



**ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО**  
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

**УТВЕРЖДЕН**

11443195.4012.054 94 ЛУ

**Аппаратно-программный модуль доверенной  
загрузки (АПМДЗ) «Аккорд-АМДЗ»**

**Правила применения**

11443195.4012.054 ПП

|               |              |              |              |              |
|---------------|--------------|--------------|--------------|--------------|
| Инов. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата |
|               |              |              |              |              |

## СОДЕРЖАНИЕ

|                                                                                                  |    |
|--------------------------------------------------------------------------------------------------|----|
| 1 ВВЕДЕНИЕ .....                                                                                 | 3  |
| 2 УСЛОВИЯ ПРИМЕНЕНИЯ ИЗДЕЛИЯ.....                                                                | 4  |
| 2.1 Группа эксплуатации аппаратуры согласно ГОСТ В 20.39.304-98.....                             | 4  |
| 2.2 Требования к аппаратным ресурсам ЭВМ.....                                                    | 4  |
| 2.3 Требования к программным ресурсам ЭВМ .....                                                  | 4  |
| 2.4 Организационно-технические требования к ЭВМ и изделию.....                                   | 5  |
| 2.5 Ограничения, связанные с особенностями и возможностями изделия по КЦ программной среды ..... | 5  |
| 2.6 Ограничения, связанные с особенностями изделия .....                                         | 6  |
| 3 УСЛОВИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И<br>СООТВЕТСТВИЯ ПРЕДЪЯВЛЕННЫМ ТРЕБОВАНИЯМ.....   | 7  |
| 3.1 Подготовка к эксплуатации.....                                                               | 7  |
| 3.2 Ввод в эксплуатацию .....                                                                    | 7  |
| 3.3 Эксплуатация .....                                                                           | 10 |
| 3.4 Вывод из эксплуатации.....                                                                   | 13 |
| 3.5 Действия при НСД и компрометации служебной информации.....                                   | 13 |
| 3.6 Обновление и модернизация.....                                                               | 14 |
| 3.7 Специальные требования .....                                                                 | 14 |
| 4 Условные обозначения.....                                                                      | 15 |
| 5 ОТВЕТСТВЕННОСТЬ ЗА ВЫПОЛНЕНИЕ ПРАВИЛ ПРИМЕНЕНИЯ.....                                           | 16 |

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

|           |      |            |       |      |                                                                        |  |  |          |  |      |        |  |
|-----------|------|------------|-------|------|------------------------------------------------------------------------|--|--|----------|--|------|--------|--|
|           |      |            |       |      | 11443195.4012.054 ПП                                                   |  |  |          |  |      |        |  |
| Изм.      | Лист | № докум.   | Подп. | Дата |                                                                        |  |  |          |  |      |        |  |
| Разраб.   |      | Староверов |       |      | Аппаратно-программный модуль доверенной загрузки (АПМДЗ) «Аккорд-АМДЗ» |  |  | Лит.     |  | Лист | Листов |  |
| Пров.     |      | Алтухов    |       |      |                                                                        |  |  |          |  | 2    | 16     |  |
|           |      |            |       |      |                                                                        |  |  | ОКБ САПР |  |      |        |  |
| Н. контр. |      | Счастный   |       |      |                                                                        |  |  |          |  |      |        |  |
| Утв.      |      | Назаров    |       |      |                                                                        |  |  |          |  |      |        |  |
|           |      |            |       |      | Правила применения                                                     |  |  |          |  |      |        |  |

**Правила применения**

**ОКБ САПР**

## 1 ВВЕДЕНИЕ

Наименование изделия - аппаратно-программный модуль доверенной загрузки (АПМДЗ) «Аккорд-АМДЗ» (далее по тексту – комплекс «Аккорд-АМДЗ», «Аккорд-АМДЗ», комплекс, изделие, АПМДЗ).

Децимальный номер изделия - 11443195.4012.054.

Изделие разработано в соответствии с ТУ 4012-054-11443195-2013, предназначено для обеспечения защиты информации от несанкционированного доступа (НСД) при многопользовательском режиме эксплуатации как в автономных средствах вычислительной техники (СВТ), так и в СВТ в составе локальных вычислительных сетей (ЛВС).

