ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ТСС»

УТВЕРЖДЕН

4012-006-61649217-18 01 95 ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

«Dcrypt 1.0 v.2»

ПРАВИЛА ПОЛЬЗОВАНИЯ

4012-006-61649217-18 01 95

Листов 68

Подпись и дата | Инв. № дубл. | Взам. инв. № | Подпись и дата | Инв. № подл.

Москва

2018

Оглавление

1 ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ДАННЫЕ И ХАРАКТЕРИСТИКИ СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «Dcrypt 1.0 v.2»

Средство криптографической защиты информации «Dcrypt 1.0 v.2» (далее – СКЗИ «Dcrypt 1.0 v.2», изделие) соответствует требованиям, содержащимся в государственных стандартах и документах ФСБ России: «Требования к средствам криптографической защиты, предназначенные для защиты информации, не содержащих сведений, составляющих государственную тайну», «Специальные требования к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации», к шифровальным (криптографическим) средствам защиты информации класса КС1 для исполнений 1, 4, 16, 19, 31 и 34, класса КС2 для исполнений 2, 5, 17, 20, 32, 35, класса КС3 для исполнений 3, 6, 18, 21, 33, 36 и дополнительно требованиям «Требования к средствам электронной подписи», к шифровальным (криптографическим) средствам защиты информации класса КС1 для исполнения 1, 4, 31 и 34, класса КС2 для исполнений 2, 5, 32 и 35, класса КС3 для исполнения 3, 6, 33 и 36.

Безопасность информации обеспечивается при выполнении требований формуляра 4012-006-61649217-18 01 30 и сохранении в тайне ключей шифрования и закрытых ключей электронной подписи.

СКЗИ «Dcrypt 1.0 v.2» может использоваться для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну, посредством выполнения следующих целевых функций:

- создание и управление ключевой информацией (СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5 и 6);
- шифрование файлов и данных, содержащихся в областях оперативной памяти (СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5, 6, 16, 17, 18, 19, 20, 21, 31, 32, 33, 34, 35 и 36);
- вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти (СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5, 6, 16, 17, 18, 19, 20, 21, 31, 32, 33, 34, 35 и 36);
- вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти (СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5, 6, 16, 17, 18, 19, 20, 21, 31, 32, 33, 34, 35 и 36);

- реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи (СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5 и 6);
- реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи (СКЗИ «Dcrypt 1.0 v.2» исп. 31, 32, 33, 34, 35 и 36);
- Защита каналов связи посредством протокола защищенного обмена по сети по схеме DTLS 1.2 (СКЗИ «Dcrypt 1.0 v.2» исп. 16, 17, 18, 19, 20 и 21).

При использовании СКЗИ «Dcrypt 1.0 v.2» в программных продуктах необходимо следовать требованиям эксплуатационной документации, входящей в состав комплекта поставки СКЗИ «Dcrypt 1.0 v.2» согласно формуляру 4012-006-61649217-18 01 30.

1.1 Операционные системы

СКЗИ «Dcrypt 1.0 v.2» предназначено для использования в среде следующих операционных систем (далее – ОС):

- MS Windows (Vista / 2008 / 2012 / 7 / 8 / 10) – для СКЗИ «Dcrypt 1.0 v.2» для исполнений 1, 2, 3, 16, 17, 18, 31, 32 и 33;
- Linux (ядра 2.6.x / 3.x / 4.x) – для СКЗИ «Dcrypt 1.0 v.2» для исполнений 4, 5, 6, 19, 20, 21, 34, 35 и 36.

1.2 Реализуемые функции

СКЗИ «Dcrypt 1.0 v.2» реализует следующие функции:

- зашифрование и расшифрование в соответствии с алгоритмом ГОСТ 28147-89 для блоков данных и файлов в режиме гаммирования с обратной связью (СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5, 6, 16, 17, 18, 19, 20, 21, 31, 32, 33, 34, 35 и 36), при этом СКЗИ «Dcrypt 1.0 v.2», исп. 19, 20 и 21 обеспечивает гарантированную скорость шифрования на программно-аппаратных платформах согласно требованиям, приведенным в формуляре 4012-006-61649217-18 01 30;
- выработка имитовставки в соответствии с алгоритмом ГОСТ 28147-89 для блоков данных и файлов (СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5, 6, 16, 17, 18, 19, 20, 21, 31, 32, 33, 34, 35 и 36);
- вычисление хэш-функции в соответствии с ГОСТ Р 34.11-2012 для блоков данных и файлов (СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5, 6, 16, 17, 18, 19, 20, 21, 31, 32, 33, 34, 35 и 36);

- выработка и проверка электронной подписи в соответствии с алгоритмом, приведённым в ГОСТ Р 34.10-2012 для блоков данных и файлов (СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5, 6, 31, 32, 33, 34, 35 и 36);
- генерация псевдослучайных последовательностей (СКЗИ «Dcrypt 1.0 v.2» исп. 31, 32, 33, 34, 35 и 36);
- генерация ключевой информации (СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5 и 6);
- выработка общего секретного значения (открытого распределения ключей) на базе математических соглашений согласно ГОСТ Р 34.10-2012 и по алгоритму Диффи-Хеллмана (RFC4357) (СКЗИ «Dcrypt 1.0 v.2» исп. 31, 32, 33, 34, 35 и 36);
- Защита каналов связи посредством протокола защищенного обмена по сети по схеме DTLS 1.2 в соответствии с ГОСТ 28147-89, ГОСТ Р 34.11-2012 (СКЗИ «Dcrypt 1.0 v.2» исп. 16, 17, 18, 19, 20 и 21).

1.3 Условные обозначения

КриптоАРМ - условное обозначение СКЗИ «Dcrypt 1.0 v.2» для исполнений 1, 2, 3, 4, 5 и 6. КриптоАРМ устанавливается на СВТ и выполняет функции, определенные в разделе 2 формуляра 4012-006-61649217-18 01 30. СКЗИ «Dcrypt 1.0 v.2» для исполнений 2, 3, 5 и 6 является центром генерации и распределения ключей с использованием аппаратно-программного модуля доверенной загрузки. СКЗИ «Dcrypt 1.0 v.2» для исполнений 1 и 4 является центром генерации и распределения ключей с учетом инициализации ПДСЧ из файла со случайной последовательностью, заранее сгенерированной аппаратно-программным модулем доверенной загрузки. Перечень поставляемых аппаратно-программных модулей доверенной загрузки приведен в таблице 4 «Состав комплекта поставки СКЗИ «Dcrypt 1.0 v.2» раздела 4 «Комплектность» документа «Средство криптографической защиты информации «Dcrypt 1.0 v.2». Формуляр. 4012-006-61649217-18 01 30».

КриптоАРМ обеспечивает выполнение следующих целевых функций:

- создание и управление ключевой информацией;
- шифрование файлов и данных, содержащихся в областях оперативной памяти;
- вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти;
- вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти;
- реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи,

проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи.

АП VPN – условное обозначение СКЗИ «Dcrypt 1.0 v.2» для исполнений 16, 17, 18, 19, 20 и 21. АП VPN устанавливается на СВТ и выполняет функции, определенные в разделе 2 формуляра 4012-006-61649217-18 01 30, обеспечивая защиту TLS-соединений, в соответствии с ГОСТ 28147-89, ГОСТ Р 34.11-2012.

АП VPN обеспечивает выполнение следующей целевой функции:

- защита каналов связи посредством протокола защищенного обмена по сети по схеме DTLS 1.2 и может использоваться для криптографической защиты (шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти) информации, не содержащей сведений, составляющих государственную тайну.

Библиотеки – условное обозначение СКЗИ «Dcrypt 1.0 v.2» для исполнений 31, 32, 33, 34, 35 и 36.

Библиотеки обеспечивают выполнение следующих целевых функций:

- шифрование файлов и данных, содержащихся в областях оперативной памяти;
- вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти;
- вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти;
- реализация функций электронной подписи в соответствии с федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи.

1.4 Требования к СВТ

Требования к конфигурации СВТ на котором функционирует СКЗИ «Dcrypt 1.0 v.2» для исполнений 1, 2, 3, 4, 5, 6, 16, 17, 18, 19, 20, 21, 31, 32, 33, 34, 35 и 36 при использовании на архитектуре Intel IA-32 отображены в таблице 1. Требования к конфигурации СВТ на котором функционирует СКЗИ «Dcrypt 1.0 v.2» для исполнений 1, 2, 3, 4, 5, 6, 16, 17, 18, 19, 20, 21, 31, 32, 33, 34, 35 и 36 при использовании на архитектуре EM64T, оснащенном процессором, совместимым с набором команд EM64T, отображены в таблице 2.

Таблица 1 – Требования к конфигурации СВТ при использовании архитектуры Intel IA-32

Элемент	**Требования**
Процессор	Не ниже семейства Pentium (i586)
Оперативная память	Не меньше 1 ГБ
Жесткий диск (свободное пространство)	Не меньше 1 ГБ
Операционная система	MS Windows (Vista / 2008 / 2012 / 7 / 8 / 10) для исполнений 1, 2, 3, 16, 17, 18, 31, 32 и 33. Linux (ядра 2.6.x / 3.x / 4.x) для 4, 5, 6, 19, 20, 21, 34, 35 и 36.

Таблица 2 – Требования к конфигурации СВТ при использовании архитектуры EM64T

Элемент	**Требования**
Процессор	Совместимый с набором команд EM64T
Оперативная память	Не меньше 1 ГБ
Жесткий диск (свободное пространство)	Не меньше 1 ГБ
Операционная система	MS Windows (Vista / 2008 / 2012 / 7 / 8 / 10) для исполнений 1, 2, 3, 16, 17, 18, 31, 32 и 33. Linux (ядра 2.6.x / 3.x / 4.x) для исполнений 4, 5, 6, 19, 20, 21, 34, 35 и 36.

2 СРЕДА ФУНКЦИОНИРОВАНИЯ СКЗИ «Dcrypt 1.0 v.2»

Средой функционирования СКЗИ «Dcrypt 1.0 v.2» для исполнений 1, 2, 3, 16, 17, 18, 31, 32 и 33 являются ОС MS Windows (Vista / 2008 / 2012 / 7 / 8 / 10).

Средой функционирования СКЗИ «Dcrypt 1.0 v.2» для исполнений 4, 5, 6, 19, 20, 21, 34, 35 и 36 являются ОС Linux (ядра 2.6.x / 3.x / 4.x).

Первоначальная инсталляция СКЗИ «Dcrypt 1.0 v.2» в среде его функционирования осуществляется посредством использования исполняемого файла «install_dcrypt».

3 ОПЕРАЦИИ, ВЫПОЛНЯЕМЫЕ АДМИНИСТРАТОРОМ БЕЗОПАСНОСТИ

3.1 Обеспечение контроля целостности

Для обеспечения контроля целостности программных модулей (файлов) СКЗИ «Dcrypt 1.0 v.2» и ОС администратору безопасности необходимо поставить на контроль целостности программные модули (файлы), приведенные в таблице 3.

Таблица 3 – Перечень программных модулей (файлов)

Исполнение СКЗИ «Dcrypt 1.0 v.2»	Архитектура процессора	Программные модули (файлы) СКЗИ «Dcrypt 1.0 v.2»	Программные модули (файлы) ОС
СКЗИ «Dcrypt 1.0 v.2», исп. 1	Intel IA-32	«DcryptLogSvc.exe», «DmCrypt.dll», «Ddmcrypt-util.exe».	Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования.
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 2	Intel IA-32	«DcryptLogSvc.exe», «DmCrypt.dll», «Ddmcrypt-util.exe».	Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования.
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 3	Intel IA-32	«DcryptLogSvc.exe», «DmCrypt.dll», «Ddmcrypt-util.exe», «DmCSEDI.dll», «DmCSE.inf», «DmCSEManager.exe», «DmCSEService.exe», «DmCSE.sys».	Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования.
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 4	Intel IA-32	«dcryptlogsvc», «dmcrypt-util», «libdmcrypt.so.1».	Ядро ОС Linux и начальный загрузочный образ[1].
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 5	Intel IA-32	«dcryptlogsvc», «dmcrypt-util», «libdmcrypt.so.1».	Ядро ОС Linux и начальный загрузочный образ[1].
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 6	Intel IA-32	«dcryptlogsvc», «dmcrypt-util», «dmiced», «libdmcrypt.so.1», «tss_sys_hook.ko».	Ядро ОС Linux и начальный загрузочный образ[1].
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 16	Intel IA-32	«DiamondVpn.exe», «DmCrypt.dl»l.	Программные модули (файлы) ОС, приведенные в приложении
	EM64T		

[1] Администратор безопасности в зависимости от конкретной сборки дистрибутива ОС Linux обязан определить системные модули ОС (ядро ОС Linux и начальный загрузочный образ), которые необходимо поставить на контроль целостности.

			«Приложение 2» настоящих правил пользования.
СКЗИ «Dcrypt 1.0 v.2», исп. 17	Intel IA-32	«DiamondVpn.exe», «DmCrypt.dll».	Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования.
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 18	Intel IA-32	«DiamondVpn.exe», «DmCrypt.dll», «DmCSEDI.dll», «DmCSE.inf», «DmCSEManager.exe», «DmCSEService.exe», «DmCSE.sys».	Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования.
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 19	Intel IA-32	« DcryptLogSvc.exe », «dmvpnd.ddl», «libdmcrypt.so.1», «libdmvpn.so.1».	Ядро ОС Linux и начальный загрузочный образ[1].
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 20	Intel IA-32	« DcryptLogSvc.exe », «dmvpnd.ddl», «libdmcrypt.so.1», «libdmvpn.so.1».	Ядро ОС Linux и начальный загрузочный образ[1].
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 21	Intel IA-32	«dcryptlogsvc», «dmiced», «dmvpnd», «libdmcrypt.so.1», «libdmvpn.so.1», «tss_sys_hook.ko».	Ядро ОС Linux и начальный загрузочный образ[1].
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 31	Intel IA-32	«DmCrypt.dll».	Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования.
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 32	Intel IA-32	«DmCrypt.dll», «Dmvpn.dll».	Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования.
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 33	Intel IA-32	«DmCrypt.dll», «DmCSEDI.dll», «DmCSE.inf», «DmCSEManager.exe», «DmCSEService.exe», «DmCSE.sys».	Программные модули (файлы) ОС, приведенные в приложении «Приложение 2» настоящих правил пользования.
	EM64T		
СКЗИ «Dcrypt 1.0 v.2», исп. 34	Intel IA-32	«libdmcrypt.so.1».	Ядро ОС Linux и начальный загрузочный образ[1].
	EM64T		

СКЗИ «Dcrypt 1.0 v.2», исп. 35	Intel IA-32 EM64T	«libdmcrypt.so.1», «libdmvpn.so.1».	Ядро ОС Linux и начальный загрузочный образ[1].
СКЗИ «Dcrypt 1.0 v.2», исп. 36	Intel IA-32 EM64T	«dmiced», «libdmcrypt.so.1», «tss_sys_hook.ko».	Ядро ОС Linux и начальный загрузочный образ[1].

3.1.1 Обеспечение контроля целостности программного обеспечения (для СКЗИ «Dcrypt 1.0 v.2» исп. 1, 4, 16, 19, 31 и 34)

Утилита «dmcrypt-ic» предназначена для контроля целостности программных модулей (файлов) СКЗИ «Dcrypt 1.0 v.2», а также программных модулей (файлов) ОС и исполняется после загрузки самой ОС. Для обеспечения возможности контроля целостности программных модулей (файлов), указанных в таблице 3 для каждого исполнения СКЗИ «Dcrypt 1.0 v.2», запуск программы «dmcrypt-ic» должен осуществляться с аргументами командной строки.

Для вычисления контрольных сумм вначале создается файл, в котором перечислены пути ко всем контролируемым файлам (например, «list.txt», в котором каждая новая строка является новым путем к контролируемому файлу), а затем вызывается утилита «dmcrypt-ic» посредством команды: «dmcrypt-ic --calc-ic /path/to/list.txt /path/to/ic.txt».

Утилита для каждого указанного файла посчитает контрольную сумму и запишет их в файл «ic.txt».

Вызов утилиты для проверки контрольных сумм осуществляется следующим образом: «dmcrypt-ic --check-ic /path/to/ic.txt».

Кроме того, утилита выведет сообщение, был ли пройден контроль целостности.

3.1.2 Обеспечение контроля целостности программного обеспечения (для СКЗИ «Dcrypt 1.0 v.2» исп. 2, 3, 5, 6, 17, 18, 20, 21, 32, 33, 35 и 36)

Контроль целостности программных модулей (файлов) СКЗИ «Dcrypt 1.0 v.2», а также программных модулей (файлов) ОС, указанных в таблице 3 для каждого исполнения СКЗИ «Dcrypt 1.0 v.2», согласно формуляру 4012-006-61649217-18 01 30 обеспечивается аппаратно-программным модулем доверенной загрузки (далее – АПМДЗ), сертифицированным по требованиям ФСБ России к АПМДЗ. Контроль целостности программных модулей (файлов) СКЗИ «Dcrypt 1.0 v.2», а также программных модулей (файлов) ОС для СКЗИ «Dcrypt 1.0 v.2» исп. 2, 3, 5, 6, 17, 18, 20, 21, 32, 33, 35 и 36 осуществляется АПМДЗ до загрузки ОС.

Для СКЗИ «Dcrypt 1.0 v.2» исп. 6, 21 и 36 дополнительно к программным модулям (файлам), приведенным в таблице 3, администратор безопасности до старта ОС должен настроить АПМДЗ на контроль целостности следующих файлов:

- файл с секретным ключом «secret.key»;
- файл со списком разрешенных файлов и их контрольными суммами «macs.txt».

Если в результате контроля целостности при загрузке ОС появляется сообщения о нарушении целостности контролируемого файла, то пользователь обязан прекратить работу и обратиться к администратору безопасности.

Администратор безопасности, проанализировав причину, приведшую к нарушению целостности, должен переустановить ПО СКЗИ «Dcrypt 1.0 v.2», либо файлы операционной среды.

