

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УТВЕРЖДЕН
ВАМБ.00108-06-ЛУ

**СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ БАНКА РОССИИ
«ЯНТАРЬ» ВЕРСИЯ 6**

ПРОГРАММА ТЕСТИРОВАНИЯ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ
КРИПТОГРАФИЧЕСКОГО СЕРВЕРА

Руководство пользователя

ВАМБ.00108-06 92 01

Аннотация

Настоящий документ содержит сведения о назначении, условиях использования, порядке работы с программным комплексом (ПК) ВАМБ.00108-06 12 07 «Программа тестирования аппаратно-программных средств криптографического сервера» (далее - ПК «Тест Янтарь») из состава ПК ВАМБ.00108-06 «Система криптографической защиты информации автоматизированных систем Банка России «Янтарь» версия 6» (далее - СКЗИ «Янтарь»).

Документ предназначен для администратора криптографического сервера, отвечающего за его управление и мониторинг.

Содержание

1	НАЗНАЧЕНИЕ И УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ПК «ТЕСТ ЯНТАРЬ»	4
2	РАБОТА С ПК «ТЕСТ ЯНТАРЬ»	6
2.1	Запуск ПК «Тест Янтарь»	6
2.2	Ошибки при запуске службы	6
2.3	Протокол ПК «Тест Янтарь»	8
2.4	Коды завершения операции	9
2.5	Действия при обнаружении неисправности аппаратных средств КС	9
	ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	10

1 НАЗНАЧЕНИЕ И УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ПК «ТЕСТ ЯНТАРЬ»

ПК «Тест Янтарь» предназначен для использования в качестве инструментария, обеспечивающего необходимую полноту и цикличность проверок работоспособности аппаратных средств криптографического сервера ВАМБ.00108-06 12 01 из состава СКЗИ «Янтарь» (далее – криптосервер или КС).

Примечание – Тестирование правильности функционирования аппаратной составляющей остальных компонентов СКЗИ «Янтарь» обеспечивается периодической (с периодом не более 72 часов) перезагрузкой операционной системы (ОС).

ПК «Тест Янтарь» позволяет выполнять тестирование в фоновом и/или циклическом режимах.

ПК «Тест Янтарь» работает под управлением серверных ОС Windows из перечня, приведённого в документе ВАМБ.00107-06 30 01 «СКАД «Сигнатура» версия 6. АПК «Средство КЗИ СКАД «Сигнатура» версия 6». Формуляр».

ПК «Тест Янтарь»:

- обеспечивает тестирование аппаратных компонентов КС без остановки аппаратной платформы КС и без перезагрузки ОС;
- не имеет негативных последствий для функционирования аппаратных и программных компонент КС;
- работает совместно с программным обеспечением КС;
- выполняет проверку правильности работы компонентов аппаратной платформы КС;
- осуществляет выдачу результатов проверки в виде сообщения на консоли ЭВМ КС и/или файла-протокола;
- обеспечивает настройку времени начала тестирования;
- в качестве способа проверки правильности работы аппаратных компонент применяет тестирование с использованием криптографических функций, идентичных функциям, реализованным в КС.

Ниже приведён список файлов, входящих в ПК «Тест Янтарь» и требующих обеспечения контроля целостности:

- **hdtest.exe** — исполняемый модуль, диспетчер ПК «Тест Янтарь»;
- **hdstop.dll** — подключаемая библиотека остановки криптосервера;
- **hdts01.dll** — подключаемая библиотека тестирования оперативной памяти;
- **hdts02.dll** — подключаемая библиотека тестирования жёсткого диска;
- **hdts03.dll** — подключаемая библиотека тестирования процессора;
- **hdts04.dll** — подключаемая библиотека проверки целостности;
- **validata.url** — файл ссылки на сайт разработчика ПК «Тест Янтарь».

Значения хэш-функции для перечисленных файлов рассчитываются с помощью ПК ВАМБ.00107-06 12 02 «Программа контроля целостности» (утилита hashfile.exe) из состава ПК ВАМБ.00107-06 «Средство КЗИ СКАД «Сигнатура»

версия 6» при установке ПК «Тест Янтарь» и сохраняются администратором информационной безопасности как эталон для последующего контроля.

2 РАБОТА С ПК «ТЕСТ ЯНТАРЬ»

2.1 Запуск ПК «Тест Янтарь»

ПК «Тест Янтарь» устанавливается как служба (сервис). Для начала работы теста запустите в программе «Диспетчер программ» ОС Windows службу **CryptoServer hardware test** или, чтобы ПК «Тест Янтарь» запускался при каждой загрузке ОС Windows, измените в свойствах службы **CryptoServer hardware test** (Рисунок 1) тип запуска на «Авто».

