

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УТВЕРЖДЕН
ВАМБ.00037-06 51 01-ЛУ

Специализированный архиватор электронных сообщений версия 6

Программа и методика испытаний

ВАМБ.00037-06 51 01

АННОТАЦИЯ

Настоящий документ предназначен для проведения предварительных и приемочных испытаний программного комплекса «Специализированный архиватор электронных сообщений» версия 6 (далее - «Специализированный архиватор электронных сообщений версия 6»).

Документ содержит характеристику объекта испытаний, цель испытаний, перечень документации, предъявляемой на испытания, а также порядок и методику проведения испытаний.

Документ разработан в соответствии с положениями ГОСТ 19.301-79 специалистами ООО «Валидата».

СОДЕРЖАНИЕ

1 ОБЪЕКТ ИСПЫТАНИЙ.....	4
2 ЦЕЛЬ ИСПЫТАНИЙ	6
3 ОБЩИЕ ПОЛОЖЕНИЯ.....	7
4 ОБЪЁМ ИСПЫТАНИЙ.....	8
5 ПОРЯДОК И МЕТОДИКА ПРОВЕДЕНИЯ ИСПЫТАНИЙ	17
6 УСЛОВИЯ ПРОВЕДЕНИЯ ИСПЫТАНИЙ.....	26
7 ОТЧЕТНОСТЬ	27
ПРИЛОЖЕНИЕ А. СХЕМА СТЕНДА.....	29
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ.....	30

1 ОБЪЕКТ ИСПЫТАНИЙ

1.1 На испытания предъявляется программный комплекс (ПК) ВАМБ.00037-06 «Специализированный архиватор электронных сообщений версия 6» (далее - ПК САЭС), предназначенный для защиты конфиденциальной информации на основе использования криптографических процедур, реализованных в СКАД «Сигнатура» версия 6.

1.2 Использование ПК САЭС совместно со СКАД «Сигнатура» версия 6 обеспечит:

1) возможность применения в автоматизированных системах (АС) и ПК Банка России (без встраивания ПК САЭС) квалифицированных электронных подписей (ЭП) и сертификатов ключей проверки ЭП (далее – квалифицированный сертификат) в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», требованиями приказов ФСБ РФ от 27.12.2011 № 795 и № 796 и методическими рекомендациями по составу квалифицированного сертификата ключа проверки электронной подписи (методические рекомендации Министерства связи и массовых коммуникаций РФ версии 1.9);

2) возможность применения в АС и ПК Банка России криптографических функций в соответствии с национальными стандартами:

– ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» (для ключей ЭП длиной 256 и 512 бит), далее - ГОСТ Р 34.10-2012;

– ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» (для хэш-значений длиной 256 и 512 бит), далее - ГОСТ Р 34.11-2012;

– ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» (блочные шифры «Магма» и «Кузнечик»), далее - ГОСТ Р 34.12-2015;

– ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» (блочные шифры «Магма» и «Кузнечик» в режимах простой замены, гаммирования и выработки имитовставки), далее - ГОСТ Р 34.13-2015;

– ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» (далее - ГОСТ 28147-89);

3) реализацию в АС и ПК Банка России криптографических преобразований в соответствии с рекомендациями Технического комитета № 26 (далее - ТК26):

– «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);

– «Использование алгоритмов ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сообщениях формата Cryptographic Message Syntax (CMS)» (Р 1323565.1.025-2019).

1.3 На испытания предъявляется комплект программных документов согласно документу ВАМБ.00037-06 «Специализированный архиватор электронных сообщений версия 6. Спецификация».

2 ЦЕЛЬ ИСПЫТАНИЙ

2.1 Предварительные испытания проводятся с целью:

- определения работоспособности ПК САЭС;
- определения соответствия ПК САЭС требованиям документа «Специализированный архиватор электронных сообщений версия 6. Техническое задание» (далее – ТЗ);
- решения вопроса о возможности приемки ПК САЭС в опытную эксплуатацию.

2.2 Приемочные испытания проводятся с целью:

- определения соответствия ПК САЭС требованиям ТЗ;
- анализа результатов опытной эксплуатации ПК САЭС;
- решения вопроса о готовности ПК САЭС к эксплуатации.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Испытания проводятся на основании и в соответствии с распорядительным документом Банка России.

3.2 Перечень подразделений Банка России и организаций, участвующих в испытаниях:

- Департамент безопасности Банка России;
- Центр компетенции информационной безопасности «Рязань» (на правах сектора) отдела безопасности Отделения по Рязанской области Главного управления Центрального банка Российской Федерации по Центральному федеральному округу (далее - ЦКИБ «Рязань» Отделения Рязань);

- ООО «Валидата».

3.3 Перечень предъявляемых для проведения испытаний документов:

- «Специализированный архиватор электронных сообщений версия 6. Техническое задание»;

- комплект программных документов согласно документу ВАМБ.00037-06 «Специализированный архиватор электронных сообщений версия 6. Спецификация».

3.4 На приемочные испытания дополнительно предъявляются документы:

- Акт приемки в опытную эксплуатацию;
- Акт о завершении опытной эксплуатации.

4 ОБЪЁМ ИСПЫТАНИЙ

4.1 Испытания проводятся в следующем объеме:

- проверка функционирования ПК САЭС, разработанного в соответствии с ТЗ;
- оценка комплектности и качества документации.

4.2 Перечень обязательных проверок приведен в таблице 1. По решению комиссии могут быть проведены дополнительные проверки, перечень которых и, при необходимости, методика их выполнения должны быть приведены в Протоколах испытаний.

