УТВЕРЖДАЮ
Генеральный директор
ООО «КРИПТО-ПРО»
_____ Н.Г.Чернова
«___» _____ 2016 года

ИЗВЕЩЕНИЕ ОБ ИЗМЕНЕНИЯХ

ООО «КРИПТО-ПРО»	ОТД	ИЗВЕЩЕНИЕ	ОБОЗНАЧЕНИЕ
	ОЛС	ЖТЯИ.00050-03.1-2016	ЖТЯИ.00050-03

ДАТА ВЫПУСКА	СРОК ИЗМЕНЕНИЯ			Лист	Листов
28.03.2016	С момента утверждения извещения об изменениях в ЖТЯИ.00050-03			1	3

ПРИЧИНА	Утверждение внешнего интерфейса	КОД 3
УКАЗАНИЯ О ЗАДЕЛЕ	Не отражается	
УКАЗАНИЯ О ВНЕДРЕНИИ	После проведения контроля	
ПРИМЕНЯЕМОСТЬ	ЖТЯИ.00050-03	
РАЗОСЛАТЬ	ФСБ России, ООО «ЦСИ», ООО «КРИПТО-ПРО»	
ПРИЛОЖЕНИЕ	Перечень вызовов…	

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
1	ЖТЯИ.00050-03 90 05. Руководство программиста. Добавлен п.4 «Использование программных интерфейсов», имеющий следующее содержание: «Разработка программного обеспечения на основе СКЗИ «КриптоПро CSP» v. 3.6.1 с учетом п. 1.5 Формуляра ЖТЯИ.00050-03 30 01 может производиться без создания новых СКЗИ в случае использования вызовов из приведенного ниже перечня в соответствии с документацией. 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)) …» Примечание: перечень вызовов, с использованием которых допускается проводить разработку систем на основе СКЗИ «КриптоПро CSP» v. 3.6.1 с учетом п. 1.5 Формуляра ЖТЯИ.00050-03 30 01 без создания нового СКЗИ, приведен в Приложении 1 к Извещению.

