УТВЕРЖДЕН

ФРКЕ.00106-04 99 01 ПП-ЛУ

Средство криптографической защиты информации

ViPNet CSP 4.2

Правила пользования

ФРКЕ.00106-04 99 01 ПП

2017

Содержание

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, предаваемых по протоколу TLS (Transport Layer Security)/SSL (Secure Sockets Layer) (только варианты исполнения 1–3);
- формирования ключей шифрования;
- формирования транспортных контейнеров ключей в формате PKCS #12 (PFX) (только варианты исполнения 1–3);
- выработки случайных двоичных последовательностей.

СКЗИ ViPNet CSP предназначено для встраивания в программное обеспечение (далее – ПО), ViPNet производства ОАО «ИнфоТеКС» и в прикладное ПО других производителей, а также для поставки конечным пользователям, использующим ПО, которое обращается к криптографическим функциям через системные интерфейсы.

СКЗИ ViPNet CSP предназначено для использования в системах защиты информации, не содержащей сведений, составляющих государственную тайну, и может вывозиться с территории Российской Федерации в соответствии с законодательством Российской Федерации в области экспортного контроля и (или) таможенным законодательством Евразийского экономического союза в качестве самостоятельных изделий или в составе указанных систем.

СКЗИ ViPNet CSP соответствует пункту 12 приложения № 2 к Положению о ввозе на таможенную территорию Евразийского экономического союза и вывозе с таможенной территории Евразийского экономического союза шифровальных (криптографических) средств (в ред. решения Коллегии Евразийской экономической комиссии от 06.10.2015 № 131).

1.1 Состав программных средств СКЗИ ViPNet CSP

СКЗИ ViPNet CSP поставляется в пяти вариантах исполнения. 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) (варианты исполнения 1-5);

- набор криптографических функций – динамическая библиотека, предназначенная для встраивания в приложения, использующие вызовы криптографических функций через интерфейс RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki) V2.30 (далее – PKCS #11) (варианты исполнения 1-5);
- 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) (варианты исполнения 1-5);
- набор криптографических функций – динамическая библиотека, предназначенная для встраивания в приложения, использующие вызовы криптографических функций через интерфейс MS CryptoApi (только для вариантов исполнения 1, 2 и 3), включая поддержку протоколов и форматов X.509, PKCS #10, CMC, PKCS#5, PKCS#12 (PFX), PKCS#7 (CMS);
- набор криптографических функций – динамическая библиотека, предназначенная для встраивания в приложения, использующие вызовы криптографических функций через интерфейс ViPNet CryptApi (только для вариантов исполнения 4 и 5), включая реализацию протоколов и форматов X.509, PKCS #10, PKCS#5, PKCS#12 (PFX), PKCS#7 (CMS);
- COM-объекты для доступа к криптографическим функциям (только для вариантов исполнения 1, 2 и 3);
- динамическая библиотека реализации протоколов SSL 2.0, SSL 3.0, TLS 1.0 (включая расширения RFC 4346, RFC 5246) (только для вариантов исполнения 1, 2 и 3);
- устройство типа «электронный замок» (только для вариантов исполнения 2, 3 и 5);
- 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 [8].

1.2 Требования к составу технических средств и операционным системам

СКЗИ ViPNet CSP предназначено для использования на компьютерах (стационарных, переносных), поддерживающих архитектуру x86, x86-64 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 (только для вариантов исполнения 1, 2 и 3):

- Windows 7 (32/64-разрядная);
- Windows 8 (64-разрядная);
- Windows 8.1 (32/64-разрядная);
- Windows 10 (32/64-разрядная);
- Windows Server 2008 R2 (64-разрядная);
- Windows Server 2012 (64-разрядная);
- Windows Server 2012 R2 (64-разрядная).

Примечания:

1 Необходимо использовать ОС, поддерживаемые их производителем. Для ОС должен быть установлен последний пакет обновления ОС (Service Pack) и все известные критические обновления, опубликованные производителем ОС.

2 При прекращении производителем поддержки ОС и связанных с этим дополнительных угрозах безопасности информации дальнейшее применение изделия должно проводиться с учетом реализации дополнительных мер защиты информации, направленных на блокирование данных угроз. В этих целях рекомендуется:

- спланировать мероприятия по переводу информационных систем на ОС, поддерживаемые их производителями;
- в случае продолжения использования ОС, не поддерживаемой производителем:
  - установить все актуальные обновления, выпущенные до прекращения поддержки данной ОС;
  - установить запрет на автоматическое обновление ОС с даты прекращения её поддержки;
  - провести настройку и обеспечивать периодический контроль механизмов защиты неподдерживаемых ОС в соответствии с руководствами по безопасной настройке и контролю ОС;

