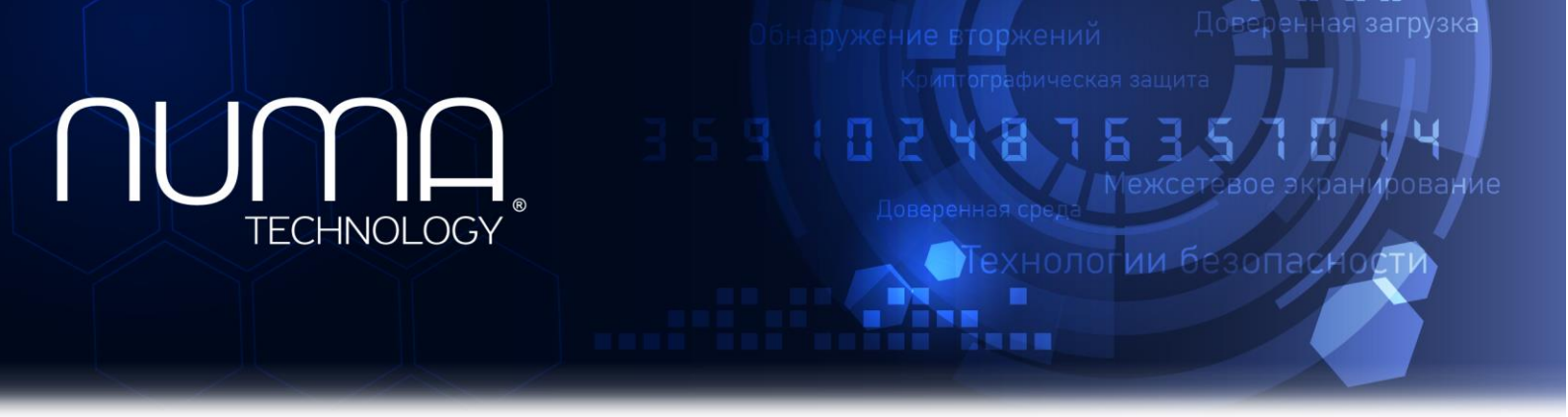

Средство доверенной загрузки уровня базовой системы ввода-вывода
модуль доверенной загрузки Numa Arce
Правила применения
643.АМБН.00032-01 ПП
Листов 14

2022

Литера

ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Название документа	Правила применения
Обозначение документа	643.АМБН.00032-01 ПП
Утвержден	643.АМБН.00032-01 ПП–ЛУ
Тип Изделия	Средство доверенной загрузки уровня базовой системы ввода-вывода
Идентификация Изделия	Модуль доверенной загрузки Numa Arce
Децимальный номер Изделия	643.АМБН.00032-01
Идентификация разработчика	ООО «НумаТех»
Ключевые слова	СДЗ, средство доверенной загрузки уровня базовой системы ввода-вывода

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

Настоящие правила применения (далее - Правила) распространяются на средство доверенной загрузки уровня базовой системы ввода-вывода «Модуль доверенной загрузки Numa Arce» 643.АМБН.00032-01 (далее - МДЗ или изделие).

Правила определяют порядок ввода в эксплуатацию, эксплуатации и вывода из эксплуатации изделия, а также действия при компрометации АИП.

Правила предназначены для следующих специалистов и организаций:

– заказчиков проектируемых автоматизированных систем (комплексов или отдельных АРМ), в составе которых предполагается применение МДЗ;

– разработчиков, проектирующих средства и системы защиты информации с применением МДЗ;

– специализированных организаций, проводящих исследования автоматизированных систем (комплексов или отдельных АРМ), спроектированных с применением МДЗ;

– экспертных подразделений, осуществляющих научно-техническое сопровождение (экспертизу) автоматизированных систем (комплексов или отдельных АРМ), спроектированных с применением МДЗ;

– администраторов, обеспечивающих эксплуатацию МДЗ на объектах заказчика.

