

ООО «ВАЛИДАТА»

УТВЕРЖДЕН  
ВАМБ.00077-06-ЛУ

**«ВАЛИДАТА КЛИЕНТ» ВЕРСИЯ 4**  
ИСПОЛНЯЕМЫЙ МОДУЛЬ КОМАНДНОЙ СТРОКИ  
Руководство пользователя

ВАМБ.00077-06 92 02

2020

## **Аннотация**

Настоящий документ содержит описание исполняемого модуля командной строки, называемого также утилитой командной строки, для операционной системы (ОС) Windows.

Документ предназначен для пользователей программного комплекса (ПК) ВАМБ.00077-06 «Валидата Клиент» версия 4» как руководство по эксплуатации исполняемого модуля командной строки.

## Содержание

<b>1 НАЗНАЧЕНИЕ</b>	<b>4</b>
1.1 Назначение модуля . . . . .	4
1.2 Требования к аппаратно-программной среде . . . . .	4
<b>2 РАБОТА С ИСПОЛНЯЕМЫМ МОДУЛЕМ</b>	<b>5</b>
2.1 Основное меню команд . . . . .	5
2.2 Расширенное меню команд . . . . .	6
2.3 Примеры использования основного меню . . . . .	7
2.3.1 Вычисление хэш-значения . . . . .	8
2.3.2 Вычисление ЭП . . . . .	8
2.3.3 Проверка ЭП . . . . .	8
2.3.4 Зашифрование . . . . .	9
2.3.5 Расшифрование . . . . .	9
2.3.6 Получение информации . . . . .	9
2.3.7 Получение и проверка штампа времени . . . . .	10
2.3.8 Статус сертификата . . . . .	10
2.4 Примеры использования расширенного меню . . . . .	10
2.4.1 Присоединение и отсоединение ЭП . . . . .	10
2.4.2 Перебор объектов справочников . . . . .	10
2.4.3 Поиск сертификатов . . . . .	10
2.4.4 Скоростные тесты . . . . .	11
2.4.5 Профили и справочники . . . . .	11
2.4.6 Импорт и экспорт . . . . .	11
2.5 Описание файла со списком поиска сертификатов получателей . . . .	12
<b>3 ОПИСАНИЕ ОШИБОЧНЫХ СИТУАЦИЙ</b>	<b>14</b>
<b>ПЕРЕЧЕНЬ СОКРАЩЕНИЙ</b>	<b>21</b>
<b>ПЕРЕЧЕНЬ ТАБЛИЦ</b>	<b>22</b>

# 1 НАЗНАЧЕНИЕ

## 1.1 Назначение модуля

Исполняемый модуль командной строки для ОС Windows предназначен для осуществления доступа пользователей к функциям ПК ВАМБ.00077-06 «“Валидата Клиент” версия 4» (далее — ПК «Валидата Клиент») из режима командной строки ОС Windows.

Исполняемый модуль позволяет осуществлять вычисление и проверку подлинности электронной подписи (ЭП) файлов, зашифрование и расшифрование файлов, а также выполнять множество других криптографических и сопутствующих функций, поддерживаемых в ПК «Валидата Клиент».

Обращение пользователей к функциям ПК «Валидата Клиент» осуществляется через вызов исполняемого модуля **zpk1utl** с заданием параметров выполнения из режима командной строки.

## 1.2 Требования к аппаратно-программной среде

Требования к аппаратно-программной среде, в которой функционирует исполняемый модуль командной строки, приведены в документах ВАМБ.00077-06 30 01 «“Валидата Клиент” версия 4. Формуляр» и ВАМБ.00060-06 30 01 «СКЗИ «Валидата CSP» версия 6. Формуляр».

Перед началом работы с исполняемым модулем необходимо установить ПК ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» в соответствии с документом ВАМБ.00060-06 91 01 «СКЗИ «Валидата CSP» версия 6. Руководство по установке и настройке» и ПК «Валидата Клиент» в соответствии с документом ВАМБ.00077-06 91 01 «“Валидата Клиент” версия 4. Руководство по установке и настройке».

## 2 РАБОТА С ИСПОЛНЯЕМЫМ МОДУЛЕМ

### 2.1 Основное меню команд

Исполняемый модуль **zpkilutl** выдает описание основного меню команд (операций) при запуске без задания операций командной строки:

Утилита командной строки (версия 6.0.451.0) использование:  
zpkilutl [ОПЕРАЦИИ] [ПАРАМЕТРЫ] [ОПЦИИ]  
операции:

- hash вычисление хэш-значения файла
- sign вычисление ЭП файла
- verify проверка ЭП файла
- encrypt зашифрование файла
- decrypt расшифрование файла
- msginf получение информации о CMS сообщении
- tssign получение штампа времени
- tsverif проверка штампа времени
- ocspinf получение статуса сертификата
- tools использование расширенных возможностей
- help показ справки по утилите

параметры:

- profile [PROFILE] установить имя профиля в PROFILE
- registry использовать настройки профилей Справочника
- algorithm [OID] объектный идентификатор алгоритма хэширования
- in [INFILE] имя входного файла INFILE
- out [OUTFILE] имя выходного файла OUTFILE
- data [DATAFILE] имя файла данных DATAFILE (для ЭП и хэш-значения)

опции:

- minimal использовать минимальный набор функций
- stream использовать потоковые криптографические функции
- format [FMT] формат хэш-значения - 1: LE число (по умолчанию); 2: LE байты; 3: BE число; 4: Base64
- silent [ERRFILE] режим без показа сообщений с записью протокола в ERRFILE
- sendcert добавлять/требовать наличия сертификата подписанта при вычислении/проверке ЭП
- crlupdate обычное обновление CAC из точек распространения
- critical критичное обновление CAC из точек распространения (требует -crlupdate)
- url [URL] адрес сервера штампов времени или сервера статуса сертификатов, URI справочника
- index [IDX] индекс ЭП штампа времени >= 1 (по умолчанию)

опции проверки ЭП:

- revtime использовать время аннулирования сертификата
- detached задать отсоединенный формат ЭП
- eku [EKU] добавить OID EKU расширенного использования ключа
- policy [POLICY] добавить OID POLICY регламента использования

сертификата

- delete [КОЛ] удалить КОЛ ЭП (с конца) после проверки
- ldap включить возможность поиска сертификатов в ССС
- aiacdp использовать точки AIA и CDP при построении цепочек
- info [FIELDS] выводимая информация о сертификате (по умолчанию: владелец, хэш)

возможные значения: serial, issuer, subject, notbefore, notafter, altname, keyid, certhash, algorithm, all

опции шифрования:

- recsubj [SUBJ] добавить сертификат с именем владельца SUBJ в список получателей
- rechash [HASH] добавить сертификат с хэшем издателя/сер. номера HASH в список получателей
- reckeyid [KEYID] добавить сертификат с идентификатором ключа KEYID в список получателей
- reclist [FILE] считать список получателей из файла FILE
- partial имена владельцев сертификатов получателей заданы частично
- nolocal исключить поиск сертификатов в хранилище ЛСП
- nocache исключить поиск сертификатов в хранилище КЭШ
- attrib использовать поиск по значению атрибута vdSubjName ССС
- 1215mg зашифровывать CMS сообщение по ГОСТ Р 34.12-2015 Магма
- 1215gh зашифровывать CMS сообщение по ГОСТ Р 34.12-2015 Кузнечик
- 1215mac вычислять и добавлять имитовставку в зашифрованное CMS сообщение
- keyagree создавать в CMS сообщении получателей типа KeyAgreement

