127 018, Москва, Улица Образцова, 38
Телефон: (095) 933 1168
Факс: (095) 933 1168
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство

Криптографической

Защиты

Информации

КриптоПро CSP

Версия 3.0

Руководство администратора безопасности

Использование СКЗИ под управлением ОС Windows 2000/XP/2003

ЖТЯИ.00005-01 90 02-01

Листов 30

2005 г.

© ООО "Крипто-Про", 2000-2005. Все права защищены.

Авторские права на средство криптографической защиты информации КриптоПро CSP и эксплуатационную документацию зарегистрированы в Российском агентстве по патентам и товарным знакам (Роспатент). Свидетельство об официальной регистрации программ для ЭВМ № 2001610275 от 14 марта 2001 года.

Документ входит в комплект поставки программного обеспечения КриптоПро CSP, и на него распространяются все условия лицензионного соглашения. Без специального письменного разрешения ООО "Крипто-Про" документ или его часть в электронном или печатном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

Содержание

1. Аннотация 5
2. Список сокращений 5
3. Основные технические данные и характеристики СКЗИ 6
3.1. Операционные системы 6
3.2. Исполнения 6
3.3. Ключевые носители 6
4. Состав и назначение компонент программного обеспечения СКЗИ в операционной среде Windows 2000/XP/2003. 7
4.1. Сервисные модули 7
4.1.1. Модуль контроля целостности дистрибутива 8
4.1.2. Дистрибутив 8
4.1.3. Модуль конфигурации 8
4.1.4. Модуль Wipefile 8
4.1.5. Модуль контроля целостности в драйвере 8
4.2. Модули настройки ПКЗИ ОС Microsoft Windows 8
4.2.1. Модуль расширения и настройки CryptoAPI 2.0 8
4.2.2. Модули инициализации настройки встроенного ПКЗИ ОС Microsoft Windows 9
4.2.3. Модуль настройки для системного DLL crypt32.dll 9
4.2.4. Модуль настройки для системного DLL inetcomm.dll 10
4.2.5. Модуль настройки для системного DLL certocm.dll 10
4.2.6. Модуль настройки для системного DLL wininet.dll 10
4.2.7. Модули настройки TLS 10
4.2.8. Модуль настройки Authenticode 10
4.2.9. Модули настройки MS Office 10
4.2.10. Модуль настройки XML 10
4.3. Криптопровайдер КриптоПро CSP (модули сопряжения со встроенным ПКЗИ Windows 2000/XP/2003) 10
4.3.1. Интерфейсная библиотека криптопровайдера 10
4.3.2. Интерфейсная библиотека криптографического сервиса 10
4.4. СКЗИ КриптоПро CSP 11
4.4.1. Реализация в форме сервиса хранения ключей для ОС Windows 2000/XP/2003 11
4.4.2. Реализация криптопровайдера в форме продгружаемых библиотек 11
4.4.3. Реализация криптопровайдера в форме драйвера ядра операционной системы 11
4.4.4. Интерфейс доступа к физическому и БиоДСЧ 11
4.4.5. Интерфейсные модули ДСЧ 11
4.4.6. Панель управления ресурсами СКЗИ КриптоПро CSP 11
4.5. Модуль поддержки сетевой аутентификации КриптоПро TLS 12
4.6. ПКЗИ КриптоПро CSP 12
4.6.1. Интерфейс доступа к ключевым носителям 12
4.6.2. Интерфейсные модули устройств хранения ключевой информации 12
4.6.3. Библиотека поддержки доступа к ключевым носителям 12

4.6.4. Модуль ASN1 12
4.6.5. Использование ключей реестра Windows 12
5. Архитектура криптографических функций в ОС Windows 13
6. Установка дистрибутивов ПО КриптоПро CSP и КриптоПро TLS 15
7. Варианты встраивания КриптоПро CSP и КриптоПро TLS в прикладное ПО 16
7.1. Встраивание на уровне CryptoAPI 2.0. 16
7.2. Встраивание на уровне CSP 16
7.3. Использование COM интерфейсов 16
7.4. Инициализация библиотеки SSP 17
7.5. Завершение сессии 18
7.6. Требования безопасности 18
7.7. Примеры встраивания 19
8. Требования по защите от НСД 19
8.1. Организационно-технические меры защиты от НСД 19
8.2. Изменения в системном реестре ОС Windows 2000/XP/2003 при установке СКЗИ 21
Литература 23
Приложение 1. Контроль целостности программного обеспечения 25
Приложение 2. Службы сертификации операционной системы Windows 27
Приложение 3. Управление протоколированием 29
Лист регистрации изменений 30

1. Аннотация

Данный документ дополняет "ЖТЯИ.00015-01 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть." при использовании СКЗИ под управлением операционных систем Windows 2000/XP/2003.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ КриптоПро CSP, должны разрабатываться с учетом требований настоящего документа.

2. Список сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
ITU-T	Международный комитет по телекоммуникациям (International Telecommunication Union)
IETF	Internet Engineering Task Force
ТМ	Устройство хранения информации на таблетке touch-memory
АС	Автоматизированная система
АРМ	Автоматизированное рабочее место
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск
КП	Конечный пользователь
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПКЗИ	Подсистема криптографической защиты информации
ПО	Программное обеспечение
Регистрация	Присвоение определенных *атрибутов* (адреса, номера ключа, прав использования и т.п.) абоненту
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах.
СВТ	Средства вычислительной техники
Сертификат	Электронный документ, подтверждающий принадлежность открытого *ключа* и определенных *атрибутов* конкретному абоненту
Сертификация	Процесс изготовления *сертификата* открытого ключа абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей. Сетевой справочник.
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ФАПСИ	Федеральное агентство правительственной связи и информации при Президенте РФ
ЭД	Электронный документ
ЭЦП	Электронная цифровая подпись

3. Основные технические данные и характеристики СКЗИ

СКЗИ КриптоПро CSP разработано в соответствии с криптографическим интерфейсом фирмы Microsoft - Cryptographic Service Provider (CSP).

Средствами СКЗИ КриптоПро CSP **НЕ ДОПУСКАЕТСЯ** защищать информацию, составляющую государственную тайну.

3.1. Операционные системы

СКЗИ КриптоПро CSP функционирует в следующих операционных системах (ОС):

- Windows 2000 (платформа IA32);
- Windows XP (платформа IA32);
- Windows 2003 (платформа IA32);
- Windows XP (платформа IA64);
- Windows 2003 (платформа IA64);

В ОС Windows 2000/XP/2003 при использовании СКЗИ "КриптоПро CSP", должна быть произведена установка следующих пакетов обновлений:

1. Microsoft Security Bulletin MS02-048. Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q323172). August 28, 2002.

   Доступ по адресу:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-048.asp

2. Microsoft Security Bulletin MS02-050. Certificate Validation Flaw Could Enable Identity Spoofing (Q328145). September 09, 2002.

   Доступ по адресу:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-050.asp

3.2. Исполнения

СКЗИ КриптоПро CSP версии 3.0 на платформах Microsoft Windows 2000/XP/2003 изготовляется и распространяется в следующих вариантах исполнения:

Исполнение 1 в составе криптопровайдера в форме подгружаемой динамической библиотеки, криптодрайвера, модуля сетевой аутентификации (TLS) и сервисных программ. Класс защиты - **КС1**. СКЗИ в исполнении 1 функционируют в программно-аппаратных средах Windows 2000/XP/2003 (IA32, IA64);

Исполнение 6 в составе криптопровайдера в форме сервиса хранения ключей, криптодрай-вера, модуля сетевой аутентификации (TLS) и сервисных программ. Класс защиты - **КС2.** СКЗИ в исполнении 6 функционируют в программно-аппаратных средах Windows 2000/XP/2003 (IA32). Исполнение 6 комплектуется аппаратными средствами защиты от НСД (см. соответствующий раздел в документе "ЖТЯИ.00015-01 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть.").

3.3. Ключевые носители

В качестве носителей закрытых ключей могут использоваться:

- дискета 3,5";
- процессорные карты MPCOS-EMV и российские интеллектуальные карты (РИК) с использованием считывателей смарт-карт, поддерживающий протокол pS/SC (GemPlus GCR-410, Towitoko, Oberthur OCR126, РИК1, Оскар);

- таблетки Touch-Memory DS1995 – DS1996 с использованием устройств Аккорд-АМДЗ, электронный замок "Соболь" или устройство чтения таблеток Touch-Memory DALLAS (DS9097E, DS9097U, DS1410E);
- электронный ключ e-Token с интерфейсом USB;
- сменный носитель с интерфейсом USB;
- реестр Windows.

Примечание 1. Во избежание потери ключевой информации при повреждении HDD рекомендуется хранить рабочую копию ключевой дискеты.

Примечание 2. Допускается использование в качестве ключевого реестра исполнения 6 при предъявлении к ПЭВМ (съемному HDD ПЭВМ) требований по защите от несанкционированного доступа как к ключевому носителю.