Для СКЗИ «Dcrypt 1.0 v.2» исп. 3, 18 и 33 дополнительно к программным модулям (файлам), приведенным в таблице 3, администратор безопасности должен настроить АПМДЗ на контроль целостности следующих значений системного реестра MS Windows до старта ОС:

- значение реестра MS Windows:

  KLM\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\ProcessingMode;
- значение реестра MS Windows:

  HKLM\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\DmCryptKey;
- все значения ключа MS Windows (рекурсивно со всеми подключами):

  HKLM\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\ProtectedList;
- все значения ключа MS Windows (рекурсивно со всеми подключами):

  HKLM\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\WhiteList.

3.2 Обеспечение динамического контроля целостности программного обеспечения посредством ЗПС (для СКЗИ «Dcrypt 1.0 v.2» исп. 3, 6, 18, 21, 33 и 36)

Динамический контроль целостности программных модулей замкнутой программной среды (далее – ЗПС) осуществляется средствами самой ЗПС согласно подразделу 3.4 «Описание и настройка замкнутой программной среды СКЗИ «Dcrypt 1.0 v.2» для исполнений 6, 21 и 36» и подразделу 3.5 «Описание и настройка замкнутой программной среды СКЗИ «Dcrypt 1.0 v.2» для исполнений 3, 18 и 33».

Администратор безопасности должен сформировать ЗПС в соответствии с требованиями настоящего документа, изложенными в подразделе 3.5 «Описание и

настройка замкнутой программной среды СКЗИ «Dcrypt 1.0 v.2» для исполнений 3, 18 и 33».

3.2.1 Обеспечение динамического контроля целостности программного обеспечения СКЗИ «Dcrypt 1.0 v.2» исп. 3, 18 и 33

В целях обеспечения ЗПС для СКЗИ «Dcrypt 1.0 v.2» для исполнений 3, 18 и 33 используются совместно средства доверенной загрузки и программные модули «DmCSE.sys» и «DmCSEManager.exe», «DmCSEDI.dll», «DmCSE.inf», «DmCSEService.exe».

На этапе настройки механизма ЗПС составляются два списка исполняемых файлов: «White List» и «Protected List».

«White List» может быть сформирован как автоматически (в режиме обучения), так и вручную. «Protected List» может быть сформирован исключительно вручную.

При этом для файлов из этих списков рассчитываются эталонные контрольные суммы для их последующего контроля.

На этапе применения настроек ЗПС выполняет контроль целостности (далее - КЦ) файлов, входящих в списки «White List» и «Protected List».

КЦ файлов осуществляется с момента перехода ЗПС в режим применения настроек «-enforce_start» до выхода из этого режима «-enforce_stop».

При выполнении команды «-enforce_start» производится верификация контрольных сумм файлов, входящих в списки «White List» и «Protected List», а затем, до выполнения команды «-enforce_stop», производится отслеживание изменений (модификации, переименования, удаления) этих файлов (т.е. выполняется динамический контроль целостности).

Несовпадение контрольной суммы файла при верификации или последующее изменение файла трактуется ЗПС как нарушение КЦ.

До тех пор, пока нарушений контроля целостности не выявлено, ЗПС допускает выполнение произвольного файла только в том случае, если он входит в список «White List» или в список «Protected List».

С момента обнаружения нарушения КЦ, ЗПС:

- Запрещает доступ к файловой системе всем пользователям, кроме следующих*:
    - SID: S-1-5-21domain-500 //Name: Administrator Description: A user account for the system administrator. By default, it is the only user account that is given full control over the system;

- SID: S-1-5-18 //Name: Local System Description: A service account that is used by the operating system;
- SID: S-1-5-19 //Name: NT Authority Description: Local Service;
- SID: S-1-5-20 //Name: NT Authority Description: Network Service;
- SID: S-1-5-90-X //Windows 8; UserName: Window Manager\DWM-1;
- SID: S-1-5-83-X //Windows 8 and Windows Server 2012; NT VIRTUAL MACHINE\XXX-XXX-XXX-XXX-XXX.

- Запрещает всем пользователям запуск файлов, входящих в список «Protected List»;
- В режиме обучения и применения настроек запрещается доступ к файлам, расположенным в сетевых папках.

** В частности, это означает что запрещенные пользователи не смогут зарегистрироваться в ОС. (Для получения дополнительной информации: https://support.microsoft.com/en-us/help/243330/well-known-security-identifiers-in-windows-operating-systems).*

3.3 Обеспечение разграничения прав доступа пользователей

Администратор безопасности, обязан распределить права доступа пользователей к конфигурационным параметрам, журналу событий ЗПС (в соответствии с пунктом 3.5.2 «Установка ЗПС» настоящего документа) и программным модулям (файлам) СКЗИ «Dcrypt 1.0 v.2», приведенным в третьем столбце таблицы 3, при помощи средств ОС или сертифицированных ФСБ России средств защиты от НСД, при условии оценки влияния СКЗИ «Dcrypt 1.0 v.2» на данные средства защиты от НСД по техническому заданию, согласованному с 8 Центром ФСБ России.

Администратор безопасности может распределять права доступа пользователей в соответствии с принятой в организации политикой разграничения прав доступа при помощи средств ОС или сертифицированных ФСБ России средств защиты от НСД, при условии оценки влияния СКЗИ «Dcrypt 1.0 v.2» на данные средства защиты от НСД по техническому заданию, согласованному с 8 Центром ФСБ России.

3.4 Описание и настройка замкнутой программной среды СКЗИ «Dcrypt 1.0 v.2» для исполнений 6, 21 и 36

Для обеспечения ЗПС в СКЗИ «Dcrypt 1.0 v.2» для вариантов исполнения 6, 21 и 36, сертифицированных по классам КС3, должны совместно использоваться средства доверенной загрузки и программные модули СКЗИ «Dcrypt 1.0 v.2» «dmiced» и «tss_sys_hook.ko».

3.4.1 Описание модуля ЗПС

Модуль ЗПС создает замкнутую среду на основе 2 списков файлов:

- «белый» список: в нем указаны файлы, которые разрешены для запуска. Все остальные программы в среде функционирования будут запрещены для запуска;
- «защищенный» список: в нем указаны файлы, которые также разрешены для запуска, но в случае нарушения целостности или НСД эти файлы будут заблокированы для запуска. «Защищенный» список предназначен для внесения в него файлов СКЗИ «Dcrypt 1.0 v.2».

В «защищенном» списке для каждого внесенного файла хранится контрольная сумма, вычисленная по алгоритму ГОСТ 28147-89 в режиме имитовставки. Ключ алгоритма берется из файла, указанного через параметр «--key».

Оба списка («белый» и «защищенный») можно наполнять вручную. Например, для внесения файла «/usr/local/sbin/dmvpnd» в «белый» список необходимо выполнить следующую команду:

«dmiced --mode addp --key ~/secret.key --white ~/whitelist.txt --protected ~/protectedlist.txt /usr/local/sbin/dmvpnd --log ~/kc3.log».

Аналогично, для внесения файла «/bin/bash» в «белый» список необходимо выполнить следующую команду:

«dmiced --mode addw --key ~/secret.key --white ~/whitelist.txt --protected ~/protectedlist.txt /bin/bash --log ~/kc3.log».

Для формирования «белого» списка в автоматическом режиме модуль ЗПС имеет режим обучения. Для этого необходимо выполнить команду:

«dmiced --mode learn --key ~/secret.key --white ~/whitelist.txt --protected ~/protectedlist.txt --log ~/kc3.log».

В этом режиме модуль ЗПС отслеживает все запускаемые на исполнение файлы, автоматически вычисляя для них контрольные суммы и добавляя в «белый» список.

3.4.2 Настройка модуля ЗПС

Настройкой модуля ЗПС должен заниматься привилегированный пользователь (администратор безопасности) среды функционирования. Вначале необходимо запретить чтение и модификацию файлов с ключевой информацией, списками и журналом для всех пользователей среды функционирования. Для этого привилегированный пользователь должен выполнить следующие команды:

«chmod 600 secret.key

chmod 600 whitelist.txt

chmod 600 protectedlist.txt

chmod 600 kc3.log».

Затем привилегированный пользователь переводит модуль ЗПС в режим обучения следующей командой:

«dmiced --mode learn --key secret.key --white whitelist.txt --protected protectedlist.txt --log kc3.log».

После этого необходимо произвести обычную работу в среде функционирования (авторизоваться, открыть файл, закрыть файл и т.д.) для того, чтобы модуль ЗПС смог составить «белый» список разрешенных программ.

Модуль ЗПС в режиме обучения приведен на рисунке 1.

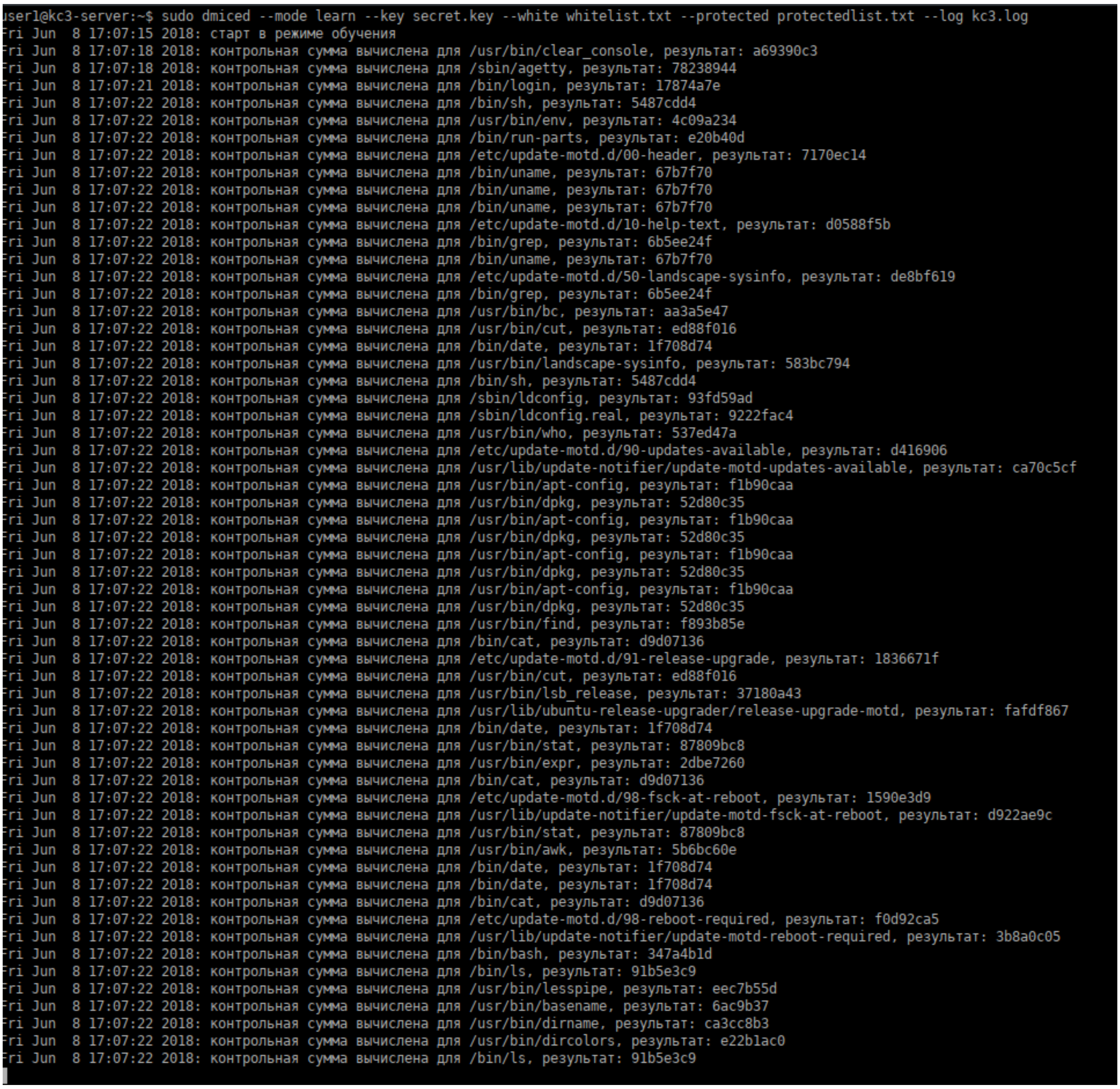

Рисунок 1 – Модуль ЗПС в режиме обучения

Файл с «белым» списком будет иметь следующее содержимое:

«

/bin/bash mac:347A4B1D

/bin/cat mac:D9D07136

/bin/date mac:1F708D74

/bin/grep mac:6B5EE24F

/bin/login mac:17874A7E

/bin/ls mac:91B5E3C9

/bin/mount mac:E15E611B

/bin/run-parts mac:0E20B40D

/bin/sh mac:5487CDD4

/bin/uname mac:067B7F70

/etc/update-motd.d/00-header mac:7170EC14

/etc/update-motd.d/10-help-text mac:D0588F5B

/etc/update-motd.d/50-landscape-sysinfo mac:DE8BF619

/etc/update-motd.d/90-updates-available mac:0D416906

/etc/update-motd.d/91-release-upgrade mac:1836671F

/etc/update-motd.d/98-fsck-at-reboot mac:1590E3D9

/etc/update-motd.d/98-reboot-required mac:F0D92CA5

/sbin/agetty mac:78238944

/sbin/dumpe2fs mac:8CE96601

/sbin/ldconfig mac:93FD59AD

/sbin/ldconfig.real mac:9222FAC4

/usr/bin/apt-config mac:F1B90CAA

/usr/bin/awk mac:5B6BC60E

/usr/bin/basename mac:06AC9B37

/usr/bin/bc mac:AA3A5E47

/usr/bin/clear_console mac:A69390C3

/usr/bin/cut mac:ED88F016

/usr/bin/dircolors mac:E22B1AC0

/usr/bin/dirname mac:CA3CC8B3

/usr/bin/dpkg mac:52D80C35

/usr/bin/env mac:4C09A234

/usr/bin/expr mac:2DBE7260

/usr/bin/find mac:F893B85E

/usr/bin/landscape-sysinfo mac:583BC794

/usr/bin/lesspipe mac:EEC7B55D

/usr/bin/lsb_release mac:37180A43

/usr/bin/stat mac:87809BC8

/usr/bin/who mac:537ED47A

/usr/lib/ubuntu-release-upgrader/check-new-release mac:1E78EF33

/usr/lib/ubuntu-release-upgrader/release-upgrade-motd mac:FAFDF867

/usr/lib/update-notifier/update-motd-fsck-at-reboot mac:D922AE9C

/usr/lib/update-notifier/update-motd-reboot-required mac:3B8A0C05

/usr/lib/update-notifier/update-motd-updates-available mac:CA70C5CF

»

После формирования «белого» списка привилегированный пользователь должен сформировать «защищенный» список из файлов СКЗИ «Dcrypt 1.0 v.2». Для этого используется следующая команда:

«dmiced --mode addp --key secret.key --white whitelist.txt --protected protectedlist.txt --log kc3.log /usr/local/sbin/dmvpnd».

Процесс отработки приведенной команды представлен на рисунке 2.

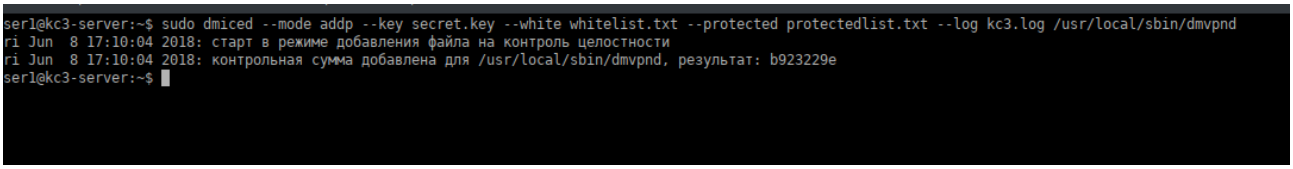

Рисунок 2 – Процесс формирования «защищенного» списка

Таким образом, после добавления всех модулей СКЗИ «Dcrypt 1.0 v.2», «защищенный» список будет выглядеть примерно следующим образом:

«

/usr/local/lib/libasiotap.so.1 mac:D908F19C

/usr/local/lib/libdmbase.so.1 mac:FBCA6EFF

/usr/local/lib/libdmcrypt.so.1 mac:4B0EFA8B

/usr/local/lib/libdmtcl.so.1 mac:3FA2BAEF

/usr/local/lib/libdmvpn.so.1 mac:F95C40D2

/usr/local/lib/libpugixml.so.1 mac:85302558

/usr/local/sbin/dmvpnd mac:B923229E

»

3.4.3 Запуск модуля ЗПС

Для запуска модуля ЗПС в режиме применения сформированных правил привилегированный пользователь (администратор безопасности) должен выполнить следующую команду:

«dmiced --mode enforce --key secret.key --white whitelist.txt --protected protectedlist.txt --log kc3.log».

Модуль ЗПС вычислит контрольные суммы для всех файлов в списках и сравнит их с зафиксированными. Если все контрольные суммы совпадают, тогда модуль ЗПС разрешает исполнение файлов из «защищенного» списка (см. рисунок 3).

