ООО «СТЭП ЛОДЖИК»

Единая интегрированная
информационная система «Соцстрах»
Фонда социального страхования
Российской Федерации

АРМ «ПОДПИСАНИЕ И ШИФРОВАНИЕ»

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

42926941.00042116.034001.008.37.6.И3

2013

Содержание

Настоящее руководство пользователя (далее – *Руководство*) содержит сведения, необходимые пользователю для эксплуатации прикладной подсистемы – автоматизированного рабочего места (*АРМ*) «Подписание и шифрование» Единой интегрированной информационной системы «Соцстрах» Фонда социального страхования Российской Федерации (далее – *ФСС РФ*, *Фонд*, *Заказчик*).

Руководство подготовлено специалистами ООО «СТЭП ЛОДЖИК» (далее – *Разработчик*) в соответствии с частными техническими заданиями на выполнение работ по технической поддержке и сервисному сопровождению программы АРМ «Подписание и шифрование» (далее – *Работы*) в рамках проекта «Техническая поддержка, сервисное сопровождение и развитие прикладных функциональных подсистем ЕИИС “Соцстрах”» (подраздел 8.1.08 и 8.2.08 приложения 1 к Государственному контракту от 25 января 2013 года номер 2013.3139/012 – *Контракт*).

Обозначение Работ: 42926941.00042116.034001.008.37.6.

1 Введение

1.1 Общие сведения о подсистеме

Полное наименование автоматизированной системы – «Единая интегрированная информационная система «Соцстрах» Фонда социального страхования Российской Федерации» (далее – *ЕИИС «Соцстрах»*).

Полное наименование подсистемы – автоматическое рабочее место «Подписание и шифрование» (далее – *подсистема АРМ «Подписание и шифрование», Подсистема)*.

Заказчик Подсистемы − Фонд социального страхования Российской Федерации: 107139, г. Москва, Орликов пер., д. 3, корп. А.

1.2 Область применения

Область применения Подсистемы:

- подписание и шифрование электронных документов;
- отправка отчетов;
- просмотр результата обработки отчета.

1.3 Уровень подготовки пользователей

Для эксплуатации Подсистемы пользователь должен иметь опыт работы в среде современных операционных систем семейства Microsoft Windows. Иметь опыт работы с современными офисными пакетами, например Microsoft Office или OpenOffice.org.

Пользователь обязан изучить настоящее Руководство.

1.4 Перечень эксплуатационной документации

Перечень эксплуатационной документации Подсистемы указан ниже (таблица 1).

Таблица 1

Наименование	Обозначение
Руководство пользователя	42926941.00042116.034001.008.37.6.И3

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

Подсистема АРМ «Подписание и шифрование» предназначена для подписания и шифрования электронных документов.

2.1 Функции Подсистемы

Подсистема АРМ «Подписание и шифрование» выполняет следующие функции:

- подписание и шифрование электронных документов;
- отправка отчётов;
- просмотр отправленных отчётов;
- просмотр результата обработки отчета.

2.2 Системные требования

Требования к операционной системе:

- Microsoft Windows версий 2000, XP, Vista, Windows 7;
- установленное СКЗИ с поддержкой алгоритмов ГОСТ Р 34.10 и ГОСТ Р 34.11.

Для функционирования Подсистемы необходимо, чтобы компьютер был подключён к сети Internet.

2.3 Установка программы

Специальной процедуры инсталляции не требуется.

При первом запуске утилита создает новый раздел в системном реестре Windows (HKEY_CURRENT_USER\Software\FSS\ARM), в котором будет запоминать параметры сеанса и настройки выхода в сеть Internet. В созданной ветке разделе реестра для каждого типа документа создается подветка. В таблице ниже приведены параметры из корневой ветки раздела, а также из подветки документа F4 (таблица 2).

