДЗ и пользователей должна выполняться своевременно (до истечения срока действия пароля – 90 дней). Перед сменой пароля узел, на котором данный пользователь зарегистрирован, должен быть предварительно активирован. Если узел не был активирован при выполнении смены пароля, то для пользователя данный узел в дальнейшем будет недоступен.*

4.2.4.7 Корректировка списка пользователей

Групповая операция.

Для выполнения удаления пользователя из списка необходимо выделить соответствующую строку (Рисунок 29) и нажать кнопку **Удалить**

пользователя. В ответ на экран выводится диалоговое окно (Рисунок 44), в котором следует нажать кнопку **Да**.

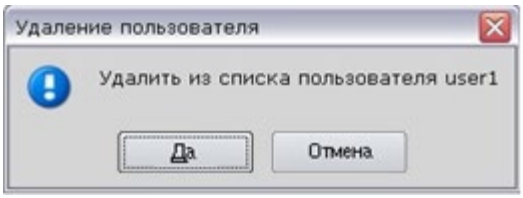

Рисунок 44 – Удаление пользователя

При успешном удалении пользователя на экран выводится сообщение (Рисунок 45).

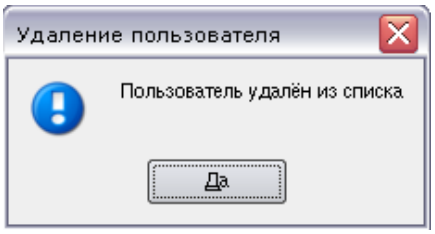

Рисунок 45 – Пользователь удален из списка

Пользователь удаляется из общего списка пользователей АГ и из списка пользователей на том узле, на котором он зарегистрирован.

Внимание!

1. При удалении пользователей/администраторов СДЗ на всех терминалах и серверах виртуализации, на которых они зарегистрированы, должна быть загружена ос или они должны быть в режиме удаленного управления.

2. Удаление первого администратора СДЗ (admin_1) запрещено.

При попытке удалить **ADMIN_1** на экран выводится сообщение (Рисунок 46).

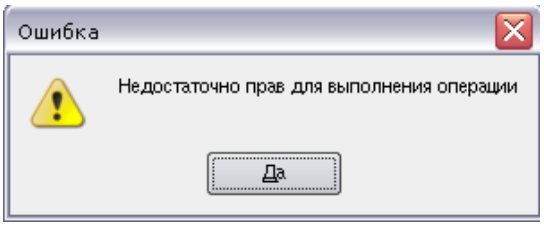

Рисунок 46 – Сообщение об ошибке при попытке удаления ADMIN_1

4.2.4.8 Проверка регистрации пользователя

Для проверки регистрации пользователя:

1. Выделить в списке строку, соответствующую пользователю (Рисунок 29).

2. Нажать кнопку **Проверка регистрации**.

   На экран будет выведен диалог проверки регистрации пользователя (Рисунок 47).

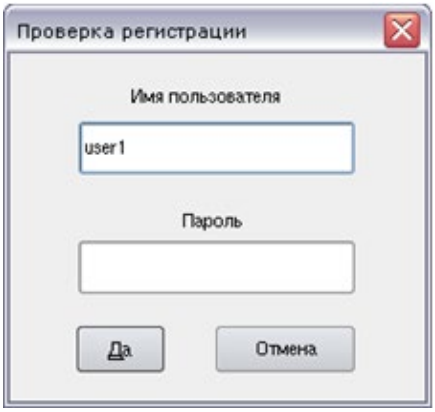

Рисунок 47 – Проверка регистрации пользователя

3. Ввести пароль пользователя и нажать кнопку **Да.**

   Появится окно с предложением установить ЭК (Рисунок 48).

4. Установить ЭК пользователя в считыватель и нажать кнопку **Да**.

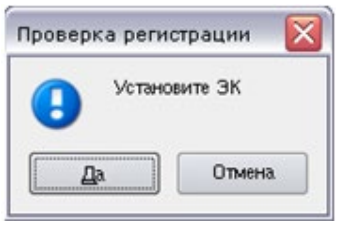

Рисунок 48 – Диалоговое окно «Проверка регистрации»

Запустится процедура аутентификации пользователя.

Если аутентификация выполнена успешно, на экран выводится сообщение (Рисунок 49).

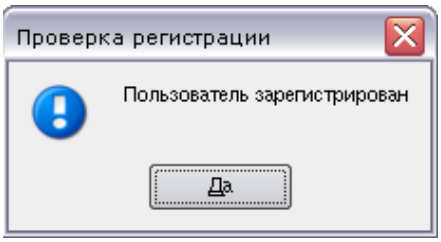

Рисунок 49 – Пользователь зарегистрирован

Если результат отрицательный, на экране выводится сообщение об ошибке (Рисунок 50).

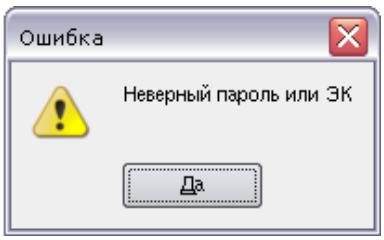

Рисунок 50 – Сообщение об ошибке регистрации пользователя

4.2.5 Журнал регистрации событий

Вкладка **Журнал регистрации событий** (ЖРС) состоит из информационного поля и кнопок, позволяющих работать с ЖРС (Рисунок 51).