- по возможности исключить подключение к сети Интернет и к ведомственным (корпоративным) локальным вычислительным сетям средств вычислительной техники или сегментов информационных систем, работающих под управлением неподдерживаемых ОС;
- при невозможности отключения от сети Интернет и/или от ведомственных (корпоративных) локальных вычислительных сетей средств вычислительной техники или сегментов информационных систем, работающих под управлением неподдерживаемых ОС, применять в обязательном порядке меры по сегментированию информационных систем и защите периметра информационной системы и выделенных сегментов (в том числе путем применения сертифицированных межсетевых экранов, средств антивирусной защиты, систем обнаружения вторжений, средств защиты от несанкционированной передачи (вывода) информации (DLP - систем), средств управления потоками информации);
- обеспечить регулярное резервное копирование информации, программного обеспечения и средств защиты информации, содержащихся на средствах вычислительной техники или в сегментах информационных систем, работающих под управлением неподдерживаемых ОС, на внешние носители информации;
- регламентировать и обеспечивать контроль за применением съемных машинных носителей информации, исключив при этом использование не зарегистрированных в информационной системе машинных носителей информации и не проверенных средствами антивирусной защиты;
- проводить периодический анализ уязвимостей сегментов информационных систем, работающих под управлением неподдерживаемых ОС, с использованием сертифицированных средств контроля (анализа) защищенности информации, а также периодический контроль целостности установленных ОС;
- проводить мониторинг общедоступных источников, публикующих сведения об уязвимостях, на предмет появления в них информации об уязвимостях в неподдерживаемых ОС и принимать меры, направленные на устранение выявленных уязвимостей или исключающие возможность

использования нарушителями выявленных уязвимостей (в том числе за счет применения дополнительных средств защиты информации);

- разработать и внедрить правила и процедуры действий должностных лиц в случае выявления уязвимостей в неподдерживаемых ОС или возникновения инцидентов информационной безопасности, связанных с их применением.

СКЗИ ViPNet CSP функционирует под управлением ОС Гослинукс 6, 6.4 (32/64-разрядных), Astra Linux 1.4, 1.5 (32/64-разрядных), а также ОС семейства Linux (32/64-разрядных) удовлетворяющих требованиям Linux Standard Base 4.1:

- CentOS 4.7, 5.2, 6.0;
- Debian 4, 5, 6, 7;
- Fedora 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18;
- Mandriva 2006, 2007, 2008, 2009, 2010, 2011;
- Mandriva Corporate Server 4;
- openSUSE 10, 11, 12;
- Oracle Linux 5, 5.3, 6;
- RHEL 4, 5, 6;
- SLES 9, 10, 11;
- Ubuntu 7, 8, 9, 10, 11, 12, 13, 14;
- Ubuntu Server 14.04.

СКЗИ ViPNet CSP (варианты исполнения 1 и 4) функционирует в виртуальных средах:

- Microsoft Hyper-V;
- VMware Workstation;
- VMware Player;
- VMware vSphere ESX;
- VirtualBox.

Примечание. На компьютерах или в ОС виртуальной среды должен быть установлен последний известный на момент установки пакет обновления ОС (Service Pack) 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 средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих

государственную тайну, СКЗИ ViPNet CSP (варианты исполнения 2, 3, 5) 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 [4].

1.3 Дополнительное программное обеспечение

Должна быть обеспечена антивирусная защита ПК ViPNet Administrator и среды функционирования криптосредства (СФК) путем использования антивирусных средств, сертифицированных ФСБ России и (или) ФСТЭК России с учетом их компетенции.

На компьютер, где установлено СКЗИ ViPNet CSP, запрещается устанавливать средства отладки и трассировки ПО. Запрещается пользоваться измененными или отладочными версиями ОС такими, как Debug/Checked Build.

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 связи[1].

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-гигиеническими 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.

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.

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

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 [8].

3.1 Порядок распространения и учета СКЗИ ViPNet CSP

СКЗИ ViPNet CSP поставляется:

– На носителях.

– 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 стопроцентную гарантию защиты дистрибутива от подмены, в отличие от скачивания через сеть связи общего пользования.

Установка должна осуществляться в соответствии с разделом 3.3 настоящих правил пользования.

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

В случае распространения СКЗИ ViPNet CSP на носителях, СКЗИ и пакет документов к нему, изготовленные производителем (ОАО «ИнфоТеКС»), поставляется в электронном виде на компакт-диске. Формуляр на изделие поставляется в печатном виде.

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.

В случае распространения СКЗИ ViPNet CSP на носителях, передача дистрибутива и пакета документов от производителя в эксплуатирующую организацию осуществляется лично или доверенным способом администратору безопасности, ответственному за установку и эксплуатацию изделия. Администратору безопасности предоставляется экземпляр

дистрибутива, формуляр изделия в бумажном виде с указанием регистрационного номера СКЗИ, серийного номера и контрольной суммы дистрибутива, размещенного на компакт-диске.

В случае распространения СКЗИ ViPNet CSP на носителях, поэкземплярный учет предоставляемого на диске дистрибутива СКЗИ ViPNet CSP осуществляется производителем – ОАО «ИнфоТеКС» в процессе подготовки комплекта изделия.

