127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро CSP Версия 5.0 R2 КС1 Исполнение 1-Base

Руководство администратора безопасности. Использование СКЗИ под управлением ОС Sailfish

ЖТЯИ.00101-02 91 10
Листов 21

2021 г

Содержание

Аннотация

Настоящее руководство содержит общее описание средства криптографической защиты информации «КриптоПро CSP» версия 5.0 R2 КС1 исполнение 1-Base и рекомендации по использованию СКЗИ под управлением операционной системы Sailfish.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» версия 5.0 R2 КС1 исполнение 1-Base под управлением ОС Sailfish, должны разрабатываться с учетом требований настоящего документа.

Список определений и сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск (Hard Disk Drive)
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
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 или ключа проверки электронной подписи и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа или ключа проверки электронной подписи абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей и ключей проверки электронной подписи. Сетевой справочник
СФ	Среда функционирования
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭП	Электронная подпись

1 Основные технические данные и характеристики СКЗИ

1.1 Программно-аппаратные среды функционирования

СКЗИ «КриптоПро CSP» версия 5.0 R2 KC1 исполнение 1-Base под управлением ОС Sailfish используется в программно-аппаратных средах:

Sailfish OS (Sailfish Mobile OS RUS) 2/3 (ОС «Аврора») (ARMv7)

1.2 Ключевые носители

Перечень поддерживаемых ключевых носителей в зависимости от программно-аппаратной платформы отражен в ЖТЯИ.00101-02 30 01. КриптоПро CSP. Формуляр, п. 3.10.

Использование носителей других типов допускается только по согласованию с ФСБ России.

Примечание. В состав дистрибутива СКЗИ входят библиотеки поддержки всех перечисленных носителей, но не входят драйверы для ОС. По вопросам получения драйверов необходимо обращаться к производителям соответствующих устройств.

2 Установка дистрибутива ПО СКЗИ

Установка, удаление и обновление ПО осуществляется от имени пользователя, имеющего права администратора (например, с использованием команды devel-su).

СКЗИ КриптоПро CSP требует следующей последовательности установки: сначала устанавливается провайдер, затем устанавливаются остальные модули, входящие в состав комплектации.

В ОС Sailfish для установки, удаления и обновления ПО применяются пакеты (packages). Пакет — архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, использующиеся инсталлятором для конфигурирования среды. В операционных системах Linux используется менеджер пакетов RPM (Red Hat Package Manager), который является гибким инструментом для установки, удаления, обновления и сборки программных пакетов. Пакеты, представленные в виде файла с расширением .rpm, содержат в себе непосредственно файлы ПО и информацию для конфигурирования среды.

Для установки пакета используется команда:

```
rpm -i <файл_пакета>
```

Например: `rpm -i ./lsb-cprocsp-base-5.0-5.noarch.rpm`

Для удаления пакета используется команда:

```
rpm -e <имя_пакета>
```

Например: `rpm -e lsb-cprocsp-base-5.0-5`

Имя пакета может не включать версию, например: `rpm -e lsb-cprocsp-base`

Пакеты зависят друг от друга, поэтому должны устанавливаться по порядку с учётом этих зависимостей, а удаляться в обратном порядке. Условно можно считать правильным порядком тот, который описан в таблице зависимостей и назначения пакетов (см. табл. 1).

Таблица 1. Зависимости и назначения пакетов

Имя пакета	Зависимости	Назначение пакета
Обязательные пакеты		
lsb-cprocsp-base	lsb	Базовый пакет КриптоПро CSP, устанавливается первым
lsb-cprocsp-rdr	lsb-cprocsp-base	Модуль поддержки основных приложений, считывателей и ДСЧ
lsb-cprocsp-kc1	lsb-cprocsp-rdr	Провайдер класса КС1
lsb-cprocsp-capilite	lsb-cprocsp-rdr, lsb-cprocsp-kc1	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS...)
Дополнительные пакеты		
cprocsp-rdr-pcsc	lsb-cprocsp-rdr, pcsclite	Модули поддержки PCSC-считывателей, смарт-карт
lsb-cprocsp-pkcs11	lsb-cprocsp-rdr	Модуль поддержки PKCS11