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

Ответственность за соблюдение Правил (разделы 3.3, 3.4, 3.5, 3.6) 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 АРМ), договором или другим документом не установлено иное.

Возможные несоответствия эксплуатационной или другой сопроводительной документации на изделие настоящим Правилам трактуются в пользу Правил.

Наименование изделия – Модуль доверенной загрузки Numa Arce.

Децимальный номер изделия – 643.АМБН.00032-01.

Точный состав комплекта поставляемого изделия определяется при заключении каждого договора поставки. Перечень составных частей (документации), доступных для заказа, указан в разделе 4 «Комплектность» формуляра 643.АМБН.00032-01 30 01.

В состав МДЗ в обязательном порядке должны быть включены следующие компоненты:

1) необходимое количество (не менее 1) аутентифицирующих носителей пользователей (АНП) «ESMART Token ГОСТ» в исполнении 3.

2) эксплуатационная документация (на оптическом диске), в том числе настоящие Правила и правила пользования на СКЗИ «ESMART Token ГОСТ» исполнение 3.

3) формуляр 643.АМБН.00032-01 30 01.

Для администрирования АНП необходима ЭВМ, соответствующая требованиям правил пользования СКЗИ «ESMART Token ГОСТ» исполнение 7, не входящая в состав изделия.

Изделие может применяться на территории Российской Федерации в качестве средства защиты от несанкционированного доступа к техническим, программным и информационным ресурсам АРМ, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну (конфиденциальную информацию с уровнем защиты до КС3 включительно) и реализует следующие целевые функции по доверенной загрузке ОС:

– защита от загрузки нештатной ОС;

– защита от обхода изделия;

– идентификация и криптографическая аутентификация пользователей АРМ;
– проверка целостности программной среды АРМ
– регистрация событий, имеющих отношение к безопасности защищаемой информации;
– настройка и тестирование изделия.

Соответствие перечисленных функций требованиям ФСБ России, предъявляемыми к механизмам доверенной загрузки, обеспечивается при выполнении перечисленных ниже требований:

– встраивание МДЗ в автоматизированные системы (комплексы или отдельные АРМ, в состав которых включается изделие) должно выполняться по методике экспертной организации;

– должно быть обеспечено соблюдение условий и выполнение необходимых работ, перечисленных в разделах 2 «Условия применения изделия» и 3 «Условия обеспечения безопасности информации и соответствия предъявляемым требованиям» Правил;

– должна сохраняться в тайне АИП администраторов и пользователей (в том числе в ходе ремонта, регламентных и пр. работ);

– СКЗИ ESMART Token ГОСТ в Исполнении 3 должно иметь действующий сертификат соответствия ФСБ России;

– должно быть обеспечено соблюдение прочих условий эксплуатации, установленных в эксплуатационной документации на изделие и не противоречащих настоящим Правилам.

Регистрационные номера приобретенных или полученных при передаче от одной организации к другой, а также утилизированных (уничтоженных) установленным порядком АНП (СКЗИ «ESMART Token ГОСТ) в исполнении 3) должны сообщаться в войсковую часть 43753-С.

2. УСЛОВИЯ ПРИМЕНЕНИЯ ИЗДЕЛИЯ

2.1. Требования к аппаратным ресурсам ЭВМ

1) МДЗ предназначен для установки в x86/64 совместимые ЭВМ перечисленные в таблице (Таблица 1) и эксплуатации в условиях, предусмотренных для аппаратуры группы 1.1 по ГОСТ РВ 20.39.304-98.

2) ЭВМ должна иметь хотя бы один свободный USB-разъем для подключения аутентифицирующих носителей и/или считывателей смарт-карт или свободный разъем на материнской плате для подключения встраиваемого считывателя смарт-карт.

3) Для администрирования АНП необходима ЭВМ соответствующая требованиям правил пользования СКЗИ «ESMART Token ГОСТ» исполнение 7.