Таблица 1

Номер проверки	Выполняемые проверки	Номер пункта ТЗ	Номер пункта методики
1	<p>ПК САЭС версия 6 должен функционировать совместно со СКАД «Сигнатура» версия 6.</p> <p><i>Примечания</i></p> <p><i>1 В состав СКАД «Сигнатура» версия 6 входят ПК «Сигнатура-сертификат» версия 6 и «Сигнатура-клиент» версия 6.</i></p> <p><i>2 ПК «Сигнатура-клиент» версия 6 содержит в своем составе ПК «Средство криптографической защиты информации СКАД «Сигнатура» версия 6» (Средство КЗИ СКАД «Сигнатура» версия 6)</i></p>	4.1.1	5.2
2	<p>ПК САЭС версия 6 должен работать в среде 32-битных и 64-битных операционных систем (ОС) семейства Microsoft Windows, в среде которых функционирует ПК «Средство КЗИ СКАД «Сигнатура» версия 6».</p> <p><i>Примечание - Перечень ОС, в среде которых функционирует ПК «Средство КЗИ СКАД «Сигнатура» версия 6», приведён в документе ВАМБ.00107-06 30 01 «Система криптографической авторизации электронных документов «Сигнатура» версия 6. «Сигнатура-клиент» версия 6. Аппаратно-программный комплекс «Средство КЗИ СКАД «Сигнатура» версия 6». Формуляр»</i></p>	4.1.2	5.3
3	<p>ПК САЭС (ВАМБ.00037-02) и ПК САЭС версия 6 должны обеспечивать прямую совместимость, то есть все файлы, подписанные и/или зашифрованные с использованием ПК САЭС (ВАМБ.00037-02), должны проверяться/расшифровываться с использованием ПК САЭС версия 6</p>	4.1.3	5.4

Номер провер ки	Выполняемые проверки	Номер пункта ТЗ	Номер пункта методики
4	<p>ПК САЭС (ВАМБ.00037-02) и ПК САЭС версия 6 должны обеспечивать частичную обратную совместимость, то есть все файлы, подписанные и/или зашифрованные с использованием ПК САЭС версия 6, должны проверяться/расшифровываться с использованием ПК САЭС (ВАМБ.00037-02), за исключением режимов работы, не поддерживаемых ПК САЭС (ВАМБ.00037-02), а именно:</p> <ul style="list-style-type: none"> – использование алгоритмов шифрования, не поддерживаемых ПК САЭС (ВАМБ.00037-02); – проверка «больших» файлов (размером более 256Мб), подписанных присоединённой подписью (при этом проверка «небольших» файлов (размером менее 256Мб), подписанных присоединённой подписью в потоковом режиме, должна выполняться); – использование для подписи и шифрования сертификатов с «длинным» (1024) открытым ключом 	4.1.4	5.5
5	ПК САЭС версия 6 должен иметь собственную инсталляционную процедуру для 32-битной (x32) и 64-битной (x64) платформ	4.2.1	5.6
6	Инсталляционная процедура должна быть выполнена в формате MSI и должна быть совместимой с технологиями удалённой установки компании Microsoft. В документе «Руководство по установке и настройке» из состава документации ПК САЭС версия 6 должна быть описана процедура удаленной установки, описаны возможные ошибки при удаленной установке ПК САЭС версия 6 и рекомендации по их устранению	4.2.2	5.7
7	ПК САЭС версия 6 должен представлять собой программный модуль, встраивающийся в контекстное меню Проводника ОС Microsoft Windows и позволяющий выполнять криптографические операции с отдельными файлами, группами файлов и каталогами. Для выполнения криптографических операций ПК САЭС версия 6 должен использовать АПК «Сигнатура-клиент» версия 6	4.2.3	5.8
8	Функционирование ПК САЭС версия 6 в виртуальной среде допускается по уровню защиты КС1	4.3.1	5.9

Номер проверки	Выполняемые проверки	Номер пункта ТЗ	Номер пункта методики
9	<p>ПК САЭС версия 6 должен выполнять следующие операции:</p> <ol style="list-style-type: none"> 1) создание присоединенной ЭП в потоковом и блочном режимах; 2) проверка присоединенной ЭП в потоковом и блочном режимах; 3) проверка присоединенной ЭП с последующим удалением ЭП в потоковом и блочном режимах; 4) шифрование файлов в потоковом и блочном режимах; 5) расшифрование файлов в потоковом и блочном режимах; 6) получение информации о файле. <p><i>Примечания</i></p> <p><i>1 Если файл подписан, то выдается издатель, серийный номер сертификата подписанта и время создания ЭП (для всех подписей).</i></p> <p><i>2 Если файл зашифрован, то выдается издатель и серийный номер сертификата получателя зашифрованного сообщения (для всех получателей).</i></p> <p><i>3 Для файлов, подписанных или зашифрованных в формате CMS с использованием дополнения "X.509 Идентификатор ключа владельца" вместо пары издатель и серийный номер сертификата выдается идентификатор ключа владельца сертификата.</i></p> <p><i>4 Обеспечивается возможность просмотра сертификата в случае, если его можно найти;</i></p> <ol style="list-style-type: none"> 7) просмотр рабочего сертификата; 8) выгрузка ключа; 9) создание отсоединенной ЭП в потоковом и блочном режимах; 10) проверка отсоединенной ЭП в потоковом и блочном режимах; 11) удаление присоединенной ЭП без проверки ЭП; 12) кодирование файла в формате Base64; 13) раскодирование файла из формата Base64; 14) вычисление хэша файла 	4.3.2	5.10

