

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-06 98 01-ЛУ

**СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«ВАЛИДАТА CSP» ВЕРСИЯ 6**

Правила пользования

ВАМБ.00060-06 98 01

2020

Аннотация

Настоящий документ содержит описание порядка использования программного комплекса ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP»).

Документ содержит описание состава и основных функций СКЗИ «Валидата CSP», описание ключевой системы, а также общие требования к обеспечению безопасности на всех этапах использования СКЗИ «Валидата CSP».

Документ предназначен для пользователей, применяющих СКЗИ «Валидата CSP».

Настоящий документ составлен в соответствии с технической спецификацией «Информационная технология. Криптографическая защита информации. Состав и содержание правил пользования средств криптографической защиты информации» (ТС 26.2.001-2020) технического комитета по стандартизации «Криптографическая защита информации» (ТК 26).

Содержание

1 НАЗНАЧЕНИЕ СКЗИ «ВАЛИДАТА CSP» И ЕГО ОСНОВНЫЕ ХАРАКТЕРИСТИКИ	5
1.1 Общие сведения	5
1.2 Состав, реализуемые криптографические преобразования и основные функции СКЗИ «Валидата CSP»	5
1.2.1 Состав СКЗИ «Валидата CSP»	5
1.2.2 Используемые криптографические преобразования в СКЗИ «Валидата CSP»	5
1.2.3 Основные функции СКЗИ «Валидата CSP»	7
1.3 Классы защиты СКЗИ «Валидата CSP»	9
1.3.1 Варианты исполнения СКЗИ «Валидата CSP» и выполняемые нормативные требования	9
1.3.2 Используемые средства создания замкнутой программной среды	10
1.3.3 Используемые СЗИ от НСД	10
1.4 Графические интерфейсы СКЗИ «Валидата CSP»	11
1.5 Среда функционирования	12
1.5.1 Общие требования к среде функционирования	12
1.5.2 Использование ДСЧ	13
2 КЛЮЧЕВАЯ СИСТЕМА И КЛЮЧЕВЫЕ ДОКУМЕНТЫ	14
2.1 Тип используемой ключевой системы	14
2.2 Типы рабочих ключей	15
2.2.1 Одинарные ключи	15
2.2.2 Неодинарные ключи	16
2.2.3 Служебные ключи	17
2.2.4 Размеры ключей	17
2.3 Сроки действия ключей и сертификатов	17
2.4 Управление ключевой системой	19
3 ПОРЯДОК РАСПРОСТРАНЕНИЯ И УЧЁТА СКЗИ «ВАЛИДАТА CSP»	21
3.1 Способы передачи и хранения СКЗИ «Валидата CSP»	21
3.2 Поэкземплярный учёт СКЗИ «Валидата CSP»	21
4 ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ СКЗИ «ВАЛИДАТА CSP»	22
4.1 Требования по обеспечению безопасности при вводе СКЗИ «Валидата CSP» в эксплуатацию	22
4.1.1 Требования к встраиванию СКЗИ «Валидата CSP» в прикладные системы и к проведению исследований СКЗИ «Валидата CSP»	22
4.1.2 Требования по размещению	22
4.1.3 Требования к персоналу, обеспечивающему функционирование СКЗИ «Валидата CSP»	24
4.1.4 Инициализация и ввод СКЗИ «Валидата CSP» в эксплуатацию	25
4.1.5 Особенности работы с различными ключевыми носителями	25

4.2	Требования по обеспечению безопасности при эксплуатации СКЗИ «Валидата CSP»	27
4.2.1	Общие требования	27
4.2.2	Порядок обеспечения целостности СКЗИ «Валидата CSP» . . .	28
4.2.3	Порядок обеспечения работоспособности СКЗИ «Валидата CSP»	29
4.2.4	Контроль правильности работы ЭВМ	30
4.3	Требования по обеспечению безопасности при выводе СКЗИ «Валидата CSP» из эксплуатации и передаче в ремонт	30

5 СВЕДЕНИЯ О СОГЛАСОВАНИИ **32**

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ **33**

1 НАЗНАЧЕНИЕ СКЗИ «ВАЛИДАТА CSP» И ЕГО ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

1.1 Общие сведения

Программный комплекс (ПК) ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP») предназначен для:

- использования в качестве криптопровайдера в составе функционально законченных средств криптографической защиты информации (СКЗИ), имеющих сертификат соответствия ФСБ России;
- обращения к криптографическим функциям в соответствии со стандартными интерфейсами CSP (Cryptography Service Provider) и CNG (Cryptography API: Next Generation) Microsoft;
- поддержки протокола Transport Layer Security (TLS 1.2 в соответствии с RFC 5246, TLS 1.0 в соответствии с RFC 2246, расширенный мастер-секрет в соответствии с RFC 7627, а также безопасное переключенное в соответствии с RFC 5746) с использованием российских криптографических стандартов;
- обращения к функциям поддержки безопасности в соответствии со стандартным криптографическим интерфейсом Microsoft — Security Support Provider Interface (SSPI);
- встраивания в операционную систему (ОС) Microsoft Windows в качестве криптографического провайдера CSP Microsoft, работающего с защищенными приложениями Microsoft;
- встраивания в ОС Microsoft Windows в качестве криптографического провайдера CNG Microsoft, работающего с защищенными приложениями Microsoft;
- встраивания в ОС Microsoft Windows в качестве провайдера безопасности SSPI Microsoft, работающего с защищенными приложениями Microsoft.

1.2 Состав, реализуемые криптографические преобразования и основные функции СКЗИ «Валидата CSP»

1.2.1 Состав СКЗИ «Валидата CSP»

В состав СКЗИ «Валидата CSP» входят:

- криптографический провайдер (далее — криптопровайдер);
- программный модуль поддержки TLS;
- программный модуль «Графический Интерфейс Пользователя Сервисов» (далее — ПМ ГИПС);
- утилиту загрузки инициализационной последовательности датчика случайных чисел функционального ключевого носителя.

1.2.2 Используемые криптографические преобразования в СКЗИ «Валидата CSP»

СКЗИ «Валидата CSP» реализует следующие криптографические преобразо-

вания:

- шифрование данных, которое производится с целью скрыть содержание сообщения;
- имитозащита данных, обеспечивающая надежное установление фактов случайного или преднамеренного искажения информации в процессе её хранения или передачи по каналам связи;
- электронная подпись (ЭП), подтверждающая авторство и целостность электронных данных, а также обеспечивающая невозможность отказа от авторства.

СКЗИ «Валидата CSP» реализует криптографические алгоритмы согласно следующим стандартам:

- ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Информационная технология. Криптографическая защита информации. Блочные шифры» (блочные шифры «Магма» и «Кузнечик»);
- ГОСТ Р 34.13-2015 и ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» (блочные шифры «Магма» и «Кузнечик» в режимах простой замены, гаммирования и выработки имитовставки);
- ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018) «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
- ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018) «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

Примечания

1 Для проверки ЭП в СКЗИ «Валидата CSP» реализована поддержка ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».

2 Межгосударственные стандарты ГОСТ 34.10-2018, ГОСТ 34.11-2018 и ГОСТ 34.12-2018 определяют криптографические механизмы, совпадающие с криптографическими механизмами, определенными в национальных стандартах ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и ГОСТ Р 34.12-2015 соответственно.