Примечание 3. Инсталлятор в качестве ключевого носителя устанавливает только дискету 3,5". Дополнительное программное обеспечение, необходимое для использования устройств хранения ключевой информации, отличных от дискеты 3.5" и реестра, можно установить с сервера http://www.cryptopro.ru/CryptoPro/products/key_moduls.asp.

Примечание 4. Для того чтобы во время подключения Аккорда-АМДЗ как ключевого носителя в СКЗИ КриптоПро CSP, тот оставался пригодным и для идентификации пользователя при загрузке компьютера, необходимо в окне свойств Аккорда во все поля первого столбца занести константу 64. Доступ к окну свойств ключевого носителя подробно описан в документации «ЖТЯИ.00015-01 90 02-05. КриптоПро CSP. Инструкции по использованию КриптоПро CSP и TLS.» (в разделе «Просмотр свойств ключевого носителя»)

4. Состав и назначение компонент программного обеспечения СКЗИ в операционной среде Windows 2000/XP/2003.

Программное обеспечение СКЗИ КриптоПро CSP в операционной среде Windows 2000/XP/2003 (далее Windows) состоит из следующих компонент:

1. Сервисные модули;
2. Модули настройки встроенной подсистемы криптографической защиты информации (ПКЗИ) ОС Microsoft Windows;
3. Модули сопряжения КриптоПро CSP со встроенным ПКЗИ ОС Microsoft Windows и интерфейс криптографического сервиса;
4. СКЗИ КриптоПро CSP, реализующее целевые функции криптопровайдера в форме:
   - библиотек, загружаемых в адресное пространство приложения;
   - криптографического сервиса хранения ключей;
   - криптографического драйвера;
   - библиотек протокола КриптоПро TLS.

Архитектура программного обеспечения СКЗИ КриптоПро CSP показана на рисунке (см. рис.1).

4.1. Сервисные модули

Сервисные модули обеспечивают контроль целостности дистрибутива КриптоПро CSP, его установку и удаление из операционной системы, а так же конфигурацию параметров СКЗИ для каждого пользователя.

4.1.1. Модуль контроля целостности дистрибутива

Модуль **cpverify.exe** предназначен для контроля целостности дистрибутива при установке ПО СКЗИ КриптоПро CSP на компьютере пользователя (поставляется совместно с дистрибутивом).

4.1.2. Дистрибутив

Дистрибутив СКЗИ КриптоПро CSP поставляется в виде пакета "Windows Installer" (файл **csprus.msi** или **cspeng.msi**). При запуске файл **csprus.msi** (**cspeng.msi**) разворачивает структуры данных дистрибутива во временный каталог и проводит установку ПО СКЗИ КриптоПро CSP.

4.1.3. Модуль конфигурации

Модуль **cpconfig.cpl** обеспечивает возможность управления пользователем конфигурацией ПО СКЗИ КриптоПро CSP, а так же содержит возможности регистрации установленного ПО и получения пользователем дополнительной информации.

4.1.4. Модуль Wipefile

Модуль **wipefile** используется для удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях.

4.1.5. Модуль контроля целостности в драйвере

Для работы с любым отладчиком модуль контроля целостности в драйвере должен быть отключен. Порядок отключения данного модуля описан в документе «ЖТЯИ.00015-01 90 04. КриптоПро CSP. Руководство программиста.».

4.2. Модули настройки ПКЗИ ОС Microsoft Windows

Модули предназначены для обеспечения использования ПО СКЗИ КриптоПро CSP в ПКЗИ ОС Microsoft Windows. Модули также реализуют форматы криптографических сообщений, используемых в защищенной электронной почте (S/MIME), Office 2003/XP, Authenticode и функциях CryptoAPI 2.0, форматы сертификатов и их обработку.

> 🕮 **Примечание.** Полный перечень поддерживаемых приложений Microsoft приведен в документе "ЖТЯИ.00015-01 90 01. КриптоПро CSP. Описание реализации.".

Модули настройки классифицируются как ПКЗИ и ответственны за использование криптопровайдера КриптоПро CSP со стороны приложений. Они обеспечивают вызов сервиса криптографических функций, но не обрабатывают ключевую и криптографически опасную информацию (не имеют доступа к ключам и т. п.).

Состав модулей настройки встроенного ПКЗИ ОС Microsoft Windows:

1. Модуль расширения и настройки CryptoAPI 2.0;
2. Модули инициализации настройки ПКЗИ ОС Microsoft Windows;
3. Модуль настройки системных библиотек ОС Microsoft Windows.

4.2.1. Модуль расширения и настройки CryptoAPI 2.0

Модуль **cpext.dll** является зарегистрированной в системном реестре Windows динамической библиотекой (DLL) расширения CryptoAPI 2.0 и обеспечивает:

- установку соответствия между идентификаторами объектов (OID) в криптографических сообщениях и сертификатах открытых ключей и функциями СКЗИ КриптоПро CSP;
- формирование и разбор криптографических сообщений и сертификатов открытых ключей.

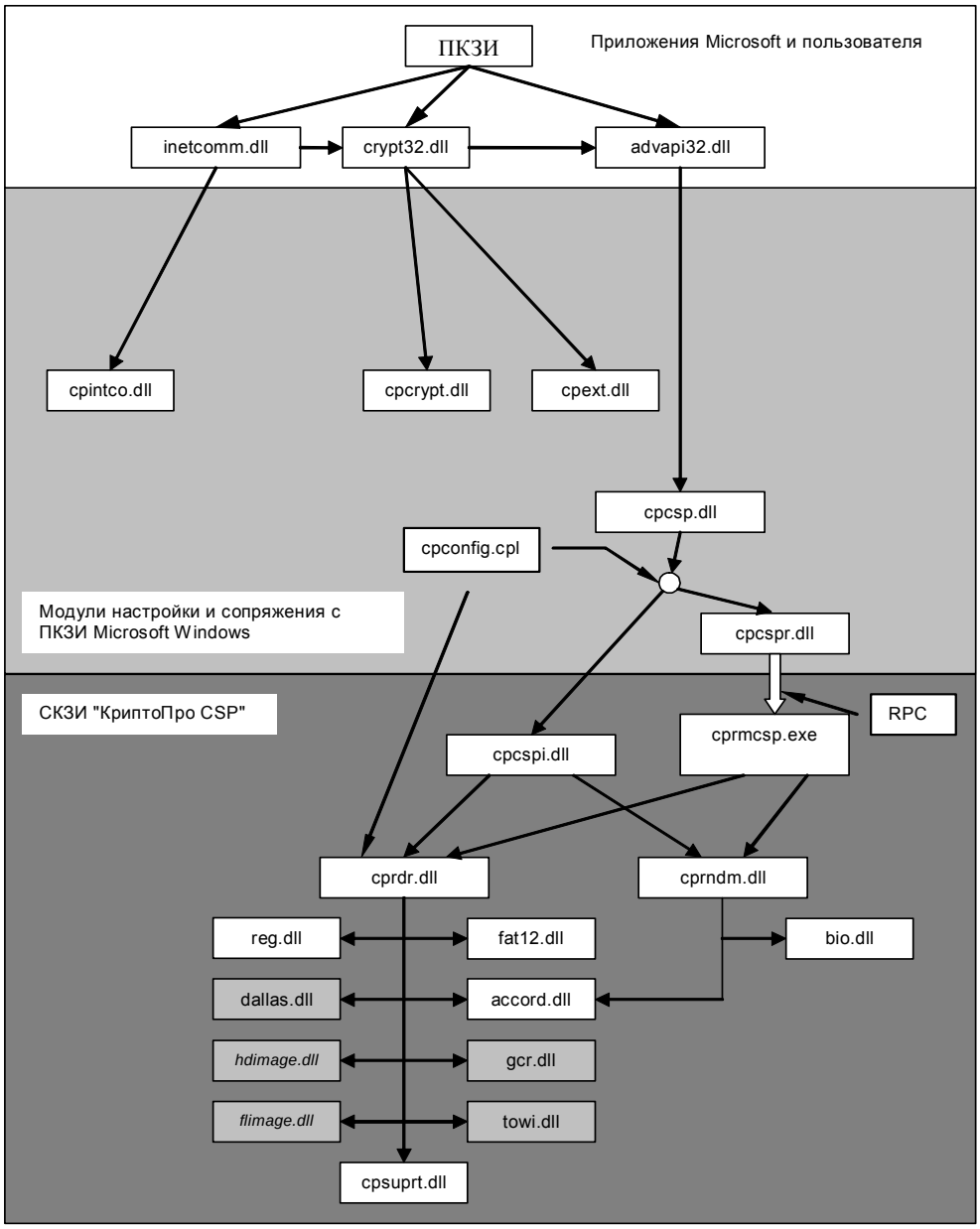


Рис. 1. Структурная схема взаимодействия модулей ПО КриптоПро CSP

4.2.2. Модули инициализации настройки встроенного ПКЗИ ОС Microsoft Windows

Модуль инициализации для ОС Windows 2000/XP/2003 реализован в виде драйвера **CProCtrl.sys**. Драйвер обеспечивает загрузку определенных динамических библиотек (DLL) в адресное пространство процессов, использующих СКЗИ.