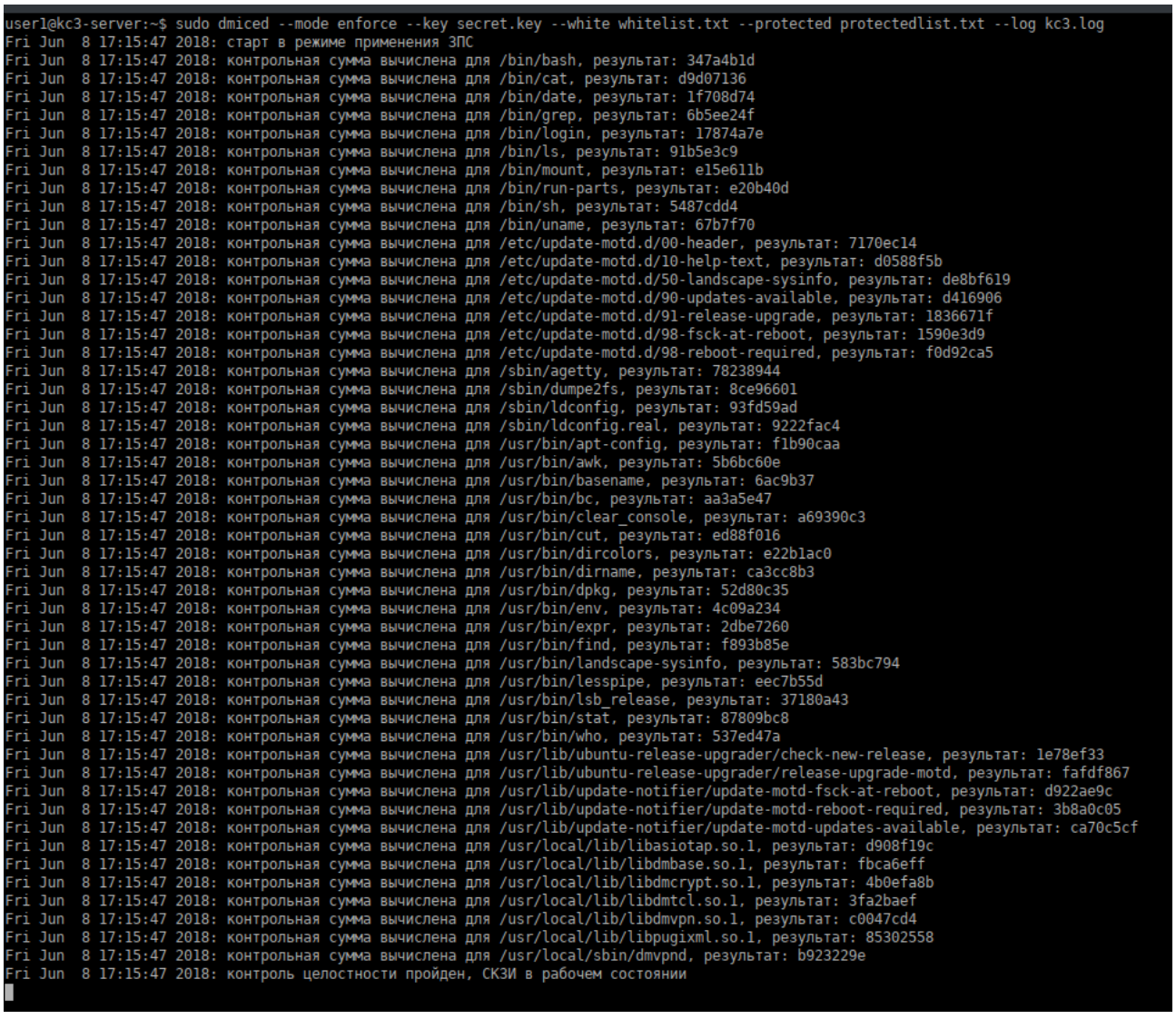

Рисунок 3 – Контроль целостности пройден

Если контрольные суммы для какого-нибудь файла не совпали, тогда все файлы из «защищенного» списка будут заблокированы для запуска пользователями (см. рисунок 4).

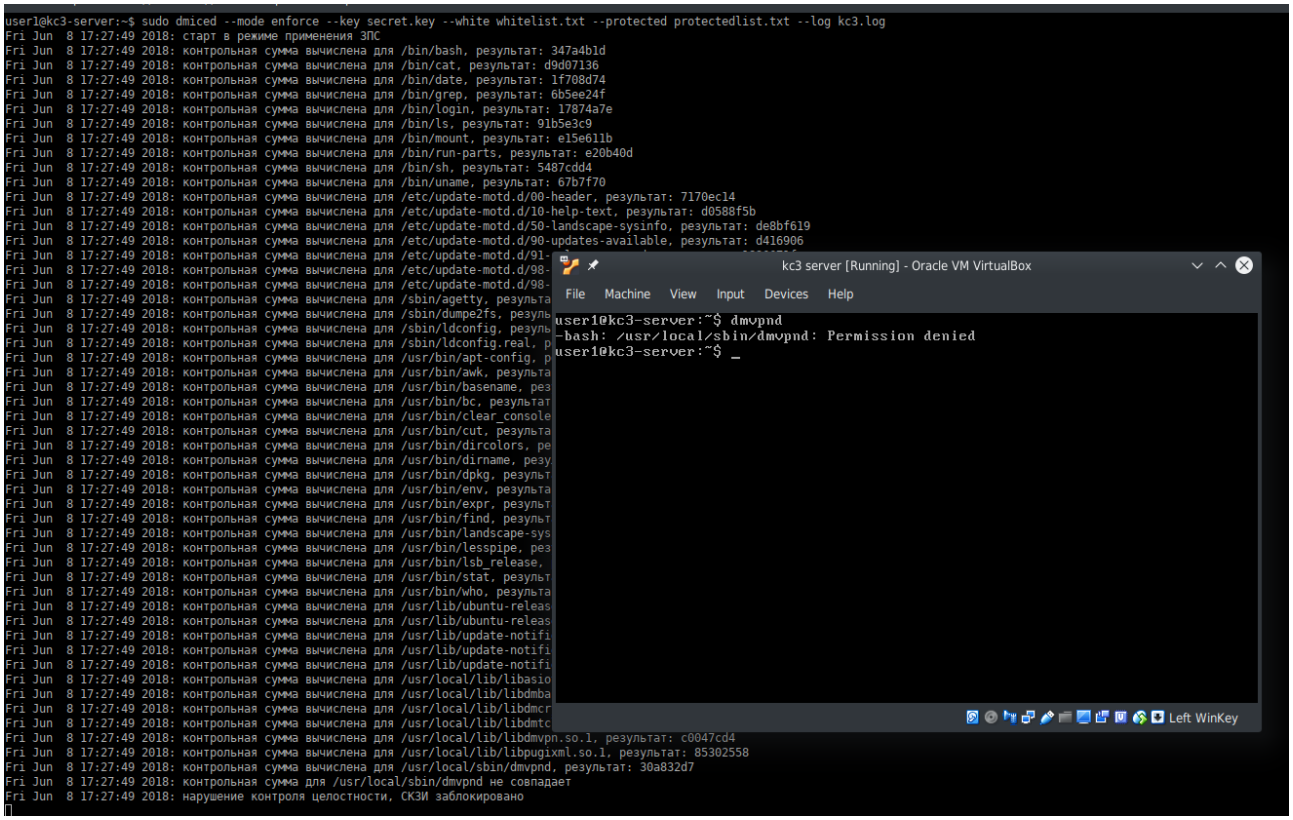

Рисунок 4 – Контроль целостности не пройден

Модуль ЗПС осуществляет также и динамический контроль целостности, отслеживая изменения файлов из списков и проверяя их контрольные суммы во время работы уполномоченных пользователей в среде функционирования. Если контрольные суммы какого-либо из файлов не совпадают с зафиксированной, тогда модуль ЗПС блокирует файлы из «защищенного» списка (см. рисунок 5).

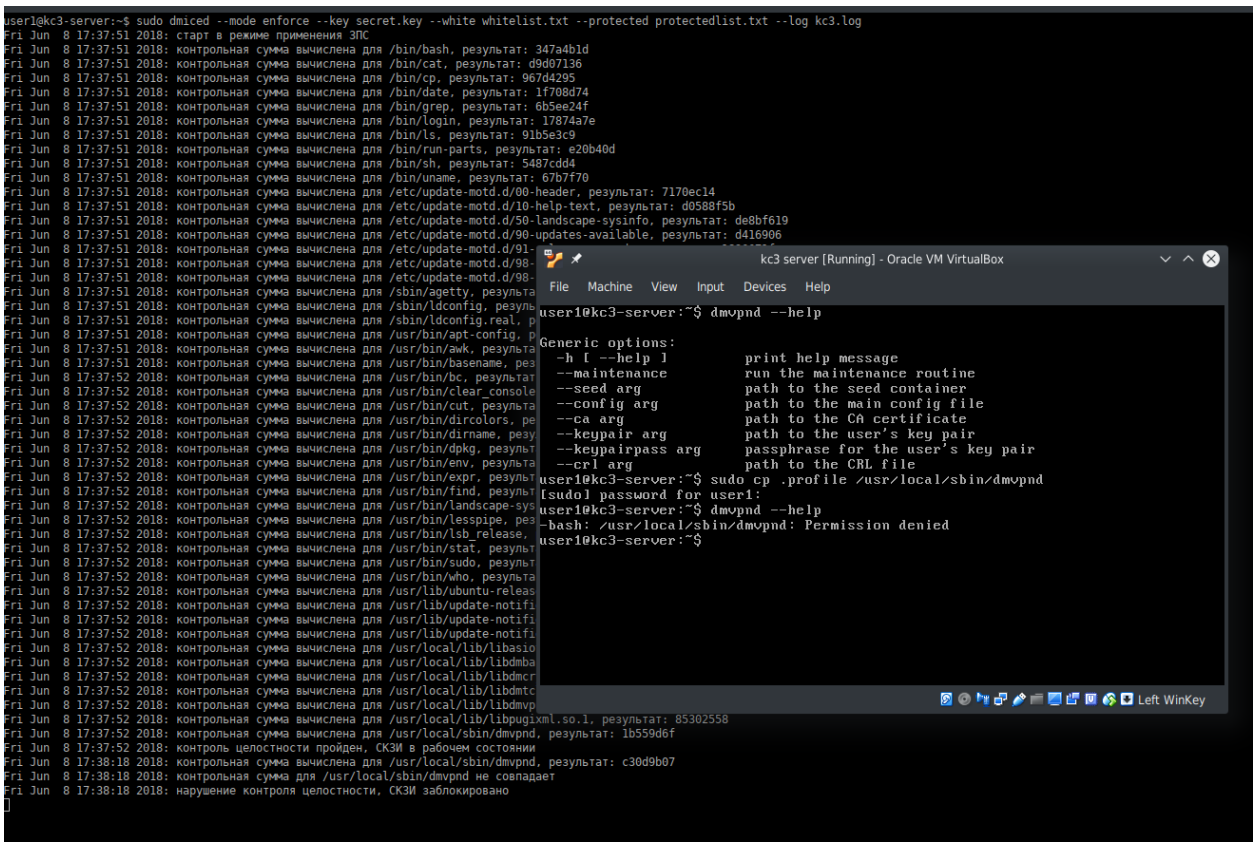

Рисунок 5 – Процедура блокирования файлов

Кроме того, модуль СКЗИ «Dcrypt 1.0 v.2» отслеживает и блокирует попытки пользователя запустить на исполнение файлы, которые не входят в «белый» список (защита от НСД) (см. рисунок 6).

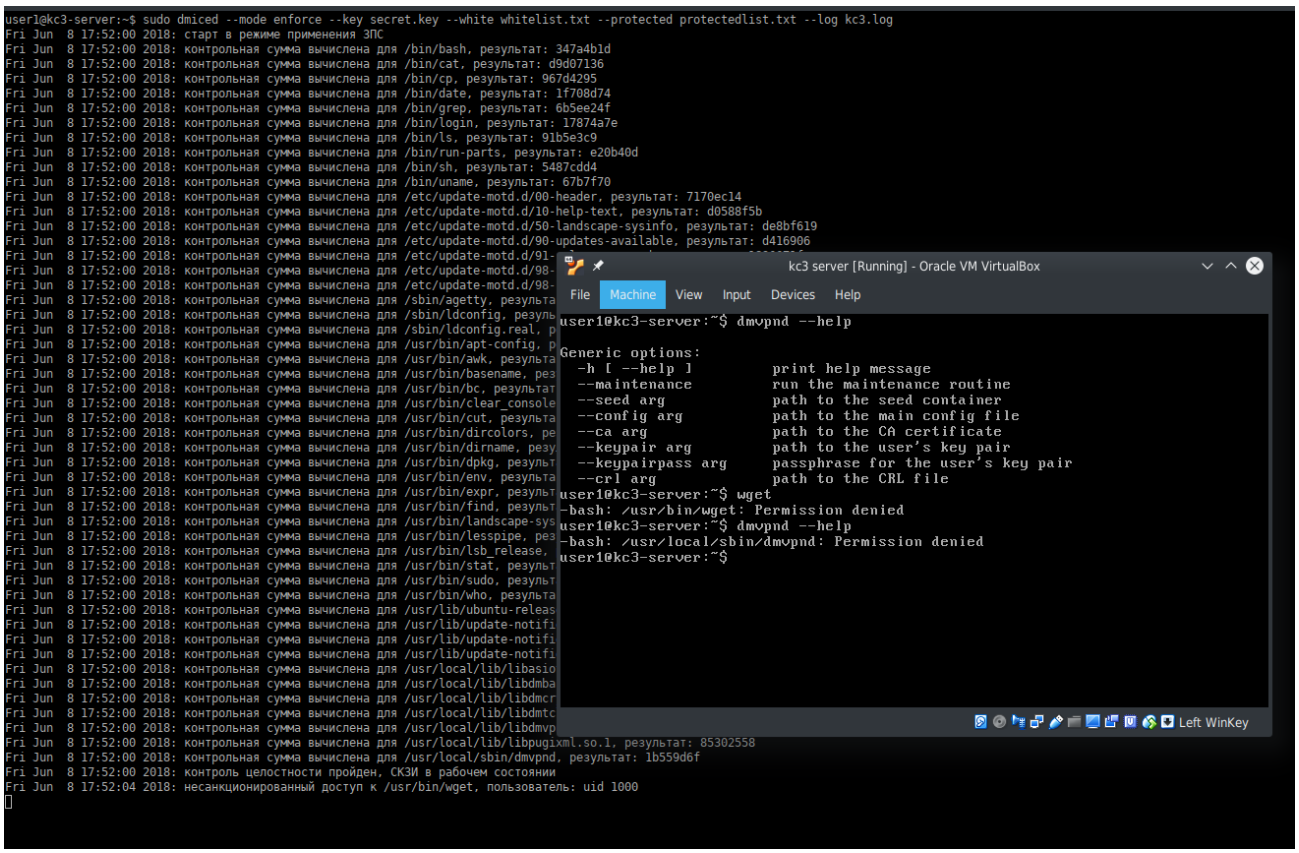

Рисунок 6 – Демонстрация защиты от НСД

3.5 Описание и настройка замкнутой программной среды СКЗИ «Dcrypt 1.0 v.2» для исполнений 3, 18 и 33

Для обеспечения ЗПС в СКЗИ «Dcrypt 1.0 v.2» для вариантов исполнения 3, 18 и 33, сертифицированных по классам КС3, должны использоваться совместно:

- средства доверенной загрузки;
- программные модули «DmCSE.sys» и «DmCSEManager.exe», «DmCSEDI.dll», «DmCSE.inf», «DmCSEService.exe».

3.5.1 Назначение ЗПС

Механизм ЗПС обеспечивает:

- контроль доступа пользователей к файловой системе компьютера;
- контроль запуска процессов.

На этапе настройки механизма ЗПС составляются два списка исполняемых файлов: «White List» и «Protected List».

«White List» может быть сформирован как автоматически (в режиме обучения), так и вручную. «Protected List» может быть сформирован исключительно вручную.

При этом для файлов из этих списков рассчитываются эталонные контрольные суммы для их последующего контроля.

3.5.2 Установка ЗПС

Обязательно должна быть включена учетная запись «Администратор|Administrator», создаваемая по умолчанию при установке операционной системы (в противном случае при нарушении контрольной целостности никто не сможет зайти в систему). Администратор безопасности должен произвести установку ЗПС согласно следующему порядку действий:

1) Определиться с битностью ЗПС (и распространяемого пакета Visual C++ для Visual Studio 2015. Их битность должна совпадать с битностью ОС.
2) Установить распространяемый пакет Visual C++ для Visual Studio 2015 соответствующей битности.
3) Создать 4 каталога: (Например: «C:\DmCse\», «C:\DmCSEManager\», «C:\DmCSEService\» и «C:\DmCSEService\Log\»).
4) Скопировать в каталог «C:\DmCse\» файлы «DmCse.sys» и «DmCse.inf», входящих в состав ЗПС.
5) Скопировать в каталог «C:\DmCSEManager\» файл «DmCSEManager.exe» входящий в состав ЗПС.
6) Скопировать в каталог «C:\DmCSEService\» файлы «DmCSEService.exe» и «DmCSEDI.dll», входящих в состав ЗПС.
7) Создать криптографический ключ и сохранить его в файле «C:\DmCSEManager\Key.bin» (Размер файла = 32 байта).
8) Запустить командную строку «cmd» с повышением привилегий.
9) Перейти в каталог «C:\DmCse\».
10) Для регистрации драйвера «DmCse.sys» выполнить команду: «RUNDLL32.EXE SETUPAPI.DLL,InstallHinfSection DefaultInstall 132 C:\DmCse\DmCse.inf».
11) Перейти в каталог «C:\DmCSEManager\».
12) Для установки криптографического ключа выполнить команду: «DmCSEManager.exe -set_key "C:\DmCSEManager\Key.bin». Где «Key.bin» - файл с криптографическим ключом (размер файла = 32 байта). После произведенной установки криптографического ключа файл с ключевой информацией «key.bin» необходимо удалить.
13) Перейти в каталог «C:\DmCSEService\».
14) Для регистрации сервиса «DmCSEService» выполнить команду: «DmCSEService /Service».
15) Ограничить доступ к конфигурационным параметрам ЗПС. Для этого запустить regedit.exe.

а) Найти ключ:
«HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters»

б) Произвести нажатие правой клавишей мыши, в меню опций выбрать: «Разрешения"|"Permissions...».

в) В появившемся диалоге нажать «дополнительно»|»Advanced».

В появившемся диалоге убрать галочку «Добавить разрешения, наследуемые от родительских объектов»|Include inheritable permissions from this object's parent».

г) В появившемся диалоге нажать «Добавить»|«Add». Нажать кнопку «OK».

д) В списке «Элементы разрешений»|«Group or user names» удалить все записи кроме «SYSTEM» и «Administrators». Нажать кнопку «OK».

16) Ограничить доступ к логам ЗПС. Для этого:

а) В проводнике Windows кликнуть правой кнопкой мыши на каталог C:\DmCSEService\Log\, выбрать «Свойства».

б) В появившемся диалоге выбрать вкладку «Безопасность».

в) В появившемся диалоге нажать «дополнительно»|«Advanced».

г) В появившемся диалоге убрать галочку «Добавить разрешения, наследуемые от родительских объектов»|«Include inheritable permissions from this object's parent».