Таблица 2 Параметры

Имя параметра	Тип	Значение по умолчанию	Назначение
ActiveMode	Симв.	F4	Тип документа по умолчанию
FSSRootCertUrl	Симв.	http://www.fss.ru/uc/GUC_FSS_RF_2013.cer	URL корневого сертификата ФСС

Имя параметра	Тип	Значение по умолчанию	Назначение
Height	Числ.		Высота окна в пикселах
Width	Числ.		Ширина окна в пикселах
ProvName	Симв.		Наименование криптопровайдера
ProvType	Числ.		Тип криптопровайдера
Proxy	Симв.		Адрес прокси-сервера
proxy_user	Симв.		Имя пользователя для прокси-сервера
F4\APCertURL	Симв.	http://www.fss.ru/uc/F4_FSS_RF_2013_qualified.cer	URL сертификата уполномоченного лица ФСС РФ
F4\GateInfoURL	Симв.	http://f4.fss.ru/service3.php	URL сервиса для получения информации об отправленном отчёте
F4\GateLoadURL	Симв.	http://f4.fss.ru/get_ack.php	URL сервиса для загрузки квитанции
F4\GateSendURL	Симв.	http://f4.fss.ru/index.php	URL сервиса для отправки отчёта
F4\EncExt	Симв.	ef4	Расширение зашифрованного и подписанного файла
F4\KvitExt	Симв.	p7e	Расширение файла-квитанции
F4\SrcExt	Симв.	xml	Расширение исходного файла

3 Описание операций

3.1 Задачи Подсистемы

Главное окно Подсистемы содержит главное меню и кнопки быстрого доступа к режимам. При помощи пунктов главного меню пользователь имеет возможность выбрать необходимый режим работы (рисунок 1).

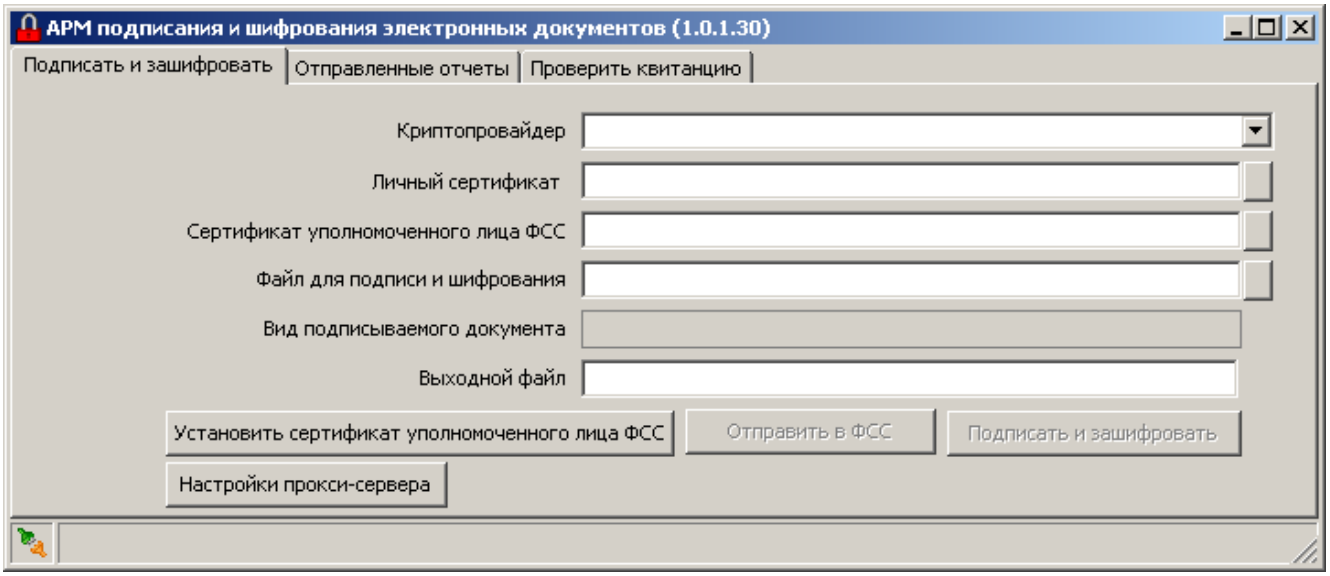

Рисунок 1 – Главное окно Подсистемы

Пользователь Подсистемы может выполнять следующие задачи:

- подписание и шифрование электронных документов;
- подготовка и отправка отчёта;
- просмотр отправленных отчётов;
- просмотр результата обработки отчёта.

Для подписания и шифрования документа необходимо выбрать:

- криптопровайдера;
- личный сертификат;
- сертификат уполномоченного лица ФСС;
- файл для подписи и шифрования;
- выходной файл.

Вид подписываемого документа проставляется автоматически при выборе данного документа.

3.1.1 Хранилище результатов

Информация обо всех отправленных отчётах сохраняется в специальном файловом хранилище **C:\Documents and Settings\<имя_пользователя>\Local Settings\Application Data\FSS\ARM\F4\ARC**.

