

УТВЕРЖДЕН

ФРКЕ.00106-03 99 01 ПП-ЛУ



Средство криптографической защиты информации

ViPNet CSP 4.2

Правила пользования

ФРКЕ.00106-03 99 01 ПП

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

2016

infotecs

Содержание

1	Общие положения	4
1.1	Состав программных средств СКЗИ ViPNet CSP	4
1.2	Требования к составу технических средств и операционным системам.....	5
1.3	Дополнительное ПО	6
2	Требования к размещению технических средств	7
3	Установка и эксплуатация СКЗИ ViPNet CSP	10
3.1	Порядок распространения и учета СКЗИ ViPNet CSP	10
3.2	Требования по установке СКЗИ ViPNet CSP, а также общесистемного и специального ПО на компьютер	11
3.3	Установка СКЗИ ViPNet CSP	12
3.4	Требования к настройкам СКЗИ ViPNet CSP	14
3.5	Ввод в эксплуатацию	14
4	Эксплуатация СКЗИ ViPNet CSP	15
4.1	Контроль целостности компьютера и ПО	15
4.2	Обновление ПО СКЗИ ViPNet CSP	18
4.3	Встраивание в приложения	18
4.3.1	Общие рекомендации.....	18
4.3.2	Требования по организации передачи данных по каналам связи	19
4.3.3	Требования по использованию криптоалгоритмов.....	19
4.3.4	Требования по контролю целостности.....	19
4.4	Восстановление работоспособности при сбоях, действия в нештатных ситуациях, связанных с использованием СКЗИ.....	20
5	Организационно-технические и административные мероприятия по защите от НСД при использовании СКЗИ ViPNet CSP	21
5.1	Общие положения.....	21
5.2	Организация работ по защите от НСД.....	21
5.3	Требования по защите от НСД при эксплуатации СКЗИ ViPNet CSP	22
6	Требования по хранению, распределению и удалению ключей.....	27
6.1	Порядок хранения и смены ключей	28
6.2	Компрометация ключей и порядок действий при компрометации.....	28
6.3	Порядок уничтожения ключей со съемных носителей	29

Список используемой литературы	30
Перечень сокращений	31
Приложение 1	32
Приложение 2	50
Приложение 3	51

1 Общие положения

Средство криптографической защиты информации ViPNet CSP 4.2 (далее – СКЗИ ViPNet CSP) предназначено для:

- шифрования информации;
- выработки значения хэш-функции;
- вычисления имитовставки;
- создания ключей электронной подписи (далее – ЭП) и ключей проверки ЭП;
- формирования ЭП и проверки ЭП;
- формирования сообщений в формате CMS (Cryptographic Message Syntax);
- защиты данных, передаваемых по протоколу TLS (Transport Layer Security)/SSL (Secure Sockets Layer);
- формирования ключей шифрования;
- формирования транспортных контейнеров ключей в формате PKCS #12 (PFX);
- выработки случайных двоичных последовательностей.

СКЗИ ViPNet CSP предназначено для встраивания в программное обеспечение (далее – ПО), а также для поставки конечным пользователям, использующим ПО, которое обращается к криптографическим функциям через системные интерфейсы.

СКЗИ ViPNet CSP предназначено для использования в приложениях и системах защиты информации, не содержащей сведений, составляющих государственную тайну, на территории Российской Федерации, а также для вывоза за рубеж или экспортных поставок в качестве самостоятельных изделий или в составе указанных приложений и систем.

1.1 Состав программных средств СКЗИ ViPNet CSP

В состав СКЗИ ViPNet CSP входят:

- набор криптографических функций (криптопровайдер) – динамическая библиотека, предназначенная для встраивания в приложения, использующие вызовы криптографических функций через интерфейс криптопровайдера Microsoft Cryptographic Service Provider (далее – MS CSP);
- набор криптографических функций – динамическая библиотека, предназначенная для встраивания в приложения, использующие вызовы криптографических функций через интерфейс RSA SecurityInc. PKCS #11 Cryptographic Token Interface (Cryptoki) V2.30 (далее – PKCS #11);
- набор криптографических функций – динамическая библиотека, предназначенная для встраивания в приложения, использующие вызовы

криптографических функций через интерфейс криптопровайдера Microsoft Cryptography API: Next Generation(далее – MS CNG);

- модули реализации прикладных протоколов и форматов данных X.509, PKCS #10, СМС, PKCS#5, PKCS#12 (PFX), PKCS#7 (CMS);
- СОМ-объекты для доступа к криптографическим функциям;
- динамическая библиотека реализации протоколов SSL 2.0, SSL 3.0, TLS 1.0 (включая расширения RFC 4346, RFC 5246);
- устройство типа «электронный замок» (только для вариантов исполнения 2 и 3);
- программа ViPNet SysLocker для настройки замкнутой среды функционирования криптосредства (далее – СФК) (только для варианта исполнения 3).

Состав каждого варианта исполнения СКЗИ ViPNet CSP указан в формуляре на данное СКЗИ [7].

1.2 Требования к составу технических средств и операционным системам

СКЗИ ViPNet CSP предназначено для использования на компьютерах архитектуры x86 и x64 (стационарных, переносных) с минимально рекомендуемой производителем операционной системы (далее – ОС) аппаратной конфигурацией, а также в виртуальной среде, поддерживающей эти архитектуры.

СКЗИ ViPNet CSP функционирует под управлением ОС MS Windows:

- Windows Vista (32/64-разрядная);
- Windows 7 (32/64-разрядная);
- Windows 8 (32/64-разрядная);
- Windows 8.1 (32/64-разрядная);
- Windows Server 2003 (32-разрядная);
- Windows Server 2008 (32/64-разрядная);
- Windows Server 2008 R2 (64-разрядная);
- Windows Server 2012 (32/64-разрядная);
- Windows Server 2012 R2 (64-разрядная).

СКЗИ ViPNet CSP (вариант исполнения 1) функционирует в виртуальных средах:

- MicrosoftHyper-V;
- VMwareWorkstation;
- VMwarePlayer;
- VMwarevSphere ESX;

– VirtualBox.

Примечание. На компьютерах или в ОС виртуальной среды должен быть установлен последний известный на момент установки пакет обновления ОС (ServicePack) и все известные критические обновления, опубликованные производителем ОС.

Для обеспечения защиты по классам КС2 (вариант исполнения 2) и КС3 (вариант исполнения 3) требований ФСБ России к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, СКЗИ ViPNet CSP (варианты исполнения 2, 3) должно работать совместно со средством защиты от несанкционированного доступа (далее – НСД) типа «электронный замок», сертифицированным ФСБ России по требованиям к аппаратно-программным модулям доверенной загрузки.

Для обеспечения защиты по классу КС3 (вариант исполнения 3) требований ФСБ России к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, совместно с СКЗИ ViPNet CSP (вариант исполнения 3) должен быть установлен компонент ViPNet SysLocker (модуль защиты СФК) в соответствии с [3].

1.3 Дополнительное ПО

Должна быть обеспечена антивирусная защита СКЗИ ViPNet CSP и СФК путем использования сертифицированных ФСБ России антивирусных средств. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ.

2 Требования к размещению технических средств

При эксплуатации СКЗИ ViPNet CSP в организации следует руководствоваться следующими рекомендациями:

- 1 Размещение, специальное оборудование и технические средства (далее – ТС), охрана и режим в помещении, в котором устанавливается изделие для эксплуатации (далее – помещение), должны обеспечивать:
 - безопасность информации и ключей;
 - невозможность доступа не допущенных к работе с СКЗИ ViPNet CSP лиц к ТС с установленным СКЗИ ViPNet CSP, к эксплуатационной документации и ключевым документам СКЗИ, к просмотру процедур работы с СКЗИ;
 - исключение возможности кражи изделия.
- 2 Помещение, в котором устанавливается СКЗИ ViPNet CSP, должно быть аттестовано в соответствии с руководящими документами специально созданной комиссией. Результатом работы комиссии является акт проверки выделенного помещения для работы с СКЗИ, утвержденный руководителем организации.
- 3 Порядок допуска в помещение определяется внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры организации, эксплуатирующей СКЗИ ViPNet CSP.
- 4 При расположении помещения на первых и последних этажах зданий, а также при размещении рядом с окнами балконов, пожарных лестниц и тому подобное, окна помещения оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими НСД в помещение. Помещение должно иметь прочные входные двери, на которые устанавливаются надежные замки.
- 5 Для хранения ключевых документов, нормативной и эксплуатационной документации помещение оснащается металлическим шкафом (хранилищем, сейфом), оборудованным внутренними замками с двумя экземплярами ключей и приспособлением для опечатывания. Дубликаты ключей от металлического шкафа и входных дверей помещения должны храниться в сейфе руководителя организации.
- 6 Устанавливаемый руководителем организации порядок охраны помещения должен предусматривать периодический контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.
- 7 Должны быть приняты меры по исключению НСД в помещение, в котором размещены ТС с установленным СКЗИ ViPNet CSP, посторонних лиц, по роду

своей деятельности не являющихся персоналом, допущенным к работе в указанном помещении.

- 8 Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключи.
- 9 Порядок охраны и организации режима помещения, в котором находится компьютер с установленным СКЗИ, регламентируется разделом IV инструкции [1].
- 10 На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством организации, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений, очередность и порядок эвакуации конфиденциальных документов и дальнейшего их хранения.
- 11 При эксплуатации ТС с установленным СКЗИ ViPNet CSP должны выполняться действующие в Российской Федерации требования по защите информации, предназначенной для шифрования, от утечки по техническим каналам, в том числе каналам связи¹.
- 12 ТС с установленными СКЗИ ViPNet CSP могут подключаться к общегородской сети электроснабжения с учетом требований инструкций по эксплуатации вычислительных средств и правил техники безопасности.
- 13 Оборудование помещений средствами вентиляции и кондиционирования воздуха должно соответствовать санитарно-гигиеническим нормам СНиП, устанавливаемым законодательством Российской Федерации.
- 14 Если ТС с установленным СКЗИ ViPNet CSP планируется разместить в помещении, в котором присутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и (или) установлены автоматизированные системы и системы приема, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну, автоматизированные системы иностранного производства, то такое помещение и ТС должны быть подвергнуты проверкам по выявлению устройств, предназначенных для негласного получения информации.