д) В появившемся диалоге нажать «Добавить»|«Add». Нажать кнопку «OK».

е) Удалить из списка «Группы и пользователи» удалить все записи кроме «Система» и «Администраторы». Нажать кнопку «OK» во всех диалоговых окнах.

ж) Запустить интерпретатор командной строки «cmd» с повышением привилегий и выполнить команду:

«sc config DmCSEService start= auto && net start DmCSEService».

3.5.3 Удаление ЗПС

Если подтверждено, что установка ЗПС была выполнена в соответствии с пунктом 3.2.3 «Установка ЗПС», для удаления ЗПС необходимо:

1) Запустить интерпретатор командной строки «cmd» с повышением привилегий.
2) Перейти в каталог «C:\DmCSEManager».
3) Выполнить команду: «DmCSEManager.exe -enforce_stop».

4) Перейти в каталог «C:\DmCSEService\».
5) Выполнить команду: «DmCSEService /UnregServer».
6) Перейти в каталог «C:\DmCse\».
7) Выполнить команду: «RUNDLL32.EXE SETUPAPI.DLL,InstallHinfSection DefaultUninstall 132 C:\DmCse\DmCse.inf».

3.5.4 Конфигурационные параметры

ЗПС хранит все свои конфигурационные параметры в следующем разделе реестра: «KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters».

ЗПС имеет следующие конфигурационные параметры:

1) Значение: «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\ProcessingMode». Тип (REG_DWORD). Допустимые значения:
   а) 0: Режим по умолчанию (DEFAULT) - Драйвер ничего не делает (Прозрачно пропускает все запросы).
   б) 1: Режим обучения (LEARNING) - Драйвер собирает информацию о запускаемых процессах.
   в) 2: Режим применения настроек (ENFORCING) - Драйвер контролирует запуск процессов в соответствии с пунктом 3.5.1 «Назначение ЗПС»).
2) Значение: «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\DmCryptKey». Тип (REG_BINARY). Содержит криптографический ключ (32 байта).
3) Ключ: «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\ProtectedList» с подключами.
   а) Содержит список «Protected List».
   б) Подключи данного ключа соответствуют серийным номерам томов файловой системы.
   в) Каждый из подключей содержит значения, соответствующие файлам, расположенным на данном томе.
4) Ключ: «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters\WhiteList» с подключами.

а) Содержит список «White List». Данные сгруппированы по томам, на которых расположены файлы.
б) Подключи данного ключа соответствуют серийным номерам томов файловой системы.
в) Каждый из подключей содержит значения, соответствующие файлам, расположенным на данном томе.

3.5.5 Безопасность конфигурационных параметров

Получить доступ к конфигурационным параметрам ЗПС можно:

1) Непосредственно обращаясь из приложения к реестру. Это контролируется следующим образом: для ключа «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DmCse\Parameters» и всех его подключей устанавливается разрешение, запрещающие доступ к ним кроме пользователя «SYSTEM» и группы «локальные администраторы» (локальными администраторами в данном контексте принято считать администраторов безопасности).
2) Опосредованно, подключившись к сервису и отдавая ему команды. Это контролируется следующим образом: При создании программного компонента «пайпа» на стороне сервера ему назначаются атрибуты безопасности, запрещающие доступ к нему всем кроме группы «локальные администраторы».
3) Опосредованно, подключившись к драйверу и отдавая ему команды. Это контролируется следующим образом: необходимо подключиться к драйверу «DmCse.sys» для того чтобы отправить ему команду. Осуществить данное действие, может только уполномоченный пользователь «SYSTEM» или член группы «локальные администраторы».

Доступ к настройкам и управлению ЗПС имеют только пользователь «SYSTEM» и члены группы «локальные администраторы».

3.5.6 Подготовка к использованию

Важно: утилита «dmcsemanager.exe» должна выполняться в контексте безопасности локального администратора с повышенными привилегиями.

Подготовка к использованию осуществляется следующим образом:

1) Для начала обучения выполнить команду: «DmCSEManager.exe -learn_start».

2) Компьютер будет автоматически перезагружен через 10 секунд. После перезагрузки ЗПС фиксирует все автоматически запускающиеся процессы при старте ОС.
3) Для автоматического добавления программ в «White List» их необходимо запустить.
4) Для завершения обучения выполнить команду: «DmCSEManager.exe -learn_stop».
5) При этом старое содержимое «White List» будет удалено и на его место будет записан новый «White List» из памяти драйвера.
6) Если необходимо, вручную добавить или удалить файлы в «White List» (файлы, которые не были учтены в «White List» при обучении), то следует выполнять следующие команды:
    а) Добавление файла «c:\1.exe» в «White List»: Необходимо выполнить команду: «DmCSEManager.exe -add_wl "c:\1.exe"».
    б) Удаление файла «c:\1.exe» из «White List»: Необходимо выполнить команду: «DmCSEManager.exe -del_wl "c:\1.exe"».
7) Вручную добавить или удалить файлы в «Protected List» посредством следующих команд:
    а) Добавление файла «c:\1.exe» в «Protected List». Необходимо выполнить команду: «DmCSEManager.exe -add_pl "c:\1.exe"».
    б) Удаление файла «c:\1.exe» из «Protected List». Необходимо выполнить команду: «DmCSEManager.exe -del_pl "c:\1.exe"».

**При ручном добавлении исполняемых файлов (расширение .exe) администратор безопасности должен убедиться в том, что все файлы, которые необходимы для функционирования данного программного модуля (расширение .dll и прочие) также были внесены в «White List» и «Protected List».*

8) Для начала применения настроек выполнить команду: «DmCSEManager.exe -enforce_start».
9) Проверить, что выполняются требования, описанные в пункте 3.5.1 «Назначение ЗПС» (для проведения проверки можно перезагрузить или выключить/включить компьютер. После загрузки операционной системы, ЗПС будет работать в режиме применения настроек.
10) Для выхода из режима применение выполнить команду: «DmCSEManager.exe -enforce_stop».

11) В любой промежуточный момент можно получить информацию о текущем состоянии ЗПС. Для этого необходимо выполнить команду: «DmCSEManager.exe –info». Если информация не умещается на экране, то можно сделать вывод в файл, выполнив команду: «DmCSEManager.exe -info >имя_файла».
12) Для получения справочной информации по параметрам утилиты «DmCseManager.exe», достаточно запустить ее без параметров или ошибиться в них.

3.6 Конфигурационные настройки СКЗИ «Dcrypt 1.0 v.2» для исполнения 16, 17 и 18

Исполняемый файл «dmvpnd.exe» представляет собой консольное приложение, предназначенное для установления защищенного VPN-соединения с сервером СКЗИ «Dcrypt 1.0 v.2».

Аргументы:

- «--adapter "{6A44349F-3AAC-4D17-BF9C-71D0681434BD}"» - идентификатор TAP-адаптера. Идентификаторы адаптеров уникальны в каждой системе. Так же при установке\удалении TAP-адаптера данные идентификаторы изменяются системой. Если параметр отсутствует или имеет пустое значение или содержит невалидный идентификатор, ПО СКЗИ «Dcrypt 1.0 v.2» попытается обнаружить подходящий адаптер в системе и использовать его для установления соединения. Если в системе отсутствуют подходящие TAP-адаптеры, пользователю/ администратору безопасности будет выведено сообщение об ошибке;
- «--seed "D:\Projects\VpnClient\dmvpnd\!testdata\seed.dsc"» - путь к файлу инициализации генератора псевдослучайных чисел. Если указанный файл отсутствует, то пользователю/ администратору безопасности будет выведено сообщение об ошибке;
- «--ca "C:\Users\TestUser\DPki\ca.crt"» - путь к файлу сертификата. Если указанный файл отсутствует, то пользователю/ администратору безопасности будет выведено сообщение об ошибке;
- «--keypair "C:\Users\TestUser\DPki\testuser.dkpc"» - путь к файлу ключевой пары. Если указанный файл отсутствуют, то пользователю/ администратору безопасности будет выведено сообщение об ошибке;
- «--passphrase "1111"» - пароль от ключевой пары. При попытке установления соединения происходит проверка пароля, при неправильном значении будет выведено

сообщение об ошибке. Факт неправильного ввода пароля также будет записан в журнал регистрации событий;

- --ip "172.20.15.183" - IP адрес сервера СКЗИ «Dcrypt 1.0 v.2»;
- --port 1024 - порт сервера СКЗИ «Dcrypt 1.0 v.2»;
- --install - ключ, при использовании которого введенные параметры запоминаются в системе. В дальнейшем можно производить установления VPN соединения с сервером простым вызовом «dmvpnd.exe» без указания параметров. Параметры сохраняются для каждого пользователя/ администратора безопасности раздельно.

Пример 1: следующая командная строка запустит попытку установления VPN соединения с сервером СКЗИ «Dcrypt 1.0 v.2» по адресу «--ip "192.168.1.100" --port 1024»:

«

> C:\Program Files\TSS Ltd\DVPN\bin\dmvpnd.exe --seed "C:\Users\TestUser\DPki\seed.dsc" --ca "C:\Users\TestUser\DPki\ca.crt" --keypair "C:\Users\TestUser\DPki\testuser.dkpc" --ip "192.168.1.100" --port 1024

».

Пример 2: следующая командная строка сохранит настройки для дальнейшего использования:

«

> C:\Program Files\TSS Ltd\DVPN\bin\dmvpnd.exe --seed "C:\Users\TestUser\DPki\seed.dsc" --ca "C:\Users\TestUser\DPki\ca.crt" --keypair "C:\Users\TestUser\DPki\testuser.dkpc" --ip "192.168.1.100" --port 1024 –install

».

3.7 Конфигурационные настройки СКЗИ «Dcrypt 1.0 v.2» для исполнения 19, 20 и 21

Необходимо создать корневой сертификат и две ключевые пары для клиента и для сервера (процесс создания ключевых пар для АП VPN – серверов и АП VPN – клиентов описан в разделе 3.8.3 «Создание ключевых пар для АП VPN -серверов и АП VPN - клиентов» настоящего документа).

Затем создать конфигурационный файл. Пример содержания конфигурационного файла client1.xml:

«

```
<?xml version="1.1" encoding="UTF-8" ?>
<msg revision="18" type="160" client_type="0" session_id="00000000-0000-0000-0000-
000000000000">
  <params>
    <vpnService mode="Client" guid="e79bdce5-8ba5-43c5-9159-972934f5c98f">
```

```
        <tap name="tapc1" mtu="10000" mac="00:00:00:00:00:00" address="9.0.0.2"
netmask="255.255.255.0"/>
        <crypto caGuid="" crlGuid="" certGuid="" keyGuid=""/>
        <client port="7777">
          <remoteServer hostname="172.20.1.52" port="1024"/>
        </client>
      </vpnService>
   </params>
</msg>
»
```

Пример содержания конфигурационного файла server.xml:

```
«
<?xml version="1.1" encoding="UTF-8" ?>
<msg revision="18" type="160" client_type="0" session_id="00000000-0000-0000-0000-
000000000000">
   <params>
      <vpnService mode="Server" guid="8e25db17-773c-4a51-a566-0d8b091e321f">
        <tap name="taps1" mtu="10000" mac="00:00:00:00:00:00" address="9.0.0.1"
netmask="255.255.255.0"/>
        <crypto caGuid="" crlGuid="" certGuid="" keyGuid=""/>
        <server port="1024">
          <dhcpServer enabled="true" startAddress="9.0.0.10" endAddress="9.0.0.100"
dnsAddress="8.8.8.8" leaseTime="3600"/>
        </server>
      </vpnService>
   </params>
</msg>
»
```

Для запуска клиента необходимо в командной строке выполнить следующую команду: dmvpnd --seed ./testdata/seed.dsc --seedpass 1111 --ca testdata/test_ca.crt --crl testdata/crl.crt --cert testdata/test_client1.crt --key testdata/test_client1.dpkc --keypass 1111 --config testdata/client1.xml

Для запуска сервера необходимо в командной строке выполнить следующую команду: dmvpnd --seed testdata/seed.dsc --seedpass 1111 --ca testdata/test_ca.crt --crl testdata/crl.crt --cert testdata/test_serv1.crt --key testdata/test_server1.dpkc --keypass 1111 --config testdata/server.xml

Команды для запуска клиента и сервера приведены в качестве примера и могут отличаться от типовых в силу отличий пути к тем или иным файлам. Подробное описание конфигурационных настроек СКЗИ «Dcrypt 1.0 v.2» для исполнения 19, 20 и 21 приведено в документе «Средство криптографической защиты информации «Dcrypt 1.0 v.2». Руководство администратора безопасности. 4012-006-61649217-18 01 91».

3.8 Учет ключевой информации

3.8.1 Виды ключевой информации и ключевые носители

Ключевая информации и ключевые носители подразделяются следующие виды:

- закрытый персональный ключ пользователя;
- открытый персональный ключ пользователя;
- закрытый корневой ключ;
- открытый корневой ключ.

Закрытые ключи хранятся в зашифрованном виде в формате ключевого контейнера. Открытые ключи хранятся в открытом виде в соответствии с RFC5280, RFC4491. Способы формирования ключевой информации описаны в эксплуатационных документах, входящих в состав комплекта поставки СКЗИ «Dcrypt 1.0 v.2». Подробное описание видов ключевой информации и ключевых носителей приведено в таблице 4.

Таблица 4 – Виды ключевой информации и ключевые носители

Наименование	Место создания	Область применения
Закрытый персональный ключ пользователя	КриптоАРМ	Шифрование / расшифрование электронных документов, формирование электронно-цифровой подписи (далее – ЭЦП) электронных документов, установление канала защищенного обмена по сети
Открытый персональный ключ пользователя	КриптоАРМ	Шифрование / расшифрование электронных документов, проверка ЭЦП электронных документов, установление канала защищенного обмена по сети
Закрытый корневой ключ	КриптоАРМ	Выдача (формирование ЭЦП) открытого ключа пользователя, отзыв открытого ключа пользователя
Открытый корневой ключ	КриптоАРМ	Проверка валидности открытого ключа пользователя

3.8.2 Способы формирования ключевой информации

Для двусторонней аутентификации при установлении канала VPN (Virtual Private Network) используются ключевые пары в соответствии с ГОСТ Р 34.10-2012. Для генерации ключевых пар и соответствующих им сертификатов X.509 возможно использование утилиты «dmcrypt-util». Главное окно программы показано на рисунке 7.

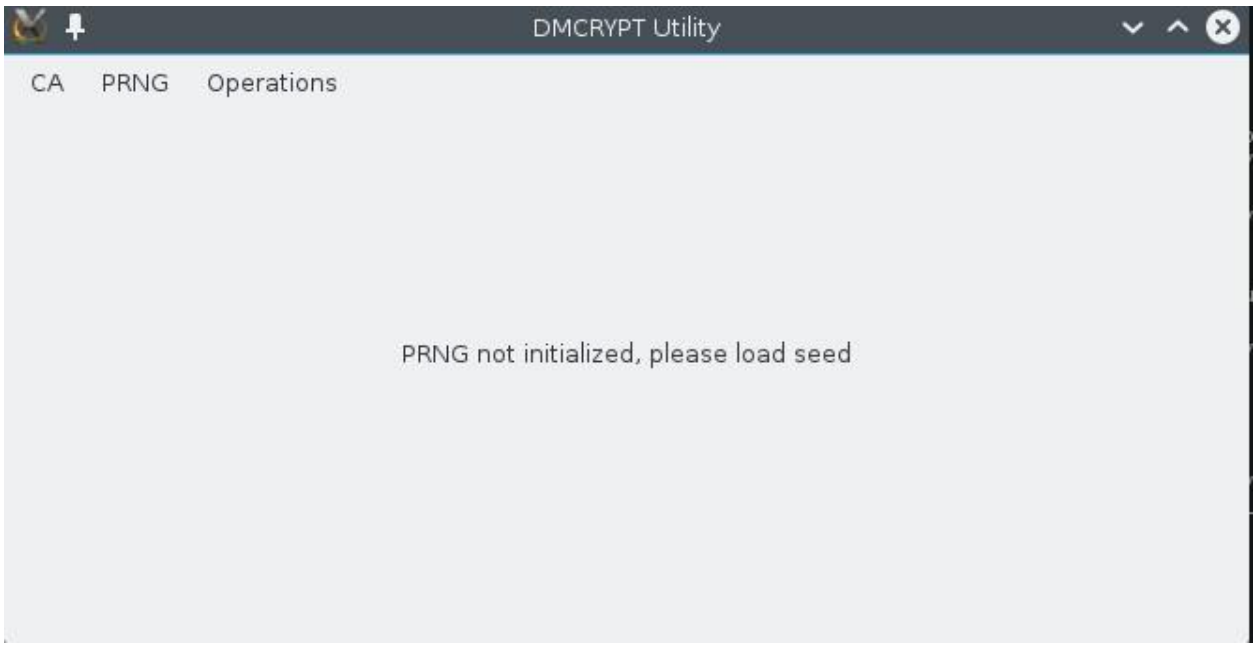

Рисунок 7 – Главное окно утилиты «dmcrypt-util»

Во время своей работы утилита использует встроенный ПДСЧ, который необходимо инициализировать случайной последовательностью, взятой с физического датчика случайных чисел (далее – ДСЧ) аппаратно-программного модуля доверенной загрузки. Встроенный ПДСЧ так же возможно инициализировать из файла со случайной последовательностью, заранее сгенерированной аппаратно-программным модулем доверенной загрузки. Перечень поставляемых аппаратно-программных модулей доверенной загрузки приведен в таблице 4 «Состав комплекта поставки СКЗИ «Dcrypt 1.0 v.2» раздела 4 «Комплектность» документа «Средство криптографической защиты информации «Dcrypt 1.0 v.2». Формуляр. 4012-006-61649217-18 01 30».