На шлюзе приёма отчётности ФСС РФ каждому отчёту присваивается уникальный номер. Для каждого отправленного на шлюз отчёта создается директория, имя которой есть уникальный номер отчёта, присвоенный шлюзом. В этой директории сохраняются результаты обработки отчёта. Расширения файлов зависят от настроек из реестра (F4\EncExt, F4\KvitExt, F4\SrcExt). В таблице ниже приводятся расширения по умолчанию (таблица 3).

Таблица 3 Расширения файлов

Файл	Назначение
имя_отчета.xml	Исходный файл отчета
имя_отчета.ef4	Подписанный и зашифрованный файл отчета
номер_отчета.inf	Информация об отправителе
номер_отчета.p7e	Зашифрованная и подписанная квитанция
номер_отчета.zip	Квитанция

3.1.2 Настройка подключения к сети Internet

При запуске утилиты производится проверка подключения к сети Internet. Настройки прокси-сервера берутся из настроек веб-обозревателей Internet Explorer или Firefox. Если указанных браузеров нет или они не настроены, и подключиться без прокси-сервера не удалось, то появляется диалоговое окно настройки прокси-сервера (рисунок 2).

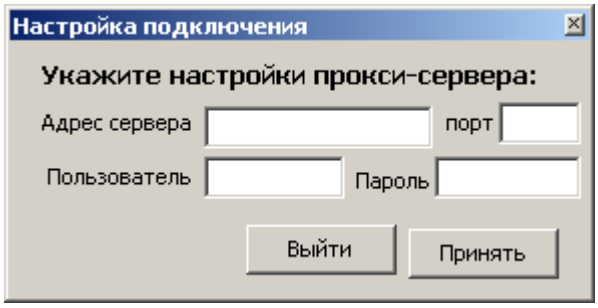

Рисунок 2 – Настройка подключения

Введя соответствующие значения в поля «**Адрес сервера**», «**порт**», «**Пользователь**», «**Пароль**» следует нажать кнопку “**Принять**” – появится окно “**АРМ подписания и шифрования электронных документов…**” (рисунок 3).

В левом нижнем углу окна (рисунок 3) есть индикатор наличия подключения к сети Internet. При щелчке правой кнопкой мыши по этому индикатору появится меню “**Настройки прокси-сервера**”, состоящее из двух пунктов:

- “**Тестировать подключение**”;
- “**Настройки прокси-сервера**”.

С помощью этих режимов можно установить настройки прокси-сервера и проверить состояние подключения (рисунок 3).

