УТВЕРЖДАЮ	**УТВЕРЖДАЮ**
Временно исполняющий обязанности Руководителя Федеральной службы государственной статистики	Генеральный директор ООО «ИБС Экспертиза»
_____ К.Э. Лайкам	_____ А.В. Соковых
«_____»_____ 2009 г.	«_____»_____ 2009 г.

СОЗДАНИЕ ЭЛЕКТРОННОГО АРХИВА ЭЛЕКТРОННЫХ ВЕРСИЙ ФОРМ СТАТИСТИЧЕСКОЙ ОТЧЕТНОСТИ, ПОЛУЧЕННОЙ ОТ ПРЕДПРИЯТИЙ С ЭЦП, И РАЗВИТИЕ ЕДИНОЙ СИСТЕМЫ СБОРА, ОБРАБОТКИ, ХРАНЕНИЯ И ПРЕДСТАВЛЕНИЯ СТАТИСТИЧЕСКИХ ДАННЫХ (ЕССО) В ЧАСТИ ЭЛЕКТРОННОГО СБОРА ДАННЫХ

ЕДИНАЯ СИСТЕМА СБОРА, ОБРАБОТКИ, ХРАНЕНИЯ И ПРЕДСТАВЛЕНИЯ СТАТИСТИЧЕСКИХ ДАННЫХ

РЕГЛАМЕНТ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В СИСТЕМЕ СБОРА СТАТИСТИЧЕСКОЙ ОТЧЕТНОСТИ РОССТАТА

СОГЛАСОВАНО	**СОГЛАСОВАНО**
ВРИО начальника Управления информационных ресурсов и технологий Росстата	Руководитель проектов ООО «ИБС Экспертиза»
_____ Ю.К. Голованов	_____ Д.Н. Лернер
«_____»_____ 2009 г.	«_____»_____ 2009 г.

2009 г.

АННОТАЦИЯ

В настоящем документе приводится Регламент использования Электронной цифровой подписи в Единой системе сбора, обработки, хранения и представления статистических данных Росстата.

Настоящий Регламент использования Электронной цифровой подписи разработан в рамках проекта «Создание Электронного архива электронных версий форм статистической отчетности, полученной от предприятий с ЭЦП, и развитию Единой системы сбора, обработки, хранения и представления статистических данных (ЕССО) в части электронного сбора данных».

СОДЕРЖАНИЕ

1. Термины и определения 6
2. Общие положения 9
2.1 Назначение документа 9
2.2 Область применения документа 9
2.2.1 Организационные рамки 9
2.2.2 Функциональные рамки 9
2.3 Соответствие требованиям нормативно-правовых актов 10
2.4 Условия признания юридической значимости ЭЦП 11
3. Требования к применению ЭЦП 12
4. Порядок приостановления действия и отзыва сертификата 13
4.1 Отзыв сертификата ключа подписи 13
4.1.1 Условия отзыва сертификата 13
4.1.2 Инициаторы отзыва сертификата 13
4.1.3 Процедура отзыва сертификата 14
4.2 Приостановление действия сертификата ключа подписи 14
4.2.1 Процедура приостановления действия сертификата 15
4.2.2 Процедура возобновления действия приостановленного сертификата 15
5. Порядок предоставления информации о статусах сертификатов 16
5.1 Распространение информации о статусах сертификатов 16
5.2 Издание списка отозванных сертификатов 16
5.3 Получение информации о статусе сертификата в реальном времени 17
6. Правила работы с ЭЦП 19
6.1 Сертификаты ключей подписи 19

6.2 Использование средств ЭЦП 20
6.3 Хранение закрытого ключа ЭЦП 20
6.4 Компрометация ключей..... 21

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Описание
АРМ	Автоматизированное рабочее место
ЕССО	Единая система сбора, обработки, хранения и представления статистических данных
ПО	Программное обеспечение
Росстат	Федеральная служба государственной статистики
СКП	Сертификат ключа подписи
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов
Спецоператор	Специализированный оператор связи
ССО	Система сбора и обработки статистических данных в составе Единой системы сбора, обработки, хранения и представления статистических данных (ЕССО)
ТОГС	Территориальные органы Федеральной службы государственной статистики
УЦ	Удостоверяющий центр
ФСБ России	Федеральная служба безопасности Российской Федерации
ФЗ	Федеральный закон
ЭА	Электронный архив
ЭЦП	Электронная цифровая подпись
AIA	Authority Information Access - точка доступа к информации УЦ
CRDP	Certificate Revocation Distribution Point - точка распространения СОС
CRL	Certificate Revocation List - список отозванных сертификатов
OCSP	Online Certificate Status Protocol - протокол получения статуса сертификата в реальном времени
PKI	Public Key Infrastructure - инфраструктура открытых ключей
RFC	Request For Comment
TSA	Time Stamping Authority - служба штампов времени

