ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-06–ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «ВАЛИДАТА CSP» ВЕРСИЯ 6

Формуляр

ВАМБ.00060-06 30 01

2020

Содержание

1 ОБЩИЕ УКАЗАНИЯ

1.1 Настоящий формуляр удостоверяет основные характеристики, определяет комплектность и общие требования по эксплуатации аппаратно-программного комплекса (АПК) ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP»).

1.2 Эксплуатирующая организация распечатывает и ведёт настоящий формуляр на бумаге. Формуляр должен находиться в подразделении, ответственном за эксплуатацию СКЗИ «Валидата CSP».

1.3 В формуляр заносят сведения о состоянии СКЗИ «Валидата CSP» в течение всего периода его эксплуатации.

1.4 Сведения об установке/удалении СКЗИ «Валидата CSP» на каждой ЭВМ эксплуатирующая организация заносит в раздел «Сведения об установке» настоящего формуляра.

Примечание — Установкой СКЗИ «Валидата CSP» считается установка любого его компонента. Удалением СКЗИ «Валидата CSP» с ЭВМ считается удаление всех его компонентов.

1.5 После полного заполнения любой из таблиц формуляра следует подготовить листы продолжения таблицы, пронумеровав их следующим образом: X.1, X.2 и т.д., где X — номер листа, на котором расположено начало таблицы.

1.6 Все записи в формуляре должны производиться отчётливо, аккуратно и должны быть заверены лицами, ответственными за эксплуатацию СКЗИ «Валидата CSP». Не допускаются записи, выполненные карандашом, смывающимися чернилами, подчистки, незаверенные исправления. Неправильная запись должна быть аккуратно зачёркнута и рядом записана новая, которую заверяет ответственное лицо. После подписи проставляют фамилию и инициалы ответственного лица (вместо подписи допускается проставлять личный штамп исполнителя).

2 ОСНОВНЫЕ ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ

2.1 СКЗИ «Валидата CSP» подлежит поэкземплярному учёту.

2.2 Установка СКЗИ «Валидата CSP» производится в соответствии с указаниями, приведёнными в эксплуатационной документации.

2.3 Эксплуатация СКЗИ «Валидата CSP» должна проводиться в соответствии с «Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» и с указаниями, приведёнными в эксплуатационной документации.

2.4 Сопровождение СКЗИ «Валидата CSP» осуществляется в установленном в эксплуатирующей организации порядке.

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

2.6 Ключевая система

2.6.1 Ключевая информация является конфиденциальной.

2.6.2 Сроки действия ключей электронной подписи (ЭП) и сертификатов ключей проверки ЭП в зависимости от условий эксплуатации приведены в документе ВАМБ.00060-06 31 01 «СКЗИ «Валидата CSP» версия 6. Описание применения».

2.7 Управление квалифицированными сертификатами ключей проверки ЭП при использовании СКЗИ «Валидата CSP» должно обеспечиваться с использованием средств удостоверяющего центра, имеющих действующий сертификат соответствия ФСБ России, а также ключ проверки ЭП в формате, соответствующем рекомендациям по стандартизации Р 1323565.1.023-2018 (утверждены приказом Росстандарта от 26.12.2018 № 1155-ст).

2.8 При обеспечении информационной безопасности в процессе использования СКЗИ «Валидата CSP» необходимо руководствоваться требованиями, изложенными в документах ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности» и ВАМБ.00060-06 93 03 «СКЗИ «Валидата CSP» версия 6. Функционирование в виртуальной среде. Руководство администратора информационной безопасности».

В случае нарушений при обеспечении информационной безопасности виновные лица должны привлекаться к ответственности в соответствии с требованиями эксплуатирующей организации.

2.9 При встраивании СКЗИ «Валидата CSP» в прикладное программное

обеспечение (прикладное ПО) необходимо проводить тематические исследования данного прикладного ПО. 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.

2.10 СКЗИ «Валидата CSP» не предназначено для защиты речевой информации.

2.11 Средствами СКЗИ «Валидата CSP» не допускается обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

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

2.13 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 программных комплексах (ПК) эксплуатирующий 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.