В случае распространения СКЗИ ViPNet CSP на носителях, поэкземплярный учет копий изделия должен осуществляться в эксплуатирующей организации. Для этого:

- Администратор безопасности при установке и вводе в эксплуатацию изделия присваивает устанавливаемой копии СКЗИ учетный номер, который должен включать регистрационный номер СКЗИ, выданный ОАО «ИнфоТеКС», и идентифицирующий копию признак (например, порядковый номер инсталляции или название (номер) ТС, на которое установлена копия изделия). Между учетным номером и идентифицирующим признаком должен находиться разделяющий знак («-» или «/»).
- Администратор безопасности вносит учетный номер в журнал поэкземплярного учета.
- Для каждого установленного СКЗИ при необходимости изготавливается копия формуляра (с пометкой «Копия»), в раздел 5 которого вносится разделяющий знак и идентифицирующий копию признак. Полученный номер СКЗИ должен совпасть с приведенным в журнале поэкземплярного учёта.

Примечания:

1. Максимально допустимое количество копий СКЗИ ViPNet CSP, устанавливаемых на ТС эксплуатирующей организации, ограничивается числом, указанным в лицензионном соглашении.
2. Допускается делать необходимое число учтённых копий компакт-диска с дистрибутивом и эксплуатационной документацией.
3. Журнал поэкземплярного учёта допускается вести в бумажном или электронном виде.

В случае распространения СКЗИ ViPNet CSP через сеть связи общего пользования с сайта http://infotecs.ru/, поэкземплярный учет СКЗИ ViPNet CSP осуществляется производителем – ОАО «ИнфоТеКС» в процессе регистрации ПО. Поэкземплярный учет СКЗИ ViPNet CSP не осуществляется в случае разработки на основе СКЗИ ViPNet CSP нового СКЗИ. В этом случае необходимо проводить распространение и учет СКЗИ в соответствии с документацией на разработанное СКЗИ.

В случае распространения СКЗИ ViPNet CSP через сеть связи общего пользования с сайта http://infotecs.ru/, организация поэкземплярного 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 идентификатора[1] дистрибьютора (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 дистрибьютера[2], информация для регистрации СКЗИ ViPNet CSP поступает производителю в виде двух идентификаторов: дистрибьютора и пользователя в информационной системе дистрибьютера, позволяющих однозначно идентифицировать пользователя. Процедура загрузки, получения кода регистрации и непосредственно регистрация экземпляра СКЗИ ViPNet CSP осуществляются автоматически.

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:

[1] Уникальный идентификатор, присваиваемый производителем технологическому партнеру.
[2] Дистрибьютер в данном случае должен обладать лицензиями на распространение СКЗИ при условии применения ViPNet CSP не для собственных нужд.

- 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, 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 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, 3, 5 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 СВТ, на котором установлено СКЗИ, необходимо проверить в соответствии с «Временными методическими рекомендациями к проведению исследований ПО BIOS по документированным возможностям».

Для вариантов исполнения 2, 3, 5 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.

При наличии в BIOS соответствующих настроек, средствами BIOS должна быть исключена возможность работы на компьютере с установленным СКЗИ ViPNet CSP без проведения встроенных тестов во время начальной загрузки.

Установка СКЗИ ViPNet CSP осуществляется в соответствии с документами [2] и [3].

При установке СКЗИ ViPNet CSP в варианте исполнения 3 должна быть установлена программа ViPNet SysLocker (модуль защиты СФК) в соответствии с [4].

При установке СКЗИ ViPNet CSP в вариантах исполнения 4 и 5 должна быть установлена библиотека qt4 для обеспечения корректной работы графических пакетов.

По завершении инициализации осуществляется настройка ПО в соответствии с требованиями раздела 3.4.

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 [4];
- 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;
- для вариантов исполнения 2 и 3 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, 3 и 5 СКЗИ ViPNet CSP необходимо включить в список контроля целостности устройства типа «электронный замок» список исполняемых модулей ОС. Список модулей, подлежащих контролю целостности для вариантов исполнения 2 и 3приведен в Приложении 3. Список модулей, подлежащих контролю целостности для варианта исполнения 5, приведен в Приложении 5.

После обновления ОС администратору необходимо скорректировать список модулей, подлежащих контролю целостности.

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.

3.6 Дополнительные требования по настройке ОС Windows 10

При установке СКЗИ ViPNet CSP (варианты исполнения 1, 2, 3) на компьютер под управлением ОС Windows 10 необходимо обеспечить дополнительную защиту от потенциальных утечек информации. Вы можете сделать это двумя способами:

- вручную, задав перечисленные ниже параметры операционной системы;
- автоматически с помощью утилиты AM Privacy Protector, разработанной в группе компаний «ИнфоТеКС» (утилита не входит в комплект поставки СКЗИ ViPNet CSP).

Чтобы обеспечить дополнительную защиту для ОС Windows 10 вручную, необходимо задать следующие параметры:

- в разделе Параметры > Конфиденциальность > Отзывы и диагностика:
  - в области «Частота формирования отзывов» необходимо выбрать в списке пункт «Никогда»,
  - в области «Данные диагностики и использования» необходимо выбрать в списке пункт «Базовые сведения»;
- необходимо отключить службу Windows Search;
- необходимо отключить голосовой помощник Cortana и службу поиска Bing в разделе настроек «Параметры Кортаны и поиска»;
- необходимо заблокировать доменные имена, на которые ОС осуществляет отправку данных, используя межсетевой экран; для этого доменные имена, указанные в Приложении 7, необходимо добавить в файл \Windows\system32\drivers\etc\hosts и для IP-адресов, указанных в Приложении 7, выполнить команду route add <IP-адрес> 0.0.0.0;
- в параметрах OneDrive необходимо снять флажок «Автоматически запускать OneDrive при входе в Windows».