¹Примечание. Требования по защите информации от утечки по техническим каналам, в том числе по каналу связи приведены, например, в СТР-К.

При эксплуатации СКЗИ частными лицами следует по возможности руководствоваться вышеперечисленными требованиями к размещению. Ответственность за сохранность СКЗИ и ключевой информации возлагается в данном случае на пользователя.

3 Установка и эксплуатация СКЗИ ViPNet CSP

Перед эксплуатацией СКЗИ ViPNet CSP необходимо внимательно ознакомиться и неукоснительно соблюдать требования, указанные в настоящем документе и другой эксплуатационной документации на изделие, приведенной в [7].

3.1 Порядок распространения и учета СКЗИ ViPNet CSP

СКЗИ ViPNet CSP поставляется:

1. На носителях.
2. Через сеть связи общего пользования с сайта производителя ОАО «ИнфоТеКС» (<http://infotecs.ru/>) или с сайта технологического партнера ОАО «ИнфоТеКС» (дистрибьютера). Экземпляр для распространения дистрибьютер получает на носителе.

Получение СКЗИ от производителя или дистрибьютера на носителях обеспечивает 100% гарантию защиты дистрибутива от подмены, в отличие от скачивания через сеть связи общего пользования.

Для обеспечения контроля целостности должны быть приняты меры по проверке контрольной суммы полученного дистрибутива согласно п. 4.1.

Время тестовой эксплуатации без регистрации продукта ограничивается 14 сутками. Во время тестовой эксплуатации запрещена обработка информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации.

Позэкземплярный учет СКЗИ ViPNet CSP осуществляется производителем – ОАО «ИнфоТеКС» в процессе регистрации ПО.

В случае распространения СКЗИ ViPNet CSP через сеть связи общего пользования с сайта <http://infotecs.ru/> организация позэкземплярного учета зависит от того, каким образом предоставлена информация о пользователе СКЗИ:

1. Серийный номер для регистрации СКЗИ ViPNet CSP выделяется при получении непосредственно от пользователя учетных данных, обеспечивающих его идентификацию. Информация о результатах регистрации на сайте <http://infotecs.ru/> дублируется письмом на электронную почту пользователя. Используя полученный серийный номер, пользователь активирует процедуру регистрации экземпляра СКЗИ ViPNet CSP и обращается в ОАО «ИнфоТеКС» за кодом регистрации. При выделении кода регистрации экземпляру СКЗИ ViPNet CSP присваивается учетный номер в соответствии с версией и присвоенным данному продукту учетным индексом.

2. Серийный номер для регистрации СКЗИ ViPNet CSP выделяется при получении учетных данных пользователя из информационной системы дистрибьютера и идентификатора² дистрибьютера (производителя прикладного ПО), позволяющих однозначно идентифицировать пользователя. Процедура загрузки, получения кода регистрации и непосредственно регистрация экземпляра СКЗИ ViPNet CSP осуществляются автоматически.

В случае распространения СКЗИ ViPNet CSP через сеть связи общего пользования с сайта дистрибьютера³ информация для регистрации СКЗИ ViPNet CSP поступает производителю в виде двух идентификаторов: дистрибьютера и пользователя в информационной системе дистрибьютера, позволяющих однозначно идентифицировать пользователя. Процедура загрузки, получения кода регистрации и непосредственно регистрация экземпляра СКЗИ ViPNet CSP осуществляются автоматически.

В случае распространения СКЗИ ViPNet CSP через сеть связи общего пользования по запросу пользователя ему может быть предоставлен формуляр изделия в электронном виде с указанием серийного номера продукта, контрольной суммы дистрибутива и присвоенного регистрационного номера СКЗИ ViPNet CSP.

3.2 Требования по установке СКЗИ ViPNet CSP, а также общесистемного и специального ПО на компьютер

К установке общесистемного и специального ПО, а также СКЗИ ViPNet CSP, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и на СКЗИ ViPNet CSP.

При установке ПО СКЗИ ViPNet CSP следует:

- на ТС, предназначенных для работы с СКЗИ ViPNet CSP, использовать только лицензионное ПО фирм – производителей;
- на компьютере исключить установку средств разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти СКЗИ ViPNet CSP и приложений, использующих СКЗИ ViPNet CSP, а также для просмотра кода и памяти СКЗИ ViPNet CSP и приложений,

² Уникальный идентификатор, присваиваемый производителем технологическому партнеру.

³ Дистрибьютер в данном случае должен обладать лицензиями на распространение СКЗИ при условии применения ViPNet CSP не для собственных нужд.

использующих СКЗИ ViPNet CSP, в процессе обработки СКЗИ ViPNet CSP защищаемой информации и/или при загруженных ключах;

- предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части ТС, на которых установлены СКЗИ ViPNet CSP (например, путем опечатывания системного блока и разъемов компьютера);
- после завершения процесса установки выполнить действия, необходимые для осуществления периодического контроля целостности установленного СКЗИ ViPNet CSP, а также его окружения в соответствии с документацией;
- из ПО, устанавливаемого на компьютер с СКЗИ ViPNet CSP, исключить содержащие возможности, позволяющие:
 - 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;
 - повышать предоставленные привилегии;
 - модифицировать настройки ОС;
 - использовать недокументированные фирмой-разработчиком функции ОС.

3.3 Установка СКЗИ ViPNet CSP

Установка СКЗИ ViPNet CSP осуществляется самостоятельно пользователем, обладающим правами администратора ОС (администратор системы), или администратором безопасности в организации, эксплуатирующей СКЗИ.

Перед установкой СКЗИ ViPNet CSP необходимо:

- проверить работоспособность компьютера и соответствие требованиям по размещению (см. раздел 2 «Требования к размещению технических средств»);
- проверить компьютер на отсутствие вирусов;
- проверить, что установленное ПО не содержит средств разработки и отладки приложений, а также средств, позволяющих осуществлять НСД к системным ресурсам;

- проверить, что отсутствуют средства, запоминающие нажатия клавиш и другие действия пользователя;
- установить права доступа к каталогам установки ПО и другим каталогам компьютера для каждой учетной записи в соответствии с полномочиями пользователя в объеме, необходимом для выполнения его обязанностей;
- отключить учетную запись для гостевого входа (Guest);
- для вариантов исполнения 2 и 3 необходимо убедиться, что сертифицированное ФСБ России устройство типа «электронный замок» установлено и правильно настроено в соответствии с документацией к нему;
- проверить целостность файла дистрибутива ПО СКЗИ ViPNet CSP.

В случае обработки информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, ПО BIOS CBT, на котором установлено СКЗИ, необходимо проверить в соответствии с «Временными методическими рекомендациями к проведению исследований ПО BIOS по документированным возможностям».

Для вариантов исполнения 2 и 3 настройка BIOS определяется эксплуатационной документацией на сертифицированное средство защиты от НСД типа «электронный замок», входящее в состав СКЗИ.

В BIOS должен быть установлен один вариант загрузки ОС – с жесткого диска, все альтернативные варианты загрузки должны быть отключены, в том числе сетевая загрузка.

Вход в BIOS компьютера должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю учетной записи администратора системы. Пароль для входа в BIOS должен быть известен только администратору системы и быть отличным от пароля для входа в систему.

Средствами BIOS должна быть исключена возможность работы на компьютере с установленным СКЗИ ViPNet CSP в случае, если во время начальной загрузки не проходят встроенные тесты.

Установка СКЗИ ViPNet CSP осуществляется в соответствии с документом [2].

При установке СКЗИ ViPNet CSP в варианте исполнения 3 должна быть установлена программа ViPNet SysLocker (модуль защиты СФК) в соответствии с [3].

По завершении инициализации осуществляется настройка ПО в соответствии с требованиями раздела 3.3.

3.4 Требования к настройкам СКЗИ ViPNet CSP

Для варианта исполнения 3 СКЗИ ViPNet CSP необходимо выполнить дополнительные настройки:

- настроить программу ViPNet SysLocker в соответствии с [3];
- установить интервал автоматического блокирования компьютера 15 минут;
- включить ведение журнала событий криптопровайдера (выбрать один из двух режимов ведения журнала в зависимости от условий эксплуатации и интенсивности использования СКЗИ ViPNet CSP);
- включить системный механизм аудита доступа к объектам для успешных попыток доступа;
- в системном списке контроля доступа (SACL) дескриптора безопасности для системного журнала аудита должны быть добавлены элементы аудита успешных попыток доступа для групповой учетной записи Windows «Everyone» («Все»).

Для вариантов исполнения 2 и 3 СКЗИ ViPNet CSP необходимо включить в список контроля целостности устройства типа «электронный замок» список исполняемых модулей ОС. Список модулей, подлежащих контролю целостности, приведен в Приложении 2.

3.5 Ввод в эксплуатацию

Ввод в эксплуатацию СКЗИ ViPNet CSP в организации осуществляется администратором безопасности.

На каждое рабочее место, оснащенное СКЗИ ViPNet CSP, оформляется акт о вводе в эксплуатацию по типовой форме. Акт может храниться у администратора безопасности или у пользователя, ответственного за эксплуатацию СКЗИ ViPNet CSP.

4 Эксплуатация СКЗИ ViPNet CSP

Все действия по обслуживанию и настройкам должны производиться самостоятельно пользователем с правами администратора ОС или администратором безопасности.

4.1 Контроль целостности компьютера и ПО

Контроль целостности и работоспособности компьютера, на который устанавливается СКЗИ ViPNet CSP, осуществляется штатными средствами BIOS при холодной перезагрузке компьютера. При включении компьютера выполняется:

- проверка регистров процессора;
- проверка контрольной суммы постоянного запоминающего устройства (ПЗУ);
- проверка системного таймера;
- тест контроллера непосредственного доступа к памяти (DMA);
- тест регенератора оперативной памяти;
- тест нижней области оперативного запоминающего устройства (ОЗУ) для проецирования резидентных программ BIOS;
- тест стандартного графического адаптера;
- тест оперативной памяти;
- тест основных устройств ввода;
- тест CMOS;
- тест основных портов ввода/вывода;
- тест накопителей на жестких магнитных дисках;
- самодиагностика функциональных подсистем BIOS.