3 Межгосударственный стандарт ГОСТ 34.13-2018 определяет криптографические механизмы, описанные в национальном стандарте ГОСТ Р 34.13-2015, и дополняет их криптографическими механизмами, описанными в Рекомендациях по стандартизации «Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования» (Р 1323565.1.017-2018) и «Режимы работы блочных шифров, реализующие аутентифицированное шифрование» (Р 1323565.1.026-2019).

4 Режим простой замены допускается использовать только для шифрования ключей.

СКЗИ «Валидата CSP» реализует криптографические преобразования в соответствии со следующими Рекомендациями по стандартизации:

- «Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования» (Р 50.1.113-2016);
- «Параметры эллиптических кривых для криптографических алгоритмов и протоколов» (Р 1323565.1.024-2019);
- «Форматы сообщений, защищенных криптографическими методами» (Р 1323565.1.025-2019);
- «Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)» (Р 1323565.1.020-2020);
- «Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS#10 инфраструктуры открытых ключей X.509» (Р 1323565.1.023-2022).

Защищаемая информация (текст, видеоизображение и т.д.) представляется в виде бинарной последовательности.

Подробная информация о защите данных с помощью криптографических преобразований в СКЗИ «Валидата CSP» приведена в документе ВАМБ.00060-06 31 01 «СКЗИ «Валидата CSP» версия 6. Описание применения».

1.2.3 Основные функции СКЗИ «Валидата CSP»

Криптопровайдер СКЗИ «Валидата CSP» обеспечивает выполнение следующих низкоуровневых криптографических функций, соответствующих интерфейсу Microsoft Windows CSP, в соответствии с государственными стандартами:

- создание ключей ЭП и вычисление ключей проверки ЭП (для ключей ЭП длиной 256 и 512 бит) в соответствии с ГОСТ Р 34.10-2012;
- создание и проверка ЭП в соответствии с ГОСТ Р 34.10-2012 для ключей ЭП длиной 256 и 512 бит. Создание и проверка ЭП CMS сообщений осуществляется в соответствии с Рекомендациями по стандартизации Р 1323565.1.025-2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами»;
- выполнение зашифрования и расшифрования данных в соответствии с ГОСТ 28147-89 в режимах гаммирования и гаммирования с обратной связью и ГОСТ Р 34.12-2015 (блочные шифры «Магма» и «Кузнечик») в режимах простой замены, гаммирования и выработки имитовставки согласно ГОСТ Р 34.13-2015. Зашифрование и расшифрование CMS сообщений осуществляются в соответствии с Рекомендациями по стандартизации Р 1323565.1.025-2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами»;
- выработка имитовставки данных в соответствии с ГОСТ 28147-89 и ГОСТ Р 34.12-2015 (блочные шифры «Магма» и «Кузнечик») согласно ГОСТ Р 34.13-2015;

- вычисление ключа парной связи Диффи-Хеллмана с использованием пар закрытых и открытых ключей по ГОСТ Р 34.10-2012 (для закрытых ключей шифрования длиной 256 и 512 бит) в соответствии с RFC 4357 и Рекомендациями по стандартизации Р 1323565.1.020-2018 «Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)»;
- вычисление хэш-функции данных (для хэш-значений длиной 256 и 512 бит) в соответствии с ГОСТ Р 34.11-2012;
- выработка случайного числа заданной длины.

Примечание — В случае когда в сертификате ключа проверки ЭП разрешено использование ключа ЭП для шифрования («Согласование ключей»), ключ ЭП является также закрытым ключом шифрования, а ключ проверки ЭП — открытым ключом шифрования.

Программный модуль поддержки TLS криптопровайдера СКЗИ «Валидата CSP» обеспечивает выполнение следующих функций поддержки протокола TLS:

- создание защищённого канала связи (с обеспечением контроля целостности передаваемой информации) между сервером и клиентом с использованием шифрования информации в соответствии с ГОСТ 28147-89 для протокола TLS 1.0;
- создание защищённого канала связи (с обеспечением контроля целостности передаваемой информации) между сервером и клиентом с использованием шифрования информации в соответствии с ГОСТ Р 34.12-2015 (блочный шифр «Кузнечик») и ГОСТ Р 34.13-2015 для протокола TLS 1.2;
- аутентификация сервера клиентом посредством вычисления ключа парной связи по способу Диффи-Хеллмана с использованием пар закрытых и открытых ключей;
- аутентификация клиента сервером посредством вычисления ЭП (на ключах ЭП и проверки ЭП клиента соответственно) согласно ГОСТ Р 34.10-2012;
- вычисление расширенного мастер-секрета для протокола TLS 1.2 в соответствии с RFC 7627;
- выполнение безопасного переподключения в соответствии с RFC 5246;
- обеспечения начальной аутентификации клиента в домене Microsoft Active Directory по протоколу Kerberos PKInit посредством вычисления ЭП и проверки ЭП (на ключах ЭП и проверки ЭП клиента соответственно) согласно ГОСТ Р 34.10-2012.

ПМ ГИПС предназначен для вывода на экран некоторых диалоговых окон СКЗИ «Валидата CSP» от процессов, запущенных как сервис (служба) с правами системной учётной записи. Необходимость использования ПМ ГИПС в СКЗИ «Валидата CSP» вызвана тем, что в ОС Windows 10 вывод диалоговых окон сервисов (служб) напрямую невозможен.

Настройка и использование ПМ ГИПС описаны в документе ВАНБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора».

Утилита загрузки инициализационной последовательности датчика случайных чисел (ДСЧ) функционального ключевого носителя (ФКН) предоставляет пользователю возможность инициализации программного ДСЧ ФКН «Валидата vdToken» и ФКН «Валидата vdToken» версия 2.0.

Подробнее работа с утилитой загрузки инициализационной последовательности ДСЧ ФКН описана в документе ВАМБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора».

1.3 Классы защиты СКЗИ «Валидата CSP»

1.3.1 Варианты исполнения СКЗИ «Валидата CSP» и выполняемые нормативные требования

СКЗИ «Валидата CSP» имеет три исполнения:

- исполнение 1, для которого использование средств защиты информации от несанкционированного доступа (СЗИ от НСД), сертифицированных ФСБ России, является рекомендательным;
- исполнение 2, для которого использование СЗИ от НСД, сертифицированных ФСБ России, является обязательным;
- исполнение 3, для которого использование СЗИ от НСД и средств создания замкнутой программной среды, сертифицированных ФСБ, является обязательным.

Используемые совместно с СКЗИ «Валидата CSP» СЗИ от НСД должны иметь действующие сертификаты и/или положительные заключения ФСБ России о соответствии одним из следующих требований:

- Требования ФСБ России к аппаратно-программным модулям доверенной загрузки ЭВМ класса не ниже ЗБ;
- Требования ФСБ России к механизмам доверенной загрузки ЭВМ (класс защиты не ниже 2, класс сервиса не ниже Б).

Примечания

1 Все исполнения имеют одну и ту же программную реализацию, не зависящую от применения совместно с СКЗИ «Валидата CSP» сертифицированных СЗИ от НСД и средств создания замкнутой программной среды.

2 В документации на СКЗИ «Валидата CSP» термин «Средство защиты от несанкционированного доступа» обозначает исключительно аппаратно-программные и программные модули доверенной загрузки (МДЗ), имеющие действующие сертификаты и/или положительные заключения ФСБ России.

СКЗИ «Валидата CSP» удовлетворяет «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» и «Требованиям к средствам электронной подписи», утверждённым приказом ФСБ России от 27.12.2011 № 796:

- для исполнения 1 — по классу КС1 при функционировании в физической и виртуальной среде;

– для исполнения 2 — по классу КС2 при функционировании в физической среде;

– для исполнения 3 — по классу КС3 при функционировании в физической среде,

а также «Специальным требованиям к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации» (СТ-Р) по уровню КС_Б.

