УТВЕРЖДЕН
ЦРПА.2.00067.01.00 30-ЛУ

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ БИОИДЕНТИФИКАЦИИ «АССаД-ID»

Формуляр

ЦРПА.2.00067.01.00 30

Листов 25

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

2024

Изм. 9

Литера

СОДЕРЖАНИЕ

1 Общие указания 3
2 Общие сведения 4
3 Основные характеристики 5
4 Комплектность 11
5 Периодический контроль основных характеристик при эксплуатации и хранении 12
6 Свидетельство о приемке 13
7 Свидетельство об упаковке и маркировке 14
8 Гарантийные обязательства 15
9 Сведения о рекламациях 16
10 Сведения о хранении 17
11 Сведения о закреплении программного изделия при эксплуатации 18
12 Сведения об обновлении 20
13 Указания по эксплуатации 21
14 Особые отметки 24

1 ОБЩИЕ УКАЗАНИЯ

1.1 Перед эксплуатацией специального программного обеспечения автоматизированной системы биоидентификации «АССаД-ID» (СПО «АССаД-ID») необходимо внимательно ознакомиться с ЭД на СПО «АССаД-ID».

1.2 В случае обнаружения дефектов на дистрибутивных носителях следует обращаться к изготовителю программы.

1.3 Претензии к качеству изготовления программного изделия направляются в адрес изготовителя.

1.4 Формуляр должен находиться у должностного лица ответственного за эксплуатацию программного изделия.

1.5 Все записи в формуляре производят только несмывающимися чернилами, отчетливо и аккуратно. Разрешается использовать при записях шариковые ручки с черной или фиолетовой (синей) пастой.

1.6 Неправильная запись должна быть аккуратно зачеркнута и рядом записана новая, которую заверяет ответственное лицо.

1.7 После подписи проставляют фамилию и инициалы ответственного лица (вместо подписи допускается проставлять личный штамп исполнителя).

1.8 В настоящем документе приняты следующие сокращения:

АСФЗ — автоматизированная система физической защиты;
АРМ — автоматизированное рабочее место;
БД — база данных;
БДУ — база данных уязвимостей;
ИБП — источник бесперебойного питания;
НСД — несанкционированный доступ;
ОС — операционная система;
ПО — программное обеспечение;
ПЭВМ — персональная вычислительная машина;
СВТ — средства вычислительной техники;
СЗИ — средства защиты информации;
СКУД — система управления и контроля доступом;
СОЭН — система оптико-электронного наблюдения;
СПО — специальное программное обеспечение;
ССОИ — система сбора и обработки информации;
СКУД — система контроля и управления доступом;
ЭД — эксплуатационные документы;
ЭП — электронная подпись.

2 ОБЩИЕ СВЕДЕНИЯ

2.1 Наименование: Специальное программное обеспечение автоматизированной системы биоидентификации «АССаД-ID».

2.2 Сокращенное наименование: СПО «АССаД-ID».

2.3 Обозначение: ЦРПА.2.00067.01.00.

2.4 Изготовитель: АО «АЛГОНТ».

2.5 Адрес изготовителя: Россия, 248009, г. Калуга, Грабцевское шоссе, д. 43.

2.6 Официальный адрес изготовителя в сети Интернет: https://www.algont.ru/

2.7 Контакты технической поддержки изделия: https://www.algont.ru/support/

3 ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1 СПО «АССаД-ID» является программным средством со встроенными средствами защиты от несанкционированного доступа к информации, составляющей служебную тайну, иной информации с ограниченным доступом и/или составляющей государственную тайну со степенью секретности не выше «секретно».

3.2 СПО «АССаД-ID» соответствует требованиям руководящего документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020 г.) по 3 уровню доверия.

3.3 СПО «АССаД-ID» может использоваться в АСФЗ 1-го класса защищенности в соответствии с требованиями руководящего документа «Системы физической защиты ядерных объектов. Автоматизированные системы физической защиты. Защита информации от несанкционированного доступа. Требования безопасности информации» (Госкорпорация «Росатом», 2011 г.).

3.4 СПО «АССаД-ID» применяется в составе Автоматизированной системы биоидентификации «АССаД-ID» (далее — система «АССаД-ID»).