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

2.15 Эксплуатация СКЗИ «Валидата CSP» разрешается только на территории Российской Федерации.

3 ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1 Наименование: «Средство криптографической защиты информации «Валидата CSP» версия 6».

Обозначение: ВАМБ.00060-06.

3.2 Разработчик: Общество с ограниченной ответственностью «Валидата».

3.3 СКЗИ «Валидата CSP» предназначено для:

– использования в качестве криптопровайдера в составе функционально законченных СКЗИ, имеющих сертификат соответствия ФСБ России;

– обращения к криптографическим функциям в соответствии со стандартными интерфейсами CSP и CNG 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 переподключение 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 защищёнными приложениями Microsoft;

– встраивания в ОС Microsoft Windows в качестве криптографического провайдера CNG Microsoft, работающего с защищёнными приложениями Microsoft;

– встраивания в ОС Microsoft Windows в качестве провайдера безопасности SSPI Microsoft, работающего с защищёнными приложениями Microsoft.

3.4 Ключевая система СКЗИ «Валидата CSP» обеспечивает возможность организации защищённой связи пользователей сети с использованием уникальных ключей, создаваемых на основе принципа открытого распределения ключей.

3.5 Варианты исполнения и выполняемые нормативные требования

3.5.1 СКЗИ «Валидата CSP» имеет три исполнения:

– исполнение 1, для которого использование аппаратно-программных средств защиты информации от несанкционированного доступа (СЗИ от НСД), сертифицированных ФСБ России, является рекомендательным;

– исполнение 2, для которого использование аппаратно-программных СЗИ от НСД, сертифицированных ФСБ России, является обязательным;

– исполнение 3, для которого использование аппаратно-программных СЗИ от НСД, сертифицированных ФСБ, и средств создания замкнутой программной

среды является обязательным.

Примечания

1 Все исполнения имеют одну и ту же программную реализацию, не зависящую от применения совместно с СКЗИ «Валидата CSP» сертифицированного СЗИ от НСД.

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

3.5.2 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 $КС_Б$.

3.6 Реализуемые криптографические алгоритмы

3.6.1 СКЗИ «Валидата CSP» реализует криптографические алгоритмы согласно:

– 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 (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, ГОСТ 34.12-2018 и ГОСТ 34.13-2018 определяют криптографические механизмы, совпадающие с криптографическими механизмами, определенными в национальных стандартах ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 соответственно.

3.6.2 СКЗИ «Валидата CSP» реализует криптографические преобразования в соответствии с 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 1323565.1.020-2018);

– «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 1323565.1.023-2018).

3.7 Среда функционирования

3.7.1 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.

3.7.2 СКЗИ «Валидата CSP» функционирует на ЭВМ с 32-битными (x86) и 64-битными (x64) архитектурами, а также на виртуальных машинах, находящихся под управлением гипервизоров Microsoft Hyper-V и VMware ESXi версий 6.0/6.5/6.7 из состава VMware vSphere, в следующих ОС Microsoft Windows:

– Windows 7 (x86 и x64) с пакетом обновлений 1 (SP1) и выше;

– Windows Server 2008 R2 (x64) с пакетом обновлений 1 (SP1) и выше;

– Windows 8.1 (x86 и x64);

– Windows Server 2012 R2 (x64);
– 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, производителем которых не выпускаются обновления, запрещается подключение СКЗИ «Валидата CSP» и ПК, функционирующих совместно с СКЗИ «Валидата CSP», к каналам связи, выходящим за пределы контролируемой территории.

3.7.3 Для ОС Windows 7/Server 2008 R2 перед установкой СКЗИ «Валидата CSP» необходимо установить обновление KB3033929. Данное обновление необходимо для обеспечения возможности проверки подписанных модулей СКЗИ «Валидата CSP» с использованием алгоритма хэширования SHA-2.