При возникновении ошибки на каком-либо этапе, дальнейшая работы компьютера должна блокироваться.

Для вариантов исполнения 2 и 3 СКЗИ ViPNet CSP дополнительно для препятствия извлечению устройства типа «электронный замок» из компьютера системные блоки компьютера должны быть опечатаны предназначенной для этих целей печатью или специальными защитными знаками. Наряду с этим допускается применение других средств контроля доступа к компьютеру.

Перед установкой ПО СКЗИ ViPNet CSP на компьютер администратор безопасности должен убедиться в отсутствии внешних признаков вскрытия системного блока и подключенного дополнительного оборудования, не предусмотренного актом о вводе в эксплуатацию.

СКЗИ ViPNet CSP оснащено встроенными механизмами проверки целостности ПО ViPNet.

Проверка целостности дистрибутива СКЗИ ViPNet CSP осуществляется перед установкой СКЗИ ViPNet CSP путем сравнения контрольной суммы. Подсчет контрольной суммы выполняется утилитой ViPNet HashCalc, входящей в комплект поставки СКЗИ ViPNet CSP.

Контрольная сумма дистрибутива СКЗИ ViPNet CSP представляет собой хэш содержимого дистрибутива, вычисленный по алгоритму ГОСТ Р 34.11-2012 и может быть вычислена с использованием независимых средств других производителей.

Значение контрольной суммы для сравнения пользователь может получить из различных независимых источников, в том числе доверенным способом.

После установки ПО СКЗИ ViPNet CSP необходимо сформировать контрольные суммы для файлов, перечень которых приведен в Приложениях 2 и 3 (соответствует содержимому файла C:\ProgramData\Infotecs\ViPNetCSP\os.prg). Для этого необходимо запустить с правами администратора утилиту make_ext_crg из каталога ViPNet CSP (по умолчанию: C:\Program Files\InfoTeCS\ViPNet CSP) со следующими параметрами:

Make_ext_crg.exe -r "C:\ProgramData\Infotecs\ViPNet CSP\os.prg".

Перед началом работы должен быть проведен контроль целостности при помощи утилиты check_crg. Контролем целостности должны быть охвачены файлы, перечень которых приведен в Приложениях 2 и 3. Для этого необходимо выполнить:

- команду: check_crg"C:\ProgramData\Infotecs\ViPNetCSP\os.prg". В результате проверки будет сформирован протокол, который заканчивается обобщенным итогом в следующей форме:

Total:

1 PRG files checked, 1 checks passed, 0 checks failed

6 files checked, 6 checks passed, 0 files corrupted, 0 checks failed;

Он не должен содержать ошибок.

- выполнить проверку целостности из контрольной панели CSP.

При каждом запуске СКЗИ ViPNet CSP осуществляется проверка модулей, входящих в СКЗИ ViPNet CSP (перечень исполняемых модулей ОС Windows, подлежащих контролю целостности, представлен в Приложении 2).

Также при обращении к криптографическим функциям (при загрузке библиотеки) производится проверка контрольных сумм всех модулей, которые могут быть задействованы.

Если выявлено искажение хотя бы одного из модулей, то все функции обращения к ключам будут возвращать ошибку исполнения.

Кроме того, пользователь СКЗИ ViPNet CSP может самостоятельно инициировать проверку целостности исполняемых файлов (подробнее см. в [2]).

При наличии установленного на компьютере устройства типа «электронный замок» необходимо использование дополнительных механизмов проверки целостности, предусмотренных такими устройствами.

Компьютер, на который установлено СКЗИ ViPNet CSP, должен перезагружаться не реже одного раза в сутки.

После обновления ОС Windows возможно возникновение ошибки при проверке контрольных сумм системных библиотек, используемых СКЗИ ViPNet CSP, что будет отражено на консоли при проверке. В этом случае необходимо:

- уведомить разработчика о несоответствии хэш-значений системных библиотек с целью постановки работ по проведению анализа обновленных системных библиотек, используемых СКЗИ ViPNet CSP установленным порядком;
- на период до получения результатов исследований следовать инструкциям разработчика, полученным им из специализированной организации.

СКЗИ ViPNet CSP не содержит штатных функций доступных пользователю и позволяющих выполнять изменение криптографических функций изделия. Изменение криптографических функций возможно лишь путем непосредственного изменения и/или редактирования исполняемых модулей изделия.

Поскольку в процессе работы СКЗИ ViPNet CSP обеспечивается контроль целостности всех исполняемых модулей (по контрольной сумме, вычисляемой по алгоритму ГОСТ 28147-89 в режиме выработки имитовставки на содержимое всего исполняемого файла, которая записывается в исполняемый файл при сборке разработчиком установочного дистрибутива СКЗИ ViPNet CSP), блокирующий работу изделия при обнаружении искажений и/или модификации, то внесение изменений в исполняемые модули СКЗИ ViPNet CSP приведет к его неработоспособности.

При обнаружении ошибок проверки целостности пользователь обязан прекратить эксплуатацию компьютера и уведомить администратора безопасности (для организаций) или службу технической поддержки производителя ОАО «ИнфоТеКС» (для пользователей – физических лиц) о возникновении ошибок.

В этом случае пользователь обязан:

- отключить компьютер с установленным СКЗИ ViPNet CSP от локальной вычислительной сети до устранения неисправностей;
- провести исследование с целью выяснения возможных причин возникновения неисправностей;
- произвести проверку работоспособности компьютера, на котором установлено СКЗИ ViPNet CSP;
- провести проверку ОС и установленного ПО на наличие вирусов и вредоносного ПО;
- провести анализ журналов аудита с целью выявления попыток НСД и сетевых атак;
- устранить обнаруженные причины возникновения неисправностей или искажений;
- при необходимости произвести переустановку СКЗИ ViPNet CSP.

4.2 Обновление ПО СКЗИ ViPNet CSP

Обновление ПО СКЗИ ViPNet CSP осуществляется только локально путем установки сертифицированной версии ПО поверх предыдущей (без предварительного удаления последней). Другие способы обновления ПО СКЗИ ViPNet CSP недопустимы.

После завершения обновления ПО СКЗИ ViPNet CSP необходимо произвести проверку настроек и работоспособности СКЗИ ViPNet CSP.

4.3 Встраивание в приложения

Разработка ПО на основе СКЗИ ViPNet CSP может производиться без создания новых СКЗИ в случае использования вызовов функций из перечня, приведенного в Приложении 1.

В случае использования прочих вызовов необходимо производить разработку отдельного СКЗИ в соответствии с действующей нормативной базой (в частности, с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. №313 и Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)).

При встраивании СКЗИ ViPNet CSP в приложения необходимо руководствоваться соответствующими руководствами разработчика ([4], [5] и [6]), а также Приложением 1 к [4].

4.3.1 Общие рекомендации

После выработки, но до ввода в эксплуатацию ключ проверки ЭП должен пройти обязательную сертификацию в Удостоверяющем центре (далее – УЦ), сертифицированном по

требованиям ФСБ России по классу, соответствующему классу средства ЭП. Кроме того, пользователь или администратор безопасности должен своевременно выводить из действия пару ключей ЭП по истечению срока действия или при компрометации ключа ЭП.

При использовании сертификата ключа проверки ЭП (далее – сертификат) должна проводиться его проверка и поиск ссылки на данный сертификат в списке аннулированных сертификатов.

4.3.2 Требования по организации передачи данных по каналам связи

При передаче данных (сообщений, ключей или аутентифицирующей информации в зашифрованном виде) между двумя абонентами, реализованной на основе криптодра СКЗИ ViPNet CSP, необходимо использовать протокол обмена информацией, обеспечивающий:

- аутентификацию обоих абонентов связи;
- целостность передаваемого блока данных;
- защиту от повторного использования ключей шифрования (перекрытия ключей);
- защиту от повторов, а также навязывания ложных данных.

Данные требования обеспечиваются в реализации протокола TLS, входящего в состав СКЗИ ViPNet CSP при использовании ПО, являющегося неотъемлемой частью используемых ОС.

Запрещается использовать алгоритм TLS без серверной аутентификации. Необходимо производить регулярную очистку кэша TLS.

4.3.3 Требования по использованию криптоалгоритмов

Для обеспечения свойств ЭП необходимо перед использованием ключа проверки подписи проверять его сертификат на предмет целостности и отсутствия в списке скомпрометированных.

Использование алгоритма шифрования в режиме простой замены с зацеплением без вычисления имитовставки не допускается.

При использовании шифрованных сообщений в формате CMS для подтверждения подлинности и обеспечения целостности сообщений рекомендуется использовать их как вложение в подписываемые CMS-сообщения.

4.3.4 Требования по контролю целостности

При создании специализированного ПО СКЗИ, использующего в качестве криптодра библиотеку ViPNet CSP, необходимо предусмотреть периодический контроль целостности библиотеки, а также установленного специализированного ПО.

4.4 Восстановление работоспособности при сбоях, действия в нештатных ситуациях, связанных с использованием СКЗИ

Все действия в нештатных ситуациях, связанных с использованием СКЗИ ViPNet CSP, а также при восстановлении работоспособности СКЗИ ViPNet CSP производятся самостоятельно пользователем, обладающим правами администратора ОС или администратором безопасности.

Для восстановления работы СКЗИ ViPNet CSP в случае искажения файлов ПО СКЗИ ViPNet CSP необходимо иметь инсталляционный диск с экземпляром дистрибутива ПО.

В случае искажения файлов ПО СКЗИ ViPNet CSP необходимо:

- 1 Произвести форматирование НЖМД (накопитель на жестких магнитных дисках), на который была установлена ОС и СКЗИ.
- 2 Произвести установку ОС и систем защиты от НСД (см. п. 5).
- 3 Произвести установку ПО СКЗИ ViPNet CSP в каталог установки с использованием инсталляционного диска с экземпляром дистрибутива СКЗИ.
- 4 Настроить сетевые интерфейсы и подсоединить компьютер к сети.
- 5 Произвести перезагрузку ОС.

В случае выхода из строя компьютера СКЗИ ViPNet CSP может быть установлен на любой аналогичный компьютер с необходимым числом сетевых интерфейсов. Для этого необходимо иметь инсталляционный диск ОС, инсталляционные диски систем защиты от НСД, инсталляционный диск СКЗИ.