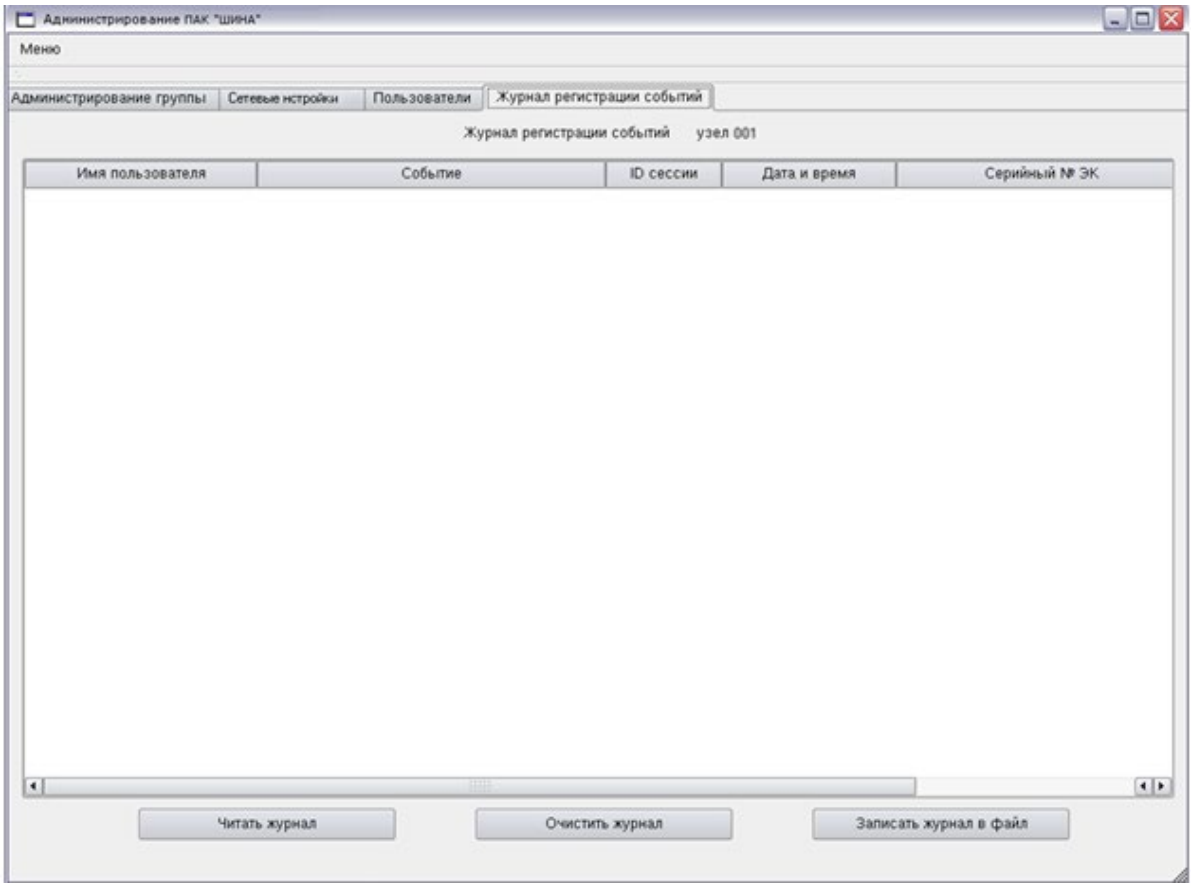

Рисунок 51 – Журнал регистрации событий

Размер журнала – 1024 записи.

Журнал формируется по принципу «кольцевого буфера».

По каждому значащему событию формируется строка, состоящая из следующих полей:

– **Имя пользователя** – имя зарегистрированного пользователя, выполнившего действие;

***Примечание**. Если к моменту наступления события имя пользователя не определено, то в данное поле выводится константа «Неопределен».*

- **Событие** – условное название события (перечень регистрируемых событий дан в приложении Д);
- **ID сессии** – идентификатор сессии;
- **Дата и время** – ДД/ММ/ГГ ЧЧ:ММ:СС,

  где:

  ДД/ММ/ГГ – дата/месяц/ год;

  ЧЧ:ММ:СС –час:минута:секунда;
- **Серийный № ЭК** – заводской номер ЭК , который участвовал в событии.

***Примечание**. Если ЭК не принимает участия в событии, то в данное поле выводится константа «Неопределен».*

4.2.5.1 Чтение информации из журнала

ЖРС предназначен для хранения записей о событиях, регистрируемых изделием. Для отображения записей журнала необходимо нажать кнопку **Читать журнал**. На экран выводится диалоговое окно (Рисунок 52), в котором необходимо выбрать номер узла и нажать кнопку **Да**.

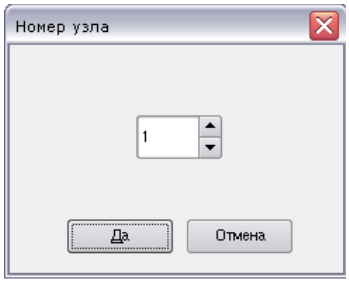

Рисунок 52 – Выбор номера узла

В информационное поле вкладки **Журнал регистрации событий** выводится список зарегистрированных событий, произошедших на узле. Записи приводятся в порядке возрастания времени регистрации события (Рисунок 53).