После инициализации ПДСЧ необходимо сгенерировать корневую ключевую пару и экспортировать корневой сертификат в отдельный файл, а для этого необходимо выполнить следующие действия:

- выбрать пункт меню «CA -> Setup CA»;
- в открывшемся мастере создания корневой ключевой пары и списка отозванных сертификатов (далее – CRL) требуется выбрать путь к файлу, в котором будет сохранена корневая ключевая пара, и задать пароль для шифрования этого контейнера, при этом следует иметь в виду, что обычно ключевая пара имеет расширение файла «.dkpc» (см. рисунок 8);
- заполнить поля создаваемого корневого сертификата (см. рисунок 9);
- выбрать файл, в котором будет сохранен пустой сгенерированный CRL (см. рисунок 10);
- нажать кнопку «Завершить» (см. рисунок 10).

При нажатии кнопки «Завершить» будет создана корневая ключевая пара и CRL, информация о которых будет отображена в главном окне утилиты «dmcrypt-util» (см. рисунок 11).

При установлении VPN-соединения необходимо указать корневой сертификат, при помощи которого будут проверяться сертификаты и сервера, а также клиенты. В этой связи, сразу после создания ключевой пары необходимо экспортировать корневой сертификат в отдельный файл. Для этого необходимо выбрать пункт меню «CA -> Export CA certificate» и путь к месту его сохранения.

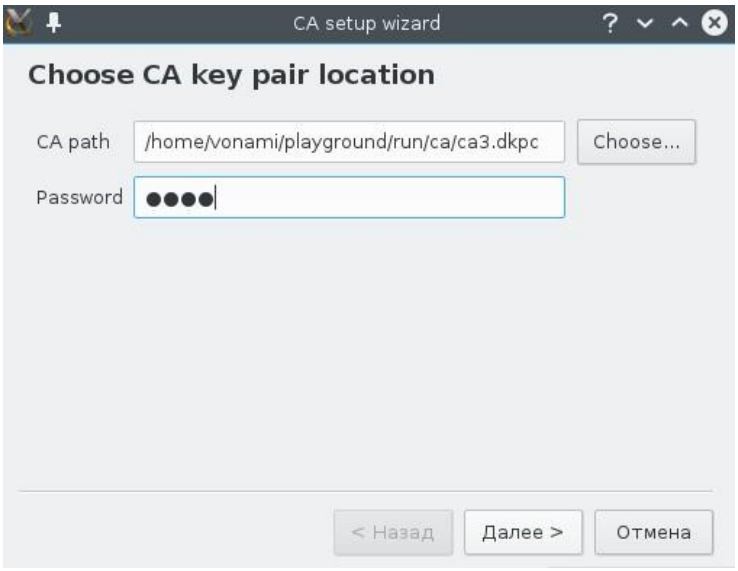

Рисунок 8 – Выбор файла для сохранения корневой ключевой пары

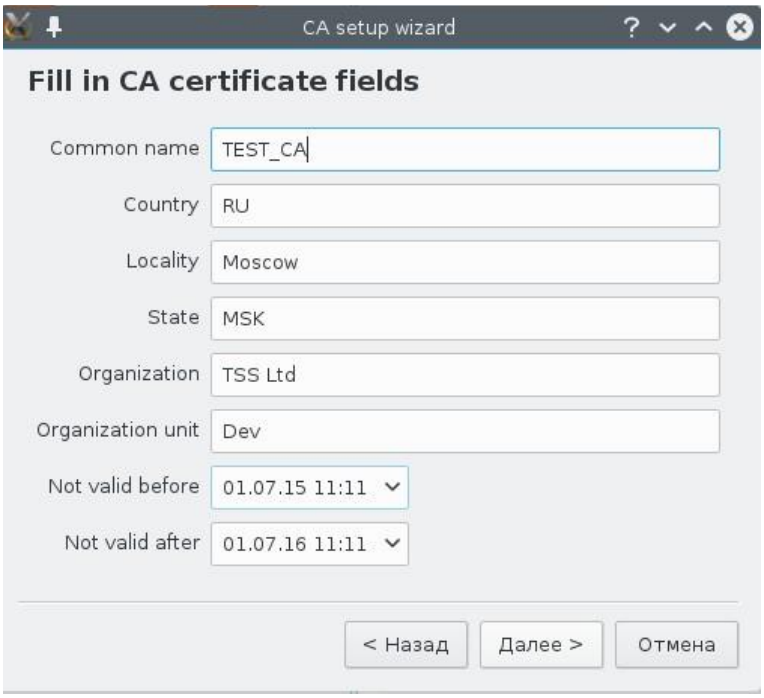

Рисунок 9 – Заполнение полей корневого сертификата

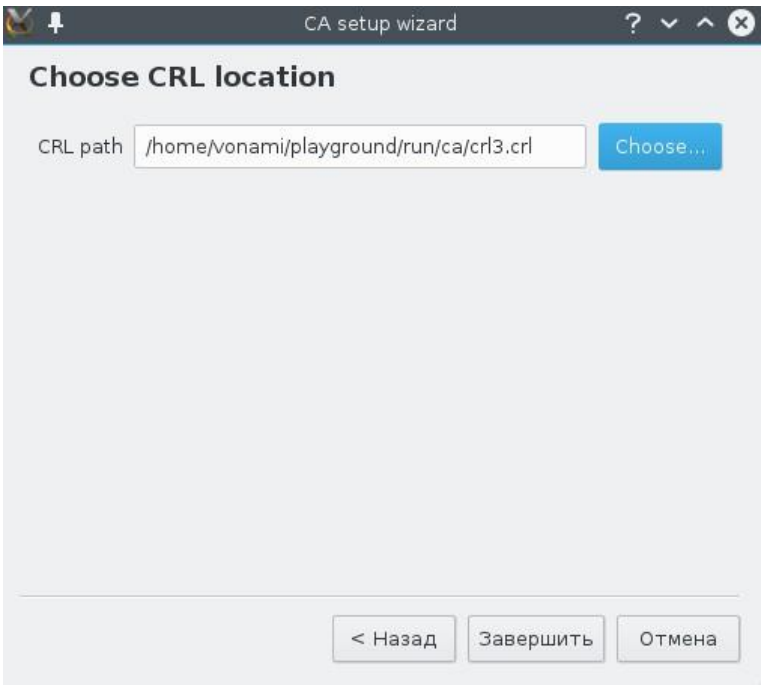

Рисунок 10 – Выбор файла для сохранения CRL

Рисунок 11 – Информация о корневом сертификате и CRL

Генерация ключевой информации также поддерживается сторонними криптопровайдерами (например, производства компании ООО «КРИПТО-ПРО») с применением RFC 4357, 4491, 5830, 5831, 5832, 7836 и прочих.

3.8.3 Создание ключевых пар для АП VPN -серверов и АП VPN -клиентов

При создании ключевых пар для АП VPN -серверов и АП VPN -клиентов необходимо выбрать в главном меню пункт «CA -> Issue a new X509 certificate» и произвести следующие действия:

- заполнить все поля создаваемого сертификата (см. рисунок 9);
- указать путь к сохраняемому файлу с ключевой парой и пароль шифрования (см. рисунок 8);

- указать путь, в котором будет сохранен отдельно сертификат X509.

При следующем запуске утилиты «dmcrypt-util» она автоматически загрузит созданную корневую ключевую пару, CRL и, таким образом, будет обеспечена возможность продолжить создание дочерних сертификатов. Если же необходимо создать новую ключевую пару, то необходимо повторить процедуру, воспользовавшись меню «CA -> Setup CA».

Кроме того, существует возможность инициализировать сертификат CA из внешних файлов, например, созданных на другом компьютере. Для этого потребуется на том же компьютере еще и экспортировать текущий серийный номер (при каждой операции создания сертификата этот номер увеличивается на единицу) через меню «CA -> Export serial number». Далее необходимо скопировать экспортированный серийный номер, файлы корневой ключевой пары и CRL на данный компьютер, а затем выбрать пункт меню «CA -> Load CA». Утилита предложит указать пути к загружаемым файлам с корневой ключевой парой, CRL и серийным номером. После этого можно продолжить выдачу дочерних сертификатов.

3.8.4 Хранение ключевых носителей

Ключевые носители пользователей рекомендуется хранить в сейфе. Пользователь несет персональную ответственность за хранение своих ключевых носителей.

При наличии в организации, эксплуатирующей СКЗИ «Dcrypt 1.0 v.2», администратора безопасности и при организованном централизованном хранении ключевых носителей, администратор безопасности несет персональную ответственность за хранение ключевых носителей пользователей. Личные ключевые носители администратора безопасности должны храниться в его личном сейфе.

3.8.5 Сроки действия ключей

Допустимый срок действия закрытых ключей – не более 1 года 3 месяцев без использования ключа «Рутокен ЭЦП 2.0» или другого сертифицированного по требованиям ФСБ России аналога, и не более 3 лет при использовании ключа «Рутокен ЭЦП 2.0» или другого сертифицированного по требованиям ФСБ России аналога, а открытых ключей – не более 15 лет. Контроль срока использования ключевой информации для СКЗИ «Dcrypt 1.0 v.2» исп. 31, 32, 33, 34, 35 и 36 возложен на администратора безопасности нового СКЗИ.

3.8.6 Уничтожение ключевой информации на ключевых носителях

Ключевые носители с ключевой информацией, срок действия которой истек, не могут использоваться ни в каком другом качестве, кроме как в качестве ключевого носителя СКЗИ «Dcrypt 1.0 v.2». Уничтожение ключевых носителей, за исключением накопителей на гибких магнитных дисках (далее – НГМД), осуществляется путем физического воздействия на них (например, посредством их расплющивания молотком на наковальне). НГМД также уничтожаются путем физического воздействия на них (например, посредством их оплавления до бесформенной массы).

3.8.7 Компрометация ключей

Под компрометацией ключевой информации понимается утрата или временная потеря ключевого носителя, разглашение и/или копирование ключевой информации, а также несанкционированный доступ к ней.

При компрометации закрытого ключа предусматривается следующий порядок действий:

1) о факте компрометации немедленно ставятся в известность администратор безопасности;
2) производится генерация новых ключей и замена скомпрометированных ключей на новые с их последующей регистрацией;
3) скомпрометированные ключи на носителе информации уничтожается путем физического воздействия на ключевой носитель или перезаписи на носитель нового закрытого ключа.

3.8.8 Учет ключевой информации

При функционировании КриптоАРМ должен вестись «Журнал учета ключей», в которых следует отображать следующую информацию:

- Ф.И.О. лица, производящего запись;
- дата создания ключа;
- идентификаторы ключа (таблицы ключей) (например: серия, номер, комплект и т.п.);
- дата передачи/получения ключа;
- Ф.И.О. получателя/отправителя ключа;
- номер акта о передаче ключа или подпись получателя;
- запись о компрометации ключа.

На абонентский пункт (далее – АП) также должен вестись «Журнал учета ключей» (возможно ведение одного журнала для нескольких АП), в котором следует отображать следующую информацию:

- дата получения/создания ключа;
- идентификатор АП (в случае ведения одного журнала для нескольких АП);
- дата установки сетевых ключей или ключей ЭЦП;
- дата вывода ключа из действия;
- номер акта о передаче (возврате на КриптоАРМ) ключа или об уничтожении ключевой информации;
- запись о компрометации ключа;
- записи, отражающие выдачу на руки пользователям (ответственным исполнителям) и сдачу ими на хранение ключевых носителей (в случае централизованного хранения).

3.9 Регистрация событий

СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 4, 5, 6, 16, 17, 18, 19, 20 и 21 обеспечивает регистрацию следующих событий:

1) Факты ввода, смены и стирания ключевой информации (в том числе технологических ключей).
2) Факты использования ключей дольше заданного срока, повторного ввода ключей.
3) Факты несанкционированного доступа к СВТ с установленным СКЗИ «Dcrypt 1.0 v.2».
4) Результаты контроля целостности ПО СКЗИ «Dcrypt 1.0 v.2».
5) Факты проведения регламентных работ.
6) Попытки неудачного ввода ключевой информации.

Регистрация событий в СКЗИ «Dcrypt 1.0 v.2» исп. 31, 32, 33, 34, 35 и 36 возложена на разработчика СКЗИ. СКЗИ «Dcrypt 1.0 v.2» исп. 31, 32, 33, 34, 35 и 36 обеспечивает регистрацию следующих событий:

1) Факты ввода, смены и стирания ключевой информации (в том числе технологических ключей).
2) Факты использования ключей дольше заданного срока, повторного ввода ключей.
3) Факты проведения регламентных работ.
4) Попытки неудачного ввода ключевой информации.

В электронном журнале событий регистрируется информация о действиях, связанных с выполнением администратором безопасности СЗКИ «Dcrypt 1.0 v.2» целевых и прочих функций.

При инсталляции СЗКИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 16, 17, 18, 31, 32 и 33 место хранения журналов событий определяется каталогом инсталляции изделия, например: «C:\Program file\Diamond Security\DmCryptUtil\Log\dcryptsvc.log», где dcryptsvc.log – журнал событий. Администратору безопасности для просмотра журнала событий необходимо открыть указанный текстовый файл.

При инсталляции СЗКИ «Dcrypt 1.0 v.2» исп. 4, 5, 6, 19, 20, 21, 34, 35 и 36 место хранения журналов событий определяется каталогом инсталляции изделия, например: «/var/lib/dcryptsvc.log», где dcryptsvc.log – журнал событий. Администратору безопасности для просмотра журнала событий необходимо открыть указанный текстовый файл.

Регистрация событий, связанных с контролем целостности ОС, обеспечивается АПМДЗ, сертифицированным по требованиям ФСБ России к АПМДЗ.

Дополнительно СКЗИ «Dcrypt 1.0 v.2» исп. 6, 21, 36 и СКЗИ «Dcrypt 1.0 v.2» исп. 3, 18, 33 регистрируют все действия привилегированного пользователя по настройке, запуску модуля ЗПС, а также события во время работы модуля ЗПС.

Для СКЗИ «Dcrypt 1.0 v.2» исп. 6, 21, 36 данные события заносятся в журнал событий, который указан в параметре «--log» (см. пункт 3.4.1 «Описание модуля ЗПС»). Файл журнала должен быть защищен от модификации со стороны пользователя, как это изложено в пункте 3.4.2 «Настройка модуля ЗПС».

Для СКЗИ «Dcrypt 1.0 v.2» исп. 3, 18, 33 внесение записей в журналы событий ведется в файлы каталога «C:\DmCSEService\Log\». Файлы имеют имена формата «DD.MM.YYYY.log». Доступ к журналам событий определяется разрешениями, установленными на каталог «C:\DmCSEService\Log\» при развертывании ЗПС согласно пункту 3.5.2 «Установка ЗПС». (Доступ запрещен всем, кроме пользователя SYSTEM и группы «локальные администраторы»).

4 РЕКОМЕНДАЦИИ ПО РАЗМЕЩЕНИЮ ТЕХНИЧЕСКИХ СРЕДСТВ С СКЗИ «Dcrypt 1.0 v.2»

При создании системы защиты информации на объектах информатизации должны выполняться действующие в Российской Федерации требования по защите информации от утечки по техническим каналам, в том числе по каналу связи (например, требования, изложенные в СТР-К).

В случае использования СКЗИ «Dcrypt 1.0 v.2» в государственных автоматизированных системах для защиты конфиденциальной информации необходимо руководствоваться приказом ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Необходимость и достаточность мер по защите информации от утечки по техническим каналам, в том числе по каналу связи, должны оцениваться порядком, предусмотренным упомянутыми руководящими документами, с учетом целевых установок предполагаемого нарушителя и угроз безопасности информации, определяемых моделью угроз и нарушителя. При этом, если объекты аттестованы на соответствие установленным требованиям по защите информации без учета оценки канала связи, то при подключении СВТ с СКЗИ «Dcrypt 1.0 v.2» к каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать любое из следующих средств:

- волоконно-оптические линии связи;
- оптические развязывающие устройства, устанавливаемые в тракт передачи информации для создания оптоволоконного сегмента сети;
- сертифицированные СКЗИ для передачи информации соответствующего уровня конфиденциальности

В соответствии с Требованиями «Положения ПКЗ-2005» данные требования необходимо выполнять 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 и в 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, выполнение работ или оказание 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 сохранению ее конфиденциальности путем установления необходимости использования средств криптографической защиты информации.

Приведенные ниже требования носят рекомендательный характер при использовании СКЗИ «Dcrypt 1.0 v.2» для защиты информации:

- доступ к которой ограничен по решению обладателя, пользователя (потребителя) данной информации, собственника (владельца) информационных ресурсов (информационных систем) или уполномоченных ими лиц, не являющихся государственными органами или организациями, выполняющими государственные заказы;
- открытых и общедоступных государственных информационных ресурсов Российской Федерации.

5 ТРЕБОВАНИЯ К ПРОГРАММНОМУ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

5.1 Требования к среде функционирования

На СВТ, оснащенных СКЗИ «Dcrypt 1.0 v.2», должно использоваться только лицензионное программное обеспечение (далее – ПО) фирм–производителей, либо ПО, сертифицированное ФСБ России. Указанное ПО не должно содержать средств разработки и отладки приложений, а также возможностей, позволяющих оказывать воздействие на функционирование СКЗИ «Dcrypt 1.0 v.2». В случае потребностей организации, эксплуатирующей СКЗИ «Dcrypt 1.0 v.2», в использовании иного ПО, его применение должно быть санкционировано администратором безопасности. В любом случае, ПО не должно содержать в себе возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- использовать недокументированные фирмами-разработчиками функции.