## 2.2 Расширенное меню команд

Исполняемый модуль **zpkilutl** выдает описание расширенного меню команд (операций) при запуске с заданием операции командной строки **-tools**:

Расширенные - Утилита командной строки (версия 6.0.451.0)

использование:

zpkilutl -tools [ОПЕРАЦИИ] [ПАРАМЕТРЫ] [ОПЦИИ]

операции:

- attach присоединение ЭП к неподписанному файлу
- detach отсоединение ЭП от подписанного файла
- enuobj перебор объектов справочников
- findcer поиск сертификатов в справочниках
- speed выполнение скоростного теста
- проверяемая операция: -hash, -sign, -verify, -encrypt, -decrypt, -findcert
- enuprof перебор настроенных профилей
- creprof создание или модификация профиля
- crestor создание хранилищ ПСП и ЛСП из заданных сертификатов и САС
- improbj импорт сертификата, САС, или обновления от ЦС или ЦР
- expreq экспорт запроса PKCS#10 или запроса на аннулирование сертификата

параметры:

- query [QUERY] логическое выражение для перебора объектов в ССС
- subject [SUBJ] имя владельца искомого сертификата
- issuer [ISSU] имя издателя искомого сертификата
- serial [SERIAL] серийный номер искомого сертификата
- cerhash [HASH] хэш издателя/сер. номера искомого сертификата
- email [EMAIL] адрес электронной почты искомого сертификата
- keyid [KEYID] идентификатор ключа ЭП искомого сертификата
- subjkid [SKID] идентификатор ключа владельца искомого сертификата

опции скоростного теста:

- iterat [ITER] количество повторений операции скоростного теста
- threads [THRS] количество потоков выполнения скоростного теста

опции профилей:

- uripse [PSE] путь к хранилищу сертификатов ПСП
- uriloc [LOCAL] путь к хранилищу сертификатов ЛСП
- urildp [LDAP] путь к хранилищу сертификатов ССС
- dercer [FCER] путь к файлу сертификата в DER- или PEM-формате
- dercrl [FCRL] путь к файлу CAC в DER- или PEM-формате

опции импорта и экспорта:

- showui отображать диалоговый интерфейс показа объекта
- signer установить рабочий сертификат пользователя
- remote принудительно импортировать объект в ССС
- 512bit формировать ключ ЭП по ГОСТ Р 34.10-2012 512 бит (по умолчанию: 256 бит)
- cargen формировать ключ ЭП внутри vdToken (ФКН) с ДСЧ
- revoke формировать запрос на аннулирование сертификата

Большинство операций из расширенного меню для корректного функционирования используют операции и параметры из основного меню.

Для операций из расширенного меню необходимо выполнять следующие правила:

- если для выполнения операции из расширенного меню используются операции и параметры из основного меню, то все они должны быть заданы в командной строке до операции **-tools**;
- все операции и параметры из расширенного меню должны быть заданы в командной строке после операции **-tools**.

## 2.3 Примеры использования основного меню

Здесь и далее документе используются следующие расширения для каждого из типов файлов:

- **.p7s** - подписанный файл (файл с присоединенной или отсоединенной ЭП);
- **.p7s.ts** - подписанный файл, хотя бы одна из ЭП которого содержит штамп времени;
- **.p7e** - зашифрованный файл;
- **.pse** - файл персонального справочника пользователя (ПСП), подписанного

запроса или обновления;

- **.gdbm** - файл локального справочника пользователя (ЛСП);
- **.cer** - файл сертификата в DER-кодировке или PEM-формате;
- **.crl** - файл списка аннулированных сертификатов (САС) в DER-кодировке или PEM-формате;
- **.req** - файл PKCS#10 запроса на получение сертификата в DER-кодировке или PEM-формате.

### 2.3.1 Вычисление хэш-значения

Блочное вычисление хэш-значения файла по ГОСТ Р 34.11-94:

```
-minimal -hash -data data -algorithm "1.2.643.2.2.9"
```

Блочное вычисление хэш-значения файла по ГОСТ Р 34.11-2012 (256 бит) с выводом результата в формате **Little-Endian байты**:

```
-minimal -hash -data data -algorithm "1.2.643.7.1.1.2.2" -format 2
```

Потоковое вычисление хэш-значения файла по ГОСТ Р 34.11-2012 (512 бит) с выводом результата в формате **Big-Endian число**:

```
-minimal -hash -data data -algorithm "1.2.643.7.1.1.2.3" -stream -  
format 3
```

### 2.3.2 Вычисление ЭП

Блочное вычисление первой присоединенной ЭП файла:

```
-sign -data data -out data.1.p7s
```

Блочное вычисление второй присоединенной ЭП файла с добавлением сертификата подписанта:

```
-sign -data data.1.p7s -out data.2.p7s -sendcert
```

Потоковое вычисление первой отсоединенной ЭП файла:

```
-sign -data data -out data.1.p7s -detached -stream
```

Потоковое вычисление второй отсоединенной ЭП файла с использованием профиля **Профиль 1** Справочника сертификатов:

```
-registry -profile "Профиль 1" -sign -data data -in data.1.p7s -out  
data.2.p7s -detached -stream
```

### 2.3.3 Проверка ЭП

Блочная проверка и удаление всех присоединенных ЭП файла с проверкой сертификатов подписантов на наличие расширенного использования ключа **Проверка подлинности клиента**:

```
-verify -in data.p7s -out data -delete -1 -eku "1.3.6.1.5.5.7.3.2"
```



Потоковая проверка всех отсоединенных ЭП файла с выводом полной информации о сертификатах подписантов, с возможностью поиска сертификатов подписантов в сетевом справочнике сертификатов (ССС), с возможностью построения и проверки цепочек сертификатов подписантов по точкам AIA и CDP, а также с критичным обновлением САС:

```
-verify -data data -in data.p7s -detached -stream -info all -ldap -  
aiacdp -crlupdate -critical
```

### 2.3.4 Зашифрование

Блочное зашифрование файла по ГОСТ 28147-89 с выбором сертификатов получателей из ЛСП с помощью графического интерфейса:

```
-encrypt -in data -out data.p7e
```

Блочное зашифрование файла по ГОСТ Р 34.12-2015 (блочный шифр «Магма») с заданием файла со списком поиска сертификатов получателей, с возможностью поиска сертификатов получателей в СССР, а также с возможностью построения и проверки цепочек сертификатов получателей по точкам AIA и CDP:

```
-encrypt -in data -out data.p7e -reclist .\reclist.txt -ldap -aiacdp  
-1215mg
```