3.5 Система «АССаД-ID» входит в состав СКУД и предназначена для контроля входа в здание и в зоны ограниченного доступа и выхода из них путем определения идентичности личности по изображению лица методом верификации и идентификации.

3.6 СПО «АССаД-ID» выполняет следующие функции:

– занесение в базу данных новых абонентов и их биометрических шаблонов;
– получение изображений для создания шаблона из указанного источника (графический файл, консоль распознавания, кадр видео);
– хранение и просмотр журнала событий;
– отображение информации на АРМ в соответствии с правами оператора;
– получение запросов на верификацию от СКУД, ССОИ и консоли распознавания и возвращение результата верификации, основанного на результате сравнения одной или более попыток сравнения в соответствии с алгоритмом верификации;
– возвращение результата идентификации — претендента с наибольшей схожестью;
– анализ живучести для противодействия попыткам фальсификации биометрических характеристик (с помощью фотографии или видеоизображения с планшетного компьютера);
– настройку аппаратной и программной части системы «АССаД-ID».

3.7 Средства защиты от несанкционированного доступа к информации (СЗИ НСД) СПО «АССаД-ID» включают:

– средства аутентификации операторов в СПО «АССаД-ID»;
– средства управления доступом операторов к ресурсам «АССаД-ID», реализованные с помощью ролей;
– средства регистрации событий, произошедших при работе СПО «АССаД-ID»;
– средства обеспечения контроля целостности.

3.8 СПО «АССаД-ID» может быть включено в состав следующих систем и подсистем, входящих в АСФЗ:

– система управления и контроля доступом (СКУД);
– система оптико-электронного наблюдения (СОЭН);
– система сбора и обработки информации (ССОИ);

– интегрированная система физической защиты, включающая любую комбинацию перечисленных выше систем.

3.9 Требования к составу технических средств

3.9.1 В системе «АССаД-ID» можно выделить основные составные части:
– сервер «АССаД-ID»;
– станция распознавания;
– консоль распознавания;
– АРМ «АССаД-ID»;
– сетевой коммутатор.

3.9.2 Компьютеры серверов, станций распознавания, а также ИБП должны быть размещены в шкафу, оснащенном датчиком вскрытия, или в помещении, дверь в которое оснащена датчиком вскрытия. Датчик вскрытия должен быть подключен к ИБП сервера «АССаД-ID» и сетевому коммутатору.

3.9.3 Технические средства компьютеров серверов «АССаД-ID», станций распознавания и АРМ должны удовлетворять минимальным требованиям, необходимым для установки на них операционной системы специального назначения «Astra Linux Special Edition» (не ниже очередного обновления версии 1.7).

3.9.4 Сервер «АССаД-ID» выполняет следующие функции:
– ведение базы данных, в которой хранятся шаблоны абонентов и конфигурационная информация системы «АССаД-ID»;
– формирование графического интерфейса пользователя системы «АССаД-ID»;
– резервирование и репликацию БД системы «АССаД-ID».

3.9.5 В состав технических средств компьютера сервера «АССаД-ID» должны входить:
– процессор с архитектурой x86-64 с характеристиками не хуже Intel Core2Duo с тактовой частотой 2,6 ГГц (рекомендуется — Intel Quad-Core Xeon);
– ОЗУ — не менее 4 ГБ;
– сетевая карта — не менее 1 Гбит/с;
– объем свободного дискового пространства — не менее 1 ТБ (для установки СПО «АССаД-ID» и хранения событий системы в течение трех месяцев);
– источник бесперебойного питания — не менее 3000 В·А с платой сетевого управления стандарта SNMP, поддерживающей подключение внешних датчиков.

Режим эксплуатации круглосуточный.

Не требует монитора или клавиатуры. Рекомендуется подключение к KVM-переключателю.

Для повышения надёжности хранения данных и для повышения скорости чтения/записи информации компьютер рекомендуется оснащать массивом независимых дисков (RAID-массив).

Для выполнения резервного копирования базы данных на внешние носители и восстановления базы данных из копий может использоваться записывающее устройство DVD±RW.

Рекомендуемое количество резервных серверов — не менее одного.