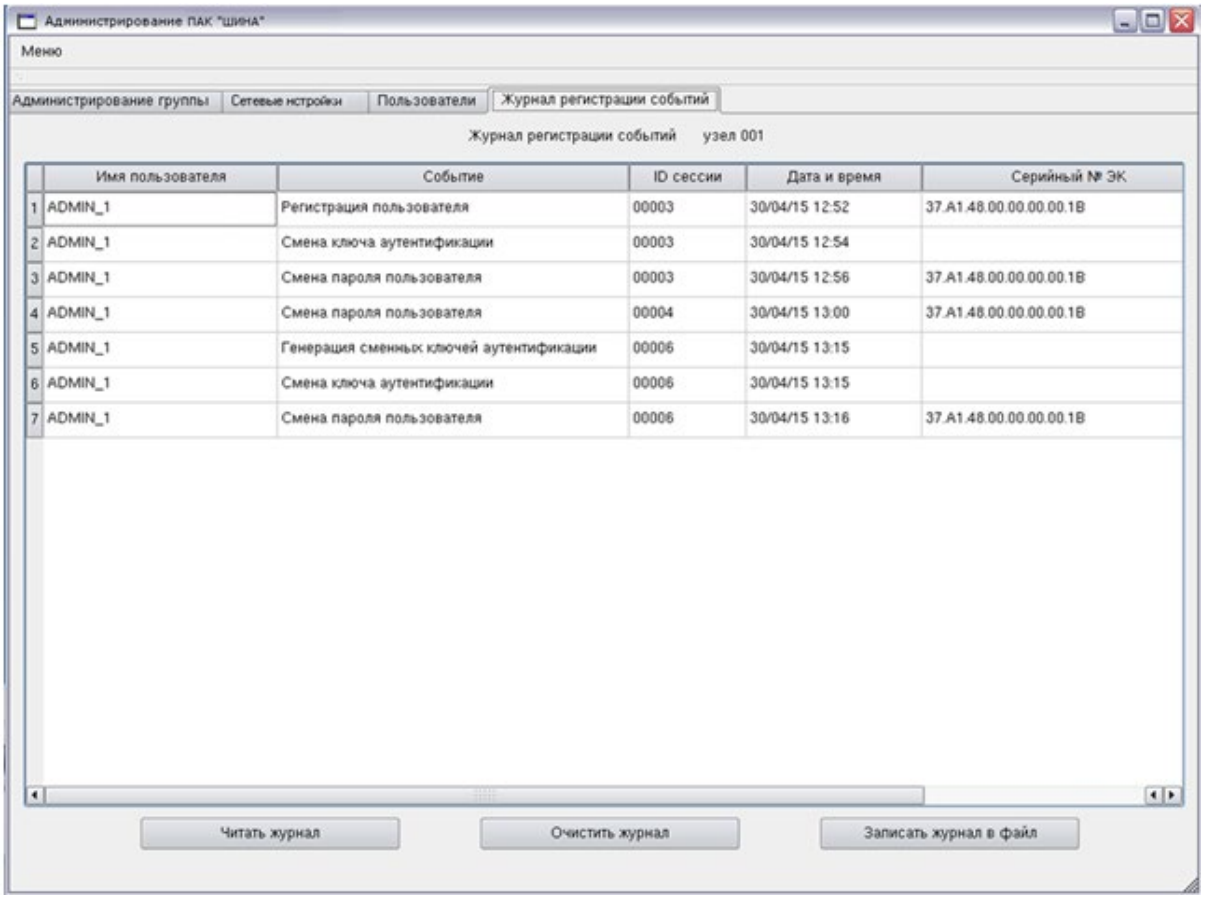

Рисунок 53 – Список событий, зарегистрированных на узле

Если при выполнении операции связь с узлом по сети отсутствует, то на экран выводится сообщение об ошибке (Рисунок 54).

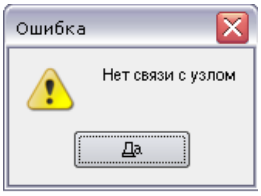

Рисунок 54 – Сообщение об отсутствии связи с узлом

В этом случае необходимо восстановить связь с узлом по сети, после чего повторить операцию чтения информации из ЖРС.

4.2.5.2 Очистка журнала

При успешном выполнении операции очистки журнала на экран выводится соответствующее сообщение (Рисунок 55).

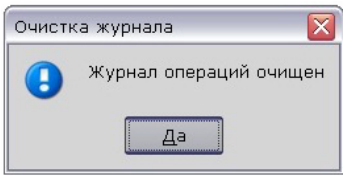

Рисунок 55 – Журнал операций очищен

Если при выполнении операции связь с узлом по сети отсутствует – на экран выводится сообщение об ошибке (Рисунок 54). В этом случае необходимо восстановить связь с узлом по сети, после чего повторить операцию.

4.2.5.3 Запись информации в файл

Для записи информации из журнала в файл:

1. Нажать кнопку **Записать журнал в файл**.
   Откроется окно выбора файла.
2. Выбрать файл для записи информации из журнала (Рисунок 56).

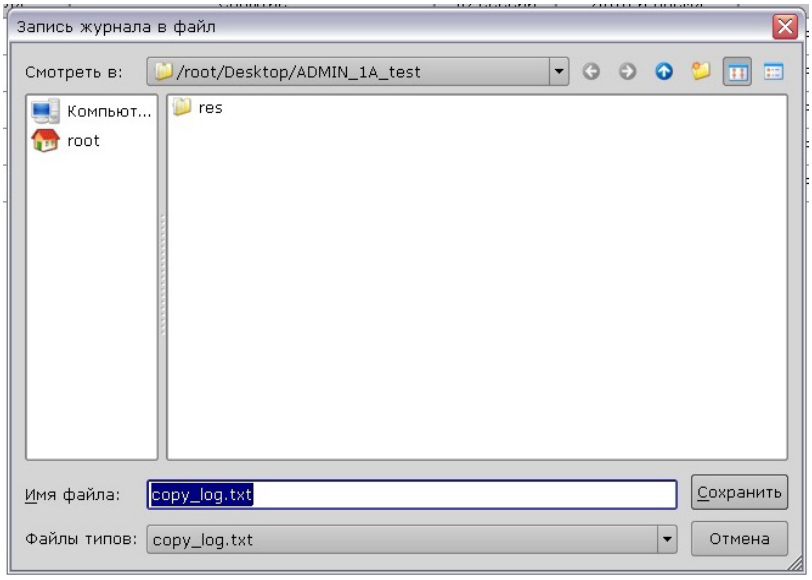

Рисунок 56 – Окно выбора файла

Если запись в журнал выполнена успешно, появится сообщение (Рисунок 57).

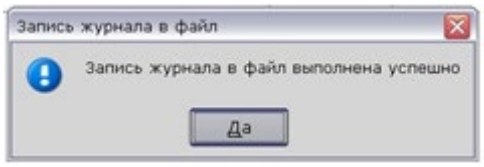

Рисунок 57 – Сообщение об успешной записи информации в файл

4.3 Подсистема контроля целостности

Подсистема контроля целостности обеспечивает контроль целостности СПО, которое поставляется на индивидуальном USB-носителе.

В зависимости от установленного режима, подсистема контроля целостности обеспечивает **посекторный** или **файловый** контроль СПО. Подсистема выполняет:

- расчет эталонных значений контрольных сумм (контрольных векторов) проверяемых секторов или файлов;
- сохранение полученных контрольных сумм в ЭНП изделия;
- проверку контрольных сумм проверяемых объектов при каждой загрузке СПО.

4.3.1 Пользователь и подсистема контроля целостности

При попытке входа пользователя в систему, подсистема контроля целостности активизируется после успешной аутентификации пользователя, перед переходом к загрузке СПО. В статусной строке появляются сообщения:

Успешная аутентификация.

и

Уберите ЭК из считывателя и нажмите Enter.

Необходимо извлечь ЭК аутентификации из считывателя и нажать клавишу **Enter**.

На экран выводятся окна, подобные представленным на рисунках ниже (Рисунок 58 и Рисунок 59), в которых показан процесс проверки целостности СПО.

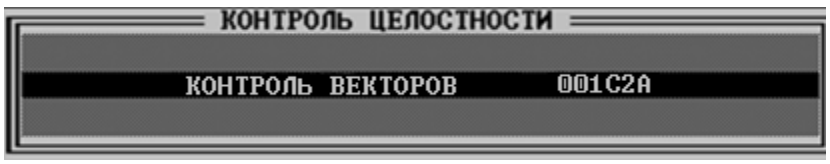

Рисунок 58 – Контроль целостности. Режим контроля – посекторный

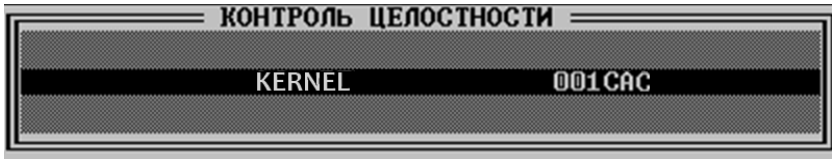

Рисунок 59 – Контроль целостности. Режим контроля – файловый

Если при проверке целостности не обнаружены ошибки, то пользователь получит доступ к запуску СПО с индивидуального USB-носителя.