Изделие предназначено для использования на территории Российской Федерации и обработки информации, содержащей сведения, составляющие государственную тайну при выполнении следующих требований:

- обязательное выполнение условий, перечисленных в разделе 2 «Условия применения изделия» и в разделе 3 «Условия обеспечения безопасности информации и соответствия предъявляемым требованиям» настоящего документа;
- соблюдение условий, перечисленных в предписании на эксплуатацию СВТ с установленным изделием;
- сохранение в тайне аутентифицирующей информации администраторов и пользователей (АИП), а также информации, записанной в энергонезависимую память изделия (в том числе в ходе ремонта, регламентных и прочих работ);
- соблюдение прочих правил эксплуатации, установленных в эксплуатационной документации на изделие.

Все возможные противоречия эксплуатационной и другой сопроводительной документации на изделие трактуются в пользу настоящих правил.

Регистрационные номера приобретенных или полученных при передаче от одной организации к другой, а также утилизированных (уничтоженных) установленным порядком изделий должны сообщаться в войсковую часть 43753-С.

|                |  |
|----------------|--|
| Подпись и дата |  |
| Инв. № дубл.   |  |
| Взам. инв. №   |  |
| Подпись и дата |  |
| Инв. № подл.   |  |

|     |      |             |         |      |                      |      |
|-----|------|-------------|---------|------|----------------------|------|
|     |      |             |         |      | 11443195.4012.054 ПП | Лист |
|     |      |             |         |      |                      | 3    |
| Изм | Лист | № документа | Подпись | Дата |                      |      |

## 2 УСЛОВИЯ ПРИМЕНЕНИЯ ИЗДЕЛИЯ

### 2.1 Группа эксплуатации аппаратуры согласно ГОСТ В 20.39.304-98

Группа эксплуатации изделия – 1.1 согласно классификации ГОСТ В 20.39.304-98. Аппаратная часть комплекса по воздействию климатических факторов относится к виду климатического исполнения УХЛ4 по ГОСТ 15150-69 и предназначена для установки в закрытых отапливаемых помещениях и эксплуатации в условиях круглосуточной или сменной работы АС (СВТ) с перерывами на техническое обслуживание в соответствии с регламентом.

Нормальными климатическими условиями эксплуатации аппаратной части комплекса являются:

|                                             |                                                |
|---------------------------------------------|------------------------------------------------|
| температура окружающего воздуха             | плюс 25±10 С                                   |
| относительная влажность окружающего воздуха | от 45 до 80%                                   |
| атмосферное давление                        | от 84,0 до 054,7 кПа (от 630 до 800 мм рт.ст.) |

### 2.2 Требования к аппаратным ресурсам ЭВМ

2.2.1 Для установки комплекса «Аккорд-АМДЗ» необходим следующий минимальный состав технических средств:

- ЭВМ типа IBM PC, сервер или рабочая станция, основанная на процессоре с архитектурой x86 (IA-32) или x86-64 (AMD64), с объемом RAM не менее 128 Мбайт, функционирующая под управлением операционной системы, поддерживающей любую из файловых систем: FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX, Ext4, ReiserFS;
- наличие свободного разъема на материнской плате СВТ, соответствующего устанавливаемому типу специализированного контроллера АПМДЗ (подробнее см. таблицу 2 Конфигуратора (К 11443195.4012.054)).

### 2.3 Требования к программным ресурсам ЭВМ

2.3.1 BIOS СВТ должен соответствовать одному из условий:

1) BIOS должен реализовывать интерфейс SMBIOS в соответствии со спецификацией версии 2.3; Plug and Play BIOS Specification, Version 1.0A, May 5, 1994; BIOS Boot Specification, Version 1.01; «El Torito» Bootable CD-ROM Format Specification, Version 1.0, January 25; VESA BIOS Extension/Serial Control Interface Standard Version: 1.0 Revision: 2;

2) для UEFI BIOS: Unified Extensible Firmware Interface Specification Version 2.4 с поддержкой CSM, соответствующей спецификации Platform Innovation Framework for EFI Compatibility Support Module Specification Rev. 97.

|                |  |
|----------------|--|
| Подпись и дата |  |
| Инв. № дубл.   |  |
| Взам. инв. №   |  |
| Подпись и дата |  |
| Инв. № подл.   |  |

|     |      |             |         |      |                      |      |
|-----|------|-------------|---------|------|----------------------|------|
|     |      |             |         |      | 11443195.4012.054 ПП | Лист |
| Изм | Лист | № документа | Подпись | Дата |                      | 4    |

| Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата |
|--------------|----------------|--------------|--------------|----------------|
|              |                |              |              |                |

- физическая охрана СВТ (АС) и ее оборудования с помощью технических средств, специального персонала, или других организационно-технических мер, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса, предотвращению перепрограммирования пользователями как BIOS системной платы, так и всех расширений BIOS, установленных в СВТ;
- наличие администратора безопасности информации – привилегированного пользователя, имеющего особый статус и абсолютные полномочия. Обязанности администратора БИ по применению комплекса изложены в документе «Руководство администратора» (11443195.4012.054 90);
- учет носителей информации и идентификаторов пользователей;
- периодическое тестирование средств защиты комплекса «Аккорд-АМДЗ».