3.9.6 Станция распознавания выполняет следующие функции:
– верификация, при которой происходит сравнение образа, полученного с консоли распознавания, с шаблоном абонента, зарегистрированным в БД сервера «АССаД-ID»;

– идентификация, при которой происходит сравнение образа, полученного с консоли распознавания, с шаблонами абонентов, зарегистрированными в БД сервера «АССаД-ID»;
– взаимодействие с консолью распознавания по результатам распознавания;
– обеспечивает возможность подключения до четырех консолей распознавания.

3.9.7 В состав технических средств компьютера станции распознавания должны входить:
– процессор с архитектурой x86-64 с характеристиками не хуже Intel Core2Duo с тактовой частотой 2,6 ГГц (рекомендуется — Intel Quad-Core Xeon);
– ОЗУ — не менее 4 ГБ;
– сетевой интерфейс — не менее 1 Гбит/с;
– объем свободного дискового пространства — не менее 1 ГБ (для установки СПО «АССаД-ID»);
– источник бесперебойного питания — не менее 3000 В·А (допускается использование ИБП сервера «АССаД-ID»).

Режим эксплуатации круглосуточный.

Не требует монитора или клавиатуры. Рекомендуется подключение к KVM-переключателю.

Количество станций распознавания определяется количеством консолей распознавания.

Рекомендуемое количество резервных станций распознавания — не менее одной.

3.9.8 В состав технических средств компьютера АРМ должны входить:
– монитор — SVGA, не менее 15″;
– клавиатура и манипулятор типа «мышь»;
– ОЗУ — не менее 1 ГБ;
– сетевой интерфейс — не менее 1 Гбит/с;
– источник бесперебойного питания — не менее 700 В·А.

В качестве компьютера АРМ может быть использована бездисковая терминальная станция («тонкий клиент»). Образ ОС для удаленной загрузки при этом должен быть расположен на сервере «АССаД-ID» или станции распознавания.

3.9.9 Консоль распознавания обеспечивает выполнение следующих функций:
– получение изображения лица абонента через встроенную видеокамеру;
– взаимодействие со станцией распознавания;
– отображение процесса и результата верификации или идентификации на мониторе;
– возможность набора PIN-кода;
– взаимодействие с техническими средства СКУД по интерфейсу RS-485.

СПО «АССаД-ID» поддерживает работу только с консолями распознавания производства АО «АЛГОНТ», замены или аналоги не допустимы.

В зависимости от исполнения консоль также может обеспечивать защиту от фальсификации путем контроля живучести изображения, измерения роста абонента, анализом глубины изображения и т. п.

Каждая станция распознавания может обслуживать не более четырех консолей распознавания одновременно.

3.9.10 Сетевой коммутатор необходим для объединения составных частей в единую ЛВС. Порты сетевого коммутатора должны поддерживать обмен со скоростью не менее

1 Гбит/с. Количество портов сетевого коммутатора определяется количеством серверов, станций распознавания, АРМ и ИБП с платами сетевого управления.

3.10 Требования к составу программных средств

3.10.1 СПО «АССаД-ID» функционирует под управлением операционной системы специального назначения «Astra Linux Special Edition» (не ниже очередного обновления версии 1.7). ОС Astra Linux имеет сертификат соответствия ФСТЭК России № 2557 от 27 января 2012 года. СПО «АССаД-ID» использует защищенную СУБД PostgreSQL (версия 11.10) из состава ОС «Astra Linux Special Edition» (не ниже очередного обновления версии 1.7), защищенный браузер Firefox, виртуальную машину Java и графический киоск Fly из состава ОС Astra Linux Special Edition (не ниже очередного обновления версии 1.7).

3.10.2 При работе СПО «АССаД-ID» используется программное обеспечение (библиотека) 3DiVi Face SDK (версия 3.7.0), программное обеспечение (библиотека) VisionLabs LUNA SDK (версия 5.16.0), не входящие в состав СПО «АССаД-ID». Библиотеки выполняют математические операции: выделение лица, создание биометрических шаблонов, сравнение биометрических шаблонов между собой.

Программное обеспечение (библиотека) 3DiVi Face SDK и программное обеспечение (библиотека) VisionLabs LUNA SDK (версия 5.16.0) не содержат средств защиты информации, не влияют на СЗИ СПО «АССаД-ID», не используются для реализации мер защиты информации, функционируют в среде сертифицированной «Операционной системы специального назначения «Astra Linux Special Edition»).