Таблица 1 – Перечень поддерживаемых платформ

Исполнение Изделия	Характеристика ЭВМ
1	Сетевая платформа Lanner NCA-1010
	Сетевая платформа Lanner FW-7573
2	Сетевая платформа Lanner NCA-4210
3	Сетевая платформа Lanner NCA-5520
4	Платформа Aquarius на базе материнской платы AQC300DC
	СВТ Aquarius Cmp NS585
5	СВТ Aquarius Cmp NS685U
	Платформа Aquarius на базе материнской платы AQH310CM
	СВТ Aquarius Cmp NS483
	СВТ Aquarius Cmp NS483R
6	Платформа Aquarius на базе материнской платы AQC246DF
7	Платформа Aquarius на базе материнской платы AQC612BJ
8	СВТ Aquarius Cmp NS685 исполнение 2
	СВТ Aquarius Cmp NS685 исполнение 3
	Платформа Aquarius на базе материнской платы AQ H410T
	СВТ Aquarius Cmp NS585 исполнение 2
9	Платформа Aquarius на базе материнской платы AQB560M
10	Платформа Aquarius на базе материнской платы AQC624CF

2.2. Требования к программным ресурсам ЭВМ

МДЗ предназначен для функционирования в среде UEFI/BIOS ЭВМ Numa BIOS 643.АМБН.00001-01, разработанной ООО «НумаТех» в соответствии со спецификацией UEFI 2.4.

2.3. Организационно-технические требования к ЭВМ

1) Аппаратная платформа ЭВМ, должна обеспечивать реализацию мер, предотвращающих перепрограммирование пользователями как BIOS системной платы, так и всех расширений BIOS, установленных в ЭВМ (например, перекусыванием контактов микросхем памяти, программированием защитных регистров микросхем памяти, применением ПСЗИ и т.д.).

2) Корпус ЭВМ должен обеспечивать (должны устанавливаться и закрываться крышки, монтироваться опечатывающие устройства, использоваться специальные наклейки и т.д.) невозможность несанкционированного доступа к техническим средствам ЭВМ, расположенным внутри корпуса ЭВМ.

3) Технические средства ЭВМ, в которую установлен МДЗ, не должны содержать аппаратно-программных механизмов, использование которых может привести к нарушению правильности его функционирования.

Для реализации перечисленных организационно-технических требований к ЭВМ, может потребоваться доработка технических средств ЭВМ.

2.4. Функциональные ограничения изделия

При встраивании изделия должны учитываться перечисленные ниже функциональные ограничения и технические характеристики.

1) Возможности механизма контроля целостности программной среды:

– изделие позволяет выполнять контроль целостности над содержимым разделов с файловыми системами FAT16, FAT32, NTFS, EXT2, EXT3, EXT4;

– поддерживаются таблицы разделов НЖМД формата GUID Partition Table (GPT);

– не поддерживается контроль целостности файлов, преобразованных криптографическими программами (BestCrypt или аналогичными), программами сжатия дисков (Drivespace и аналогичными) и т.п.;

– не поддерживается контроль целостности для логических дисков, являющихся наборами томов (например, LVM, StripeSet или Software RAID);

– не поддерживается контроль альтернативных потоков (streams) данных для директорий, расположенных на разделах (томах) с файловой системой NTFS (контролируются только альтернативные потоки данных для файлов);

– не поддерживается контроль альтернативных потоков данных (streams) для файлов, расположенных на разделах (томах) с файловой системой NTFS (контролируются только следующие потоки: DATA – «0x80»; FILE_NAME – «0x30»);

– не поддерживается контроль целостности объектов файловых систем, расположенных на динамических дисках.