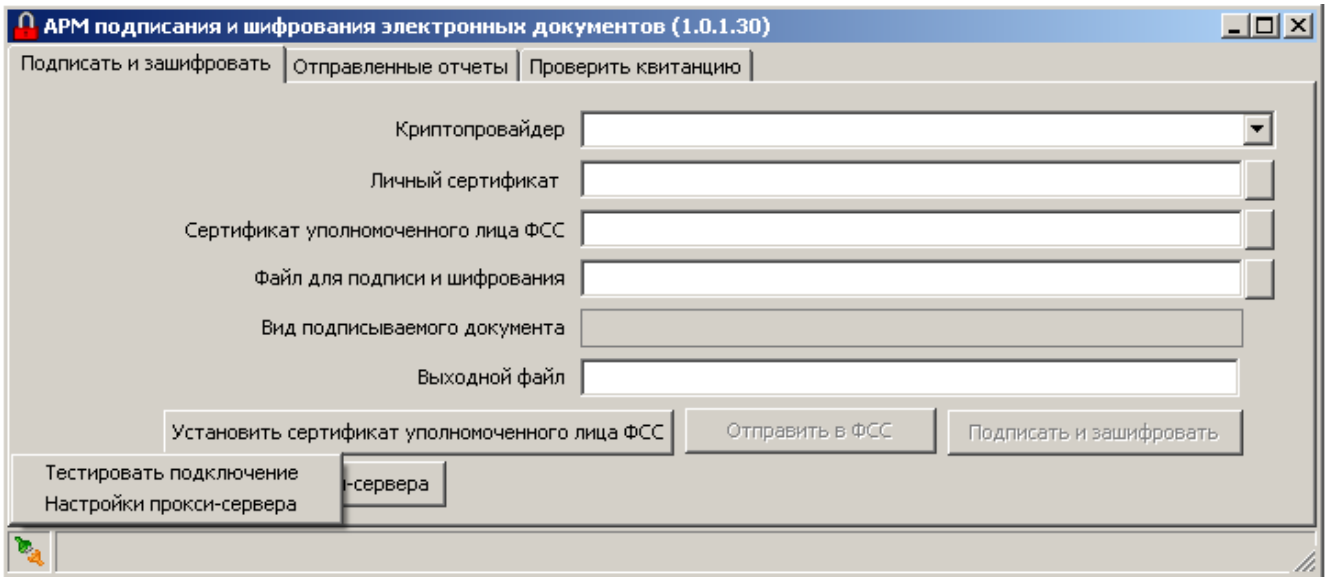

Рисунок 3 – Индикатор подключения к сети Internet

3.1.3 Подготовка и отправка отчёта

Чтобы подготовить и отправить отчёт в ФСС РФ, необходимо открыть вкладку “**Подписать и зашифровать**” (см. рисунок 3). При первом запуске утилиты все поля на этой вкладке будут пустыми. При последующих запусках будут отображаться последние введённые значения.

Сначала необходимо выбрать криптопровайдера. В раскрывающемся списке будут указаны все криптопровайдеры, ПО которых, поддерживающее алгоритм ГОСТ Р 34.10 и ГОСТ Р 34.11, установлено на компьютере. Необходимо выбрать одного из них.

Далее необходимо нажать кнопку “**Личный сертификат**” (см. рисунок 3) и выбрать в открывшемся окне “**Выбор сертификата**” (см. рисунок 4) личный сертификат

пользователя. Этот сертификат будет использоваться при подписании отчёта и должен быть связан с закрытым ключом.