Номер проверки	Выполняемые проверки	Номер пункта ТЗ	Номер пункта методики
10	<p>Настройки ПК САЭС версия 6 должны храниться в ветке системного реестра ОС Windows «HKEY_CURRENT_USER». Настройки должны содержать следующие параметры:</p> <ol style="list-style-type: none"> 1) «Отключить протокол выполненных операций» (по умолчанию выкл.); 2) «Не выдавать диалог сохранения файла» (по умолчанию: выкл.); 3) «Перезаписывать файлы без предупреждения» (по умолчанию: выкл.); 4) «Не выдавать предварительный диалог с количеством файлов» (по умолчанию: выкл.); 5) «Расширенная диагностика криптографических ошибок (стек)» (по умолчанию: выкл.); 6) «Каталог для сохранения подписанных/зашифрованных файлов» (по умолчанию: не задан); 7) «Каталог для сохранения проверенных/расшифрованных файлов» (по умолчанию: не задан); 8) «Каталог для сохранения файлов групп пользователей» (по умолчанию: не задан); 9) «Выгружать ключ после каждой операции» (по умолчанию: выкл.); 10) «Не проверять предыдущие подписи перед созданием ЭП» (по умолчанию: выкл.); 11) «Не добавлять сертификат в ЭП» (по умолчанию: выкл.); 12) «Не добавлять сертификат в локальный справочник» (по умолчанию: выкл.); 13) «Обновлять список аннулированных сертификатов (САС) из точки распространения» (по умолчанию: выкл.); 14) «Не использовать сетевой справочник (LDAP)» (по умолчанию: выкл.); 15) «Использовать TSP сервер» (по умолчанию: выкл.); <p><i>Примечание - TSP (Time Stamp Protocol) представляет из себя криптографический протокол, позволяющий создавать доказательства факта существования электронного документа в определенный момент времени.</i></p> <ol style="list-style-type: none"> 16) «Проверять штамп времени (TSP) при проверке подписи» (по умолчанию: выкл.); 17) «Отсутствие штампа времени (TSP) при проверке подписи считать ошибкой» (по умолчанию: выкл.); 	4.3.3	5.11

Номер проверки	Выполняемые проверки	Номер пункта ТЗ	Номер пункта методики
	<p>18) «Разрешить доступ к точкам AIA и CDP при построении цепочек» (по умолчанию: вкл.);</p> <p>19) «Использовать OCSP сервер» (по умолчанию: выкл.).</p> <p><i>Примечание - OCSP (Online Certificate Status Protocol) представляет из себя протокол проверки статуса сертификата, альтернативный или дополняющий работу с помощью списков CAC. OCSP сервер используется для отображения статуса сертификата после просмотра.</i></p> <p>20) «Режим шифрования и подписи: переключатель потоковый – блочный» (по умолчанию: потоковый);</p> <p>21) «Алгоритм шифрования» - раскрывающийся список со значениями:</p> <p>1) ГОСТ 28147-89 (по умолчанию),</p> <p>2) ГОСТ Р 34.12-2015/ГОСТ Р 34.13-2015 «Магма»,</p> <p>3) ГОСТ Р 34.12-2015/ГОСТ Р 34.13-2015 «Магма» с имитовставкой,</p> <p>4) ГОСТ Р 34.12-2015/ГОСТ Р 34.13-2015 «Кузнечик»,</p> <p>5) ГОСТ Р 34.12-2015/ГОСТ Р 34.13-2015 «Кузнечик» с имитовставкой;</p> <p>22) «Расширение файла с присоединённой подписью» (по умолчанию: «p7s»);</p> <p>23) «Расширение файла с отдельной подписью» (по умолчанию: «p7d»);</p> <p>24) «Расширение зашифрованного файла» (по умолчанию: «enc»);</p> <p>25) «Расширение файла в кодировке Base64» (по умолчанию: «b64»);</p> <p>26) «Расширение файла, содержащего хэш» (по умолчанию: «hsh»);</p> <p>27) «Список дополнительных расширений файлов» (по умолчанию: p7s);</p> <p>28) «Сохранять в файл список сертификатов при шифровании (по умолчанию – выкл)</p>		
11	Если настройки пользовательской конфигурации отсутствуют, то нужно считать, что заданы значения по умолчанию	4.3.4	5.12
12	ПК САЭС версия 6 должен позволять сохранять настройки в файл и загружать их из файла	4.3.5	5.13
13	Инсталляция программы должна устанавливать «иконки» на расширения файлов, заданные в конфигурации по умолчанию	4.3.6	5.14
14	<p>Функция получения «информации о файле» должна выдавать три варианта:</p> <p>1) файл зашифрован (дополнительная информация о зашифрованном файле);</p> <p>2) файл подписан (дополнительная информация о подписанном файле);</p> <p>3) файл не зашифрован и не подписан (отсутствие дополнительной информации)</p>	4.3.7	5.15

Номер проверки	Выполняемые проверки	Номер пункта ТЗ	Номер пункта методики
15	Функция подписи должна применяться к любому файлу. В том случае, когда необходимо подписать уже подписанный файл (или файл с подписями для отсоединенного формата), новая подпись должна добавляться к предыдущим подписям	4.3.8	5.16
16	В случае подписи файла, уже подписанного присоединённой подписью, новая подпись устанавливается в том режиме (блочный - потоковый), в котором установлена уже имеющаяся подпись. В этом случае значение конфигурационного параметра «Режим шифрования и подписи» игнорируется	4.3.9	5.17
17	Если необходимо подписать файл, который уже имеет предыдущую отсоединенную подпись, то программа должна добавлять ЭП в существующий отдельный файл с ЭП	4.3.10	5.18
18	Если выполняется групповая операция (ЭП, шифрование, ...) над несколькими файлами, то запрещается выдавать более одного диалогового окна с результатами операций	4.3.11	5.19
19	Необходимо обеспечить групповую обработку как нескольких файлов, так и нескольких директорий со всеми вложенными поддиректориями и файлами	4.3.12	5.20
20	При обработке нескольких файлов выдавать диалоговое окно со списком файлов и результатами, обеспечив возможный подробный просмотр каждого из этих файлов отдельным дополнительным нажатием кнопки. В случае обработки одного файла нужно показывать сразу подробный результат обработки	4.3.13	5.21
21	В случае совпадения имени при записи файла, нужно выдать стандартный диалог сохранения файла. Если в конфигурации установлен флаг «Не выдавать диалог сохранения файла», то выдать предупреждение «Перезаписать файл – «Да», «Нет», «Отмена»». Если в конфигурации установлен флаг «Перезаписывать файлы без предупреждения», то перезаписать файл	4.3.14	5.22
22	При выполнении проверки ЭП сообщения обеспечить опциональную возможность проверки меток времени для каждой из ЭП сообщения	4.3.15	5.23
23	Обеспечить возможность проверки сертификата (после успешного просмотра) на OCSP сервере	4.3.16	5.24
24	Обеспечить возможность доступа к точкам CRL Distribution Point и Authority Information Access для поиска сертификатов промежуточных Центров сертификации и САС, необходимых при построении цепочек сертификации	4.3.17	5.25
25	В случае недоступности обновления списка отозванных сертификатов должно выдаваться сообщение с объяснением причины	4.3.18	5.26