Утилита AM Privacy Protector доступна по следующей ссылке:
http://amonitoring.ru/cc/program/am-privacy-protector-w10/

Утилита не требует установки. После запуска утилиты для обеспечения защиты информации необходимо в группе «Windows 10» установить следующие флажки:

- «Отключить DiagTrack»;
- «Отключить Cortana, Bing, Windows Search»;
- «Настроить hosts»;
- «Отключить OneDrive».

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 ТС и ПО

В СКЗИ ViPNet CSP не предусмотрено мер контроля целостности и работоспособности ТС. Данный контроль 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, 3, 5 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.

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

Контрольные суммы дистрибутива и исполняемых модулей СКЗИ ViPNet CSP представляют собой хэш содержимого дистрибутива, вычисленный по алгоритму ГОСТ Р 34.11-2012 (длина хэш-кода 256 бит).

Указанные контрольные суммы публикуются на веб-сайте производителя ОАО «ИнфоТеКС», приводятся в формуляре на изделие, а также дублируется электронным письмом о результатах регистрации для обеспечения независимого контроля целостности.

СКЗИ ViPNet CSP оснащено встроенными механизмами проверки целостности собственных исполняемых модулей.

Для вариантов исполнения 1, 2, 3 перечень этих модулей приведен в Приложении 2. Для вариантов исполнения 4, 5 перечень этих модулей приведен в Приложении 4.

Перед запуском СКЗИ ViPNet CSP (вариант исполнения 1, 2, 3) необходимо проверить, что в папке установки СКЗИ есть пары файлов с расширениями *.crg и *.prg со следующими именами:

- Vcsp;
- Vcsp_Api;
- Vcsp_Csp;
- Vcsp_csp64;
- Vcsp_Tls;
- vcsp_ui.

Перед запуском СКЗИ ViPNet CSP (вариант исполнения 4, 5) необходимо проверить, что для каждого установленного пакета в каталоге установки СКЗИ есть соответствующая пара файлов для контроля целостности пакета: <имя пакета>.prg и <имя пакета>.crg.

Для СКЗИ ViPNet CSP (вариант исполнения 1) требования по контролю целостности реестра Windows не предъявляются.

Для СКЗИ ViPNet CSP (варианты исполнения 2, 3) целостность разделов реестра Windows обеспечивается с помощью средства защиты от НСД типа «электронный замок».

В СКЗИ ViPNet CSP (варианты исполнения 2, 3, 5) контроль целостности исполняемых модулей ОС Windows осуществляется с помощью средства защиты от НСД типа «электронный замок».

СКЗИ ViPNet CSP (варианты исполнения 1, 4) оснащено встроенными механизмами проверки целостности исполняемых модулей ОС. После установки СКЗИ ViPNet CSP в

указанных вариантах исполнения необходимо сформировать список исполняемых модулей ОС и вычислить контрольные суммы этих модулей.

Для варианта исполнения 1: типовой перечень исполняемых модулей ОС приведен в Приложении 3. Этот перечень соответствует содержимому файла os.prg, расположенного в каталоге C:\ProgramData\Infotecs\ViPNetCSP. Часть файлов из перечня может отсутствовать в некоторых сборках ОС Windows. Чтобы создать перечень исполняемых модулей ОС, под управлением которой работает конкретный компьютер, системному администратору необходимо получить в ОАО «ИнфоТеКС» специальные утилиты и запустить их со следующими параметрами:

- Infotecs.DependencyGenerator.exe depends.exe "C:\Program Files\InfoTeCS\ViPNet CSP" os.prg — для 32-разрядных ОС Windows.
- Infotecs.DependencyGenerator.exe depends.exe "C:\Program Files (x86)\InfoTeCS\ViPNet CSP" os.prg — для 64-разрядных ОС Windows.

В результате будет сформирован файл os.prg, подходящий для конкретной ОС. Для варианта исполнения 4 необходимо создать в каталоге opt/itcs файл os.prg и вписать в него перечень модулей ОС, подлежащих контролю целостности. В данный перечень должны быть включены файлы, указанные в Приложении 5.

Для вычисления контрольных сумм файлов из перечня os.prg необходимо в каталоге ViPNet CSP запустить с правами администратора утилиту make_ext_crg со следующими параметрами:

- Make_ext_crg.exe –r “C:\ProgramData\Infotecs\ViPNet CSP\os.prg” – для варианта исполнения 1.
- make_ext_crg –r /opt/itcs/os.prg – для варианта исполнения 4.

После обновления ОС системному администратору необходимо создать новый файл os.prg с перечнем исполняемых модулей ОС, а затем для редактирования этого файла требуются права администратора ОС. Для вновь сформированного списка файлов пересчитать контрольные суммы. Для этого следует выполнить те же действия, что и при начальном формировании списка.

Перед началом работы СКЗИ ViPNet CSP должен быть проведен контроль целостности при помощи утилиты check_crg. Контролем целостности должны быть охвачены файлы, перечень которых приведен в приложениях 2, 3, 4 и 5. Для этого необходимо выполнить:

- команду check_crg “C:\ProgramData\Infotecs\ViPNet CSP\os.prg” – для варианта исполнения 1;
- команду check_crg /opt/itcs/os.prg – для варианта исполнения 4.