3.7.4 СКЗИ «Валидата CSP» (32-битная реализация) работает только в среде 32-битных ОС, СКЗИ «Валидата CSP» (64-битная реализация) работает только в среде 64-битных ОС. Выбор реализации осуществляется во время установки СКЗИ «Валидата CSP» на ЭВМ.

3.7.5 При необходимости совместно с СКЗИ «Валидата CSP» могут использоваться сетевой адаптер и устройство резервного копирования информации на отчуждаемый носитель (например, CD-RW).

3.8 Совместно с СКЗИ «Валидата CSP» (исполнение 3) допускается использовать следующие средства создания замкнутой программной среды:

– средство защиты информации «Secret Net Studio 8.4».

3.9 Используемые СЗИ от НСД

3.9.1 Совместно с СКЗИ «Валидата CSP» (исполнение 1, исполнение 2, исполнение 3) допускается использовать следующие СЗИ от НСД, которые имеют в своём составе сертифицированный аппаратный датчик случайных чисел (ДСЧ):

– программно-аппаратный комплекс (ПАК) «Аккорд-АМДЗ» версия 3.2;
– ПАК «Соболь» версия 3.0 (версии кода расширения BIOS 1.0.99, 1.0.180);
– ПАК «Соболь» версия 3.1 (исполнения 1 и 2);
– ПАК «Соболь» версия 3.2 (исполнения 1 и 2).

3.9.2 Также допускается использование СКЗИ «Валидата CSP» (исполнение 1, исполнение 2) совместно со следующими СЗИ от НСД:

– ПАК «Аккорд-АМДЗ» (исполнения GX, GXM2, GXMH);

– 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»).

Использование данных СЗИ от НСД совместно со средствами Удостоверяющего центра запрещается.

3.9.3 Использование СКЗИ «Валидата CSP» совместно с указанными выше СЗИ от НСД допускается только при наличии у них действующих сертификатов соответствия требованиям к АПМДЗ по классу не ниже 3Б, выданных ФСБ России.

3.10 Используемые ключевые носители

3.10.1 В качестве ключевых носителей могут использоваться:

– USB-ключи типа смарт-карта ruToken S, ruToken Lite, ruToken PKI, ruToken ЭЦП, ruToken ЭЦП 2.0, eToken Pro (Java), JaCarta (PRO, PKI, LT), JaCarta-2 (ГОСТ, PKI/ГОСТ, PRO/ГОСТ) (только для хранения извлекаемых ключей);

– смарт-карты eToken Pro (Java), JaCarta (PRO, PKI), JaCarta-2 (ГОСТ, PKI/-ГОСТ, PRO/ГОСТ) (только для хранения извлекаемых ключей);

Примечание — Все указанные выше носители должны использоваться только в качестве пассивного хранилища ключевой информации без использования реализованных в них криптографических функций.

– функциональные ключевые носители (ФКН) «Валидата vdToken» (ФКН «vdToken») и ФКН «Валидата vdToken» версия 2.0 (ФКН «vdToken 2.0»). Данные ключевые носители могут использоваться для хранения неизвлекаемых и извлекаемых ключей, а также как функциональные внешние устройства для выполнения криптографических функций;

– flash-накопители с USB-интерфейсом;

– реестр ОС Windows;

– Touch Memory DS1995, DS1996 через считыватель ПАК «Аккорд-АМДЗ»;

– Touch Memory DS1995, DS1996 через съемник информации с контактным устройством DS-USB;

– Touch Memory DS1995, DS1996 через считыватель ПАК «Соболь»;

– Touch Memory DS1995, DS1996 через считыватель COM-порта типа Dallas (DS 9097E и DS 9097U);

– Touch Memory DS1995, DS1996 через считыватель Secret Net в средах Secret Net 7 и Secret Net Studio 8.

Примечания

1 Обеспечена возможность хранения нескольких ключей на носителях всех

типов. Количество хранимых ключей ограничено только объёмом памяти носителя. Обеспечена возможность хранения сертификатов вместе с соответствующими им ключами на устройствах типа смарт-карта.

2 Драйверы для работы с перечисленными 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».