## 2.5 Ограничения, связанные с особенностями и возможностями изделия по КЦ программной среды

Изделие поддерживает схемы разметки дисков MBR и GPT.

Максимальное количество файлов, которые можно установить на контроль, зависит от операционной системы, длины пути к каталогу, где находятся файлы и выбранного режима контроля целостности (КЦ). Среднее количество составляет 200 файлов.

В операционной системе Linux предусмотрена возможность контроля файловых систем, размещённых на логических томах, созданных с использованием LVM2 (Logical Volume Manager).

Изделие поддерживает полные имена файлов длиной до 500 символов.

## 2.6 Ограничения, связанные с особенностями изделия

Максимальное количество учетных записей пользователей (пользователь «Гл.Администратор», пользователи, входящие в группы «Администраторы» и «Обычные»), зарегистрированных на одной СВТ – 1022.

Размер энергонезависимой памяти, в которой размещается системный журнал, составляет 256 Кбайт. Такой объем памяти позволяет вместить в журнале не менее 1000 записей. При штатной работе «Аккорд-АМДЗ» (когда в системе отсутствуют серийные нарушения целостности файлов/реестра и не используется чрезмерно глубокая вложенность файлов в каталогах) количество записей в журнале может быть больше этого значения в десятки или сотни раз.

Комплекс не накладывает ограничений на работу с клавиатурой и манипулятором типа «мышь», подключаемыми в СВТ по USB-интерфейсу.

|              |                |              |              |                |                      |  |  |  |  |      |
|--------------|----------------|--------------|--------------|----------------|----------------------|--|--|--|--|------|
| Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата |                      |  |  |  |  |      |
|              |                |              |              |                |                      |  |  |  |  |      |
|              |                |              |              |                |                      |  |  |  |  |      |
| Изм          | Лист           | № документа  | Подпись      | Дата           | 11443195.4012.054 ПП |  |  |  |  | Лист |
|              |                |              |              |                |                      |  |  |  |  | 6    |

### 3 УСЛОВИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СООТВЕТСТВИЯ ПРЕДЪЯВЛЕННЫМ ТРЕБОВАНИЯМ

#### 3.1 Подготовка к эксплуатации

Перед началом эксплуатации комплекса необходимо:

3.1.1 Проверить соответствие рабочего места (РМ) условиям применения комплекса, приведенным в разделе 2 «Условия применения изделия», и специальным требованиям, приведенным в разделе 3.7 «Специальные требования» настоящего документа.

3.1.2 Проверить комплектность поставки комплекса в соответствии с п. 4 «Комплектность поставки» и наличие всех необходимых записей и отметок, в соответствии п. 5 «Свидетельство о приемке» Формуляра (11443195.4012.054 ФО).

3.1.3 Провести исследование технических средств СВТ (в том числе исследование системной программы BIOS) на предмет отсутствия в их реализации аппаратно-программных механизмов, которые могут привести к нарушению правильности функционирования СВТ и комплекса или к утечке защищаемой информации. Объем и глубина исследований технических средств определяется степенью секретности (конфиденциальности) защищаемой информации и зависит от принятой модели нарушителя и актуальных угроз, изложенных в соответствующих требованиях. По результатам проведенных исследований принимается решение о возможности использования комплекса в СВТ конкретного типа.

3.1.4 Определить перечень объектов программной среды СВТ, целостность которых подлежит контролю средствами комплекса. Сформированный перечень должен быть достаточным для гарантированной загрузки штатной операционной системы, контроля целостности программных средств защиты информации (при их наличии) и контроля необходимых файлов пользователей.

3.1.5 Выполнить следующие организационно-технические меры:

3.1.5.1 Установить комплекс с учетом необходимых аппаратных и программных средств, перечисленных в разделе 2 «Условия применения изделия» настоящего документа, необходимых для выполнения комплексом своих защитных функций.

3.1.5.2 Обеспечить меры противодействия НСД к техническим средствам СВТ (физическая охрана, меры по сохранению целостности корпуса и т.п.) и комплекса на всех стадиях его использования, транспортировки и хранения.

