Руководителям организаций,
участвующих в электронном обмене
с Банком России
(по списку, кроме ДПУ, ПУ)

О тестировании СКЗИ «Янтарь» версии 6
и СКАД «Сигнатура» версии 6

Информационное сообщение ВН-16-4-6-1/10303 от 22.11.2019 года.

Центр эксплуатации платежной системы Департамента информационных технологий (далее – ЦЭПС ДИТ) сообщает участникам обмена (далее – УО), что в настоящее время по заказу Банка России завершается разработка системы криптографической авторизации электронных документов (далее - СКАД) «Сигнатура» версия 6 и системы криптографической защиты информации (далее - СКЗИ) «Янтарь» версия 6 (далее вместе именуемые СКЗИ). Перечисленные программные продукты предназначены для замены СКАД «Сигнатура» версия 5 и СКЗИ «Янтарь» версия 5 в информационно-телекоммуникационных системах (далее - ИТС) Банка России и клиентов Банка России, взаимодействующих с ИТС Банка России, а также операционным и платежным клиринговым центром системы быстрых платежей (далее – ИТС клиентов Банка России).

Мероприятия по замене СКЗИ версии 5 на СКЗИ версии 6 в режиме функциональных возможностей, совпадающих с СКЗИ 5 (далее – режим старого функционала) планируется начать с июля 2020 года, после окончания сертификационных исследований СКЗИ и получения соответствующих документов из ФСБ России.

Помимо функциональных возможностей, реализованных в СКЗИ версии 5, СКЗИ версии 6 содержат новый функционал, в том числе в них реализовано шифрование по ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Работы по переводу АС (ППК) на использование СКЗИ версии 6 в режиме шифрования с использованием ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015 предполагается инициировать в 2021 году.

После окончания мероприятий по замене СКАД «Сигнатура» версия 5 и СКЗИ «Янтарь» версия 5 будут выведены из эксплуатации и их поддержка прекратится.

С целью проверки готовности функционирования автоматизированных систем клиентов Банка России с использованием СКЗИ версии 6 в режиме старого функционала, ЦЭПС ДИТ предлагает принять участие в тестировании сборок СКЗИ, прошедших приемочные испытания в Банке России.

В связи с этим ЦЭПС ДИТ просит УО в срок до 29.11.2019 предоставить информацию о необходимости получения СКЗИ для проведения тестирования.

Данную информацию в форме заявки необходимо направлять на адрес электронной почты helpdeskmci@cbr.ru с указанием в теме сообщения «Заявка на получение СКАД». В тексте сообщения в соответствии с шаблоном, приведенным в приложении к данному информационному сообщению, необходимо указать БИК/УИС организации, наименование организации, тип используемого СКЗИ количество лицензий, необходимых для установки, о необходимости изготовления тестовой ключевой информации (в целях тестирования СКЗИ версии 6 возможно использование имеющейся актуальной тестовой ключевой информации, изготовленной ранее для СКЗИ версии 5), контакты ответственных лиц.

Установочные комплекты СКЗИ будут переданы УО, направившим информацию о необходимости получения СКЗИ для тестирования, установленным порядком после окончания приемочных испытаний в Банке России. Срок окончания приемочных испытаний - ориентировочно – 22 ноября 2019 г.).

О возможности получения СКЗИ для тестирования УО, направившие сведения, будут проинформированы дополнительно.

Рекомендуемые сроки тестирования в ИТС клиентов Банка России – до 13 марта 2020 г.

ЦЭПС обращает внимание УО на то, что дистрибутив СКЗИ «Янтарь» версии 6 будет предоставлен для промышленной эксплуатации только тем УО, с

которыми ГУ по ЦФО заключило соглашения о передаче программного обеспечения СКЗИ СКАД «Янтарь».

Данное сообщение будет размещено на сайте Банка России www.cbr.ru/mcirabis/ в разделе «Информация о работе платежной системы Банка России».