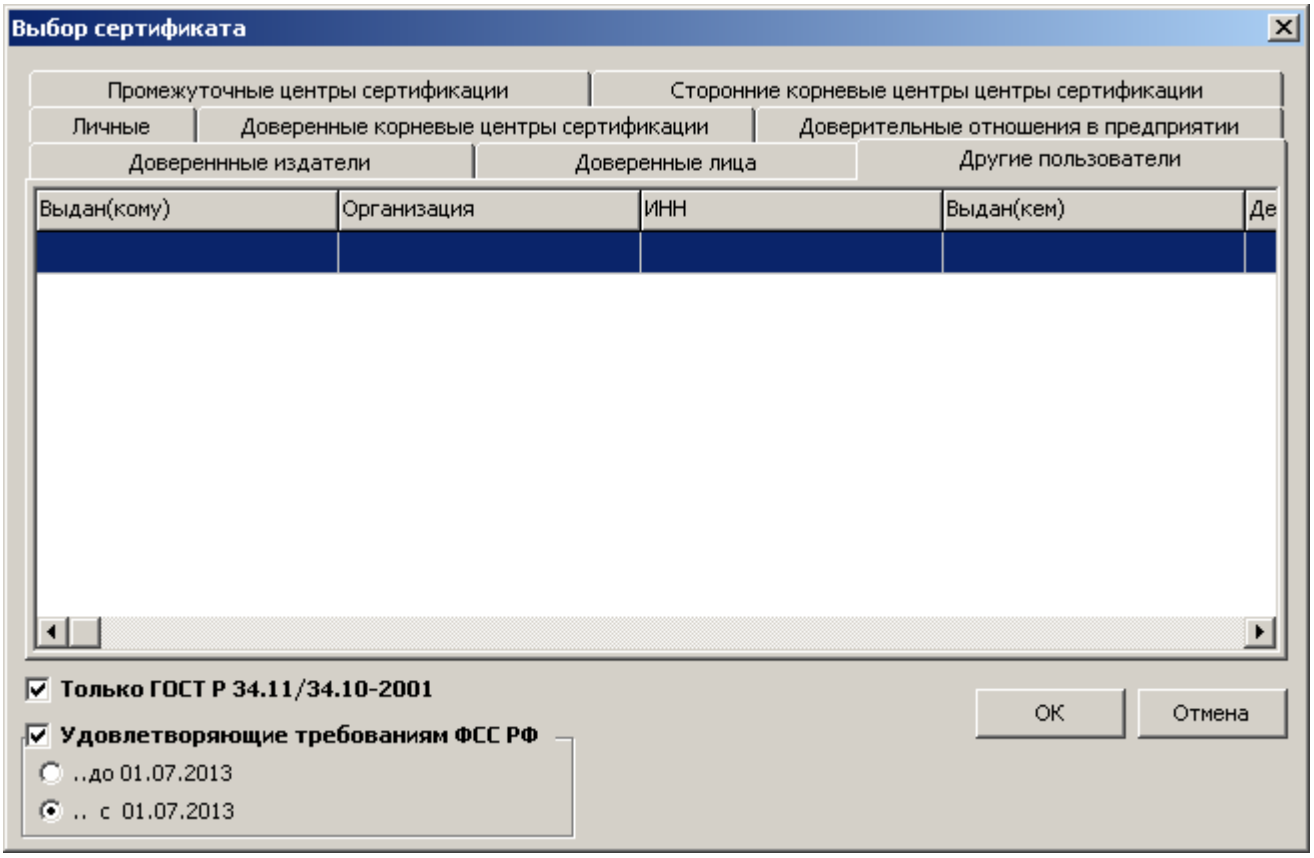

Рисунок 4 – Выбор сертификата

Личный сертификат должен удовлетворять следующим требованиям:

- иметь закрытый ключ;
- поддерживать ГОСТ Р 34.10 и ГОСТ Р 34.11;
- удовлетворять требованиям ФСС РФ (до 01.07.2013 содержать в поле “Субъект” “РНС ФСС” и “КП ФСС”, с 01.07.2013 также соответствовать параметрам усиленных квалифицированных сертификатов ЭП (см.таблица 4, таблица 5 и таблица 6).

Таблица 4 Обязательные поля раздела Issuer

Обозначение	Наименование	OID
CN	Общее имя	2.5.4.3
C	Страна	2.5.4.6
S	Регион	2.5.4.8
L	Населённый пункт	2.5.4.7
O	Организация	2.5.4.10
INN	ИНН	1.2.643.3.131.1.1

Таблица 5 Обязательные поля раздела Subject

Обозначение	Наименование	OID
CN	Общее имя	2.5.4.3
C	Страна	2.5.4.6
S	Регион	2.5.4.8
L	Населённый пункт	2.5.4.7
O	Организация	2.5.4.10
T	Должность	2.5.4.12
SNILS	СНИЛС	1.2.643.100.3
INN	ИНН	1.2.643.3.131.1.1

Таблица 6 Обязательные атрибуты сертификата

Обозначение	Наименование	OID
certificatePolicies	Политики сертификата	2.5.29.32
subjectSignTool	Средство ЭП владельца	1.2.643.100.111
IssuerSignTool	Средство ЭП УЦ	1.2.643.100.112

По умолчанию, открывается вкладка “**Личные**”. Если сертификат находится в другом хранилище, то необходимо выбрать соответствующую вкладку. Выбрав сертификат, следует нажать правую кнопку мыши – появится контекстное меню из двух пунктов:

- “**Показать сертификат**” – отображает системный диалог для просмотра содержимого сертификата.
- “**Проверить закрытый ключ**” – проверяет наличие закрытого ключа.

Выбрав сертификат, следует нажать кнопку “**ОК**”.

Далее необходимо выбрать сертификат уполномоченного лица ФСС РФ. При нажатии кнопки выбора отобразится диалог выбора сертификата. Сертификат должен поддерживать ГОСТ Р 34.10 и ГОСТ Р 34.11.

По умолчанию открывается вкладка “**Другие пользователи**” (см. рисунок 4). Если сертификат находится в другом хранилище, необходимо выбрать соответствующую вкладку. Если сертификат уполномоченного лица еще не установлен, его можно установить автоматически. Для этого следует нажать кнопку “**Установить сертификат уполномоченного лица ФСС**” (рисунок 5).