lsb-cprocsp-devel	lsb-cprocsp-base	Пакет для разработчика приложений, использующих КриптоПро CSP
cprocsp-curl	lsb-cprocsp-capilite	Библиотека libcurl с поддержкой российских криптоалгоритмов
cprocsp-stunnel	lsb-cprocsp-capilite	Универсальный SSL/TLS туннель
cprocsp-stunnel-msspi	lsb-cprocsp-capilite	Универсальный SSL/TLS туннель с поддержкой интерфейса msspi
lsb-cprocsp-import-ca-certs	lsb-cprocsp-capilite	Корневые сертификаты доверенных ЦС
Поддержка ключевых носителей		
cprocsp-rdr-cpfkc	cprocsp-rdr-pcsc	Модуль поддержки ФКН с поддержкой SESPAKE
cprocsp-rdr-edoc	cprocsp-rdr-pcsc	Модуль поддержки платформы eDoc (УЛГ)
cprocsp-rdr-emv	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт Gemalto (EMV)
cprocsp-rdr-infocrypt	cprocsp-rdr-pcsc	Модуль поддержки токенов InfoCrypt
cprocsp-rdr-mskey	cprocsp-rdr-pcsc	Модуль поддержки токенов Multisoft MS_Key
cprocsp-rdr-rutoken	cprocsp-rdr-pcsc	Модуль поддержки смарт-карт и токенов Рутокен

3 Обновление ПО СКЗИ

Для обновления ПО СКЗИ на ОС Sailfish необходимо:

- запомнить текущую конфигурацию КриптоПро CSP;
  - набор установленных пакетов;
  - настройки провайдера (для простоты можно сохранить /etc/opt/cprocsp/config.ini);
- удалить штатными средствами ОС все пакеты СКЗИ;
- установить аналогичные новые пакеты СКЗИ;
- при необходимости внести изменения в настройки (можно посмотреть diff старого и нового config.ini);
- ключи и сертификаты сохраняются автоматически.

4 Настройка СКЗИ

4.1 Доступ к утилите для настройки СКЗИ

Настройка СКЗИ осуществляется с помощью утилиты cpconfig, которая входит в состав дистрибутива и расположена в директории /opt/cprocsp/sbin/arm.

4.2 Ввод серийного номера лицензии

При установке программного обеспечения КриптоПро CSP без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер с бланка лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).

Для просмотра информации о лицензии выполните:

```
# cpconfig -license -view
```

Для ввода лицензии выполните:

```
# cpconfig -license -set <серийный_номер>
```

Серийный номер следует вводить с соблюдением регистра символов.

4.3 Настройка оборудования СКЗИ

Утилита cpconfig также предназначена для изменения набора устройств хранения (носителей) и считывания (считывателей) ключевой информации и датчиков случайных чисел. Предустановленными являются считыватели flash-носителей и файлов на жестком диске, а также консольный БиоДСЧ и считыватель внешней гаммы.

Для просмотра списка настроенных считывателей:

```
# ./cpconfig -hardware reader -view
```

Для просмотра списка настроенных ДСЧ:

```
# ./cpconfig -hardware rndm -view
```

Для использования внешней гаммы надо скопировать файлы с данными, полученными с помощью «АРМ выработки внешней гаммы». Пример копирования файлов (положим, что они лежат в /tmp/db[1,2]):

```
# cp /tmp/db1/kis_1 /var/opt/cprocsp/dsrf/db1/kis_1

# cp /tmp/db2/kis_1 /var/opt/cprocsp/dsrf/db2/kis_1
```

При необходимости консольный БиоДСЧ и считыватель внешней гаммы возможно добавить вручную.