Потоковое зашифрование файла по ГОСТ Р 34.12-2015 (блочный шифр «Кузнечик») с имитовставкой, с поиском сертификатов получателей по части имени владельца на совпадение со значением атрибута **vdSubjName** исключительно в СССР, а также с возможностью построения и проверки цепочек сертификатов получателей по точкам AIA и CDP:

```
-encrypt -in data -out data.p7e -recsubj "OU=123456789" -recsubj "OU  
=987654321" -partial -nolocal -nocache -attrib -ldap -aiacdp -1215  
gh -1215mac -stream
```

### 2.3.5 Расшифрование

Блочное расшифрование файла:

```
-decrypt -in data.p7e -out data
```

Потоковое расшифрование файла:

```
-decrypt -in data.p7e -out data -stream
```

### 2.3.6 Получение информации

Блочное получение информации о подписанном файле:

```
-minimal -msginf -in data.p7s
```

Потоковое получение информации о зашифрованном файле:

```
-minimal -msginf -in data.p7e -stream
```

### 2.3.7 Получение и проверка штампа времени

Блочное получение штампа времени ЭП №1 подписанного файла:

```
-tssign -in data.p7s -out data.p7s.ts -url http://tsocs.x509.ru/tsp/
```

Потоковая проверка штампа времени ЭП №2 подписанного файла:

```
-tsverif -in data.p7s.ts -index 2 -stream
```

### 2.3.8 Статус сертификата

Получение статуса сертификата:

```
-ocspinf -in data.cer -url http://tsocs.x509.ru/ocsp/
```

## 2.4 Примеры использования расширенного меню

### 2.4.1 Присоединение и отсоединение ЭП

Блочное присоединение ЭП к файлу:

```
-minimal -data data -in data.det.p7s -out data.att.p7s -tools -attach
```

Потоковое отсоединение ЭП от файла:

```
-minimal -data data -in data.att.p7s -out data.det.p7s -stream -tools  
-detach
```

### 2.4.2 Перебор объектов справочников

Перебор всех сертификатов и САС из ПСП, ЛСП и ССС:

```
-ldap -tools -enuobj
```

Перебор всех сертификатов и САС в заданном контейнере (и всех его под-контейнерах) ССС по логическому выражению LDAP с выводом полной информации о сертификатах:

```
-minimal -url "ldap://ldap.x509.ru/C=RU,O=Валидата,OU=Разработка" -  
info all -tools -enuobj -query "(&(title=*специалист*)(  
extensionAttribute10=*отдел*))"
```

### 2.4.3 Поиск сертификатов

Поиск сертификата (единственного) в ПСП и ЛСП по идентификатору ключа ЭП:

```
-tools -findcer -keyid 1209ABSCDI01
```

Поиск сертификатов (одного или нескольких) в ПСП, ЛСП и ССС по имени владельца сертификата, с возможностью построения и проверки цепочек сертификатов по точкам AIA и CDP:

```
-ldap -aiacd -tools -findcer -subject "CN=Иванов Иван Иванович,O=000  
Валидата,C=RU"
```

#### 2.4.4 Скоростные тесты

Скоростной тест потокового вычисления хэш-значения по ГОСТ Р 34.11-2012 (512 бит):

```
-minimal -hash -data data -algorithm "1.2.643.7.1.1.2.3" -stream -  
tools -speed -threads 4 -iter 1000
```

Скоростной тест блочного вычисления присоединенной ЭП:

```
-sign -data data -tools -speed -threads 4 -iter 1000
```

Скоростной тест потоковой проверки отсоединенной ЭП:

```
-verify -data data -in data.p7s -detached -tools -speed -threads 4 -  
iter 1000
```

Скоростной тест блочного зашифрования по ГОСТ Р 34.12-2015 (блочный шифр «Кузнечик») с поиском сертификатов получателей по части имени владельца исключительно в ССС, а также с возможностью построения и проверки цепочек сертификатов получателей по точкам AIA и CDP:

```
-encrypt -data data -recsubj "OU=123456789" -partial -nolocal -nocache  
-ldap -aiacdp -1215gh -tools -speed -threads 4 -iter 1000
```

Скоростной тест потокового расшифрования:

```
-decrypt -data data.p7e -stream -tools -speed -threads 4 -iter 1000
```

#### 2.4.5 Профили и справочники

Отображение списка настроенных профилей Справочника сертификатов:

```
-minimal -tools -enuprof
```

Добавление нового профиля **Профиль 2** с заданными ПСП, ЛСП и ССС:

```
-minimal -profile "Профиль 2" -tools -creprof -uripse "pse://signed/C  
:\Profiles\Профиль 2\local.pse" -uriloc "file:///C:\Profiles\Профиль  
2\local.gdbm" -urildp "ldap://ldap.x509.ru/C=RU"
```

Формирование новых ПСП и ЛСП на основании сертификатов и САС в DER-кодировке или PEM-формате:

```
-minimal -tools -crestor -uripse "pse://signed/C:\Profiles\Профиль 2\  
local.pse" -uriloc "file:///C:\Profiles\Профиль 2\local.gdbm" -  
dercer user.cer -dercer root.cer -dercrl root.crl
```

#### 2.4.6 Импорт и экспорт

Формирование первичного ключа ЭП и PKCS#10 запроса с помощью Мастера:

```
-minimal -out data.req -tools -expreq
```

Формирование первичного ключа ЭП по ГОСТ Р 34.10-2012 (512 бит) и PKCS#10 запроса на основании XML-шаблона:

```
-minimal -data data.xml -out data.req -tools -expreq -512bit
```

Формирование непервичного ключа ЭП и PKCS#10 запроса на плановую смену сертификата с его последующим отображением:

```
-out data.pse -tools -expreq -showui
```

Формирование запроса на аннулирование/прекращение действия сертификата с его последующим отображением:

```
-out data.pse -tools -expreq -showui -revoke
```

Импорт подписанного обновления, сформированного удостоверяющим центром:

```
-in data.pse -tools -impobj
```

Импорт сертификата, выпущенного удостоверяющим центром, и установка его рабочим:

```
-in user.cer -tools -impobj -signer
```

## 2.5 Описание файла со списком поиска сертификатов получателей

В исполняемом модуле командной строки реализована возможность использования **INI-файла**, содержащего список поиска сертификатов получателей для зашифрования. Имя данного файла **с полным путем** передается в качестве параметра опции **-reclist**. В случае, если файл находится в текущем каталоге исполняемого модуля командной строки, к его имени необходимо добавить префикс **.\**.

Ниже приведены пример и формализованное описание содержимого такого файла:

```
[General]
Number=4

[Recipient1]
Type=KeyId
Value=1209ABSCDI01

[Recipient2]
Type=Subject
Value=CN=Иванов Иван Иванович,O=000 Валидата,C=RU

[Recipient3]
Type=Hash
Value=71:3E:47:27:3C:8D:44:6F:72:37:8A:6E:83:09:86:B0:21:B6:E6:83:2F
      :79:13:31:7B:C0:87:4B:72:F9:5D:4B

[Recipient4]
Type=Mail
```

Value=IvanovII@x509.ru

Строка комментария должна начинаться символом ;.