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 модулей ViPNet CSP с помощью программы ViPNet CSP (для вариантов исполнения 1, 2, 3) или с помощью соответствующей утилиты (для вариантов исполнения 4, 5).

При каждом запуске СКЗИ ViPNet CSP осуществляется проверка модулей, входящих в СКЗИ ViPNet CSP (перечень исполняемых модулей, подлежащих контролю целостности, представлен в Приложениях 2 и 4).

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] и [3]). Такая проверка должна быть настроена для всех драйверов и библиотек, поставляемых совместно с внешними устройствами, используемыми CSP, в соответствии требованиями документации на эти устройства. 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 месяц.

После обновления ОС 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, 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 для вариантов исполнения 1-3 осуществляется только локально путем установки сертифицированной версии ПО поверх предыдущей (без предварительного удаления последней). Другие способы обновления ПО СКЗИ ViPNet CSP

недопустимы. Для вариантов исполнения 4 и 5 обновление ПО СКЗИ ViPNet CSP осуществляется путем удаления предыдущей версии и установки новой.

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 ([5], [6] и [7]), а также Приложением 1.

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 криптоядра СКЗИ ViPNet CSP, необходимо использовать протокол обмена информацией, обеспечивающий:

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

Данные требования обеспечиваются в реализации протокола TLS, входящего в состав СКЗИ ViPNet CSP (варианты исполнения 1-3), 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 криптоядра библиотеку ViPNet CSP, необходимо предусмотреть периодический контроль целостности установленного специализированного ПО.

4.3.5 Хранение аутентификационных данных

Хранение пароля от контейнера ключей и PIN-кода от съемного носителя для вариантов исполнения 1 и 3 допускается только на ТС с установленным СКЗИ ViPNet CSP, работающем в необслуживаемом или однопользовательском режиме, при условии обеспечения дополнительных организационных мер, исключающих доступ посторонних лиц к данному ТС. Во всех остальных случаях хранение пароля от контейнера ключей и PIN-кода от съемного носителя для вариантов исполнения 1 и 3 запрещено.

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 СКЗИ ViPNet CSP 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 При необходимости провести первичную инициализацию ключевой информации из имеющегося дистрибутива ключей.
4 Настроить сетевые интерфейсы и подсоединить компьютер к сети.
5 Произвести перезагрузку операционной системы.

4.5 Контроль работоспособности и соблюдения правил эксплуатации

В СКЗИ ViPNet CSP производится автоматический контроль работоспособности, который включает в себя тестовые проверки криптографических функций криптопровайдера.

Контроль работоспособности выполняется аналогичным образом для всех криптопровайдеров, входящих в СКЗИ ViPNet CSP.

Подсистема контроля работоспособности криптопровайдеров представляет собой группу функций, периодически выполняющих контрольные тесты, и основана на криптографических примитивах, реализованных в криптоядре Crypto Underground.

Первоначальный контрольный тест выполняется при запуске криптопровайдера. Затем контрольные тесты выполняются при запуске криптографических функций в случае, если аналогичный тест не выполнялся за последние 10 минут.

При обнаружении фактов сбоев в работе ПО или нарушения правил эксплуатации пользователь обязан обратиться к администратору безопасности.

4.6 Порядок выполнения технического обслуживания и регламентных работ

Регламентное техническое обслуживание устройства типа «электронный замок» проводится производителем в соответствии с документацией на это устройство.

Контрольная проверка СКЗИ ViPNet CSP выполняется в следующих случаях:

- при вводе СКЗИ ViPNet CSP в эксплуатацию;
- при изменении лица, ответственно за эксплуатацию СКЗИ;
- периодически, периодичность определяется инструкцией администратора безопасности в зависимости от числа обслуживаемых им СКЗИ и других факторов. Рекомендуемое значение – 1 раз в месяц.

Результаты проверки оформляются в виде протокола проверки в соответствии с Приложением 6.

4.7 Порядок вывода из эксплуатации и утилизации СКЗИ

Утилизация СКЗИ ViPNet CSP регламентируется разделом III «Порядок обращения с СКЗИ», утвержденным приказом ФАПСИ от 13 июня 2001 г. № 152.

Эксплуатация и утилизация устройства типа «электронный замок» и ТС, на котором функционирует ViPNet CSP, осуществляется производителем в соответствии с документацией на него.

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.

Для вариантов исполнения 1 и 3 в процессе получения доступа к внешнему устройству или контейнеру ключей запрещается включать опции «Сохранить ПИН-код» и «Сохранить пароль».

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 отчистку 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. Для вариантов исполнения 1, 2 и 3 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.

Твердотельный накопитель не должен использоваться для хранения файла подкачки. В случае использования твердотельного накопителя для хранения файлов аппаратное удаление этих файлов не гарантируется.

В вариантах исполнения 1, 2, 3, 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 /VERIFYONLY. Также, в качестве организационной меры обеспечения безопасной эксплуатации, необходимо в ОС выполнить следующие настройки:

- для политики «Время до сброса счетчика блокировки» установить значение «15 мин.»;

- для политики «Пороговое значение блокировки» – «10 ошибок входа в систему»;
- для политики «Продолжительность блокировки учетной записи» – «15 мин.».