В противном случае выдается сообщение:

Ошибка при КОНТРОЛЕ ВЕКТОРОВ.

или

<имя файла> ERR,

необходимо нажать клавишу **Enter** – выдается сообщение:

Ошибка при КОНТРОЛЕ ВЕКТОРОВ.

и ПЭВМ блокируется.

***Примечание**. Подсистема контроля целостности работает в **жестком** режиме, т.е. при нарушении целостности информации на носителе пользователя запрещается загрузка СПО. При нарушении целостности информации на носителе администратора СДЗ загрузка СПО разрешена. Сообщения о нарушении целостности носителя заносятся в ЖРС.*

4.3.2 Администратор и подсистема контроля целостности

4.3.2.1 *Терминал* и *сервер виртуализации*

При попытке входа в систему на *терминале* или *сервере виртуализации* подсистема контроля целостности активизируется после успешной аутентификации администратора СДЗ и после отказа от удаленного управления (см. п. 4.1.3.3). На экран в окно **Контроль целостности** выводится запрос на выполнение установки векторов (Рисунок 60).

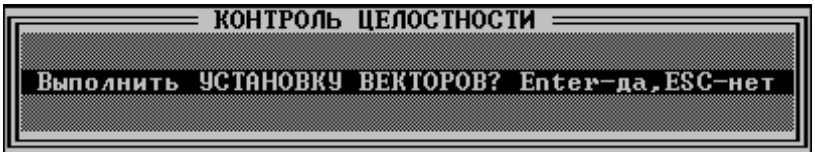

Рисунок 60 – Запрос на установку векторов

Для отказа от выполнения процедуры установки векторов нажать клавишу **Esc**. Далее выполняется переход к процедуре контроля целостности установленного носителя.

Если при проверке целостности не обнаружены ошибки, то выполняется запуск СПО.

В противном случае, появятся сообщения аналогичные представленным на рисунках выше (Рисунок 58 и Рисунок 59), а затем будет выполнена загрузка СПО с установленного носителя.

4.3.2.2 АРМ Администратора

Подсистема контроля целостности активизируется после успешной аутентификации администратора СДЗ. На экран в окно **Контроль целостности** выводится запрос на выполнение установки векторов (Рисунок 60).

Для отказа от выполнения процедуры установки векторов, необходимо нажать клавишу **Esc**, далее аналогично описанию проверки целостности СПО в п. 4.3.2.1.

Для выполнения процедуры установки векторов необходимо в окне **Контроль целостности** (Рисунок 60) нажать клавишу **Enter**. Процедура установки векторов выполняется в соответствии с п 4.1.3.2.3.

Внимание! *На АРМ администратора выполняется расчет эталонных значений контрольных сумм (установка векторов) всех используемых в АГ носителей СПО. Носитель СПО, для которого осуществляется установка векторов, должен устанавливаться в системный блок до включения питания ПЭВМ.*

5 Операции со сменными ключами

В процессе эксплуатации периодически (1 раз в 90 дней) необходимо выполнять смену ключей маскирования.

Для смены ключей маскирования:

1. Выполнить на узле **№001** генерацию сменных ключей.
2. Выполнить рассылку сгенерированных ключей для всех узлов АГ.
3. Послать всем узлам АГ команду смены ключей.

***Примечание**. Для успешной работы, на всех узлах АГ дата и время должны быть синхронизированы.*

5.1 Генерация сменных ключей

Генерация сменных ключей выполняется администратором на узле **№001**. Генерация сменных ключей описана в п. 4.2.2.

5.2 Рассылка сменных ключей

Рассылка сменных ключей выполняется администратором СДЗ на узле **№001** после выполнения процедуры генерации сменных ключей (см. п. 4.2.2).

5.3 Процедура смены ключей

Выполнение процедуры смены ключей АГ выполняется администратором СДЗ на узле **№001** после выполнения процедуры рассылки сменных ключей (см. п. 4.2.2).

6 Действия администратора при компрометации

6.1 Действия администратора при компрометации ЭК аутентификации

Под компрометацией ЭК аутентификации понимается их утрата, хищение, захват или другие происшествия, в результате которых ключи аутентификации утрачены.

При компрометации ЭК пользователя необходимо обратиться к администратору СДЗ, у которого ЭК в рабочем состоянии, для получения нового ЭК взамен скомпрометированного.

При компрометации ЭК второго администратора СДЗ (**ADMIN_2**) или третьего (**ADMIN_3**), первому администратору СДЗ необходимо выполнить следующие действия:

1) блокировать данного администратора СДЗ на всех узлах АГ;
2) выполнить удаление данного администратора СДЗ;
3) создать заново ЭК данного администратора СДЗ используя новый носитель;
4) провести повторную регистрацию данного администратора СДЗ в АГ.

В случае компрометации ЭК первого администратора СДЗ (**ADMIN_1**), необходимо заново выполнить развертывание всей АГ.

Внимание!

1 ЭК аутентификации должны храниться таким образом, чтобы исключить возможность несанкционированного доступа к информации на них.

2 Должна обеспечиваться смена пароля администраторов СДЗ при каждой смене их ЭК.

6.2 Действия администратора при компрометации терминала/сервера виртуализации

Изделие считается скомпрометированным, если имеются факты несанкционированного вскрытия корпуса терминала/сервера виртуализации посторонними лицами.

Необходимо выполнить следующие действия:

1) выполнить инициализацию скомпрометированного изделия;
2) выполнить внеочередную генерацию сменных ключей;

3) сформировать инсталляционный ключ;
4) выполнить инсталляцию скомпрометированного изделия;
5) выполнить внеочередную рассылку сменных ключей.

6.3 Действия администратора при компрометации АРМ Администратора

Изделие считается скомпрометированным, если имеются факты несанкционированного вскрытия корпуса АРМ Администратора.

В случае компрометации АРМ Администратора, необходимо заново выполнить развертывание всей АГ.

ПРИЛОЖЕНИЕ А Установка аппаратной части

А. 1 Требования к ПЭВМ

ПЭВМ, на которую устанавливается изделие, должна удовлетворять следующим требованиям:

- требования к аппаратной платформе сервера виртуализации:
  - процессор класса x86 с поддержкой технологии Intel-VT или AMD-V;
  - жесткий диск не менее 100 Гб;
  - наличие шины PCI-Express;
  - наличие разъема SATA на материнской плате;
  - оперативная память не менее 4 Гб.
- требования к аппаратной платформе терминала:
  - процессор класса x86 не ниже Pentium 4;
  - наличие шины PCI-Express;
  - наличие разъема SATA на материнской плате;
  - оперативная память не менее 256 Мб.