Номер проверки	Выполняемые проверки	Номер пункта ТЗ	Номер пункта методики
26	<p>Требования к функциям зашифрования файлов:</p> <p>1) зашифрование файла осуществляется на группы получателей зашифрованного сообщения;</p> <p>2) группа получателей зашифрованного сообщения представляет собой совокупность записей о получателях, представленную таблицей, включающей в себя следующие графы: «Ф.И.О.», «Организация», «Должность», «Структурное подразделение», «SubjectName»;</p> <p>3) должна быть обеспечена возможность сортировки группы получателей по каждой графе таблицы;</p> <p>4) перечень группы получателей зашифрованного сообщения может быть заполнен данными о пользователях путём загрузки файла группы получателей;</p> <p>5) перечень группы получателей зашифрованного сообщения может быть очищен от всех загруженных получателей;</p> <p>6) из перечня группы получателей зашифрованного сообщения возможно выбрать флажком используемых и неиспользуемых получателей;</p> <p>7) перечень группы получателей должен обеспечивать сохранение своего последнего состояния между перезапусками ПК САЭС версия 6;</p> <p>8) файл группы получателей формируется при помощи диалога формирования групп;</p> <p>9) диалог формирования групп обеспечивает возможность выборки сертификатов из локального справочника СКАД «Сигнатура» (без дополнительной фильтрации в ходе загрузки, за исключением проверки действительности сертификата и возможности его использования для шифрования) либо из Единой системы каталогов Банка России (с фильтрацией по полям LDAP);</p> <p>10) в процессе формирования группы получателей возможно запускать операцию поиска, аналогичную фильтрации по полям LDAP, которая устанавливает флажки для получателей, удовлетворяющих условиям поиска;</p> <p>11) диалог формирования групп содержит таблицу с полями, соответствующими полям группы получателей зашифрованного сообщения: «Ф.И.О.», «Организация», «Должность», «Структурное подразделение», «SubjectName»;</p>	4.3.19	5.27

Номер проверки	Выполняемые проверки	Номер пункта ТЗ	Номер пункта методики
	<p>12) соответствие содержимого, отображаемого в полях таблицы с соответствующими полями контейнера LDAP (для сертификата, найденного в Единой системе каталогов Банка России) или полями сертификата (для сертификата, найденного в локальном справочнике пользователя) представлено ниже:</p> <p>Поле таблицы получателей:</p> <ul style="list-style-type: none"> - Ф.И.О., - Организация, - Должность, - Структурное подразделение, - SubjectName <p>и соответствующее каждому Полю таблицы получателей Поле сертификата:</p> <ul style="list-style-type: none"> - Графа «Фамилия» из состава поля «X509v3 Альтернативное имя владельца», - Графа «Организация» из состава поля «X509v3 Альтернативное имя владельца», - Графа «Должность» из состава поля «X509v3 Альтернативное имя владельца», - Графа «Зарегистрированный адрес» из состава поля «X509v3 Альтернативное имя владельца», - Расширение «Предыдущее имя владельца», а при его отсутствии поле «Имя владельца», <p>а также соответствующее Поле LDAP:</p> <ul style="list-style-type: none"> - Поле «displayName», - Поле «company», - Поле «title», - Конкатенация (через пробел) расширенных атрибутов exchange №№15, 14, 13, 12, - Поле «vdsSubjName», а при его отсутствии поле «distinguishedName». <p><i>Примечания</i></p> <p>1 Для корректной работы ПК САЭС версия 6 значения полей сертификатов, находящихся в контейнере LDAP, должны совпадать со значениями соответствующих полей данного контейнера.</p> <p>2 Поиск в ЕСК по полю «Структурное подразделение» производится не по результату конкатенации, а отдельно по составляющим его атрибутам. Если хотя бы один атрибут соответствует условиям поиска, пользователь добавляется в список.</p>		

Номер провер ки	Выполняемые проверки	Номер пункта ТЗ	Номер пункта методики
	<p>13) диалог формирования групп должен предоставлять возможности сохранения текущего перечня найденных пользователей в файл группы получателей, открытия ранее созданного файла группы получателей, добавления содержания файла группы получателей к имеющемуся перечню пользователей и очистки этого перечня;</p> <p>14) среди перечня группы получателей диалога формирования групп возможно выбрать флажком получателей, подлежащих сохранению в заново создаваемый файл группы получателей;</p> <p>15) должна обеспечиваться возможность переноса списка найденных пользователей из диалогового окна формирования групп в диалог подготовки к шифрованию (без предварительного сохранения списка пользователей в файл группы)</p>		
27	ПК САЭС версия 6 должен вести протокол работы в системном журнале «Приложение» ОС Windows. Протоколироваться должны выполняемые операции, результаты выполнения операций и сообщения, выдаваемые СКАД «Сигнатура»	4.4	5.28
28	ПК САЭС версия 6 должен поставляться на оптических носителях, не допускающих перезапись информации	4.5.1	5.29
29	Оптический носитель с ПК САЭС версия 6 должен иметь маркировку с обозначением товарного знака компании-разработчика, наименованием ПК и номером сборки	4.5.2	5.30
30	Оценка комплектности и качества программной документации	5.1, 5.2	5.31
31	Проверка выполнения рекомендаций и устранения замечаний по результатам предварительных испытаний и опытной эксплуатации ПК САЭС (при необходимости)	-	5.32

5 ПОРЯДОК И МЕТОДИКА ПРОВЕДЕНИЯ ИСПЫТАНИЙ

5.1 Проверки осуществляются путем выполнения задач, в состав которых входит проверяемая функция. Результаты выполнения отображаются на экране, выводятся на печатающее устройство или помещаются в файлы данных.