Контактные данные Единой службы поддержки пользователей Департамента информационных технологий:

многоканальный телефон - 8 (495) 957-80-01;

адрес электронной почты - helpdeskmci@cbr.ru

Приложения: 1. Заявка на получение СКЗИ – 1 л.
2. «СКАД «Сигнатура» версии 6. АПК Средство КЗИ СКАД «Сигнатура» версии 6. Формуляр. ВАМБ.00107-06 30 01» - 1 файл.

Заместитель директора Департамента
информационных технологий –
директор Центра эксплуатации
платежной системы М.Н. Шашлов

Приложение 1

Заявка на получение СКЗИ

БИК/УИС организации	
Наименование организации	
ФИО, контактные данные ответственного специалиста	
СКАД «Сигнатура» версия 6 и/или СКЗИ «Янтарь» версия 6	
Количество лицензий для СКАД «Сигнатура» версия 6 и/или СКЗИ «Янтарь» версия 6	
Необходимо ли изготовление тестовой ключевой информации	

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УТВЕРЖДЕН
ВАМБ.00107-06–ЛУ

СИСТЕМА КРИПТОГРАФИЧЕСКОЙ АВТОРИЗАЦИИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ «СИГНАТУРА» ВЕРСИЯ 6

АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ СКАД «СИГНАТУРА» ВЕРСИЯ 6

Формуляр

ВАМБ.00107-06 30 01

2019

Содержание

1 ОБЩИЕ УКАЗАНИЯ

1.1 Настоящий формуляр удостоверяет основные характеристики, определяет комплектность и общие требования по эксплуатации аппаратно-программного комплекса (АПК) ВАМБ.00107-06 «Средство криптографической защиты информации СКАД «Сигнатура» версия 6» (далее — АПК «Средство КЗИ») из состава программного комплекса (ПК) ВАМБ.00104-06 «Система криптографической авторизации электронных документов «Сигнатура» версия 6» (далее — СКАД «Сигнатура»).

1.2 Эксплуатирующая организация распечатывает и ведёт настоящий формуляр на бумаге. Формуляр должен находиться в подразделении, ответственном за эксплуатацию АПК «Средство КЗИ».

1.3 В формуляр заносят сведения о состоянии АПК «Средство КЗИ» в течение всего периода его эксплуатации.

1.4 Сведения об установке/удалении АПК «Средство КЗИ» на каждой ЭВМ эксплуатирующая организация заносит в раздел «Сведения об установке» настоящего формуляра.

Примечание — Установкой АПК «Средство КЗИ» считается установка любого его компонента. Удалением АПК «Средство КЗИ» 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: Х.1, Х.2 и т.д., где Х — 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 АПК «Средство КЗИ». 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 АПК «Средство КЗИ» подлежит поэкземплярному учёту.

2.2 Установка АПК «Средство КЗИ» производится в соответствии с указаниями, приведёнными в эксплуатационной документации.

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

2.4 Сопровождение АПК «Средство КЗИ» осуществляется в установленном в эксплуатирующей организации порядке.

2.5 К установке, эксплуатации и сопровождению АПК «Средство КЗИ» допускаются специалисты, изучившие соответствующие эксплуатационные документы.

2.6 Ключевая система

2.6.1 Ключевая информация является конфиденциальной.

2.6.2 Сроки действия ключей и сертификатов в зависимости от условий эксплуатации приведены в документе ВАМБ.00107-06 31 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Описание применения».

2.7 Управление квалифицированными сертификатами ключей проверки электронной подписи (ЭП) при использовании АПК «Средство КЗИ» должно обеспечиваться с использованием удостоверяющего центра, реализуемого посредством сертифицированного ФСБ России АПК ВАМБ.00105-06 «Сигнатура-сертификат» версия 6» из состава СКАД «Сигнатура», либо другой сертифицированной ФСБ России схемы распределения ключей.

2.8 При обеспечении информационной безопасности в процессе использования АПК «Средство КЗИ» необходимо руководствоваться требованиями, изложенными в документах ВАМБ.00107-06 93 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Руководство администратора информационной безопасности» и ВАМБ.00107-06 93 03 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» 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 АПК «Средство КЗИ» не предназначен для защиты речевой информации.