А. 2 Настройка BIOS

Изделие, установленное на *терминале/АРМ Администратора*, взаимодействует с СПО, загружаемой с USB-носителя, и допускает сокращенную конфигурацию дисков:

- один USB-носитель;
- ни одного ЖМД.

Изделие, установленное на *сервере виртуализации*, взаимодействует с СПО, загружаемой с USB-носителя, и допускает ограниченную конфигурацию дисков:

- один USB-носитель;
- количество ЖМД не регламентируется.

Настройка представления USB-носителей в качестве ЖМД должна быть выполнена в системном BIOS перед началом работы с платой изделия.

Например, для BIOS материнской платы P5b, в меню Boot, в разделе *Hard Disk Drives* установить для *1st Drive* USB-носитель:

«**USB: название контроллера**», на котором лежит образ СПО.

Загрузка СПО происходит с индивидуального USB-носителя любого администратора/пользователя, входящего в АГ.

СПО загружается из неизменяемого образа, целостность которого контролируется средствами изделия.

А. 3 Порядок установки изделия

Вынуть из упаковки плату изделия, считыватель, шлейфы и носитель с СПО, произвести их внешний осмотр, убедиться в отсутствии механических повреждений печатных плат, проводников и элементов.

1) Плата МИиКДС:

– выключить ПЭВМ, в которую предполагается установить изделие;
– подключить шлейф блокировки ПЭВМ:
  - отключить стандартный шлейф питания от материнской платы ПЭВМ;
  - подключить шлейф блокировки ПЭВМ, входящий в комплект поставки изделия, к стандартному шлейфу питания и к материнской плате ПЭВМ;
  - присоединить двухштырьковый соединитель шлейфа блокировки ПЭВМ к контактам на плате МИиКДС (Рисунок 61);
– установить плату в свободный слот PCI-Express ПЭВМ.

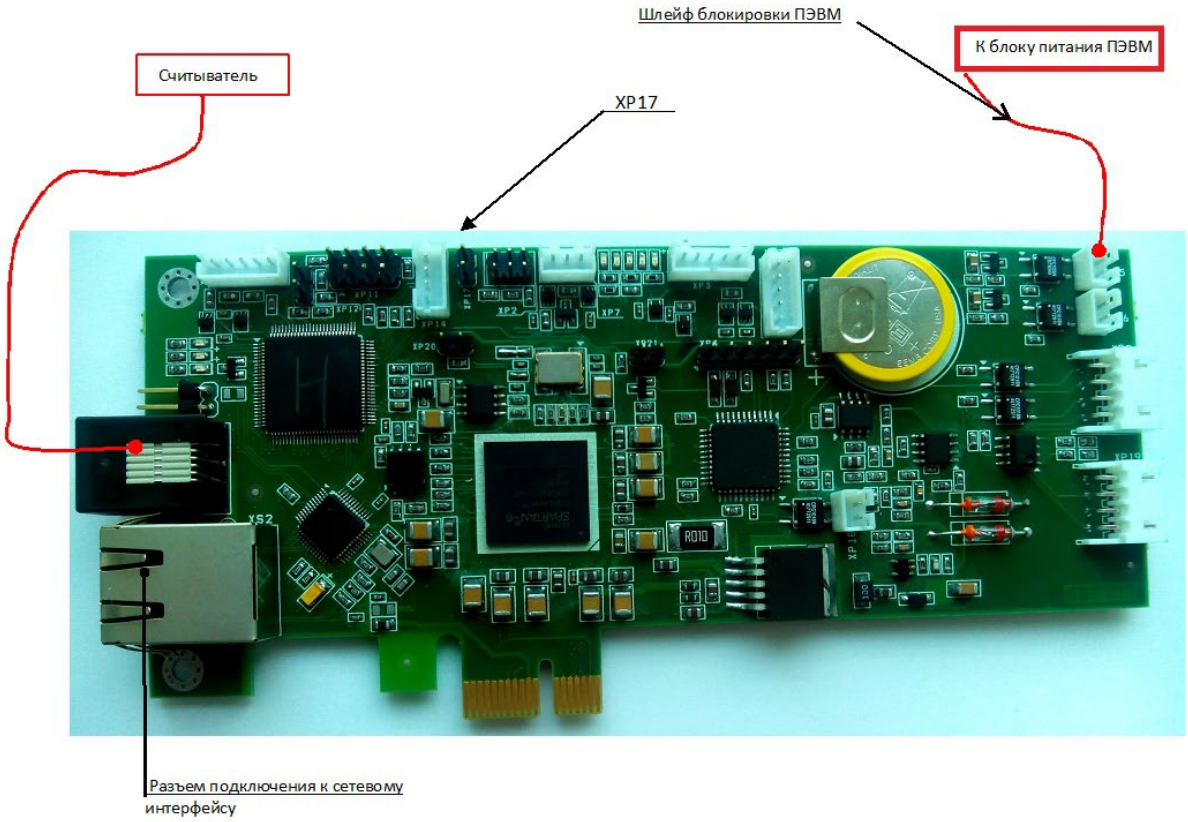

Рисунок 61 – Плата МИиКДС

2) СПО МИиКДС «Шина»:

СПО МИиКДС «Шина» поставляется на USB-носителе. Перед началом работы с платой изделия необходимо, в соответствии с п. А.2, выполнить настройку системного BIOS. USB-носитель, содержащий СПО МИиКДС «Шина», должен использоваться в качестве загрузочного ЖМД.

Внимание! *СПО МИиКЛС «Шина» устанавливается только на АРМ администратора.*

3) СПО «Терминал-Сервер»:

СПО «Терминал-Сервер» поставляется на USB-носителе, действия по установке аналогичны, описанным на шаге 1).

4) Считыватель:

Закрыть корпус системного блока и подключить считыватель - контактное устройство RDS-13, с помощью шлейфа, входящего в его состав, к разъему на плате МИиКДС (Рисунок 61).

А. 4 Подключение внешних интерфейсов

1. Подключить сетевые кабели:

– подключить разъем сетевого кабеля к разъему внешнего интерфейса (разъем подключения сетевого интерфейса) (Рисунок 61) на плате МИиКДС (локальная сеть для обслуживания АГ с установленными изделиями, связывающая все платы МИиКДС);

– подключить разъем сетевого кабеля к свободному разъему внешнего интерфейса материнской платы (локальная сеть, связывающая все ПЭВМ).

2. Подключить монитор, клавиатуру.
3. Подключить вилку шнура электропитания к однофазной сети переменного тока (220 В) с заземленной нейтралью.