СОСТАВИЛ	МОШНИНА Д.А.			Н.КОНТРОЛЬ		
ИЗМЕНЕНИЕ ВНЕС				МОШНИНА Д.А. 28.03.2016		

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ
2	ЖТЯИ.00050-03 30 01. Формуляр В Таблицы «Комплектность исполнения 3» и «Комплектность исполнения 4» добавлен Secure Pack Rus версия 3.0. Старая редакция: «… КриптоПро EFS. Формуляр. — ЖТЯИ.00051-01 30 02 Secure Pack Rus версия 3.0. Формуляр. — EAPM.5090005.032-01 30 01 …» Новая редакция: «… КриптоПро EFS. Формуляр. — ЖТЯИ.00051-01 30 02 Secure Pack Rus версия 3.0. — EAPM.5090005.032-01 Secure Pack Rus версия 3.0. Формуляр. — EAPM.5090005.032-01 30 01 …» В Примечании 1 уточнена версия СЗИ Secret Net 6. Старая редакция: «СЗИ Secret Net 6.» Новая редакция: «СЗИ Secret Net 6 (версии 6.5.333.100).»
3	ЖТЯИ.00051-01 30 02. Формуляр В п.3 «Основные характеристики» убрана строка: «- шифрование общих файлов (CIFS);»
4	Под контроль целостности на ОС Windows установлены следующие библиотеки: crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, cryptsp.dll, sspicli.dll, kerberos.dll ЖТЯИ.00050-03 90 02-08. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Windows ЖТЯИ.00050-03 90 02-01. КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ класса защиты КС3 под управлением ОС Windows Новая редакция: «. . .**Windows 2000/2003 32-bit:** • accord.dll, apmdz.dll, bio.dll, charismathics.dll, cpadvai.dll, cpcertocm.dll, cpconfig.cpl, cpcrypt.dll, cpcsp.dll, cpcspi.dll, cpcspr.dll, cpdrvlib.sys, cpet.dll, cpExSec.dll, cpext.dll, cpintco.dll, cpkdc.dll, cpkrb.dll, cplicmgmt.dll, cpmail.dll, cpMSO.dll, cpoutlm.dll, cprastls.dll, cprdr.dll, cprevchk.dll, cprndm.dll, CProCtrl.sys, CProDs64.dll.IA, CProDspr.dll.IA, cpschan.dll, cpsecur.dll, cpssl.dll, cpsslsdk.dll, spsspap.dll, cpsuprt.dll, cpui.dll, cpverify.exe, cpwinet.dll, cpXML5.dll, csptest.exe, dallas.dll, detoured.dll, ds199x.dll, dsrf.dll, emv.dll, esmarttoken.dll, etok.dll, fat12.dll, genkpim.exe, inpapspot.dll, isbc.dll, jcard.dll, pcsc.dll, pkimgmt.dll, pkivalidator.dll,reg.dll, reprovmgmt.dll, ric.dll, rtsupcp.dll, sable.dll, setuptest.exe, snet.dll, usbccid.sys, winlogonmgmt.dll, wipefile.exe, crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, kerberos.dll. **Дополнительно для Windows Vista/7/2008/2008R2/8/2012** • cpcng.dll, cpenroll.dll, cpksp.sys, cryptsp.dll, sspicli.dll. **Windows 2003 Itanium (x86)** • bio.dll, cpadvai.dll, cpcertocm.dll, cpconfig.cpl, cpcrypt.dll, cpcsp.dll, cpcspi.dll, cpcspr.dll, cpenroll.dll, cpExSec.dll, cpext.dll, cpintco.dll, cpmail.dll, cpMSO.dll, cpoutlm.dll, cprdr.dll, cprevchk.dll, cprndm.dll, cpschan.dll, cpsecur.dll,cpssl.dll, cpsslsdk, cpsspap.dll, cpsuprt.dll, cpui.dll, cpverify.exe, cpwinet.dll, cpXML5.dll, csptest.exe, detoured.dll, dsrf.dll, emv.dll, fat12.dll, genkpim.exe, pcsc.dll, reg.dll, ric.dll, setuptest.exe, snet.dll, wipefile.exe, crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, kerberos.dll. **Windows 2003 Itanium (ia64)** • bio.dll, cpadvai.dll, cpcertocm.dll, cpcng.dll, cpconfig.cpl, cpcrypt.dll, cpcsp.dll, cpcspi.dll, cpcspr.dll, cpdrvlib.sys, cpext.dll, cpintco.dll, cpmail.dll, cprdr.dll, cprevchk.dll, cprndm.dll, CProCtrl.sys, CProDs64.dll, CProDspr.dll, cpschan.dll, cpsecur.dll, cpsuprt.dll, cpui.dll, cpverify.exe, cpwinet.dll, csptest.exe, detoured.dll, dsrf.dll, emv.dll, fat12.dll, pcsc.dll, reg.dll, ric.dll, setuptest.exe, snet.dll, wipefile.exe; cpssl.dll, cpsspap.dll, crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, kerberos.dll.