Дополнительно этот модуль осуществляет контроль целостности установленного ПО КриптоПро CSP **и ПКЗИ** (периодический и при загрузке ОС).

4.2.3. Модуль настройки для системного DLL crypt32.dll

Модуль **cpcrypt.dll** загружается в виртуальное адресное пространство каждого процесса, к которому подгружается **crypt32.dll**, для установления перехватов функций, использующих провайдер КриптоПро CSP.

Настройка заключается в добавлении ПКЗИ возможности обработки идентификаторов алгоритмов, реализуемых криптопровайдером КриптоПро CSP.

4.2.4. Модуль настройки для системного DLL inetcomm.dll

Модуль **cpintco.dll** загружается в виртуальное адресное пространство каждого процесса, использующего **inetcomm.dll**, для установления перехватов функций.

Настройка заключается в поддержке дополнительных идентификаторов алгоритмов и возмож-ностей S/MIME, реализуемых криптопровайдером КриптоПро CSP, при использовании в ПО Microsoft Outlook и Microsoft Outlook Express.

4.2.5. Модуль настройки для системного DLL certocm.dll

Модуль **cpcertocm.dll** загружается в виртуальное адресное пространство процесса установки центра сертификации (CA) ОС Windows.

Модуль позволяет настроить центр сертификации при его установке так, чтобы поддерживались алгоритмы КриптоПро CSP.

4.2.6. Модуль настройки для системного DLL wininet.dll

Модуль **cpwinet.dll** загружается в виртуальное адресное пространство процесса Internet Explorer, если в него отображается **wininet.dll**.

Модуль позволяет правильно отображать алгоритмы КриптоПро TLS в Internet Explorer.

4.2.7. Модули настройки TLS

Модуль **cpsecur.dll** и модуль **cpschan.dll** загружаются в виртуальное адресное пространство процесса Internet Explorer, если он использует TLS.

Модули позволяют использовать алгоритмы КриптоПро TLS в Internet Explorer.

4.2.8. Модуль настройки Authenticode

Модуль **cpmssign.dll** загружается в виртуальное адресное пространство процессов, использующих технологию Authenticode, и добавляет поддержку алгоритмов КриптоПро CSP.

4.2.9. Модули настройки MS Office

Модуль **cpMSO.dll** загружается в виртуальное адресное пространство процессов MS Word и MS Excell и позволяет подписывать документы с помощью алгоритмов КриптоПро CSP.

Модуль **cpExSec.dll** загружается в виртуальное адресное пространство процесса MS Outlook, и настраивает его для правильной работы с КриптоПро CSP.

4.2.10. Модуль настройки XML

Модуль **cpXML.dll** загружается в виртуальное адресное пространство процессов, использующих XML, и позволяет применять алгоритмы КриптоПро CSP для подписи XML.

4.3. Криптопровайдер КриптоПро CSP (модули сопряжения со встроенным ПКЗИ Windows 2000/XP/2003)

4.3.1. Интерфейсная библиотека криптопровайдера

Интерфейсная библиотека **cpcsp.dll** реализует стандартный интерфейс криптопровайдера, соответствующий спецификации Microsoft Cryptographic Service Provider, и обеспечивает данный интерфейс для обычных приложений через криптографический сервис по RPC, или для привилегированных приложений (имеющих право доступа к устройствам носителей ключевого контейнера) - непосредственно.

4.3.2. Интерфейсная библиотека криптографического сервиса

Интерфейсная библиотека **cpcspr.dll** обеспечивает возможность обращения обычных приложений к сервису криптографических функций по протоколу RPC.

4.4. СКЗИ КриптоПро CSP

Собственно СКЗИ КриптоПро CSP реализует целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, доступ к физическим ДСЧ, реализует БиоДСЧ.

4.4.1. Реализация в форме сервиса хранения ключей для ОС Windows 2000/XP/2003

Модуль **cprmcsp.exe** реализует целевые функции криптографической защиты информации при обращении по RPC с локального компьютера для интерфейсной библиотеки криптографического сервиса.

Модуль обеспечивает:

- хранение и работу с контекстом уровня библиотеки;
- хранение криптографических объектов:
  - Ключевых пар (постоянных и временных);
  - Открытых ключей (временных);
  - Ключей сессий (временных симметричных);
  - Объектов функции хеширования.
- выполнение криптографических преобразований

4.4.2. Реализация криптопровайдера в форме продгружаемых библиотек

Интерфейс **cpcspi.dll** реализует целевые функции криптографической защиты информации для **Интерфейсной библиотеки криптопровайдера** (см. 4.3.1) в варианте функционирования ПО КриптоПро CSP без использования **Интерфейса криптографического сервиса** (см. 4.3.2).

4.4.3. Реализация криптопровайдера в форме драйвера ядра операционной системы

Интерфейс **cpdrvlib.sys** реализует подмножество целевых функций криптографической защиты информации для **Интерфейсной библиотеки криптопровайдера** (см. 4.3.1) в варианте функционирования ПО КриптоПро CSP в ядре ОС Windows. Драйвер поддерживает выполнение функций шифрования, имитозащиты, хеширования, проверки подписи и выработку ключей согласования на эфемерных ключах. Драйвер не поддерживает работу с пользовательскими ключами.

4.4.4. Интерфейс доступа к физическому и БиоДСЧ

Библиотека **cprndm.dll** обеспечивает унифицированный интерфейс доступа к физическому или БиоДСЧ.

4.4.5. Интерфейсные модули ДСЧ

Обеспечивают реализацию доступа к конкретным типам ДСЧ:

bio.dll БиоДСЧ

accord.dll ДСЧ ПАК "Аккорд-АМДЗ"

sable.dll ДСЧ электронного замка "Соболь"

4.4.6. Панель управления ресурсами СКЗИ КриптоПро CSP

Управление ресурсами СКЗИ КриптоПро CSP осуществляется командным файлом **cpconfig.cpl** через панель управления ”Свойства: КриптоПро CSP”. К основным средствам управления ресурсами СКЗИ относятся средства управления:

- лицензиями;
- ДСЧ;

- библиотеками считывания ключевой информации;
- закрытыми ключами и сертификатами открытых ключей;
- параметрами СКЗИ.

Определение правил пользования данными средствами приводится в документе «ЖТЯИ.00015-01 90 02-05. КриптоПро CSP. Инструкции по использованию КриптоПро CSP и TLS.»

4.5. Модуль поддержки сетевой аутентификации КриптоПро TLS

Модуль поддержки сетевой аутентификации реализуется в форме подгружаемой библиотеки и реализует подмножество интерфейса Microsoft SSPI(SSP/AP) (см. соответствующий раздел MSDN). Модуль обеспечивает аутентичное защищенное соединение между пользователем и сервером. **cpssl.dll**, **cptls.dll**, **cpsspap.dll** – при установке модуля аутентификации поддерживающего аутентификацию в домене, **cpsspcore.dll**, **ssp.dll** – без возможности доменной аутентификации.

4.6. ПКЗИ КриптоПро CSP

4.6.1. Интерфейс доступа к ключевым носителям

Библиотека **cprdr.dll** обеспечивает унифицированный интерфейс доступа к ключевым носителям вне зависимости от их типа.

4.6.2. Интерфейсные модули устройств хранения ключевой информации

Модули обеспечивают реализацию доступа к конкретным типам ключевых носителей и считывателей:

fat12.dll - к дисководу и дискете 3.5"

reg.dll - к системнному реестру и ключам в них

accord.dll - к ПАК Аккорд-АМДЗ

sable.dll - к электронному замку "Соболь"

dallas.dll - к считывателю Touch-memory Dallas

ric.dll - к смарткарте РИК и Оскар

emv.dll - к смарткарте MPCOS EMV/3DES

hs.dll - к электронному ключу eToken

pcsc.dll - к считывателям смарт-карт и eToken, поддерживающим интерфейс PC/SC

ds199x.dll - к таблеткам DS1996, DS1995

4.6.3. Библиотека поддержки доступа к ключевым носителям

Библиотека **cpsuprt.dll** обеспечивает реализацию общих функций доступа к различным устройствам хранения ключевых носителей.

4.6.4. Модуль ASN1

Поддерживает функции преобразования структур данных в машинно-независимое представление.

4.6.5. Использование ключей реестра Windows

Установка программного обеспечения должна производится пользователем с правами администратора. При этом программа установки требует доступ к следующим ключам реестра:

- HKEY_LOCAL_MACHINE - полный доступ;
- HKEY_CLASSES_ROOT - полный доступ.

При использовании СКЗИ КриптоПро CSP и создании ключей пользователей без использования флага CRYPT_LOCALMACHINE требуется доступ к следующим ключам реестра:

- HKEY_LOCAL_MACHINE - чтение, перечисление;
- HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\USERS - создание подключей, чтение, перечисление;
- HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\USERS\SID - полный доступ; SID - SID пользователя.