Параметр **Number** в секции **[General]** задаёт длину списка поиска сертификатов получателей. Для каждого из элементов списка должна быть задана секция **[RecipientN]**, где **N** – порядковый номер элемента, который начинается с **1**.

В секции каждого из элементов списка необходимо задать тип идентификации (тип поиска) в параметре **Type**, а значение для поиска - в параметре **Value**.

Поддерживаются следующие типы идентификации:

- **KeyId** - поиск сертификата получателя (единственного) по строке идентификатора ключа ЭП;
- **Subject** - поиск сертификатов получателей (одного или нескольких) по строке имени владельца сертификата;
- **Hash** - поиск сертификата получателя (единственного) по хэш-значению пары ( Имя издателя сертификата ; Серийный номер сертификата ) в шестнадцатеричном представлении, где байты разделены двоеточием;
- **Mail** - поиск сертификатов получателей (одного или нескольких) по строке адреса электронной почты альтернативного имени владельца сертификата.

### 3 ОПИСАНИЕ ОШИБОЧНЫХ СИТУАЦИЙ

Ниже (Таблица 1) приведено описание возможных ошибочных ситуаций. В левой колонке указано символьное имя ошибки и шестнадцатеричное значение ее кода, в правой колонке приведено детальное описание и причина возникновения ошибки.

Таблица 1 – Описание ошибочных ситуаций

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_OK (0x00000000)	Успешное завершение функции
VCERT_E_GENERIC (0xE0700001)	Общая (внутренняя) ошибка библиотеки. Указывает на возможную ошибку в самой библиотеке или на искажения в ее настройках
VCERT_E_INVALID_PARAMETER (0xE0700002)	В функцию был передан неверный параметр. Возникает в случае передачи нулевого указателя, неверно заполненной структуры объекта системы управления сертификатами (СУС) или параметров или при неверном размере блока памяти
VCERT_E_INVALID_CONTEXT (0xE0700003)	Неверный контекст библиотеки, потоковой или другой операции. Вероятно, искажены настройки профиля пользователя или обнаружена ошибка в синтаксисе конфигурационного файла <b>pkil.conf</b>
VCERT_E_OPERATION_NOT_SUPPORTED (0xE0700004)	Операция (или функция) не поддерживается. Выполнен вызов функции или операции, не поддерживаемой библиотекой или не разрешенной для контекста библиотеки
VCERT_E_INVALID_FLAG (0xE0700005)	В функцию был передан неверный флаг. В параметре или в структуре параметров функции указана неверная маска (побитовое ИЛИ) флагов
VCERT_E_NO_MEMORY (0xE0700006)	Недостаточно оперативной памяти. Вероятно, произведен вызов блочной функции над слишком большим блоком памяти или файлом
VCERT_E_DIGEST (0xE0700007)	Ошибка вычисления хэш-значения. Вероятно, неверен объектный идентификатор (OID) алгоритма хэширования
VCERT_E_CERT_USAGE (0xE0700008)	Неверное использование сертификата. В рабочем сертификате отсутствует требуемое разрешенное использование ключа проверки ЭП/открытого ключа шифрования, регламент или расширенное использование ключа проверки ЭП/открытого ключа шифрования
VCERT_E_CERT_FIND_PRIVATE_KEY (0xE0700009)	Не найден ключ ЭП, соответствующий данному сертификату. Отсутствует ключевой носитель с требуемым ключом ЭП, неверен ПИН-код устройства типа смарт-карта или неверен пароль ключа ЭП
VCERT_E_CMS_ADD_SIGNATURE (0xE070000C)	Ошибка добавления ЭП к сообщению в формате CMS/PKCS#7. Вероятно, что недостаточно ресурсов для выполнения операции, произошел сбой аппаратного датчика случайных чисел (ДСЧ) или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_CMS_ASN1_DECODE (0xE070000F)	Ошибка выполнения ASN.1-распаковки сообщения в формате CMS/PKCS#7. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_CMS_ASN1_ENCODE (0xE0700010)	Ошибка выполнения ASN.1-упаковки сообщения в формате CMS/PKCS#7. Вероятно, возникла нехватка ресурсов для выполнения операции
VCERT_E_SIGN_HASH (0xE0700012)	Ошибка вычисления ЭП хэш-значения. Вероятно, неверна длина хэш-значения, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_VERIFY_POLICY (0xE0700013)	Ошибка добавления регламента в контекст проверки сертификата. Вероятно, объектный идентификатор (OID) регламента неверен
VCERT_E_VERIFY_EXTKEYUSAGE (0xE0700014)	Ошибка добавления расширенного использования ключа в контекст проверки сертификата. Вероятно, объектный идентификатор (OID) расширенного использования ключа проверки ЭП/открытого ключа шифрования неверен
VCERT_E_OVERFLOW (0xE0700016)	Ошибка переполнения - либо данные слишком велики, либо буфер слишком мал. Вероятно, произведен вызов блочной функции над слишком большим блоком памяти или файлом
VCERT_E_PKCS10_DAMAGED (0xE0700017)	PKCS#10 запрос на сертификат поврежден или искажен
VCERT_E_REVREQ_DAMAGED (0xE0700018)	Запрос на аннулирование сертификата поврежден или искажен
VCERT_E_VERIFY (0xE0700019)	Общая ошибка проверки ЭП CMS/PKCS#7 сообщения. Возникла ошибка при проверке хотя бы одной ЭП CMS-сообщения
VCERT_E_CMS_INVALID_TYPE (0xE0700022)	Неверный тип содержимого сообщения в формате CMS/PKCS#7. Вероятно, в функцию проверки ЭП передано зашифрованное CMS-сообщение или наоборот
VCERT_E_CMS_NO_RECIPIENTS (0xE0700024)	Отсутствуют или неверны данные сертификатов получателей зашифрованного сообщения в формате CMS/PKCS#7. CMS-сообщение повреждено или искажено