ИЗМ:	СОДЕРЖАНИЕ ИЗМЕНЕНИЯ

	Windows 2003 64-bit (x86)
	• accord.dll, apmdz.dll, bio.dll, charismathics.dll, cpadvai.dll, cpcertocm.dll, cpconfig.cpl, cpcrypt.dll, cpcsp.dll, cpcspi.dll, cpcspr.dll, cpenroll.dll, cpet.dll, cpExSec.dll, cpext.dll, cpintco.dll, cpkrb.dll, cpkdc.dll, cpkrb.dll, cplicmgmt.dll, cpmail.dll, cpMSO.dll, cpoutlm.dll, cprastls.dll, cprdr.dll, cprndm.dll, cprevchk.dll, cpschan.dll, cpsecur.dll,cpsuprt.dll, cprndm.dll, cpsslsdk.dll, cpui.dll, cpverify.exe, cpwinet.dll, cpXML5.dll, csptest.exe, dallas.dll, detoured.dll, ds199x.dll, dsrf.dll, emv.dll, esmarttoken.dll, etok.dll, fat12.dll, genkpim.exe, inpaspot.dll, isbc.dll, jcard.dll, pcsc.dll, pkimgmt.dll, pkivalidator.dll, reg.dll, reprovmgmt.dll, ric.dll, rtsupcp.dll, sable.dll, setuptest.exe, snet.dll, winlogonmgmt.dll, wipefile.exe; cpssl.dll, cpsspap.dll, crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, kerberos.dll.
	Дополнительно для Windows Vista/7/2008/2008R2/8/2012
	• cpcng.dll, cpenroll.dll, cryptsp.dll, sspicli.dll.
	Windows 2003 64-bit (amd64)
	• accord.dll, apmdz.dll, bio.dll, charismathics.dll, cpadvai.dll, cpcertocm.dll, cpconfig.cpl, cpcrypt.dll, cpcsp.dll, cpcspi.dll, cpcspr.dll, cpenroll.dll, cpet.dll, cpext.dll, cpintco.dll, cpkrb.dll, cpkdc.dll, cpkrb.dll, cplicmgmt.dll, cpmail.dll, cpoutlm.dll, cprastls.dll, cprdr.dll, cprevchk.dll, cprndm.dll, CProDs64.dll, CProDspr.dll, cpschan.dll, cpsecur.dll,cpsuprt.dll, cprndm.dll, cpui.dll, cpverify.exe, cpwinet.dll, csptest.exe, dallas.dll, detoured.dll, ds199x.dll, dsrf.dll, emv.dll, esmarttoken.dll, etok.dll, fat12.dll, genkpim.exe, inpaspot.dll, isbc.dll, jcard.dll, pcsc.dll, pkimgmt.dll, pkivalidator.dll, reg.dll, reprovmgmt.dll, ric.dll, rtsupcp.dll, sable.dll, setuptest.exe, snet.dll, winlogonmgmt.dll, wipefile.exe; cpssl.dll, cpsspap.dll, crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, kerberos.dll.
	Дополнительно для Windows Vista/7/2008/2008R2/8/2012
	• cpcng.dll, cpenroll.dll, cpksp.sys, cryptsp.dll, sspicli.dll.
	Для добавления под контроль целостности следующих файлов:
	crypt32.dll, inetcomm.dll, wininet.dll, schannel.dll, winscard.dll, cryptsp.dll, sspicli.dll, kerberos.dll.
	необходимо reg-файл данного вида импортировать в реестр.
	Для 64разрядных систем:
	`Windows Registry Editor Version 5.00`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\CProIntegrity]`
	`"HaltFileCorrupt"=dword:00000000`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\CProIntegrity\system\{название библиотеки}]`
	`"Path"="C:\\Windows\\SysWOW64\\{название библиотеки}"`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\CProIntegrity\system\{название библиотеки}.64]`
	`"Path"="C:\\Windows\\system32\\{название библиотеки}"`
	`Для 32разрядных систем необходима только одна строка для каждой библиотеки:`
	`[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\CProIntegrity\system\{название библиотеки}]`
	`"Path"="C:\\Windows\\system32\\{название библиотеки}"`
	`Затем необходимо в командной строке от имени администратора выполнить команду:`
	`cpverify -rm system…»`

5	Прекращена поддержка платформы Windows XP. Внесены изменения в документацию: ЖТЯИ.00050-03 30 01. Формуляр, ЖТЯИ.00050-03 90 01. Описание реализации, ЖТЯИ.00050-03 90 02. Руководство администратора безопасности. Общая часть, ЖТЯИ.00050-03 90 02-01. Руководство администратора безопасности. СКЗИ класса защиты КС3 под управлением ОС Windows, ЖТЯИ.00050-03 90 02-08. Руководство администратора безопасности. Windows, ЖТЯИ.00050-03 90 04, АРМ выработки внешней гаммы, ЖТЯИ.00050-03 90 07. Приложение командной строки для подписи и шифрования файлов. Новая редакция: «…Windows 2003/Vista/2008/7/2008R2/8/2012 (ia32, ia64, x64)».

Приложение 1.

Перечень вызовов, с использованием которых допускается проводить разработку систем на основе СКЗИ «КриптоПро CSP» v. 3.6.1 с учетом п. 1.5 Формуляра ЖТЯИ.00050-03 30 01 без создания нового СКЗИ.