Проверки, приведенные в таблице 1 настоящего документа, выполняются на стендовом оборудовании в соответствии с программной документацией ПК САЭС.

Результаты проверок считаются положительными, если в ходе их проведения все действия выполнены успешно, а результаты выполнения задач соответствуют требованиям ТЗ и отображаются в соответствии с эксплуатационной документацией ПК САЭС.

5.2 Проверка 1 таблицы 1

Проверка выполняется путем изучения документации и просмотра состава программного обеспечения (ПО), установленного на компьютерах с ПК САЭС.

Результат проверки считается положительным, если в документе ВАМБ.00037-06 91 01 есть запись о том, что ПК САЭС функционирует совместно со СКАД «Сигнатура» версия 6, а также на каждом компьютере стенда с ПК САЭС версия 6 установлена СКАД «Сигнатура» версия 6.

5.3 Проверка 2 таблицы 1

Проверка производится путем изучения дистрибутива ПК САЭС и просмотра установленного на компьютерах стенда ПК САЭС.

Результат проверки считается положительным, если в состав дистрибутива ПК САЭС входят 32-битные и 64-битные инсталляционные процедуры, а также на стенде присутствуют ПК САЭС, функционирующие в 32-битных и 64-битных операционных системах (ОС) семейства Microsoft Windows.

5.4 Проверка 3 таблицы 1

Проверка выполняется путем подписи и зашифрования файлов с помощью ПК САЭС ВАМБ.00037-02 (предыдущей версии), использующей СКАД «Сигнатура» версия 5.

Результат проверки считается положительным, если эти файлы были успешно расшифрованы и проверены с помощью ПК САЭС версия 6.

5.5 Проверка 4 таблицы 1

Проверка выполняется путем подписи и зашифрования файлов с помощью ПК САЭС версия 6, за исключением режимов работы, не поддерживаемых ПК САЭС ВАМБ.00037-02 (предыдущей версии).

Результат проверки считается положительным, если эти файлы были успешно расшифрованы и проверены с помощью ПК САЭС ВАМБ.00037-02 (предыдущей версии), использующей СКАД «Сигнатура» версия 5.

5.6 Проверка 5 таблицы 1

Проверка осуществляется путем изучения дистрибутива ПК САЭС.

Результат проверки считается положительным, если ПК САЭС имеет собственные инсталляционные процедуры для 32-битной (x32) и 64-битной (x64) платформ.

5.7 Проверка 6 таблицы 1

Проверка выполняется путем изучения документа ВАМБ.00037-06 91 01 «Специализированный архиватор электронных сообщений версия 6. Руководство по установке и настройке» и удалённой установки ПК САЭС на компьютеры стенда, где должен быть установлен ПК САЭС (русскоязычное исполнение). Если ПК САЭС уже установлен на этих компьютерах, он должен быть предварительно деинсталлирован вручную.

Результат проверки считается положительным, если ПК САЭС (после истечения тайм-аута применения политики и перезагрузки компьютеров) оказывается установлен на указанные компьютеры, а в документе описана процедура удаленной установки ПК САЭС, описаны возможные ошибки при удаленной установке ПК САЭС и даны рекомендации по их устранению.

5.8 Проверка 7 таблицы 1

Проверка выполняется путем выполнения криптографических операций ПК САЭС из контекстного меню Проводника ОС Microsoft Windows.

Результат проверки считается положительным, если ПК САЭС позволяет выполнять криптографические операции с отдельными файлами, группами файлов и каталогами из контекстного меню Проводника ОС Microsoft Windows.

5.9 Проверка 8 таблицы 1

Проверка выполняется путем изучения документации на ПК САЭС версия 6.

Результат проверки считается положительным, если в документе ВАМБ.00037-06 30 01 «Специализированный архиватор электронных сообщений версия 6. Формуляр» присутствует запись о том, что функционирование ПК САЭС в виртуальной среде допускается по уровню защиты KCI.

5.10 Проверка 9 таблицы 1

Проверка осуществляется с использованием ПК САЭС выполнением следующих операций:

- 1) создание присоединенной ЭП в потоковом и блочном режимах;
- 2) проверка присоединенной ЭП в потоковом и блочном режимах;
- 3) проверка присоединенной ЭП с последующим удалением ЭП в потоковом и блочном режимах;
- 4) шифрование файлов в потоковом и блочном режимах;
- 5) расшифрование файлов в потоковом и блочном режимах;
- 6) получение информации о файле.

- 7) просмотр рабочего сертификата;
- 8) выгрузка ключа;
- 9) создание отсоединенной ЭП в потоковом и блочном режимах;
- 10) проверка отсоединенной ЭП в потоковом и блочном режимах;
- 11) удаление присоединенной ЭП без проверки ЭП;
- 12) кодирование файла в формате Base64;
- 13) раскодирование файла из формата Base64;
- 14) вычисление хэша файла.

Результат проверки считается положительным, если все вышеперечисленные операции выполнены успешно.

5.11 Проверка 10 таблицы 1

Проверка выполняется путем сравнения настроек ПК САЭС в диалоге «Настройки пользователя» (пункт контекстного меню «Дополнительно -> Настройки пользователя») со значениями в ветке системного реестра ОС Windows `\HKEY_CURRENT_USER\Software\MDPREI\spkishxx`.

Результат проверки считается положительным, если все настройки ПК САЭС содержатся в системном реестре.

5.12 Проверка 11 таблицы 1

Проверка выполняется путем удаления настроек ПК САЭС из ветки системного реестра и перезапуска Проводника ОС Microsoft Windows.