3.1.5.3 Обеспечить меры противодействия нештатной модификации встроенного ПО СВТ (в том числе BIOS).

#### 3.2 Ввод в эксплуатацию

3.2.1 При вводе изделия в эксплуатацию необходимо сделать запись в Паспорте или Формуляре о вводе комплекса в эксплуатацию.

|              |                |              |              |                |                      |  |  |  |  |      |
|--------------|----------------|--------------|--------------|----------------|----------------------|--|--|--|--|------|
| Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата |                      |  |  |  |  | Лист |
|              |                |              |              |                |                      |  |  |  |  |      |
|              |                |              |              |                |                      |  |  |  |  |      |
|              |                |              |              |                |                      |  |  |  |  |      |
| Изм          | Лист           | № документа  | Подпись      | Дата           | 11443195.4012.054 ПП |  |  |  |  | 7    |

3.2.2 При вводе изделия в эксплуатацию выполняется процедура проверки администратором возможности блокировки ЭВМ в случае непередачи управления на «Аккорд-АМДЗ».

Последовательность действий при проверке:

- установить таймаут сторожевого таймера на время, заведомо достаточное для загрузки ОС после прохождения контрольных процедур согласно документации на комплекс;
- в утилите управления комплексом перейти на вкладку «Регламенты», напротив поля «Проверка блокировки» нажать кнопку <Проверить>;
- убедиться, что появилось окно с сообщением «Проверка включена», нажать ОК;
- выйти из утилиты управления с перезагрузкой.

Критерий оценки: проверка завершилась успешно, если однократно (в следующем сеансе) через указанный таймаут работа ОС заблокирована.

В случае если средствами «Аккорд-АМДЗ» не удалось заблокировать ЭВМ, эксплуатация «Аккорд-АМДЗ» на данном ЭВМ должна быть запрещена.

3.2.3 Для каждой учетной записи пользователя комплекса в соответствии с внутренними документами организации заказчика, а также организационно-распределительными документами учреждения и должностными инструкциями работников, администратором комплекса должны быть установлены соответствующий идентификатор и пароль, а также установлены следующие групповые/персональные значения следующих параметров:

«Персональные параметры» (отображаются только при смене идентификатора):

- «Дата начала срока действия АИП\_АНП» – дата начала срока действия аутентифицирующей информации, хранящейся на аутентифицирующем носителе пользователя;
- «Дата окончания срока действия АИП\_АНП» – дата окончания срока действия аутентифицирующей информации, хранящейся на аутентифицирующем носителе пользователя.
- «Дата начала срока действия пароля» – дата начала срока действия пароля пользователя;
- «Дата окончания срока действия пароля» – дата окончания срока действия пароля пользователя;
- «Количество неудачных попыток доступа» – количество неудачных подряд идущих попыток доступа пользователя, по превышении которого работа пользователя блокируется;
- «Общее количество всех попыток доступа» – общее количество всех попыток доступа пользователя, по превышении которого работа пользователя блокируется;

«Параметры пароля»:

- «Минимальная длина» - параметр определяет количество символов, контролируемое при создании и смене пароля. Минимальная длина пароля – 8 символов.
- «Время действия» - параметр определяет количество дней, в течении которого пароль будет действовать.

|              |                |              |              |                |                      |      |
|--------------|----------------|--------------|--------------|----------------|----------------------|------|
| Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата | 11443195.4012.054 ПП | Лист |
|              |                |              |              |                |                      | 8    |
| Изм          | Лист           | № документа  | Подпись      | Дата           |                      |      |

- «Попыток для смены» - количество попыток смены пароля: от 0 (не ограничено) до 5. Этот параметр определяет допустимое число попыток смены пароля, если пользователю разрешено самому выполнять такую операцию. Если за отведенное число попыток пароль не сменен корректно, выполняется перезагрузка компьютера.
- «Кто может менять пароль» - смену пароля осуществляет только администратор.
- «Алфавит пароля» - определяет набор символов, которые обязательно должны использоваться при вводе пароля. При установке флага «Только генерировать» пароль генерируется таким образом, чтобы в нем обязательно присутствовал хотя бы один символ из набора, заданного в параметре «Алфавит пароля».

«Время действия»:

- «Дата начала работы» – определяет дату, с наступлением которой работа для пользователей, входящих в группу «Администраторы», разрешается на текущем компьютере;
- «Дата конца работы» – определяет дату, с наступлением которой работа для пользователей, входящих в группу «Администраторы», запрещается на текущем компьютере.