Функция	**Описание**	**Ограничения на использование функции**
Функции инициализации и настройки провайдера		
CryptAcquireContext	Функция CryptAcquireContext() используется для создания дескриптора криптопровайдера с именем ключевого контейнера, определённым параметром pszContainer	
CryptReleaseContext	Функция CryptReleaseContext() используется для удаления дескриптора криптопровайдера, созданного CryptAcquireContext().	
CryptContextAddRef	Управляет счетчиком дескрипторов созданного CryptAcquireContext().	
CryptEnumProviders	Перечисление установленных криптопровайдеров	
CryptEnumProviderTypes	Перечисление установленных типов криптопровайдеров	
CryptGetDefaultProvider	Получение контекста провайдера, установленного в системе по умолчанию	
CryptGetProvParam	Функция CryptGetProvParam() получает параметры криптопровайдера.	
CryptSetProvParam	Функция CryptSetProvParam() устанавливает параметры криптопровайдера.	
FreeCryptProvFromCertEx	Функция используется для удаления дескриптора криптопровайдера, созданного CryptAcquireContext() или через CNG.	
CryptInstallDefaultContext, CryptSetProvider, CryptSetProviderEx, CryptUninstallDefaultContext	Функции управления контекстом провайдера по умолчанию	
Функции генерации и обмена ключами, создание конфигурирование и удаление ключей		
CryptGenKey	Функция CryptGenKey() генерирует случайные криптографические ключи или ключевую пару (закрытый/открытый ключи).	
CryptDestroyKey	Функция CryptDestroyKey() удаляет ключ,	

	передаваемый через параметр hKey. После удаления ключ (дескриптор ключа) не может использоваться.	
CryptExportKey	Функция CryptExportKey() используется для экспорта криптографических ключей из ключевого контейнера криптопровайдера, сохраняя их в защищённом виде.	Разрешено экспортировать только открытые ключи (PUBLICKEYBLOB).
CryptGenRandom	Функция CryptGenRandom() заполняет буфер случайными байтами.	
CryptGetKeyParam	Функция CryptGetKeyParam() возвращает параметры ключа.	
CryptGetUserKey	Функция CryptGetUserKey() возвращает дескриптор одной из долговременных ключевых пар в ключевом контейнере.	
CryptImportKey	Функция CryptImportKey() используется для импорта криптографического ключа из ключевого блоба в контейнер криптопровайдера.	Разрешено импортировать только открытые ключи (PUBLICKEYBLOB).
CryptSetKeyParam	Функция CryptSetKeyParam() устанавливает параметры ключа.	Разрешено использование только со следующими символьными аргументами: KP_CERTIFICATE, KP_CIPHEROID, KP_DHOID, KP_HASHOID.
Функции обработки криптографических сообщений		
CryptSignMessage	Функция CryptSignMessage создает хэш определенного содержания, подписывает хэш и затем производит закодирование и текста исходного сообщения, и подписанного хэша	
CryptVerifyMessage-Signature	Функция CryptVerifyMessage-Signature проверяет электронно-цифровую подпись подписанного сообщения.	
CryptVerifyDetached-MessageSignature	Функция CryptVerifyDetached-MessageSignature проверяет подписанное сообщение, содержащее отсоединенную (detached) подпись или подписи	
CryptDecodeMessage	Функция декодирует, расшифровывает и проверяет сообщение	
CryptDecryptAndVerifyMessageSignature	Функция декодирует и проверяет сообщение	

CryptEncryptMessage	Функция CryptEncryptMessage зашифровывает и производит закодирование сообщения. Аутентичность сообщения не обеспечивается.	
CryptDecryptMessage	Функция CryptDecryptMessage производит раскодирование и расшифрование сообщения. Проверка аутентичности сообщения не производится. *Примечание*: Не допускается автоматический анализ результата работы функции, направленный на проверку корректности 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 откреплённый хэш	
CryptVerifyMessageHash	Функция проверяет хэшированное сообщение	
CryptVerifyMessageSignatureWithKey	Функция проверяет подписанное сообщение	
CryptMsgCalculate-EncodedLength	Функция CryptMsgCalculate-EncodedLength вычисляет максимальное количество байтов, необходимое для закодированного криптографического сообщения, заданного типом сообщения, параметрами кодирования и общей длиной информации, которая должна быть закодирована.	
CryptMsgOpenToEncode	Функция CryptMsgOpenToEncode открывает криптографическое сообщение для закодирования и возвращает дескриптор открытого сообщения.	
CryptMsgOpenTo-Decode	Функция CryptMsgOpenTo-Decode открывает криптографическое сообщение для раскодирования и возвращает дескриптор открытого сообщения.	
CryptMsgUpdate	Функция CryptMsgUpdate пополняет текст криптографического сообщения.	
CryptMsgGetParam	Функция CryptMsgGetParam получает параметр сообщения после того, как криптографическое	