Результат проверки считается положительным, если все параметры настроек ПК САЭС в диалоге «Настройки пользователя» соответствуют значениям «по умолчанию».

5.13 Проверка 12 таблицы 1

Проверка выполняется путем сохранения настроек ПК САЭС в файл, последующим их изменением и загрузкой из файла.

Результат считается положительным, если после загрузки настроек из файла все параметры вернулись к состоянию до внесения изменений.

5.14 Проверка 13 таблицы 1

Проверка выполняется путем проверки наличия «иконки» на расширения файлов, заданных в конфигурации по умолчанию.

Результат считается положительным, если инсталляция ПК САЭС устанавливает эти «иконки».

5.15 Проверка 14 таблицы 1

Проверка осуществляется путем выполнения функции получения «информации о файле» на трёх файлах – подписанном, зашифрованном и простом текстовом.

Результат считается положительным, если эта функция выдает три варианта:

- 1) файл зашифрован (дополнительная информация о зашифрованном файле);*
- 2) файл подписан (дополнительная информация о подписанном файле);*
- 3) файл не зашифрован и не подписан (отсутствие дополнительной информации).*

5.16 Проверка 15 таблицы 1

Проверка выполняется путем выполнения функции подписи к подписанному файлу.

Результат считается положительным, если при подписи уже подписанного файла (или файла с подписями для отсоединенного формата) новая подпись добавляется к предыдущим подписям.

5.17 Проверка 16 таблицы 1

Проверка выполняется путем подписи в разных режимах двух файлов, один из которых уже подписан присоединённой подписью в блочном режиме, а второй файл подписан присоединённой подписью в потоковом режиме.

Результат считается положительным, если подпись добавляется в том же режиме, что и предыдущая подпись, а значение конфигурационного параметра «Режим шифрования и подписи» игнорируется.

5.18 Проверка 17 таблицы 1

Проверка выполняется путем подписи файла, который уже имеет предыдущую отсоединённую подпись.

Результат проверки считается положительным, если ЭП добавляется в существующий отдельный файл с ЭП.

5.19 Проверка 18 таблицы 1

Проверка осуществляется путем выполнения групповых операций (ЭП, шифрование, ...) над несколькими файлами.

Результат считается положительным, если при этом выдается не более одного диалогового окна с результатами операций.

5.20 Проверка 19 таблицы 1

Проверка выполняется путем выполнения операций над несколькими файлами и несколькими директориями с вложенными поддиректориями и файлами.

Результат считается положительным, если такие групповые операции выполняются над всеми выбранными файлами и всеми файлами в выбранных директориях и поддиректориях.

5.21 Проверка 20 таблицы 1

Проверка осуществляется путем выполнения обработки нескольких файлов и одного файла.

Результат считается положительным, если при обработке нескольких файлов выдается диалоговое окно со списком файлов и результатами, что обеспечивает возможность подробного

просмотра каждого из этих файлов отдельным дополнительным нажатием кнопки. В случае обработки одного файла сразу показывается подробный результат обработки этого файла.

5.22 Проверка 21 таблицы 1

Проверка осуществляется путем создания ситуации с совпадением имен файлов во время их сохранения в одном каталоге. Такую проверку нужно провести при четырех разных режимах конфигурации:

- флаги, регулирующие сохранение файлов, не установлены;
- установлен флаг «Не выдавать диалог сохранения файла»;
- установлен флаг «Перезаписывать файлы без предупреждения»;
- установлены оба флага.

Результат считается положительным, если при сохранении в одном каталоге файлов с одинаковыми именами выполняются соответствующие четырем режимам конфигурации действия:

- *выдается стандартный диалог сохранения файла, а затем (при выборе существующего)*
- *предупреждение;*
- *выдается предупреждение «Перезаписать файл – Да, Нет» или «Перезаписать файл – Да, Нет, Отмена» - для операций с несколькими файлами;*
- *выдается стандартный диалог сохранения файла;*
- *файл перезаписывается без предупреждения.*

5.23 Проверка 22 таблицы 1

Проверка осуществляется путем проверки файла, подписанного с использованием сервера проверок меток времени (создать такой файл можно, выполнив подпись при установленном в настройках режиме «Использовать TSP сервер»). Проверка проводится два раза с установленным и не установленным в настройках режимом «Проверять штамп времени при проверке подписи».

Результат считается положительным, если при проверке без установленного режима «Проверять штамп времени при проверке подписи» результат проверки выглядит как при обычной проверке подписи, а при проверке с установленным режимом «Проверять штамп времени при проверке подписи» результат проверки содержит дополнительную запись с информацией о штампе времени.

5.24 Проверка 23 таблицы 1

Проверка выполняется путем открытия диалога просмотра сертификата из диалога «Информация о файле» с последующим нажатием кнопки «ОК» при условии, что в настройках включён режим «Использовать OCSP-сервер».

Результат проверки считается положительным, если ПК САЭС отображает на экране диалог, содержащий информацию о результатах проверки сертификата на OCSP-сервере.

5.25 Проверка 24 таблицы 1

Проверка выполняется путем двух проверок файла, подписанного сертификатом, для которого в локальном справочнике отсутствуют объекты, необходимые для построения цепочки (сертификаты ЦС и/или САС). Режим «Не использовать сетевой справочник» отключён. Режим «Разрешить доступ к точкам AIA и CDP при построении цепочек» во время первой проверки выключен, во время второй – включён.

Результат проверки считается положительным, если первая проверка завершается с ошибкой «Сертификат издателя не найден» (или «САС издателя не найден»), а вторая - успешно.

5.26 Проверка 25 таблицы 1

Проверка выполняется путем создания условий недоступности обновления списка аннулированных сертификатов (например, отключения сети). Режим «Обновлять САС из точки распространения» должен быть включён. Если обновление уже происходило в процессе предыдущих испытаний, необходимо подождать время, указанное в параметре настроек «Периодичность» либо удалить параметр реестра ОС Windows \HKEY_CURRENT_USER\Software\MDPREI\LastCIUpdate. Затем необходимо выполнить в ПК САЭС любую операцию, требующую загрузки ключа.