«Атрибуты доступа» (для пользователей, входящих в группу «Администраторы»):

- «Редактирование настроек». При установке данного флага выбранный пользователь может изменять общие настройки комплекса.
- «Управление журналом». При установке данного флага выбранный пользователь может просматривать и очищать системный журнал.
- «Редактирование пользователей». При установке данного флага выбранный пользователь может выполнять редактирование списков пользователей.
- «Редактирование контроля». При установке данного флага выбранный пользователь может выполнять редактирование списков контроля целостности аппаратуры и реестра, служебных областей жестких дисков, файлов.

3.2.4 Администратором комплекса должны быть установлены настройки параметров работы комплекса (при необходимости изменения значений, установленных по умолчанию):

«Данные конфигурации»:

- «Страница идентификатора» – определяет, с какой страницы внутренней памяти персонального идентификатора располагается служебная информация комплекса «Аккорд-АМДЗ». Данный параметр изменять не рекомендуется. Изменение допускается, если используется ПО других производителей, которое осуществляет запись/чтение в идентификатор именно в 0-1 страницу памяти. Номер страницы должен быть четным.
- «Таймаут для идентификатора» и «Таймаут для пароля» определяют интервал времени, отведенный для процедур начальной идентификации и аутентификации соответственно.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                |             |         |      |                      |                |  |  |  |      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------|---------|------|----------------------|----------------|--|--|--|------|
| Инв. № подл.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Подпись и дата |             |         |      | Инв. № дубл.         | Подпись и дата |  |  |  |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                |             |         |      |                      |                |  |  |  |      |
| Взам. инв. №                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                |             |         |      |                      |                |  |  |  |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                |             |         |      |                      |                |  |  |  |      |
| Подпись и дата                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                |             |         |      |                      |                |  |  |  |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                |             |         |      |                      |                |  |  |  |      |
| <p>пользователь может изменять общие настройки комплекса.</p> <ul style="list-style-type: none"><li>– «Управление журналом». При установке данного флага выбранный пользователь может просматривать и очищать системный журнал.</li><li>– «Редактирование пользователей». При установке данного флага выбранный пользователь может выполнять редактирование списков пользователей.</li><li>– «Редактирование контроля». При установке данного флага выбранный пользователь может выполнять редактирование списков контроля целостности аппаратуры и реестра, служебных областей жестких дисков, файлов.</li></ul> <p>3.2.4 Администратором комплекса должны быть установлены настройки параметров работы комплекса (при необходимости изменения значений, установленных по умолчанию):</p> <p>«Данные конфигурации»:</p> <ul style="list-style-type: none"><li>– «Страница идентификатора» – определяет, с какой страницы внутренней памяти персонального идентификатора располагается служебная информация комплекса «Аккорд-АМДЗ». Данный параметр изменять не рекомендуется. Изменение допускается, если используется ПО других производителей, которое осуществляет запись/чтение в идентификатор именно в 0-1 страницу памяти. Номер страницы должен быть четным.</li><li>– «Таймаут для идентификатора» и «Таймаут для пароля» определяют интервал времени, отведенный для процедур начальной идентификации и аутентификации соответственно.</li></ul> |                |             |         |      |                      |                |  |  |  |      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                |             |         |      |                      |                |  |  |  | Лист |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                |             |         |      | 11443195.4012.054 ПП |                |  |  |  | 9    |
| Изм                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Лист           | № документа | Подпись | Дата |                      |                |  |  |  |      |

- |              |                |              |              |                |
|--------------|----------------|--------------|--------------|----------------|
| Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата |
|              |                |              |              |                |

ИИВ. № 1

|              |  |
|--------------|--|
| Взам. инв. № |  |
|--------------|--|

|                |  |
|----------------|--|
| Подпись и дата |  |
|----------------|--|

|       |  |
|-------|--|
| ПОДЛ. |  |
|-------|--|

- генератор случайных чисел (исправность и качество).

### 3.3.1.1 Проверка компонентов.

- а. Конфигурация ПЛИС (исправность и целостность).

#### Последовательность действий при проверке:

- включить ЭВМ и осуществить вход Администратором.

#### Критерии оценки:

Испытание завершилось успешно, если в результате выполнения программы не зафиксировано сообщений об ошибках.

- б. Тракт ввода информации с персонального идентификатора (исправность).