1. Термины и определения

Владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи, и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Закрытый ключ ЭЦП – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Инфраструктура открытых ключей (Public Key Infrastructure – PKI) – интегрированный набор служб и средств администрирования для создания и развертывания приложений, использующих криптографию с открытыми ключами; обеспечивает функции управления открытыми ключами.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Открытый ключ ЭЦП – уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная любому Участнику информационной системы и предназначенная для подтверждения с использованием средств ЭЦП подлинности электронной цифровой подписи в электронном документе. Открытый ключ Пользователя является действующим на момент подписания, если он зарегистрирован (сертифицирован), введен в действие и не включен в список отозванных сертификатов (СОС).

Подтверждение подлинности ЭЦП в электронном документе – положительный результат проверки принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутст-

вия искажений в подписанном данной электронной цифровой подписью электронном документе.

Пользователь УЦ – физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.

Проверка ЭЦП – процесс, в котором на основе имеющегося электронного документа и соответствующей ЭЦП, а также заданного алгоритма проверки ЭЦП, определяются корректность, ошибочность (некорректность) или невозможность проверки корректности ЭЦП.

Респондент – юридическое лицо или индивидуальный предприниматель, осуществляющий деятельность без образования юридического лица, представляющий первичные статистические данные в соответствии с действующим законодательством.

Сертификат ключа подписи (СКП, сертификат открытого ключа) – документ на бумажном носителе или электронный документ с ЭЦП уполномоченного должностного лица удостоверяющего центра, включающий в себя открытый ключ ЭЦП и/или шифрования, которые выдаются удостоверяющим центром участнику информационного обмена электронными документами для подтверждения подлинности ЭЦП, идентификации владельца сертификата ключа подписи и/или обеспечения защиты от искажения информации в электронном документе.

Территориальный орган Федеральной службы государственной статистики (ТОГС) – территориальный орган Федеральной службы государственной статистики, ответственный за сбор первичных статистических данных по формам федерального статистического наблюдения с зарегистрированных на территории Субъекта Российской Федерации Респондентов.

Средство криптографической защиты информации (СКЗИ) – средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения её безопасности.

Специализированный оператор связи (спецоператор) – организация, предоставляющая услуги по обмену открытой и конфиденциальной информацией между органами государственной статистики и Респондентами, в том числе гарантирующая доставку электронных документов в границах своей зоны ответственности, установленной договорами с территориальными органами государственной статистики и Респондентами, и обеспечивающая формирование и выдачу подтверждений.

Формирование (создание) ЭЦП – процесс, в качестве исходных данных которого используются электронный документ, закрытый ключ ЭЦП и параметры ЭЦП, результатом которого является электронная цифровая подпись.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

2. Общие положения

2.1 Назначение документа

Регламент описывает общие принципы использования ЭЦП в процессе организации информационного обмена при представлении юридическими лицами, их филиалами и представительствами, гражданами, занимающимися предпринимательской деятельностью без образования юридического лица статистической информации в электронном виде по телекоммуникационным каналам связи (далее – представление статистической информации в электронном виде).

2.2 Область применения документа

2.2.1 Организационные рамки

Требования настоящего Регламента распространяются на всех участников информационного обмена, взаимодействующих при представлении статистической информации в электронном виде, использующих электронную цифровую подпись:

- на Респондентов;
- на Спецоператоров;
- на Территориальные органы Федеральной службы государственной статистики (ТОГС).

2.2.2 Функциональные рамки

Настоящий регламент определяет:

- требования к применению ЭЦП;
- порядок получения сертификата ключа подписи;
- порядок приостановления действия и отзыва сертификата;
- порядок предоставления информации о статусах сертификатов;
- правила работы с ЭЦП.