– не допускается использование символических ссылок в файловой системе NTFS (NTFS Symbolic Link), точек соединения ОС Windows (Windows Junction Point) и жестких ссылок NTFS (NTFS Hardlink);

– максимальное количество контролируемых файлов — 3000;

– максимальное количество контролируемых записей реестра ОС Windows – 1024;

– максимальная длина полного имени (включая путь) любого контролируемого файла для файловых систем EXT2, EXT3, EXT4 – 249 символов;

– максимальная длина полного имени (включая путь) любого контролируемого файла для файловой системы FAT16, FAT32 – 249 символов;

– максимальная длина полного имени (включая путь) любого контролируемого файла для файловой системы NTFS – 249 символов.

2) Максимальное количество учетных записей пользователей (в том числе не менее 5 администраторов), зарегистрированных на одном АРМ - 20.

2.5. Проверка совместимости изделия с аппаратной платформой

Для принятия решения о возможности применения МДЗ в ЭВМ на базе аппаратных платформ (Таблица 1), при создании автоматизированных рабочих мест с использованием МДЗ необходимо проверить совместимость МДЗ и ЭВМ, в составе которых предполагается его использование. По результатам проведенных проверок принимается решение о необходимости доработки ЭВМ и возможности использования МДЗ для создания автоматизированных рабочих мест.

3. УСЛОВИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И СООТВЕТСТВИЯ ПРЕДЪЯВЛЯЕМЫМ ТРЕБОВАНИЯМ

В данном разделе сформулированы условия и ограничения по применению изделия, влияющие на обеспечение безопасности защищаемой с его помощью информации. Перечисленные ниже сведения должны использоваться при организации процесса эксплуатации изделия на местах в составе конкретного АРМ вычислительной системы. При этом должны учитываться степень конфиденциальности обрабатываемой информации и политика безопасности, действующая на объекте эксплуатации вычислительной системы (в эксплуатирующей организации), а также принятая модель нарушителя.

3.1. Подготовка к эксплуатации

До начала эксплуатации МДЗ должны быть выполнены следующие условия:

1) АРМ, в составе которого предполагается использование МДЗ, должно соответствовать условиям применения, перечисленным в разделе 2 Правил.

2) Для ЭВМ, должны быть проведены исследования технических средств ЭВМ (в том числе исследования системной программы BIOS) на предмет отсутствия в их реализации аппаратно-программных механизмов, которые могут привести к нарушению правильности функционирования ЭВМ и МДЗ или к утечке защищаемой информации (перечисление 3) раздела 2.3 Правил). Объем и глубина исследований технических средств определяются степенью конфиденциальности защищаемой информации и зависят от принятой модели нарушителя и актуальных угроз безопасности защищаемой при помощи МДЗ информации. По результатам проведенных исследований принимается решение о возможности использования МДЗ в ЭВМ конкретного типа (необходимости ее доработки), а также формируется перечень необходимых настроек BIOS.

3) Должен быть определен перечень объектов программной среды ЭВМ, целостность которых подлежит контролю средствами МДЗ. 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.

4) При определении указанного перечня должны учитываться возможности механизма контроля целостности программной среды, перечисленные в п. 1) раздела 2.4 Правил.

5) В качестве АНП в МДЗ может применяться только СКЗИ «ESMART Token ГОСТ» в исполнении 3. Необходимые работы по встраиванию данного исполнения СКЗИ проведены в рамках тематических исследований МДЗ и подтверждены экспертизой в установленном порядке. При необходимости использования СКЗИ «ESMART Token ГОСТ» для других целей, кроме применения в качестве АНП для аутентификации в МДЗ, должна быть дополнительно проведена оценка корректности встраивания СКЗИ в соответствии с правилами пользования на «ESMART Token ГОСТ» в исполнении 3.

6) На АРМ, в составе которого предполагается использование МДЗ, должна быть разрешена по требованиям информационной безопасности обработка несекретной информации (конфиденциального характера), согласно принятой в информационной системе модели угроз (нарушителя).

Обоснование выполнения перечисленных выше условий 1) - 6) раздела 3.1 Правил должно проводиться специализированной организацией с последующей экспертизой в установленном порядке.