Рекомендуется сделать полную резервную копию рабочего каталога СКЗИ ViPNet CSP, тогда будут сохранены и указанные выше настройки, а также журналы СКЗИ ViPNet CSP.

В случае выхода из строя компьютера с установленным СКЗИ ViPNet CSP, помимо перечисленного выше, необходимо:

- 1 Произвести, по необходимости и при наличии возможности, копирование каталога установки СКЗИ ViPNet CSP на другой компьютер в каталог с теми же путями, что и на вышедшем из строя компьютере.
- 2 Произвести установку ПО СКЗИ ViPNet CSP в этот каталог с использованием инсталляционного диска с экземпляром СКЗИ.
- 3 Настроить сетевые интерфейсы и подсоединить компьютер к сети.
- 4 Произвести перезагрузку операционной системы.

5 Организационно-технические и административные мероприятия по защите от НСД при использовании СКЗИ ViPNet CSP

5.1 Общие положения

Защита аппаратного и программного обеспечения от НСД при установке и использовании СКЗИ ViPNet CSP является составной частью общей задачи обеспечения безопасности информации в системе, в состав которой входит СКЗИ ViPNet CSP.

Наряду с применением средств защиты от НСД необходимо выполнение ряда мер, включающих в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности использования технических средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

В приведенных ниже разделах содержатся основные требования по выполнению указанных мер защиты.

5.2 Организация работ по защите от НСД

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.

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости администратором безопасности или пользователем.

В организации, эксплуатирующей СКЗИ ViPNet CSP, должен быть назначен администратор безопасности, на которого возлагаются задачи организации работ по использованию СКЗИ ViPNet CSP, выработки соответствующих инструкций для пользователей, а также контроль над соблюдением описанных ниже требований.

Правом доступа к рабочим местам, с установленными СКЗИ ViPNet CSP, должны обладать только определенные (выделенные для эксплуатации) лица (пользователи), прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя СКЗИ ViPNet CSP с документацией на СКЗИ ViPNet CSP, а также с другими нормативными документами, созданными на ее основе.

5.3 Требования по защите от НСД при эксплуатации СКЗИ ViPNet CSP

При организации работ по защите информации от НСД необходимо обеспечить выполнение следующих требований:

- необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:
 - длина пароля должна быть не менее 6 символов;
 - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);
 - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
 - при смене пароля новое значение должно отличаться от предыдущего не менее чем в четырех позициях (периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев);
 - личный пароль пользователь не имеет права сообщать никому.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.

Запрещается:

- оставлять без контроля компьютер, на котором эксплуатируется СКЗИ ViPNet CSP, после ввода ключей, либо иной конфиденциальной информации;
- вносить какие-либо изменения в ПО СКЗИ ViPNet CSP;
- осуществлять несанкционированное администратором безопасности копирование носителей с ключами;
- записывать на носители с ключами постороннюю информацию;
- разглашать содержимое носителей с ключами или передавать сами носители лицам, к ним не допущенным, выводить ключи на дисплей, принтер и иные средства отображения информации;
- использовать носители с ключами в режимах, не предусмотренных функционированием СКЗИ ViPNet CSP.

Администратор безопасности должен сконфигурировать ОС, в среде которой планируется использовать СКЗИ ViPNet CSP, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- не использовать нестандартные, измененные или отладочные версии ОС;
- исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;
- исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек;
- на компьютере должна быть установлена только одна ОС;
- правом установки и настройки ОС и СКЗИ ViPNet CSP должен обладать только администратор безопасности;
- все неиспользуемые ресурсы ОС необходимо отключить (протоколы, сервисы и т.п.);
- 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;
- установить атрибуты безопасности процессов и потоков в соответствии с требованиями безопасности всей системы в целом;
- отказаться от использования режима автоматического входа пользователя в ОС при ее загрузке;
- ограничить с учетом выбранной в организации политики безопасности использование пользователями запуска программ по расписанию;
- запретить интерактивный вход пользователей через сеть;
- ограничить количество неудачных попыток входа в систему;
- использовать систему аудита, организовать регулярный анализ результатов аудита;
- настроить ОС на завершение работы при переполнении журнала аудита;
- необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
 - файлы конфигурации;
 - файлы и каталоги;
 - временные файлы;
 - журналы системы;
 - файлы подкачки;

- кэшируемая информация (пароли и т.п.);
- отладочная информация.

Период непрерывной работы всех компонентов СКЗИ ViPNet CSP без выключения питания не должен превышать 1 сутки. По окончании этого срока необходимо проводить перезагрузку компьютера с установленными компонентами СКЗИ ViPNet CSP.

При установке параметров, позволяющих создавать криптографически незащищенные соединения, должны быть приняты меры, исключающие утечку требующей защиты информации с защищаемого объекта информатизации. Проверка достаточности принятых мер защиты проводится при аттестации объекта информатизации с СКЗИ ViPNet CSP по требованиям информационной безопасности.

Необходимо организовать регулярное архивирование журналов аудита. Не допускается выполнить очистку журнала регистрации событий СКЗИ ViPNet CSP без создания резервной копии.

Архивирование журнала и разграничение доступа к архиву журнала обеспечивается средствами ОС. Для этого администратор безопасности должен написать скрипт, который будет запускаться по расписанию с правами администратора, и копировать архив журнала в отдельную папку. Доступ к этой папке должны иметь только учетные записи администратора безопасности и администратора СУ: в свойствах данной папки на вкладке **Безопасность** администратор должен удалить все учетные записи, кроме учетной записи администратора безопасности и администратора СУ.

Кроме того, необходимо организовать затирание (по окончании сеанса работы СКЗИ ViPNet CSP) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ ViPNet CSP. Если это не выполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к носителям с ключами:

- должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;
- необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;
- в случае подключения компьютера с установленным СКЗИ ViPNet CSP 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;

- при использовании СКЗИ ViPNet CSP на компьютерах, подключенных к общедоступным сетям связи, с целью исключения возможности НСД к системным ресурсам используемых ОС, к ПО, в окружении которого функционирует СКЗИ ViPNet CSP, и к компонентам СКЗИ ViPNet CSP 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;
- организовать и использовать систему аудита, организовать регулярный анализ результатов аудита;
- организовать и использовать комплекс мероприятий антивирусной защиты;
- исключить одновременную работу в ОС с работающим СКЗИ ViPNet CSP и загруженными ключами нескольких пользователей.

Примечание. Под однопользовательским режимом в данном случае подразумевается такой режим, при котором все пользователи данной рабочей станции имеют одинаковый доступ к ключам на этой рабочей станции.

Дополнительно, в качестве организационной меры обеспечения эксплуатации СКЗИ ViPNet CSP рекомендуется при каждой загрузке операционной системы проверять целостность защищенных системных файлов с помощью утилиты sfc, входящей в состав ОС. Для этого необходимо через командную строку запустить утилиту с правами администратора и проверить файлы с помощью команды /VERIFONLY.

Также, в качестве организационной меры обеспечения безопасной эксплуатации, необходимо в ОС выполнить следующие настройки:

- для политики «Время до сброса счетчика блокировки» установить значение «1 мин.»;
- для политики «Пороговое значение блокировки» – «10 ошибок входа в систему»;
- для политики «Продолжительность блокировки учетной записи» – «1 мин.».

Настройка данных параметров безопасности осуществляется путем вызова через панель управления: «Администрирование» -> «Локальная политика безопасности» -> «Политики учетных записей» -> «Политика блокировки учетной записи».

6 Требования по хранению, распределению и удалению ключей

Должны быть приняты меры по надежному хранению ключей, размещенных на жестком диске компьютера с установленным СКЗИ ViPNet CSP (в виде файлов) и на съемных носителях. Все ключи на жестком диске хранятся только в зашифрованном на парольном ключе виде.

Отделяемые устройства хранения ключей разделяются на три категории:

- 1 Файловые устройства. Это устройства, не имеющие собственных механизмов защиты ключей и предоставляющие файловую систему для сохранения произвольных данных. К таким устройствам относятся флэш-карты, некоторые типы смарт-карт. В таких случаях формат и методы защиты ключей на картах идентичны случаю хранения на жестком диске.
- 2 Устройства PKCS #11, не имеющие аппаратной реализации алгоритмов ГОСТ. Для таких устройств объекты, содержащие секретные ключи, размещаются в защищенной памяти устройств. Механизмы защиты от НСД определяются производителем устройства.
- 3 Устройства PKCS #11, реализующие криптографические алгоритмы по стандартам ГОСТ. В подобных устройствах ключ является не извлекаемым. Вопросы защиты ключей полностью обеспечиваются производителем устройств.

Сроки действия ключей шифрования и ключей ЭП не должны превышать 1 года и 3 месяцев при хранении на носителях с файловой системой.

При использовании СКЗИ ViPNet CSP совместно с сертифицированными СКЗИ Рутокен ЭЦП, КриптоToken ЭП и ESMART Token ГОСТ срок действия закрытых ключей ЭП этих устройств, определенный в эксплуатационной документации этих устройств, не превышает 3-х лет.

В остальных случаях срок действия ключей шифрования и ключей ЭП не должен превышать 1 год и 3 месяца, а срок действия ключа проверки ЭП не должен превышать срок действия ключа ЭП более чем на 15 лет.

Пользователь должен следить за временем действия ключа ЭП и ключа шифрования и заблаговременно, например, за месяц до истечения срока действия, инициировать процедуру плановой смены ключа ЭП.

В СКЗИ ViPNet CSP не допускается использовать ключи ЭП и ключи шифрования, срок действия которых уже истек или еще не наступил. По истечении срока действия ключи подлежат уничтожению.

При деинсталляции ПО СКЗИ ViPNet CSP в случае прекращения эксплуатации на компьютере должна быть удалена вся ключевая информация. Удаление ключевой информации должно производиться с использованием утилиты clean.exe, входящей в состав ПО ViPNet.

6.1 Порядок хранения и смены ключей

При эксплуатации СКЗИ ViPNet CSP в организации съемные носители (отделяемые устройства хранения ключей) должны храниться в металлическом контейнере (в хранилище), опечатанном личной печатью администратора безопасности или пользователя.

Порядок плановой смены ключей или смены ключей в случае их компрометации описан в п. 6.2.