2.10 Средствами АПК «Средство КЗИ» не допускается обрабатывать информацию, содержащую сведения, составляющие государственную тайну.

2.11 АПК «Средство КЗИ» не должен эксплуатироваться в помещениях, где присутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и (или) установлены технические средства и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну.

2.12 ЭВМ, на которых предполагается эксплуатация АПК «Средство КЗИ», 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) Банка России. Данное требование не предъявляется в случае эксплуатации АПК «Средство КЗИ» при обработке открытой информации, доступ к которой не ограничивается согласно законодательству Российской Федерации.

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

2.14 Эксплуатация АПК «Средство КЗИ» разрешается только на территории Российской Федерации.

3 ОБЩИЕ СВЕДЕНИЯ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1 Наименование: «Средство криптографической защиты информации СКАД «Сигнатура» версия 6».

Обозначение: ВАМБ.00107-06.

3.2 Разработчик: Общество с ограниченной ответственностью (ООО) «Валидата».

3.3 АПК «Средство КЗИ» предназначен 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 АПК «Средство КЗИ» 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 АПК «Средство КЗИ» имеет два варианта 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.

Примечания

1 Оба варианта исполнения имеют одну и ту же программную реализа-

цию, не зависящую от применения совместно с АПК «Средство КЗИ» или ПК «Средство КЗИ» сертифицированного СЗИ от НСД. В связи с этим, применяемые в эксплуатационной документации АПК «Средство КЗИ» обозначения АПК и ПК идентичны.

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

3.5.2 АПК «Средство КЗИ» удовлетворяет «Требованиям к шифровальным (криптографическим) средствам, 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,

а также «Специальным требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации» по классу КС.

3.6 АПК «Средство КЗИ» 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 работы с архивными ЭП в АПК «Средство КЗИ» 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.

3.7 Среда функционирования

3.7.1 АПК «Средство КЗИ» 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).

Для указанных ОС, а также для гипервизоров должно быть обеспечено получение обновлений безопасности. В случае использования ОС, производителем которых не выпускаются обновления, запрещается подключение АПК «Средство КЗИ» и АПК, функционирующих совместно с АПК «Средство КЗИ», к каналам связи, выходящим за пределы контролируемой территории.

Для возможности проверки подписанных модулей АПК «Средство КЗИ» с использованием алгоритма хэширования SHA-2 в ОС Windows 7/Server 2008 R2 должно быть установлено обновление KB3033929.

3.7.2 АПК «Средство КЗИ» (32-битная реализация) работает только в среде 32-битных ОС, АПК «Средство КЗИ» (64-битная реализация) работает только в среде 64-битных ОС. Выбор реализации осуществляется во время установки АПК «Средство КЗИ» на ЭВМ.

3.8 Используемые СЗИ от НСД

3.8.1 Совместно с АПК «Средство КЗИ» 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).

При функционировании АПК «Средство КЗИ» (как в исполнении 1, так и в исполнении 2) совместно с перечисленными выше СЗИ от НСД допускается использование как аппаратного, так и «биологического» ДСЧ для инициализации ДСЧ АПК «Средство КЗИ».

3.8.2 Допускается использование АПК «Средство КЗИ» совместно с ПАК «Аккорд-АМДЗ» (исполнения GX, GXM2, GXMH) в случае использования «биологического» ДСЧ для инициализации ДСЧ АПК «Средство КЗИ». Использование указанного СЗИ от НСД совместно со средствами Удостоверяющего центра запрещается.

3.8.3 Использование АПК «Средство КЗИ» 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.

3.9 Используемые ключевые носители

3.9.1 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), JaCarta (PKI) (только для хранения извлекаемых ключей);

– смарт-карты eToken Pro (Java), JaCarta (PRO), JaCarta (PKI) (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» и ФКН «Валидата 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;

– 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 АПК «Средство КЗИ» не входят и приобретаются эксплуатирующей организацией самостоятельно. Для обеспечения правильного взаимодействия АПК «Средство КЗИ» с устройствами считывания ключевой инфор-

мации необходимо произвести установку драйверов и другого необходимого ПО в соответствии с требованиями документации производителей до установки АПК «Средство КЗИ».