1.3.2 Используемые средства создания замкнутой программной среды

Совместно с СКЗИ «Валидата CSP» (исполнение 3) допускается использовать средство защиты информации «Secret Net Studio» в качестве средства создания замкнутой программной среды при наличии у него действующего сертификата ФСБ России о соответствии требованиям к средствам защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, от несанкционированного доступа, класса АКЗ.

1.3.3 Используемые СЗИ от НСД

Допускается использование СКЗИ «Валидата CSP» совместно с СЗИ от НСД, перечисленными в таблице ниже (Таблица 1) только при наличии у них действующих сертификатов и/или положительных заключений ФСБ России о соответствии требованиям, указанным в п. 1.3.1 настоящего документа.

Таблица 1 – СЗИ от НСД, допустимые к использованию совместно с СКЗИ «Валидата CSP»

Наименование СЗИ от НСД	Поддержка аппаратного ДСЧ СЗИ от НСД
ПАК «Соболь» версия 3.0 (версии кода расширения BIOS 1.0.99, 1.0.180, 1.0.991, 1.0.280)	+
ПАК «Соболь» версия 3.1 (исполнения 1 и 2)	+
ПАК «Соболь» версия 3.2 (исполнения 1 и 2)	+
ПАК «Соболь» версия 4 (исполнения: PCIE K, MiniH-K, M2-K, PCIE-7K, M2-7K, версия расширения UEFI/BIOS – 4.3.363.0)	+
АПМДЗ «Криптон-замок/УМ2» («Аппаратно-программный модуль доверенной загрузки АПМДЗ-УМ2 исполнение 1», «Аппаратно-программный модуль доверенной загрузки АПМДЗ-УМ2 исполнение 2»)	–
АПМДЗ «Криптон-замок/Е» («Аппаратно-программный модуль доверенной загрузки с удаленным управлением для шины PCI Express M-526E», «Аппаратно-программный модуль доверенной загрузки с удаленным управлением для шины PCI Express M-526E исполнение 1»)	–
Средство доверенной загрузки уровня базовой системы ввода-вывода «Модуль доверенной загрузки Numa Arce 643.АМБН.00032-01» (исполнения: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10)	–
АПМДЗ ЭВМ «Аккорд-АМДЗ» (исполнения GXM2 v.P, GXM2 v.P (Вариант 2), GXM2 v.P (Вариант 3), GXM2 v.S (Вариант 1), GXM2 v.S (Вариант 2))	–
Программно-аппаратный комплекс (ПАК) «Аккорд-АМДЗ» (исполнения GX, GXM2, GXMH)	–
ПК «ViPNet SafeBoot 3» (исполнение 1)	–

1.4 Графические интерфейсы СКЗИ «Валидата CSP»

СКЗИ «Валидата CSP» предоставляет следующие графические интерфейсы для взаимодействия с пользователем:

- программа конфигурации СКЗИ «Валидата CSP»;
- монитор TLS.

Подробная информация о порядке работы с перечисленными выше интерфейсами приведена в документах ВАНБ.00060-06 31 01 «СКЗИ «Валидата CSP» версия 6. Описание применения» и ВАНБ.00060-06 95 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора».

1.5 Среда функционирования

1.5.1 Общие требования к среде функционирования

Минимальные требования к ЭВМ, на которых функционирует СКЗИ «Валидата CSP»:

- объем жесткого диска и оперативной памяти должен удовлетворять минимальным требованиям для установленной на данной ЭВМ версии ОС Microsoft Windows;
- следует использовать Intel-совместимый процессор с микроархитектурой Intel Core 2 или более новый, поддерживающий расширения инструкций SSE2, SSE3, SSSE3;
- для повышения производительности рекомендуется использовать процессор с поддержкой расширений инструкций SSE4.1, AVX.

СКЗИ «Валидата CSP» функционирует на ЭВМ с 32-битными (x86) и 64-битными (x64) архитектурами, а также на виртуальных машинах (только для исполнения 1), находящихся под управлением гипервизоров Microsoft Hyper-V и VMware ESXi версий 6.5/6.7/7.0 из состава VMware vSphere, в следующих ОС Microsoft Windows:

- Windows 10 (x86 и x64);
- Windows Server 2016 (x64);
- Windows Server 2019 (x64).

В указанных ОС должна быть установлена поддержка следующих русскоязычных кодировок:

- CP 866;
- CP 1251 (Windows-1251);
- UTF-16 Little Endian.

Для указанных ОС, а также для гипервизоров должно быть обеспечено получение обновлений безопасности.

В случае использования ОС, поддержка которых прекращена производителем, допускается подключение ЭВМ с установленными СКЗИ «Валидата CSP» и ПК, функционирующих совместно с СКЗИ «Валидата CSP», только к корпоративным сетям связи. При подключении ЭВМ к корпоративным сетям связи, выходящим за пределы контролируемой зоны, должны дополнительно выполняться требования к защите такого подключения, изложенные в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности». Иначе подключение ЭВМ с установленными СКЗИ «Валидата CSP» и ПК, функционирующих совместно с СКЗИ «Валидата CSP», должно выполняться только к корпоративным сетям связи, расположенным в пределах контролируемой зоны, в которой эксплуатируется СКЗИ «Валидата CSP».

При необходимости совместно с СКЗИ «Валидата CSP» могут использоваться

сетевой адаптер и устройство резервного копирования информации на отчуждаемый носитель (например, CD-RW).

1.5.2 Использование ДСЧ

В процессе функционирования СКЗИ «Валидата CSP» используется программный ДСЧ.

Программный ДСЧ используется в процессе генерации ключей ЭП, синхропосылок, случайных данных, необходимых для выполнения ЭП по ГОСТ Р 34.10-2012, а также других данных, которые могут передаваться по каналу в открытом виде.

Для инициализации программного ДСЧ используется физический ДСЧ.

В СКЗИ «Валидата CSP» реализована поддержка следующих типов физических ДСЧ:

- аппаратные ДСЧ, входящие в состав СЗИ от НСД, перечисленных в п. 1.3.3 настоящего документа;
- «биологический» ДСЧ;
- ДСЧ ФКН «Валидата vdToken» версия 2.0.

Примечание — Для всех типов ДСЧ, кроме «биологического» ДСЧ, требуется установка на компьютере специального аппаратного и программного обеспечения.

2 КЛЮЧЕВАЯ СИСТЕМА И КЛЮЧЕВЫЕ ДОКУМЕНТЫ

2.1 Тип используемой ключевой системы

Ключевая система СКЗИ «Валидата CSP» является системой с открытым распределением ключей на основе асимметричной криптографии, в которой используется пара асимметричных ключей: открытый (ключ проверки ЭП, открытый ключ шифрования) и закрытый (ключ ЭП, закрытый ключ шифрования).

В СКЗИ «Валидата CSP» реализована ЭП на базе криптографических алгоритмов, соответствующих ГОСТ Р 34.10-2012.

Ключ ЭП используется для выработки ЭП и должен сохраняться пользователем в тайне.

Ключ проверки ЭП используется для проверки подлинности подписанного документа, а также для предупреждения мошенничества со стороны владельца ключа ЭП в виде его отказа от подписи документа. Ключ проверки ЭП может быть опубликован, так как он вычисляется как значение некоторой функции от ключа ЭП, но знание ключа проверки ЭП не даёт возможности определить ключ ЭП.