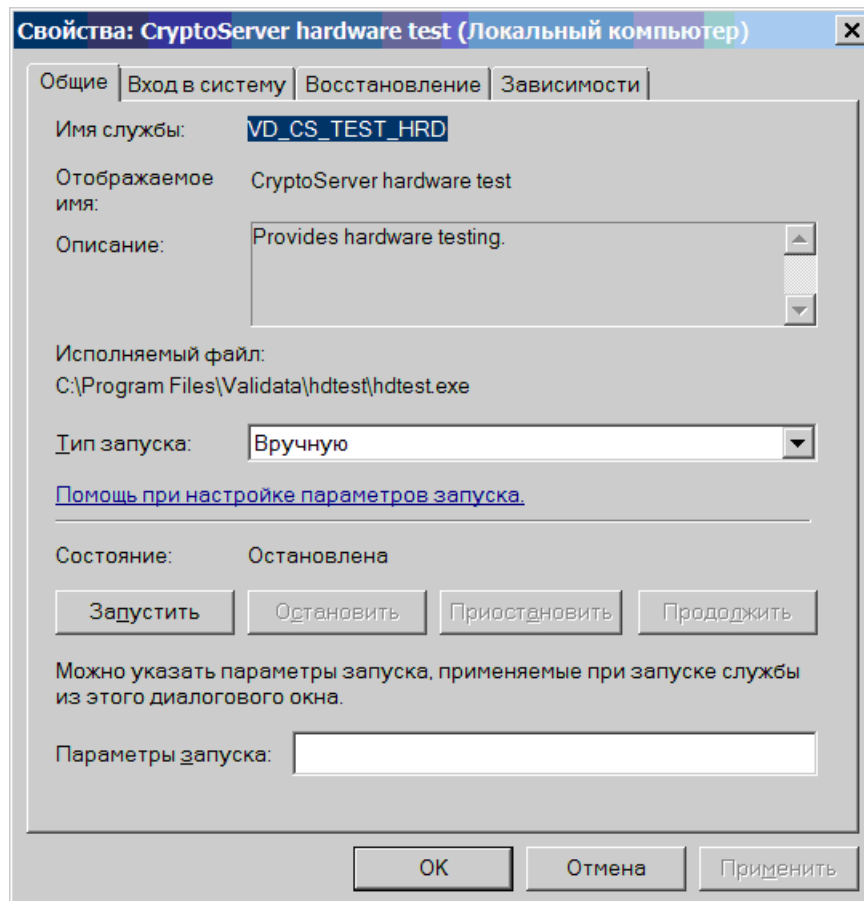


Рисунок 1 – Служба CryptoServer hardware test

Для завершения работы теста остановите в программе «Диспетчер программ» службу **CryptoServer hardware test**.

ПК «Тест Янтарь» можно запустить не как службу, а как консольное приложение. Для этого в каталоге установки выполните команду **hctest.exe -debug**.

Для остановки ПК «Тест Янтарь», запущенного как консольное приложение, нажмите клавишу «Q».

2.2 Ошибки при запуске службы

Если в процессе запуска ПК «Тест Янтарь» (в качестве службы) произошла ошибка, на экран будет выдано сообщение (Рисунок 2).

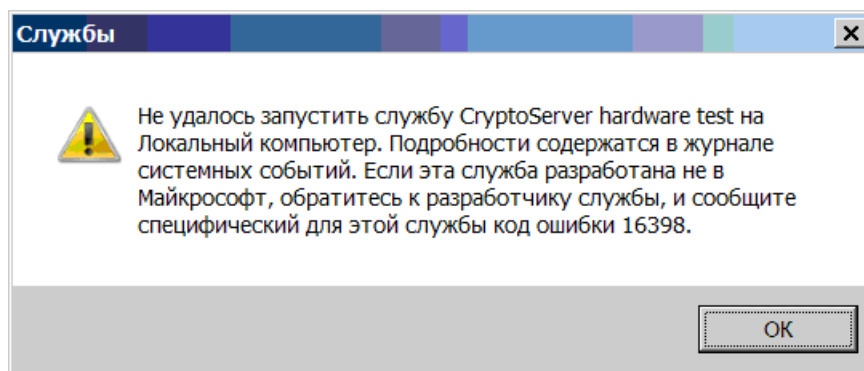


Рисунок 2 – Сообщение об ошибке при запуске ПК «Тест Янтарь»

Подробнее описание ошибки можно посмотреть в системном протоколе ошибок (Рисунок 3).