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

4 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, ключи ЭП длиной 512 бит не поддерживаются, поддерживаются исключительно эллиптические кривые A, B, C из RFC 4357.

3.10.2 В качестве ключевых носителей при функционировании в виртуальной среде могут использоваться:

– USB-ключи типа смарт-карта ruToken S, ruToken Lite, ruToken PKI, ruToken ЭЦП, ruToken ЭЦП 2.0, eToken Pro (Java), JaCarta (PRO, PKI, LT), JaCarta-2 (ГОСТ, PKI/ГОСТ, PRO/ГОСТ) (только для хранения извлекаемых ключей);

– смарт-карты eToken Pro (Java), JaCarta (PRO, PKI), JaCarta-2 (ГОСТ, PKI/-ГОСТ, PRO/ГОСТ) (только для хранения извлекаемых ключей);

Примечание — Все указанные выше носители должны использоваться только в качестве пассивного хранилища ключевой информации без использования реализованных в них криптографических функций.

– ФКН «Валидата vdToken» и ФКН «Валидата vdToken» версия 2.0. Данные ключевые носители могут использоваться для хранения неизвлекаемых и извлекаемых ключей, а также как функциональные внешние устройства для выполнения криптографических функций;

– flash-накопители с USB-интерфейсом;

– реестр ОС Windows;

– Touch Memory DS1995, DS1996 через съемник информации с контактным устройством DS-USB.

3.11 Используемые ДСЧ

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

– сертифицированные аппаратные ДСЧ, входящие в состав СЗИ от НСД;

– «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.

3.11.2 При функционировании СКЗИ «Валидата CSP» совместно с перечисленными в п.3.9.1 СЗИ от НСД допускается использование аппаратного, «биологического» ДСЧ или ДСЧ ФКН «vdToken 2.0» для инициализации ДСЧ СКЗИ «Валидата CSP».

3.11.3 При функционировании СКЗИ «Валидата CSP» совместно с перечисленными в п.3.9.2 СЗИ от НСД допускается использование «биологического» ДСЧ или ДСЧ ФКН «vdToken 2.0» для инициализации ДСЧ СКЗИ «Валидата CSP».

3.12 Сведения о сборках СКЗИ «Валидата CSP»

3.12.1 Ниже (Таблица 1) приведена информация о сборках СКЗИ «Валидата CSP», прошедших сертификационные испытания на соответствие требованиям, указанным в п. 3.5 настоящего документа.

Таблица 1 – Сведения о сборках СКЗИ «Валидата CSP»

Номер сборки	**Регистрационный номер эталонного образца**	**Обозначение извещения об изменении**
6.0.451.0	№ XXXX-XXXXXX	-

3.12.2 Настоящий формуляр определяет комплектность и содержит сведения об СКЗИ «Валидата CSP» сборки 6.0.451.0, которая соответствует эталонному образцу № XXXX-XXXXXX и в которой реализованы изменения согласно всем указанным выше (Таблица 1) извещениям об изменении.

4 КОМПЛЕКТНОСТЬ

4.1 Комплектность СКЗИ «Валидата CSP» приведена ниже (Таблица 2).

Таблица 2 – Комплектность СКЗИ «Валидата CSP»

Обозначение	Наименование	Примечание
Программные комплексы		
ВАМБ.00060-06	«СКЗИ «Валидата CSP» версия 6»	
Эксплуатационная документация		
-	Комплект эксплуатационных документов согласно ВАМБ.00060-06 20 01 «СКЗИ «Валидата CSP» версия 6. Ведомость эксплуатационных документов»	
Прочее		
-	Лицензия на использование СКЗИ «Валидата CSP»	По запросу эксплуатирующей организации
-	Средство защиты информации от несанкционированного доступа согласно п. 3.9 настоящего формуляра	Приобретает эксплуатирующая организация
-	Средство создания замкнутой программной среды согласно п. 3.8 настоящего формуляра	Приобретает эксплуатирующая организация

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

4.3 ФКН «vdToken» соответствует ВАМБ.467649.001 ТУ.

