

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00096-06-ЛУ

**СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«ВАЛИДАТА КРИПТОСЕРВЕР» ВЕРСИЯ 4**

Формуляр

ВАМБ.00096-06 30 01

2020

Содержание

1 ОБЩИЕ УКАЗАНИЯ	3
2 ОСНОВНЫЕ ТРЕБОВАНИЯ К ЭКСПЛУАТАЦИИ	4
3 ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ	8
4 КОМПЛЕКТНОСТЬ	13
5 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ	14
6 ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА	15
7 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ	16
8 СВЕДЕНИЯ ОБ УСТАНОВКЕ	17
9 ОСОБЫЕ ОТМЕТКИ	18

1 ОБЩИЕ УКАЗАНИЯ

1.1 Настоящий формуляр удостоверяет основные характеристики, определяет комплектность и общие требования по эксплуатации программного комплекса (ПК) ВАМБ.00096-06 «Средство криптографической защиты информации «Валидата Криптосервер» версия 4» сборки 6.0.482.0 (далее — СКЗИ «Валидата Криптосервер»).

1.2 Эксплуатирующая организация ведёт настоящий формуляр в бумажном или электронном виде. Допускается вести формуляр в электронном виде только в случае согласования порядка ведения такого формуляра с ФСБ России.

1.3 Формуляр должен находиться в подразделении, ответственном за эксплуатацию СКЗИ «Валидата Криптосервер».

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

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

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

1.6 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.

1.7 Все записи в формуляре в бумажном виде должны производиться отчётливо, аккуратно и должны быть заверены лицами, ответственными за эксплуатацию СКЗИ «Валидата Криптосервер». 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 Криптосервер» подлежит поэкземпляроному учёту.

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

2.3 Эксплуатация СКЗИ «Валидата Криптосервер» 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 Криптосервер» осуществляется в установленном в эксплуатирующей организации порядке.

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

2.6 Ключевая система

2.6.1 В качестве ключевой системы СКЗИ «Валидата Криптосервер» используется ключевая система, реализованная в ПК ВАМБ.00060-06 «СКЗИ «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP»).

2.6.2 Ключевая информация является конфиденциальной.

2.6.3 Максимальные сроки действия ключей электронной подписи (ЭП) и сертификатов ключей проверки ЭП 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 Криптосервер» должно обеспечиваться с использованием средств удостоверяющего центра, имеющих действующий сертификат соответствия (положительное заключение) 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).

2.8 При обеспечении информационной безопасности в процессе использования СКЗИ «Валидата Криптосервер» необходимо руководствоваться требованиями, изложенными в документе ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

В случае нарушений при обеспечении информационной безопасности виновные лица должны привлекаться к ответственности в соответствии с тре-

бованиями эксплуатирующей организации.

2.9 СКЗИ «Валидата Криптосервер» предназначено для использования в автоматизированных системах и программных комплексах (АС и ПК) эксплуатирующей организации, осуществляющих автоматическое создание и автоматическую проверку ЭП.

Примечание — В связи с этим требования п. 8 и п. 9 «Требований к средствам ЭП», утверждённых приказом ФСБ России от 27.12.2011 № 796, о визуализации подписываемых и проверяемых данных не применяются к СКЗИ «Валидата Криптосервер».

2.10 Требования к встраиванию

2.10.1 Встраивание СКЗИ «Валидата Криптосервер» в прикладные системы должно выполняться с использованием библиотек прикладного программного интерфейса, входящих в состав СКЗИ «Валидата Криптосервер» или в состав ПК ВАМБ.00136-06 «Средство криптографической защиты информации «Валидата Криптосервер L» версия 6».