3.10.3 СПО сервера устанавливается на компьютер сервера «АССаД-ID» под управлением ОС «Astra Linux Special Edition» (не ниже очередного обновления версии 1.7).

3.10.4 СПО станции распознавания устанавливается на компьютер станции распознавания под управлением ОС «Astra Linux Special Edition» (не ниже очередного обновления версии 1.7).

3.10.5 При необходимости СПО сервера «АССаД-ID» и СПО станции распознавания могут быть установлены на один компьютер.

3.10.6 Доступ к интерфейсу пользователя СПО «АССаД-ID» предоставляется через браузер Firefox с компьютера АРМ под управлением ОС «Astra Linux Special Edition» (не ниже очередного обновления версии 1.7) в режиме графического киоска Fly.

3.10.7 На объектах вычислительной техники с установленным СПО «АССаД-ID» запрещается выполнять установку любых программных средств, не предусмотренных политикой безопасности предприятия, а также любых средств разработки и отладки программного обеспечения.

3.10.8 Контроль целостности изделия осуществляется в процессе сверки контрольных сумм поставочного диска.

Проверку контрольной суммы поставочного диска СПО «АССаД-ID» с помощью программы «ФИКС» выполнить следующим образом:

1 Войти в ОС на ПЭВМ, где установлена программа «ФИКС».
2 Установить CD-диск, подлежащий проверке, в устройство чтения дисков.
3 Запустить программу «ФИКС».
4 На вкладке «Задание» выбрать следующие значения параметров:

– «Алгоритм КС» — «Уровень 3»;
– «Код» — «Const 1»;
– «Контролируемые файлы» — путь к CD-диску;

5 Запустить расчет контрольной суммы кнопкой «Пуск».

6 На вкладке «Гл.Отчет» убедиться, что расчет был выполнен с помощью алгоритма «Уровень 3, программно», а в строке «ВСЕГО» в столбце «КС» получено значение «6d369f24».

Проверку контрольной суммы поставочного диска СПО «АССаД-ID» с помощью программы gostsum из состава ОС «Astra Linux Special Edition» выполнить следующим образом:

1 Войти в ОС «Astra Linux Special Edition» под учетной записью суперпользователя root.
2 Установить CD-диск, подлежащий проверке, в устройство чтения дисков.
3 Запустить эмулятор терминала из состава ОС (например, fly-term).
4 Набрать в командной строке «gostsum –d /dev/cdrom».
5 Ожидать завершения процесса подсчета контрольной суммы.
6 Убедиться, что получено значение:
«3d7bc612c32c66c46a83f91e5d262fe666952950f3e7ca1bc9969065bdb3348b»

Контрольные суммы диска рассчитаны с помощью программы фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.2) 643.53132931.501254-04 (лицензия на право использования «ФИКС 2.0.2»: регистрационный № ЦС 50-8797Л815538, № знака соответствия Л8155, сертификат соответствия №1548, выдан ФСТЭК России выдан 15 января 2008 года), алгоритм «Уровень 3, программно» и с помощью программы gostsum из состава операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (заводской № 150556, № знака соответствия Д972043, сертификат соответствия № 2557, выдан ФСТЭК России 27 января 2012 года).

3.10.9 Подлинность и неизменность программного обеспечения и эксплуатационной документации, распространяемых по сетям связи, подтверждаются путём проверки усиленной электронной подписи изготовителя.

3.10.10 Подлинность и неизменность файлов СЗИ подтверждаются средствами контроля целостности путём вычисления и сравнения контрольных сумм файлов СЗИ, хранящимися в файле gostsumsIST.txt, размещённом на установочном диске (см. раздел 4) и обновлениях изделия (см. п. 3.10.13), в соответствии с описанием, приведённом в документе ЦРПА.2.00067.01.00 92 Специальное программное обеспечение автоматизированной системы биоидентификации «АССаД-ID». Руководство администратора безопасности. Контрольные суммы файлов СЗИ, приведенные в файле gostsumsIST.txt, рассчитаны в соответствии с алгоритмом ГОСТ Р 34.11-2012 256 бит с помощью программы gostsum из состава операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (заводской № 150556, № знака соответствия Д972043, сертификат соответствия № 2557, выдан ФСТЭК России 27 января 2012 года).