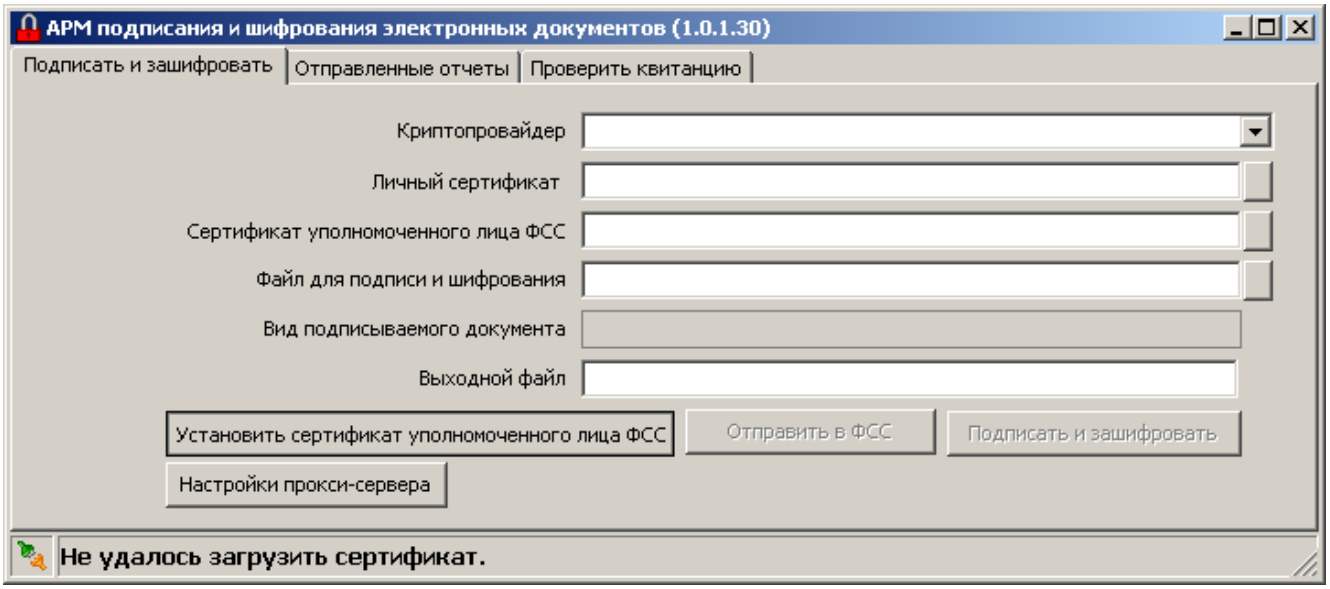

Рисунок 5 – Установка сертификата уполномоченного лица ФСС

В появившемся окне “**Предупреждение о безопасности**”(рисунок 6) необходимо подтвердить установку корневого сертификата, нажав кнопку “**Да**”.

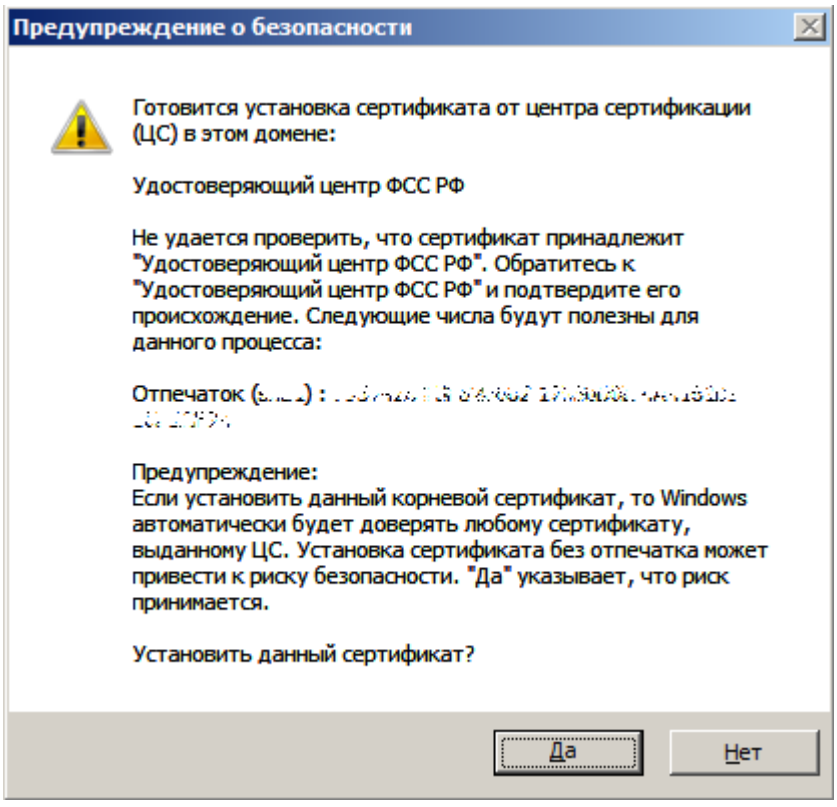

Рисунок 6 – Подтверждение установки корневого сертификата

Далее следует выбрать исходный файл с отчётом, нажав кнопку “**Файл для подписи и шифрования**” (см. рисунок 5) и указать имя выходного файла, который представляет собой подписанный и зашифрованный отчёт.