Среда функционирования СКЗИ «Dcrypt 1.0 v.2» должна отвечать следующим требованиям:

- в BIOS СВТ с СКЗИ «Dcrypt 1.0 v.2» или в загрузчике ЭВМ должны быть заданы установки, исключающие возможность загрузки ОС, отличной от установленной на жестком диске – тем самым исключается возможность загрузки ОС с гибкого диска, привода CD-ROM и прочих нестандартных видов загрузки ОС, включая сетевую загрузку;
- должно быть исключено применение СВТ с BIOS и загрузчиком ЭВМ, в которых не предусмотрена возможность отключения сетевой загрузки ОС;
- в BIOS СВТ или в загрузчике ЭВМ должны быть заданы установки, запрещающие удаленное управление СВТ / ЭВМ при его наличии, и в этой связи не должны использоваться СВТ с BIOS и загрузчики ЭВМ, исключающие возможность отключения удаленного управления;

- средствами BIOS СВТ или загрузчика ЭВМ должна быть исключена возможность использования пользователем «горячих клавиш» для активации или отключения встроенных функциональных возможностей ПО BIOS или загрузчика ЭВМ;
- средствами BIOS СВТ или загрузчика ЭВМ должна быть исключена возможность:
  - отключения пользователями средств доверенной загрузки и средств защиты информации или модификации доверенного BIOS;
  - манипулирования критическими параметрами СВТ;
  - загрузки нештатных копий ОС;
  - перепрограммирования микросхем, программируемого постоянного запоминающего устройства с ПО BIOS и загрузчика ЭВМ;
- вход в BIOS СВТ или в загрузчик ЭВМ должен быть защищен паролем, который должен быть известен только администратору безопасности и быть отличным от пароля администратора безопасности для входа в ОС;
- средствами BIOS СВТ или загрузчика ЭВМ должна быть исключена возможность работы на СВТ с СКЗИ «Dcrypt 1.0 v.2», если во время начальной загрузки СВТ не проходят встроенные тесты;
- программные модули СКЗИ «Dcrypt 1.0 v.2» (прикладного ПО со встроенным изделием) должны быть доступны только по чтению / запуску, при этом в атрибутах файлов должна быть запрещена запись и модификация;
- администратором безопасности должно быть проведено опечатывание системного блока СВТ с установленным СКЗИ «Dcrypt 1.0 v.2», исключающее возможность несанкционированного изменения аппаратной части СВТ;
- при обновлении ОС необходимо произвести анализ изменений и обновить файлы с контрольными суммами;
- при эксплуатации средств доверенной загрузки или доверенного BIOS в составе СКЗИ «Dcrypt 1.0 v.2» должны выполняться требования, изложенные в формуляре, разработанном на изделие.

В условиях:

- когда информация, обрабатываемая СВТ с СКЗИ «Dcrypt 1.0 v.2», подлежит защите в соответствии с законодательством Российской Федерации;
- организации криптографической защиты информации в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;
- организации криптографической защиты, обрабатываемой СВТ с СКЗИ «Dcrypt 1.0 v.2» информации, в организациях независимо от их организационно-правовой формы и

формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд, для ограничения возможности влияния аппаратных компонентов СВТ на функционирование СКЗИ «Dcrypt 1.0 v.2» следует обеспечить соответствие ПО BIOS или загрузчика ЭВМ, на которых установлено СКЗИ «Dcrypt 1.0 v.2», требованиям «Временных методических рекомендаций к проведению исследований программного обеспечения BIOS по документированным возможностям».

6 ТРЕБОВАНИЯ ПО ЗАЩИТЕ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

При условии выполнения требований настоящего раздела изделие обеспечивает защиту конфиденциальной информации по классу КС1 (СКЗИ «Dcrypt 1.0 v.2» в исполнениях 1, 4, 16, 19, 31 и 34), по классу КС2 (СКЗИ «Dcrypt 1.0 v.2» в исполнениях 2, 5, 17, 20, 32, 35) и по классу КС3 (СКЗИ «Dcrypt 1.0 v.2» в исполнениях 3, 6, 18, 21, 33 и 36).

6.1 Принципы защиты информации от несанкционированного доступа

Защита информации от несанкционированного доступа (далее – НСД) в автоматизированной системе (далее – АС) обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер, к числу которых относятся:

- применение специальных программно-аппаратных средств защиты;
- организация системы контроля безопасности информации;
- физическая охрана СВТ и его компонентов;
- администрирование информационной безопасности;
- учет носителей информации;
- сигнализация о попытках нарушения защиты;
- периодическое тестирование технических и программных средств защиты;
- использование сертифицированных и лицензионных программных и технических средств.

Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе, при проведении ремонтных и регламентных работ.

Кроме того, защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или контролирующими органами.

Каждый исполнитель работ, будучи пользователем сети конфиденциальной связи, должен быть зарегистрирован у администратора службы безопасности.

В организации–пользователе СВТ с СКЗИ «Dcrypt 1.0 v.2» должно быть назначено специальное должностное лицо - администратор безопасности, функции которого должны заключаться в выполнении процедур установки ПО, настройки системного окружения, установки, настройки, обслуживания и обеспечения функционирования средств защиты.

Администратор безопасности должен иметь возможность доступа ко всей информации, обрабатываемой на СВТ.

Каждый исполнитель работ как пользователь сети конфиденциальной связи должен быть зарегистрирован у администратора безопасности.

В организации–пользователе СВТ с СКЗИ «Dcrypt 1.0 v.2» должны вестись журналы регистрации администраторов безопасности и пользователей (допускается ведение одного журнала для всей организации), в которые заносятся следующие данные:

- Ф.И.О. регистрируемого лица;
- наименование подразделения организации (при ведении общего журнала);
- степень допуска регистрируемого лица (администратор/пользователь);
- дата регистрации;
- дата окончания срока действия регистрации.

6.2 Организационные меры защиты информации от НСД

При использовании СКЗИ «Dcrypt 1.0 v.2» для защиты информации от НСД должны быть реализованы следующие организационные меры:

- должен быть исключён доступ к СВТ с установленным СКЗИ «Dcrypt 1.0 v.2» лицам, не ознакомленным с правилами пользования и не изучившим эксплуатационную документацию на СКЗИ «Dcrypt 1.0 v.2»;
- должно быть исключено осуществление несанкционированного администратором безопасности копирования ключевых носителей;
- должна быть исключена передача ключевых носителей лицам, к ним не допущенным;
- должно быть исключено использование ключевых носителей в режимах, не предусмотренных правилами пользования СКЗИ «Dcrypt 1.0 v.2», либо использование ключевых носителей сторонних СВТ;
- должна быть исключена запись на ключевые носители посторонней информации;
- должна быть исключена бесконтрольная эксплуатация СВТ с установленным СКЗИ «Dcrypt 1.0 v.2» после ввода ключевой информации, а при уходе пользователя от СВТ с установленным СКЗИ «Dcrypt 1.0 v.2» должно осуществляться автоматическое включение парольной заставки.

6.3 Организационно-технические меры защиты от НСД

При использовании СКЗИ «Dcrypt 1.0 v.2» должен быть реализован комплекс организационно-технических мер защиты информации от НСД, приведенный ниже.

1. Перед началом процесса установки ПО со встроенными модулями СКЗИ «Dcrypt 1.0 v.2», либо автономных программных модулей СКЗИ «Dcrypt 1.0 v.2» должен осуществляться контроль целостности устанавливаемого ПО утилитой «dmcrypt-util», входящей в состав СКЗИ «Dcrypt 1.0 v.2» (см. подраздел 3.1.1 «Обеспечение контроля целостности программного обеспечения» настоящих правил пользования).

2. При каждом запуске СВТ с установленным СКЗИ «Dcrypt 1.0 v.2» должен осуществляться контроль целостности ПО, входящего в состав СКЗИ «Dcrypt 1.0 v.2», а также самой ОС и всех исполняемых файлов, функционирующих совместно с изделием. При использовании СКЗИ «Dcrypt 1.0 v.2» для исполнений 1, 4, 16, 19, 31 и 34, контроль должен осуществляться утилитой «dmcrypt-ic», входящей в состав изделия, а при использовании СКЗИ «Dcrypt 1.0 v.2» для исполнений 2, 3, 5, 6, 17, 18, 20, 21, 32, 33, 35 и 36 — дополнительно средством доверенной загрузки или доверенным BIOS.

3. В случае обнаружения «посторонних» (не зарегистрированных) программ или нарушения целостности ПО СКЗИ «Dcrypt 1.0 v.2» работа должна быть прекращена.

4. Пользователь должен запускать только те приложения, которые разрешены администратором безопасности.

5. Для пользователя должен быть установлен пароль входа в систему длиной не менее 6 символов, реализуемый средствами BIOS СВТ или средствами загрузчика ЭВМ. Администратор безопасности должен периодически (не реже 1 раза в год) менять пароль входа в систему.

6. При использовании СКЗИ «Dcrypt 1.0 v.2» для исполнений 2, 3, 5, 6, 17, 18, 20, 21, 32, 33, 35 и 36 идентификация и аутентификация должны производиться средствами доверенной загрузки или доверенным BIOS. Пароль или идентификатор должен меняться не реже 1 раза в год. Число попыток ввода пароля одним пользователем не должно превышать 10.

7. Администратор безопасности должен сконфигурировать ОС, в среде которой планируется использовать СКЗИ «Dcrypt 1.0 v.2», и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- исключить использование нестандартных, измененных или отладочных версий ОС;
- исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации ОС и её настроек;
- на СВТ с СКЗИ «Dcrypt 1.0 v.2» должна быть установлена только одна операционная система;

- правом установки и настройки ОС и СКЗИ «Dcrypt 1.0 v.2» должен обладать только администратор безопасности;
- ОС должна быть настроена только для работы с СКЗИ «Dcrypt 1.0 v.2», а все неиспользуемые ресурсы ОС (протоколы, сервисы и т.п.) необходимо отключить;
- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.

8. Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам ОС:

- системный реестр;
- файлы и каталоги;
- временные файлы;
- журналы системы;
- файлы подкачки;
- кэшируемая информация (пароли и т.п.);
- отладочная информация,

а при определённых условиях предусмотреть меры, обеспечивающие полное удаление указанных ресурсов или их неиспользуемых частей.

Кроме того, по окончанию сеанса работы СКЗИ «Dcrypt 1.0 v.2» необходимо организовать удаление временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы изделия. Если это невыполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

Примечание: *в нашем случае под однопользовательским режимом подразумевается такой режим, при котором все пользователи данного СВТ имеют одинаковый комплект ключевой информации этой СВТ.*

9. Должно быть исключено попадание в ОС программ, позволяющих, пользуясь уязвимостями ОС, повышать предоставленные привилегии.

10. СВТ с установленным СКЗИ «Dcrypt 1.0 v.2» необходимо перезагружать 1 раз в 3 суток.

11. Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы на предмет их безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.

Кроме того, по окончанию сеанса работы СКЗИ «Dcrypt 1.0 v.2» необходимо организовать удаление временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы изделия. Если это невыполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

12. В случае подключения СВТ с установленным СКЗИ «Dcrypt 1.0 v.2» к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.

13. При использовании СКЗИ «Dcrypt 1.0 v.2» на СВТ, подключенных к общедоступным сетям связи, с целью исключения возможности НСД к системным ресурсам используемых ОС, а также к ПО, в окружении которого функционирует СКЗИ «Dcrypt 1.0 v.2», и к компонентам изделия со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN-сетей и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.

14. Должна быть организована и использована система аудита безопасности, а также осуществляться регулярный анализ результатов аудита.

15. Должна быть исключена возможность одновременной работы нескольких пользователей в ОС с работающим СКЗИ «Dcrypt 1.0 v.2» и загруженной ключевой информацией.

16. Для обеспечения замкнутой программной среды (далее – ЗПС) в СКЗИ «Dcrypt 1.0 v.2» для вариантов исполнения 3, 6, 18, 21, 33 и 36, сертифицированных по классам КС3, должны использоваться совместно АПМДЗ сертифицированные ФСБ по требованиям, предъявляемым к АПМДЗ и программные модули СКЗИ «Dcrypt 1.0 v.2» – «dmiced» и «tss_sys_hook.ko». Настройки ЗПС приведены в подразделе 3.4 «Описание и настройка замкнутой программной среды СКЗИ «Dcrypt 1.0 v.2» для исполнений 6, 21 и 36» и подразделе 3.5 «Описание и настройка замкнутой программной среды СКЗИ «Dcrypt 1.0 v.2» для исполнений 3, 18 и 33» настоящих правил пользования.

7 ТРЕБОВАНИЯ ПО ИСПОЛЬЗОВАНИЮ СКЗИ «Dcrypt 1.0 v.2» ИСП. 31, 32, 33, 34, 35 И 36 В ПРОГРАММНЫХ ПРОДУКТАХ

Разработка прикладного ПО с использованием СКЗИ «Dcrypt 1.0 v.2» для исполнений 31, 32, 33, 34, 35 и 36 может производиться без создания новых изделий и без проведения тематических исследований в случае использования вызовов функций, описанных в приложении «Приложение 1» к настоящим правилам пользования.

Прикладное ПО должно анализировать коды возврата функций библиотеки и прекращать выполнение операции при ошибочном коде возврата. Коды возврата функций библиотек приведены в документе «Средство криптографической защиты информации «Dcrypt 1.0 v.2». Руководство разработчика. 4012-006-61649217-18 01 92».

При использовании функций шифрования должны выполняться следующие требования:

- не должны использоваться алгоритмы выработки ключей (включая алгоритмы ключевого обмена), отличные от описанных в подразделе 3.8 «Учет ключевой информации» настоящего документа;
- при использовании режимов шифрования, требующих синхропосылки, необходимо применять протоколы, обеспечивающие надежную (без искажений) передачу синхропосылки получателю;
- необходимо обеспечить защиту от повторного использования синхропосылки с одним и тем же ключом шифрования;
- перед зашифрованием сообщение должно быть подписано ЭП которая должна быть проверена после расшифрования;
- необходимо уничтожать контекст шифрования сразу после использования.

При использовании функций, реализующих алгоритмы ЭП, должны выполняться следующие требования:

- при распространении открытых ключей ЭП необходимо применять методы, обеспечивающие целостность открытых ключей и аутентификацию их владельцев;
- при выработке / проверке ЭП необходимо использовать функции хеширования данных, реализованные в СКЗИ «Dcrypt 1.0 v.2»;
- при проведении процедур проверки ЭП необходимо выполнять аутентификацию владельца открытого ключа, а также проверку целостности и действительности ключа на момент проверки;
- необходимо уничтожать контекст ЭП сразу после использования.

При использовании функций, реализующих алгоритмы ключевого обмена, должны выполняться следующие требования:

- при распространении открытых ключей шифрования необходимо применять методы, обеспечивающие целостность открытых ключей и аутентификацию их владельцев;
- для исключения атаки «man–in–the–middle» необходимо применять меры, обеспечивающие аутентификацию общего ключа шифрования, выработанного с помощью процедур ключевого обмена;
- необходимо использовать меры, предотвращающие повторение ранее выполненных процедур ключевого обмена;
- необходимо уничтожать контекст ключевого обмена сразу после использования.

При использовании СКЗИ «Dcrypt 1.0 v.2» в СВТ без автоматического создания и (или) автоматической проверки ЭП ПО, изделие, использующее библиотеки, должно реализовывать следующие функции при создании ЭП:

- показывать лицу, подписывающему электронный документ, содержание информации, которую он подписывает;
- создавать ЭП только после подтверждения лицом, подписывающим электронный документ, операции по созданию ЭП;
- однозначно показывать, что ЭП создана;
- при проверке ЭП:
  - показывать содержание электронного документа, подписанного ЭП;
  - показывать информацию о внесении изменений в подписанный ЭП электронный документ;
  - указывать на лицо, с использованием ключа ЭП которого подписаны электронные документы.

Приложение 1

Перечень вызовов, использование которых при разработке прикладного ПО с применением СКЗИ «Dcrypt 1.0 v.2» возможно без проведения дополнительных тематических исследований

- std::string errorMessage() const;
- bool open(const std::string& seedId, const std::string& serialId);
- void close();
- bool generateKeyPair(const Pki::CertificateRequest* request, const std::string& userKeyPairId, const std::string& caKeyPairId);
- bool serializeKeyPair(const std::string& keyPairId, const char* passphrase, const std::string& outId);
- bool loadKeyPair(const std::string& keyPairId, const char* passphrase, const std::string& inId);
- bool loadCrl(const std::string& crlId, const std::string& inId, const std::string& caKeyPairId);
- bool serializeCertificate(const std::string& keyPairId, const std::string& outId);
- bool loadCertificate(const std::string& certificateId, const std::string& inId);
- bool encrypt(EncryptionProcessor* ep, const std::string& senderKeyPairId, const std::string& receiverCertificateId, const std::string& crlId, const std::string& caKeyPairId);
- bool decrypt(DecryptionProcessor* dp, const std::string& receiverKeyPairId, const std::string& senderCertificateId, const std::string& crlId, const std::string& caKeyPairId);
- bool calculateMac(CalculateMacProcessor* ep, const std::string& senderKeyPairId, const std::string& receiverCertificateId, const std::string& crlId, const std::string& caKeyPairId);
- bool verifyMac(VerifyMacProcessor* dp, const std::string& receiverKeyPairId, const std::string& senderCertificateId, const std::string& crlId, const std::string& caKeyPairId);
- bool sign(SignProcessor* sp, const std::string& senderKeyPairId, const std::string& crlId, const std::string& caKeyPairId);
- bool verify(VerifyProcessor* vp, const std::string& senderCertificateId, const std::string& crlId, const std::string& caKeyPairId);
- bool calculateHash(HashingProcessor* hp);
- bool compareHash(HashCompareProcessor* hp).

Подробная информация по применению библиотечных вызовов СКЗИ «Dcrypt 1.0 v.2» приведена в документе «Средство криптографической защиты информации «Dcrypt 1.0 v.2». Руководство разработчика. 4012-006-61649217-18 01 92».