Для консольного БиоДСЧ требуется пакет пакет lsb-cprocsp-kc1, кроме того он работает только с KC1 провайдером. Для добавления консольного БиоДСЧ:

```
# ./cpconfig -hardware rndm -add bio_tui -level 5 -name "Console BioRNG"
```

Для добавления использования внешней гаммы:

```
# ./cpconfig -hardware rndm -add cpsd -name 'cpsd rng' -level 3

# ./cpconfig -hardware rndm -configure cpsd -add string /db1/kis_1 /var/opt/cprocsp/dsrf/db1/k

# ./cpconfig -hardware rndm -configure cpsd -add string /db2/kis_1 /var/opt/cprocsp/dsrf/db2/k
```

Для получения подробной справки по cpconfig:

```
# ./cpconfig -help

# ./cpconfig -hardware -help
```

4.4 Установка параметров журналирования

СКЗИ позволяет собирать отладочную информацию и имеет возможность протоколирования событий. Информация записывается в системный журнал. Существует возможность изменения настроек журналирования различных модулей СКЗИ. Существует возможность изменения уровня журналирования и формата выводимых отладочных сообщений.

Для получения справки по настройкам журналирования:

```
# cpconfig -loglevel -help
```

Подробнее опции управления протоколированием модулями СКЗИ см. в Приложении А.

4.5 Настройка криптопровайдера по умолчанию

Проводить настройку криптопровайдера по умолчанию нужно только в особых случаях для совместимости. Для просмотра типов доступных криптопровайдеров:

```
# ./cpconfig -defprov -view_type
```

Для просмотра свойств криптопровайдера нужного типа:

```
# ./cpconfig -defprov -view -provtype <provtype>
```

Для установки провайдера по умолчанию для нужного типа:

```
# ./cpconfig -defprov -setdef -provtype <provtype> -provname <provname>
```

Для получения имени провайдера по умолчанию для нужного типа:

```
# ./cpconfig -defprov -getdef -provtype <provtype>
```

4.6 Включение режима усиленного контроля использования ключей

Режим усиленного контроля использования ключей обеспечивает осуществление контроля срока действия долговременных ключей электронной подписи и ключевого обмена, контроля доверенности ключей проверки электронной подписи и контроля корректного использования программного датчика случайных чисел. После успешной инсталляции необходимо включить данный режим, выполнив команду:

```
#./cpconfig -ini '\config\parameters' -add long StrengthenedKeyUsageControl 1
```

Для обеспечения корректного функционирования провайдера в части выработки электронной подписи, а также работы с временными ключами (в частности, для работы в рамках TLS-соединения без аутентификации клиента) и генерации случайных данных необходимо произвести выработку долговременных ключей или запустить утилиту csptest, предварительно проверив, что зарегистрирован хотя бы один датчик случайных чисел:

```
# ./csptest -keyset -verifycontext -hard_rng
```

Примечание. Использование СКЗИ без включения режима усиленного контроля использования ключей разрешается исключительно в тестовых целях.

4.7 Настройка параметров алгоритмов

Для установки параметров алгоритмов (для провайдеров типа 75):

параметры алгоритма шифрования:

```
# ./cpconfig -ini '\config\OID' -add string cipher <OID>
```

параметры алгоритма подписи:

```
# ./cpconfig -ini '\config\OID' -add string sign_el_2001 <OID>
```

параметры алгоритма Диффи-Хеллмана:

```
# ./cpconfig -ini '\config\OID' -add string dh_el_2001 <OID>
```

Для установки параметров алгоритмов (для провайдеров типа 80):

параметры алгоритма шифрования:

```
# ./cpconfig -ini '\config\OID' -add string cipher_2012 <OID>
```

параметры алгоритма подписи:

```
# ./cpconfig -ini '\config\OID' -add string sign_el_2012 <OID>
```

параметры алгоритма Диффи-Хеллмана:

```
# ./cpconfig -ini '\config\OID' -add string dh_el_2012 <OID>
```

Для установки параметров алгоритмов (для провайдеров типа 81):

параметры алгоритма шифрования:

```
# ./cpconfig -ini '\config\OID' -add string cipher_2012 <OID>
```

параметры алгоритма подписи:

```
# ./cpconfig -ini '\config\OID' -add string sign_el512 <OID>
```

параметры алгоритма Диффи-Хеллмана:

```
# ./cpconfig -ini '\config\OID' -add string dh_el512 <OID>
```

Перечень поддерживаемых в КриптоПро CSP идентификаторов криптографических параметров алгоритмов указан в `CSP_5_0.chm`.