7) Должны быть предусмотрены и приняты меры:

– обеспечивающие невозможность модификации (перепрограммирования) как системной программы BIOS, так и расширений BIOS в ЭВМ, с установленным МДЗ;

– по сохранению целостности корпуса ЭВМ, исключающие несанкционированный доступ к техническим средствам ЭВМ, расположенным внутри корпуса ЭВМ, после установки и настройки МДЗ;

– исключающие несанкционированный доступ к программным средствам МДЗ при его транспортировке (например, к месту эксплуатации, ремонта и т.д.) и хранении.

8) Должна быть обеспечена невозможность загрузки нештатной копии ОС после передачи управления от ПО МДЗ программе-загрузчику штатной ОС (например, путем установки на АРМ единственной ОС, сертифицированной ФСБ России или имеющей положительное заключение экспертизы, или путем настройки профиля загрузки в режиме загрузки ядра ОС (Linux-загрузка).

Проверка выполнения данных условий может проводиться в ходе исследований по пп. 1) или 2) раздела 3.1 Правил.

9) При использовании АНП должны выполняться режимные меры и запреты, установленные в пп. 2.4.1, 2.4.3, 2.4.6-2.4.8, 2.4.4, а также п. 2.7.1 (с 1 – 7 и с 10 - 13 дефисы) правил пользования на «ESMART Token ГОСТ» исполнение 3.

10) Для администрирования АНП необходима выделенная ЭВМ, в полном объеме удовлетворяющая требованиям правил пользования СКЗИ «ESMART Token ГОСТ» в исполнении 7, с установленным СКЗИ, а также доступ к сертифицированному ФСБ России удостоверяющему центру для выпуска сертификатов формата X.509.

3.2. Ввод в эксплуатацию

При вводе изделия в эксплуатацию должны выполняться следующие условия:

1) Параметры БСВВ должны быть установлены в соответствии со значениями, определенными в ходе исследований по условию 2) раздела 3.1 Правил.

2) Администратор должен установить перечисленные ниже значения параметров:

Загрузка ОС/Конфигуратор:

Необходимо создать профиль загрузки, указав в нем параметры загрузки штатной операционной системы (см. п. 4.4.2.1 Руководства администратора).

Параметры МДЗ:

– Пользователи:

При создании профиля пользователя необходимо установить следующие параметры:

  – «DIGEST» – значение «Вкл.»;
  – «Количество попыток входа» – «Вкл.»;

– Сертификаты:

Необходимо загрузить с АНП администратора или USB-накопителя корневой сертификат удостоверяющего центра, сертифицированного ФСБ России по классу защиты не ниже КС3.

– Политика паролей:
  – «Кол-во попыток входа» – любое доступное значение;
– Журнал аудита:
  – «Уровень журналирования» – значение не ниже «6 Системная информация»;
  – «Автоматическая перезапись» – значение «Выкл.»
– Параметры безопасности:
  – «Защита EFI-переменных» – значение «Вкл.»;
  – «Контроль транзакций Ext4» – значение «Вкл.»;
  – «Контроль транзакций NTFS» – значение «Блокировка».

Примечание. *Установка параметров «Контроль транзакций Ext4» и/или «Контроль транзакций NTFS» производится в случае использования данных файловых систем иначе устанавливаются значения «Выкл.» и/или «Отключено» соответственно.*

– PCIe: запуск OpRom.

Должен быть запрещен запуск устройств, а при необходимости, возможность запуска OpRom должна определяться в ходе работ по перечислению 2) п. 3.1 Правил.

3) После настройки параметров работы МДЗ должна быть произведена настройка механизма контроля целостности программной среды в соответствии с перечнем, полученным по результатам выполнения работ по условию 3) раздела 3.1 Правил, а также рассчитаны эталонные контрольные суммы.

4) Значения параметров МДЗ могут отличаться от перечисленных в условиях 1) – 3) раздела 3.2 Правил только при соответствующем обосновании специализированной организацией с последующей экспертизой в установленном порядке.