После этого станет доступна кнопка “**Подписать и зашифровать**” (см. рисунок 3), нажатие которой приводит к выдаче подписанного и зашифрованного отчёта.

Отчет можно отправить в ФСС РФ, нажав кнопку “**Отправить в ФСС**” (см. рисунок 5). В случае успеха, в строке состояния будет отображен уникальный номер отчёта, присвоенный шлюзом приёма отчётности ФСС РФ.

3.1.4 Отправленные отчеты

Чтобы узнать результат обработки отчёта необходимо перейти на вкладку “**Отправленные отчеты**” (рисунок 7).

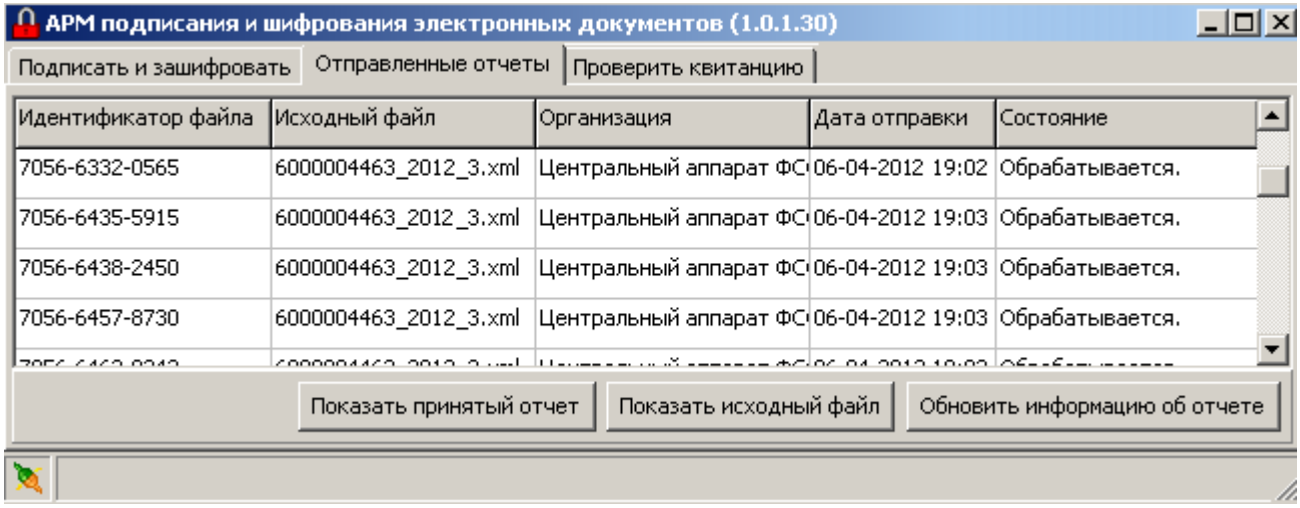

Рисунок 7 – Вкладка «Отправленные отчеты»

Далее необходимо выбрать запрос, щелкнув по соответствующей строке левой кнопкой мыши, и нажать кнопку “**Обновить информацию об отчете**”. В поле “**Состояние**” отобразится текущее состояние отчёта. Это поле может содержать одно из значений:

- “**Обрабатывается**” – отчёт находится на стадии обработки;
- “**Обнаружены ошибки**” – отчёт обработан, но обнаружены ошибки;
- “**Успешно обработан**” – отчёт успешно обработан.

В двух последних случаях утилита автоматически откроет вкладку “**Проверить квитанцию**” и отобразит протокол обработки отчёта.

Для просмотра исходного файла следует выбрать отчёт и нажать кнопку “**Показать исходный файл**”.

3.1.5 Проверка квитанции

Чтобы просмотреть результат обработки отчёта (квитанцию), необходимо перейти на вкладку “**Проверить квитанцию**”. Далее следует выбрать файл квитанции и нажать кнопку “**Проверить**”. В случае успеха в форме будет отображён протокол обработки отчёта (рисунок 8).