Для вариантов исполнения 1, 2 и 3 настройка данных параметров безопасности осуществляется путем вызова через панель управления: «Администрирование» -> «Локальная политика безопасности» -> «Политики учетных записей» -> «Политика блокировки учетной записи».

Для вариантов исполнения 4 и 5 настройка данных параметров безопасности осуществляется в модуле Pluggable Authentication Modules (PAM) в соответствии с OSF-RFC 86.0 «Open Software Foundation. Request For Comments: 86.0. Pluggable Authentication Modules (PAM)». Для ОС Debian и Ubuntu настройка осуществляется следующим образом: после установки библиотеки libpam-cracklib, необходимо открыть файл /etc/pam.d/common-password и задать параметры настройки password requisite pam_cracklib.so minlen=6 auth required pam_tally2.so deny=10 unlock_time=900. Затем открыть файл /etc/login.defs и изменить максимальный срок действия пароля на 180 дней, указав значение параметра PASS_MAX_DAYS равным 180.

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 ключе защиты (например, 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.

Для варианта исполнения 3 ключи, зашифрованные на парольном ключе, должны храниться на съёмных носителях.

Твердотельный накопитель не должен использоваться для хранения ключевой информации в случае её хранения в зашифрованном на парольном ключе виде. В случае использования твердотельного накопителя для хранения файлов аппаратное удаление этих файлов не гарантируется.

При размещении ключей во встроенной защищенной памяти съемного носителя, являющегося сертифицированным СКЗИ и поддерживающим интерфейс доступа PKCS#11 и алгоритмы ГОСТ Р 34.10-2001 и/или ГОСТ Р 34.10-2012, следует руководствоваться эксплуатационной документацией на данное СКЗИ.

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, Криптотокен ЭП и ESMART Token ГОСТ сроки действия закрытых ключей ЭП этих

устройств, определенные в эксплуатационной документации этих устройств, не превышают 3 лет.

При использовании СКЗИ ViPNet CSP совместно с сертифицированным ПАК ViPNet HSM сроки действия закрытых ключей ЭП, хранящихся на этом ПАК и определенных в эксплуатационной документации этого ПАК, не превышают 5 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 следующих утилит, входящих в состав ПО ViPNet:

- clean.exe – для вариантов исполнения 1, 2, 3;
- wipe – для вариантов исполнения 4, 5.

6.1 Порядок ввода в эксплуатацию и переноса ключевой информации

Пользователь или администратор СКЗИ ViPNet CSP должен либо сгенерировать ключевые носители с помощью СКЗИ ViPNet CSP, либо ввести в эксплуатацию предварительно сгенерированную ключевую информацию в формате ключевого контейнера ViPNet CSP.

Пользователю или администратору СКЗИ ViPNet CSP разрешается производить перенос (использование) ключевой информации доверенным способом только в приведенных ниже случаях.

- Допускается использование ключевой информации, хранящейся на устройствах PKCS #11 (как с аппаратной реализацией алгоритмов ГОСТ, так и без нее) или на файловых устройствах, сгенерированных на рабочем месте с установленным ViPNet CSP, на разных рабочих местах с установленным СКЗИ ViPNet CSP.
- Допускается перенос файлов формата PKCS #12 с других СКЗИ на рабочее место с установленным СКЗИ ViPNet CSP на файловых носителях (в соответствии с рекомендациями ТК26 «Транспортный ключевой контейнер»).

- Допускается перенос ключевых файлов в формате ключевых контейнеров ViPNet CSP с одного рабочего места с установленным СКЗИ ViPNet CSP на другое рабочее место с установленным СКЗИ ViPNet CSP на файловых носителях.

6.2 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.

6.3 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.

6.4 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 (для вариантов исполнения 1, 2, 3) или утилиты wipe (для вариантов исполнения 4, 5), 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.00106-04 34 01.

3 ViPNet CSP Linux 4.2. Руководство пользователя, ФРКЕ.00106-03 34 02.

4 ViPNet SysLocker 1.0. Руководство администратора, ФРКЕ.00158-01 34 01.

5 Криптографический интерфейс ViPNet CSP 4.2. Руководство разработчика, ФРКЕ.00106-04 33 01.

6 Криптографический интерфейс ViPNet CNG 4.2. Руководство разработчика, ФРКЕ.00106-04 33 03.

7 Криптографический интерфейс ViPNet PKCS #11 VT 4.2. Руководство разработчика, ФРКЕ.00106-04 33 02.

8 Средство криптографической защиты информации ViPNet CSP 4.2. Формуляр ФРКЕ.00106-04 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`[4]	+	+	Функция используется для создания дескриптора криптопровайдера с именем контейнера ключей, определенным параметром `pszContainer`.
`CryptReleaseContext`	+	+	Функция используется для удаления дескриптора криптопровайдера, созданного `CryptAcquireContext()`.
`CryptContextAddRef`	+	+	Управляет счетчиком дескриптора, созданного `CryptAcquireContext()`.
`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. Использование разрешено при всех типах символьных аргументов, кроме PP_USER_ENCRYPTPARAMS.
`FreeCryptProvFromCertEx`	+	+	Функция используется для удаления дескриптора криптопровайдера, созданного `CryptAcquireContext()` или через CNG.