ПРИЛОЖЕНИЕ Б Правила работы с электронными ключами DS1977 и DS1995 и контактным устройством RDS-13

Б.1 Назначение электронного ключа

Электронный ключ DS1977 предназначен для хранения ключевой информации администраторов, а также для создания инсталляционного и транспортного ключей.

Электронный ключ DS1995 предназначен для хранения ключевой информации пользователей.

Ключевая информация необходима для идентификации и аутентификации пользователя/администратора при входе в систему.

Администратор может работать с одним и тем же электронным ключом на нескольких ПЭВМ, входящих в АГ.

Для работы администратора/пользователя в составе АГ необходимо, чтобы электронный ключ был создан и зарегистрирован в изделиях, установленных на ПЭВМ, к которым разрешен доступ данного администратора/пользователя. Процедура создания и регистрации электронных ключей выполняется действующим администратором АГ на АРМ Администратора.

После создания электронного ключа администратору или пользователю выдается данный электронный ключ и сообщается пароль для входа в систему.

Электронный ключ и пароль необходимы для подтверждения права работать с установленным изделием. Электронный ключ требуется при каждой загрузке ПЭВМ.

Б.2 Технические характеристики DS1977 и DS1995 из семейства iButton

Электронные ключи DS1977 и DS1995 из семейства iButton работают в составе изделия, информация считывается и записывается в электронный ключ с помощью считывателя (контактное устройство RDS-13).

Хранение данных в памяти электронного ключа – в течение 10 лет.

Контактная стойкость – не менее 10^6 циклов запись/стирание.

Работоспособность электронного ключа обеспечивается при температуре окружающей среды от минус 40 до плюс 85 °С для DS1977 и от минус 40 до плюс 70 °С для DS1995.

Б.3 Порядок работы с электронным ключом DS1977/DS1995

Электронный ключ − это устройство в форме таблетки, вмонтированной в пластиковый держатель. В памяти электронного ключа хранится ключевая информация.

Электронный ключ работает совместно со считывателем, который, в свою очередь, подсоединен к плате изделия. Компактный профиль в форме таблетки позволяет электронному ключу автоматически центрироваться в считывателе, что дает возможность пользователям легко им оперировать. Доступ к данным может происходить при касании электронным ключом контактной площадки считывателя (Рисунок 62).

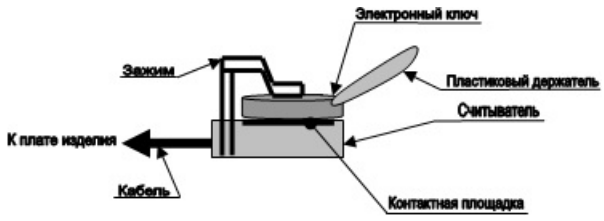

Рисунок 62 – Считыватель

На предложение системы установить электронный ключ пользователь должен плотно приложить к считывателю электронный ключ (Рисунок 62) и на предложение системы ввести пароль ввести свой пароль с помощью клавиатуры.

После этих действий доступ к ПЭВМ (запуск ОС) будет разрешен владельцам только тех электронных ключей, которые зарегистрированы в изделии на данной ПЭВМ, и при условии неизменности контролируемых объектов (список контролируемых объектов определяет администратор).

Если электронный ключ неправильно установлен, если в процессе чтения возникли ошибки или система обнаружила нарушения в структуре информации электронного ключа, в статусную строку выдаются соответствующие сообщения об ошибках. В этом случае следует убедиться, что электронный ключ правильно установлен и затем, после нажатия клавиши

Enter, повторить попытку ввода информации с электронного ключа. Если ошибка повторится, то необходимо обратиться к администратору (администратор должен заменить электронный ключ).

Если длительность процесса аутентификации превышает значение, установленное в плате изделия (120 секунд), то работа изделия будет остановлена и ПЭВМ заблокируется.

ПРИЛОЖЕНИЕ В Список сообщений об ошибках, выдаваемых в статусной строке при инсталляции и аутентификации

№, п/п	Сообщение	Тип сообщения	Пояснения и рекомендации
1	Истекло время аутентификации	О	Превышено время аутентификации. Необходимо перезагрузить ПЭВМ
2	Некорректный номер группы	О	Ввести корректный номер группы (от 1 до 21)
3	Некорректный номер узла	О	Ввести корректный номер узла (от 2 до 128)
4	Неправильный пароль или ЭК	О	Установить правильный ЭК или ввести правильный пароль
5	Неправильный сервисный код	О	Ввести правильный сервисный код. Сервисные коды поставляются на объект эксплуатации установленным порядком отдельно от изделий
6	Неправильный формат ИК	О	Неправильный формат ключа. Установить корректный ИК
7	Несовпадение паролей	О	Повторить ввод паролей аутентификации
8	Ошибка при загрузке изделия	С	Сбой изделия. При многократных сообщениях - изделие считать неисправным
9	Ошибка при установке векторов	С	Сбой носителя или носитель не установлен
10	Ошибка при КОНТРОЛЕ ВЕКТОРОВ	О	В процессе контроля целостности носителя информации была обнаружена ошибка
11	<имя файла> ERR	О	В процессе контроля целостности файла была обнаружена ошибка
12	Пользователь заблокирован.	И	Вход пользователя заблокирован в списке пользователей изделия
13	Превышено число попыток входа	И	Количество неудачных попыток входа пользователя/адинистратора больше 10
14	РАБОТА ИЗДЕЛИЯ ОСТАНОВЛЕНА	И	Необходимо перезагрузить ПЭВМ
15	Сбой при чтении ЭК	О/С	1 Вставлен неверный тип ЭК. 2 Сбой изделия
16	ЭК не установлен	О	1 Проверить ЭК и/или считыватель. 2 Сбой изделия
	Примечание. *Сообщения в статусной строке могут быть четырех*		

№, п/п	Сообщение	Тип сообщения	Пояснения и рекомендации
	типов: *1) сообщения, связанные с ошибками администратора/пользователя (О);* *2) сообщения о сбоях изделия (С);* *3) сообщения о событиях, которые могут быть вызваны или ошибками администратора/пользователя или сбоями изделия (О/С);* *4) информационные сообщения (И).*		