Смена всех используемых ключей осуществляется периодически (не реже одного раза в год) в соответствии с принятым планом смены ключей, а также в случае компрометации ключей.

6.2 Компрометация ключей и порядок действий при компрометации

Под компрометацией ключей понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации, защищаемой с их использованием: хищение, утрата, разглашение, несанкционированное копирование, а также другие происшествия, в результате которых ключевые документы могли стать доступными лицам, не допущенным к ним, или использоваться с нарушением правил пользования (нештатным образом), изложенным в разделе 5.3.

Ключи можно считать скомпрометированными в следующих случаях:

- потеря ключевых носителей;
- потеря ключевых носителей с их последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- нарушение правил пользования и хранения ключей, которое могло привести к их компрометации;
- возникновение обоснованных подозрений на утечку информации;
- нарушение печати на сейфе со съемными носителями.

Первые четыре события должны трактоваться как явная компрометация действующих ключей. Остальные события (неявная компрометация) требуют специального рассмотрения в каждом конкретном случае.

Порядок действий по локализации последствий при компрометации ключей должен быть разработан эксплуатирующей организацией и отражен в регламенте по безопасности.

Порядок смены ключей в случае их компрометации:

- связаться с администратором УЦ и сообщить о компрометации;
- при угрозе утечки важных данных заблокировать СКЗИ ViPNet CSP.

Ключи, в отношении которых возникло подозрение в компрометации, необходимо немедленно вывести из действия. О выводе ключей из действия необходимо сообщить в соответствующий УЦ.

После получения новых ключевых документов администратор безопасности выполняет действия, аналогичные первичной установке ключевых документов.

Администратором безопасности в кратчайший срок проводится замена скомпрометированных ключей. Представители органа криптографической защиты организации совместно с администратором безопасности проводят расследование факта компрометации ключевых документов, результаты которого оформляются Актом и утверждаются руководителем организации, эксплуатирующей СКЗИ ViPNet CSP.

6.3 Порядок уничтожения ключей со съемных носителей

Ключи, используемые СКЗИ ViPNet CSP, выводятся из действия в следующих случаях:

- при плановой смене ключей;
- при компрометации ключей;
- при повреждении носителя с ключевой информацией.

Для уничтожения выведенных из действия ключей создается комиссия из лиц, допущенных к обращению с ключевыми документами. Об уничтожении ключей комиссией составляется Акт, который утверждается руководством организации, и делается соответствующая запись в журнале учета выдачи ключевых документов.

Выведенные из действия ключи уничтожаются со всех носителей не позднее чем через трое суток после момента их вывода из действия. Сами ключевые носители либо уничтожаются физически, либо после уничтожения на них информации программами гарантированного уничтожения (например, при помощи программы clean.exe, входящей в комплект поставки СКЗИ) могут использоваться в дальнейшей работе с ключами.

Список используемой литературы

- 1 Инструкция 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, утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152.
- 2 ViPNet CSP 4.2. Руководство пользователя ФРКЕ.00106-03 34 01.
- 3 ViPNet SysLocker 1.0. Руководство администратора ФРКЕ.00158-01 34 01.
- 4 Криптографический интерфейс ViPNet CSP 4.2. Руководство разработчика ФРКЕ.00106-03 33 01.
- 5 Криптографический интерфейс ViPNet CNG 4.2. Руководство разработчика ФРКЕ.00106-03 33 03.
- 6 Криптографический интерфейс ViPNet PKCS #11 VT 4.2. Руководство разработчика ФРКЕ.00106-03 33 02.
- 7 Средство криптографической защиты информации ViPNet CSP 4.2. Формуляр ФРКЕ.00106-03 30 01 ФО.

Перечень сокращений

НСД	– несанкционированный доступ
ОС	– операционная система
ПО	– программное обеспечение
СКЗИ	– средство криптографической защиты информации
ТС	– техническое средство
УЦ	– Удостоверяющий центр
ЭП	– электронная подпись

ПРИЛОЖЕНИЕ 1

Перечень функций, использование которых при разработке систем на основе СКЗИ ViPNet CSP возможно без дополнительных тематических исследований

Функции для инициализации и настройки провайдера (cryptsp.dll, libadvapi32.so)

Функция	Windows	Linux	Описание
CryptAcquireContext	+	+	Функция используется для создания дескриптора криптопровайдера с именем контейнера ключей, определенным параметром <code>pszContainer</code> .
CryptReleaseContext	+	+	Функция используется для удаления дескриптора криптопровайдера, созданного <code>CryptAcquireContext()</code> .
CryptContextAddRef	+	+	Управляет счетчиком дескриптора, созданного <code>CryptAcquireContext()</code> .
CryptEnumProviders	+	+	Перечисление установленных криптопровайдеров.
CryptEnumProviderTypes	+	+	Перечисление установленных типов криптопровайдеров.
CryptGetDefaultProvider	+	+	Получение контекста провайдера, установленного в системе по умолчанию.
CryptGetProvParam	+	+	Функция получает параметры криптопровайдера.
CryptSetProvParam	+	+	Функция устанавливает параметры криптопровайдера.
FreeCryptProvFromCertEx	+	+	Функция используется для удаления дескриптора криптопровайдера, созданного <code>CryptAcquireContext()</code> или через CNG.
CryptInstallDefaultContext		-	Функция управления контекстом провайдера по умолчанию.
CryptUninstallDefaultContext	+	-	Функция управления контекстом провайдера по умолчанию.

Функции для генерации, создания, конфигурирования, удаления ключей и обмена ключами (cryptsp.dll, libadvapi32.so)

Функция	Windows	Linux	Описание	Комментарий
CryptGenKey	+	+	Функция генерирует случайные криптографические ключи или пару ключей (закрытый и открытый ключи).	
CryptDestroyKey	+	+	Функция удаляет ключ, передаваемый через параметр hKey. После удаления ключ (дескриптор ключа) не может использоваться.	
CryptExportKey	+	+	Функция используется для экспорта криптографических ключей из контейнера ключей криптопровайдера, сохраняя их в защищенном виде.	Использование разрешено для экспорта открытых ключей (PUBLICKEYBLOB). Использование для экспорта симметричных секретных ключей или секретных частей ключевых пар запрещено без создания отдельного криптосредства.
CryptGenRandom	+	+	Функция заполняет буфер случайными байтами.	
CryptGetKeyParam	+	+	Функция возвращает параметры ключа.	

CryptGetUserKey	+	+	Функция возвращает дескриптор одной из долговременных ключевых пар в контейнере ключей.	
CryptImportKey	+	+	Функция используется для импорта криптографического ключа из ключевого блока в контейнер ключей криптопровайдера.	Использование разрешено для импорта открытых ключей (PUBLICKEYBLOB), как для формирования в провайдере ключа проверки электронной подписи (доступен далее по дескриптору). Использование для импорта симметричных секретных ключей или секретных частей ключевых пар, а также формирование ключей по алгоритму VKO запрещено без создания отдельного криптосредства.
CryptSetKeyParam	+	+	Функция устанавливает параметры ключа.	Запрещено без создания отдельного криптосредства использование с аргументом KP_X (с отличным от NULL параметром), KP_MODE, KP_MIXMODE.

Функции для работы с алгоритмами хэширования (cryptsp.dll, libadvapi32.so)

Функция	Windows	Linux	Описание	Комментарий
CryptCreateHash	+	+	Функция инициализирует дескриптор нового объекта функции хэширования потока данных.	Разрешено использование при всех видах аргументов, кроме CALG_G28147_IMIT.
CryptDestroyHash	+	+	Функция удаляет объект функции хэширования.	

CryptDuplicateHash	+	+	Функция создает точную копию объекта функции хэширования, включая все его переменные, определяющие внутреннее состояние объекта функции хэширования.	
CryptGetHashParam	+	+	Функция возвращает параметры объекта функции хэширования и значение функции хэширования.	
CryptHashData	+	+	Функция передает данные указанному объекту функции хэширования.	
CryptSetHashParam	+	+	Функция устанавливает параметры объекта хэширования.	Разрешается использование при всех типах символьных аргументов за исключением HP_HASHVAL.
CryptSignHash	+	+	Функция возвращает значение электронной подписи от значения функции хэширования.	
CryptVerifySignature	+	+	Функция проверяет электронную подпись.	

Функции для обработки криптографических сообщений (crypt32.dll, libcrypt32.so)

Обработка криптографических сообщений

Функция	Windows	Linux	Описание
CryptSignMessage	+	+	Функция создает хэш определенного содержания, подписывает хэш и затем производит закодирование и текста исходного сообщения, и подписанного хэша.
CryptVerifyMessageSignature	+	+	Функция проверяет электронную подпись подписанного сообщения.
CryptVerifyDetachedMessageSignature	+	+	Функция проверяет подписанное сообщение, содержащее одну или несколько открепленных электронных подписей.
CryptDecodeMessage	+	+	Функция декодирует, расшифровывает и проверяет сообщение.
CryptDecryptAndVerifyMessageSignature	+	+	Функция декодирует и проверяет сообщение.
CryptEncryptMessage	+	+	Функция зашифровывает и производит закодирование сообщения.
CryptDecryptMessage	+	+	Функция производит раскодирование и расшифрование сообщения.
CryptGetMessageCertificates	+	+	Функция возвращает хранилище сертификатов и списки аннулированных сертификатов из сообщения.
CryptGetMessageSignerCount	+	+	Функция возвращает количество подписавших сообщение.
CryptHashMessage	+	+	Функция создает хэшированное сообщение.
CryptSignAndEncryptMessage	+	+	Функция создает подписанное и зашифрованное сообщение.
CryptSignMessageWithKey	+	+	Функция создает подписанное сообщение.
CryptVerifyDetachedMessageHash	+	+	Функция проверяет открепленный хэш.
CryptVerifyMessageHash	+	+	Функция проверяет хэшированное сообщение.
CryptVerifyMessageSignatureWithKey	+	+	Функция проверяет подписанное сообщение.