3.10.11 Подлинность и неизменность изделия подтверждаются с помощью программы gostsum из состава операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 путём вычисления и сравнения контрольных сумм неизменяемых файлов с эталонными значениями, хранящимися в файле gostsums.txt, размещённом на установочном диске (см. раздел 4) и обновлениях изделия (см. п. 3.10.13). Контрольные суммы неизменяемых файлов, приведенные в файле gostsums.txt, рассчитаны в соответствии с алгоритмом ГОСТ Р 34.11-2012 256 бит с помощью программы gostsum из состава операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (заводской № 150556, № знака соответствия Д972043, сертификат соответствия № 2557, выдан ФСТЭК России 27 января 2012 года).

3.10.12 Исходные тексты изделия и контрольные суммы файлов исходных текстов представлены на диске ЦРПА.2.00067.01.00 12.

3.10.13 В целях обеспечения соответствия изделия требованиям безопасности информации определён порядок устранения недостатков и уязвимостей, и доведения обновлений изделия и входящих в его состав компонентов до потребителей. Сведения о порядке выпуска и доведения обновлений изделия приведены в документе ЦРПА.2.00067.01.00 92 Специальное программное обеспечение автоматизированной системы биоидентификации «АССаД-ID». Руководство администратора безопасности.

4 КОМПЛЕКТНОСТЬ

4.1 Специальное программное обеспечение автоматизированной системы биоидентификации «АССаД-ID» поставляется на диске ЦРПА.467371.025.

4.2 Комплектность поставки должна соответствовать таблице 1.

Таблица 1 — Комплектность поставки программы

Обозначение	Наименование	Количество	Примечание
ЦРПА.2.00067.01.00	Специальное программное обеспечение автоматизированной системы биоидентификации «АССаД-ID»	1	*
ЦРПА.2.00067.01.00 30	Формуляр	1	**
ЦРПА.2.00067.01.00 31	Описание применения	1	**
ЦРПА.2.00067.01.00 32	Руководство системного программиста	1	**
ЦРПА.2.00067.01.00 34	Руководство оператора	1	**
ЦРПА.2.00067.01.00 92	Руководство администратора безопасности	1	**
	Сертификат соответствия ФСТЭК России (копия)	1	***
Примечания * - на диске CD-R ЦРПА.467371.025; ** - бумажная копия; *** - бумажная копия, заверенная держателем подлинника сертификата.			

5 ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ

5.1 Контроль программного изделия проводится при первичном закреплении за ответственным лицом и в дальнейшем — не реже одного раза в год в процессе проведения регламентных работ.

5.2 Контроль состоит из визуального выявления механических повреждений диска, проверки температуры, влажности, давления в помещении хранения и контрольной суммы.

5.3 Проверка сохранности информации осуществляется путем подсчета контрольных сумм диска и сравнения их с указанными в п.3.10.8 значениями. Если фактические и указанные значения не совпадают, необходимо обратиться к предприятию-изготовителю.

5.4 Результаты контроля фиксируются в таблице 2.

Таблица 2 — Периодический контроль основных характеристик

Проверяемая характеристика		Дата проведения проверки					
		20___г.		20___г.		20___г.	
Наименование измерения	Величина	Фактическая величина	Замерил (должность, подпись)	Фактическая величина	Замерил (должность, подпись)	Фактическая величина	Замерил (должность, подпись)
Температура	от 278 до 313 К (от плюс 5 ºС до плюс 40 ºС)						
Влажность	не более 65 %						
Давление	от 84 до 106,7 кПа (от 630 до 800 мм рт. ст.)						
Контрольная сумма	Соответствует указанной в п. 3.10.8						

6 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Специальное программное обеспечение автоматизированной системы биоидентификации «АССаД-ID» ЦРПА.2.00067.01.00 соответствует техническим условиям ЦРПА.2.00067.01.00 98 и признано годным для эксплуатации.