В СКЗИ «Валидата CSP» реализована поддержка следующих наборов параметров эллиптических кривых для ключей ЭП длиной 256 бит:

- набор параметров A (RFC 4357);
- набор параметров B (RFC 4357);
- набор параметров C (RFC 4357);
- набор параметров TK26_A_256 (Эдвардса);
- набор параметров TK26_B_256;
- набор параметров TK26_C_256;
- набор параметров TK26_D_256,

а также следующих наборов параметров эллиптических кривых для ключей ЭП длиной 512 бит:

- набор параметров TK26_A_512;
- набор параметров TK26_B_512;
- набор параметров TK26_C_512 (Эдвардса).

Объектные идентификаторы (ОИД) для приведенных выше наборов параметров описаны в Рекомендациях по стандартизации Р 1323565.1.023-2022 «Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509».

В СКЗИ «Валидата CSP» для шифрования/расшифрования данных используются симметричные алгоритмы криптографического преобразования данных,

определенные ГОСТ Р 34.12-2015 (зашифрование и расшифрование осуществляются с использованием одного и того же ключа).

В СКЗИ «Валидата CSP» для формирования симметричного ключа используется пара асимметричных ключей: открытый и закрытый ключи шифрования.

В качестве закрытого ключа шифрования в СКЗИ «Валидата CSP» используется ключ ЭП, а в качестве открытого ключа шифрования — ключ проверки ЭП. Для этого в сертификате ключа проверки ЭП должна быть установлена область использования ключа «Согласование ключей». Иначе выполнение шифрования/расшифрования данных с использованием данных ключей невозможно.

2.2 Типы рабочих ключей

Под «ключом» понимается вся ключевая информация, записываемая на ключевой носитель. Эта информация представляет собой некоторую структуру данных, содержащую как собственно ключи ЭП и/или шифрования (т.е. ключи в формате криптографических стандартов), так и сопутствующую им информацию, такую как идентификаторы алгоритмов, ключи защиты ключей, имитовставки, а также информацию, необходимую для идентификации и аутентификации пользователя — владельца ключевого носителя.

Далее ключи, понимаемые как вся совокупность ключевой информации, будем продолжать называть просто ключами. Собственно ключи ЭП и шифрования будем называть «криптографическими ключами».

СКЗИ «Валидата CSP» поддерживает два типа ключей: **одинарные** и **неодинарные**.

Одинарными ключами называются ключи, существующие в виде одного единственного компонента, хранящегося на одном ключевом носителе и содержащего всю информацию, необходимую для функционирования ключа.

Неодинарными ключами называются ключи, существующие в виде нескольких компонентов, каждый из которых хранится на отдельном ключевом носителе в извлекаемом виде.

2.2.1 Одинарные ключи

В СКЗИ «Валидата CSP» различают два вида одинарных ключей:

- одинарный ключ, содержащий только криптографический ключ ЭП в соответствии с ГОСТ Р 34.10-2012;

- одинарный ключ, содержащий криптографический ключ, одновременно являющийся криптографическим ключом ЭП в соответствии с ГОСТ Р 34.10-2012 и криптографическим ключом шифрования в соответствии с ГОСТ Р 34.10-2012 и криптографическим ключом шифрования в соответствии с ГОСТ Р 28147-89 или ГОСТ Р 34.12-2015 (блочные шифры «Магма» и «Кузнечик») совместно с ГОСТ Р 34.13-2015 (блочные шифры «Магма» и «Кузнечик» в режимах простой замены, гаммирования и выработки имитовставки). В этом случае в сертификате ключа проверки ЭП должна быть установлена область использования ключа «Согласование ключей».

2.2.1.1 Открытый и закрытый ключи шифрования

В связи с тем, что СКЗИ «Валидата CSP» предназначено для использования в системе с открытым распределением ключей, каждый пользователь формиру-

ет два ключа шифрования: закрытый и открытый (далее — ключи шифрования или долговременные ключи шифрования). Закрытый ключ шифрования должен храниться в тайне. Открытый ключ шифрования может быть опубликован для использования всеми пользователями системы, которые обмениваются зашифрованными сообщениями. Знание открытого ключа шифрования не даёт практической возможности определить закрытый ключ шифрования.

Примечание — В качестве закрытого ключа шифрования используется ключ ЭП, а в качестве открытого ключа шифрования — ключ проверки ЭП.

Пользователя, который зашифровывает сообщение, будем в дальнейшем называть отправителем; а пользователя, который расшифровывает сообщение — получателем.

Кроме долговременных ключей шифрования в процессе шифрования могут использоваться **эфемерные** ключи шифрования: **эфемерный закрытый ключ шифрования**, создаваемый отправителем сообщения с использованием генератора случайных чисел, и **эфемерный открытый ключ шифрования**, соответствующий эфемерному закрытому ключу шифрования.

Каждый эфемерный закрытый ключ шифрования используется только в одной операции шифрования. Эфемерный открытый ключ шифрования передается получателю вместе с сообщением.

Различают два вида шифрования: **неанонимное** и **анонимное**.

При **неанонимном** шифровании сообщения отправителем вычисляется общий ключ по алгоритму Диффи-Хеллмана на основе долговременного закрытого ключа шифрования отправителя и долговременного открытого ключа шифрования получателя. Для расшифрования этого сообщения получателем вычисляется тот же общий ключ на основе долговременного закрытого ключа шифрования получателя и долговременного открытого ключа шифрования отправителя.

При **анонимном** шифровании сообщения отправителем вычисляется общий ключ по алгоритму Диффи-Хеллмана на основе эфемерного закрытого ключа шифрования отправителя и долговременного открытого ключа шифрования получателя. Для расшифрования этого сообщения получателем вычисляется тот же общий ключ на основе долговременного закрытого ключа шифрования получателя и эфемерного открытого ключа шифрования отправителя.

Таким образом, для обеспечения связи с другими абонентами каждому пользователю необходимо иметь:

- собственный закрытый ключ шифрования;
- сертификаты открытых ключей шифрования пользователей сети конфиденциальной связи, изданные Центром сертификации.

Далее ключи шифрования упоминаться не будут, и возможность использования ключа ЭП для шифрования будет определяться разрешённой областью применения соответствующего сертификата ключа проверки ЭП.

2.2.2 Неодинарные ключи

СКЗИ «Валидата CSP» поддерживает два особых типа неодинарных ключей:

- ключ в формате «3 из 6», создаваемый и загружаемый по схеме разделения секрета «3 из 6»;
- ключ в формате «2 из 3», создаваемый и загружаемый по схеме разделения секрета «2 из 3».

Ключи, используемые по схемам разделения секрета, предназначены для использования в качестве дополнительной меры, обеспечивающей устойчивость ключевой системы к компрометациям.

Ключи форматов «3 из 6» и «2 из 3» могут использоваться только как краткосрочные ключи (ключи со сроком до 15-ти месяцев).

2.2.3 Служебные ключи

Служебными ключами называются ключи, обеспечивающие функционирование служб (подсистем) криптопровайдера.

2.2.3.1 Ключи защиты

Ключами защиты называются используемые в СКЗИ «Валидата CSP» симметричные ключи, предназначенные для защиты (посредством шифрования) других ключей (рабочих ключей и других ключей защиты).