Режим пошаговой обработки блоков сообщения

Функция	Windows	Linux	Описание
CryptMsgCalculateEncodedLength	+	+	Функция вычисляет максимальное количество байтов, необходимое для закодированного криптографического сообщения, заданного типом сообщения, параметрами кодирования и общей длиной информации, которая должна быть закодирована.
CryptMsgOpenToEncode	+	+	Функция открывает криптографическое сообщение для закодирования и возвращает дескриптор открытого сообщения.
CryptMsgOpenToDecode	+	+	Функция открывает криптографическое сообщение для раскодирования и возвращает дескриптор открытого сообщения.
CryptMsgUpdate	+	+	Функция дополняет текст криптографического сообщения.
CryptMsgGetParam	+	+	Функция получает параметр сообщения после того, как криптографическое сообщение было раскодировано или закодировано.
CryptMsgControl	+	+	Функция выполняет контрольное действие.
CryptMsgClose	+	+	Функция закрывает дескриптор криптографического сообщения.
CryptMsgDuplicate	+	+	Функция дублирует дескриптор криптографического сообщения путем увеличения счетчика ссылок.

Функции для работы со списками аннулированных сертификатов (crypt32.dll, libcrypt32.so)

Функция	Windows	Linux	Описание
CertAddCRLContextToStore	+	+	Функция добавляет контекст списка аннулированных сертификатов (CRL) в хранилище сертификатов.
CertAddCRLLinkToStore	+	-	Функция создает ссылку на список CRL в другом хранилище.
CertAddEncodedCRLToStore	+	+	Функция создает контекст CRL из закодированного CRL и добавляет его в хранилище сертификатов. Функция создает копию контекста CRL перед добавлением его в хранилище.
CertEnumCRLsInStore	+	+	Функция получает первый или следующий CRL в хранилище. Используется в цикле для того, чтобы последовательно получить все CRL в хранилище.
CertFreeCRLContext	+	+	Функция освобождает контекст CRL, уменьшая счетчик ссылок на единицу. Когда счетчик ссылок обнуляется, функция освобождает память, выделенную под контекст CRL.
CertCreateCRLContext	+	+	Функция создает контекст CRL из закодированного CRL. Созданный контекст не помещается в хранилище сертификатов. В созданном контексте функция размещает копию закодированного CRL.
CertDeleteCRLFromStore	+	+	Функция удаляет список CRL из хранилища.
CertDuplicateCRLContext	+	+	Функция дублирует контекст CRL, увеличивая счетчик ссылок на CRL на единицу.

CertFindCRLInStore	+	+	Функция находит первый или следующий контекст СОС в хранилище сертификатов, который соответствует критерию поиска, определяемому параметром dwFindType и связанным с ним pvFindPara. Функция может быть использована в цикле для того, чтобы найти все CRL в хранилище сертификатов, удовлетворяющие заданному критерию поиска.
CertDeleteCertificateFromStore	+	-	Функция удаляет определенный контекст CRL из хранилища сертификатов.
CertFindCertificateInCRL	+	+	Функция выполняет поиск заданного сертификата в списке CRL.
CertGetCRLFromStore	+	+	Функция получает первый или следующий контекст CRL для определенного издателя сертификата из хранилища сертификатов. Эта функция также выполняет возможную проверку CRL.
CertSerializeCRLStoreElement	+	+	Функция сериализации списка CRL со своими свойствами.

**Функции для работы с расширенными свойствами сертификата CRL и CTL
(crypt32.dll, libcrypt32.so)**

Функция	Windows	Linux	Описание
CertGetCRLContextProperty	+	+	Функция получает расширенные свойства определенного контекста CRL.
CertSetCRLContextProperty	+	+	Функция устанавливает расширенные свойства определенного контекста CRL.
CertGetCertificateContextProperty	+	+	Функция получает информацию, содержащуюся в расширенных свойствах контекста сертификата.

CertEnumCertificateContextProperties	+	+	Функция позволяет перечислить информацию, содержащуюся в расширенных свойствах контекста сертификата.
CertSetCertificateContextProperty	+	+	Функция устанавливает расширенные свойства для определенного контекста сертификата.
CertEnumCRLContextProperties	+	+	Перечисление расширенных свойств списка аннулированных сертификатов.
CertEnumCTLContextProperties	+	-	Перечисление расширенных свойств CTL.
CertGetCTLContextProperty	+	-	Получение расширенного свойства CTL.
CertSetCTLContextProperty	+	-	Задание расширенных свойств CTL.

Функции для работы с сертификатами (crypt32.dll, libcrypt32.so)

Функция	Windows	Linux	Описание
CertAddCertificateContextToStore	+	+	Функция добавляет контекст сертификата в хранилище сертификатов.
CertAddCertificateLinkToStore	+	-	Добавляет ссылку на сертификат в другом хранилище.
CertAddEncodedCertificateToStore	+	+	Функция создает контекст сертификата из закодированного сертификата и добавляет его в хранилище сертификатов. Созданный контекст не содержит никаких расширенных свойств.
CertEnumCertificatesInStore	+	+	Функция получает первый или следующий сертификат в хранилище сертификатов. Эта функция используется в цикле для того, чтобы последовательно получить все сертификаты в хранилище сертификатов.
CertFreeCertificateContext	+	+	Функция освобождает контекст сертификата, уменьшая счетчик ссылок на единицу.

CertCreateCertificateContext	+	+	Функция создает контекст сертификата из закодированного сертификата. Созданный контекст не помещается в хранилище сертификатов. В созданном контексте функция размещает копию закодированного сертификата.
CertDuplicateCertificateContext	+	+	Функция дублирует контекст сертификата, увеличивая счетчик ссылок на единицу.
CertFindCertificateInStore	+	+	Функция находит первый или следующий контекст сертификата в хранилище сертификатов, который соответствует критерию поиска, определяемому параметром dwFindType и связанным с ним pvFindPara.
CertDeleteCertificateFromStore	+	+	Функция удаляет определенный контекст сертификата из хранилища сертификатов.
CertGetSubjectCertificateFromStore	+	+	Функция получает контекст сертификата из хранилища сертификатов, однозначно определяемый его издателем и серийным номером.
CertGetIssuerCertificateFromStore	+	+	Поиск сертификатов издателей заданного сертификата.
CertGetSubjectCertificateFromStore	+	+	Поиск сертификата по серийному номеру и издателю.
CertGetValidUsages	+	-	Поиск пересечения KeyUsage для массива сертификатов.
CertSerializeCertificateStoreElement	+	+	Сериализация элемента хранилища.
CertRetrieveLogoOrBiometricInfo	+	-	Получение дополнительных расширений из сертификата.

Функции для работы с протоколом OCSP (crypt32.dll)

Функция	Windows	Linux	Описание
CertAddRefServerOcspResponse	+	-	Увеличение счетчика ссылок на OCSP-ответ.
CertAddRefServerOcspResponseContext	+	-	Увеличение счетчика ссылок на контекст OCSP-ответа.
CertCloseServerOcspResponse	+	-	Закрытие дескриптора OCSP-ответа.
CertGetServerOcspResponseContext	+	-	Получение контекста OCSP-ответа.
CertOpenServerOcspResponse	+	-	Открытие дескриптора OCSP-ответа для заданной цепочки сертификатов.

Функции для работы с окнами (cryptui.dll, libcryptui.so)

Функция	Windows	Linux	Описание
CertSelectCertificate	+	-	Отображение диалога выбора сертификата по заданным критериям.
CryptUIDlgCertMgr	+	-	Отображение диалога управления сертификатами.
CryptUIDlgSelectCertificate	+	-	Отображение диалога выбора сертификата.
CryptUIDlgSelectCertificateFromStore	+	-	Отображение диалога выбора сертификата из хранилища.
CryptUIDlgViewCertificate	+	-	Отображение диалога со свойствами сертификата.
CryptUIDlgViewContext	+	+	Отображение сертификата, списка CRL или CTL.
CryptUIDlgViewSignerInfo	+	-	Отображение диалога с информацией о подписавшем.
CertSelectionGetSerializedBlob	+	-	Сериализация сертификата из структуры, используемой для отображения.
GetFriendlyNameOfCert	+	-	Преобразование имени сертификата к «читаемому» виду.

Функции для проверки цепочек сертификатов (crypt32.dll, libcrypt32.so)

Функция	Windows	Linux	Описание
CertVerifyCertificateChainPolicy	+	+	Функция проверяет цепочку сертификатов на достоверность, включая соответствие ее некоторому критерию истинности.
CertGetCertificateChain	+	+	Функция строит цепочку сертификатов, начиная с последнего сертификата, в обратном направлении до доверенного корневого сертификата, если это возможно.
CertFreeCertificateChain	+	+	Функция освобождает цепочку сертификатов путем уменьшения счетчика ссылок. Если счетчик ссылок равен нулю, то память, выделенная под цепочку, освобождается.
CertCreateCertificateChainEngine	+	+	Функция создает контекст HCERTCHAINENGINE, который позволяет изменять параметры механизма построения цепочки сертификатов. Позволяет ограничивать множество доверенных сертификатов.
CertFreeCertificateChainEngine	+	+	Функция CertFreeCertificateChainEngine освобождает контекст HCERTCHAINENGINE.
CertCreateCTLEntryFromCertificateContextProperties	+	-	Создание CTL на основе свойств атрибутов контекста сертификата.
CertDuplicateCertificateChain	+	+	Дублирование контекста цепочки.
CertFindChainInStore	+	-	Функция построения цепочки по заданным критериям из хранилища.
CertFreeCertificateChainList	+	-	Функция освобождения массива цепочек.
CertIsValidCRLForCertificate	+	+	Функция проверки наличия сертификата в списке CRL.
CertSetCertificateContextPropertiesFromCTLEntry	+	-	Установка свойств в контекст сертификата на основе CTL.

**Функции для работы с расширенными свойствами сертификата (EKU)
(crypt32.dll, libcrypt32.so)**

Функция	Windows	Linux	Описание	Комментарий
CertGetEnhancedKeyUsage	+	-	Функция получает информацию о расширенном использовании ключа из соответствующего расширения или из расширенных свойств сертификата. Расширенное использование ключа служит признаком правомерного использования сертификата.	
CryptAcquireCertificatePrivateKey	+	+	Функция получает дескриптор HCRYPTPROV и параметр dwKeySpec для определенного контекста сертификата.	