Дата изготовления _____
год, месяц, число

_____
должность

М.П. _____ _____
личная подпись инициалы, фамилия

_____
должность

М.П. _____ _____
личная подпись инициалы, фамилия

7 СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

Специальное программное обеспечение автоматизированной системы биоидентификации «АССаД-ID» ЦРПА.2.00067.01.00 упаковано АО «АЛГОНТ» согласно требованиям, предусмотренным техническими условиями ЦРПА.2.00067.01.00 98.

Маркировано согласно сертификату соответствия системы сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00):_____

Заводской номер _____

Идентификатор соответствия требованиям Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00: _____

Дата упаковки _____
год, месяц, число

Упаковку произвел:

_____
должность

_____ _____
личная подпись инициалы, фамилия

Изделие после упаковки принял:

_____
должность

_____ _____
личная подпись инициалы, фамилия

8 ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

8.1 Изготовитель СПО «АССаД-ID» гарантирует соответствие качества записи, изготовления ЭД и работоспособности программы требованиям технических условий ЦРПА.2.00067.01.00 98 при соблюдении потребителем требований при вводе в эксплуатацию, эксплуатации и хранении.

8.2 Гарантийный срок эксплуатации СПО «АССаД-ID» — 1 год с момента приемки заказчиком.

8.3 Действие гарантийных обязательств прекращается, если потребителем внесены изменения в СПО «АССаД-ID» без согласия изготовителя или оно передано другому предприятию (потребителю).

8.4 Гарантийные обязательства изготовителя НЕ РАСПРОСТРАНЯЮТСЯ на копии СПО «АССаД-ID», изготовленные по инициативе потребителя.

9 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

9.1 Рекламации предъявляются изготовителю в письменном виде с указанием даты обнаружения неисправности, содержания и условий возникновения неисправности.

9.2 Рекламации подписываются руководителем подразделения, принимающего и (или) эксплуатирующего программное изделие.

9.3 Сведения о предъявленных рекламациях регистрируются в таблице 3.

Таблица 3 — Учет предъявленных рекламаций

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

10 СВЕДЕНИЯ О ХРАНЕНИИ

10.1 Диск с записью программных средств хранится на предназначенном для этих целей стеллаже в упаковке, поставленной изготовителем, при температуре окружающего воздуха от 278 до 313 К (от плюс 5 ºС до плюс 40 ºС) и среднемесячной относительной влажности воздуха не более 65 % при 298 К (25 ºС).

10.2 В помещении для хранения диска с записью программных средств не должно быть агрессивных примесей (паров кислот, щелочей).

10.3 При хранении не допускаются резкие изменения температуры окружающего воздуха более 293 К (20 ºС) в час.

10.4 Сроки хранения и условия хранения диска указываются в таблице 4.
Примечание — Срок хранения диска при условии соблюдения правил хранения не ограничен.

Таблица 4 — Сведения о хранении диска

Дата		Условия хранения	Должность, фамилия и подпись лица, ответственного за хранение
установки на хранение	снятие с хранения		

11 СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ПРОГРАММНОГО ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ

11.1 Сведения о закреплении программного изделия

Сведения о закреплении заносятся в таблицу 5. При первичном закреплении необходимо провести контроль СПО «АССаД-ID» согласно разделу 5.

Таблица 5 — Сведения о закреплении программного изделия

Должность ответственного лица	Фамилия ответственного лица	Номер и дата приказа		Подпись ответственного лица
		о назначении	об освобождении	

11.2 Сведения о закреплении эксплуатационной документации

Сведения о закреплении ЭД СПО «АССаД-ID» заносятся в таблицу 6.

Таблица 6 — Сведения о закреплении эксплуатационной документации

Фамилия и должность ответственного лица	Номер и дата приказа		Подпись ответственного лица
	о назначении	об освобождении	

12 СВЕДЕНИЯ ОБ ОБНОВЛЕНИИ

12.1 Сведения об обновлении СПО «АССаД-ID» заносятся в таблицу 7.