Приложение 2

Перечень программных модулей (файлов) ОС, которые необходимо ставить на контроль целостности при использовании СКЗИ «Dcrypt 1.0 v.2» исп. 1, 2, 3, 16, 17, 18, 31, 32 и 33

C:\WINDOWS\SYSTEM32\ACPPAGE.DLL
C:\WINDOWS\SYSTEM32\ACTIONCENTER.DLL
C:\WINDOWS\SYSTEM32\ACTXPRXY.DLL
C:\WINDOWS\SYSTEM32\ADVAPI32.DLL
C:\WINDOWS\SYSTEM32\AEPIC.DLL
C:\WINDOWS\SYSTEM32\ALTTAB.DLL
C:\WINDOWS\SYSTEM32\APPHELP.DLL
C:\WINDOWS\SYSTEM32\APPHLPDM.DLL
C:\WINDOWS\SYSTEM32\APPINFO.DLL
C:\WINDOWS\SYSTEM32\ASPNET_COUNTERS.DLL
C:\WINDOWS\SYSTEM32\ATL.DLL
C:\WINDOWS\SYSTEM32\AUDIODG.EXE
C:\WINDOWS\SYSTEM32\AUDIOENG.DLL
C:\WINDOWS\SYSTEM32\AUDIOKSE.DLL
C:\WINDOWS\SYSTEM32\AUDIOSES.DLL
C:\WINDOWS\SYSTEM32\AUDIOSRV.DLL
C:\WINDOWS\SYSTEM32\AUTHUI.DLL
C:\WINDOWS\SYSTEM32\AUTHZ.DLL
C:\WINDOWS\SYSTEM32\AUTOCHK.EXE
C:\WINDOWS\SYSTEM32\AVRT.DLL
C:\WINDOWS\SYSTEM32\BASESRV.DLL
C:\WINDOWS\SYSTEM32\BATMETER.DLL
C:\WINDOWS\SYSTEM32\BCRYPT.DLL
C:\WINDOWS\SYSTEM32\BCRYPTPRIMITIVES.DLL
C:\WINDOWS\SYSTEM32\BFE.DLL
C:\WINDOWS\SYSTEM32\BIOCREDPROV.DLL
C:\WINDOWS\SYSTEM32\BITSPERF.DLL
C:\WINDOWS\SYSTEM32\BROWCLI.DLL
C:\WINDOWS\SYSTEM32\BROWSER.DLL
C:\WINDOWS\SYSTEM32\BTHPROPS.CPL
C:\WINDOWS\SYSTEM32\CATSRV.DLL

C:\WINDOWS\SYSTEM32\CATSRVPS.DLL

C:\WINDOWS\SYSTEM32\CATSRVUT.DLL

C:\WINDOWS\SYSTEM32\CDD.DLL

C:\WINDOWS\SYSTEM32\CERTCLI.DLL

C:\WINDOWS\SYSTEM32\CERTCREDPROVIDER.DLL

C:\WINDOWS\SYSTEM32\CERTENROLL.DLL

C:\WINDOWS\SYSTEM32\CERTPROP.DLL

C:\WINDOWS\SYSTEM32\CFGMGR32.DLL

C:\WINDOWS\SYSTEM32\CLBCATQ.DLL

C:\WINDOWS\SYSTEM32\CLUSAPI.DLL

C:\WINDOWS\SYSTEM32\CMD.EXE

C:\WINDOWS\SYSTEM32\CNGAUDIT.DLL

C:\WINDOWS\SYSTEM32\COMCTL32.DLL

C:\WINDOWS\SYSTEM32\COMDLG32.DLL

C:\WINDOWS\SYSTEM32\COMRES.DLL

C:\WINDOWS\SYSTEM32\COMSVCS.DLL

C:\WINDOWS\SYSTEM32\CONHOST.EXE

C:\WINDOWS\SYSTEM32\CONSENT.EXE

C:\WINDOWS\SYSTEM32\CPCNG.DLL

C:\WINDOWS\SYSTEM32\CPSSPAP.DLL

C:\WINDOWS\SYSTEM32\CREDSSP.DLL

C:\WINDOWS\SYSTEM32\CREDUI.DLL

C:\WINDOWS\SYSTEM32\CRYPT32.DLL

C:\WINDOWS\SYSTEM32\CRYPTBASE.DLL

C:\WINDOWS\SYSTEM32\CRYPTDLL.DLL

C:\WINDOWS\SYSTEM32\CRYPTNET.DLL

C:\WINDOWS\SYSTEM32\CRYPTSP.DLL

C:\WINDOWS\SYSTEM32\CRYPTSVC.DLL

C:\WINDOWS\SYSTEM32\CRYPTUI.DLL

C:\WINDOWS\SYSTEM32\CSCAPI.DLL

C:\WINDOWS\SYSTEM32\CSCDLL.DLL

C:\WINDOWS\SYSTEM32\CSCOBJ.DLL

C:\WINDOWS\SYSTEM32\CSCSVC.DLL

C:\WINDOWS\SYSTEM32\CSCUI.DLL

C:\WINDOWS\SYSTEM32\CSRSRV.DLL

C:\WINDOWS\SYSTEM32\CSRSS.EXE

C:\WINDOWS\SYSTEM32\D3D10_1.DLL

C:\WINDOWS\SYSTEM32\D3D10_1CORE.DLL

C:\WINDOWS\SYSTEM32\D3D11.DLL
C:\WINDOWS\SYSTEM32\DAVCLNT.DLL
C:\WINDOWS\SYSTEM32\DAVHLPR.DLL
C:\WINDOWS\SYSTEM32\DBGHELP.DLL
C:\WINDOWS\SYSTEM32\DEVICECENTER.DLL
C:\WINDOWS\SYSTEM32\DEVOBJ.DLL
C:\WINDOWS\SYSTEM32\DEVRTL.DLL
C:\WINDOWS\SYSTEM32\DHCPCORE.DLL
C:\WINDOWS\SYSTEM32\DHCPCORE6.DLL
C:\WINDOWS\SYSTEM32\DHCPCSVC.DLL
C:\WINDOWS\SYSTEM32\DHCPCSVC6.DLL
C:\WINDOWS\SYSTEM32\DIAGPERF.DLL
C:\WINDOWS\SYSTEM32\DIFXAPI.DLL
C:\WINDOWS\SYSTEM32\DIMSJOB.DLL
C:\WINDOWS\SYSTEM32\DLLHOST.EXE
C:\WINDOWS\SYSTEM32\DNSAPI.DLL
C:\WINDOWS\SYSTEM32\DNSEXT.DLL
C:\WINDOWS\SYSTEM32\DNSRSLVR.DLL
C:\WINDOWS\SYSTEM32\DOT3API.DLL
C:\WINDOWS\SYSTEM32\DPS.DLL
C:\WINDOWS\SYSTEM32\DRIVERS\AFD.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\AGILEVPN.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\BEEP.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\BLBDRIVE.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\BOWSER.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\CDROM.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\CMBATT.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\COMPOSITEBUS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\CPROCTRL.4.0.0.17.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\CRASHDMP.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\CSC.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\DFSC.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\DISCACHE.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\DISKDUMP.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\DRMK.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\DUMPFVE.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\DXAPI.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\DXGKRNL.SYS

C:\WINDOWS\SYSTEM32\DRIVERS\DXGMMS1.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\E1G6032E.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\HDAUDBUS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\HDAUDIO.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\HIDCLASS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\HIDPARSE.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\HIDUSB.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\HTTP.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\I8042PRT.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\INTELPPM.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\KBDCLASS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\KS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\KSTHUNK.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\LLTDIO.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\LSI_SAS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\LUAFV.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\MONITOR.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\MOUCLASS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\MOUHID.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\MPSDRV.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\MRXSMB.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\MRXSMB10.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\MRXSMB20.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\MSFS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\MSSMBIOS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\NDISTAPI.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\NDISWAN.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\NDPROXY.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\NETBIOS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\NETBT.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\NPFS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\NSIPROXY.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\NULL.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\PACER.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\PEAUTH.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\PORTCLS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\RASL2TP.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\RASPPPOE.SYS

C:\WINDOWS\SYSTEM32\DRIVERS\RASPPTP.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\RASSSTP.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\RDBSS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\RDPBUS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\RDPCDD.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\RDPDR.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\RDPENCDD.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\RDPREFMP.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\RDPWD.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\RSPNDR.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\SERENUM.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\SERIAL.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\SRV.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\SRV2.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\SRVNET.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\SWENUM.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\TCPIPREG.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\TDI.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\TDTCP.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\TDX.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\TERMDD.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\TSSECSRV.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\TUNNEL.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\UMBUS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\USBCCGP.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\USBD.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\USBEHCI.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\USBHUB.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\USBPORT.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\USBUHCI.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\VGA.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\VIDEOPRT.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\VM3DMP.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\VMHGFS.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\VMMEMCTL.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\VMMOUSE.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\VMRAWDSK.SYS
C:\WINDOWS\SYSTEM32\DRIVERS\VMUSBMOUSE.SYS

C:\WINDOWS\SYSTEM32\DRIVERS\WANARP.SYS

C:\WINDOWS\SYSTEM32\DRIVERS\WATCHDOG.SYS

C:\WINDOWS\SYSTEM32\DRIVERS\WFPLWF.SYS

C:\WINDOWS\SYSTEM32\DRIVERS\WS2IFSL.SYS

C:\WINDOWS\SYSTEM32\DRPROV.DLL

C:\WINDOWS\SYSTEM32\DSROLE.DLL

C:\WINDOWS\SYSTEM32\DUI70.DLL

C:\WINDOWS\SYSTEM32\DUSER.DLL

C:\WINDOWS\SYSTEM32\DWM.EXE

C:\WINDOWS\SYSTEM32\DWMAPI.DLL

C:\WINDOWS\SYSTEM32\DWMCORE.DLL

C:\WINDOWS\SYSTEM32\DWMREDIR.DLL

C:\WINDOWS\SYSTEM32\DXGI.DLL

C:\WINDOWS\SYSTEM32\DXP.DLL

C:\WINDOWS\SYSTEM32\EAPPCFG.DLL

C:\WINDOWS\SYSTEM32\EAPPPRXY.DLL

C:\WINDOWS\SYSTEM32\EFSLSAEXT.DLL

C:\WINDOWS\SYSTEM32\EHSTORAPI.DLL

C:\WINDOWS\SYSTEM32\EHSTORSHELL.DLL

C:\WINDOWS\SYSTEM32\ES.DLL

C:\WINDOWS\SYSTEM32\ESENT.DLL

C:\WINDOWS\SYSTEM32\ESENTPRF.DLL

C:\WINDOWS\SYSTEM32\EXPLORERFRAME.DLL

C:\WINDOWS\SYSTEM32\FDPNP.DLL

C:\WINDOWS\SYSTEM32\FDRESPUB.DLL

C:\WINDOWS\SYSTEM32\FIREWALLAPI.DLL

C:\WINDOWS\SYSTEM32\FLTLIB.DLL

C:\WINDOWS\SYSTEM32\FNTCACHE.DLL

C:\WINDOWS\SYSTEM32\FONTSUB.DLL

C:\WINDOWS\SYSTEM32\FRAMEDYNOS.DLL

C:\WINDOWS\SYSTEM32\FUNDISC.DLL

C:\WINDOWS\SYSTEM32\FVEAPI.DLL

C:\WINDOWS\SYSTEM32\FVECERTS.DLL

C:\WINDOWS\SYSTEM32\FWPUCLNT.DLL

C:\WINDOWS\SYSTEM32\FWREMOTESVR.DLL

C:\WINDOWS\SYSTEM32\FXSAPI.DLL

C:\WINDOWS\SYSTEM32\FXSMON.DLL

C:\WINDOWS\SYSTEM32\FXSRESM.DLL

C:\WINDOWS\SYSTEM32\FXSST.DLL

C:\WINDOWS\SYSTEM32\GAMEUX.DLL

C:\WINDOWS\SYSTEM32\GDI32.DLL

C:\WINDOWS\SYSTEM32\GPAPI.DLL

C:\WINDOWS\SYSTEM32\GPSVC.DLL

C:\WINDOWS\SYSTEM32\HGCPL.DLL

C:\WINDOWS\SYSTEM32\HID.DLL

C:\WINDOWS\SYSTEM32\HNETCFG.DLL

C:\WINDOWS\SYSTEM32\HOTSTARTUSERAGENT.DLL

C:\WINDOWS\SYSTEM32\HTTPAPI.DLL

C:\WINDOWS\SYSTEM32\ICAAPI.DLL

C:\WINDOWS\SYSTEM32\ICMP.DLL

C:\WINDOWS\SYSTEM32\ICONCODECSERVICE.DLL

C:\WINDOWS\SYSTEM32\IDSTORE.DLL

C:\WINDOWS\SYSTEM32\IEFRAME.DLL

C:\WINDOWS\SYSTEM32\IERTUTIL.DLL

C:\WINDOWS\SYSTEM32\IKEEXT.DLL

C:\WINDOWS\SYSTEM32\IMAGEHLP.DLL

C:\WINDOWS\SYSTEM32\IMAPI2.DLL

C:\WINDOWS\SYSTEM32\IMM32.DLL

C:\WINDOWS\SYSTEM32\INETPP.DLL

C:\WINDOWS\SYSTEM32\IPHLPAPI.DLL

C:\WINDOWS\SYSTEM32\IPHLPSVC.DLL

C:\WINDOWS\SYSTEM32\IPSECSVC.DLL

C:\WINDOWS\SYSTEM32\KBDRU.DLL

C:\WINDOWS\SYSTEM32\KBDUS.DLL

C:\WINDOWS\SYSTEM32\KERBEROS.DLL

C:\WINDOWS\SYSTEM32\KERNEL32.DLL

C:\WINDOWS\SYSTEM32\KERNELBASE.DLL

C:\WINDOWS\SYSTEM32\KSUSER.DLL

C:\WINDOWS\SYSTEM32\KTMW32.DLL

C:\WINDOWS\SYSTEM32\LINKINFO.DLL

C:\WINDOWS\SYSTEM32\LMHSVC.DLL

C:\WINDOWS\SYSTEM32\LOADPERF.DLL

C:\WINDOWS\SYSTEM32\LOCALSPL.DLL

C:\WINDOWS\SYSTEM32\LOGONCLI.DLL

C:\WINDOWS\SYSTEM32\LOGONUI.EXE

C:\WINDOWS\SYSTEM32\LPK.DLL

C:\WINDOWS\SYSTEM32\LSASRV.DLL
C:\WINDOWS\SYSTEM32\LSASS.EXE
C:\WINDOWS\SYSTEM32\LSM.EXE
C:\WINDOWS\SYSTEM32\LSMPROXY.DLL
C:\WINDOWS\SYSTEM32\MAPI32.DLL
C:\WINDOWS\SYSTEM32\MFCSUBS.DLL
C:\WINDOWS\SYSTEM32\MFPLAT.DLL
C:\WINDOWS\SYSTEM32\MIDIMAP.DLL
C:\WINDOWS\SYSTEM32\MMCSS.DLL
C:\WINDOWS\SYSTEM32\MMDEVAPI.DLL
C:\WINDOWS\SYSTEM32\MPR.DLL
C:\WINDOWS\SYSTEM32\MPRAPI.DLL
C:\WINDOWS\SYSTEM32\MPSSVC.DLL
C:\WINDOWS\SYSTEM32\MSACM32.DLL
C:\WINDOWS\SYSTEM32\MSACM32.DRV
C:\WINDOWS\SYSTEM32\MSASN1.DLL
C:\WINDOWS\SYSTEM32\MSCOREE.DLL
C:\WINDOWS\SYSTEM32\MSCTF.DLL
C:\WINDOWS\SYSTEM32\MSCTFMONITOR.DLL
C:\WINDOWS\SYSTEM32\MSDTC.EXE
C:\WINDOWS\SYSTEM32\MSDTCLOG.DLL
C:\WINDOWS\SYSTEM32\MSDTCPRX.DLL
C:\WINDOWS\SYSTEM32\MSDTCTM.DLL
C:\WINDOWS\SYSTEM32\MSDTCUIU.DLL
C:\WINDOWS\SYSTEM32\MSDTCVSP1RES.DLL
C:\WINDOWS\SYSTEM32\MSFTEDIT.DLL
C:\WINDOWS\SYSTEM32\MSI.DLL
C:\WINDOWS\SYSTEM32\MSIDLE.DLL
C:\WINDOWS\SYSTEM32\MSIMG32.DLL
C:\WINDOWS\SYSTEM32\MSLS31.DLL
C:\WINDOWS\SYSTEM32\MSPRIVS.DLL
C:\WINDOWS\SYSTEM32\MSSCNTRS.DLL
C:\WINDOWS\SYSTEM32\MSSHOOKS.DLL
C:\WINDOWS\SYSTEM32\MSSPRXY.DLL
C:\WINDOWS\SYSTEM32\MSSRCH.DLL
C:\WINDOWS\SYSTEM32\MSSVP.DLL
C:\WINDOWS\SYSTEM32\MSTASK.DLL
C:\WINDOWS\SYSTEM32\MSUTB.DLL