Функции для работы с объектными идентификаторами (crypt32.dll, libcrypt32.so)

Функция	Windows	Linux	Описание
CryptFindOIDInfo	+	+	Функция CryptFindOIDInfo получает первую предопределенную или зарегистрированную структуру CRYPT_OID_INFO, согласованную с определенным типом ключа и с ключом.
CryptEnumOIDInfo	+	+	Перечисление зарегистрированных идентификаторов и получение информации для них

Функции для работы с хранилищем сертификатов (crypt32.dll, libcrypt32.so)

Функция	Windows	Linux	Описание
CertOpenStore	+	+	Функция открывает хранилище сертификатов, используя заданный тип провайдера.
CertDuplicateStore	+	+	Функция дублирует дескриптор хранилища, увеличивая счетчик ссылок на хранилища на единицу.
CertOpenSystemStore	+	+	Функция используется для открытия наиболее часто используемых хранилищ сертификатов.
CertCloseStore	+	+	Функция закрывает дескриптор хранилища сертификатов и уменьшает счетчик ссылок на хранилища на единицу.
CertAddStoreToCollection	+	+	Добавление хранилища в коллекцию.
CertControlStore	+	-	Установка нотификации при различиях в заэкшированном хранилище и физическом хранилище.

Функции для работы с открытыми данными и объектами (crypt32.dll)

Функция	Windows	Linux	Описание
CryptImportPublicKeyInfoEx2	+	-	Функция импортирует информацию об открытом ключе в CNG и возвращает дескриптор открытого ключа.
CryptImportPublicKeyInfoEx	+	+	Функция импортирует информацию об открытом ключе в CSP и возвращает дескриптор открытого ключа.
CryptImportPublicKeyInfo	+	+	Функция преобразует и импортирует информацию об открытом ключе в провайдер и возвращает дескриптор открытого ключа.
CryptExportPublicKeyInfoEx	+	+	Функция экспортирует информацию об открытом ключе, связанную с соответствующим секретным ключом провайдера.

Функция	Windows	Linux	Описание
CryptExportPublicKeyInfo	+	+	Функция экспортирует информацию об открытом ключе, ассоциированную с соответствующим секретным ключом провайдера.
CertCompareIntegerBlob	+	+	Функция сравнивает два целочисленных блока для того чтобы определить, представляют ли они собой два равных числа.
CryptExportPublicKeyInfoFromBCryptKeyHandle	+	-	Экспортирует информацию об открытом ключе, ассоциированную с соответствующим секретным ключом провайдера.
CertComparePublicKeyInfo	+	+	Функция сравнивает два закодированных открытых ключа на предмет их идентичности.
CertVerifyCRLRevocation	+	+	Функция проверяет список CRL, чтобы определить, аннулирован ли переданный в функцию сертификат или нет.
CertVerifyCRLTimeValidity	+	+	Функция проверяет время действия CRL.
CertVerifyRevocation	+	+	Функция проверяет статус отзыва сертификатов из массива rgpvContext.
CryptQueryObject	+	-	Функция получает информацию об объекте криптографического API, таком как сертификат, список CRL или список доверия сертификатов (CTL).
CertGetPublicKeyLength	+	-	Функция возвращает размер открытого ключа в битах.
CryptHashCertificate	+	+	Функция хэширует целиком закодированный сертификат, включая его подпись.
CryptHashCertificate2	+	-	Функция хэширует блок данных с помощью криптопровайдера хэша CNG.
CryptHashToBeSigned	+	-	Функция вычисляет хэш закодированного контента из подписанного и закодированного сертификата.
CertVerifyTimeValidity	+	+	Функция используется для проверки времени действия сертификата.

Функция	Windows	Linux	Описание
CertVerifyValidityNesting	+	-	Функция используется для проверки того, что интервал времени действия сертификата субъекта корректно содержится внутри интервала времени действия сертификата издателя.
CryptFindCertificateKeyProvInfo	+	-	Функция перебирает все провайдеры и все контейнеры ключей этих провайдеров для того, чтобы найти контейнер с закрытым ключом, соответствующий открытому ключу сертификата.
CryptSignAndEncodeCertificate	+	+	Функция кодирует и подписывает сертификат, список CRL, список доверенных сертификатов (CTL) или запрос на сертификат.
CryptSignCertificate	+	+	Функция подписывает to-be-signed-информацию в закодированном подписанном контенте.
CryptVerifyCertificateSignature	+	+	Функция проверяет подпись сертификата, списка CRL или запроса на сертификат. Функция не требует доступа к закрытому ключу.
CryptVerifyCertificateSignatureEx	+	+	Функция проверяет подпись сертификата, список CRL или запроса на сертификат. Функция не требует доступа к закрытому ключу.

Функции для кодирования и декодирования сертификатов (crypt32.dll, libcrypt32.so)

Функция	Windows	Linux	Описание
CryptDecodeObject	+	+	Функция используются для декодирования сертификатов, списков CRL и запросов на сертификаты.
CryptDecodeObjectEx	+	+	Функция используются для декодирования сертификатов, списков CRL и запросов на сертификаты
CryptEncodeObject	+	+	Функция используются для кодирования сертификатов, списков CRL и запросов на сертификаты.
CryptEncodeObjectEx	+	+	Функция используются для кодирования сертификатов, списков CRL и запросов на сертификаты.

Функции для получения объектов из удаленных источников (cryptnet.dll, libcryptnet.so)

Функция	Windows	Linux	Описание
CryptRetrieveObjectByUrlA	+	+	Функция получает объект инфраструктуры открытых ключей по заданному URL.
CryptRetrieveObjectByUrlW	+	+	Функция является Unicode-версией функции CryptRetrieveObjectByUrlA.
CryptGetObjectUrl	+	+	Функция извлекает URL удаленного объекта из сертификата.

Функции для работы с данными формата PFX (crypt32.dll)

Функция	Windows	Linux	Описание
PFXExportCertStore	+	-	Экспорт сертификата и ассоциированного секретного ключа (если такой существует).
PFXExportCertStoreEx	+	-	Экспорт сертификата и ассоциированного секретного ключа (если такой существует).
PFXImportCertStore	+	-	Импорт сертификата и ассоциированного секретного ключа (если такой существует) в провайдер.
PFXIsPFXBlob	+	-	Проверка, имеют ли данные формат PFX.
PFXVerifyPassword	+	-	Проверка соответствия переданного пароля паролю для расшифрования PFX.

Функции для подписи и формирования штампов времени (mssign32.dll)

Функция	Windows	Linux	Описание
SignerTimeStamp	+	-	Получение штампа времени для Authenticode.
SignerTimeStampEx	+	-	Получение штампа времени для Authenticode.
SignerTimeStampEx2	+	-	Получение штампа времени в соответствии с RFC 5161 и Authenticode.

SignerTimeStampEx3	+	-	Получение штампа времени в соответствии с RFC 5161 и Authenticode.
SignError	+	-	Преобразование кода ошибки.
SignerSign	+	-	Подпись файла со штампом времени.
SignerSignEx	+	-	Подпись файла со штампом времени.
SignerSignEx2	+	-	Подпись файла со штампом времени.
SignerFreeSignerContext	+	-	Освобождение контекста подписи.
CryptVerifyTimeStampSignature	+	-	Функция выполняет проверку подписи под штампом времени.
CryptRetrieveTimeStamp	+	-	Функция кодирует запрос на получение метки времени и получает метку времени от сервера TSA (TimeStampingAuthority), расположенного по заданному URL.

ПРИЛОЖЕНИЕ 2

Перечень исполняемых модулей для проверки целостности при запуске СКЗИ ViPNet CSP

Минимальный список контроля целостности: boost_chrono-vc90-mt-32-1_58.dll, boost_date_time-vc90-mt-32-1_58.dll, boost_filesystem-vc90-mt-32-1_58.dll, boost_program_options-vc90-mt-32-1_58.dll, boost_regex-vc90-mt-32-1_58.dll, boost_serialization-vc90-mt-32-1_58.dll, boost_system-vc90-mt-32-1_58.dll, boost_thread-vc90-mt-32-1_58.dll, softtoken_pkcs11.dll, token_manager.exe, itcipc.dll, tools2.dll, itccsp.dll, itccspex.dll, itccspgui.dll, logdisp.dll, itcctrls.dll, itcscapi.dll, cert.dll, nonmfc.dll, certui.dll, guiext.dll, certcspactivex.dll, vpnpx.dll, clean.exe, magpkcs11.dll, rngprops.dll, ui_interface_mfc.dll, winsysevtrc.dll, asntools.dll, itcad.dll, pwdgen.dll, rngaccord.dll, rngaggregator.dll, rngbiowin.dll, rngdsdr.dll, rngtokenjava.dll, rngsobel.dll, stgsui.dll, storedev.dll, structfiles.dll, uecpkcs11.dll, boxregmgr.dll, \windows\system32\itcssp.dll, \windows\system32\itccng.dll, \windows\system32\itcspea.dll, \windows\system32\itcs-cng-provider.dll, \windows\system32\drivers\itcspe.sys, \windows\system32\drivers\itckcng.sys, \windows\system32\drivers\itcs-cng-krn.sys.

Дополнительно для платформы Win64: boost_chrono-vc90-mt-64-1_58.dll, boost_date_time-vc90-mt-64-1_58.dll, boost_filesystem-vc90-mt-64-1_58.dll, boost_program_options-vc90-mt-64-1_58.dll, boost_regex-vc90-mt-64-1_58.dll, boost_serialization-vc90-mt-64-1_58.dll, boost_system-vc90-mt-64-1_58.dll, boost_thread-vc90-mt-64-1_58.dll, softtoken_pkcs11_64.dll, softtoken_pkcs11_64.dll, itccsp64.dll, itccspgui64.dll, itccspex64.dll, itcipc64.dll, logdisp64.dll, magpkcs11_64.dll, tools2_64.dll, vpnpx64.dll, rngprops64.dll, boxregmgr64.dll, asntools64.dll, itcad64.dll, pwdgen.dll, rngaccord64.dll, rngaggregator64.dll, rngbiowin64.dll, rngdsdr64.dll, rngtokenjava64.dll, rngsobel64.dll, stgsui64.dll, storedev64.dll, structfiles64.dll, uecpkcs11_64.dll, csp_settings.dll, csp_settings_app.exe, uec_pkcs11_settings.exe, itccspksr64.dll, itccspbsr64.dll, itccspksr64.dll, itccspks64.dll, itccspbs64.dll, itccspxs64.dll, \windows\SysWOW64\itccng.dll, \windows\SysWOW64\itcspea.dll, \windows\SysWOW64\itcssp.dll, \windows\SysWOW64\itcs-cng-provider.dll, \windows\system32\itcspea64.dll, \windows\system32\drivers\itcspe64.sys, \windows\system32\drivers\itckcng64.sys, \windows\system32\drivers\itcs-cng-krn64.sys.