2.10.2 При встраивании СКЗИ «Валидата Криптосервер» в прикладные системы необходимо проводить проверку (оценку) влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, с которыми предполагается его штатное функционирование, на выполнение предъявленных к данному средству требований, в следующих случаях:

- если информация конфиденциального характера подлежит защите в соответствии с законодательством Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;
- при организации криптографической защиты информации конфиденциального характера в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнении работ или оказании услуг для государственных нужд;
- если обязательность защиты информации конфиденциального характера возлагается законодательством Российской Федерации на лиц, имеющих доступ к этой информации или наделенных полномочиями по распоряжению сведениями, содержащимися в данной информации;
- при обработке информации конфиденциального характера, обладателем которой являются государственные органы или организации, выполняющие государственные заказы, в случае принятия ими мер по охране ее конфиденциальности путём использования средств криптографической защиты;
- при обработке информации конфиденциального характера в государственных органах и в организациях, выполняющих государственные заказы, обладатель которой принимает меры к охране её конфиденциальности путём установления необходимости криптографической защиты данной информации.

В остальных случаях указанная проверка носит рекомендательный характер.

2.10.3 В рамках работ по проверке (оценке) влияния необходимо проводить следующие исследования:

- проверку выполнения требований и рекомендаций, указанных в документации на СКЗИ «Валидата Криптосервер»;
- проверку отсутствия ухудшений инженерно-криптографических свойств СКЗИ «Валидата Криптосервер»;
- проверку выполнения требований к контролю целостности;
- анализ документации прикладного программного обеспечения, использующего СКЗИ «Валидата Криптосервер»;
- проверку ПО BIOS/UEFI ЭВМ, на которой функционирует СКЗИ «Валидата Криптосервер», в соответствии с нормативно-методическими документами ФСБ России в части проведения исследования ПО BIOS/UEFI.

2.10.4 Указанная проверка (оценка) должна проводиться по техническому заданию, согласованному с Центром защиты информации и специальной связи ФСБ России. Проверка должна производиться специализированными организациями, имеющими лицензию ФСБ России на указанный вид деятельности и соответствующую аккредитацию испытательной лаборатории.

2.11 СКЗИ «Валидата Криптосервер» не предназначено для защиты речевой информации.

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

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

2.14 Технические средства, на которых предполагается эксплуатация СКЗИ «Валидата Криптосервер», 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 Криптосервер» 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 переда-

чи 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.

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

2.16 Эксплуатация СКЗИ «Валидата Криптосервер» разрешается только на территории Российской Федерации.

3 ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1 Наименование: «Средство криптографической защиты информации «Валидата Криптосервер» версия 4».

Обозначение: ВАМБ.00096-06.

3.2 Разработчик: Общество с ограниченной ответственностью «Валидата».

3.3 СКЗИ «Валидата Криптосервер» предназначено для:

- предоставления (в качестве сервера) криптографических функций прикладным серверам, клиентским рабочим местам, обращающимся к нему по протоколу удаленного вызова процедур (DCE RPC);
- контроля целостности, подтверждения авторства, неотрекаемости от авторства и обеспечения конфиденциальности электронных документов, передаваемых в режимах on-line и off-line между клиентскими рабочими местами и центрами обработки информации (ЦОИ) АС и ПК эксплуатирующей организации;
- обеспечения работы криптографического сервера (далее — КС или Криптосервер) в среде операционной системы (ОС) Windows как на одной ЭВМ, так и на нескольких ЭВМ, объединенных в кластер для повышения отказоустойчивости и/или обеспечения балансировки сетевой нагрузки (NLB);
- обеспечения удаленной загрузки ключевой информации в КС;
- использования в качестве инструментария, обеспечивающего проверку работоспособности КС.

3.4 СКЗИ «Валидата Криптосервер» образуют следующие компоненты:

- ПК ВАМБ.00096-06 12 01 «Криптографический сервер»;
- ПК ВАМБ.00096-06 12 02 «Автоматизированное рабочее место управления криптографическим сервером»;
- ПК ВАМБ.00096-06 12 03 «Автоматизированное рабочее место формирования отчётов»;
- ВАМБ.00096-06 12 04 «Библиотека прикладного программного интерфейса криптографического сервера для C/C++»;
- ВАМБ.00096-06 12 05 «Конфигурация криптографического сервера»;
- ВАМБ.00096-06 12 06 «Монитор криптографического сервера»;
- ВАМБ.00096-06 12 07 «Программа тестирования аппаратно-программных средств криптографического сервера»;
- ВАМБ.00096-06 12 08 «Библиотека прикладного программного интерфейса криптографического сервера для платформ “Java” и “IBM WebSphere Application Server”».