	сообщение было раскодировано или закодировано.	
CryptMsgControl	Функция CryptMsgControl выполняет контрольное действие.	
CryptMsgClose	Функция CryptMsgClose закрывает дескриптор криптографичекого сообщения.	
CryptMsgDuplicate	Функция CryptMsgDuplicate дублирует дескриптор криптографического сообщения путем увеличения счетчика ссылок	
Функции работы с алгоритмами хэширования		
CryptCreateHash	Функция CryptCreateHash() инициализирует дескриптор нового объекта функции хэширования потока данных.	Разрешено использование только со следующими символьными аргументами: CALG_GR3411, CALG_GR3411_HMAC, CALG_SHAREDKEY_HASH.
CryptDestroyHash	Функция CryptDestroyHash() удаляет объект функции хэширования.	
CryptDuplicateHash	Функция CryptDuplicateHash() создаёт точную копию объекта функции хэширования, включая все его переменные, определяющие внутреннее состояние объекта функции хэширования.	
CryptGetHashParam	Функция CryptGetHashParam() возвращает параметры объекта функции хэширования и значение функции хэширования.	
CryptHashData	Функция CryptHashData() передаёт данные указанному объекту функции хэширования.	
CryptSetHashParam	Функция CryptSetHashParam() устанавливает параметры объекта хэширования.	Разрешено использование только с символьными аргументами HP_HASHSIZE, HP_OID/KP_HASHOID, HP_OPEN.
CryptSignHash	Функция CryptSignHash() возвращает значение электронной цифровой подписи от значения функции хэширования.	Разрешено использование только с дескрипторами ключей, полученных ранее с помощью вызова CryptImportPublicKeyInfo

		(CryptImportPublicKeyInfoEx) из сертификата, проверенного с помощью функции CertVerifyCertificateChainPolicy
CryptVerifySignature	Функция CryptVerifySignature() осуществляет проверку цифровой подписи.	Разрешено использование только с ключевыми контейнерами, полученными ранее с помощью вызова CertGetCertificateContextProperty из сертификата, проверенного с помощью функции CertVerifyCertificateChainPolicy
Функции работы с сертификатами, списками аннулированных сертификатов, хранилищем сертификатов		
Списки аннулированных сертификатов		
CertAddCRLContext-ToStore	Функция CertAddCRLContext-ToStore добавляет контекст COC в хранилище сертификатов.	
CertAddCRLLinkToStore	Функция создает ссылку на список аннулированных сертификатов в другом хранилище	
CertAddEncodedCRL-ToStore	Функция CertAddEncoded-CRLToStore создает контекст COC из закодированного COC и добавляет его в хранилище сертификатов. Функция создает копию контекста COC перед добавлением его в хранилище.	
CertEnumCRLsInStore	Функция CertEnumCRLsIn-Store получает первый или следующий COC в хранилище. Эта функция используется в цикле для того, чтобы последовательно получить все COC в хранилище.	
CertFreeCRLContext	Функция CertFreeCRLContext освобождает контекст COC, уменьшая счетчик ссылок на единицу. Когда счетчик ссылок обнуляется, функция CertFreeCRLContext освобождает память, выделенную под контекст COC.	
CertCreateCRLContext	Функция CertCreateCRL-Context создает контекст COC из закодированного COC. Созданный контекст не помещается в хранилище сертификатов. В созданном контексте функция размещает копию закодированного COC.	