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_E_CMS_NOT_RECIPIENT (0xE0700026)	Владелец сертификата не является получателем зашифрованного сообщения в формате CMS/PKCS#7. Идентификатор рабочего сертификата отсутствует в списке получателей зашифрованного CMS-сообщения
VCERT_E_CMS_KEY_DECRYPT (0xE0700027)	Ошибка расшифрования сеансового ключа зашифрованного CMS/PKCS#7 сообщения. Вероятно, CMS-сообщение повреждено или искажено, или нет доступа к ФКН vdToken с неизвлекаемым закрытым ключом шифрования
VCERT_E_DATA_DECRYPT (0xE0700028)	Ошибка расшифрования блока данных. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_RANDOM (0xE0700029)	Ошибка генерации случайного числа. Вероятно, произошел сбой аппаратного ДСЧ
VCERT_E_OPEN_CONFIG (0xE071002A)	Ошибка доступа к конфигурационному файлу <b>pkil.conf</b> . В текущем рабочем каталоге процесса не найден конфигурационный файл <b>pkil.conf</b>
VCERT_E_READ_CONFIG (0xE071002B)	Ошибка разбора конфигурационного файла <b>pkil.conf</b> . Обнаружена ошибка в формате конфигурационного файла <b>pkil.conf</b>
VCERT_E_NO_DEFAULT_CONFIG (0xE071002C)	Профиль по умолчанию не указан в конфигурационном файле <b>pkil.conf</b> . Вероятно, была произведена попытка инициализации контекста библиотеки с профилем по умолчанию
VCERT_E_OPEN_PSTORE (0xE070002D)	Ошибка доступа к ПСП или к подписанному справочнику. Вероятно, путь (URI) к ПСП или подписанному справочнику неверен
VCERT_E_OPEN_LOCALSTORE (0xE070002E)	Ошибка доступа к ЛСП. Вероятно, путь (URI) к ЛСП неверен
VCERT_E_VERIFY_STORE_USAGE (0xE070002F)	Подписанный справочник имеет неверный идентификатор использования. Вероятно, произведена попытка использовать подписанное обновление от Центра сертификации (ЦС) или Центра регистрации (ЦР) вместо ПСП или наоборот
VCERT_E_VERIFY_STORE (0xE0700030)	Ошибка проверки целостности ПСП или подписанного справочника. Вероятно, произошла ошибка построения или проверки цепочки сертификата подписанта или подписанный справочник поврежден или искажен
VCERT_E_OPEN_LDAPSTORE (0xE0700031)	Ошибка доступа к ССС. Вероятно, путь (URI) к ССС неверен, отсутствует сетевое подключение к ССС или доступ к ССС запрещен из-за отсутствия билета Kerberos
VCERT_E_VERIFY_CERT (0xE0700034)	Ошибка построения и проверки цепочки сертификата. Вероятно, срок действия рабочего сертификата или ключа ЭП истек, не найдены сертификат ЦС или САС, необходимые для построения цепочки, или срок действия САС истек
VCERT_E_CERT_MISSING (0xE0700035)	Сертификат издателя не был найден в доступных справочниках. В доступных справочниках отсутствует сертификат ЦС, необходимый для построения цепочки, при этом не разрешен или отсутствует доступ к точкам AIA
VCERT_E_CERT_EXPIRED (0xE0700036)	Срок действия сертификата уже истек
VCERT_E_CERT_DAMAGED (0xE0700037)	Сертификат поврежден или искажен
VCERT_E_CERT_BROKEN - CONSTRAINT (0xE0700038)	Нарушены базовые ограничения цепочки сертификата
VCERT_E_CERT_REVOKED (0xE0700039)	Сертификат был аннулирован издателем
VCERT_E_CERT_UNTRUSTED (0xE070003A)	Цепочка сертификации не оканчивается доверенным сертификатом. В ПСП отсутствует необходимый сертификат корневого ЦС
VCERT_E_CRL_MISSING (0xE070003B)	САС издателя не был найден в доступных справочниках. В доступных справочниках отсутствует САС, необходимый для построения цепочки, при этом не разрешен или отсутствует доступ к точкам CDP
VCERT_E_CRL_EXPIRED (0xE070003C)	Срок действия САС уже истек
VCERT_E_CRL_DAMAGED (0xE070003D)	САС поврежден или искажен
VCERT_E_CERT_BROKEN - HIERARCHY (0xE070003E)	Нарушено ограничение иерархии цепочки сертификата
VCERT_E_CHAIN_ERROR (0xE070003F)	Общая ошибка построения и проверки цепочки сертификата. Вероятно, цепочка слишком длинная
VCERT_E_INVALID_USAGE (0xE0700041)	Ошибка использования сертификата не по назначению. В проверяемом сертификате отсутствует требуемое разрешенное использование ключа проверки ЭП/открытого ключа шифрования, регламент или расширенное использование ключа проверки ЭП/открытого ключа шифрования

## BAMБ.00077-06 92 02

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_E_INVALID_SIGNATURE (0xE0700042)	ЭП недостоверна. Проверяемые данные повреждены или искажены, или неверен ключ проверки ЭП, который был использован для проверки ЭП
VCERT_E_PUBKEY_NOT_FOUND (0xE0700043)	У сертификата неизвестный ключ проверки ЭП/открытый ключ шифрования. Вероятно, неверен алгоритм ключа проверки ЭП/открытого ключа шифрования сертификата
VCERT_E_UPDATECRL (0xE0700045)	Общая ошибка обновления САС. Вероятно, при критичном обновлении одного из САС, находящихся в ЛСП, произошла ошибка
VCERT_E_CERT_NOT_FOUND (0xE0700046)	Сертификат не был найден в доступных справочниках. При поиске в доступных справочниках не был найден ни один сертификат, удовлетворяющий заданному шаблону
VCERT_E_CERT_NOT_YET_VALID (0xE0700047)	Срок действия сертификата еще не наступил
VCERT_E_NO_ATTACHED_SIGNER (0xE070004A)	Сертификат подписанта отсутствует в сообщении в формате CMS/PKCS#7. Вероятно, был установлен флаг проверки ЭП <b>FLAG_CMS_VERIFY_REQUIREATTACHEDSIGNER</b>
VCERT_E_KERBEROS_FAILURE (0xE070004B)	Ошибка получения или обновления билета Kerberos. Вероятно, нет доступа к Центру распределения ключей (Key Distribution Center, KDC) или имя пользователя и пароль неверны
VCERT_E_KEY_EXPIRED (0xE070004C)	Ключ ЭП/закрытый ключ шифрования уже истек
VCERT_E_KEY_NOT_YET_VALID (0xE070004D)	Ключ ЭП/закрытый ключ шифрования еще недействителен
VCERT_E_CRL_NOT_YET_VALID (0xE070004E)	Срок действия САС еще не наступил
VCERT_E_INIT_CSP (0xE070004F)	Ошибка выполнения инициализации Средства КЗИ. Вероятно, Средство КЗИ не установлено, или его конфигурация искажена
VCERT_E_ENUM_OBJECTS (0xE0700050)	Ошибка доступа к справочнику при переборе объектов. Вероятно, путь (URI) к справочнику неверен, или отсутствует подключение к справочнику по сети
VCERT_E_ENUM_NO_MORE (0xE0700051)	В справочнике больше нет объектов для перебора. Перебор справочника завершен, все объекты были успешно считаны
VCERT_E_INVALID_X500_NAME (0xE0700052)	Текстовая строка, содержащая X.500-имя, имеет неверное представление. Вероятно, строка с X.500-именем искажена или содержит неверный RDN
VCERT_E_INVALID_HEX_STRING (0xE0700053)	Текстовая строка, содержащая шестнадцатеричное число, имеет неверное представление. Текстовая строка с шестнадцатеричным числом должна иметь вид 00:01:0E:0F
VCERT_E_CMS_STREAM_MISMATCH (0xE0700054)	Обнаружено несоответствие между потоковым признаком обрабатываемых данных и вызванной функцией. Вероятно, произошла попытка вызова блочной функции для обработки CMS-сообщения, имеющего ASN.1 кодировку неопределенной длины, или наоборот
VCERT_E_CMS_DETACH_MISMATCH (0xE0700055)	Обнаружено несоответствие между признаком отсоединенной ЭП обрабатываемых данных и вызванной функцией. Вероятно, произошла попытка вызова функции, предназначенной для обработки CMS-сообщений с присоединенными ЭП, для обработки CMS-сообщения с отсоединенными ЭП, или наоборот
VCERT_E_CMS_INVALID_DIGESTS (0xE0700056)	Отсутствуют или неверны данные алгоритмов хэширования подписанного сообщения в формате CMS/PKCS#7. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_CMS_INVALID_SIGNERS (0xE0700057)	Отсутствуют или неверны данные сертификатов подписантов подписанного сообщения в формате CMS/PKCS#7. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_CMS_INVALID_CIPHER (0xE0700058)	Зашифрованное сообщение в формате CMS/PKCS#7 содержит неизвестный или неверный алгоритм шифрования. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_CMS_DATA_SIGNING (0xE0700059)	Ошибка вычисления ЭП подписанного сообщения в формате CMS/PKCS#7. Вероятно, что недостаточно ресурсов для выполнения операции, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_CMS_OMAC_MISMATCH (0xE070005A)	Имитовставка зашифрованного сообщения в формате CMS/PKCS#7 не совпадает с вычисленной. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_FIND_SESSION (0xE0700081)	Требуемая сессия криптосервера не была найдена. В функцию библиотеки был передан идентификатор несуществующей сессии КС
VCERT_E_CMS_NOT_ENCRYPTED (0xE0700083)	CMS/PKCS#7-сообщение не зашифровано или формат сообщения поврежден или искажен. Вероятно, CMS-сообщение повреждено или искажено
VCERT_E_ADD_OBJECT (0xE0700087)	Ошибка добавления объекта в справочник сертификатов. Вероятно, такой объект уже существует или добавление объекта в ССС запрещено