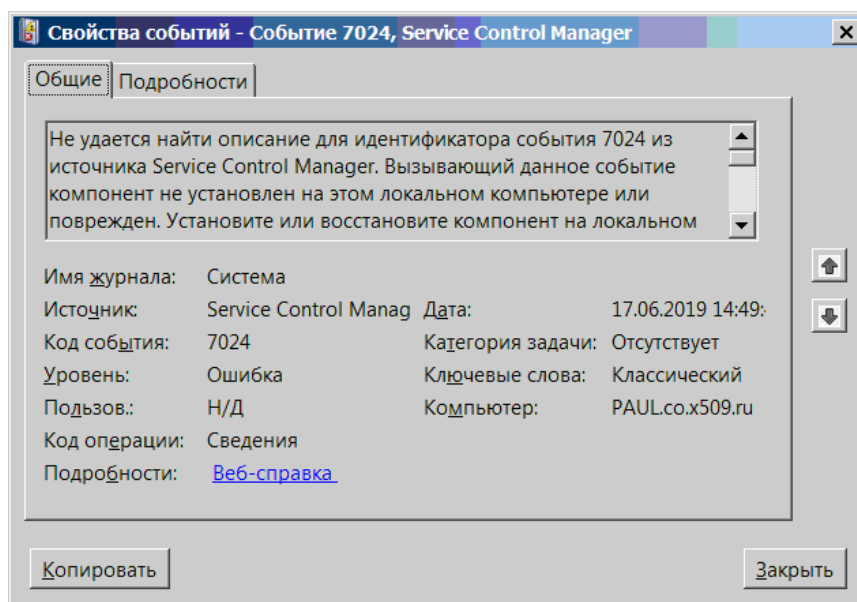


Рисунок 3 – Описание ошибки при запуске ПК «Тест Янтарь»

При запуске и в процессе работы ПК «Тест Янтарь» могут возвращаться приведенные ниже ошибки (Таблица 1).

Таблица 1 – Ошибки в работе ПК «Тест Янтарь»

Десятичный код	Шестнадцатичный код	Описание ошибки
16385	0x4001	Нехватка оперативной памяти
16386	0x4002	Ошибка открытия файла
16387	0x4003	Ошибка определения размера файла
16388	0x4004	Ошибка чтения файла
16389	0x4005	Ошибка записи файла
16390	0x4006	Отсутствуют конфигурационные данные
16391	0x4007	В разделе конфигурационного файла не указано имя

Десятичный код	Шестнадцатичный код	Описание ошибки
16392	0x4008	Ошибочные данные конфигурационного файла
16393	0x4009	В конфигурационном файле задан параметр, который не принадлежит ни одному разделу
16394	0x400A	Не задано имя конфигурационного параметра
16395	0x400B	Не задано значение конфигурационного параметра
16396	0x400C	В конфигурационном файле не задан параметр NumTest в разделе Common
16397	0x400D	В конфигурационном файле не задан параметр LogDir в разделе Common
16398	0x400E	Ошибка подключения тестовой библиотеки
16399	0x400F	Ошибка получения имени функции в подключенной библиотеке
16400	0x4010	Ошибка системной функции в тестовом модуле
16401	0x4011	Ошибка функции тестирования компьютерного оборудования
16402	0x4012	Ошибка добавления записи в файл протокола
16403	0x4013	Ошибка подключения библиотеки остановки криптосервера
16404	0x4014	Ошибка получения имени функции остановки КС в подключенной библиотеке
16405	0x4015	Команда управления криптосервером не выполнена
16406	0x4016	Криптосервер заблокирован
16407	0x4017	Криптосервер остановлен
16408	0x4018	Режим работы криптосервера изменен
16409	0x4019	Ошибка чтения переменной среды

2.3 Протокол ПК «Тест Янтарь»

Протоколы ПК «Тест Янтарь» по формату совместимы с протоколами криптосервера. Разделителем полей является запятая, а поля имеют следующие значения:

- а) дата/время события в формате DD/MM/YYYY HH:MM:SS;
- б) имя криптосервера, заполняется на основании параметра **ComputerName** конфигурационного файла;
- в) не используется, заполняется нулями;
- г) не используется, заполняется нулями;
- д) источник события: 0 — диспетчер ПК «Тест Янтарь», >0 — номер подключаемого теста;
- е) уровень серьезности ошибки:
 - 20 — критическая (требует остановки криптосервера);
 - 30 — ошибка системной функции;
 - 60 — информация (об успешном тестировании);
- ж) не используется, заполняется нулями;
- и) код завершения операции (см. подраздел 2.4);
- к) не используется;

- л) не используется;
- м) текстовое описание.

