

# ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ



## Общие принципы проверки соответствия средств ЭП и УЦ требованиям приказов ФСБ России №№ 795 и 796

Камышев Сергей Николаевич  
Евдокимов Алексей Юрьевич

## Федеральный орган исполнительной власти в области обеспечения безопасности

Устанавливает требования к форме квалифицированного сертификата

Устанавливает требования к средствам электронной подписи и средствам удостоверяющего центра

Осуществляет подтверждение соответствия средств ЭП и средств УЦ требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи», и публикует перечень таких средств

## Порядок подтверждения соответствия

Федеральный закон «Об электронной подписи» не установил обязанность ФСБ России по определению порядка подтверждения соответствия средств ЭП и средств УЦ требованиям, установленным в соответствии с указанным Федеральным законом

Подтверждение соответствия шифровальных (криптографических) средств осуществляется на этапе их разработки в соответствии с требованиями и порядком, установленным Положением ПКЗ-2005

К средствам ЭП и средствам УЦ предъявляются требования, закрепленные Положением ПКЗ-2005 для шифровальных (криптографических) средств (п.6 приложений № 1,2 Приказа ФСБ России № 796)

## Стадии подтверждения соответствия средств УЦ

Согласование заказчиком средств УЦ с ФСБ России ТТЗ (ТЗ) по созданию (модернизации) средств УЦ

Согласование заказчиком средств УЦ с ФСБ России модели угроз и нарушителя информационной безопасности средств УЦ. Принимается либо базовая модель из Требований, либо разрабатывается конкретизированная модель. На основе модели определяется класс средств УЦ

Согласование разработчиком средств УЦ с ФСБ России эксплуатационной документации на средства УЦ

Согласование специализированной организацией с ФСБ России программы и методики проведения тематических исследований

# Проведение специализированной организацией тематических исследований средств УЦ

## Проведение ФСБ России экспертизы результатов тематических исследований средств УЦ

### Оформление сертификата соответствия ФСБ России на средство УЦ по определенному классу защиты с опубликованием сведений о выданном сертификате в сети Интернет ([www.clsz.fsb.ru](http://www.clsz.fsb.ru))

 КОДЕКС

**ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Система сертификации РОСС RU.0001.030001

**СЕРТИФИКАТ СООТВЕТСТВИЯ**

Регистрационный номер **СФ/128-1824** от **01** июня 2012 г.  
Действителен до **31** декабря 2014 г.

Выдан федеральному государственному автономному научному учреждению «Центр информационных технологий в системе органов исполнительной власти».

Настоящий сертификат удостоверяет, что изделие «Корпоративный удостоверяющий центр «ИнтерФид» в составе согласно формуляру ИТВБ.422790.021ФДО

соответствует Требованиям к средствам удостоверяющего центра, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для классов КСЗ, и Требованиям к форме идентификационного сертификата и листа протока электронной подписи, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 795, и может использоваться для реализации функций удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Сертификат выдан на основании результатов проведенных Международным центром по информации и электронике (InterNET) № 679-001001 сертификационных испытаний образца продукции

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями нормативных документов, формуляра ИТВБ.422790.021ФДО и при условии наличия действующего сертификата соответствия ФСБ России на средства защиты информации, входящие в состав изделия.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России  А.М.Ивашко



Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.  
Защищен ключом шифрования по алгоритму ГОСТ Р 34.11-2012

 КОДЕКС

**ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Система сертификации РОСС RU.0001.030001

**СЕРТИФИКАТ СООТВЕТСТВИЯ**

Регистрационный номер **СФ/128-2175** от **20** июня 2012 г.  
Действителен до **20** июня 2016 г.

Выдан закрытому акционерному обществу Научно-Инженерное Предприятие «Информатика».

Настоящий сертификат удостоверяет, что изделие «Программно-аппаратный комплекс «Юнисер» ГОСТ», Версия 2.1» в составе согласно формуляру RU.40308570.501430.004.ФДО

соответствует Требованиям к средствам удостоверяющего центра, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для классов КСЗ, и Требованиям к форме идентификационного сертификата и листа протока электронной подписи, утвержденными приказом ФСБ России от 27 декабря 2011 г. № 795, и может использоваться для реализации функций удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Сертификат выдан на основании результатов проведенных Закрытым акционерным обществом «ИНИТ» № 400А-001005 сертификационных испытаний образца продукции

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями нормативных документов, формуляра RU.40308570.501430.004.ФДО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России  А.М.Ивашко



Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.  
Защищен ключом шифрования по алгоритму ГОСТ Р 34.11-2012

## Цели проведения подтверждения соответствия

Проверка выполнения требований приказов ФСБ России № 795,796

Проверка выполнения целевых функций УЦ

Проверка корректности встраивания криптосредств и средств ЭП в ПО УЦ

Оценка механизмов защиты, реализованных в УЦ (идентификация и аутентификация, разграничение доступа, аудит и т.д.)