C:\WINDOWS\SYSTEM32\MSV1_0.DLL

C:\WINDOWS\SYSTEM32\MSVCP140.DLL

C:\WINDOWS\SYSTEM32\MSVCR120_CLR0400.DLL

C:\WINDOWS\SYSTEM32\MSVCRT.DLL

C:\WINDOWS\SYSTEM32\MSWSOCK.DLL

C:\WINDOWS\SYSTEM32\MSXML6.DLL

C:\WINDOWS\SYSTEM32\MTXCLU.DLL

C:\WINDOWS\SYSTEM32\MTXOCI.DLL

C:\WINDOWS\SYSTEM32\MYDOCS.DLL

C:\WINDOWS\SYSTEM32\NAPINSP.DLL

C:\WINDOWS\SYSTEM32\NATURALLANGUAGE6.DLL

C:\WINDOWS\SYSTEM32\NCI.DLL

C:\WINDOWS\SYSTEM32\NCOBJAPI.DLL

C:\WINDOWS\SYSTEM32\NCRYPT.DLL

C:\WINDOWS\SYSTEM32\NCSI.DLL

C:\WINDOWS\SYSTEM32\NEGOEXTS.DLL

C:\WINDOWS\SYSTEM32\NETAPI32.DLL

C:\WINDOWS\SYSTEM32\NETCFGX.DLL

C:\WINDOWS\SYSTEM32\NETFXPERF.DLL

C:\WINDOWS\SYSTEM32\NETJOIN.DLL

C:\WINDOWS\SYSTEM32\NETLOGON.DLL

C:\WINDOWS\SYSTEM32\NETMAN.DLL

C:\WINDOWS\SYSTEM32\NETMSG.DLL

C:\WINDOWS\SYSTEM32\NETPROFM.DLL

C:\WINDOWS\SYSTEM32\NETSHELL.DLL

C:\WINDOWS\SYSTEM32\NETUTILS.DLL

C:\WINDOWS\SYSTEM32\NETWORKEXPLORER.DLL

C:\WINDOWS\SYSTEM32\NLAAPI.DLL

C:\WINDOWS\SYSTEM32\NLASVC.DLL

C:\WINDOWS\SYSTEM32\NLSDATA0009.DLL

C:\WINDOWS\SYSTEM32\NLSDATA0019.DLL

C:\WINDOWS\SYSTEM32\NLSLEXICONS0009.DLL

C:\WINDOWS\SYSTEM32\NLSLEXICONS0019.DLL

C:\WINDOWS\SYSTEM32\NORMALIZ.DLL

C:\WINDOWS\SYSTEM32\NPMPROXY.DLL

C:\WINDOWS\SYSTEM32\NRPSRV.DLL

C:\WINDOWS\SYSTEM32\NSI.DLL

C:\WINDOWS\SYSTEM32\NSISVC.DLL

C:\WINDOWS\SYSTEM32\NTDLL.DLL
C:\WINDOWS\SYSTEM32\NTDSAPI.DLL
C:\WINDOWS\SYSTEM32\NTLANMAN.DLL
C:\WINDOWS\SYSTEM32\NTMARTA.DLL
C:\WINDOWS\SYSTEM32\NTSHRUI.DLL
C:\WINDOWS\SYSTEM32\ODBC32.DLL
C:\WINDOWS\SYSTEM32\ODBCINT.DLL
C:\WINDOWS\SYSTEM32\OLE32.DLL
C:\WINDOWS\SYSTEM32\OLEACC.DLL
C:\WINDOWS\SYSTEM32\OLEAUT32.DLL
C:\WINDOWS\SYSTEM32\ONEX.DLL
C:\WINDOWS\SYSTEM32\PAUTOENR.DLL
C:\WINDOWS\SYSTEM32\PCASVC.DLL
C:\WINDOWS\SYSTEM32\PCWUM.DLL
C:\WINDOWS\SYSTEM32\PDH.DLL
C:\WINDOWS\SYSTEM32\PEERDIST.DLL
C:\WINDOWS\SYSTEM32\PERFCTRS.DLL
C:\WINDOWS\SYSTEM32\PERFDISK.DLL
C:\WINDOWS\SYSTEM32\PERFNET.DLL
C:\WINDOWS\SYSTEM32\PERFOS.DLL
C:\WINDOWS\SYSTEM32\PERFPROC.DLL
C:\WINDOWS\SYSTEM32\PERFTRACK.DLL
C:\WINDOWS\SYSTEM32\PERFTS.DLL
C:\WINDOWS\SYSTEM32\PKU2U.DLL
C:\WINDOWS\SYSTEM32\PLAYSNDSRV.DLL
C:\WINDOWS\SYSTEM32\PNIDUI.DLL
C:\WINDOWS\SYSTEM32\PNPTS.DLL
C:\WINDOWS\SYSTEM32\PNRPNSP.DLL
C:\WINDOWS\SYSTEM32\PORTABLEDEVICEAPI.DLL
C:\WINDOWS\SYSTEM32\PORTABLEDEVICECONNECTAPI.DLL
C:\WINDOWS\SYSTEM32\PORTABLEDEVICETYPES.DLL
C:\WINDOWS\SYSTEM32\POWERTRACKER.DLL
C:\WINDOWS\SYSTEM32\POWRPROF.DLL
C:\WINDOWS\SYSTEM32\PRINTISOLATIONPROXY.DLL
C:\WINDOWS\SYSTEM32\PRNFLDR.DLL
C:\WINDOWS\SYSTEM32\PROFAPI.DLL
C:\WINDOWS\SYSTEM32\PROFSVC.DLL
C:\WINDOWS\SYSTEM32\PROPSYS.DLL

C:\WINDOWS\SYSTEM32\PROVSVC.DLL
C:\WINDOWS\SYSTEM32\PSAPI.DLL
C:\WINDOWS\SYSTEM32\QAGENT.DLL
C:\WINDOWS\SYSTEM32\QUTIL.DLL
C:\WINDOWS\SYSTEM32\RADARDT.DLL
C:\WINDOWS\SYSTEM32\RASADHLP.DLL
C:\WINDOWS\SYSTEM32\RASAPI32.DLL
C:\WINDOWS\SYSTEM32\RASCTRS.DLL
C:\WINDOWS\SYSTEM32\RASDLG.DLL
C:\WINDOWS\SYSTEM32\RASMAN.DLL
C:\WINDOWS\SYSTEM32\RASPLAP.DLL
C:\WINDOWS\SYSTEM32\RDPCOREKMTS.DLL
C:\WINDOWS\SYSTEM32\RDPWSX.DLL
C:\WINDOWS\SYSTEM32\REGAPI.DLL
C:\WINDOWS\SYSTEM32\RESUTILS.DLL
C:\WINDOWS\SYSTEM32\RPCEPMAP.DLL
C:\WINDOWS\SYSTEM32\RPCRT4.DLL
C:\WINDOWS\SYSTEM32\RPCRTREMOTE.DLL
C:\WINDOWS\SYSTEM32\RPCSS.DLL
C:\WINDOWS\SYSTEM32\RSAENH.DLL
C:\WINDOWS\SYSTEM32\RTUTILS.DLL
C:\WINDOWS\SYSTEM32\SAMCLI.DLL
C:\WINDOWS\SYSTEM32\SAMLIB.DLL
C:\WINDOWS\SYSTEM32\SAMSRV.DLL
C:\WINDOWS\SYSTEM32\SCARDSVR.DLL
C:\WINDOWS\SYSTEM32\SCECLI.DLL
C:\WINDOWS\SYSTEM32\SCESRV.DLL
C:\WINDOWS\SYSTEM32\SCEXT.DLL
C:\WINDOWS\SYSTEM32\SCHANNEL.DLL
C:\WINDOWS\SYSTEM32\SCHEDSVC.DLL
C:\WINDOWS\SYSTEM32\SEARCHFILTERHOST.EXE
C:\WINDOWS\SYSTEM32\SEARCHFOLDER.DLL
C:\WINDOWS\SYSTEM32\SEARCHINDEXER.EXE
C:\WINDOWS\SYSTEM32\SEARCHPROTOCOLHOST.EXE
C:\WINDOWS\SYSTEM32\SECHOST.DLL
C:\WINDOWS\SYSTEM32\SECUR32.DLL
C:\WINDOWS\SYSTEM32\SENDMAIL.DLL
C:\WINDOWS\SYSTEM32\SENS.DLL

C:\WINDOWS\SYSTEM32\SERVICES.EXE

C:\WINDOWS\SYSTEM32\SESSENV.DLL

C:\WINDOWS\SYSTEM32\SETUPAPI.DLL

C:\WINDOWS\SYSTEM32\SFC.DLL

C:\WINDOWS\SYSTEM32\SFC_OS.DLL

C:\WINDOWS\SYSTEM32\SHACCT.DLL

C:\WINDOWS\SYSTEM32\SHDOCVW.DLL

C:\WINDOWS\SYSTEM32\SHELL32.DLL

C:\WINDOWS\SYSTEM32\SHFOLDER.DLL

C:\WINDOWS\SYSTEM32\SHLWAPI.DLL

C:\WINDOWS\SYSTEM32\SHSVCS.DLL

C:\WINDOWS\SYSTEM32\SLC.DLL

C:\WINDOWS\SYSTEM32\SMARTCARDCREDENTIALPROVIDER.DLL

C:\WINDOWS\SYSTEM32\SMSS.EXE

C:\WINDOWS\SYSTEM32\SNDVOLSSO.DLL

C:\WINDOWS\SYSTEM32\SNMPAPI.DLL

C:\WINDOWS\SYSTEM32\SPINF.DLL

C:\WINDOWS\SYSTEM32\SPOOLSS.DLL

C:\WINDOWS\SYSTEM32\SPOOLSV.EXE

C:\WINDOWS\SYSTEM32\SPOOL\PRTPROCS\X64\TPWINPRN.DLL

C:\WINDOWS\SYSTEM32\SPOOL\PRTPROCS\X64\WINPRINT.DLL

C:\WINDOWS\SYSTEM32\SQMAPI.DLL

C:\WINDOWS\SYSTEM32\SRCHADMIN.DLL

C:\WINDOWS\SYSTEM32\SRVCLI.DLL

C:\WINDOWS\SYSTEM32\SRVSVC.DLL

C:\WINDOWS\SYSTEM32\SSCORE.DLL

C:\WINDOWS\SYSTEM32\SSDPAPI.DLL

C:\WINDOWS\SYSTEM32\SSPICLI.DLL

C:\WINDOWS\SYSTEM32\SSPISRV.DLL

C:\WINDOWS\SYSTEM32\STOBJECT.DLL

C:\WINDOWS\SYSTEM32\STRUCTUREDQUERY.DLL

C:\WINDOWS\SYSTEM32\SVCHOST.EXE

C:\WINDOWS\SYSTEM32\SXS.DLL

C:\WINDOWS\SYSTEM32\SXSSRV.DLL

C:\WINDOWS\SYSTEM32\SYNCCENTER.DLL

C:\WINDOWS\SYSTEM32\SYNCENG.DLL

C:\WINDOWS\SYSTEM32\SYNCREG.DLL

C:\WINDOWS\SYSTEM32\SYNCUI.DLL

C:\WINDOWS\SYSTEM32\SYSMAIN.DLL
C:\WINDOWS\SYSTEM32\SYSNTFY.DLL
C:\WINDOWS\SYSTEM32\TAPIPERF.DLL
C:\WINDOWS\SYSTEM32\TASKCOMP.DLL
C:\WINDOWS\SYSTEM32\TASKHOST.EXE
C:\WINDOWS\SYSTEM32\TASKSCHD.DLL
C:\WINDOWS\SYSTEM32\TBS.DLL
C:\WINDOWS\SYSTEM32\TCPMON.DLL
C:\WINDOWS\SYSTEM32\TDH.DLL
C:\WINDOWS\SYSTEM32\TERMSRV.DLL
C:\WINDOWS\SYSTEM32\THEMESERVICE.DLL
C:\WINDOWS\SYSTEM32\THUMBCACHE.DLL
C:\WINDOWS\SYSTEM32\TIMEDATE.CPL
C:\WINDOWS\SYSTEM32\TLSCSP.DLL
C:\WINDOWS\SYSTEM32\TPRDPW32.DLL
C:\WINDOWS\SYSTEM32\TPVMMON.DLL
C:\WINDOWS\SYSTEM32\TPVMW32.DLL
C:\WINDOWS\SYSTEM32\TQUERY.DLL
C:\WINDOWS\SYSTEM32\TRKWKS.DLL
C:\WINDOWS\SYSTEM32\TSDDD.DLL
C:\WINDOWS\SYSTEM32\TSPKG.DLL
C:\WINDOWS\SYSTEM32\TWEXT.DLL
C:\WINDOWS\SYSTEM32\TXFLOG.DLL
C:\WINDOWS\SYSTEM32\UBPM.DLL
C:\WINDOWS\SYSTEM32\UCRTBASE.DLL
C:\WINDOWS\SYSTEM32\UDWM.DLL
C:\WINDOWS\SYSTEM32\UIANIMATION.DLL
C:\WINDOWS\SYSTEM32\UIAUTOMATIONCORE.DLL
C:\WINDOWS\SYSTEM32\UMB.DLL
C:\WINDOWS\SYSTEM32\UMPNPMGR.DLL
C:\WINDOWS\SYSTEM32\UMPO.DLL
C:\WINDOWS\SYSTEM32\UMRDP.DLL
C:\WINDOWS\SYSTEM32\URLMON.DLL
C:\WINDOWS\SYSTEM32\USBMON.DLL
C:\WINDOWS\SYSTEM32\USBPERF.DLL
C:\WINDOWS\SYSTEM32\USER32.DLL
C:\WINDOWS\SYSTEM32\USERENV.DLL
C:\WINDOWS\SYSTEM32\USERINIT.EXE

C:\WINDOWS\SYSTEM32\USP10.DLL
C:\WINDOWS\SYSTEM32\UTILDLL.DLL
C:\WINDOWS\SYSTEM32\UXINIT.DLL
C:\WINDOWS\SYSTEM32\UXSMS.DLL
C:\WINDOWS\SYSTEM32\UXTHEME.DLL
C:\WINDOWS\SYSTEM32\VAULTCLI.DLL
C:\WINDOWS\SYSTEM32\VAULTCREDPROVIDER.DLL
C:\WINDOWS\SYSTEM32\VCRUNTIME140.DLL
C:\WINDOWS\SYSTEM32\VERSION.DLL
C:\WINDOWS\SYSTEM32\VIRTDISK.DLL
C:\WINDOWS\SYSTEM32\VM3DUM64_10.DLL
C:\WINDOWS\SYSTEM32\VMHGFS.DLL
C:\WINDOWS\SYSTEM32\VMICTIMEPROVIDER.DLL
C:\WINDOWS\SYSTEM32\VPNIKEAPI.DLL
C:\WINDOWS\SYSTEM32\VSOCKLIB.DLL
C:\WINDOWS\SYSTEM32\VSSAPI.DLL
C:\WINDOWS\SYSTEM32\VSSTRACE.DLL
C:\WINDOWS\SYSTEM32\VSSVC.EXE
C:\WINDOWS\SYSTEM32\VSS_PS.DLL
C:\WINDOWS\SYSTEM32\W32TIME.DLL
C:\WINDOWS\SYSTEM32\WBEMCOMN.DLL
C:\WINDOWS\SYSTEM32\WBEM\CIMWIN32.DLL
C:\WINDOWS\SYSTEM32\WBEM\ESSCLI.DLL
C:\WINDOWS\SYSTEM32\WBEM\FASTPROX.DLL
C:\WINDOWS\SYSTEM32\WBEM\REPDRVFS.DLL
C:\WINDOWS\SYSTEM32\WBEM\WBEMCORE.DLL
C:\WINDOWS\SYSTEM32\WBEM\WBEMESS.DLL
C:\WINDOWS\SYSTEM32\WBEM\WBEMPROX.DLL
C:\WINDOWS\SYSTEM32\WBEM\WBEMSVC.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIAPRPL.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIAPSRV.EXE
C:\WINDOWS\SYSTEM32\WBEM\WMIDCPRV.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIPERFCLASS.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIPERFINST.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIPROV.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIPRVSD.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIPRVSE.EXE
C:\WINDOWS\SYSTEM32\WBEM\WMISVC.DLL

C:\WINDOWS\SYSTEM32\WBEM\WMIUTILS.DLL

C:\WINDOWS\SYSTEM32\WDI.DLL

C:\WINDOWS\SYSTEM32\WDIASQMMODULE.DLL

C:\WINDOWS\SYSTEM32\WDIGEST.DLL

C:\WINDOWS\SYSTEM32\WDMAUD.DRV

C:\WINDOWS\SYSTEM32\WDSCORE.DLL

C:\WINDOWS\SYSTEM32\WEBCHECK.DLL

C:\WINDOWS\SYSTEM32\WEBIO.DLL

C:\WINDOWS\SYSTEM32\WEBSERVICES.DLL

C:\WINDOWS\SYSTEM32\WER.DLL

C:\WINDOWS\SYSTEM32\WEVTAPI.DLL

C:\WINDOWS\SYSTEM32\WEVTSVC.DLL

C:\WINDOWS\SYSTEM32\WFAPIGP.DLL

C:\WINDOWS\SYSTEM32\WIARPC.DLL

C:\WINDOWS\SYSTEM32\WIN32K.SYS

C:\WINDOWS\SYSTEM32\WIN32SPL.DLL

C:\WINDOWS\SYSTEM32\WINBIO.DLL

C:\WINDOWS\SYSTEM32\WINBRAND.DLL

C:\WINDOWS\SYSTEM32\WINDOWSCODECS.DLL

C:\WINDOWS\SYSTEM32\WINHTTP.DLL

C:\WINDOWS\SYSTEM32\WININET.DLL

C:\WINDOWS\SYSTEM32\WININIT.EXE

C:\WINDOWS\SYSTEM32\WINLOGON.EXE

C:\WINDOWS\SYSTEM32\WINMM.DLL

C:\WINDOWS\SYSTEM32\WINNSI.DLL

C:\WINDOWS\SYSTEM32\WINRNR.DLL

C:\WINDOWS\SYSTEM32\WINSCARD.DLL

C:\WINDOWS\SYSTEM32\WINSPOOL.DRV

C:\WINDOWS\SYSTEM32\WINSRV.DLL

C:\WINDOWS\SYSTEM32\WINSTA.DLL

C:\WINDOWS\SYSTEM32\WINTRUST.DLL

C:\WINDOWS\SYSTEM32\WKSCLI.DLL

C:\WINDOWS\SYSTEM32\WKSSVC.DLL й

C:\WINDOWS\SYSTEM32\WLANAPI.DLL

C:\WINDOWS\SYSTEM32\WLANHLP.DLL

C:\WINDOWS\SYSTEM32\WLANUTIL.DLL

C:\WINDOWS\SYSTEM32\WLDAP32.DLL

C:\WINDOWS\SYSTEM32\WLS0WNDH.DLL

C:\WINDOWS\SYSTEM32\WMALFXGFXDSP.DLL

C:\WINDOWS\SYSTEM32\WMSGAPI.DLL

C:\WINDOWS\SYSTEM32\WPDBUSENUM.DLL

C:\WINDOWS\SYSTEM32\WPDSHEXT.DLL

C:\WINDOWS\SYSTEM32\WPDSHSERVICEOBJ.DLL

C:\WINDOWS\SYSTEM32\WS2_32.DLL

C:\WINDOWS\SYSTEM32\WSCAPI.DLL

C:\WINDOWS\SYSTEM32\WSCISVIF.DLL

C:\WINDOWS\SYSTEM32\WSCPROXYSTUB.DLL

C:\WINDOWS\SYSTEM32\WSDAPI.DLL

C:\WINDOWS\SYSTEM32\WSDMON.DLL

C:\WINDOWS\SYSTEM32\WSHIP6.DLL

C:\WINDOWS\SYSTEM32\WSHTCPIP.DLL

C:\WINDOWS\SYSTEM32\WSNMP32.DLL

C:\WINDOWS\SYSTEM32\WSOCK32.DLL

C:\WINDOWS\SYSTEM32\WTSAPI32.DLL

C:\WINDOWS\SYSTEM32\WWANAPI.DLL

C:\WINDOWS\SYSTEM32\WWAPI.DLL

C:\WINDOWS\SYSTEM32\XMLLITE.DLL

C:\WINDOWS\SYSTEM32\XOLEHLP.DLL

C:\WINDOWS\SYSTEM32\ZIPFLDR.DLL