2.2.3.2 Парольный ключ

Парольный ключ — симметричный ключ, на котором зашифровываются ключи защиты при хранении их на носителе. Данный ключ представляет собой хэш-значение пароля, защищающего доступ к носителю ключевой информации абонента. Парольный ключ не записывается на ключевой носитель. В памяти ЭВМ он существует только при выполнении процедуры загрузки ключей в течение времени, необходимого для расшифрования ключей защиты рабочих ключей. После выполнения своей функции парольный ключ затирается случайной последовательностью. Проверка пароля осуществляется с использованием специального контрольного значения, записываемого в ключевой контейнер и представляющего собой дважды прохэшированный пароль (хэш-значение от хэш-значения пароля). Парольная защита устанавливается или не устанавливается по выбору пользователя при генерации ключей. При наличии парольной защиты при вводе ключа запрашивается пароль.

2.2.4 Размеры ключей

Длина ключей ЭП, используемых в СКЗИ «Валидата CSP»:

- ключ ЭП — 256 бит или 512 бит;
- ключ проверки ЭП — 512 бит или 1024 бита, соответственно.

2.3 Сроки действия ключей и сертификатов

Сроки действия ключей и сертификатов устанавливаются в процессе выпуска сертификатов.

Максимальные сроки действия ключей и сертификатов, в зависимости от условий эксплуатации приведены ниже (Таблица 2 и Таблица 3).

Таблица 2 – Максимальные сроки действия ключей и сертификатов пользователей Центра сертификации

Ключ/сертификат	Срок действия	Условия применения
Ключ ЭП, находящийся в режиме неизвлекаемого ключа на функциональном ключевом носителе (ФКН) «Валидата vdToken» или «Валидата vdToken» версия 2.0	Не более 3 лет (36 месяцев)	Только при использовании СКЗИ «Валидата CSP» в варианте исполнения 1 или 2
Ключ ЭП, сформированный с помощью СКЗИ «Валидата CSP» в устройстве Hardware Security Module (HSM) в неизвлекаемом и неэкспортируемом виде	Не более 3 лет (36 месяцев)	Без ограничений
Ключ ЭП (для всех ключей ЭП, отличных от указанных выше в настоящей таблице, в том числе для ключей, записываемых на ФКН в режиме извлекаемого ключа)	Не более 15 месяцев	Без ограничений
Ключ проверки ЭП, сертификат ключа проверки ЭП	Не более 15 лет (180 месяцев) после окончания срока действия соответствующего ключа ЭП, максимальный срок действия — 18 лет (216 месяцев)	Без ограничений

Таблица 3 – Максимальные сроки действия ключей и сертификатов Администраторов Центра сертификации

Ключ/сертификат	Срок действия	Условия применения
Ключ ЭП, находящийся в режиме неизвлекаемого ключа на ФКН «Валидата vdToken», «Валидата vdToken» версия 2.0 или на устройстве HSM	Не более 5 лет (60 месяцев), из которых подписание сертификатов и списков аннулированных сертификатов возможно не более первых 3 лет (36 месяцев), далее — только подписание списков аннулированных сертификатов	Предназначены для использования только в Центрах сертификации удостоверяющих центров.
Ключ проверки ЭП, сертификат ключа проверки ЭП	Не более 15 лет (180 месяцев) после окончания срока, в который разрешено подписание сертификатов соответствующим ключом ЭП, максимальный срок действия — 18 лет (216 месяцев)	Без ограничений

2.4 Управление ключевой системой

Управление квалифицированными сертификатами ключей проверки ЭП при использовании СКЗИ «Валидата CSP» должно обеспечиваться с использованием средств удостоверяющего центра (УЦ), имеющих действующий сертификат соответствия ФСБ России, а также ключ проверки ЭП в формате, соответствующем рекомендациям по стандартизации Р 1323565.1.023-2022 (утверждены приказом Росстандарта от 09.03.2022 № 123-ст).

При работе с СКЗИ «Валидата CSP» каждый пользователь, обладающий правом подписи (или шифрования), самостоятельно формирует или получает в УЦ личные ключ ЭП (на отчуждаемом носителе) и ключ проверки ЭП (в составе сертификата ключа проверки ЭП, издаваемого УЦ).

В качестве носителей криптографических ключей должны использоваться носители, указанные в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

Владелец ключевой информации должен обеспечить ее сохранность, а также принимать все возможные меры для предотвращения ее потери, раскрытия, модифицирования или несанкционированного использования.

Ответственным за организацию работ по безопасному использованию СКЗИ «Валидата CSP», в том числе, ключевой информации, является администратор информационной безопасности.

Порядок обеспечения безопасности ключевой информации, в том числе:

- полномочия и обязанности администратора информационной безопасности;
- организационно-технические меры и средства, необходимые для обеспечения безопасности ключевой информации;
- порядок обращения с ключевыми носителями, включая правила хранения ключевых носителей;
- порядок резервирования ключевой информации;
- порядок действий при компрометации ключевой информации;
- порядок уничтожения ключей,

приведен в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

3 ПОРЯДОК РАСПРОСТРАНЕНИЯ И УЧЁТА СКЗИ «ВАЛИДАТА CSP»

3.1 Способы передачи и хранения СКЗИ «Валидата CSP»

Передача дистрибутива СКЗИ «Валидата CSP» в эксплуатирующую организацию осуществляется на оптическом носителе, не допускающем перезапись информации, или в электронном виде с обеспечением целостности дистрибутива посредством ЭП.

Дистрибутив сопровождается ведомостью машинного носителя записи (ВМНЗ), содержащей информацию о хэш-кодах архивов с программным обеспечением и документацией, вычисленных по алгоритму хэширования согласно ГОСТ Р 34.11-2012 (в формате протокола проверки, формируемого программой контроля целостности).

При получении дистрибутива эксплуатирующая организация осуществляет внешний контроль носителя (проверка маркировки), а также внутренний контроль (проверка комплектности и контроль целостности дистрибутива). Контроль целостности дистрибутива осуществляется в соответствии с документами ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности», ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности» и ВАМБ.00060-06 92 01 «СКЗИ «Валидата CSP» версия 6. Программа контроля целостности. Руководство пользователя».

Эталонные дистрибутивы с подтвержденной целостностью должны храниться в условиях, исключающих возможность подмены установочных файлов и файлов верификации.

3.2 Поэкземплярный учёт СКЗИ «Валидата CSP»

СКЗИ «Валидата CSP» подлежит поэкземплярному учёту с использованием индексов или условных наименований и регистрационных номеров, определяемых ФСБ России.

4 ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ СКЗИ «ВАЛИДАТА CSP»

4.1 Требования по обеспечению безопасности при вводе СКЗИ «Валидата CSP» в эксплуатацию

4.1.1 Требования к встраиванию СКЗИ «Валидата CSP» в прикладные системы и к проведению исследований СКЗИ «Валидата CSP»

При использовании в прикладном программном обеспечении (ПО) криптографических функций СКЗИ «Валидата CSP», описанных в документе ВАМБ.00060-06 33 01 «СКЗИ «Валидата CSP» версия 6. Руководство программиста», необходимо проведение тематических исследований (сертификации) полученной реализации прикладного ПО на соответствие нормативным требованиям ФСБ России. Указанные исследования должны проводиться по техническому заданию, согласованному с Центром защиты информации и специальной связи ФСБ России. Исследования должны производиться специализированными организациями, имеющими лицензию ФСБ России на указанный вид деятельности и соответствующую аккредитацию испытательной лаборатории.