Результат проверки считается положительным, если выдается сообщение о невозможности обновления САС с указанием причины.

5.27 Проверка 26 таблицы 1

Проверка осуществляется путем выполнения следующих тестов:

Тест 1. В диалоге формирования групп создаётся группа из нескольких пользователей (например, из локального справочника), в диалоге зашифрования созданная группа открывается и на неё производится зашифрование. Затем к полученному зашифрованному файлу применяется функция «Информация о файле».

Результат проверки считается положительным, если файл оказывается зашифрованным на сертификаты тех и только тех пользователей, которые указаны в созданной группе (плюс рабочий сертификат профиля).

Тест 2. В диалоге зашифрования открываем ранее созданную группу.

Результат проверки считается положительным, если группа получателей зашифрованного сообщения представляет собой совокупность записей о получателях, представленную таблицей, включающей в себя следующие графы: «Ф.И.О.», «Организация», «Должность», «Структурное подразделение», «SubjectName»;

Тест 3. В диалоге зашифрования открываем ранее созданную группу и кликаем мышью в области заголовка таблицы.

Результат проверки считается положительным, если группа получателей

зашифрованного сообщения пересортируется по любой графе таблицы.

Тест 4. В диалоге зашифрования открываем ранее созданную группу.

Результат проверки считается положительным, если группа получателей зашифрованного сообщения заполнилась данными о пользователях.

Тест 5. В диалоге зашифрования открываем ранее созданную группу, а затем нажимаем кнопку «Очистить список».

Результат проверки считается положительным, если перечень группы получателей зашифрованного сообщения оказался очищен от всех загруженных получателей.

Тест 6. В диалоге зашифрования открываем ранее созданную группу, отмечаем флажком некоторых пользователей и нажимаем кнопку «Зашифровать». Затем к полученному зашифрованному файлу применяется функция «Информация о файле».

Результат проверки считается положительным, если файл оказывается зашифрованным на сертификаты тех и только тех пользователей, которые указаны в созданной группе и отмечены флажками (плюс рабочий сертификат профиля).

Тест 7. Повторно открываем диалог зашифрования.

Результат проверки считается положительным, если перечень группы получателей оказался в том же состоянии (состав, сортировка, установленные флажки), которое было непосредственно перед предыдущим зашифрованием.

Тест 8. Проверка осуществляется при выполнении тестов 9 и 10 (см. ниже).

Тест 9. В диалоге формирования групп формируем две группы: нажимаем кнопку «Из справочника», а затем (после очистки списка) нажимаем кнопку «Из ЕСК», задаём параметры поиска и нажимаем «ОК».

Результат проверки считается положительным, если в первую группу заносятся все пользователи, чьи сертификаты содержатся в локальном справочнике (и на которые возможно шифрование), а во вторую – пользователи, удовлетворяющие заданным параметрам поиска.

Тест 10. В диалоге формирования групп создаём или открываем любую группу, снимаем флажки со всех пользователей нажимаем кнопку «Поиск», задаём критерии поиска и нажимаем «ОК».

Результат проверки считается положительным, если в списке группы флажками отмечены только те пользователи, которые удовлетворяют заданным параметрам поиска.

Тест 11. В диалоге формирования групп создаём или открываем любую группу.

Результат проверки считается положительным, если группа получателей зашифрованного сообщения представляет собой совокупность записей о получателях, представленную таблицей, включающей в себя следующие графы: «Ф.И.О.», «Организация», «Должность», «Структурное подразделение», «SubjectName»;

Тест 12. В диалоге формирования групп создаём любую группу поиском из ЕСК, отмечаем флажком одного получателя, затем выполняем шифрование. Затем к полученному зашифрованному файлу применяется функция «Информация о файле» и в открывшемся диалоге просматриваем сертификаты, на которые выполнено шифрование (кроме рабочего сертификата профиля).

Результат проверки считается положительным, если значения полей LDAP, записанные в группу, совпадают с соответствующими полями сертификатов, на которые выполнено шифрование.

Тест 13. В диалоге формирования групп создаём любую группу, выделяем часть пользователей флажками, сохраняем группу, очищаем список, открываем эту группу, нажав кнопку «Открыть группу», затем добавляем другую группу, нажав кнопку «Из группы».

Результат проверки считается положительным, если в результате перечень пользователей содержит пользователей первой группы, выделенных флажками и всех пользователей второй группы.

Тест 14. Проверка перечисления 14) п.4.3.19 ТЗ выполнена в рамках теста 13.

Тест 15. Из диалога зашифрования переходим в диалог формирования групп, там поиском в ЕСК выбираем несколько пользователей и, не сохраняя их в группу, нажимаем кнопку «Зашифровать».

Результат проверки считается положительным, если в результате перечень пользователей в диалоге зашифрования содержит тех и только тех пользователей, которые были выбраны в диалоге формирования групп.

5.28 Проверка 27 таблицы 1

Проверка осуществляется путем просмотра системного журнала «Приложение» ОС Windows.

Результат проверки считается положительным, если в системном журнале «Приложение» ОС Windows обнаружены записи (источник SPKISHXX), содержащие результаты выполнения операций и сообщения об ошибках, выдаваемые СКАД «Сигнатура».

5.29 Проверка 28 таблицы 1

Проверка осуществляется путем экспертной оценки предоставленных Заказчику носителей с ПК САЭС.

Результат проверки считается положительным, если ПК САЭС предоставлен Заказчику на оптических носителях, не допускающих перезапись информации.

5.30 Проверка 29 таблицы 1

Проверка осуществляется путем осмотра этикетки оптического носителя с записанным на нем ПК САЭС.

Результат проверки считается положительным, если оптический носитель с ПК САЭС иметь маркировку с обозначением товарного знака компании-разработчика, наименованием ПК и номером сборки.