3.5 Варианты исполнения и выполняемые нормативные требования

3.5.1 СКЗИ «Валидата Криптосервер» имеет два 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.

Используемые совместно с СКЗИ «Валидата Криптосервер» СЗИ от НСД должны иметь действующие сертификаты и/или положительные заключения ФСБ России о соответствии требованиям, указанным в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

Примечания

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

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

3.5.2 СКЗИ «Валидата Криптосервер» удовлетворяет:

– «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;

– «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;

– «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну»:

- для исполнения 1 — по классу КС1 при функционировании в физической и виртуальной среде;
- для исполнения 2 — по классу КС2 при функционировании в физической среде.

3.5.3 СКЗИ «Валидата Криптосервер» поддерживает работу с сертификатами, удовлетворяющими «Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи», утверждённым приказом ФСБ России от 27.12.2011 № 795.

3.6 Среда функционирования

3.6.1 СКЗИ «Валидата Криптосервер» функционирует совместно с ПК ВАМБ.00077-06 «“Валидата Клиент” версия 4» (далее — ПК «Валидата Клиент»), имеющим положительное заключение ФСБ России о соответствии:

- «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;
- «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классам КС1, КС2;
- «Требованиям к средствам электронной подписи», утверждённым приказом ФСБ России от 27.12.2011 № 796, по классам КС1, КС2.

3.6.2 ПК «Валидата Клиент» функционирует совместно с СКЗИ «Валидата CSP», имеющим положительное заключение ФСБ России о соответствии:

- «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;
- «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классам КС1, КС2;
- «Требованиям к средствам электронной подписи», утверждённым приказом ФСБ России от 27.12.2011 № 796, по классам КС1, КС2.

3.6.3 ПК «Валидата Клиент» и СКЗИ «Валидата CSP» при эксплуатации в рамках СКЗИ «Валидата Криптосервер» по исполнению должны соответствовать СКЗИ «Валидата Криптосервер» (исполнение 1 или исполнение 2).

3.6.4 СКЗИ «Валидата Криптосервер» работает:

- в физической среде, использующей аппаратное обеспечение платформы функционирования ЭВМ, соответствующей требованиям, указанным в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр»;
- в виртуальной среде (использующей программную эмуляцию аппаратного обеспечения платформы функционирования ЭВМ) на виртуальных машинах, находящихся под управлением гипервизоров из перечня, приведённого в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

3.6.5 СКЗИ «Валидата Криптосервер» функционирует на ЭВМ с 32-битными (x86) и 64-битными (x64) архитектурами, а также на виртуальных машинах в ОС Microsoft Windows из перечня, приведённого в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

3.6.6 32-битные реализации ПК из состава СКЗИ «Валидата Криптосервер» как в физической среде, так и на виртуальных машинах функционируют и в

среде 32-битных, и в среде 64-битных ОС семейства Windows. 64-битные реализации ПК из состава СКЗИ «Валидата Криптосервер» функционируют только в среде 64-битных ОС семейства Windows. Выбор реализации осуществляется во время установки ПК из состава СКЗИ «Валидата Криптосервер».

3.6.7 КС может функционировать как на одной отдельной ЭВМ/ВМ, так и на нескольких ЭВМ/ВМ, объединенных в кластер для повышения отказоустойчивости и/или обеспечения балансировки сетевой нагрузки.

3.6.8 СКЗИ «Валидата Криптосервер» функционирует совместно с системами управления базами данных из перечня, приведенного в документе ВАМБ.00077-06 30 01 «“Валидата Клиент” версия 4. Формуляр».