При использовании СКЗИ и создании ключей с использованием флага CRYPT_LOCALMACHINE дополнительно требуется доступ к следующим ключам реестра:

- HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings - полный доступ.

Для изменения конфигурации СКЗИ КриптоПро CSP с использованием панели управления (Control Panel), кроме того, требуется полный доступ к ключу реестра HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro.



Примечание. По умолчанию КриптоПро CSP может использовать до 65536 описателей криптографических объектов. Для увеличения этого значения необходимо добавить в реестр (HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\Parameters) параметр DWORD равный требуемому числу описателей, но не более 1048576.

5. Архитектура криптографических функций в ОС Windows

Использование CryptoAPI в ОС Windows преследует две главные цели:

4. Обеспечить прикладному уровню доступ к криптографическим функциям для генерации ключей, формирования/проверки электронной цифровой подписи, шифрования/расшифрования данных в условиях изолирования прикладного уровня от уровня реализаций криптографических функций. Приложениям и прикладным программистам не нужно детально вникать в особенности реализации того или иного алгоритма или изменять в зависимости от алгоритма прикладные программы.
5. Обеспечить одновременное использование разных алгоритмов и различных их реализаций как программных, так и аппаратных.

Общая архитектура криптографических функций показана на рис. 2.

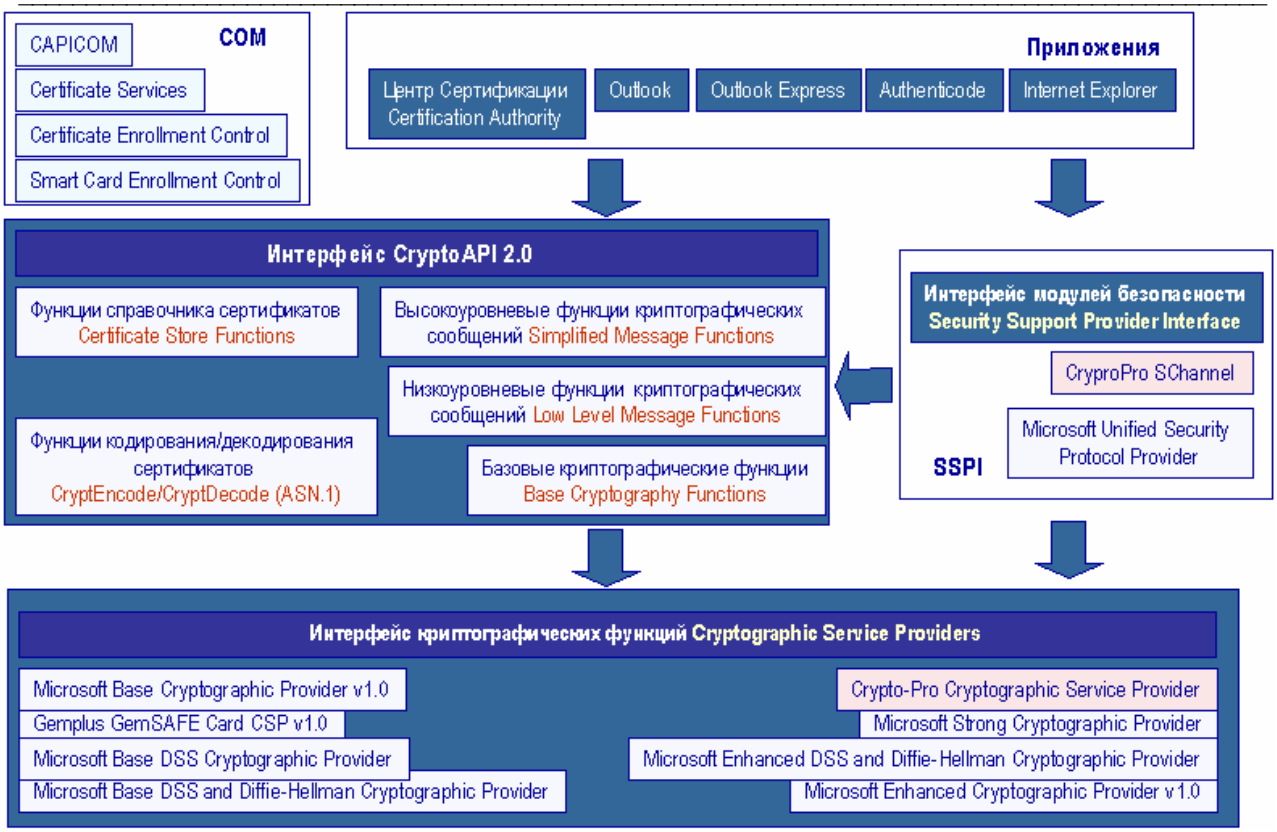


Рис. 2. Архитектура криптографических функций в ОС Windows

Общая архитектура CryptoAPI 2.0 представлена пятью основными функциональными группами:

Базовые криптографические функции

К базовым функциям относятся:

- функции инициализации (работы с контекстом).

Эти функции предоставляют приложению возможность выбрать определенный криптопровайдер по типу имени или по требуемой функциональности;

- функции генерации ключей.

Эти функции предназначены для формирования и хранения криптографических ключей различных типов;

- функции обмена ключами.

Эти функции предназначены для того, чтобы приложения могли обмениваться различными типами ключевой информации для обеспечения взаимодействия между собой;

Функции кодирования/декодирования

Данные функции предназначены для преобразования (кодирования) из внутреннего представления объектов, используемых в CryptoAPI, во внешнее представление и обратно. В качестве внешнего представления объектов используется формат ASN.1 (Abstract Syntax Notation One), определенный серией рекомендаций X.680.

К этой же группе функций относится набор функций, позволяющих расширить функциональность CryptoAPI, путем реализации и регистрации собственных типов объектов.

Функции работы со справочниками сертификатов

Эта группа функций предназначена для хранения и обработки сертификатов в различных типах справочников. Причем в качестве справочника могут использоваться самые различные типы хранилищ: от простого файла до LDAP.

Высокоуровневые функции обработки криптографических сообщений

Эта группа функций (Simplified Message Functions) в первую очередь предназначена для использования в прикладном ПО. С помощью этих функций можно

Зашифровать/расшифровать сообщение от одного пользователя к другому.

Подписать данные.

Проверить подпись данных.

Эти функции (так же как и функции низкого уровня) оперируют сертификатами открытых ключей X.509 для адресации отправителя/получателя данных. В качестве формата данных, формируемых функциями, используется формат PKCS#7 (RFC 2315) или CMS (RFC 2630) в Windows 2000/XP/2003.

Низкоуровневые функции обработки криптографических сообщений

Данная группа функций (Low Level Message Functions) предназначена для аналогичных целей, что и группа высокоуровневых функций, но обладает большей функциональностью и требует от прикладного программиста более детальных знаний в области прикладной криптографии.

6. Установка дистрибутивов ПО КриптоПро CSP и КриптоПро TLS

Установка дистрибутива КриптоПро CSP должна производится пользователем, имеющим права администратора. Перед установкой дистрибутива, удалите все ранее существующие версии устанавливаемого программного обеспечения. Если модуль криптографической поддержки не удален, новая версия не будет установлена. Для этого используете пункты основного меню Windows **Пуск, Настройка, Панель управления, Установка и удаление программ**.

Для установки программного обеспечения вставьте компакт-диск в привод считывателя. Программа установки запуститься автоматически. Если компьютер не настроен на автоматический запуск приложений с компакт-диска, запустите программу **AUTORUN.EXE** с компакт-диска.



Рис. 3. Содержание диска КриптоПро CSP

Для дальнейшей установки КриптоПро CSP, выберите значок **Установить КриптоПро CSP**.

Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

Иерархическая архитектура криптографических функций в операционной системе Windows позволяет использовать российские криптографические алгоритмы, реализованные в КриптоПро CSP на самых различных уровнях.

7. Варианты встраивания КриптоПро CSP и КриптоПро TLS в прикладное ПО

7.1. Встраивание на уровне CryptoAPI 2.0.

КриптоПро CSP может быть использовано в прикладном программном обеспечении (как и любой другой криптопровайдер, поставляемый с ОС Windows) через интерфейс CryptoAPI 2.0, подробное описание которого приведено в программной документацией MSDN (Microsoft Developer Network) http://msdn.microsoft.com/library/psdk/crypto/aboutcrypto_6fl5.htm. В этом случае способ выбора криптографического алгоритма в прикладном ПО может определятся идентификатором алгоритма открытого ключа отправителя/получателя, содержащегося в сертификате X.509.

Встраивание на уровне CryptoAPI 2.0 позволяет воспользоваться большим набором функций, решающих большинство проблем связанных с представлением (форматами) различных криптографических сообщений (подписанных, зашифрованных), способами представления открытых ключей в виде цифровых сертификатов, способами хранения и поиска сертификатов в различных справочниках, включая LDAP.