5 Состав и назначение компонент ПО СКЗИ

5.1 Базовые модули СКЗИ

ПО СКЗИ содержит следующие базовые модули:

`libcsp`	динамически загружаемая библиотека КриптоПро CSP; реализует целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям, БиоДСЧ
`libcspr`	обеспечивает удаленный доступ к криптопровайдеру, функционирующему как отдельный сервис
`libssp`	обеспечивает реализацию протокола сетевой аутентификации КриптоПро TLS (общее описание протокола приведено в документе ЖТЯИ.00101-02 90 01. Описание реализации)
`cpverify`	модуль контроля целостности при установке СКЗИ и функционировании ПО СКЗИ КриптоПро CSP на ПЭВМ пользователя
`wipefile`	модуль удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях
`cryptcp`	приложение командной строки для работы с сертификатами с использованием инфраструктуры открытых ключей, шифрования/расшифрования сообщений, содержащихся в файлах, создания/проверки электронных подписей и хэширования сообщений, содержащихся в файле или группе файлов (подробное описание см. в ЖТЯИ.00101-02 93 01. Приложение командной строки для подписи и шифрования файлов)
`certmgr`	приложение командной строки для управления сертификатами, списками отзыва сертификатов (CRL) и хранилищами (подробное описание см. в ЖТЯИ.00101-02 93 02. Приложение командной строки для работы с сертификатами)
`stunnel`	приложение для создания TLS-туннеля, предназначенного для создания TLS защищенного соединения между клиентом и локальным (linetd-запускаемым) или удаленным сервером (подробное описание см. в ЖТЯИ.00101-02 93 03. Приложение для создания TLS-туннеля)

В названиях дистрибутивов СКЗИ в качестве префикса используется обозначение cprocsp.

5.2 Модули подсистемы программной среды функционирования криптосредства (СФ)

5.2.1 Модуль libcapi20

Модуль libcapi20 используется для управления сертификатами открытых ключей, а также для обеспечения выполнения криптографических запросов на уровне интерфейса CryptoAPI 2.0. Интерфейс модуля libcapi20 является подмножеством интерфейса CryptoAPI 2.0.

5.2.2 Модуль librdrfat12

Библиотека librdrsup обеспечивает реализацию общих функций доступа к различным устройствам хранения ключевой информации.

Следующие модули обеспечивают реализацию доступа к конкретным типам ключевых носителей:

`librdrcpfkc.so`	токены и смарт-карты с поддержкой SESPAKE
`librdredoc.so`	платформа eDoc (УЛГ)
`librdremv.so`	смарт-карты Gemalto (EMV)
`librdrfat12.so`	съемные диски и раздел HDD/SDD
`librdrinfocrypt.so`	токены InfoCrypt
`librdrmskey.so`	токены Multisoft MS_Key
`librdrpcsc.so`	базовый считыватель носителей, поддерживающих интерфейс PC/SC
`librdrric.so`	смарт-карты Оскар и Форос (Магистра)
`librdrrutoken.so`	смарт-карты и токены Рутокен

5.2.3 Модули датчиков случайных чисел

Библиотеки librdrdsrf и librdrrndmbio обеспечивают поддержку работы с внешней гаммой и БиоДСЧ соответственно.

5.2.4 Библиотека libcpasn1 поддержки формата ASN1

Библиотека libcpasn1 содержит функции преобразования структур данных в машинно-независимое представление.

6 Требования по защите от НСД

6.1 Организационно-технические меры защиты от НСД

Должны выполняться требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации СКЗИ в объеме раздела 5 ЖТЯИ.00101-02 95 01. Правила пользования.