Проверка корректности реализации внутренних и внешних протоколов работы, используемых УЦ при реализации им целевых функций (TLS, PKCS#10, #7, CMP, CRMF, OCSP и т.д.)

## Проверка соответствия сертификатов «Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи»

Анализ наличия в средствах УЦ механизма,  
позволяющего ввести поля сертификата,  
предусмотренные требованиями

Анализ наличия в средствах УЦ механизма,  
контролирующего или реализующего правильность  
заполнения введенных полей

Анализ документированности в эксплуатационной  
документации на средства УЦ настроек профиля  
сертификата ключа проверки ЭП для реализации  
требований

## Проверка выполнения в средствах УЦ Требований к средствам ЭП по отображению электронного документа

Выделение и анализ всех функций (операций) создания и проверки ЭП при функционировании средств УЦ

Выделение объектов (электронных документов), с которыми данные операции подписи осуществляются

Анализ реализации механизма отображения данных объектов в средствах УЦ при выполнении операций создания или проверки ЭП

Оценка документированности процедуры (порядка) отображения средствами УЦ электронных документов (объектов) при создании или проверке ЭП в ЭД на средства УЦ

## Опыт подтверждения соответствия средств УЦ рекомендует

Необходимо приводить подробную функциональную сетевую (распределенную) схему взаимодействия компонентов УЦ с подробным описанием всех протоколов указанного взаимодействия

При использовании сертифицированных средств УЦ безопасность информации обеспечивается при использовании средств УЦ в соответствии с требованиями нормативных документов указанных в соответствующих сертификатах соответствия

Документирование распределенных сетевых схем взаимодействия компонентов УЦ позволяет однозначно определять необходимость проведения дополнительных тематических исследований при встраивании средств УЦ в конкретные информационные системы

Проверка выполнения п.8 и п.9 «Требований к средствам электронной подписи» для СКЗИ (средств ЭП)  
не проводится в случаях

1. Реализация функций прикладного уровня, осуществляющих в соответствии с системными требованиями автоматическое создание и (или) автоматическую проверку электронных подписей

2. Реализация функций прикладного уровня, осуществляющих неавтоматическое создание и (или) неавтоматическую проверку электронных подписей  
**при одновременном выполнении следующих условий**

1) Средство ЭП используется в среде функционирования, включающей в себя:

- стандартное ПО, входящее в состав ОС семейства Windows, указанных в правилах пользования средств ЭП.
- «Microsoft Office 2007» (SP2) и выше или «Adobe Acrobat Reader версии 8.0» и выше.

2) Содержание информации при формировании и при проверке электронной подписи электронного документа показывается пользователю

3) Электронный документ представлен в форматах ODF (Microsoft Office 2007 (SP2) или выше), XML (Microsoft Internet Explorer версии 6.0 или выше), PDF (Adobe Acrobat Reader версии 8.0 или выше)

В остальных случаях, при встраивании средств ЭП в прикладные системы должна быть проведена проверка выполнения пунктов 8 и 9 раздела II «Требований к средствам электронной подписи»

**Федеральный закон «Об электронной подписи»**

**Сертифицировано 19 средств УЦ**

**Сертифицировано более 25 средств ЭП**

**Государственные органы (Федеральное  
Казначейство, ФНС, ФТС и др.), государственные  
внебюджетные фонды (ПФР, ФСС и др.), а также  
коммерческие организации обеспечены  
сертифицированными средствами**

**Задачи ФСБ России по введению в действие  
Федерального закона  
«Об электронной подписи»  
выполнены в полном объеме**

После завершения сроков действия заключений ФСБ России на средства УЦ данные средства должны подвергаться контрольным тематическим исследованиям.

**ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**



**СПАСИБО ЗА ВНИМАНИЕ**