## ВАНБ.00077-06 92 02

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_E_TOO_MANY_CERTS_FOUND (0xE0720089)	Слишком много сертификатов найдено по уникальному критерию поиска. Вероятно, несколько сертификатов содержат один и тот же идентификатор ключа ЭП
VCERT_E_USER_CANCEL (0xE072008A)	Операция была отменена пользователем
VCERT_E_OPEN_INFILE (0xE070008B)	Ошибка открытия входного файла. Вероятно, путь или имя файла неверны или доступ к файлу запрещен
VCERT_E_OPEN_OUTFILE (0xE070008C)	Ошибка открытия выходного файла. Вероятно, путь или имя файла неверны или доступ к файлу запрещен
VCERT_E_READ_FILE (0xE070008D)	Ошибка чтения из входного файла. Вероятно, произошло искажение файловой системы
VCERT_E_WRITE_FILE (0xE070008E)	Ошибка записи в выходной файл. Вероятно, на файловой системе закончилось свободное пространство
VCERT_E_FILE_LENGTH (0xE070008F)	Неверный размер файла (нулевой или более 2Гб)
VCERT_E_DELETE_OBJECT (0xE0700091)	Ошибка удаления объекта из справочника сертификатов. Указанный объект не был удален из кэша контекста библиотеки или сессии КС или из ЛСП сессии КС по команде с АРМ УКС
VCERT_E_TOO_FEW_SIGNATURES (0xE0700092)	Подписанный документ содержит недостаточное количество ЭП. Вероятно, были установлены флаги проверки ЭП <b>FLAG_CMS_VERIFY_DELETESIGNATURES</b> или <b>FLAG_CMS_VERIFY_MINIMUMSIGNATURES</b> , или индекс ЭП для операции со штампом времени слишком велик
VCERT_E_GET_PUBKEY (0xE0700094)	Ошибка получения ключа проверки ЭП/открытого ключа шифрования сертификата. Вероятно, возникла нехватка ресурсов или неверен алгоритм ключа проверки ЭП/открытого ключа шифрования сертификата
VCERT_E_PKCS10_CREATE (0xE0700098)	Ошибка создания нового PKCS#10 запроса. Вероятно, произошла ошибка при генерации или записи ключа ЭП на ключевой носитель или XML шаблон имеет неверный формат
VCERT_E_PKCS10_SIGN (0xE070009A)	Ошибка вычисления ЭП PKCS#10 запроса. Вероятно, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_REVREQ_CREATE (0xE070009B)	Ошибка создания нового запроса на аннулирование. Вероятно, возникла нехватка ресурсов
VCERT_E_REVREQ_SIGN (0xE070009C)	Ошибка вычисления ЭП запроса на аннулирование. Вероятно, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_LOAD_PRIVATE_KEY (0xE070009D)	Ошибка загрузки ключа ЭП/закрытого ключа шифрования. Отсутствует ключевой носитель с требуемым ключом ЭП/закрытым ключом шифрования, неверен ПИН-код устройства типа смарт-карта или неверен пароль ключа ЭП/закрытого ключа шифрования
VCERT_E_ADD_SIGNER (0xE070009E)	Ошибка добавления ЭП к ЛСП или к подписанному справочнику. Вероятно, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_OPEN_IDP (0xE07000A1)	Ошибка доступа к точке распространения САС. Вероятно, к точке CDP запрещен доступ или в точке CDP отсутствует требуемый САС
VCERT_E_READ_IDP (0xE07000A2)	Ошибка чтения из точки распространения САС. Вероятно, возникла проблема с сетевым подключением или в точке CDP отсутствует требуемый САС
VCERT_E_INVALID_CREDENTIALS (0xE02000A8)	Ошибочные данные аутентификации при доступе к сессии криптосервера. Вероятно, длина данных аутентификации равна 0
VCERT_E_ACCESS_DENIED (0xE02000A9)	Доступ к сессии криптосервера запрещен. Вероятно, данные аутентификации неверны
VCERT_E_SESSION_BLOCKED (0xA02000AA)	Сессия криптосервера заблокирована
VCERT_E_CLIENT_INFO (0xE02000AB)	Ошибка получения информации о клиенте из протокола DCE-RPC. Вероятно, произошла системная ошибка библиотеки DCE-RPC при получении сетевого адреса клиента
VCERT_E_UNSECURE_CREDENTIALS (0xE02000AC)	Небезопасные (слишком короткие) данные аутентификации сессии криптосервера. Длина данных аутентификации должна быть не менее 8 символов
VCERT_E_SESSION_TIMEOUT (0xA07000AE)	Истек интервал ожидания доступа к сессии КС из-за того, что данная сессия КС в настоящий момент заблокирована и не готова обрабатывать поступающие запросы. Данная ошибка может возникнуть, только если для данной сессии КС настроен ненулевой интервал ожидания доступа