ПРИЛОЖЕНИЕ Г Список сообщений об ошибках, выдаваемых программой администратора

№, п/п	Сообщение	Тип сообщения	Пояснения и рекомендации
1	Зарегистрировано максимальное количество пользователей	О	При попытке зарегистрировать 126-го пользователя. Чтобы создать нового пользователя – необходимо удалить одного из существующих
2	Зарегистрированы все 3 администратора	О	При попытке зарегистрировать 4-го администратора. Чтобы создать нового администратора – необходимо удалить одного из существующих
3	Минимальная длина имени пользователя – 3 символа	О	Введено недостаточно длинное имя пользователя
4	Неверный пароль или ЭК	О	При проверке регистрации введен неправильный пароль или вставлен незарегистрированный ЭК. Выполнить проверку регистрации заново с правильным паролем и ЭК
5	Неверный тип ЭК	О	Не удалось прочитать ЭК или ЭК не является DS1977
6	Недостаточно прав для выполнения операции	О	При попытке выполнить недопустимую операцию
7	Нет связи с узлом	О	Запрашиваемый узел не отвечает. Проверить, установлена ли связь с узлом по сети, после чего выполнить операцию заново
8	Отсутствует линк	О	При отсутствии сигнала Link у сетевого интерфейса платы. Подключить плату к сети
9	Ошибка при записи в SPI	С	Сбой изделия. При многократных сообщениях - изделие считать неисправным
10	Ошибка при записи данных в STM	С	Сбой изделия. При многократных сообщениях - изделие считать неисправным
11	Ошибка при записи информации на ЭК	С	Сбой изделия. При многократных сообщениях - изделие считать неисправным
12	Ошибка при обращении к RTC	С	Сбой изделия. При многократных сообщениях - изделие считать неисправным

№, п/п	Сообщение	Тип сообщения	Пояснения и рекомендации
13	Ошибка при приеме/передаче данных через UART	С	Сбой изделия. При многократных сообщениях - изделие считать неисправным
14	Ошибка при проверке целостности данных	С	Сбой изделия. Выполнить инициализацию
15	Ошибка при чтении информации с ЭК	С	Сбой изделия. При многократных сообщениях - изделие считать неисправным
16	Ошибка при маскировании данных	С	Сбой изделия. При многократных сообщениях - изделие считать неисправным
17	Ошибка: неверный CRC	С	Сбой изделия. При многократных сообщениях - изделие считать неисправным
18	Ошибка: некорректный код команды	С	Сбой изделия. При многократных сообщениях - изделие считать неисправным
19	Пользователь с таким именем уже зарегистрирован	О	При создании пользователя на *АРМ Администратора*. Пользователь с таким именем был создан ранее. Создать пользователя с другим именем
20	Пользователь с таким номером ЭК уже зарегистрирован	О	При создании пользователя на *АРМ Администратора*. Пользователь с таким номером ЭК был создан ранее. Создать пользователя с другим ЭК
21	Пользователя с таким именем не существует	О	При проверке регистрации введено неправильное имя пользователя. Выполнить проверку регистрации заново с правильным именем пользователя
22	Пользователя не зарегистрирован на данном узле	О	Выполнена попытка прочитать статистику пользователя на узле, на котором он не зарегистрирован
23	Требуемая длина пароля – 8 символов	О	Введен недостаточно длинный пароль
24	ЭК не установлен	О	1 Проверить ЭК и/или считыватель. 2 Сбой изделия
Примечание - *Сообщения могут быть двух типов:* *1) сообщения, связанные с ошибками администратора/пользователя (О);* *2) сообщения о сбоях изделия (С).*			

ПРИЛОЖЕНИЕ Д Список сообщений журнала регистрации событий

№, п/п	Сообщение	Тип сообщения	Пояснения и рекомендации
1	Аутентификация	И	Выполнена успешная аутентификация пользователя/администратора на данном узле
2	Блокировка пользователя	И	Выполнена блокировка пользователя/администратора на данном узле
3	Ввод рабочего ключа KEY_1	И	Выполнена запись рабочего ключа KEY_1 с ЭК в плату изделия на данном узле
4	Ввод рабочего ключа KEY_2	И	Выполнена запись рабочего ключа KEY_2 с ЭК в плату изделия на данном узле
5	Ввод сменного ключа KEY_1	И	Выполнена запись сменного ключа KEY_1 с ЭК в плату изделия на данном узле
6	Ввод сменного ключа KEY_2	И	Выполнена запись сменного ключа KEY_2 с ЭК в плату изделия на данном узле
7	Вывод рабочих ключей KEY_1	И	Выполнено чтение рабочих ключей KEY_1 из платы изделия на АРМ Администратора и запись на ЭК
8	Вывод рабочих ключей KEY_2	И	Выполнено чтение рабочих ключей KEY_2 из платы изделия на АРМ Администратора и запись на ЭК
9	Генерация рабочих ключей KEY_1	И	На АРМ Администратора выполнена генерация рабочих ключей KEY_1
10	Генерация рабочих ключей KEY_2	И	На АРМ Администратора выполнена генерация рабочих ключей KEY_2
11	Генерация сменных ключей KEY_1	И	На АРМ Администратора выполнена генерация сменных ключей KEY_1
12	Генерация сменных ключей KEY_2	И	На АРМ Администратора выполнена генерация сменных ключей KEY_2
13	Загрузка ОС	И	Переход к загрузке ОС
14	Ошибка аутентификация	О	Произошла ошибка при выполнении аутентификации пользователя (неверный ЭК или пароль) на данном узле
15	Ошибка при контроле	О	Нарушена целостность носителя данных

№, п/п	Сообщение	Тип сообщения	Пояснения и рекомендации
	векторов		(СПО) на данном узле
16	Прием команды смены ключей маскирования	И	На данном узле принята команда смены ключей маскирования
17	Разблокировка пользователя	И	На данном узле выполнено снятие блокировки пользователя
18	Регистрация пользователя	И	На АРМ Администратора – выполнено создание нового пользователя. На терминале/сервере – выполнена регистрация существующего пользователя, созданного ранее на АРМ Администратора
19	Смена ключей маскирования	И	На терминале/сервере выполнена смена ключей маскирования
20	Смена пароля пользователя	И	Выполнена смена пароля пользователя/администратора на данном узле
21	Старт сессии	И	Начало работы очередной сессии
22	Удаление пользователя	И	Выполнено удаление пользователя из списка
23	Установка векторов	И	Успешно выполнена установка векторов
	Примечание. *Сообщения в ЖРС могут быть двух типов:* *информационные сообщения (И);* *сообщения, связанные с ошибками администратора/пользователя (О).*		

ПРИЛОЖЕНИЕ Е Структура журнала групповых операций

Журнал групповых операций (ЖГО) содержит информацию по групповым операциям, которые выполняются программой администрирования.

К групповым операциям относятся:

- рассылка сменных ключей маскирования в узлы АГ;
- смена ключей маскирования на всех узлах АГ;
- смена пароля пользователя;
- исключение пользователя из списка пользователей АГ.

Выполнение каждой из пяти групповых операций сопровождается записями в ЖГО.