#### Последовательность действий при проверке:

- включить ЭВМ и осуществить вход Администратором;
- согласно документации на комплекс выполнить регистрацию нового пользователя: задать данные аутентификации, назначить персональный идентификатор и пароль. В процессе регистрации для данного пользователя персонального идентификатора выбрать вариант работы с секретным ключом – «Генерировать»;
- убедиться, что пользователь добавлен в базу данных «Аккорд-АМДЗ»: имя пользователя появилось в списке пользователей на вкладке «Пользователи», в журнале событий сделана соответствующая запись о регистрации нового пользователя;
- удалить пользователя из базы данных «Аккорд-АМДЗ»;
- согласно документации на комплекс, выполнить регистрацию нового пользователя: назначить персональный идентификатор и пароль. В процессе регистрации для данного пользователя персонального идентификатора выбрать вариант работы с секретным ключом – «Использовать существующий»;
- убедиться, что пользователь добавлен в базу данных «Аккорд-АМДЗ»: имя пользователя появилось в списке пользователей на вкладке «Пользователи»; для данного пользователя автоматически установлены данные аутентификации, заданные на этапе первичной регистрации данного пользователя (с использованием варианта работы с секретным ключом «Генерировать»); в журнале событий сделана соответствующая запись о регистрации нового пользователя.

#### Критерии оценки:

Испытание завершилось успешно, если в результате выполнения описанной последовательности действий не зафиксировано сообщений об ошибках.

- с. Флеш-память с ПО «Аккорд-АМДЗ» и базой данных (исправность и целостность)

#### Последовательность действий при проверке:

- включить ЭВМ и осуществить вход Администратором;
- в утилите управления комплексом перейти на вкладку «Регламенты», напротив поля «Проверка целостности ПО» нажать кнопку <Проверить>.

|              |                |              |              |                |                      |      |
|--------------|----------------|--------------|--------------|----------------|----------------------|------|
| Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата | 11443195.4012.054 ПП | Лист |
|              |                |              |              |                |                      | 11   |
|              |                |              |              |                |                      |      |
|              |                |              |              |                |                      |      |
|              |                |              |              |                |                      |      |
| Изм          | Лист           | № документа  | Подпись      | Дата           |                      |      |

- в утилите управления комплексом перейти на вкладку «Регламенты», напротив поля «Проверка целостности данных» нажать кнопку <Проверить>.

*Критерии оценки:*

Испытание завершилось успешно, если в результате выполнения программы не зафиксировано сообщений об ошибках.

d. Генератор случайных чисел (исправность и качество)

*Последовательность действий при проверке:*

- включить ЭВМ и осуществить вход Администратором;
- в утилите управления комплексом перейти на вкладку «Регламенты», напротив поля «Проверка ФГСЧ» нажать кнопку <Проверить>.

*Критерии оценки:*

Испытание завершилось успешно, если в результате выполнения программы не зафиксировано сообщений об ошибках.

3.3.2 При эксплуатации комплекса необходимо выполнить меры по обеспечению своевременной смены АИП.

### 3.3.3 Учетная запись пользователя может быть автоматически заблокирована:

- при превышении пользователем неудачных подряд попыток авторизации;
- при превышении общего количества всех попыток доступа пользователя;
- по окончании срока действия пароля.

Данные ограничения устанавливаются администратором комплекса при настройке учетной записи пользователя.

В случаях блокирования учетной записи пользователя необходимо провести исследование причин блокирования. В случае невозможности определения причин блокирования, а также в случае выявления факта попытки несанкционированного доступа к информации необходимо на всех контроллерах комплекса, где пользователь был зарегистрирован, провести смену его пароля, АИП на АНП, либо удалить его учетные записи (при необходимости может быть проведена его перерегистрация).

В случае блокировки учетной записи пользователя при попытке авторизации отображается сообщение о том, что учетная запись пользователя заблокирована и нужно обратиться к администратору.

В этом случае администратор комплекса в соответствии с внутренними регламентными документами может либо отредактировать АИП на АНП и позволить пользователю работать вновь, либо временно заблокировать его учетную запись, либо вообще удалить учетную запись пользователя.