Отсутствуют для платформы Win64: \windows\system32\drivers\itcspe.sys, \windows\system32\drivers\itckcng.sys, \windows\system32\itcspea.dll, \windows\system32\drivers\itcs-cng-krn64.sys.

ПРИЛОЖЕНИЕ 3

Перечень исполняемых модулей ОС Windows и разделов реестра, подлежащих контролю целостности

Перечень исполняемых модулей:

\windows\apppatch\acgenral.dll
\windows\explorer.exe
\windows\system32\activeds.dll
\windows\system32\actxprxy.dll
\windows\system32\adsldpc.dll
\windows\system32\advapi32.dll
\windows\system32\advpack.dll
\windows\system32\alg.exe
\windows\system32\apphelp.dll
\windows\system32\atl.dll
\windows\system32\audiosrv.dll
\windows\system32\authz.dll
\windows\system32\autochk.exe
\windows\system32\basesrv.dll
\windows\system32\batmeter.dll
\windows\system32\bootvid.dll
\windows\system32\browser.dll
\windows\system32\browseui.dll
\windows\system32\cabinet.dll
\windows\system32\certcli.dll
\windows\system32\clbcatq.dll
\windows\system32\clusapi.dll
\windows\system32\cnbjmon.dll
\windows\system32\colbact.dll
\windows\system32\comctl32.dll
\windows\system32\comdlg32.dll
\windows\system32\comres.dll
\windows\system32\comsvcs.dll
\windows\system32\credui.dll
\windows\system32\crypt32.dll
\windows\system32\cryptdll.dll
\windows\system32\cryptsvc.dll
\windows\system32\cryptui.dll
\windows\system32\cscdll.dll
\windows\system32\cscui.dll
\windows\system32\csrssrv.dll
\windows\system32\csrss.exe
\windows\system32\ctfrnon.exe
\windows\system32\davclnt.dll
\windows\system32\dhcpcsvc.dll
\windows\system32\dmserver.dll
\windows\system32\dmusic.dll
\windows\system32\dnsapi.dll
\windows\system32\dnsrslvr.dll

\windows\system32\dpcdll.dll
\windows\system32\drprov.dll
\windows\system32\dssenh.dll
\windows\system32\ersvc.dll
\windows\system32\es.dll
\windows\system32\esent.dll
\windows\system32\eventlog.dll
\windows\system32\framebuf.dll
\windows\system32\gdi32.dll
\windows\system32\hal.dll
\windows\system32\hnetcfg.dll
\windows\system32\icaapi.dll
\windows\system32\icmp.dll
\windows\system32\imagehlp.dll
\windows\system32\imapi.exe
\windows\system32\inetpp.dll
\windows\system32\iphlpapi.dll
\windows\system32\ipnathlp.dll
\windows\system32\kbdru.dll
\windows\system32\kbdus.dll
\windows\system32\kdcom.dll
\windows\system32\kerberos.dll
\windows\system32\kernel32.dll
\windows\system32\linkinfo.dll
\windows\system32\lmhsvc.dll
\windows\system32\localspl.dll
\windows\system32\lsasrv.dll
\windows\system32\lsass.exe
\windows\system32\mfc42.dll
\windows\system32\midimap.dll
\windows\system32\mnmdd.dll
\windows\system32\mpr.dll
\windows\system32\mprapi.dll
\windows\system32\msacm32.dll
\windows\system32\msasn1.dll
\windows\system32\msctf.dll
\windows\system32\msgina.dll
\windows\system32\msi.dll
\windows\system32\msidle.dll
\windows\system32\msimg32.dll
\windows\system32\msisip.dll
\windows\system32\mspacha.dll
\windows\system32\msprivs.dll
\windows\system32\mstask.dll
\windows\system32\mstlsapi.dll
\windows\system32\msutb.dll
\windows\system32\msvl_0.dll
\windows\system32\msvc60.dll
\windows\system32\msvcrt.dll
\windows\system32\mswsock.dll
\windows\system32\msxml3.dll

\windows\system32\mtxclu.dll
\windows\system32\ncobjapi.dll
\windows\system32\nddeapi.dll
\windows\system32\netapi32.dll
\windows\system32\netcfgx.dll
\windows\system32\netlogon.dll
\windows\system32\netman.dll
\windows\system32\netmsg.dll
\windows\system32\netrap.dll
\windows\system32\netshell.dll
\windows\system32\netui0.dll
\windows\system32\netuil.dll
\windows\system32\ntdll.dll
\windows\system32\ntdsapi.dll
\windows\system32\ntlanman.dll
\windows\system32\ntmarta.dll
\windows\system32\ntoskrnl.exe
\windows\system32\ntshrui.dll
\windows\system32\odbc32.dll
\windows\system32\odbcint.dll
\windows\system32\ole32.dll
\windows\system32\oleacc.dll
\windows\system32\oleaut32.dll
\windows\system32\pautoenr.dll
\windows\system32\pjlmon.dll
\windows\system32\powrprof.dll
\windows\system32\profmap.dll
\windows\system32\psapi.dll
\windows\system32\psbase.dll
\windows\system32\pstorsvc.dll
\windows\system32\rasatlilp.dll
\windows\system32\rasapi32.dll
\windows\system32\raschap.dll
\windows\system32\rasdlg.dll
\windows\system32\rasman.dll
\windows\system32\rastls.dll
\windows\system32\regapi.dll
\windows\system32\regsvc.dll
\windows\system32\resutils.dll
\windows\system32\riched20.dll
\windows\system32\rpcrt4.dll
\windows\system32\rpcss.dll
\windows\system32\rsaenh.dll
\windows\system32\rtutils.dll
\windows\system32\rundll32.exe
\windows\system32\samlib.dll
\windows\system32\samsrv.dll
\windows\system32\scecli.dll
\windows\system32\scesrv.dll
\windows\system32\schannel.dll
\windows\system32\schedsvc.dll

\windows\system32\seclogon.dll
\windows\system32\secur32.dll
\windows\system32\sens.dll
\windows\system32\services.exe
\windows\system32\setupapi.dll
\windows\system32\sfc.exe
\windows\system32\sfc_os.dll
\windows\system32\sfcfiles.dll
\windows\system32\shdoclc.dll
\windows\system32\shdocvw.dll
\windows\system32\shell32.dll
\windows\system32\shfolder.dll
\windows\system32\shimeng.dll
\windows\system32\shlwapi.dll
\windows\system32\shsvcs.dll
\windows\system32\smss.exe
\windows\system32\spoolss.dll
\windows\system32\spoolsv.exe
\windows\system32\srsvc.dll
\windows\system32\svrsvc.dll
\windows\system32\ssdpapi.dll
\windows\system32\ssdpsrv.dll
\windows\system32\stobject.dll
\windows\system32\svchost.exe
\windows\system32\sxs.dll
\windows\system32\tapi32.dll
\windows\system32\tcpmon.dll
\windows\system32\termsrv.dll
\windows\system32\themeui.dll
\windows\system32\trkwks.dll
\windows\system32\twext.dll
\windows\system32\umpnpgmgr.dll
\windows\system32\upnp.dll
\windows\system32\urlmon.dll
\windows\system32\usbmon.dll
\windows\system32\user32.dll
\windows\system32\userenv.dll
\windows\system32\userinit.exe
\windows\system32\uxtheme.dll
\windows\system32\version.dll
\windows\system32\vga.dll
\windows\system32\vga256.dll
\windows\system32\vga64k.dll
\windows\system32\vssapi.dll
\windows\system32\w32time.dll
\windows\system32\watchdog.sys
\windows\system32\wbem\esscli.dll
\windows\system32\wbem\fastprox.dll
\windows\system32\wbem\ncprov.dll
\windows\system32\wbem\repdrvfs.dll
\windows\system32\wbem\wbemcomn.dll

\windows\system32\wbem\wbemcons.dll
\windows\system32\wbem\wbemcore.dll
\windows\system32\wbem\wbemess.dll
\windows\system32\wbem\wbemprox.dll
\windows\system32\wbem\wbemsvc.dll
\windows\system32\wbem\wmiprvse.dll
\windows\system32\wbem\wmisvc.dll
\windows\system32\wbem\wmiutils.dll
\windows\system32\wdigest.dll
\windows\system32\webcheck.dll
\windows\system32\webclnt.dll
\windows\system32\win32k.sys
\windows\system32\wm32spl.dll
\windows\system32\winhttp.dll
\windows\system32\wminet.dll
\windows\system32\winlogon.exe
\windows\system32\winmm.dll
\windows\system32\winnr.dll
\windows\system32\winscard.dll
\windows\system32\winpool.exe
\windows\system32\winsrv.dll
\windows\system32\winsta.dll
\windows\system32\wintrust.dll
\windows\system32\wkssvc.dll
\windows\system32\wldap32.dll
\windows\system32\wlnotify.dll
\windows\system32\wmi.dll
\windows\system32\ws2_32.dll
\windows\system32\ws2help.dll
\windows\system32\wscsv.dll
\windows\system32\wshext.dll
\windows\system32\wshnetbs.dll
\windows\system32\wshtcpip.dll
\windows\system32\wsock32.dll
\windows\system32\wtsapi32.dll
\windows\system32\wuauclt.exe
\windows\system32\wuaueng.dll
\windows\system32\wuauserv.dll
\windows\system32\wups.dll
\windows\system32\wzcsapi.dll
\windows\system32\wzcsv.dll
\windows\system32\xpob2res.dll
\windows\system32\xpsp2res.dll
\ntldr
\ntdetect.com

Перечень разделов реестра:

HKLM\System\CurrentControlSet\Control

HKLM\System\CurrentControlSet\Services

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
HKLM\Software\Microsoft\Windows\CurrentVersion\Shell Extensions

Дополнительно для платформы Win64:

\Windows\SysWOW64

[illegible]