2.3 Соответствие требованиям нормативно-правовых актов

Настоящий Регламент разработан с учётом требований следующих нормативно-правовых актов:

- Федеральный закон от 29.11.2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации»;
- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи»;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 30.12.2001 № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (Собрание законодательства Российской Федерации, 2002г. №1, ч.1, ст.1);
- Положение о Федеральной службе государственной статистики, утвержденное постановлением Правительства Российской Федерации от 2 июня 2008 года № 420;
- Временный порядок получения от Респондентов первичных статистических данных по формам федерального статистического наблюдения в электронном виде территориальными органами Росстата через специализированных операторов связи от 8 июля 2008 года;
- Руководящий документ ФСБ России «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (Приложение к приказу ФСБ России от 9 февраля 2005 г. № 66);
- Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (При-

ложение к Приказу Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152).

2.4 Условия признания юридической значимости ЭЦП

При представлении статистической информации в электронном виде электронная цифровая подпись (ЭЦП) в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность ЭЦП в электронном документе;
- ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа подписи.

В случае заключения соответствующего соглашения между взаимодействующими сторонами, ЭЦП в электронном документе признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.

При подтверждении подлинности ЭЦП в электронном документе проверяется принадлежность ЭЦП владельцу сертификата ключа подписи, выданного соответствующим доверенным Удостоверяющим центром.

3. Требования к применению ЭЦП

Согласно статье 4 Федеральным законом от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи», ЭЦП признаётся равнозначной собственноручной подписи в документе на бумажном носителе при условии, что сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания.

4. Порядок приостановления действия и отзыва сертификата

В процессе управления сертификатами ключей подписи Удостоверяющий центр, входящий в единую сеть доверенных Удостоверяющих центров Росстата[1], имеет возможность отзыва и приостановления действия выпущенных им сертификатов ключей подписи, что необходимо для досрочного прекращения их действия.

4.1 Отзыв сертификата ключа подписи

4.1.1 Условия отзыва сертификата

Сертификат ключа подписи должен быть отозван (аннулирован) в случае утраты доверия к нему. Причинами отзыва сертификата ключа подписи могут быть:

- компрометация закрытого ключа ЭЦП;
- потеря закрытого ключа ЭЦП;
- подозрение на компрометацию закрытого ключа ЭЦП;
- несоблюдение пользователем УЦ правил, установленных УЦ;
- увольнения, смены места работы пользователя УЦ.
- истечение срока действия сертификата ключа подписи;
- утрата юридической силы сертификата соответствующих средств электронной цифровой подписи;
- прекращение действия документа, на основании которого оформлен сертификат ключа подписи;
- заявление владельца сертификата ключа подписи.

4.1.2 Инициаторы отзыва сертификата

Запрос на отзыв сертификата ключа подписи может быть сделан:

[1] На текущий момент определяется список Удостоверяющих Центров, входящих в сеть Доверенных Удотоверяющих Центров Росстата. Количество и названия Удостоверяющих Центров, которые войдут в сеть пока не определены.

- владельцем сертификата – пользователем УЦ;
- Удостоверяющим центром;
- Руководителем организации, сотрудником который является пользователь УЦ (ТОГС, Спецоператор, Респондент), но это должно быть установлено в соответствующем соглашении с УЦ.

4.1.3 Процедура отзыва сертификата

Отзыв сертификата ключа подписи, изготовленного Удостоверяющим центром (УЦ), осуществляется УЦ по заявлению на отзыв сертификата ключа подписи.

В случае необходимости отзыва сертификата ключа подписи, пользователь УЦ должен немедленно сообщить об этом в УЦ. Для этого пользователь УЦ формирует заявление на отзыв сертификата.

Заявление на отзыв сертификата ключа подписи подается в УЦ пользователем УЦ, либо руководителем организации, сотрудником которой является пользователь УЦ, в бумажном виде, если это предусмотрено соответствующим соглашением с УЦ.

Удостоверяющий центр после получения запроса на отзыв сертификата ключа подписи в максимально короткие сроки (установленные в регламенте функционирования данного УЦ), аннулирует сертификат.

Отозванный сертификат немедленно помещается в список отозванных сертификатов (СОС).

4.2 Приостановление действия сертификата ключа подписи

Приостановление действия сертификата ключа подписи Удостоверяющим центром позволяет впоследствии возобновить действие приостановленного сертификата ключа подписи.