Таблица 7 — Сведения об обновлении программного изделия

Дата	Идентификатор обновления	Краткое содержание работ	Должность и фамилия ответственного лица	Подпись ответственного лица

13 УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

13.1 При размещении компьютеров с установленным СПО «АССаД-ID»:

– должна осуществляться физическая защита СВТ АСФЗ (оборудования и носителей информации), предусматривающая охрану территорий и зданий, где размещается оборудование АСФЗ, с помощью персонала физической защиты и технических средств физической защиты, пропускной и внутриобъектовый режим, специальное оборудование помещений (пунктов управления, серверных, коммутационных шкафов, хранилищ и т. д.);

– должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены компьютеры с установленным СПО «АССаД-ID», посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях;

– внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию;

– используемые в АСФЗ линии связи, проходящие по контролируемой территории, должны быть защищены организационно-техническими мерами, исключающими несанкционированное физическое к ним подключение. Линии связи, проходящие по неконтролируемой (неохраняемой) территории, должны быть защищены специальными (криптографическими или другими) средствами. При этом такие средства защиты должны быть сертифицированы по требованиям безопасности информации;

– должен проводиться контроль (автоматизированный) физического доступа к оборудованию или в шкафы и/или помещения, где установлено оборудование.

13.2 При установке и обновлении СПО «АССаД-ID» следует руководствоваться следующими правилами:

– к установке общесистемного и специального программного обеспечения, включая СПО «АССаД-ID», допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО;

– для ОС среды функционирования СПО «АССаД-ID» должны быть установлены все актуальные обновления программного обеспечения, выпущенные разработчиками данных ОС;

– установка СПО «АССаД-ID» должна производиться только с поставочного диска. Перед установкой администратор безопасности должен выполнить проверку контрольных сумм диска согласно п. 3.10.8;

– по мере модернизации СПО «АССаД-ID» либо исправления ошибок в нём изготовитель выпускает обновления;

– информирование о появлении обновлений СПО «АССаД-ID» производится путем размещения информации на официальном сайте изготовителя или по электронной почте на адрес потребителя, указанный в лицензионном договоре;

– изготовитель размещает обновление СПО «АССаД-ID» на своём официальном сайте в разделе «Обновление ПО». Доступ к разделу предоставляется по логину и паролю. Для выдачи логина и пароля потребителям необходимо обратиться в техническую поддержку изготовителя любым из способов, указанных в разделе сайта «Поддержка»;

– для поддержания СПО «АССаД-ID» в сертифицированном статусе администратор безопасности должен устанавливать обновления, предоставляемые изготовителем;

– установка обновления СПО «АССаД-ID» должна производиться только администратором безопасности;

– перед установкой обновления СПО «АССаД-ID» администратор безопасности должен выполнить проверку контрольных сумм файлов обновления на соответствие значениям, указанным в информации об обновлении;

– после установки обновления СПО «АССаД-ID» администратор безопасности должен проверить корректность установки обновления путём проверки соответствия номера

версии, указанного в информации об обновлении, и номера версии, указанного в разделе «О программе» СПО «АССаД-ID».

13.3 При эксплуатации СПО «АССаД-ID» следует руководствоваться следующими правилами:

– на объектах вычислительной техники с установленным СПО «АССаД-ID» запрещается выполнять установку любых программных средств, не предусмотренных политикой безопасности предприятия, а также любых средств разработки и отладки программного обеспечения;

– на АРМ должна быть произведена настройка среды функционирования согласно руководству администратора безопасности ЦРПА.2.00067.01.00 92;

– при эксплуатации СПО «АССаД-ID» вход в ОС на АРМ должен выполняться с помощью учетной записи, созданной согласно руководству администратора безопасности ЦРПА.2.00067.01.00 92. Учетную запись root может использовать только администратор безопасности для выполнения перезагрузки компьютеров, переустановки или обновления СПО «АССаД-ID», запуска скриптов архивации и восстановления БД;

– установленные администратором безопасности роли персонала должны соответствовать их функциональным обязанностям и не включать излишние для них права и полномочия;

– подключение системы «АССаД-ID» к внешним информационным системам должно выполняться в соответствии с Требованиями по технической защите информации, содержащей сведения, составляющие государственную тайну, введёнными в действие приказом ФСТЭК России от 20 октября 2016 г. №25;

