

ООО «ВТР»

СОГЛАСОВАНО

Заместитель директора  
ГБУЗ «Самарский областной  
медицинский информационно-  
аналитический центр»

  
\_\_\_\_\_  
А.В. Игнатова  
« 21 » декабря 2020 г.

УТВЕРЖДАЮ

Директор ООО «ВТР»

  
\_\_\_\_\_  
Т.И. Ушаков  
« 21 » декабря 2020 г.

**Сервис взаимодействия с Фондом социального страхования в  
части ведения и учета электронных родовых сертификатов**

**Руководство администратора**

Контракт от «20» ноября 2020 г. №60/20-ДБУ  
Этап 2 Календарного плана ТЗ к Контракту

## Содержание

Перечень терминов и сокращений .....	3
<b>1 Введение .....</b>	<b>4</b>
<b>2 Настройки интеграции в ЕМИАС .....</b>	<b>5</b>
2.1 Добавление внешней системы «fss» .....	5
<b>3 Настройка интеграции через СМЭВ 3.....</b>	<b>9</b>
<b>4 ФСС ЭРС: Шифрование и подписание сообщений .....</b>	<b>14</b>
4.1 Шифрование данных .....	16
4.1.1 Структура зашифрованного сообщения.....	16

## Перечень терминов и сокращений

Термин, сокращение	Определение
XML	eXtensible Markup Language – расширяемый язык разметки, текстовый формат, предназначенный для хранения структурированных данных и для обмена информацией между программами
ГОСТ	Государственный стандарт
ЕГИСЗ	Единая государственная информационная система в сфере здравоохранения
ЛН	Листок нетрудоспособности
МО	Медицинская организация
Система, ЕМИАС	Единая медицинская информационно-аналитическая система, обеспечивающая ведение централизованных информационных ресурсов в сфере здравоохранения Самарской области, информационное взаимодействие с ЕГИСЗ, организацию электронного медицинского документооборота
СМЭВ	Система межведомственного электронного взаимодействия
СТП	Служба технической поддержки
ФСС	Фонд социального страхования
ЭП	Электронная подпись
ЭРС	Электронный родовой сертификат

## 1 Введение

В Системе реализованы функциональные возможности, автоматизирующие следующие процессы:

- направление запроса с целью формирования ЭРС, получения номера, сформированного ЭРС;
- направление запроса на получение сведений сформированного ранее ЭРС;
- формирование и направление сведений ЭРС данными женской консультации (Талон 1);
- формирование и направление сведений ЭРС данными родильного дома (Талон 2);
- формирование и направление сведений ЭРС данными детской поликлиники за первые полгода наблюдения ребенка (детей) (Талон 3-1);
- формирование и направление сведений ЭРС данными детской поликлиники за вторые полгода наблюдения ребенка (детей) (Талон 3-2);
- формирование и направление сведений о постановке детей на учет в детской поликлинике;
- формирование и направление сведений платежных документов (счет на оплату, реестр талонов);
- направление запроса на получение сведений по статусу счета на оплату;
- направление запроса на получение сведений о переданных талонах ЭРС, находящихся в определенных статусах (например, с целью получения данных о неоплаченных талонах) в рамках заданного периода времени;
- направление запроса на закрытие ЭРС.

## 2 Настройки интеграции в ЕМИАС

### 2.1 Добавление внешней системы «fss»

Для передачи данных в ФСС, а также получения данных из нее, добавьте внешнюю систему «fss».

Для добавления внешней системы выберите в главном меню пункт «Система/ Интеграция/ Настройка внешних систем». В разделе «Внешние системы» вызовите контекстное меню и выберите пункт «Добавить» (Рисунок 1).



Рисунок 1 – Выбор пункта контекстного меню «Добавить» в разделе «Внешние системы»

В открывшемся окне «Внешние системы: Добавление» (Рисунок 2) заполните следующие поля:

- «Код» – введите «fss»;
- «Наименование» – введите «Фонд Социального Страхования»;
- «Сервис приостановлен» – введите «Нет». Также регулируется видимость функций для работы с ЭРС. При выборе значения «Да» кнопки, пункты контекстного меню и поля, которые относятся к функциям ЭРС, не будут видны или будут заблокированы.