Функции CryptoAPI 2.0 позволяют полностью реализовать представление и обмен данными в соответствии с международными рекомендациями и Инфраструктурой Открытых Ключей (Public Key Infrastructure).

7.2. Встраивание на уровне CSP

КриптоПро CSP может быть непосредственно использовано в прикладном программном обеспечении путем загрузки модуля с использованием функции LoadLibrary(). Для этих целей в комплект поставки включается **Руководство программиста**, описывающее состав функций и тестовое ПО. При такой реализации прикладному ПО доступен лишь ограниченный набор низкоуровневых криптографических функций, соответствующий интерфейсу Microsoft CSP.

7.3. Использование COM интерфейсов

КриптоПро CSP может быть использовано из COM интерфейсов, разработанных Microsoft.

- CAPICOM 1.0
- Certificate Services
- Certificate Enrollment Control

Certificate Enrollment Control

COM интерфейс Certificate Enrollment Control (реализованный в файле xenroll.dll) предназначен для использования ограниченного количества функций CryptoAPI 2.0, связанных с генерацией ключей, запросов на сертификаты и обработкой сертификатов, полученных от Центра Сертификации с использованием языков программирования Visual Basic, C++, JavaScript, VBScript и среды разработки Delphi.

Именно этот интерфейс используют различные публичные Центры Сертификации (Verisign, Thawte и т. д.) при формировании сертификатов пользователей на платформе Windows.

CAPICOM 1.0

CAPICOM (реализованный в файле capicom.dll) предоставляет COM интерфейс, использующий основные функции CryptoAPI 2.0. Этот компонент является добавлением к уже существующему COM интерфейсу Certificate Enrollment Control (xenroll.dll), который реализуют клиентские функции генерации ключей, запросов на сертификаты и обмена с центром сертификации.

С выпуском данного компонента стало возможным использование функций формирования и проверки электронной цифровой подписи, построения и проверки цепочек сертификатов, взаимодействия с различными справочниками сертификатов (включая Active Directory) с использованием Visual Basic, C++, JavaScript, VBScript и среды разработки Delphi. Использование CAPICOM позволяет реализовать функциональность "тонкого" клиента в интерфейсе броузера Internet Explorer.

Компонент CAPICOM является свободно распространяемым и поставляется в составе Redistributable инструментария разработчика Microsoft Platform SDK.

Подробную информацию об интерфейсе CAPICOM можно получить на сервере http://www.cryptopro.ru/capicom. Дистрибутив интерфейса и примеры использования находятся на компакт-диске в директории "**\REDISTR\CAPICOM**".

Certificate Services

Certificate Services включает в себя несколько COM интерфейсов, позволяющих изменить функциональность Центра Сертификации, входящего в состав ОС Windows 2000 Server. При помощи данных интерфейсов возможно:

- обрабатывать поступающие от пользователей запросы на сертификаты;
- изменить состав данных (в том числе дополнений X.509), записываемых в издаваемые центром сертификаты;
- определить дополнительный способ публикации (хранения) изданных центром сертификатов.

7.4. Инициализация библиотеки SSP

Производится загрузка библиотеки Secur32.dll при работе с операционными системами Windows 2000, Windows XP, Windows 2003.

С помощью функции GetProcAddress получается указатель на функцию InitSecurityInterfaceA (InitSecurityInterfaceW в случае компиляции с Unicode).

Вызовом функции InitSecurityInterfaceA (InitSecurityInterfaceW в случае компиляции с Unicode) получается таблица функций SSPI.

Или, вместо использования GetProcAddress, достаточно поключить библиотеку импорта secur32.lib (входит в MS Platform SDK)

Заполняется структура SCHANNEL_CRED. Поля этой структуры должны быть нулевыми, кроме:

```
SchannelCred.dwVersion = SCHANNEL_CRED_VERSION;

SchannelCred.dwFlags      =      SCH_CRED_NO_DEFAULT_CREDS      |
SCH_CRED_MANUAL_CRED_VALIDATION;
```

Для сервера и не анонимного клиента заполняются также поля:

```
SchannelCred.cCreds     = 1;

SchannelCred.paCred     = &pCertContext.
```

Примечание. Контекст сертификата pCertContext должен содержать ссылку на закрытый ключ.

Производится вызов функции создания Credentials: AcquireCredentialsHandle с передачей ей структуры SCHANNEL_CRED и имени пакета - UNISP_NAME ("Microsoft Unified Security Protocol Provider").

Инициализация соединения клиентом производится вызовом InitializeSecurityContext без входного буфера и сервером – вызовом AcceptSecurityContext, после чего идет обычный цикл Handshake.

После установления соединения, но до начала передачи данных, приложение должно выполнить проверку параметров соединения и сертификата удаленной стороны.

Для получения сертификата удаленной стороны вызывается функция QueryContextAttributes с аргументом SECPKG_ATTR_REMOTE_CERT_CONTEXT.

Для построения цепочки сертификатов рекомендуется использование функции CertGetCertificateChain, описанную в MSDN/Platform SDK/Security, (с флагами проверки, соответствующими выбранному уровню безопасности. Рекомендуется использовать флаг

CERT_CHAIN_CACHE_END_CERT | CERT_CHAIN_REVOCATION_CHECK_CHAIN.

Цепочка сертификатов проверяется функцией CertVerifyCertificateChainPolicy, описанной там же, с аргументом pszPolicy, равным OIDCERT_CHAIN_POLICY_SSL, и аргументом pPolicyPara, заполненным следующим образом:

```
ZeroMemory(&polHttps, sizeof(HTTPSPolicyCallbackData));
polHttps.cbStruct           = sizeof(HTTPSPolicyCallbackData);
polHttps.dwAuthType         = AUTHTYPE_SERVER;
polHttps.fdwChecks          = 0;
polHttps.pwszServerName     = pwszServerName;
memset(&PolicyPara, 0, sizeof(PolicyPara));
PolicyPara.cbSize            = sizeof(PolicyPara);
PolicyPara.pvExtraPolicyPara = &polHttps;
```

Необходимо, чтобы для каждого сертификата в цепочке

pCertContext->pCertInfo->SubjectPublickeyInfo->Algoritm->pszObjId заканчивалась на szOID_GR3410.

Вызывается функция QueryContextAttributes с аргументом ulAttribute, равным SECPKG_ATTR_CONNECTION_INFO, для получения параметров соединения и их проверки на выполнение условий:

```
ConnectionInfo.dwProtocol == SP_PROT_TLS1_CLIENT
ConnectionInfo.aiCipher   ==   CALG_G28147,   ConnectionInfo.aiHash   ==
CALG_GR3411
aiExch=CALG_DH_EX_EPHEM или CALG_DH_EX_SF
```

Цикл шифрования/рас Для получения параметров соединения шифрования данных реализуется с помощью функций EncryptMessage/DecryptMessage.

Примечание. Должна быть обеспечена корректная обработка кодов возврата функций SSPI. При этом следует учитывать, что требуется разная обработка в зависимости от того, является код возврата кодом успешного выполнения функции, кодом не фатальной ошибки, не требующей разрыва соединения, кодом фатальной ошибки, требующей разрыва соединения. Все необрабатываемые коды возврата ошибок должны приводить к разрыву соединения.

7.5. Завершение сессии

Корректное завершение сессии осуществляется вызовом функции ApplyControlToken/

7.6. Требования безопасности

1. Применение модуля поддержки сетевой аутентификации допускается только при использовании открытых ключей сервера и клиента, сертифицированных доверенным центром сертификации

2. Приложением должны обеспечиваться проверка сертификатов в сообщениях Certificate и CertVerify, проверка 12 байт в сообщениях Finished клиента и сервера,

являющихся имитовставками к информации всего диалога клиент-сервер в процессе установления сессии, контроль соответствия имени клиента (сервера) IP-адресу, по которому установлена сессия.

7.7. Примеры встраивания

Примеры встраивания модуля поддержки сетевой аутентификации имеются в тестовом ПО разработки ООО "Крипто-Про" (http://www.cryptopro.ru/load_sample.htm, файлы WebClient.c, WebServer.c, tls.c), а также в составе Microsoft Platform SDK (<PSDKDir>\Samples\WinBase\Security\SSL).

8. Требования по защите от НСД

СКЗИ КриптоПро CSP в варианте исполнения 1 уровня КС1 при условии выполнения настоящих Правил обеспечивают защиту конфиденциальной информации от внешнего нарушителя, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

СКЗИ КриптоПро CSP в варианте исполнения 6 уровня КС2 со средствами защиты от НСД ПАК "Соболь" либо "Аккорд АМДЗ" при условии выполнения настоящих Правил обеспечивают защиту конфиденциальной информации также от внутреннего нарушителя, не являющегося пользователем средств вычислительной техники, на которых реализованы СКЗИ и ПКЗИ, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

Запрещается использование СКЗИ КриптоПро CSP в случае обнаружения отказа оборудования либо программного обеспечения ПАК защиты от НСД.