5.31 Проверка 30 таблицы 1

Оценка комплектности и качества документации выполняется экспертным методом путем анализа документации на соответствие требованиям нормативно-технических документов. Номенклатура разработанных документов определяется ТЗ. Содержание документов проверяется на соответствие требованиям стандартов Единой системы программной документации, оформление – руководящего документа Банка России «Правила определения видов, наименований и обозначений разрабатываемой документации автоматизированных систем, технических и программных средств» (утв. 15.05.2013).

Результат проверки считается положительным, если выполнено требование ТЗ.

5.32 Проверка 31 таблицы 1

Проверка выполняется при проведении приемочных испытаний (при необходимости).

Результат проверки считается положительным, если комиссия путём проверки функционирования ПК САЭС и оценки программной документации установила, что все замечания и рекомендации с целью доработки ПК САЭС по результатам предварительных испытаний согласно Акту приемки в опытную эксплуатацию и по результатам опытной эксплуатации согласно Акту о завершении опытной эксплуатации ПК САЭС устранены и учтены.

6 УСЛОВИЯ ПРОВЕДЕНИЯ ИСПЫТАНИЙ

6.1 Испытания ПК САЭС проводятся на стенде ЦКИБ «Рязань» Отделения Рязань.

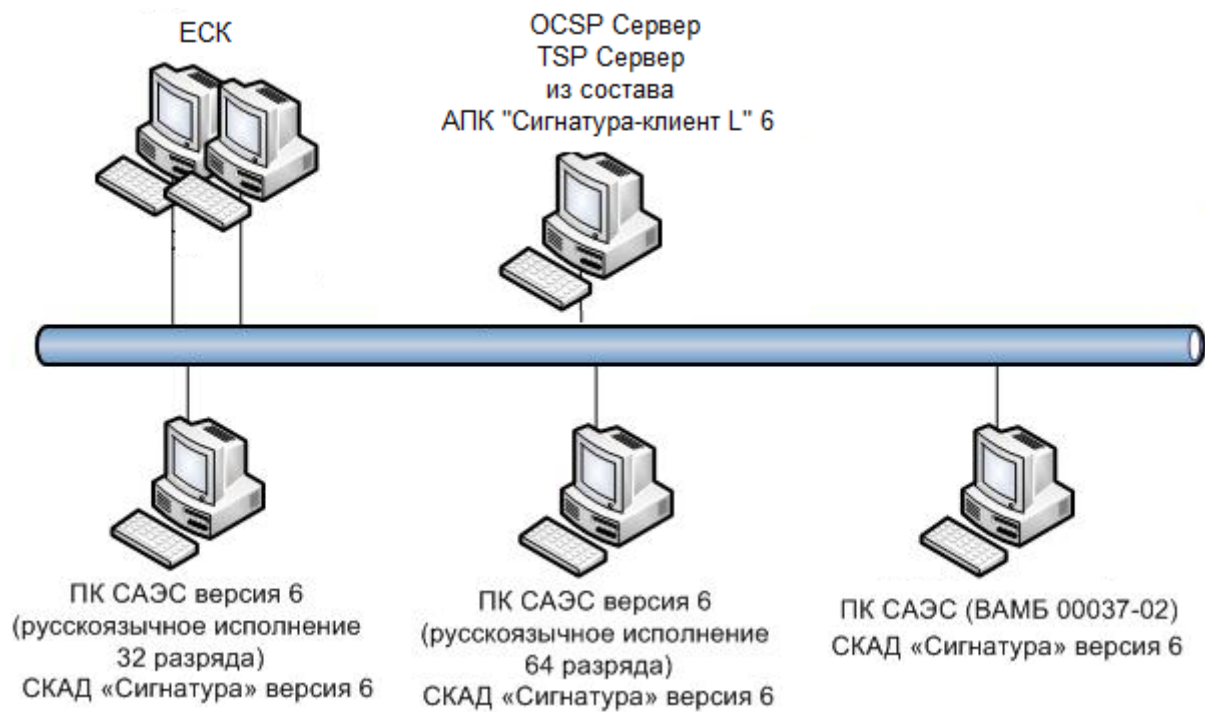
6.2 Испытания проводятся на тестовых данных с использованием тестовых ключевых документов. Схема стенда приведена в приложении А к настоящему документу. Описание стенда необходимо привести в Протоколах испытаний.

7 ОТЧЕТНОСТЬ

7.1 По результатам предварительных испытаний оформляют Протокол предварительных испытаний и Акт приемки ПК САЭС версия 6 в опытную эксплуатацию.

7.2 По результатам приемочных испытаний оформляют Протокол приемочных испытаний и Акт о готовности ПК САЭС версия 6 к эксплуатации.

ПРИЛОЖЕНИЕ А
(справочное)
СХЕМА СТЕНДА



ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АПК	Аппаратно-программный комплекс
АС	Автоматизированная система
ЕСК	Единая служба каталогов Банка России
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
ПП	Программный продукт
САЭС	Специализированный архиватор электронных сообщений
САС	Список аннулированных сертификатов
СКАД	Система криптографической авторизации электронных документов
Средство КЗИ	Средство криптографической защиты информации
ТЗ	Техническое задание
ЭП	Электронная подпись

СОСТАВИЛИ

Наименование организации	Должность	Фамилия, инициалы	Подпись, дата
ООО «Валидата»	Ведущий специалист	Елин А.Л.	
ООО «Валидата»	Ведущий специалист	Садовский М.А.	

СОГЛАСОВАНО

[illegible]

СОГЛАСОВАНО

Наименование организации	Должность	Фамилия, инициалы	Подпись, дата
ЦКИБ «Рязань» Отделения Рязань	заведующий	Рябцев Б.Е.	
ЦКИБ «Рязань» Отделения Рязань	главный инженер	Гора С.Ю.	
ЦКИБ «Рязань» Отделения Рязань	главный инженер	Майоров Г.О.	
ЦКИБ «Рязань» Отделения Рязань	ведущий инженер	Барышев А.В.	