5) Значения параметров МДЗ, не перечисленных в пп. 1) - 3) раздела 3.2 Правил, определяются политикой безопасности, действующей на объектах эксплуатации.

6) При вводе в эксплуатацию АНП должны быть выполнены действия, в соответствии с п. 3.1 (перечисления 1, 2, 5, 6, 12-14) правил пользования на «ESMART Token ГОСТ» исполнение 3.

3.3. Эксплуатация

При эксплуатации изделия необходимо выполнять перечисленные ниже условия:

1) Один сеанс работы изделия, то есть время между включением (перезагрузкой) ЭВМ и началом загрузки ОС, не должен превышать 24 часов.

2) Администратор должен проводить своевременное обновление сертификатов исходя из срока их действия (3 месяца), одновременно необходимо производить смену ПИН-кода АНП, а также действия, предусмотренные в п. 4 правил пользования на «ESMART Token ГОСТ» исполнение 3.

3) После истечения срока действия сертификата пользователя, в случае невозможности его смены, учетная запись данного пользователя должна быть заблокирована или удалена на всех МДЗ, где он зарегистрирован.

4) Периодичность просмотра администратором системного журнала регистрации событий МДЗ должна быть определена из конкретных условий эксплуатации таким образом, чтобы исключить возможность бесконтрольной перезаписи информации, вызванной переполнением журнала. Необходимо также обеспечить защиту от несанкционированного доступа к копиям системного журнала.

5) Для просмотра и выгрузки на USB-носитель системного журнала администратор может зарегистрировать в МДЗ учетную запись с ролью аудитора. При этом аудитор должен быть назначен только из числа администраторов (квалифицированный и доверенный сотрудник эксплуатирующей организации).

6) Администратор должен осуществлять контроль уровня заряда батареи RTC, и проводить своевременную замену батареи с низким уровнем заряда (или неисправной) на новую.

7) АНП администратора/пользователя после их создания, являются материальными носителями, содержащими служебную информацию ограниченного распространения (ДСП). Указанные носители должны храниться таким образом, чтобы исключить возможность несанкционированного доступа к записанной в них информации.

8) При использовании АНП должны выполняться режимные меры и запреты, установленные в пп. 2.4.1, 2.4.3, 2.4.6-2.4.8, 2.4.4, а также п. 2.7.1 (с 1 – 7 и с 10 - 13 дефисы) и п. 9.3 правил пользования на «ESMART Token ГОСТ» исполнение 3.

9) При каждой загрузке сертификата в АНП на АРМ администратора с установленным СКЗИ «ESMART Token ГОСТ» в исполнении 7 должны выполняться мероприятия по контролю целостности для АНП, предусмотренные в п. 4 правил пользования на «ESMART Token ГОСТ» исполнение 3, при этом контроль целостности дистрибутивов не требуется, так как соответствующие дистрибутивы не устанавливаются.

10) При эксплуатации АНП должны выполняться организационно-технические и административные мероприятия, перечисленные в п. 6 правил пользования на «ESMART Token ГОСТ» исполнение 3.

11) При эксплуатации АНП необходимо руководствоваться требованиями п. 7 «Порядок управления ключами», с учетом перечисления 2) данного раздела, а также требованиями п. 8.2 «Аутентификация в СКЗИ» правил пользования на «ESMART Token ГОСТ» исполнение 3.

3.4. Вывод из эксплуатации

1) АНП, использовавшиеся для регистрации администратора или пользователей, после их инициализации с удалением всех объектов из памяти (стирания информации) согласно процедуре, описанной в правилах пользования на «ESMART Token ГОСТ» исполнение 3 (первый дефис п. 3.2) в дальнейшем могут быть использованы для регистрации других пользователей или администраторов, или выведены из эксплуатации.

2) При повторном использовании АНП (для регистрации других пользователей или администраторов) необходимо выполнить выгрузку системного журнала регистрации событий МДЗ на USB носитель с последующей очисткой журнала.