ЖГО дает возможность администратору определить, на каких узлах данная групповая операции была успешно выполнена, а для каких узлов необходимо повторное выполнение данной групповой операции.

ЖГО представляет из себя файл ***group_log.txt***, который находится в каталоге ***/root***. В нем содержится информация по групповым операциям нескольких сессий.

Информация по каждой сессии сопровождается записью следующего формата:

Сессия: № сессии Дата Время

Каждая команда групповой операции сопровождается записью следующего формата:

Название операции Номер узла Статус завершения операции

Пример журнала групповых операций

Сессия: 007 02/12/2015 13:27

Пересылка ключей маскирования Узел 022 Ошибка: Нет связи с узлом

Пересылка ключей маскирования Узел 030 Выполнено

Сессия: 007 02/12/2015 13:29

Пересылка команды смены ключей маскирования Узел 001 Выполнено

Пересылка команды смены ключей маскирования Узел 022 Ошибка: Нет связи с узлом

Пересылка команды смены ключей маскирования Узел 030 Выполнено

Сессия: 007 02/12/2015 13:56

Пересылка ключей маскирования Узел 022 Ошибка: Нет связи с узлом

Пересылка ключей маскирования Узел 030 Выполнено

Сессия: 007 02/12/2015 13:57

Пересылка команды смены ключей маскирования Узел 001 Выполнено

Пересылка команды смены ключей маскирования Узел 022 Ошибка: Нет связи с узлом

Пересылка команды смены ключей маскирования Узел 030 Выполнено

Сессия: 007 02/12/2015 14:14

Смена пароля пользователя user_1 Узел 001 Выполнено

Смена пароля пользователя user_1 Узел 030 Выполнено.

ПРИЛОЖЕНИЕ Ж Демонтаж изделия

Ж.1 Порядок демонтажа изделия

Для демонтажа изделия необходимо выполнить следующие действия:

- проинициализировать плату изделия согласно п. 4.2.2 настоящего руководства;
- изъять из ПЭВМ аппаратную части изделия согласно приложению к документу (ПРИЛОЖЕНИЕ Е).

Ж.2 Демонтаж аппаратной части изделия

Демонтаж аппаратной части изделия выполняется в следующей последовательности:

- выключить ПЭВМ;
- отключить внешние интерфейсы;
- отключить считыватель;
- вскрыть корпус ПЭВМ;
- изъять плату изделия из разъема системной шины PCI-Express;
- отключить установленный шлейф блокировки ПЭВМ и заменить его на стандартный;
- закрыть корпус системного блока ПЭВМ.

ПРИЛОЖЕНИЕ И Описание программ тестирования функций безопасности изделия

Администратор имеет возможность выполнять процедуры тестирования функций безопасности изделия с помощью трех программ тестирования, входящих в СПО МИиКДС «Шина».

Программы тестирования находятся в каталоге ***/usr/bin***. Для перехода в данный каталог, ввести в командную строку:

```
cd /usr/bin
```

Программа «Тест целостности программного кода» (файл ***test_iv_code***) выполняет проверку целостности программного кода прошивки изделия.

Программа запускается из командной строки:

```
    ./test_iv_code nnn
```

где **nnn** – номер тестируемого узла.

При успешной проверке целостности программы прошивки на заданном узле тест выдает сообщение:

test_iv_code ok

Программа «Тест целостности данных в плате» (файл ***test_iv_data***) выполняет проверку целостности данных, хранимых в плате изделия.

Программа запускается из командной строки:

```
./ test_iv_data nnn
```

где **nnn** – номер тестируемого узла.

При успешной проверке целостности данных, хранимых в плате заданного узла, тест выдает сообщение:

test_iv_data ok

Программа «Тест переполнения ЖРС» (файл ***test_log***) – выполняется тестирование на переполнение ЖРС.

Программа запускается из командной строки:

```
./ test_log nnn
```

где **nnn** – номер тестируемого узла.

Тестирование выполняется около 25-ти минут. При успешном выполнении тестирования выполняется ***очистка*** ЖРС на тестируемом узле и выдает сообщение:

test_log ok

Тестирование всех узлов АГ выполняется на *АРМ Администратора*. Тестируемый узел должен быть доступен для *АРМ администратора* по сетевому интерфейсу.

В таблице ниже приведен список кодов сообщений, выдаваемые программами тестирования.

Список сообщений программ тестирования:

Код сообщения	Сообщение	Пояснения и рекомендации
0xAA	Код успешного выполнения операции	-
0xCA	Недостаточно прав для выполнения операции	Запуск теста возможен только с правами администратора
0xD2	Ошибка при проверке целостности данных	Нарушена целостность данных, хранящихся в плате изделия
0xD3	Ошибка при записи в SPI	Сбой изделия. При многократных сообщениях, изделие считать неисправным
0xD4	Ошибка при обращении к RTC	Сбой изделия. При многократных сообщениях, изделие считать неисправным
0xD5	Ошибка при обращении к ДСЧ	Сбой изделия. При многократных сообщениях, изделие считать неисправным
0xD6	Неудачное завершение теста ДСЧ	Сбой изделия. При многократных сообщениях, изделие считать неисправным
0xD7	Ошибка при шифровании данных	Сбой изделия. При многократных сообщениях, изделие считать неисправным
0xD8	Ошибка при приеме/передаче через UART	Сбой изделия. При многократных сообщениях, изделие считать неисправным
0xF1	Ошибка при записи данных в STM	Сбой изделия. При многократных сообщениях, изделие считать неисправным

Код сообщения	Сообщение	Пояснения и рекомендации
0xF2	Нет связи с узлом	Запрашиваемый узел не отвечает. Проверить, установлена ли связь с узлом по сети, после чего выполнить операцию заново
0xF3	Отсутствует линк	При отсутствии сигнала Link у сетевого интерфейса платы. Подключить плату к сети
0xDD	Ошибка: неверный CRC	Сбой изделия. При многократных сообщениях - изделие считать неисправным

Перечень принятых сокращений

Сокращение	Расшифровка
АГ	Административная группа
АРМ	Автоматизированное рабочее место
ГИС	Государственная информационная система
ДСЧ	Физический датчик случайных чисел
ИК	Инсталляционный ключ
ЖГО	Журнал групповых операций
ЖМД	Жесткий магнитный диск
ЖРС	Журнал регистрации событий
ЛВС	Локальная вычислительная сеть
МИиКДС	Модуль идентификации и контроля доверенной среды
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
ПЭВМ	Персональная электронная вычислительная машина
СДЗ	Средство доверенной загрузки
СПО	Специальное программное обеспечение
ТК	Транспортный ключ
ЭК	Электронный ключ
ЭНП	Энергонезависимая память

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					