4.4 ФКН «vdToken 2.0» соответствует ВАМБ.467649.002 ТУ.

5 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

5.1 ПК ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6», разработанный ООО «Валидата», регистрационный номер № XXXX-_____, соответствует эталону и признан готовым к эксплуатации.

Дата выпуска «_____» _____ _____ г.

От ООО «Валидата» _____
(подпись, расшифровака)
М.П.

6 ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

6.1 Пользователь приобретает изделие СКЗИ «Валидата CSP» и несёт ответственность за его использование в соответствии с требованиями, изложенными в эксплуатационной документации.

6.2 Предприятие-изготовитель гарантирует работоспособность изделия в соответствии с объявленными характеристиками при соблюдении пользователем требований эксплуатационной документации на изделие.

В случае выявления в изделии дефектов, не связанных с нарушением правил эксплуатации, транспортирования и хранения, изделие подлежит рекламации, и предприятие-изготовитель обязуется по получении рекламации в возможно короткий срок устранить дефекты своими силами и средствами вплоть до поставки нового изделия, а также принять меры, исключающие эти дефекты во всех остальных экземплярах изделия.

6.3 Гарантийный срок изделия — 12 (двенадцать) месяцев.

6.4 Начальной датой исчисления гарантийного срока изделия является дата поставки изделия (см. п. 6.6).

6.5 Действие гарантийных обязательств прекращается при истечении гарантийного срока.

Предложения по развитию направлять по адресу:

127287, г. Москва, ул. 2-я Хуторская, д.38А, стр. 1, 7 этаж, офис 709

Тел: (495) 730-74-13

Консультации по вопросам эксплуатации системы осуществляются отделом криптографических средств защиты по телефону (495) 730-74-13.

6.6 Данные о поставке (продаже) изделия:

_____

_____

(наименование организации-поставщика (продавца) изделия)

Дата поставки: «_____» _____ _____ г.

М.П.

(подпись)

Примечание — При отсутствии данных, приведённых в п. 6.6, датой поставки изделия считается дата выпуска, указанная в разделе 5.

7 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

7.1 Рекламации, связанные с эксплуатацией изделия, должны направляться предприятию-изготовителю в письменном виде по адресу, указанному в пункте 6.5 настоящего формуляра.

7.2 Срок рассмотрения рекламации — 1 (один) месяц со дня получения рекламации.

7.3 При несоответствии поставляемого изделия, его тары, упаковки, консервации, маркировки и комплектности требованиям сопроводительной документации, пользователь обязан направить рекламацию предприятию-изготовителю в течение 60 дней со дня поставки изделия.

7.4 Предприятие-изготовитель принимает рекламацию, если не установлена вина получателя в возникновении дефекта в изделии.

7.5 Сведения о рекламациях заносятся в таблицу ниже (Таблица 3).

Таблица 3 – Сведения о рекламациях

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

8 СВЕДЕНИЯ ОБ УСТАНОВКЕ

8.1 Сведения об установке/удалении СКЗИ «Валидата CSP», включая сведения об установке СЗИ от НСД (при наличии), следует заносить в таблицу ниже (Таблица 4).

Таблица 4 – Сведения об установке/удалении СКЗИ «Валидата CSP»

Регистрационный номер и разрядность СКЗИ «Валидата CSP»	Наименование и зав. номер СЗИ от НСД [1]	Наименование ЭВМ	Дата начала эксплуатации	Дата удаления окончания эксплуатации	Должность, ФИО ответственного за эксплуатацию

[1] Заполняется при наличии СЗИ от НСД

9 СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ

9.1 Сведения о закреплении СКЗИ «Валидата CSP» заносятся в таблицу ниже (Таблица 5).

Таблица 5 – Сведения о закреплении СКЗИ «Валидата CSP»

Наименование и регистрационный номер изделия	Дата	Должность, ФИО, подпись ответственного лица	Примечание

10 ОСОБЫЕ ОТМЕТКИ

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного докум и дата	Подп	Дата
Изм	изменённых	заменённых	новых	аннулированных					