В том случае, если по истечении срока приостановления действия не поступает указания о возобновлении действия сертификата ключа подписи, он подлежит аннулированию.

4.2.1 Процедура приостановления действия сертификата

Приостановление действия сертификата ключа подписи, изготовленного Удостоверяющим центром (УЦ), осуществляется УЦ по заявлению на приостановление сертификата ключа подписи его владельца.

Заявление на приостановление действия сертификата ключа подписи подается пользователем УЦ в бумажной форме.

Срок рассмотрения заявления на приостановление действия сертификата ключа подписи устанавливается регламентом функционирования соответствующего УЦ.

Действие сертификата ключа подписи может быть приостановлено Удостоверяющим центром (УЦ) на основании указания лиц или органов, имеющих такое право в силу закона или договора.

4.2.2 Процедура возобновления действия приостановленного сертификата

Возобновление действия приостановленного сертификата ключа подписи, изготовленного Удостоверяющим центром (УЦ), осуществляется УЦ по соответствующему заявлению его владельца.

Заявление на возобновление действия приостановленного сертификата ключа подписи подается заявителем бумажной форме в УЦ.

Срок рассмотрения заявления на возобновление действия сертификата ключа подписи устанавливается регламентом функционирования соответствующего УЦ.

5. Порядок предоставления информации о статусах сертификатов

После осуществления отзыва, приостановления и возобновления действия сертификатов Удостоверяющий центр должен оповестить пользователей об изменении статуса сертификатов.

5.1 Распространение информации о статусах сертификатов

В соответствии с Федеральным законом от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи» в случае отзыва (приостановления действия) сертификата ключа подписи Удостоверяющий центр оповещает об этом пользователей сертификатов ключей подписей путем внесения в реестр сертификатов ключей подписей соответствующей информации с указанием даты и времени отзыва (приостановления действия) сертификата ключа подписи, за исключением случаев аннулирования сертификата ключа подписи по истечении срока его действия.

Удостоверяющие центры (УЦ) могут предоставлять различные методы распространения информации об отзыве, приостановлении и возобновлении действия сертификатов ключей подписи:

- распространение списка отозванных сертификатов (СОС, Certificate Revocation List, CRL) путём публикации их в узлах CRDP (Certificate Revocation Distribution Point);
- получение информации о статусе сертификата в реальном времени на основе протокола OCSP (Online Certificate Status Protocol).

5.2 Издание списка отозванных сертификатов

Список отозванных сертификатов (СОС) представляет собой список аннулированных или приостановленных сертификатов, издаваемый периодически УЦ и заверенный электронной цифровой подписью УЦ. СОС не отражает информацию о статусах сертификатов ключей подписи в реальном времени, а также имеет ряд других недостатков.

В течение процедуры отзыва сертификата формируется список отозванных сертификатов (СОС). СОС содержит серийный номер отзываемого сертификата ключа подписи и время отзыва сертификата ключа подписи.

Электронная цифровая подпись (ЭЦП), созданная с помощью закрытого ключа ЭЦП, соответствующего открытому ключу ЭЦП в отозванном сертификате, будет признана недействительной, если время создания ЭЦП позже времени отзыва соответствующего сертификата, указанного в СОС.

Формат и применение списка отозванных сертификатов определены в рекомендациях международного стандарта ITU-T X.509 версии 3 и в рекомендациях IETF RFC 2459 (RFC 3280).

Для указания адреса, по которому доступен СОС, в сертификаты ключей подписи включается информация об узлах CRDP (Certificate Revocation Distribution Point – точка распространения СОС). Таких узлов может быть несколько. Узел CRDP может содержать фрагмент СОС.

Частота обновления списка отозванных сертификатов (СОС) устанавливается Удостоверяющим центром.

5.3 Получение информации о статусе сертификата в реальном времени

Протокол OCSP (Online Certificate Status Protocol) – протокол получения статуса сертификата в реальном времени применяется для предоставления пользователям УЦ актуальной информации о статусах сертификатов ключей подписи.

Протокол OCSP (Online Certificate Status Protocol) описан в рекомендациях IETF RFC 2560.

Концептуальное отличие протокола OCSP от СОС заключается в выдаче ответа по запросу статуса конкретных сертификатов. Ответ на запрос по протоколу OCSP представляет собой подписанный Удостоверяющим центром СОС, но с информацией только о запрошенных сертификатах ключей подписи.