При использовании СКЗИ «Валидата CSP» в качестве криптопровайдера в составе функционально законченных СКЗИ, имеющих сертификат соответствия ФСБ России, программный модуль поддержки TLS из состава СКЗИ «Валидата CSP» может использоваться без проведения работ по оценке влияния совместно со следующими компонентами ОС Windows и веб-браузерами:

- Microsoft Internet Explorer (IE) версии 11.0;
- Remote Desktop Client (RDC) версии 10.0;
- Internet Information Server (IIS) версии 10 (из состава Microsoft Windows Server 2016/2019);
- Terminal Services (TS) из состава ОС Microsoft Windows Server;
- Terminal Services Gateway (TS Gateway) из состава ОС Microsoft Windows Server;
- Chromium GOST версий 96 — 143.

4.1.2 Требования по размещению

При эксплуатации, размещении и хранении технических средств с установленным СКЗИ «Валидата CSP» пользователь должен обеспечить режим эксплуатации, размещения и хранения технических средств, исключающий несанкционированный доступ к этим техническим средствам.

При размещении стационарных ЭВМ с установленным СКЗИ «Валидата CSP»:

- должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства с установленным СКЗИ «Валидата CSP», лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях;

– в случае необходимости присутствия посторонних лиц в указанных помещениях должен быть обеспечен контроль за их действиями;

– внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать сохранность конфиденциальных документов и сведений, включая ключевую информацию, пользователей СКЗИ «Валидата CSP».

Размещение и эксплуатация СКЗИ «Валидата CSP» в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

Требования к информативности сигналов линейной передачи и сигналов ПЭМИН (Побочные электромагнитные излучения и наводки) не предъявляются.

Технические средства, на которых предполагается эксплуатация СКЗИ «Валидата CSP», должны быть допущены для обработки информации ограниченного доступа по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе по каналу связи (например, СТР-К) с учетом модели угроз, принятой в автоматизированных системах и ПК эксплуатирующей организации. Данное требование не предъявляется в случае эксплуатации СКЗИ «Валидата CSP» при обработке открытой информации, доступ к которой не ограничивается согласно законодательству Российской Федерации.

Если технические средства аттестованы на соответствие установленным требованиям по защите информации без учета оценки каналов связи, то при их подключении к проводным каналам связи, выходящим за пределы контролируемой территории, необходимо использовать любое из следующих средств:

- волоконно-оптические линии связи;
- оптические развязывающие устройства, устанавливаемые в тракт передачи информации для создания оптоволоконного фрагмента сети;
- сертифицированные средства криптографической защиты информации для передачи информации соответствующего уровня конфиденциальности.

Для технических средств, подключенных к беспроводным каналам связи, для обеспечения защиты информации по уровню КС от утечки по каналу линейной передачи достаточно, чтобы канал связи был реализован в виде радиоканала GSM, GPRS, 3G/4G, WiFi, а также других каналов мобильной или беспроводной связи, работающих в диапазоне частот несущей выше 800 МГц с цифровой модуляцией штатного информационного сигнала.

Требования по защите от НСД к СКЗИ «Валидата CSP» приведены в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

Перечень требований к хранению эталонного дистрибутива СКЗИ «Валидата CSP», содержащего, в том числе, эксплуатационную документацию, приведен в документе ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности».

4.1.3 Требования к персоналу, обеспечивающему функционирование СКЗИ «Валидата CSP»

К установке, эксплуатации и сопровождению СКЗИ «Валидата CSP» допускаются специалисты, изучившие соответствующие эксплуатационные документы.

Персонал должен знать и строго выполнять правила эксплуатации СКЗИ «Валидата CSP», изложенные в эксплуатационной документации, а также требования соответствующих руководящих, нормативных, методических и организационно-распорядительных документов.

Помимо пользователей СКЗИ «Валидата CSP» в обеспечении безопасного функционирования СКЗИ «Валидата CSP» участвуют администратор информационной безопасности и системный администратор.

Администратор информационной безопасности выполняет следующие функции:

- осуществляет создание инструкций, направленных на обеспечение безопасности функционирования СКЗИ «Валидата CSP», доведение данных инструкций до пользователей и контроль за их соблюдением;
- контроль соблюдения описанных в настоящем руководстве требований;
- осуществляет организацию контроля целостности СКЗИ «Валидата CSP»;
- осуществляет управление доступом пользователей к ПО и данным, включая установку и периодическую смену паролей;
- при централизованном хранении личных контейнеров с ключевыми носителями (опечатываемых личной печатью владельца ключей) обеспечивает это централизованное хранение;
- осуществляет определение конкретных настроек операционной системы и её конфигурирование в целях защиты СКЗИ «Валидата CSP» от НСД;
- производит настройку средств создания замкнутой программной среды;
- производит настройку аппаратно-программных или программных средств, обеспечивающих защиту от НСД к СКЗИ «Валидата CSP».

Примечание — Более подробно сведения о функциях, выполняемых администратором информационной безопасности, приведены в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

Системный администратор выполняет следующие функции:

- производит установку СКЗИ «Валидата CSP»;
- производит установку аппаратно-программных или программных средств, обеспечивающих защиту от НСД к СКЗИ «Валидата CSP»;
- производит установку средств создания замкнутой программной среды;
- производит администрирование ОС.

При выполнении своих обязанностей системному администратору необходимо руководствоваться требованиями, приведенными в документах ВАМБ.00060-06 91 01 «СКЗИ «Валидата CSP» версия 6. Руководство по уста-

новке и настройке» и ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

Примечание — Возможно совмещение ролей администратора информационной безопасности и системного администратора.

Процедура назначения и смены персонала всех ролей, а также процедура включения/исключения персонала из ролевой модели определяется эксплуатирующей организацией.

4.1.4 Инициализация и ввод СКЗИ «Валидата CSP» в эксплуатацию

Установка и первоначальная настройка СКЗИ «Валидата CSP» выполняются в соответствии с документом ВАМБ.00060-06 91 01 «СКЗИ «Валидата CSP» версия 6. Руководство по установке и настройке».

Требования по обеспечению безопасности при установке СКЗИ «Валидата CSP», а также при настройке и эксплуатации ЭВМ приведены в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

4.1.5 Особенности работы с различными ключевыми носителями

В качестве носителей криптографических ключей должны использоваться носители, указанные в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

При загрузке ключей с ключевого носителя TouchMemory DS1995, DS1996 необходимо использовать считыватель того же типа (Аккорд, Соболев, Dallas или Secret Net), который применялся при формировании (создании или копировании) используемого ключевого носителя.

Драйверы для работы с носителями ключевой информации в состав СКЗИ «Валидата CSP» не входят и приобретаются эксплуатирующей организацией самостоятельно. Для обеспечения правильного взаимодействия СКЗИ «Валидата CSP» с устройствами считывания ключевой информации необходимо произвести установку драйверов и другого необходимого ПО в соответствии с требованиями документации производителей до установки СКЗИ «Валидата CSP».

Для работы с ФКН «Валидата vdToken» и ФКН «Валидата vdToken» версия 2.0 не нужно устанавливать на ЭВМ никаких дополнительных программ, сервисов и драйверов, так как данные ключевые носители используют стандартные сервисы и драйверы, входящие в ОС Windows для поддержки «смарт-карт».

Использование ФКН «Валидата vdToken» приводит к ограничению в поддерживаемом функционале по сравнению с ФКН «Валидата vdToken» версия 2.0, а именно: шифрование осуществляется исключительно по ГОСТ 28147-89, не поддерживаются ключи ЭП длиной 512 бит, поддерживаются исключительно эллиптические кривые А, В, С из RFC 4357.