CertDeleteCRLFrom Store	Функция удаляет список аннулированных сертификатов из хранилища	
CertDuplicateCRL-Context	Функция CertDuplicateCRL-Context дублирует контекст COC, увеличивая счетчик ссылок на COC на единицу.	
CertFindCRLInStore	Функция CertFindCRLInStore находит первый или следующий контекст COC в хранилище сертификатов, который соответствует критерию поиска, определяемому параметром dwFindType и связанным с ним pvFindPara. Эта функция может быть использована в цикле для того, чтобы найти все COC в хранилище сертификатов, удовлетворяющие заданному критерию поиска.	
CertDeleteCertificate -FromStore	Функция CertDeleteCertificate-FromStore удаляет определенный контекст COC из хранилища сертификатов.	
CertFindCertificateIn CRL	Функция осуществляет поиск заданного сертификата в списке аннулированных сертификатов	
CertGetCRLFromSto re	Функция CertGetCRLFrom-Store получает первый или следующий контекст COC для определенного издателя сертификата из хранилища сертификатов. Эта функция также осуществляет возможную проверку COC.	
CertSerializeCRLSto reElement	Функция сериализации списка аннулированных сертификатов со своими свойствами	
Расширенные свойства сертификата списка аннулированных сертификатов и CTL		
CertGetCRLContext-Property	Функция CertGetCRLContext-Property получает расширенные свойства определенного контекста COC.	
CertSetCRLContext-Property	Функция CertSetCRLContext-Property устанавливает расширенные свойства определенного контекста COC.	
CertGetCertificate-ContextProperty	Функция CertGetCertificate-ContextProperty получает информацию, содержащуюся в расширенных свойствах контекста сертификата.	
CertEnumCertificate-ContextProperties	Функция CertEnumCertificate-ContextProperties позволяет перечислить информацию, содержащуюся в расширенных свойствах контекста сертификата.	
CertSetCertificate-ContextProperty	Функция CertSetCertificate-ContextProperty устанавливает расширенные свойства для определенного контекста сертификата.	
CertEnumCRLConte xtProperties	Перечисление расширенных свойств списка аннулированных сертификатов	
CertEnumCTLConte	Перечисление расширенных свойств CTL	

xtProperties		
CertGetCTLContext Property	Получение расширенного свойства CTL	
CertSetCTLContextP roperty	Установка расширенных свойств CTL	
Функции работы с сертификатами		
CertAddCertificate-ContextToStore	Функция CertAddCertificate-ContextToStore добавляет контекст сертификата в хранилище сертификатов.	
CertAddCertificateLi nkToStore	Добавляет ссылку на сертификат в другом хранилище	
CertAddEncoded-CertificateToStore	Функция CertAddEncoded-CertificateToStore создает контекст сертификата из закодированного сертификата и добавляет его в хранилище сертификатов. Созданный контекст не содержит никаких расширенных свойств.	
CertEnumCertificate s-InStore	Функция CertEnumCertificates-InStore получает первый или следующий сертификат в хранилище сертификатов. Эта функция используется в цикле для того, чтобы последовательно получить все сертификаты в хранилище сертификатов.	
CertFreeCertificate-Context	Функция CertFreeCertificate-Context освобождает контекст сертификата, уменьшая счетчик ссылок на единицу.	
CertCreateCertificate -Context	Функция CertCreate-CertificateContext создает контекст сертификата из закодированного сертификата. Созданный контекст не помещается в хранилище сертификатов. В созданном контексте функция размещает копию закодированного сертификата.	
CertDuplicate-CertificateContext	Функция CertDuplicate-CertificateContext дублирует контекст сертификата, увеличивая счетчик ссылок на единицу.	
CertFindCertificate-InStore	Функция CertFindCertificate-InStore находит первый или следующий контекст сертификата в хранилище сертификатов, который соответствует критерию поиска, определяемому параметром dwFindType и связанным с ним pvFindPara.	
CertDeleteCertificate -FromStore	Функция CertDeleteCertificate-FromStore удаляет определенный контекст сертификата из хранилища сертификатов.	
CertGetSubject-CertificateFromStore	Функция CertGetSubject-CertificateFromStore 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	
CertSerializeCertificateStoreElemene	Сериализация элемента хранилища	
OCSP		
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	
Оконные функции		
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 аннулированных сертификатов 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 проверки цепочек		
CertVerifyCertificate-ChainPolicy	Функция CertVerifyCertificate-ChainPolicy проверяет цепочку сертификатов на достоверность, включая соответствие критерию истинности.	
CertGetCertificateChain	Функция CertGetCertificate-Chain строит цепочку сертификатов, начиная с последнего сертификата, в обратном направлении до доверенного корневого сертификата, если это возможно.	
CertFreeCertificate-Chain	Функция CertFreeCertificate-Chain освобождает цепочку сертификатов путем уменьшения счетчика ссылок. Если счетчик ссылок равен нулю, то память, выделенная под цепочку, освобождается.	
CertCreateCertificate-ChainEngine	Функция CertCreateCertificate-ChainEngine создает контекст HCERTCHAINENGINE, который позволяет изменять параметры механизма построения цепочки сертификатов. Позволяет ограничивать множество доверенных сертификатов.	
CertFreeCertificate-ChainEngine	Функция CertFreeCertificate-ChainEngine освобождает контекст HCERTCHAINENGINE.	
CertCreateCTLEntryFromCertificateContextProperties	Создание CTL на основе свойст 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 аннулированных сертификатов	
CertSetCertificateContextPropertiesFromCTLEntry	Установка свойств в контекст сертификата на основе CTL	
Расширенные свойства сертификата (EKU)		
CertGetEnhancedKey-Usage	Функция CertGetEnhanced-KeyUsage получает информацию о расширенном использовании ключа из соответствующего расширения или из расширенных свойств сертификата. Расширенное использование ключа служит признаком правомерного использования	