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_E_TSP_HASH_LENGTH (0xE0700100)	Неверная длина хэш-значения при создании запроса на штамп времени. Длина хэш-значения не соответствует указанному алгоритму хэширования
VCERT_E_TSP_HASH_ALGORITHM (0xE0700101)	Неверный алгоритм хэширования при создании запроса на штамп времени. Объектный идентификатор (OID) алгоритма хэширования неверен
VCERT_E_TSP_CERT_PURPOSE (0xE0700102)	Сертификат не может быть использован для подписи штампов времени. Сертификат не удовлетворяет условиям использования на сервере штампов времени
VCERT_E_TSP_SIGN_FAILED (0xE0700103)	Ошибка вычисления ЭП штампа времени. Вероятно, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_TSP_NO_DIGEST (0xE0700104)	В списке атрибутов отсутствует хэш-значение ЭП и/или данных. Вероятно, штамп времени поврежден или искажен
VCERT_E_TSP_INVALID_SIGNER_NUM (0xE0700105)	Штамп времени содержит неверное количество ЭП. Вероятно, штамп времени поврежден или искажен
VCERT_E_TSP_NO_TST_INFO (0xE0700106)	Ошибка при получении информационного блока штампа времени. Вероятно, штамп времени поврежден или искажен
VCERT_E_TSP_RESP_ASN1_DECODE (0xE0700107)	Ошибка выполнения ASN.1-распаковки подписанного штампа времени. Вероятно, штамп времени поврежден или искажен
VCERT_E_TSP_RESP_NOT_ISSUED (0xE0700108)	Штамп времени не был выдан авторитетным источником. Вероятно, произошла внутренняя ошибка сервера штампов времени
VCERT_E_TSP_DIGEST_MISMATCH (0xE0700109)	Штамп времени содержит хэш-значение, отличное от хэш-значения ЭП CMS/PKCS#7 сообщения. Вероятно, штамп времени поврежден или искажен
VCERT_E_OCSP_CERT_PURPOSE (0xE0700140)	Сертификат не может быть использован для вычисления ЭП ответов сетевого ответчика. Сертификат не удовлетворяет условиям использования на сервере OCSP ответчика
VCERT_E_OCSP_SIGN_FAILED (0xE0700141)	Ошибка вычисления ЭП ответа сетевого ответчика. Вероятно, произошел сбой аппаратного ДСЧ или нет доступа к ФКН vdToken с неизвлекаемым ключом ЭП
VCERT_E_OCSP_RESP_ASN1_DECODE (0xE0700142)	Ошибка выполнения ASN.1-распаковки подписанного ответа сетевого ответчика. Вероятно, ответ сервера OCSP ответчика поврежден или искажен
VCERT_E_OCSP_RESP_NOT_ISSUED (0xE0700143)	Подписанный ответ не был выдан сетевым ответчиком. Вероятно, произошла внутренняя ошибка сервера OCSP ответчика
VCERT_E_OCSP_NOT_BASICRESP (0xE0700144)	Неверный (небазовый) тип подписанного ответа сетевого ответчика. Вероятно, ответ сервера OCSP ответчика содержит статус более чем для одного сертификата
VCERT_E_OCSP_CERTID_MISMATCH (0xE0700145)	Идентификатор сертификата из подписанного ответа сетевого ответчика не соответствует запрашиваемому. Вероятно, ответ сервера OCSP ответчика поврежден или искажен
VCERT_E_OCSP_ISSUER_MISMATCH (0xE0700146)	Издатель сертификата сетевого ответчика не соответствует издателю проверяемого сертификата. Вероятно, ответ сервера OCSP ответчика поврежден или искажен
VCERT_E_TLS_UNSUPPORTED (0xE0700180)	Функции протокола TLS не могут быть использованы с данным контекстом библиотеки. Вероятно, произведена попытка использования функций протокола TLS с минимальным контекстом библиотеки
VCERT_E_TLS_NEW_CONTEXT (0xE0700181)	Ошибка создания контекста нового сеанса связи протокола TLS. Вероятно, возникла нехватка ресурсов, произошел сбой аппаратного ДСЧ или использован контекст проверки библиотеки
VCERT_E_TLS_INVALID_STATE (0xE0700182)	Контекст сеанса связи протокола TLS находится в неверном состоянии. Вероятно, произведена попытка обмена данными между клиентом и сервером, когда защищенный канал еще не сформирован
VCERT_E_TLS_HANDSHAKE (0xE0700183)	Ошибка выполнения переговоров при формировании нового сеанса связи протокола TLS. Клиент и сервер не смогли сформировать защищенный канал, вероятно из-за отсутствия общих наборов криптографических алгоритмов
VCERT_E_TLS_NOT_COMPLETE (0xE0700184)	Переговоры при формировании нового сеанса связи протокола TLS еще не завершены
VCERT_E_TLS_NO_QUERY_DATA (0xE0700185)	Запрашиваемые данные в контексте сеанса связи протокола TLS отсутствуют. Вероятно, на сервере был выполнен запрос на получение сертификата клиента в DER-кодировке при выполнении односторонней аутентификации
VCERT_E_TLS_WRONG_CERT (0xE0700186)	Сертификат противоположной стороны сеанса связи TLS протокола неверен или искажен
VCERT_E_TLS_WRONG_NAME (0xE0700187)	Сертификат противоположной стороны сеанса связи TLS протокола имеет неверное имя. Вероятно, сертификат сервера имеет в дополнении "Альтернативное имя владельца" DNS-имя отличное от того, которое указал клиент