### 3.3.4 При утере АНП или компрометации пароля администратор должен:

- заблокировать учетную запись пользователя. При этом все параметры пользователя, входящего в группу «Администраторы», сохраняются в базе данных, но вход в систему и работа данного пользователя будут запрещены;
- в соответствии с внутренними регламентными документами организации заказчика произвести внутреннее расследование данного инцидента и при решении восстановить учетную запись пользователя:
  - если был утерян АНП, зарегистрировать за пользователем новый АНП;
  - если был скомпрометирован пароль, установить новый пароль;

|              |                |              |              |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |      |
|--------------|----------------|--------------|--------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата | Данные ограничиваются устанавливаются администратором комплекса при настройке учетной записи пользователя.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |      |
|              |                |              |              |                | <p>В случаях блокирования учетной записи пользователя необходимо провести исследование причин блокирования. В случае невозможности определения причин блокирования, а также в случае выявления факта попытки несанкционированного доступа к информации необходимо на всех контроллерах комплекса, где пользователь был зарегистрирован, провести смену его пароля, АИП на АНП, либо удалить его учетные записи (при необходимости может быть проведена его перерегистрация).</p> <p>В случае блокировки учетной записи пользователя при попытке авторизации отображается сообщение о том, что учетная запись пользователя заблокирована и нужно обратиться к администратору.</p> <p>В этом случае администратор комплекса в соответствии с внутренними регламентными документами может либо отредактировать АИП на АНП и позволить пользователю работать вновь, либо временно заблокировать его учетную запись, либо вообще удалить учетную запись пользователя.</p> <p>3.3.4 При утере АНП или компрометации пароля администратор должен:</p> <ul style="list-style-type: none"><li>– заблокировать учетную запись пользователя. При этом все параметры пользователя, входящего в группу «Администраторы», сохраняются в базе данных, но вход в систему и работа данного пользователя будут запрещены;</li><li>– в соответствии с внутренними регламентными документами организации заказчика произвести внутреннее расследование данного инцидента и при решении восстановить учетную запись пользователя:<ul style="list-style-type: none"><li>– если был утерян АНП, зарегистрировать за пользователем новый АНП;</li><li>– если был скомпрометирован пароль, установить новый пароль;</li></ul></li></ul> |      |
| Изм          | Лист           | № документа  | Подпись      | Дата           | 11443195.4012.054 ПП                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Лист |
|              |                |              |              |                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 12   |

- разблокировать учетную запись пользователя.

3.3.5 Доступ к журналу регистрации событий имеет только администратор комплекса. Периодичность его просмотра и/или резервного копирования определяется внутренними руководящими документами организации заказчика, исходя из условий эксплуатации. При этом необходимо исключить возможность бесконтрольной перезаписи информации, вызванной переполнением журнала. Необходимо обеспечить защиту от несанкционированного доступа к копиям системного журнала.

3.3.6 На каждом РМ с установленным комплексом рекомендуется создавать одну резервную копию учетной записи администратора безопасности.

3.3.7 При выводе комплекса из эксплуатации администратору комплекса необходимо:

- произвести резервное копирование журнала регистрации событий;
- произвести форматирование комплекса, при котором очищаются база пользователей, списки контролируемых объектов, журнал регистрации событий и все установки сбрасываются в значение «по умолчанию».
- извлечь аппаратный контроллер АПМДЗ из СВТ и поместить его в упаковку производителя;
- сделать в формуляре запись о выводе комплекса из эксплуатации;
- сдать аппаратный контроллер АПМДЗ и формуляр на ответственное хранение.

3.3.8 Никаких ограничений по вторичному использованию АНП комплексом не накладывается.

### 3.4 Вывод из эксплуатации

При выводе изделия из эксплуатации или при передаче изделия в ремонт администратору изделия необходимо:

- произвести резервное копирование журнала регистрации событий;
- сделать в формуляре запись о выводе изделия из эксплуатации;
- сдать АПМДЗ и формуляр на ответственное хранение.

Повторное использование АНП запрещается.

### 3.5 Действия при НСД и компрометации служебной информации

В случаях выявления следующих событий в организации, эксплуатирующих изделие, необходимо обратиться к сотруднику (администратору безопасности информации), на которого возложена обязанность за решение данных вопросов:

- блокирование рабочего места и/или учетных записей пользователей\администраторов;
- утеря аутентифицирующего носителя пользователя или компрометация аутентифицирующей информации пользователя\администратора.

|              |                |              |              |                |                      |  |  |  |  |      |
|--------------|----------------|--------------|--------------|----------------|----------------------|--|--|--|--|------|
| Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата |                      |  |  |  |  | Лист |
|              |                |              |              |                |                      |  |  |  |  |      |
|              |                |              |              |                |                      |  |  |  |  |      |
|              |                |              |              |                |                      |  |  |  |  |      |
|              |                |              |              |                |                      |  |  |  |  |      |
| Изм          | Лист           | № документа  | Подпись      | Дата           | 11443195.4012.054 ПП |  |  |  |  | 13   |

### 3.6 Обновление и модернизация

3.6.1 Обновление, модернизация аппаратных и/или программных компонентов изделия (в том числе, использование встроенных в изделие функций обновления) может осуществляться только по методике, согласованной с экспертной организацией, с обязательной регистрацией установленным порядком указанных действий в эксплуатационной документации.