	сертификата.	
CryptAcquireCertificatePrivateKey	Функция CryptAcquire-CertificatePrivateKey получает дескриптор HCRYPTPROV и параметр dwKeySpec для определенного контекста сертификата.	
Функции работы с идентификаторами		
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 работы с хранилищем		
CertOpenStore	Функция CertOpenStore открывает хранилище сертификатов, используя заданный тип провайдера.	
CertDuplicateStore	Функция CertDuplicateStore дублирует дескриптор хранилища, увеличивая счетчик ссылок на хранилища на единицу.	
CertOpenSystemStore	Функция CertOpenSystemStore используется для открытия наиболее часто используемых хранилищ сертификатов.	
CertCloseStore	Функция CertCloseStore закрывает дескриптор хранилища сертификатов и уменьшает счетчик ссылок на хранилища на единицу.	
CertAddStoreToCollection	Добавление хранилища в коллекцию	
CertControlStore	Установка нотификации при различиях в закешированном хранилище и физическом хранилище	
Функции, используемые для работы с открытыми данными и объектами		
CryptImportPublicKey-InfoEx2	Функция CryptImportPublic-KeyInfoEx2 импортирует информацию об открытом ключе в CNG и возвращает дескриптор открытого ключа.	
CryptImportPublicKey-InfoEx	Функция CryptImportPublic-KeyInfoEx импортирует информацию об открытом ключе в CSP и возвращает дескриптор открытого ключа.	
CryptImportPublicKey-Info	Функция CryptImportPublic-KeyInfo преобразовывает и импортирует информацию об открытом ключе в провайдер и возвращает дескриптор открытого ключа.	
CryptExportPublicKey-InfoEx	Функция CryptExportPublic-KeyInfoEx экспортирует информацию об открытом ключе, связанную с соответствующим секретным ключом провайдера.	

CryptExportPublicKey-Info	Функция CryptExportPublic-KeyInfo экспортирует информацию об открытом ключе, ассоциированную с соответствующим секретным ключом провайдера.	
CertCompareCertificate	Функция CertCompare-Certificate сравнивает два сертификата для того, чтобы определить, являются ли они идентичными.	
CertCompareInteger-Blob	Функция CertCompareInteger-Blob сравнивает два целочисленных блоба для определения того, представляют ли они собой два равных числа.	
CryptExportPublicKeyInfoFromBCryptKeyHandle	Экспортирует информацию об открытом ключе, ассоциированную с соответствующим секретным ключом провайдера.	
Функции кодирования/декодирования		
CryptDecodeObject	Функция CryptDecodeObject используются для декодирования сертификатов, списков аннулированных сертификатов (COC) и запросов на сертификаты.	
CryptDecodeObjectEx	Функция CryptDecodeObjectEx используются для декодирования сертификатов, списков аннулированных сертификатов и запросов на сертификаты	
CryptEncodeObject	Функция CryptEncodeObject используются для кодирования сертификатов, списков аннулированных сертификатов и запросов на сертификаты.	
CryptEncodeObjectEx	Функция CryptEncodeObjectEx используются для кодирования сертификатов, списков аннулированных сертификатов и запросов на сертификаты.	
Получение объектов из удаленных источников		
CryptRetrieveObject-ByUrlA	Функция CryptRetrieveObject-ByUrlA получает объект инфраструктуры открытых ключей по заданному URL.	
CryptRetrieveObject-ByUrlW	Функция CryptRetrieveObject-ByUrlW является unicode версией функции CryptRetrieveObject-ByUrlA.	