8.1. Организационно-технические меры защиты от НСД

Должен быть реализован следующий комплекс организационно-технических мер защиты от НСД:

1. В системе регистрируется один пользователь с именем root, обладающий правами администратора, на которого возлагается обязанность конфигурировать ОС Windows 2000/XP/2003, настраивать безопасность ОС Windows 2000/XP/2003, а также конфигурировать ПЭВМ, на которую установлена ОС Windows 2000/XP/2003.
2. Для администратора выбирается надежный пароль входа в систему, удовлетворяющий следующим требованиям: длина пароля не менее 6 символов, среди символов пароля встречаются заглавные символы, прописные символы, цифры и специальные символы, срок смены пароля не реже одного раза в месяц, доступ к паролю должен быть обеспечен только пользователю root.
3. Всем пользователям, зарегистрированным в ОС Windows 2000/XP/2003, администратор в соответствии с политикой безопасности, принятой в организации, дает минимально возможные для нормальной работы права. Каждый пользователь ОС Windows 2000/XP/2003, не являющийся администратором, может просматривать и редактировать только свои установки в рамках прав доступа, назначенных ему администратором.
4. На компьютере устанавливается только одна ОС Windows 2000/XP/2003. Не используют нестандартные, измененные или отладочные версии ОС Windows 2000/XP/2003 такие, например, как Debug/Checked Build. На всех HDD должна быть установлена файловая система NTFS.
5. Права доступа к каталогам %Systemroot%\System32\ Config, %Systemroot%\System32\SPOOL, %Systemroot%\Repair, %Systemroot%\COOKIES, %Systemroot%\FORMS, %Systemroot%\HISTORY, %Systemroot%\SENDTO, %Systemroot%\PROFILES, %Systemroot%\OCCASHE, \TEMP, а также файлам boot.ini, autoexec.bat, config.sys, ntdetect.com и ntldr

должны быть установлены в соответствии с политикой безопасности, принятой в организации.

6. Должны быть установлены ограничения на доступ пользователей к системному реестру в соответствии с принятой в организации политикой безопасности, что реализуется при помощи ACL или установкой прав доступа при наличие NTFS.
7. Должна быть исключена возможность удаленного редактирования системного реестра.
8. Должна быть проведена установка SECURITY_ATTRIBUTES процессов и потоков в соответствии с требованиями безопасности всей системы в целом.
9. Если нет необходимости, не следует использовать протокол SMB. В случае необходимости использования протокола SMB параметры EnableSecuritySignature (REG_DWORD) и RequareSecuritySignature(REG_DWORD) в ключе HKLM\System\CurrentControlSet \Services\LanManServer\Parametrs должны быть установлены со значениями 1.
10. У группы Everyone должны быть удалены все привилегии.
11. Должен быть переименован пользователь Administrator.
12. Должна быть отключена учетная запись для гостевого входа (Guest);
13. Должно быть исключено использование режима автоматического входа пользователя в операционную систему при ее загрузке.
14. Должно быть ограничено с учетом выбранной в организации политики безопасности использование пользователями сервиса Sheduler.
15. Должен быть отключен сервис DCOM.
16. Должны быть отключены сетевые протоколы, не используемые на данной ПЭВМ.
17. В случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных должно быть исключено использование JavaScript, VBScript, ActiveX и других программных объектов, загружаемых из сети.
18. Должна быть исключена возможность сетевого администрирования для всех, включая группу Administrators.
19. Должен быть закрыт доступ ко всем не используемым портам.
20. Должны включаться фильтры паролей, устанавливаемые вместе с пакетами обновлений ОС Windows 2000/XP/2003.
21. Должны быть исключены исполнение и открытие файлов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов.
22. Должны быть удалены все общие ресурсы на ПЭВМ с установленным СКЗИ «КриптоПро CSP» (в том числе и создаваемые по умолчанию при установке ОС Windows 2000/XP/2003), которые не используются. Права доступа к используемым общим ресурсам должны быть заданы в соответствии с политикой безопасности принятой в организации.
23. После установки операционной системы из каталога %Systemroot%\System32\Config должен быть удален файл sam.sav.
24. Должны использоваться наиболее защищенные протоколы аутентификации, реализованные в Windows 2000/XP/2003, если функционирование СКЗИ не предусматривает применение других протоколов.
25. По возможности следует применять самые сильные шаблоны безопасности (Templates).
26. Должна быть разработана система назначения и смены паролей.
27. Должно быть запрещено использование функции резервного копирования паролей (ОС Windows XP).

28. Должны быть отключены режимы отображения окна всех зарегистрированных на ПЭВМ пользователей и быстрого переключения пользователей (ОС Windows XP).
29. Должна быть отключена возможность удаленного администрирования ПЭВМ с установленным СКЗИ «КриптоПро CSP». (ОС Windows XP).
30. Должно быть ограничено количество неудачных попыток входа в систему, в соответствие с политикой безопасности, принятой в организации. Рекомендуется блокировать систему после трех неудачных попыток.
31. Должны использоваться система аудита в соответствие с политикой безопасности, принятой в организации, и организован регулярный анализ результатов аудита.
32. Должен проводиться регулярный просмотр сообщений в журнале событий Event viewer.
33. ОС Windows 2000/XP/2003 должна быть настроена на завершение работы при переполнении журнала аудита.
34. Должна быть обеспечена невозможность модификации ОС Windows 2000/XP/2003 через общедоступные каналы передачи данных (Windows Update, Remote Assistance, и т.п.);
35. После инсталляции ОС Windows 2000/XP/2003 должен быть установлен последний официальный Service Pack от фирмы Microsoft, существующий на момент установки ОС Windows 2000/XP/2003.
36. Должны использоваться подписанные драйверы. (для ОС Windows 2000/XP).
37. На все директории, содержащие системные файлы Windows и программы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем пользователям, кроме Администратора (Administrator), Создателя/Владельца (Creator/Owner) и Системы (System).
38. Должна быть исключена возможность создания аварийного дампа оперативной памяти, так как он может содержать криптографически опасную информацию.

8.2. Изменения в системном реестре ОС Windows 2000/XP/2003 при установке СКЗИ

На ПЭВМ с установленной ОС Windows 2000/XP/2003 при установке СКЗИ необходимо внести следующие изменения в системный реестр:

- в ключе HKLM\System\CurrentControlSet\Control\LSA, установить параметр RestrictAnonymous (REG_DWORD) со значением 1 для исключения доступа анонимного пользователя (null-session) к списку разделяемых ресурсов, а также для исключения доступа к содержимому системного реестра;
- для исключения утечки информации при передаче данных по именованному каналу \\server\PIPE\SPOOLSSудалить имя SPOOLSS из ключа HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes;
- в ключе HKLM\System\CurrentControlSet\Services\ LanManServer\Parameters установить параметры AutoShareWks и AutoShareServer, имеющие тип REG_DWORD, со значением 0 для запрета автоматического создания скрытых совместных ресурсов;
- в ключе HKLM\Software\Microsoft\WindowsNT\ CurrentVersion\Winlogon установить параметр CashedLogonCount (REG_DWORD) со значением 0 для отключения кэширования паролей последних десяти пользователей, вошедших в систему;
- в ключе HKLM\System\CurrentControlSet\Services\Eventlog\ <LogName> (LogName – имя журнала для которого следует ограничить доступ пользователям группы Everyone) установить параметр RestrictGuestAccess (REG_DWORD) со значением 1 для исключения доступа группы Everyone к системному журналу и журналу приложений;
- в ключе HKLM\System\CurrentControlSet\Control\ SessionManager\MemoryManagment установить параметр

ClearPageFileAtShutDown (REG_DWORD) со значением 1 для включения механизма затирания файла подкачки при перезагрузке;

- в ключе HKLM\System\CurrentControlSet\Control\SecurePipeServers\ установить в соответствии с политикой безопасности принятой в организации разрешения на доступ к параметру winreg для ограничения удаленного доступа к реестру;
- в ключе HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ Winlogon\ установить параметр AllocateFloppies (REG_SZ) со значением 1 для исключения параллельного использования дисковода для гибких дисков;
- в ключе HKLM\System\CurrentControlSet\Control\Lsa установить параметр AuditBaseObjects (REG_DWORD) со значением 1 для включения аудита на базовые объекты системы;
- в ключе HKLM\System\CurrentControlSet\Control\Lsa установить параметр FullPrivilegeAuditing (REG_BINARY) со значением 1 для включения аудита привилегий;
- для исключения передачи пароля пользователей по сети в открытом виде (ОС Windows 2000/XP) в ключе HKLM\SYSTEM\CurrentControlSet\Services\MRxSmb\Parameters установить параметр EnablePlainTextPassword (REG_DWORD) со значением 0.