3.6.2 Консультационная поддержка осуществляется с понедельника по пятницу с 10-00 до 18-00 (по московскому времени) по телефону: +7 (495) 994-49-96, +7 (495) 994-49-97, +7 (926) 762-17-72, или по электронной почте [help@okbsapr.ru](mailto:help@okbsapr.ru).

### 3.7 Специальные требования

3.7.1 «Аккорд-АМДЗ» не накладывает ограничений на ведение переговоров, содержащих сведения со степенью секретности не выше «совершенно секретно», в помещениях размещения.

3.7.2 При эксплуатации «Аккорд-АМДЗ» запрещается вносить изменения в его состав и конструкцию.

[illegible]

## 4 УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

|       |                                                    |
|-------|----------------------------------------------------|
| АИП   | - аутентифицирующая информация пользователя        |
| АПМДЗ | - аппаратно-программный модуль доверенной загрузки |
| АНП   | - аутентифицирующий носитель пользователя          |
| АС    | - автоматизированная система                       |
| ДСЧ   | - датчик случайных чисел                           |
| ЛВС   | - локальная вычислительная сеть                    |
| НСД   | - несанкционированный доступ                       |
| ОС    | - операционная система                             |
| ПЛИС  | - программируемая логическая интегральная схема    |
| ПСЗИ  | - программное средство защиты информации           |
| СВТ   | - персональная электронная вычислительная машина   |
| РМ    | - рабочее место                                    |
| СВТ   | - средство вычислительной техники                  |
| ТУ    | - технические условия                              |
| ФПО   | - функциональное программное обеспечение           |
| ЭВМ   | - электронно-вычислительная машина                 |

|              |                |              |              |                |                      |  |  |  |  |      |
|--------------|----------------|--------------|--------------|----------------|----------------------|--|--|--|--|------|
| Инв. № подл. | Подпись и дата | Взам. инв. № | Инв. № дубл. | Подпись и дата |                      |  |  |  |  |      |
|              |                |              |              |                |                      |  |  |  |  |      |
|              |                |              |              |                |                      |  |  |  |  |      |
|              |                |              |              |                |                      |  |  |  |  |      |
| Изм          | Лист           | № документа  | Подпись      | Дата           | 11443195.4012.054 ПП |  |  |  |  | Лист |
|              |                |              |              |                |                      |  |  |  |  | 15   |

5 ОТВЕТСТВЕННОСТЬ ЗА ВЫПОЛНЕНИЕ ПРАВИЛ ПРИМЕНЕНИЯ

Ответственность за выполнение подготовительных работ (разделы 3.1 и 3.2), предусмотренных условиями на этапах подготовки к эксплуатации изделия и ввода его в эксплуатацию, несет специализированная организация, проводящая тематические исследования автоматизированной системы (комплекса или отдельного рабочего места, в состав которых включается изделие), совместно с разработчиком данной системы (комплекса или отдельного рабочего места).

Ответственность за соблюдение правил (разделы 3.3, 3.4 и 3.5) на местах эксплуатации несет администратор или другой сотрудник эксплуатирующей организации, на которого установленным порядком возложена эта обязанность, если техническим заданием на создание автоматизированной системы (комплекса или отдельного рабочего места), договором или другим документом не установлено иное.

|              |                |             |         |      |                      |                |  |  |  |              |              |                |              |
|--------------|----------------|-------------|---------|------|----------------------|----------------|--|--|--|--------------|--------------|----------------|--------------|
| Инв. № подл. | Подпись и дата |             |         |      | Инв. № дубл.         | Подпись и дата |  |  |  | Взам. инв. № | Инв. № дубл. | Подпись и дата | Инв. № подл. |
|              |                |             |         |      |                      |                |  |  |  |              |              |                |              |
|              |                |             |         |      |                      |                |  |  |  |              |              |                |              |
|              |                |             |         |      |                      |                |  |  |  |              |              |                |              |
| Изм          | Лист           | № документа | Подпись | Дата | 11443195.4012.054 ПП |                |  |  |  |              |              |                | Лист         |
|              |                |             |         |      |                      |                |  |  |  |              |              |                | 16           |