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 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.

3.9.2 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), JaCarta (PKI) (только для хранения извлекаемых ключей);

– смарт-карты eToken Pro (Java), JaCarta (PRO), JaCarta (PKI) (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 2.0»;

– flash-накопители с USB-интерфейсом;

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

3.10 Сведения о сертификационных испытаниях АПК «Средство КЗИ»

3.10.1 Ниже (Таблица 1) приведена информация о сборках АПК «Средство КЗИ», прошедших сертификационные испытания на соответствие требованиям, указанным в п. 3.5.

Таблица 1 – Сведения о сертификационных испытаниях АПК «Средство КЗИ»

Номер сборки	**Регистрационный номер эталонного образца**	**Обозначение извещения об изменении**
6.0.408.0		-

3.10.2 Настоящий формуляр определяет комплектность и содержит сведения об АПК «Средство КЗИ» сборки 6.0.408.0, в которой реализованы изменения согласно всем указанным выше (Таблица 1) извещениям об изменении.

4 КОМПЛЕКТНОСТЬ

4.1 Комплектность АПК «Средство КЗИ» приведена ниже (Таблица 2).

Таблица 2 – Комплектность АПК «Средство КЗИ»

Обозначение	Наименование	Примечание
Программные комплексы		
ВАМБ.00107-06	«Средство КЗИ СКАД «Сигнатура» версия 6»	
ВАМБ.00108-06 12 07	СКЗИ «Янтарь» версия 6. Программа тестирования аппаратно-программных средств криптографического сервера	
Эксплуатационная документация		
-	Комплект эксплуатационных документов согласно ВАМБ.00107-06 20 01 «СКАД «Сигнатура» версия 6. Средство КЗИ СКАД «Сигнатура» версия 6. Ведомость эксплуатационных документов»	
ВАМБ.00108-06 91 02	СКЗИ «Янтарь» версия 6. Программа тестирования аппаратно-программных средств криптографического сервера. Руководство по установке и настройке	
ВАМБ.00108-06 92 01	СКЗИ «Янтарь» версия 6. Программа тестирования аппаратно-программных средств криптографического сервера. Руководство пользователя	
Прочее		
-	Средство защиты информации от несанкционированного доступа согласно п. 3.8 настоящего формуляра	Приобретает эксплуатирующая организация
-	Носители ключевой информации со считывателями (включая драйверы) согласно п. 3.9 настоящего формуляра	Приобретает эксплуатирующая организация

4.2 АПК «Средство КЗИ» поставляется на компакт-диске, не допускающем перезапись информации.

4.3 Компакт-диск имеет маркировку с обозначением товарного знака компании–разработчика, обозначением, полным наименованием АПК, номером сборки и датой изготовления.

4.4 ФКН «vdToken» соответствует ВАМБ.467649.001 ТУ.

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

5 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

5.1 АПК ВАМБ.00107-06 «Средство криптографической защиты информации СКАД «Сигнатура» версия 6» в соответствии с результатами приемочных испытаний признан работоспособным и готовым к эксплуатации.

6 СВЕДЕНИЯ ОБ УСТАНОВКЕ

6.1 Сведения об установке/удалении АПК «Средство КЗИ», включая сведения об установке СЗИ от НСД (при наличии), следует заносить в таблицу ниже (Таблица 3).

Таблица 3 – Сведения об установке/удалении АПК «Средство КЗИ»

Регистрационный номер и разрядность АПК «Средство КЗИ»	Наименование и зав. номер СЗИ от НСД	Наименование организации/ подразделения	Заводской или инвентарный номер ЭВМ	Дата установки АПК и СЗИ от НСД, должность, фамилия, инициалы выполнившего установку	Дата удаления АПК и СЗИ от НСД, должность, фамилия, инициалы выполнившего удаление

7 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					