3.6.9 СКЗИ «Валидата Криптосервер» может функционировать совместно с СЗИ от НСД, указанными в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

3.6.10 В СКЗИ «Валидата Криптосервер» обеспечена возможность использования сетевого справочника сертификатов.

3.7 Реализуемые криптографические алгоритмы

3.7.1 Для реализации криптографических преобразований информации в СКЗИ «Валидата Криптосервер» используется СКЗИ «Валидата CSP», выполняющее следующие криптографические функции:

- электронная подпись (создание и проверка) в соответствии с ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018) «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

- хэширование данных в соответствии с ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018) «Информационная технология. Криптографическая защита информации. Функция хэширования»;

- шифрование в соответствии с ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Информационная технология. Криптографическая защита информации. Блочные шифры» (блочные шифры «Магма» и «Кузнечик») и 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);

- шифрование в соответствии с 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.

3.7.2 СКЗИ «Валидата Криптосервер» реализует криптографические преобразования в соответствии с Рекомендациями по стандартизации, приведёнными в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

3.8 Перечень ключевых носителей, которые могут использоваться в СКЗИ «Валидата Криптосервер», приведён в документе ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

3.9 Сведения о сборках СКЗИ «Валидата Криптосервер»

3.9.1 Ниже (Таблица 1) приведена информация о сборках СКЗИ «Валидата Криптосервер», имеющих подтверждение соответствия требованиям, указанным в п. 3.5 настоящего документа.

Таблица 1 – Сведения о сборках СКЗИ «Валидата Криптосервер»

Номер сборки	Регистрационный номер эталонного образца	Обозначение извещения об изменении
6.0.482.0	№ 748Б-001003	ВАМБ.096-06.002

3.9.2 Допустимые сроки эксплуатации указанной выше (Таблица 1) сборки определяются положительным заключением и/или сертификатом соответствия, выданным ФСБ России по результатам сертификационных испытаний соответствующего эталонного образца.

3.9.3 Настоящий формуляр определяет комплектность и содержит сведения о СКЗИ «Валидата Криптосервер» сборки 6.0.482.0, которая соответствует эталонному образцу № 748Б-001003 и в которой реализованы изменения согласно указанному выше (Таблица 1) извещению об изменении.

4 КОМПЛЕКТНОСТЬ

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

Таблица 2 – Комплектность СКЗИ «Валидата Криптосервер»

Обозначение	Наименование	Примечание
<i>Программные комплексы</i>		
ВАМБ.00096-06	«СКЗИ «Валидата Криптосервер» версия 4»	
<i>Эксплуатационная документация</i>		
-	Комплект эксплуатационных документов согласно ВАМБ.00096-06 20 01 «СКЗИ «Валидата Криптосервер» версия 4. Ведомость эксплуатационных документов»	
<i>Прочее</i>		
-	Лицензия на использование СКЗИ «Валидата Криптосервер»	По запросу эксплуатирующей организации
-	Средство защиты информации от несанкционированного доступа согласно п. 3.6.9 настоящего формуляра	Приобретает эксплуатирующая организация

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

5 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

5.1 ПК ВАМБ.00096-06 «Средство криптографической защиты информации «Валидата Криптосервер» версия 4», регистрационный номер:

№ 748Б _____,

соответствует эталону и признан готовым к эксплуатации.

Дата «_____» _____ г.

От ООО «Валидата» _____
(подпись, расшифровка)

М.П.

6 ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

6.1 Пользователь приобретает изделие СКЗИ «Валидата Криптосервер» 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, исключаящие 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

8.1 Сведения об установке/удалении СКЗИ «Валидата Криптосервер» следует заносить в таблицу ниже (Таблица 4).

Для СКЗИ «Валидата Криптосервер» (исполнение 2) сведения об установке СЗИ от НСД следует заносить в соответствующий раздел документа ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

[illegible]

9 ОСОБЫЕ ОТМЕТКИ

[illegible]