Литература

1. Закон РФ № 24-ФЗ от 20.02.95 г. "Об информации, информатизации и защите информации".
2. Закон РФ № 5485-1 от 21.07.93 г. "О государственной тайне".
3. Закон РФ № 2446-1 от 05.03.92 г. "О безопасности".
4. Закон РФ № 15-ФЗ от 16.02.95 г. "О связи".
5. Закон РФ № 5151-1 от 10.06.93 г. "О сертификации продукции и услуг".
6. Закон РФ № 5154-1, 1993 г. "О стандартизации".
7. Закон РФ № 4871-1, 1993 г. "Об обеспечении единства измерений".
8. Закон РФ № 4524-1 от 19.02.93 г. "О федеральных органах правительственной связи и информации".
9. Гражданский кодекс Российской Федерации. Ч. 1. Принят Государственной Думой 21 октября 1994 г. Одобрен Советом Федерации.
10. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
11. ГОСТ 28147-89. Государственный стандарт Российской Федерации. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
12. ГОСТ Р 34.10-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
13. ГОСТ Р 34.10-2001. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
14. ГОСТ Р 34.11-94. Государственный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.
15. ГОСТ Р 50739-95. Государственный стандарт Российской Федерации. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
16. ГОСТ Р 1.0-92. Государственная система стандартизации Российской Федерации. Основные положения.
17. ГОСТ 16487-83. Делопроизводство и архивное дело. Термины и определения.
18. ГОСТ Р 50922-96. Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения.
19. Положение о государственном лицензировании деятельности в области защиты информации. Утверждено Решением Государственной технической комиссии при Президенте Российской Федерации и Федерального агентства правительственной связи и информации при Президенте Российской Федерации № 10 от 27 апреля 1994 г.
20. Гостехкомиссия России. Руководящий документ. Защита от НСД к информации. Термины и определения. - М.: Воениздат, 1992.
21. Гостехкомиссия России. Концепция защиты информации в системах ее обработки, 1995.
22. Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем от НСД к информации. Москва, 1992 г.
23. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. Москва, 1992 г.
24. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. Москва, 1992 г.
25. Халянин Д.В., Ярочкин В.И. Основы защиты промышленной и коммерческой информации. Термины и определения: Словарь / ИПКИР. - М., 1994.

26. Бияшев Р.Г., Диев С.И., Размахнин М.К. Основные направления развития и совершенствования криптографического закрытия информации / Зарубежная радиоэлектроника. 1989. № 12. С. 76-91.

27. Толковый словарь по информатике. - М.: Финансы и статистика, 1991.

28. Терминология в области защиты информации: Справочник / ВНИИстандарт, 1993.

29. ЖТЯИ.00003-01 90 01. КриптоПро CSP. Формуляр.

30. ЖТЯИ.00015-01 90 01. КриптоПро CSP. Описание реализации.

31. ЖТЯИ.00015-01 90 02. КриптоПро CSP. Руководство администратора безопасности. Общая часть.

32. ЖТЯИ.00015-01 90 04. КриптоПро CSP. Руководство программиста.

33. ЖТЯИ.00015-01 90 02-05. КриптоПро CSP. Инструкции по использованию КриптоПро CSP и TLS.

34. [X.680-X.699]. OSI NETWORKING AND SYSTEM ASPECTS. Abstract Syntax Notation One (ASN.1)

35. [X.509]. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.

36. [PKIX]. RFC 2459. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", January 1999.

Приложение 1. Контроль целостности программного обеспечения

Модуль **cpverify.exe** позволяет осуществлять контроль целостности установленного программного обеспечения. Контроль целостности файлов осуществляется при загрузке файла на исполнение (и периодически во время выполнения) или при ручном запуске программы контроля целостности (см. опцию **–rv** ниже).

При помощи перечисленных ниже опций модуль **cpverify.exe** может быть использован для следующих контрольных целей:

- **cpverify –r2x out_file [xmlcatname]** - формирование xml-файла с именем **out_file**, содержащего список файлов, находящихся в каталоге **xmlcatname** под контролем целостности;
- **cpverify –x2r in_file [xmlcatname]** - установление под контроль целостности файлов из каталога **xmlcatname**, перечисленных в xml-файле с именем **in_file**;
- **cpverify –xv in_file [xmlcatname]** - проверка целостности файлов из каталога **xmlcatname**, перечисленных в xml-файле с именем **in_file**;
- **cpverify –rv [xmlcatname]** - проверка целостности файлов из каталога **xmlcatname**;
- **cpverify –xm in_file out_file [xmlcatname]** - вычисление значения хеш-функции для каждого из файлов, содержащихся в каталоге **xmlcatname** и перечисленных в xml-файле с именем **in_file**, и запись полученных значений в xml-файл с именем **out_file**. Текущее значение хеш-функций при этом заменяется на вновь посчитанное.
- **cpverify –rm [xmlcatname]** - вычисление значения хеш-функции для каждого из файлов, содержащихся в каталоге **xmlcatname**. Текущее значение хеш-функций при этом заменяется на вновь посчитанное.
- **cpverify –d [catname]** – удаление каталога **catname** из списка контрлируемых файлов.
- **cpverify –mk filename –** вычисление значения хеш-функции для файла с именем **filename**.

Во всех перечисленных выше случаях, если не указано имя каталога **xmlcatname**, то принимается имя каталога **cpcsp,** используемое csp для контроля целостности входящих в его состав модулей. Список контролируемых модулей зависит от исполнения и может быть получен при помощи команды **cpverify –r2x in_file cpcsp**.

Для того, чтобы поставить под контроль целостности установленное программное обеспечение, нужно выполнить следующую последовательность действий:

1. Создать xml-файл, содержащий список устанавливаемых под контроль целостности файлов. Данный xml-файл должен иметь следующую структуру:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<CProIntegrity>
    <catalog name="TestControl">
        <entry name="calc.exe">
            <Path>C:\WINDOWS\system32\calc.exe</Path>
        </entry>
        <entry name=" verifier.exe">
            <Path>C:\WINDOWS\system32\verifier.exe</Path>
        </entry>
    </catalog>
    </CProIntegrity>
```

2. Запустить модуль **cpverify –xm in_file out_file TestControl**, указав в качестве параметра **in_file** имя созданного xml-файла. Результатом работы модуля будет являться xml-файл с именем **out_file**, содержащий вычисленные значения хеш-функции для перечисленных в **in_file** файлов и имеющий следующую структуру:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<CProIntegrity>
    <catalog name="TestControl">
        <entry name="calc.exe">
<Path>C:\WINDOWS\system32\calc.exe</Path>
<Tag>0941E781760004B3AEE0DF6BC53CF460A6B137083948C0BF6D5DD153D255FE86</Tag>
        </entry>
        <entry name=" verifier.exe">
<Path>C:\WINDOWS\system32\verifier.exe</Path>
<Tag>A9CD3307A16F76DCE4E6E3A67ED7359658202C44D9812C532FCD8E07B1D7A7D6</Tag>
        </entry>
    </catalog>
    </CProIntegrity>
```

3. Установить под контроль целостности файлы, для которых было вычислено значение хеш-функции, используя модуль **cpverify –x2r in_file TestControl**, где параметром **in_file** является xml-файл, полученный в результате вычисления значения хеш-функции в пункте 2.

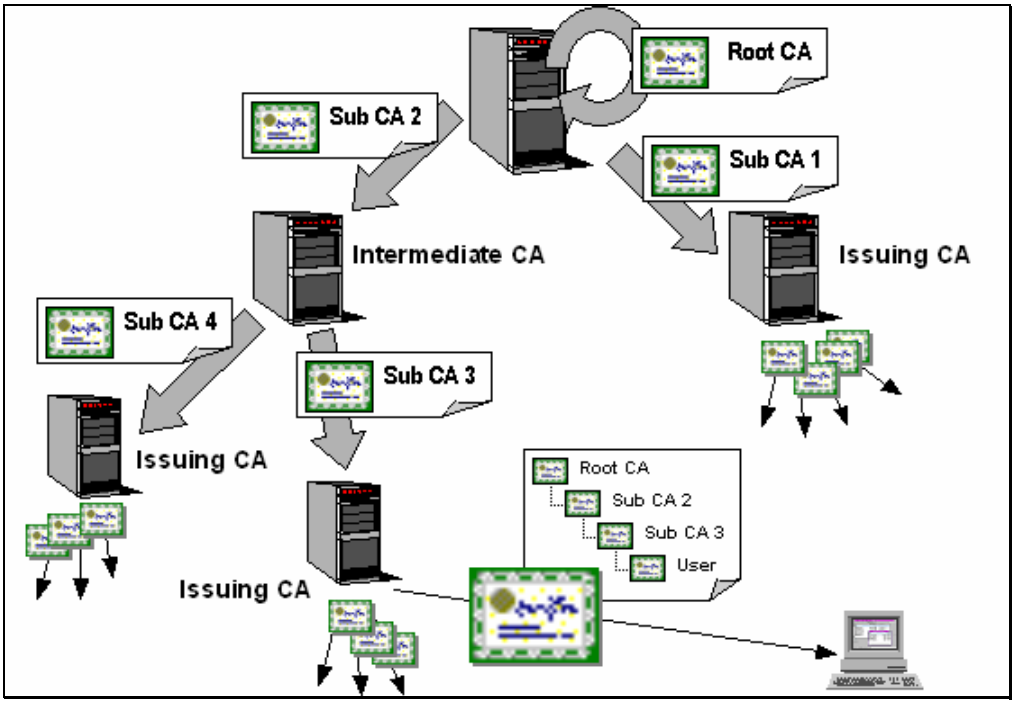
Приложение 2. Службы сертификации операционной системы Windows

Ведущие мировые производители системного и прикладного программного обеспечения активно интегрируют решения, основанные на Инфраструктуре открытых ключей в операционные системы и приложения. Ярким примером является операционная система Windows, полностью поддерживающая ИОК.