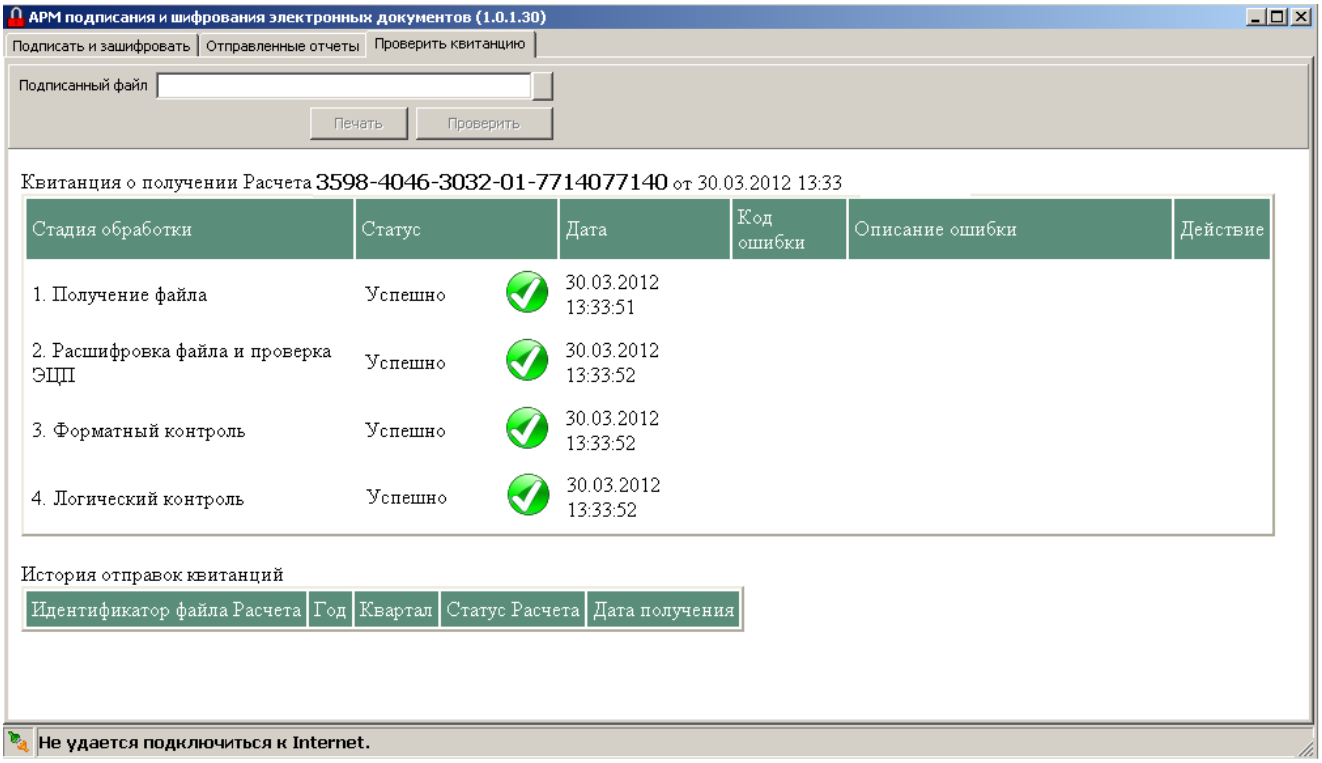

Рисунок 8 – Протокол обработки отчёта

Чтобы распечатать протокол следует нажать кнопку “**Печать**”.

При вызове утилиты с параметром – именем файла с квитанцией – окно проверки квитанции открывается автоматически.

4 Аварийные ситуации

При работе с Подсистемой могут возникнуть следующие ситуации:

- при запущенном антивирусе лаборатории Касперского не будут работать функции, связанные с выходом в сеть Internet. Выход – на время отключить антивирус;
- установленный личный сертификат может не иметь закрытого ключа. Выход – повторить установку личного сертификата в хранилище Windows средствами криптопровайдера.

5 Рекомендации по освоению

Для успешного освоения приложения необходимо иметь навыки работы с ПК, а также изучить:

- принципы работы с современными операционными системами семейства MS Windows;
- принципы работы с современными офисными приложениями семейства MS Office или OpenOffice.org;
- настоящее Руководство.

6 Перечень используемых источников

1) ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.

2) ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

3) ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

4) РД 50-34.698-90. Информационная технология. Автоматизированные системы. Требования к содержанию документов.

5) Государственный контракт от 25 января 2013 года номер 2013.3139/012 «Выполнение работ по технической поддержке, сервисному обслуживанию и развитию информационных систем и ресурсов ФСС РФ», подраздел 8.1.08 и 8.2.08 приложения 1 к Государственному контракту.

6) IEEE 1063-2001. SOFTWARE USER DOCUMENTATION.