Протоколы ПК «Тест Янтарь» могут просматриваться различными Windows-приложениями, например, Notepad или MS Excel, но для серьёзного анализа протоколов рекомендуется использовать ПК ВАМБ.00108-06 12 03 «Автоматизированное рабочее место формирования отчётов» (далее — АРМ ФО) из состава СКЗИ «Янтарь», использующийся также для анализа протоколов криптосервера.

2.4 Коды завершения операции

Ниже (Таблица 2) приведены коды завершения операций ПК «Тест Янтарь».

Таблица 2 – Коды завершения операций

Код завершения	Описание
0	Операция завершена успешно
0xEDDD0001	Нехватка оперативной памяти
0xEDDD0002	Сбой памяти
0xEDDD0003	Ошибка открытия файла
0xEDDD0004	Ошибка определения размера файла
0xEDDD0005	Ошибка чтения файла
0xEDDD0006	Ошибка записи файла
0xEDDD0007	Ошибка создания потока
0xEDDD0008	Ошибка тестирования криптографических алгоритмов по ГОСТ 28147-89
0xEDDD0009	Ошибка тестирования криптографических алгоритмов по ГОСТ Р 34.12-2015/34.13-2015 (Кузнечик)
0xEDDD000A	Ошибка тестирования криптографических алгоритмов по ГОСТ Р 34.11-94
0xEDDD000B	Ошибка тестирования криптографических алгоритмов по ГОСТ Р 34.12-2015/34.13-2015 (Магма)
0xEDDD000C	Ошибка тестирования криптографических алгоритмов по ГОСТ Р 34.11-2012 (256/512 бит)
0xEDDD000D	Ошибка тестирования криптографических алгоритмов по ГОСТ Р 34.10-2012 (256 бит)
0xEDDD000E	Ошибка тестирования криптографических алгоритмов по ГОСТ Р 34.10-2012 (512 бит)
0xEDDD0018	Ошибка при хэшировании файла
0xEDDD0019	Ошибка в файле со списком для контроля целостности
0xEDDD001A	Хэш-значение файла не совпадает с заранее вычисленным
0xEDDD001B	Размер файла не совпадает с заранее вычисленным
0xEDDD001C	Файл из списка для контроля целостности не найден
0xEDDD03E9	Некорректная команда управления криптосервером
0xEDDD03EA	Ошибка открытия менеджера служб
0xEDDD03EB	Ошибка открытия службы криптосервера
0xEDDD03EC	Ошибка остановки службы криптосервера
0xEDDD03ED	Служба криптосервера не запущена

2.5 Действия при обнаружении неисправности аппаратных средств КС

В случае обнаружения неисправности аппаратных средств КС ПК «Тест Янтарь» действует в соответствии с настройками конфигурационного файла. Если параметру **StopFunc** установлено значение 1, ПК «Тест Янтарь» попытается

остановить КС. Если параметру **ShowMessage** установлено значение 1, на экран будет выдано диалоговое окно (Рисунок 4).

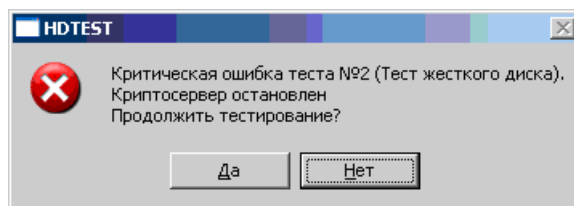


Рисунок 4 – Диалог, сообщающий об остановке КС

Если оператор нажмёт кнопку «Нет» (рекомендуется), работа ПК «Тест Янтарь» будет остановлена, если кнопку «Да» – продолжена. В случае, если криптосервер остановить не удалось, на экран будет выдано диалоговое окно (Рисунок 5).

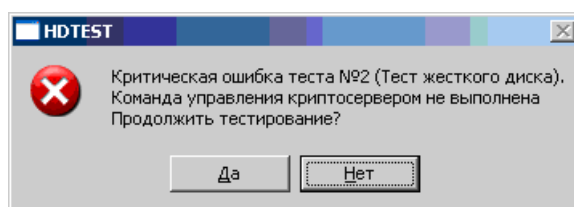


Рисунок 5 – Диалог, сообщающий о невозможности остановить КС

Более полную информацию о возникшей проблеме можно получить из протокола ПК «Тест Янтарь».

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ ФО	Автоматизированное рабочее место формирования отчё- тов
КС	Криптографический сервер
ОС	Операционная система
ПК	Программный комплекс

[illegible]