В операционной системе Microsoft Windows 2000 в полном объеме реализована Инфраструктура открытых ключей. Эта инфраструктура представляет собой интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих криптографию с открытыми ключами, а также для управления ими.

Инфраструктура открытых ключей предполагает иерархическую модель построения центров сертификации. Такая модель обеспечивает масштабируемость, удобство администрирования и согласованность с растущим числом продуктов и центров сертификации. Простейшая форма иерархии состоит из одного центра сертификации, а в общем случае – из множества с явно определенными отношениями родительский-дочерний.

Инфраструктура открытых ключей, реализованная в операционной системе Microsoft Windows 2000 полностью поддерживает и позволяет создать иерархическую модель центров сертификации.



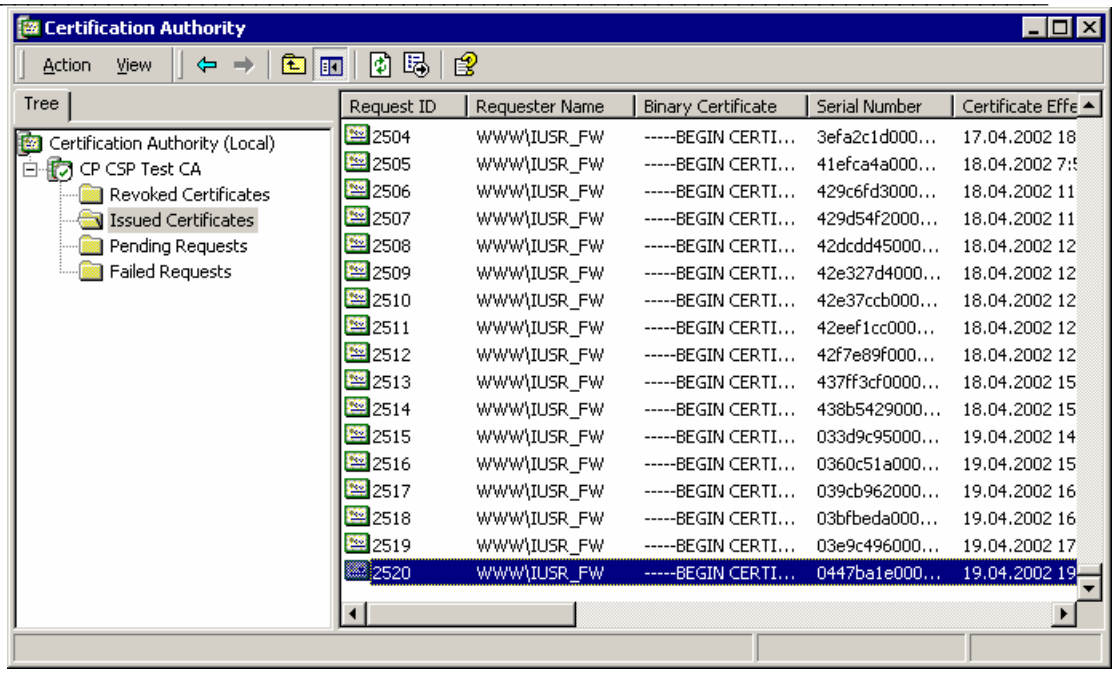
В состав служб сертификации операционной системы Windows 2000 входят следующие службы и компоненты.

Сервис сертификации

Сервис сертификации предоставляет набор служб для выпуска, управления и использования сертификатов открытых ключей в защищенных технологиях и приложениях, использующих ИОК. Сервис сертификации выполняет основную роль в управлении безопасностью технологий и приложений и обеспечивает процесс достоверного и конфиденциального обмена информацией.

Консоль центра сертификации

Консоль центра сертификации является рабочим местом администратора безопасности, позволяющим управлять сертификатами открытых ключей.



Средства расширения функциональности сервиса сертификации

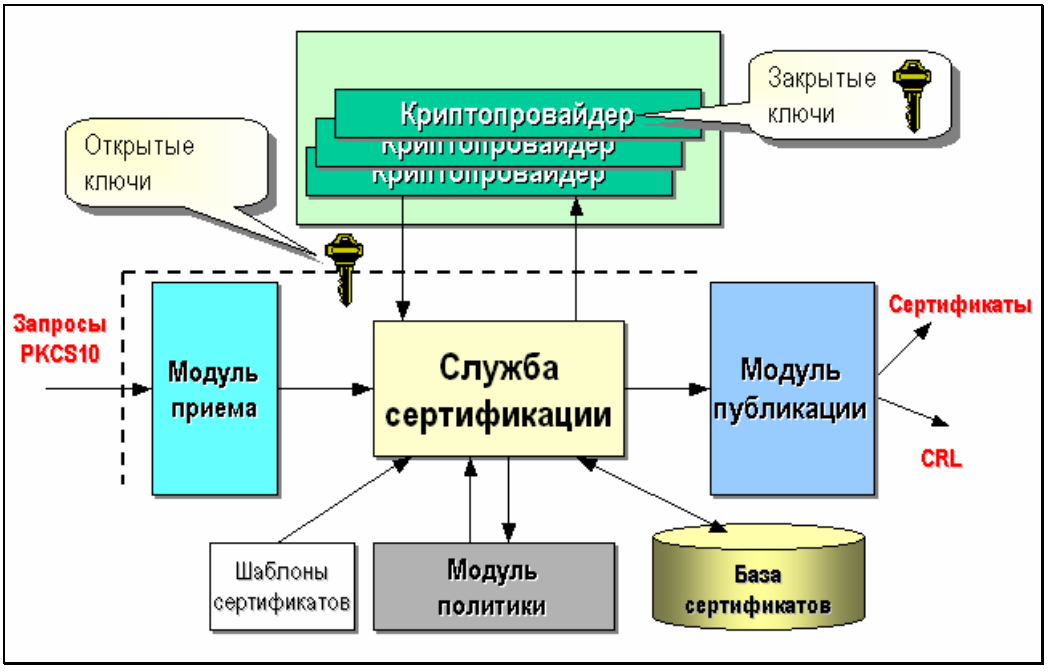
Средства расширения функциональности сервиса сертификации предоставляют набор методов, позволяющих изменять и развивать функциональность стандартного сервиса сертификации для удовлетворения потребности конкретной прикладной системы или технологии. Эти средства позволяют интегрировать сервиса сертификации с различными сетевыми справочниками и приложениями, формировать состав сертификатов открытых ключей, модифицировать процесс управления сертификатами.

Клиентские средства взаимодействия со службой сертификации

Клиентские средства предоставляют пользователям различные методы для формирования закрытых ключей, запросов на сертификаты и обработки сертификатов, выпущенных службой сертификации.

Архитектура сервиса сертификации

Архитектура сервиса сертификации представлена на следующем рисунке.



Приложение 3. Управление протоколированием

Для включения/отключения значение log используйте:

a) для Windows 32/ Windows 64 KC1 добавьте в реестр в

HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\debug\

DWORD параметр cprmcsp для определения уровня протокола

DWORD параметр cprmcsp_fmt для определения формата протокола

b) для Windows 32/ Windows 64 KC2 добавьте в реестр в

HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\debug\
DWORD параметр cpcspi для определения уровня протокола

DWORD параметр cpcspi_fmt для определения формата протокола

c) для Windows 32/ Windows 64 драйвер

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\cpdrvlib\

DWORD параметр debug для определения уровня протокола

DWORD параметр format для определения формата протокола

Значением параметра уровнь протокола является битовая маска:
N_DB_ERROR = 1 # сообщения об ошибках
N_DB_LOG = 8 # сообщения о вызовах

Значением параметра формат протокола является битовая маска:
DBFMT_MODULE = 1 # выводить имя модуля

DBFMT_THREAD = 2 # выводить номер нитки

DBFMT_FUNC = 8 # выводить имя функции

DBFMT_TEXT = 0x10 # выводить само сообщение

DBFMT_HEX = 0x20 # выводить HEX дамп

DBFMT_ERR = 0x40 # выводить GetLastError

Лист регистрации изменений

Лист регистрации изменений									
	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводи-тельного докум. и дата	Подп.	Дата
Изм	изменен-ных	замененных	новых	аннулиро-ванных					