Имя и код ошибки	Описание и причина возникновения ошибки
VCERT_E_TLS_WRITE_ERROR (0xE0700188)	Ошибка при записи данных сеанса связи протокола TLS. Вероятно, возникла нехватка ресурсов или данные TLS протокола искажены
VCERT_E_TLS_READ_ERROR (0xE0700189)	Ошибка при чтении данных сеанса связи протокола TLS. Вероятно, данные TLS протокола искажены
VCERT_E_TLS_READ_MORE (0xE0700190)	Следует продолжить чтение данных сеанса связи протокола TLS. Вероятно, необходимо продолжить переговоры для завершения создания защищенного канала
ERR_PROFILES_BAD_PARAM (0xE0D50001)	При вызове какой-либо функции библиотеки ей передан параметр с недопустимым значением - скорее всего нулевой указатель
ERR_PROFILES_BUFFER_SIZE (0xE0D50002)	При работе со строками (копирование, чтение из реестра и пр.) размер выделенного буфера недостаточен для размещения строки
ERR_PROFILES_NO_MEMORY (0xE0D50003)	Ошибка выделения памяти - либо произошло исчерпание памяти системы, либо при выделении памяти запрошен неадекватный размер
ERR_PROFILES_GET_INSTANCE (0xE0D50004)	Не инициализирована переменная CRYPTO_hinstance, содержащая HINSTANCE исполняемого модуля, содержащего ресурсы
ERR_PROFILES_CREATE_DLG (0xE0D50005)	Ошибка инициализации модального диалога - скорее всего испорчены ресурсы или неправильно инициализирована переменная CRYPTO_hinstance, содержащая HINSTANCE исполняемого модуля, содержащего ресурсы
ERR_PROFILES_GET_DLG_ITEM (0xE0D50006)	Ошибка доступа к элементам управления (кнопка, поле редактирования, список и т.д.) модального диалога - скорее всего испорчены ресурсы
ERR_PROFILES_GET_USER_DIR (0xE0D50007)	Ошибка при вызове функции SHGetFolderPath() библиотеки shell32.dll, возвращающей каталог пользователя по умолчанию - скорее всего проблемы с файловой системой
ERR_PROFILES_GET_WND_RECT (0xE0D50008)	Ошибка функции GetWindowRect() получающей координаты окна. Глобальные проблемы системы
ERR_PROFILES_SET_WND_POS (0xE0D50009)	Ошибка функции SetWindowPos() устанавливающей положение окна. Глобальные проблемы системы
ERR_PROFILES_CLN_TO_SCR (0xE0D5000A)	Ошибка функции ScreenToClient() приводящей экранные координаты окна к клиентским. Глобальные проблемы системы
ERR_PROFILES_USER_CANCEL (0xE0D5000B)	Пользователь нажал кнопку "Отмена" или клавишу ESC
ERR_PROFILES_NO_REG_KEY (0xE0D5000C)	Отсутствует ключ реестра
ERR_PROFILES_DONT_OPEN_- REG_KEY (0xE0D5000D)	Ошибка открытия ключа реестра
ERR_PROFILES_DONT_CREATE_- REG_KEY (0xE0D5000E)	Ошибка создания ключа реестра
ERR_PROFILES_ACCESS_DENY_- REG_KEY (0xE0D5000F)	Недостаточно прав для создания ключа в реестре
ERR_PROFILES_DONT_DEL_- REG_KEY (0xE0D50010)	Ошибка удаления ключа реестра
ERR_PROFILES_AC_DENY_DEL_- REG_KEY (0xE0D50011)	Недостаточно прав для удаления ключа в реестре
ERR_PROFILES_NO_REG_VAL (0xE0D50012)	Отсутствует значение в реестре
ERR_PROFILES_DONT_READ_- REG_VAL (0xE0D50013)	Ошибка чтения значения в реестре
ERR_PROFILES_DONT_WRITE_- REG_VAL (0xE0D50014)	Ошибка записи значения в реестр
ERR_PROFILES_ACCESS_DENY_- REG_VAL (0xE0D50015)	Недостаточно прав для записи значения в реестр
ERR_PROFILES_BAD_TYPE_- REG_VAL (0xE0D50016)	Неправильный тип значения в реестре
ERR_PROFILES_DONT_ENUM_- REG_VAL (0xE0D50017)	Ошибка перечисления значений в ключе реестра

## ВАМБ.00077-06 92 02

Имя и код ошибки	Описание и причина возникновения ошибки
ERR_PROFILES_NO_PROFILE (0xE0D50018)	При попытке выбора профиля (не в режиме редактирования) в реестре не обнаружено ни одного профиля либо при записи информации о профилях в реестр не было сформировано ни одного профиля
ERR_PROFILES_BAD_CONFIG (0xE0D50019)	Либо в реестре содержится неадекватное (меньше 2) значение параметра "count" обозначающего количество хранилищ для профиля. Либо в конфигурационном файле профиля (cfg.ini) в разделе [ODBC] не задан или задан пустой параметр local.gdbm при параметре local.gdbm_type равном 2
ERR_PROFILES_PROFILE_NOT_FOUND (0xE0D5001A)	Не найден профиль с заданным именем
ERR_PROFILES_PROF_ALREADY_EXISTS (0xE0D5001B)	При попытке добавления нового профиля без флага, разрешающего перезапись, обнаружено, что профиль с таким именем уже есть
ERR_PROFILES_BAD_PROF_INDEX (0xE0D5001C)	Не найден профиль с заданным номером
ERR_PROFILES_FILE_INSTEAD_DIR (0xE0D5001D)	При попытке создания директории (каталога) для хранения профиля обнаружено, что существует файл с таким именем
ERR_PROFILES_AC_DENY_CREATE_DIR (0xE0D5001E)	Недостаточно прав для создания директории (каталога)
ERR_PROFILES_CREATE_DIR_NO_PARENT (0xE0D5001F)	Попытка создать поддиректорию (подкаталог) отсутствующей директории (каталога)
ERR_PROFILES_CREATE_DIR_NO_ROOT (0xE0D50020)	Попытка создать поддиректорию (подкаталог) при отсутствии корня (например, диска)
ERR_PROFILES_DONT_CREATE_DIR (0xE0D50021)	Ошибка создания директории (каталога), не относящаяся к вышеперечисленным
ERR_PROFILES_ODBC (0xE0D50022)	Ошибка вызова функций SQLAllocHandle(), или SQLSetEnvAttr(), или SQLDriverConnect() библиотеки odbc32.dll. Проблемы библиотеки ODBC
ERR_PROFILES_BAD_LDAP_STRING (0xE0D50023)	Ошибка разбора строки LDAP-соединения
ERR_PROFILES_OPEN_MY_STORE (0xE0D50024)	Ошибка функции CertOpenStore() библиотеки Crypt32.dll, открывающей хранилище личных сертификатов
ERR_PROFILES_ENUM_MY_CERTS (0xE0D50025)	Ошибка функции CertEnumCertificatesInStore() библиотеки Crypt32.dll перечисляющей сертификаты из хранилища личных
ERR_PROFILES_GET_CERT_SUBJECT (0xE0D50026)	Ошибка функции CertNameToStr() Crypt32.dll, получающей имя владельца сертификата. Возможно, испорчен сертификат
ERR_PROFILES_NO_MY_CERTS (0xE0D50027)	Не найдено ни одного сертификата в хранилище личных сертификатов
ERR_PROFILES_FILETIME_TO_SYSTIME (0xE0D50028)	Ошибка функции FileTimeToLocalFileTime() или ф-ии FileTimeToSystemTime() библиотеки Kernel32.dll. Возможно, в сертификате указано неадекватное время
ERR_PROFILES_NO_SUBJ_KEY_ID (0xE0D50029)	В сертификате не найдено расширение 'Идентификатор ключа владельца'
ERR_PROFILES_DECODE_OBJECT (0xE0D5002A)	Ошибка функции CryptDecodeObject(), декодирующей объект в ASN1 кодировке. Возможно, испорчен сертификат
ERR_PROFILES_FIND_CERT_BY_KEYID (0xE0D5002B)	Ошибка поиска сертификата ф-ией CertFindCertificateInStore() с параметром CERT_FIND_CERT_ID по идентификатору ключа владельца. Возможно, сертификат отсутствует
ERR_PROFILES_SHOW_CERT (0xE0D5002C)	Ошибка функции CryptUIDlgViewContext(), отображающей сертификат

## **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ**

ДСЧ	Датчик случайных чисел
КЗИ	Криптографическая защита информации
ЛСП	Локальный справочник пользователя (Local Certificate Store)
ОС	Операционная система (Operating System)
ПК	Программный комплекс
ПСП	Персональный справочник пользователя (Personal Security Environment)
САС	Список аннулированных сертификатов (Certificate Revocation List)
ССС	Сетевой справочник сертификатов (Network Certificate Store)
ЦР	Центр регистрации
ЦС	Центр сертификации
ЭП	Электронная подпись (Digital Signature)

**ПЕРЕЧЕНЬ ТАБЛИЦ**

1	Описание ошибочных ситуаций . . . . .	14
---	---------------------------------------	----

[illegible][illegible]