ФКН «Валидата vdToken» версия 2.0, реализованный на базе микроконтроллера МК20DX256 (на аппаратной базе ФКН «Валидата vdToken»), не поддерживает генерацию ключей ЭП длиной 512 бит с использованием эллип-

тической кривой С (Эдвардса).

В случае использования устройства HSM «Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0» (исполнение 1, комплектация 1) (далее — ПАКМ «КриптоПро HSM») необходимое для совместного функционирования с ним Средство криптографической защиты информации «КриптоПро CSP» следует устанавливать после установки СКЗИ «Валидата CSP». При этом СКЗИ «Валидата CSP» должен устанавливаться без программного модуля поддержки TLS.

Использование ПАКМ «КриптоПро HSM» приводит к ограничению в поддерживаемом функционале, а именно: не поддерживаются эллиптические кривые В, С, D (для ключей ЭП длиной 256 бит) из Рекомендаций по стандартизации Р 1323565.1.024-2019.

Поскольку доступ к ключам ЭП, хранящимся в устройстве ПАКМ «КриптоПро HSM», осуществляется через CSP с идентификаторами *Crypto-Pro GOST R 34.10-2012 Strong HSM Svc CSP* и *Crypto-Pro GOST R 34.10-2012 HSM Svc CSP*, необходимо в соответствии с эксплуатационной документацией на данное устройство HSM настроить и запустить сервис (службу ОС Windows) КриптоПро HSM, входящий в состав клиентского ПО устройства ПАКМ «КриптоПро HSM».

В клиентской библиотеке PKCS#11 устройства ПАК «ViPNet HSM» разработчиком реализовано ограничение, не позволяющее её использование одновременно более чем 10 процессами ОС. При достижении указанного предела функция *C_Initialize()* указанной библиотеки выдает ошибку *CKR_FUNCTION_FAILED*, что приводит к выдаче СКЗИ «Валидата CSP» сообщения об ошибке «Конфигурация INFOTECs HSM не найдена». При этом после завершения процесса ОС, осуществлявшего доступ к ПАК «ViPNet HSM», должно пройти не менее 30 секунд перед запуском следующего процесса, который будет осуществлять доступ к указанному HSM.

В случае возникновения ошибки 0xE0BE50DE «Ошибка ф-ии *RtlLoginToken*» при использовании считывателя РуТокен, необходимо отключить кэширование PIN-кодов на вкладке Настройки Панели управления РуТокен, запустив ее из Панели управления ОС Windows (Рисунок 1).

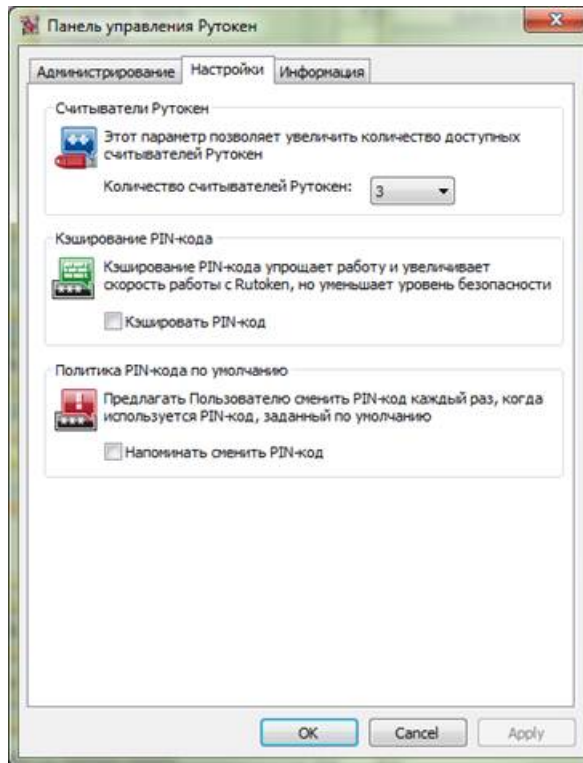


Рисунок 1 – Панель управления РуТокен

4.2 Требования по обеспечению безопасности при эксплуатации СКЗИ «Валидата CSP»

4.2.1 Общие требования

При эксплуатации СКЗИ «Валидата CSP» следует принять следующие общие организационные меры:

- право доступа к ЭВМ с установленным СКЗИ «Валидата CSP» предоставляется только лицам, изучившим соответствующие эксплуатационные документы СКЗИ «Валидата CSP», а также другие документы, созданные на их основе;
- запрещается использование СКЗИ «Валидата CSP» для защиты сведений, составляющих государственную тайну;
- должны быть выполнены требования, изложенные в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности», в том числе требования, определяющие:

- комплекс организационно-технических мероприятий по защите от НСД перед началом и во время работы СКЗИ «Валидата CSP»;
- перечень мер по обеспечению безопасности защищенной связи;
- порядок использования сторонних средств защиты от НСД;
- порядок контроля выполнения требований эксплуатационной документации СКЗИ «Валидата CSP»;
- требования к аутентификации пользователей, в том числе, с использованием парольных механизмов;

- порядок разграничения доступа;

– в случае функционирования СКЗИ «Валидата CSP» в виртуальной среде должны быть выполнены требования, изложенные в документе ВАМБ.00060-06 93 03 «СКЗИ «Валидата CSP» версия 6. Функционирование в виртуальной среде. Руководство администратора информационной безопасности»;

– на ЭВМ с установленным СКЗИ «Валидата CSP» должно использоваться только лицензионное ПО фирм-производителей;

– запрещается вносить какие-либо изменения в ПО СКЗИ «Валидата CSP».

4.2.2 Порядок обеспечения целостности СКЗИ «Валидата CSP»

При использовании СКЗИ «Валидата CSP» необходимо организовать контроль целостности СКЗИ «Валидата CSP», системного ПО и всех исполняемых файлов, функционирующих совместно с СКЗИ «Валидата CSP», в соответствии с требованиями документов ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности» и ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности».

Мероприятия по контролю целостности СКЗИ «Валидата CSP» должны включать в себя следующие виды работ:

– контроль целостности дистрибутивов;

– первичный контроль — контроль целостности, выполняемый при установке и обновлении ПО;

– текущий (ежедневный) контроль — контроль целостности, выполняемый в процессе работы с ПО (в начале работы, во время работы или по завершении работы) пользователем или уполномоченным контролирующим лицом;

– периодический (регламентный) контроль — контроль целостности, выполняемый администратором информационной безопасности в соответствии с принятым в эксплуатирующей организации регламентом.

В общем случае для контроля целостности допускается применять один из следующих подходов:

– в качестве основного средства контроля целостности используется программа hashfile.exe. Целостность программы hashfile.exe и эталона верификации при этом обеспечивается либо средствами СЗИ от НСД, либо организационно-техническими мерами, такими как финализированная запись этих объектов на отчуждаемый носитель (CD- или DVD-диск), правила обращения с которым соответствуют правилам обращения с ключевыми носителями;

– в качестве основного средства контроля целостности используется СЗИ от НСД, а программа hashfile.exe при необходимости используется в качестве дополнительного средства контроля. Целостность исполняемого файла программы hashfile.exe и эталона верификации при этом обеспечивается средствами СЗИ от НСД.