Адрес для доступа к серверам OCSP указывается в AIA (Authority Information Access – точка доступа к информации УЦ) сертификатов ключей подписи. Таких точек доступа может быть несколько.

6. Правила работы с ЭЦП

Представление статистической информации в электронном виде допускается при обязательном использовании сертифицированных Федеральной службой безопасности Российской Федерации (ФСБ России) средств электронной цифровой подписи, позволяющих идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации, содержащейся в статистической информации в электронном виде.

6.1 Сертификаты ключей подписи

Сертификат ключа подписи должен быть внесен Удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи.

Сертификат ключа подписи должен содержать следующие обязательные сведения:

- владелец сертификата ключа подписи (фамилия, имя и отчество физического лица);
- открытый ключ ЭЦП;
- уникальный регистрационный номер сертификата ключа подписи;
- даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра (УЦ);
- наименование и место нахождения УЦ, выдавшего сертификат ключа подписи;
- наименование средств ЭЦП, с которыми используется данный открытый ключ ЭЦП;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение;

- область (области) использования сертификата ключа подписи, при которых электронный документ с электронной цифровой подписью будет иметь юридическое значение;
- точка распространения списка аннулированных (отозванных) сертификатов ключей подписи, изданных Удостоверяющим центром.

Дополнительные данные о владельце сертификата ключа подписи могут включаться в сертификат ключа подписи только с его письменного согласия.

6.2 Использование средств ЭЦП

Средства электронной цифровой (средства ЭЦП) подписи обеспечивают реализацию следующих функций:

- создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи;
- подтверждение подлинности электронной цифровой подписи в электронном документе с использованием открытого ключа электронной цифровой подписи (сертификата ключа подписи);
- создание закрытого ключа и открытого ключа электронной цифровой подписи.

Применение отчитывающимися субъектами ЭЦП в рамках работы с ЕСО и Электронным архивом не требует получения специальной лицензии.

6.3 Хранение закрытого ключа ЭЦП

В соответствии со Статьёй 12 Федерального закона от 10.01.2002 г. № 1-ФЗ «Об электронной цифровой подписи» владелец сертификата ключа подписи обязан хранить в тайне закрытый ключ электронной цифровой подписи (ЭЦП).

Носитель информации, содержащий закрытый ключ ЭЦП, находится на ответственном хранении у владельца сертификата ключа подписи (пользователя Удостоверяющего центра) и должен храниться в условиях, исключающих

возможность его компрометации. Передавать закрытый ключ ЭЦП другому лицу запрещено.

Обращение с носителем информации, содержащим закрытый ключ ЭЦП, должно осуществляться в соответствии с эксплуатационной документацией на средства электронной цифровой подписи и в соответствии с требованиями Удостоверяющего центра (УЦ).

Не допускается:

- записывать на носитель ключевой информации постороннюю информацию;
- подключать носитель ключевой информации к техническим средствам обработки информации, не предусмотренным штатным режимом эксплуатации ЕССО и ЭА.

Необходимо ограничить доступ к автоматизированным рабочим местам (АРМ), которые используются для создания ЭЦП к электронным документам.

На данные АРМ не должно устанавливаться программное обеспечение (ПО), не связанное с выполнением служебных обязанностей сотрудников, работающих на этих АРМ.

Ответственность за компрометацию или утрату закрытого ключа ЭЦП возлагается на владельца сертификата ключа подписи (пользователя Удостоверяющего центра).

6.4 Компрометация ключей

Под компрометацией закрытого ключа электронной цифровой подписи (ЭЦП) понимается его утрата, хищение, разглашение, несанкционированное копирование, увольнение сотрудника, имеющего доступ к закрытому ключу ЭЦП, любые другие виды разглашения закрытого ключа ЭЦП, а также такие случаи, когда нельзя достоверно установить, что произошло с носителем, содержащим закрытый ключ ЭЦП.

При компрометации (или подозрении на компрометацию) закрытого ключа ЭЦП пользователя Удостоверяющего центра (УЦ) он должен немедлен-

но прекратить использование данного закрытого ключа ЭЦП и сообщить в УЦ, выдавший данный закрытый ключ ЭЦП, о факте компрометации (или подозрении на компрометацию).