– должен проводиться ежемесячный поиск актуальных уязвимостей и сведений об уязвимостях изделия и среды функционирования, анализ идентифицированных уязвимостей на предмет возможности их использования для нарушения безопасности. В случае обнаружения уязвимостей, должно производиться их устранение в соответствии с методами и процедурами, приведенными в документе ЦРПА.2.00067.01.00 92 Специальное программное обеспечение автоматизированной системы биоидентификации «АССаД-ID». Руководство администратора безопасности;

– к эксплуатации СПО «АССаД-ID» допускается персонал, обладающий знаниями и навыками работы с компьютерами, графическим пользовательским интерфейсом, техническими средствами вычислительных сетей и изучившими ЭД на СПО «АССаД-ID»;

– аутентификация персонала АСФЗ в СПО «АССаД-ID» производится по логину и паролю, заданным в СПО «АССаД-ID». При использовании в АСФЗ 1-го класса защищенности должен быть установлен срок действия пароля не более 1-го месяца, в АСФЗ 2-го класса защищенности — не более 3-х месяцев;

– должен быть установлен порядок формирования и смены паролей персонала АСФЗ, а также порядок ознакомления с ними персонала АСФЗ, обеспечивающие конфиденциальность паролей;

– должны быть установлены процедуры передачи системы между сменами, обеспечивающие её подлинность и целостность;

– в составе персонала АСФЗ должен быть назначен администратор безопасности, ответственный за контроль безопасности АСФЗ и ведение СЗИ НСД. Администратор безопасности должен выполнять анализ отчетов по событиям безопасности и устанавливать имена пользователей, пароли и роли для новых операторов и системных администраторов, проводить периодический контроль СЗИ;

– после установки СПО «АССаД-ID» из конфигурации АРМ должны быть исключены все съемные накопители информации, за исключением специально выделенных АРМ. Для этого следует в BIOS компьютеров АРМ отключить такие устройства, запретить загрузку системы с таких устройств и защитить BIOS паролем;

– операторы не должны иметь доступа к режиму настройки BIOS или системному загрузчику;

– в процессе эксплуатации СПО «АССаД-ID» во время приёма-сдачи смены операторами не должна осуществляться перезагрузка ОС на АРМ. Перезагрузка ОС на АРМ выполняется операторами только при аварийной ситуации или сбое в работе компьютера;

– работа со съёмными носителями информации в АСФЗ должна проводиться только на специально выделенном компьютере (компьютерах) под контролем администратора безопасности;

– должен проводиться учёт всех носителей информации АСФЗ с помощью их защищённой маркировки, учёт носителей должен проводиться в журнале с регистрацией их выдачи/приёма. Учёт, обращение, хранение и уничтожение секретных носителей информации АСФЗ должен осуществляться в соответствии с требованиями секретного делопроизводства. Все накопители и носители информации АСФЗ должны учитываться по максимальному грифу секретности (уровню конфиденциальности) обрабатываемой в АСФЗ информации;

– регистрация и учёт выходных печатных (графических) документов должны проводиться в соответствии с требованиями делопроизводства соответствующего уровня конфиденциальности (степени секретности). Выдача печатных (графических) документов должна осуществляться только в соответствии с установленным перечнем выходных документов с указанием их уровня конфиденциальности (степени секретности) и, при необходимости, на предварительно учтённые в режимно-секретном подразделении листы бумаги;

– перед вводом любых данных в АСФЗ со съёмного носителя информации, последний должен пройти проверку на отсутствие вредоносных программ («вирусов», «червей», «троянов» и т. д.) и, при необходимости, соответствующую очистку от вредоносных кодов с помощью антивирусных средств;

– должно резервироваться (дублироваться) критичное оборудование, отказ которого может привести к отказу всей АСФЗ (серверы, станции распознавания, коммуникационное оборудование, линии связи и т. д.), для станций распознавания должна быть создана группа резервирования;

– в случае необходимости резервирования на серверах должна быть настроена репликация баз данных и ha-кластер;

– в качестве библиотеки распознавания на всех станциях распознавания должна быть выбрана библиотека 3DiVi или VisionLabs.

14 ОСОБЫЕ ОТМЕТКИ

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докумен-та	Входящий № сопровод-ительного документа и дата	Подп.	Дата
	изменных	заменных	новых	аннулированных					
9	-	все	-	-	25	ЦРПА.0255-24			