3) Для вывода из эксплуатации (или передачи в ремонт) МДЗ в составе ЭВМ должна быть очищена ее энергонезависимая память путем переинициализации, согласно руководству администратора 643.АМБН.00032-01 32 01 (п. 1.4.6).

4) При невозможности очистки ЭВМ с установленным МДЗ является материальным носителем, содержащим служебную информацию ограниченного распространения (ДСП) до перенинициализации всех МДЗ, обслуживаемых тем же администратором.

3.5. Действия при НСД и компрометации служебной информации

1) В случаях автоматического блокирования учетной записи пользователя средствами изделия 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 МДЗ, где пользователь был зарегистрирован, провести смену его АИП и ПИН-кода, либо удалить его учетные записи (при необходимости может быть проведена его перерегистрация с новой АИП).

2) При утере АНП пользователя учетные записи, соответствующие данному АНП, в кратчайшие сроки должны быть удалены на всех МДЗ, в которых он был зарегистрирован. После этого может быть выполнено создание и регистрация пользователя с новой АИП.

3) При компрометации содержимого АНП пользователя, в кратчайшие сроки необходимо провести смену АИП и ПИН-кода данного пользователя на всех МДЗ, где он был зарегистрирован.

4) При утере или компрометации содержимого основного или резервного АНП администратора должна быть проведена переинициализация всех МДЗ, обслуживаемых данным администратором. При компрометации содержимого также должна быть выполнена процедура стирания информации (согласно условию 1) раздела 3.4 Правил.

5) При использовании АНП необходимо также руководствоваться требованиями пп. 7.6, 7.7 правил пользования на «ESMART Token ГОСТ» исполнение 3.

3.6. Обновление и модернизация

Обновление 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 (Формуляр 643.АМБН.00032-01 30 01).

4. УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

АИП	аутентифицирующая информация пользователя/администратора (закрытый ключ ЭП и сертификат пользователя/администратора (открытый ключ)), используемая при его аутентификации и хранящаяся в защищенной памяти АНП
АНП	аутентифицирующий носитель пользователя/администратора
АРМ	автоматизированное рабочее место вычислительной системы (представляет собой ЭВМ или устройство на ее базе)
МДЗ	модуль доверенной загрузки
ДСП	ограничительная пометка для служебной информации ограниченного распространения (для служебного пользования).
НЖМД	накопитель на жестком магнитном диске
НСД	несанкционированный доступ
ОС	операционная система
ПСЗИ	программные средства защиты информации.
ЭВМ	электронно-вычислительная машина (персональная электронно-вычислительная машина или сервер)
BIOS	Basic Input Output System (базовая система ввода-вывода ЭВМ).
EXT	Extended File System (расширенная файловая система)
FAT	File Allocation Table (файловая система)
GPT	Guide Partition Table
LVM	Logical Volume Manager (менеджер логических томов)
MBR	Master Boot Record (главная загрузочная запись)
NTFS	New Technology File System (стандартная файловая система для семейства ОС Windows)
RAID	Redundant array of independent disks (избыточный массив независимых жестких дисков)
USB	Universal Serial Bus (универсальная последовательная шина)

5. ПРИЛОЖЕНИЕ

Таблица 2 – Перечень платформ, для которых проведены исследования ПО BIOS

№	Тип платформы	Сведения о заключении
1.	Сетевая платформа Lanner NCA-4210	149/3/4/4/32 от 18.04.2023
2.	Сетевая платформа Lanner NCA-5520	149/3/4/4/33 от 18.04.2023
3.	Платформа Aquarius на базе материнской платы AQC300DC	149/3/4/4/34 от 20.04.2023

**__Примечание.__ Комплектации и контрольные суммы образов ПО BIOS ЭВМ, перечисленных в данном перечне, должны соответствовать выпискам из заключений по результатам исследований ПО BIOS.*

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					