При эксплуатации СКЗИ на платформе Sailfish при обработке конфиденциальной информации для конкретного мобильного устройства, работающего под управлением ОС Sailfish, должны выполняться действующие в Российской Федерации требования по защите открытой (конфиденциальной) информации от утечки по техническим каналам. Данное требование не предъявляется в случае эксплуатации СКЗИ на платформе Sailfish при обработке открытой информации, доступ к которой не ограничивается согласно законодательству Российской Федерации. Внос и использование мобильного устройства, работающего под управлением ОС Sailfish, в помещениях, в которых ведутся переговоры секретного содержания или проводятся работы секретного характера, без проведения его специальных исследований и специальной проверки запрещаются.

При использовании СКЗИ КриптоПро CSP под управлением ОС Sailfish необходимо предпринять дополнительные меры организационного и технического характера и выполнить дополнительные настройки операционной системы. При этом ставится задача не только обеспечить дополнительную защиту устройства и ОС от НСД, но и обеспечить бесперебойный режим работы и исключить возможности «отказа в обслуживании», вызванного внутренними причинами (например, переполнением файловых систем).

6.2 Дополнительные настройки ОС Sailfish и операционных систем, к которым подключается устройство

6.2.1 Индивидуальная настройка Sailfish

В настройках Sailfish в разделе «Безопасность — Блокировка устройства» необходимо включить пароли. Необходимо задать сложность пароля и настройки для количества попыток ввода пароля, соответствующие требованиям п. 5.4 документа ЖТЯИ.00101-02 95 01. Правила пользования.

6.2.2 Корпоративная настройка Sailfish

Корпоративная настройка Sailfish может быть выполнена средствами набора управления мобильными устройствами (англ. Mobile device management, MDM). Данные средства не поставляются в комплекте с операционной системой, но могут работать с ОС Sailfish путём использования предусмотренного системного API.

Путём создания профилей средствами MDM или в индивидуальном порядке в рамках корпоративной настройки на каждом устройстве Sailfish, на котором эксплуатируется СКЗИ КриптоПро CSP, должны быть применены следующие параметры:

1) На вход в устройство должен быть установлен пароль со следующими настройками:
   - максимальный срок действия пароля не должен превышать 6 месяцев;
   - устанавливаемый пароль должен не совпадать с последними 6 использованными паролями;
   - сложность пароля и настройки для удаления данных в случае неправильного ввода пароля должны соответствовать требованиям п. 5.4 документа ЖТЯИ.00101-02 95 01. Правила пользования.

2) Должны быть отключены все разрешения, которые не являются необходимыми для выполнения работы. Должна быть отключена возможность установки приложений. Если эта возможность необходима для

работы, её необходимо оставить, но настроить ограничения через средства MDM (см. ниже).

3) Если в организации имеется сервер для управления мобильными устройствами (MDM server), то необходимо настроить подключение к нему. Сервер может быть использован для получения настроек (в том числе новых профилей настроек) и приложений.

6.2.3 Настройка ОС, к которой подключается устройство

1) Выполните рекомендации по дополнительной настойке ОС из руководства администратора безопасности для соответствующей ОС.

2) Если на устройстве хранятся закрытые ключи, резервные копии устройства должны быть зашифрованы. Для этого:

- Установите на компьютер, к которому подключается устройство, ПО для шифрования файлов (например, КриптоПро EFS).
- Выполните резервное копирование данных устройства на компьютер.
- С помощью ПО для шифрования файлов выполните зашифрование резервной копии.

7 Требования по криптографической защите

Должны выполняться требования по криптографической защите раздела 6 документа ЖТЯИ.00101-02 95 01. Правила пользования в части, касающейся ОС Sailfish.

Необходимо выполнить настройку операционной системы для работы с СКЗИ по разд. 6.2.