[4] Большинство функций CryptoAPI состоят из Unicode (W версия) и MultiByte (A версия) версий и макроопределения (в зависимости от макроопределения UNICODE) на один из вариант. Использование любой из этих функций и макроопределения допускается без проведения дополнительных тематических исследований. Например, допускается использование CryptAcquireContextA, CryptAcquireContextW и CryptAcquireContext. Ограничения, накладываемые на функцию должны применяться для вызова обоих вариантов и макроопределения.

Функция	Windows	Linux	Описание
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 блоба 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 откреплённых 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 откреплённыйхэш.
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 COC 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. **Примечание**. Запрещено использование с параметром dwPropId, равным CERT_KEY_PROV_INFO_PROP_ID, при условии передачи через параметр pvData структуры CRYPT_KEY_PROV_INFO, хранящей параметры PP_SIGNATURE_PIN и PP_KEYEXCHANGE_PIN, без создания отдельного криптосредства.
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 закэшированном хранилище и физическом хранилище.

Функции для работы с открытыми данными и объектами (crypt32.dll, libcrypt32.so)

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 блоба 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 криптопровайдерахэша 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.
CertGetNameString	+	+	Функция получает имя издателя или субъекта из контекста сертификата и преобразует его в строку символов с завершающим нулем.
CertNameToStr	+	+	Функция преобразует закодированное в блоб имя сертификата в строку символов с завершающим нулем.
CertCompareCertificateName	+	+	Функция сравнивает два сертификата по имени.
CertFindExtension	+	+	Функция находит первое расширение в массиве расширений сертификата или CRL, выполняя поиск по объектному идентификатору (OID).
CryptMemFree	+	+	Функция освобождения памяти

Функция	Windows	Linux	Описание
CertStrToName	+	+	Функция преобразует строковое представление имени сертификата в закодированное имя сертификата.
CryptStringToBinary	+	+	Функция преобразует форматированную строку в байтовый массив.
CryptBinaryToString	+	+	Функция преобразует байтовый массив в форматированную строку.

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 (варианты исполнения 1, 2 и 3)

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, vpnpfx.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, rngetokenjava.dll, rngsobol.dll, stgsui.dll, storedev.dll, structfiles.dll, uecpkcs11.dll, boxregmngr.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, vpnpfx64.dll, rngprops64.dll, boxregmngr64.dll, asntools64.dll, itcad64.dll, pwdgen.dll, rngaccord64.dll, rngaggregator64.dll, rngbiowin64.dll, rngdsdr64.dll, rngetokenjava64.dll, rngsobol64.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, itccspxsr64.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

Типовой 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\csrsrv.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\Iinkinfo.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\msasnI.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\mspatcha.dll
\windows\system32\msprivs.dll
\windows\system32\mstask.dll
\windows\system32\mstlsapi.dll
\windows\system32\msutb.dll
\windows\system32\msvl_0.dll
\windows\system32\msvcp60.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\rasadlilp.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\system32Vresutils.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\srvsvc.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\umpnpmgr.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\system32wbem\wbemcore.dll
\windows\system32\wbem\wbemess.dll
\windows\system32\wbem\wbemprox.dll
\windows\system32\wbem\wbemsvc.dll
\windows\system32\wbem\wmiprvsd.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\winrnr.dll
\windows\system32\winscard.dll
\windows\system32\winspool.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\wscsvc.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\wzcsvc.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

ПРИЛОЖЕНИЕ 4

Перечень исполняемых модулей для проверки целостности при использовании СКЗИ ViPNet CSP (варианты исполнения 4 и 5)

/opt/itcs/bin

certmgr, certmgr-gui, certreq, check_prg, cryptofile, csp-integral-test, license, regsvr32, rngcmgr, rngqtmgr, token_manager, wipe, csp-gost, make_ext_crg.

/opt/itcs/lib

libadvapi32.so, libbcrypt.so, libcrypt32.so, libcryptnet.so, libcryptui.so, libipc.so, libitcad.so, libitccspex.so, libitcscng.so, libkernel32.so, librngaccord.so, librngaggregator.so, librngbiokb.so, librngbiox11.so, librngdsdr.so, librngpropsqt.so, librngunixdev.so, libshell32.so, libsofttoken_pkcs11.so, libstoredev.so, libstructfiles.so, libvipnetcsp-cui.so, libvipnetcsp-gui.so, libvipnetcsp.so, librngsobol.so.

ПРИЛОЖЕНИЕ 5

Перечень исполняемых модулей ОС Linux, подлежащих контролю целостности

- Master Boot Record;
- загрузочный сектор основного раздела ОС Linux (PBR);
- сектора 1-63 относительно начала загрузочного раздела (grub stage - 1.5);
- непосредственно сам загрузчик (/boot/grub/stage2);
- файлы конфигурации загрузчика (/boot/grub/grub.conf);
- ядро Linux (/boot/vmlinuz-xxx, /boot/kernel-xxx);
- initramfs-образ (/boot/initrd-xxx);
- прочие файлы конфигурации и критичные данные ОС.