Примечание — Эталон верификации – один из следующих объектов:

– создаваемый программой **hashfile.exe** файл, содержащий список файлов, подлежащих контролю целостности, и значение хэш-функции для каждого файла из данного списка;

– ветка реестра ОС Windows, содержащая перечень файлов, подлежащих контролю целостности, и значения хэш-функции для каждого файла из данного перечня.

Подробная информация об организации контроля целостности для каждого из перечисленных выше подходов, видов контроля целостности и каждого исполнения СКЗИ «Валидата CSP», а также порядок действий в случае нарушения контроля целостности приведены в документе ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности».

Список объектов СКЗИ «Валидата CSP», системного ПО и ПО средств виртуализации, подлежащих контролю целостности, приведен в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

4.2.3 Порядок обеспечения работоспособности СКЗИ «Валидата CSP»

В СКЗИ «Валидата CSP» реализована процедура самотестирования криптографических алгоритмов. Она выполняется при запуске СКЗИ «Валидата CSP», а затем во время его работы при выполнении какой-либо криптографической операции в случае, если с момента запуска предыдущей процедуры самотестирования прошло 10 минут или более.

СКЗИ «Валидата CSP» поддерживает пять типов протоколируемых событий:

- критические ошибки;
- ошибки;
- предупреждения;
- информационные сообщения;
- отладочные сообщения.

Описание настройки уровня протоколирования выполняется в соответствии с документом ВАМБ.00060-06 91 01 «СКЗИ «Валидата CSP» версия 6. Руководство по установке и настройке».

Создание резервных копий СКЗИ «Валидата CSP» выполняется в соответствии с документом ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности».

Дополнительно должны быть созданы резервные копии следующих веток реестра ОС Windows, в которых хранятся настройки СКЗИ «Валидата CSP»:

- HKEY_LOCAL_MACHINE\SOFTWARE\Validata;
- HKEY_CURRENT_USER\SOFTWARE\Validata.

Порядок действий по восстановлению работоспособности СКЗИ «Валидата CSP» при сбоях и в случаях нештатных ситуаций приведен в документе

ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности». Порядок действий в случае нарушения контроля целостности приведен в документе ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности».

4.2.4 Контроль правильности работы ЭВМ

Для обеспечения контроля правильности работы ЭВМ с установленным СКЗИ «Валидата CSP» необходимо с периодом не более 168 часов (7 суток) производить перезагрузку работающей ЭВМ с установленным СКЗИ «Валидата CSP».

При этом перезагрузку работающей ЭВМ необходимо производить с отключением и последующим включением питания ЭВМ с целью выполнения встроенных в постоянное запоминающее устройство ЭВМ тестов проверки работоспособности аппаратных ресурсов. В случае когда после отключения питания ЭВМ дальнейшей работы с данной ЭВМ не требуется, производить перезагрузку не требуется.

В случае, когда условия эксплуатации СКЗИ «Валидата CSP» требуют непрерывной работы ЭВМ в течение длительного времени (более 7 суток), необходимо принять во внимание, что СКЗИ «Валидата CSP» может использоваться только в качестве криптопровайдера в составе сертифицированных функционально законченных СКЗИ (далее — ФЗ СКЗИ) с высокоуровневым криптографическим интерфейсом.

Правила пользования ФЗ СКЗИ, использующих СКЗИ «Валидата CSP», должны содержать требования, при выполнении которых допускается выполнять перезагрузку ЭВМ (с целью проверки правильности работы ЭВМ) с периодом, большим 7 суток. При отсутствии таких требований или при невозможности их выполнения перезагрузку работающей ЭВМ с установленным СКЗИ «Валидата CSP» необходимо производить с периодом не более 168 часов (7 суток).

4.3 Требования по обеспечению безопасности при выводе СКЗИ «Валидата CSP» из эксплуатации и передаче в ремонт

Ключи ЭП, прекратившие свое действие, уничтожаются порядком, установленным документом ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности», а ключи проверки ЭП (в составе соответствующих сертификатов ключей проверки ЭП) установленным порядком сохраняются в архивах для возможности в последующем выполнения процедуры разбора конфликтных ситуаций.

При обновлении СКЗИ «Валидата CSP» необходимо выполнить подготовку к переходу на новую версию СКЗИ «Валидата CSP», руководствуясь требованиями эксплуатационной документации новой версии СКЗИ «Валидата CSP». После выполнения всех необходимых подготовительных действий (при их наличии) необходимо удалить текущую версию СКЗИ «Валидата CSP».

Требования к порядку проведения ремонтных и регламентных работ при-

ведены в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

Для вывода СКЗИ «Валидата CSP» из эксплуатации на одном рабочем месте необходимо выполнить следующие действия:

- с использованием штатных средств СКЗИ «Валидата CSP» удалить ключи ЭП, хранящиеся в реестре ОС Windows (не требуется при переходе на новую версию СКЗИ «Валидата CSP»);

- удалить СКЗИ «Валидата CSP» в соответствии с документом ВАМБ.00060-06 91 01 «СКЗИ «Валидата CSP» версия 6. Руководство по установке и настройке»;

- в случае если СКЗИ «Валидата CSP» выводится из эксплуатации без установки новой версии СКЗИ «Валидата CSP», необходимо осуществить гарантированное уничтожение всех данных, хранящихся на жестком диске, например, путем четырехкратной перезаписи памяти жесткого диска случайными данными. Конкретный способ гарантированного уничтожения данных должен определяться исходя из модели угроз информационной безопасности, принятой в эксплуатирующей организации.

В случае вывода СКЗИ «Валидата CSP» из эксплуатации на всех рабочих местах эксплуатирующей организации без установки новой версии СКЗИ «Валидата CSP» необходимо выполнить следующие действия:

- прекратить действие ключей ЭП согласно положениям документа ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности» и требованиям УЦ;

- вывести СКЗИ «Валидата CSP» из эксплуатации на каждом рабочем месте в соответствии с требованиями, приведенными выше;

- вывести из эксплуатации на каждом рабочем месте эксплуатационную документацию СКЗИ «Валидата CSP» (например, путем удаления с ЭВМ). Рекомендуется архивировать журналы (см. документ ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности») и формуляр в бумажном виде, который находятся в подразделении, ответственном за эксплуатацию СКЗИ «Валидата CSP». Конкретный перечень подлежащих архивированию документов и срок их архивного хранения определяются эксплуатирующей организацией.

Действия, выполняемые с эталонными дистрибутивами, связанные с выводом из эксплуатации СКЗИ «Валидата CSP», определяются эксплуатирующей организацией. В случае уничтожения оптических носителей с эталонными дистрибутивами СКЗИ «Валидата CSP», данные носители должны быть уничтожены (утилизированы) способом, гарантированно исключающим восстановление информации (физическое разрушение, сжигание, разламывание, разрезание и т.п.).

5 СВЕДЕНИЯ О СОГЛАСОВАНИИ

Положения настоящего документа согласованы с ФСБ России.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ДСЧ	Датчик случайных чисел
МДЗ	Модуль доверенной загрузки
НСД	Несанкционированный доступ
ОС	Операционная система (Operating System)
ПАК	Программно-аппаратный комплекс
ПК	Программный комплекс
ПО	Программное обеспечение
СЗИ от НСД	Средство защиты информации от несанкционированного доступа
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр
ФЗ СКЗИ	Функционально законченные средства криптографической защиты информации
ФКН	Функциональный ключевой носитель
ЭВМ	Электронно-вычислительная машина
ЭП	Электронная подпись (Digital Signature)

[illegible][illegible]