Контролем целостности должны быть охвачены файлы:

```
/opt/cprocsp/bin/arm/certmgr
/opt/cprocsp/bin/arm/cpverify
/opt/cprocsp/bin/arm/cryptcp
/opt/cprocsp/bin/arm/csptest
/opt/cprocsp/bin/arm/csptestf
/opt/cprocsp/bin/arm/der2xer
/opt/cprocsp/bin/arm/genkpim
/opt/cprocsp/bin/arm/inittst
/opt/cprocsp/bin/arm/wipefile
/opt/cprocsp/sbin/arm/cpconfig
/opt/cprocsp/sbin/arm/mount_flash.sh
/opt/cprocsp/sbin/arm/unreg_prov_type_name.sh
/opt/cprocsp/lib/arm/libasn1data_XER.so.4.0.4
/opt/cprocsp/lib/arm/libcapi10.so.4.0.4
/opt/cprocsp/lib/arm/libcapi20.so.4.0.4
/opt/cprocsp/lib/arm/libcpalloc.so.0.0.0
/opt/cprocsp/lib/arm/libcpasn1.so.4.0.4
/opt/cprocsp/lib/arm/libcpext.so.4.0.4
/opt/cprocsp/lib/arm/libcplib.so.4.0.4
/opt/cprocsp/lib/arm/libcpui.so.4.0.4
/opt/cprocsp/lib/arm/libcsp.so.4.0.4
/opt/cprocsp/lib/arm/libenroll.so.4.0.4
/opt/cprocsp/lib/arm/librdrdsrf.so.4.0.4
/opt/cprocsp/lib/arm/librdrfat12.so.4.0.4
/opt/cprocsp/lib/arm/librdrrndmbio_tui.so.4.0.4
/opt/cprocsp/lib/arm/librdrsup.so.4.0.4
/opt/cprocsp/lib/arm/libssp.so.4.0.4
/opt/cprocsp/lib/arm/libsspdrv.a
/opt/cprocsp/lib/arm/liburlretrieve.so.4.0.4
```

Приложение А
Управление протоколированием

Уровень, содержание и методы вывода информации независимо устанавливаются для выделенных модулей аудита (см. табл. А1). Несколько библиотек могут использовать один модуль аудита, возможна и обратная ситуация.

Таблица А1. Модули аудита

Модуль (name)	**Описание**
`capi10`	CryptoAPI 1.0
`capi20`	CryptoAPI 2.0
`ssp`	TLS
`cspr`	клиентский RPC
`cpext`	расширения CryptoAPI
`cloud`	облачный провайдер
`csp`	ядро CSP
`pcsc`	считыватели PC/SC

Для определения **уровня протокола** (`levelmask`, см. табл. А2):

```
/opt/cprocsp/sbin/arm/cpconfig -loglevel <name> -mask <levelmask>
```

Для задания **формата протокола** (`formatmask`, см. табл. А3):

```
/opt/cprocsp/sbin/arm/cpconfig -loglevel <name> -format <formatmask>
```

Для просмотра текущих значений уровня и формата протокола:

```
/opt/cprocsp/sbin/arm/cpconfig -loglevel <name> -view
```

Таблица А2. Уровни протоколирования

N_DB_ERROR = 1 (0x01)	критические ошибки
N_DB_WARN = 2 (0x02)	некритические ошибки
N_DB_CALL = 4 (0x04)	информация о вызове функции
N_DB_LOG = 8 (0x08)	нейтральная информация
N_DB_TRACE = 16 (0x10)	отладочная информация
N_DB_CRUCIAL = 32 (0x20)	информация о важных событий (например, создание ключа, удаление ключевого контейнера, ...)

Таблица А3. Форматы протокола

DBFMT_MODULE = 0x01	выводить имя модуля
DBFMT_THREAD = 0x02	выводить номер нитки
DBFMT_FLINE = 0x04	выводить номер линии
DBFMT_FUNC = 0x08	выводить имя функции
DBFMT_TEXT = 0x10	выводить само сообщение
DBFMT_HEX = 0x20	выводить HEX дамп
DBFMT_ERR = 0x40	выводить GetLastError
DBFMT_PID = 0x80	выводить идентификатор процесса
DBFMT_PROCESS = 0x100	выводить имя процесса

Лист регистрации изменений

Лист регистрации изменений									
№ п/п	Номера листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					