ПРИЛОЖЕНИЕ 6

Протокол контрольной проверки СКЗИ ViPNet CSP (варианты исполнения 1, 2, 3)

«___» _____ 20___ г.

СКЗИ ViPNet CSP установлен

в_____
наименование подразделения

по адресу_____

в соответствии с эксплуатационной документацией и введен в эксплуатацию.

в помещении №_____.

Акт о вводе в эксплуатацию №_____от _____.

Таблица 1 – Состав и результаты проверок и контрольных тестов

Описание действий	**Ожидаемый результат**	**Результат (+/-)**
Формирование тестового запроса на сертификат с созданием контейнера ключей на жестком диске компьютера	Создание контейнера ключей с ключевой парой на жестком диске компьютера	
Формирование тестового запроса на сертификат с созданием контейнера ключей на внешнем устройства	Создание контейнера ключей с ключевой парой на внешнем устройстве	
Экспорт контейнера ключей в формате PKCS #12	Создание транспортного контейнера PFX	
Проверка «биологического» ДСЧ с помощью соответствующей кнопки в разделе **Датчик случайных чисел** программы настройки ViPNet CSP	Появление окна с сообщением об успешной проверке ДСЧ	

Запуск регламентной проверки ДСЧ с помощью кнопки **Запустить статический контроль ДСЧ** в разделе **Дополнительно** программы настройки ViPNet CSP	Появление окна с сообщением об успешной проверке ДСЧ	
Проверка событий ViPNet CSP в системном журнале Windows	Отсутствие ошибок, вызванных ViPNet CSP, в системном журнале Windows	

Протокол контрольной проверки СКЗИ ViPNet CSP (варианты исполнения 4, 5)

«___» _____ 20___ г.

СКЗИ ViPNet CSP установлен

в_____
наименование подразделения

по адресу_____

в соответствии с эксплуатационной документацией и введен в эксплуатацию.

в помещении №_____.

Акт о вводе в эксплуатацию №_____от _____.

Таблица 2 – Состав и результаты проверок и контрольных тестов

Описание действий	**Ожидаемый результат**	**Результат (+/-)**
Формирование тестового запроса на сертификат с созданием контейнера ключей на жестком диске компьютера с помощью утилиты certreq	Создание контейнера ключей с ключевой парой на жестком диске компьютера	
Формирование тестового запроса на сертификат с созданием контейнера ключей на внешнем устройства	Создание контейнера ключей с ключевой парой на внешнем устройстве	
Проверка «биологических» ДСЧ с помощью утилиты rngcmgr или rngqtmgr	Появление окна с сообщением об успешной проверке ДСЧ	
Проверка событий ViPNet CSP в системном журнале регистрации событий	Отсутствие ошибок, вызванных ViPNet CSP, в системном журнале регистрации событий	

ПРИЛОЖЕНИЕ 7

IP-адреса и доменные имена, на которые ОС Windows 10 осуществляет отправку данных

65.52.108.92
64.4.54.117
a.ads1.msn.com
a-0001.a-msedge.net
a-0002.a-msedge.net
a-0003.a-msedge.net
a-0004.a-msedge.net
a-0005.a-msedge.net
a-0006.a-msedge.net
a-0007.a-msedge.net
a-0008.a-msedge.net
a-0009.a-msedge.net
ads.msn.com
az361816.vo.msecnd.net
az512334.vo.msecnd.net
choice.microsoft.com
choice.microsoft.com.nsatc.net
compatexchange.cloudapp.net
corp.sts.microsoft.com
corpext.msitadfs.glbdns2.microsoft.com
df.telemetry.microsoft.com
diagnostics.support.microsoft.com
feedback.microsoft-hohm.com
feedback.search.microsoft.com
feedback.windows.com
i1.services.social.microsoft.com
i1.services.social.microsoft.com.nsatc.net
msnbot-65-55-108-23.search.msn.com
oca.telemetry.microsoft.com
oca.telemetry.microsoft.com.nsatc.net
pre.footprintpredict.com
preview.msn.com
rad.msn.com
redir.metaservices.microsoft.com
reports.wes.df.telemetry.microsoft.com
services.wes.df.telemetry.microsoft.com
settings-sandbox.data.microsoft.com
sls.update.microsoft.com.akadns.net
sqm.df.telemetry.microsoft.com
sqm.telemetry.microsoft.com
sqm.telemetry.microsoft.com.nsatc.net
ssw.live.com
statsfe2.update.microsoft.com.akadns.net
statsfe2.ws.microsoft.com
survey.watson.microsoft.com
telecommand.telemetry.microsoft.com
telecommand.telemetry.microsoft.com.nsatc.net
telemetry.appex.bing.net
telemetry.microsoft.com
telemetry.urs.microsoft.com
vortex.data.microsoft.com
vortex-sandbox.data.microsoft.com
vortex-win.data.microsoft.com
watson.live.com
watson.microsoft.com
watson.ppe.telemetry.microsoft.com
watson.telemetry.microsoft.com
watson.telemetry.microsoft.com.nsatc.net
wes.df.telemetry.microsoft.com

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					