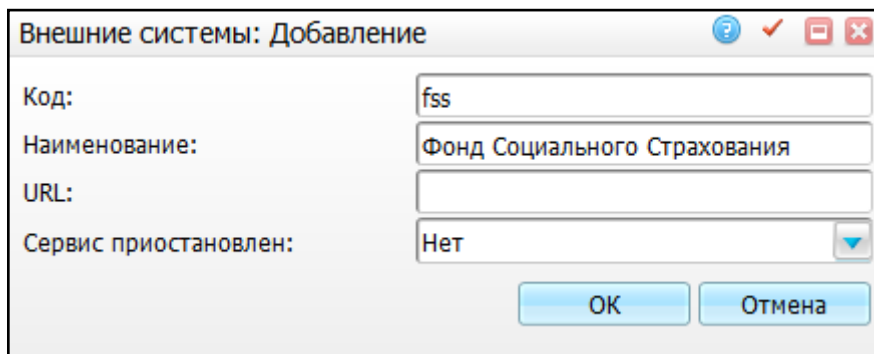


Рисунок 2 – Окно «Внешние системы: Добавление»

Нажмите кнопку «ОК».

Для внешней системы «fss» добавьте сервисы. Для этого в разделе «Сервисы внешних систем» вызовите контекстное меню и выберите пункт «Добавить» (Рисунок 3).

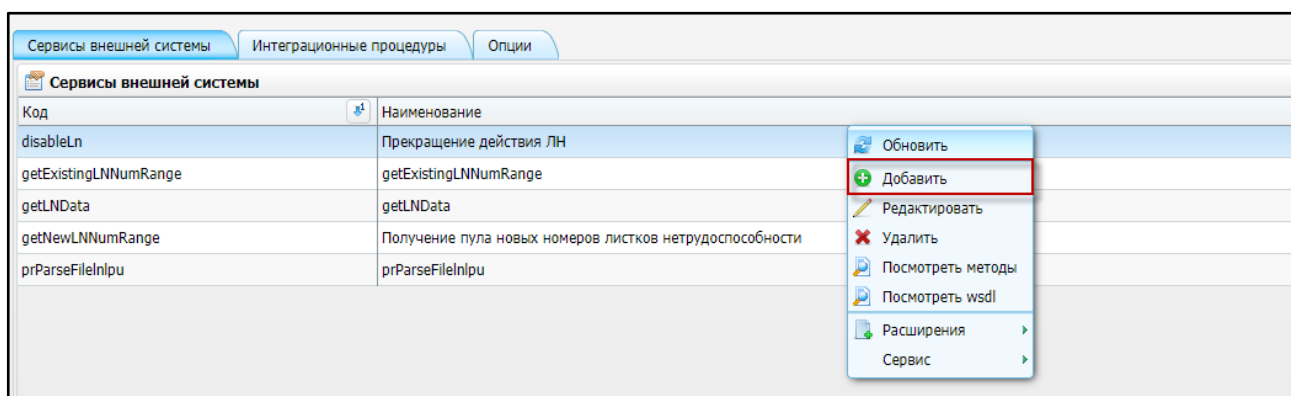


Рисунок 3 – Выбор пункта контекстного меню «Добавить»

В открывшемся окне «Сервис интеграции: добавление» (Рисунок 4) заполните поля данными из таблицы (Таблица 1).

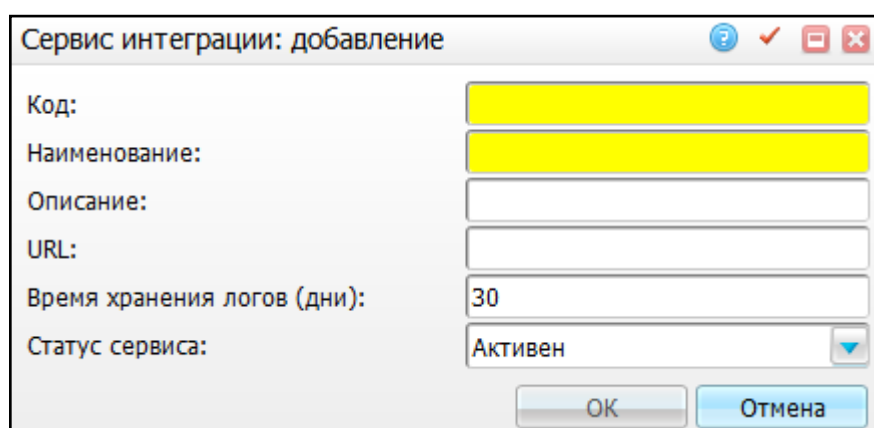


Рисунок 4 – Окно «Сервис интеграции: добавление»

Таблица 1 – Сервисы ФСС

№	Код	Наименование	URL	Статус
1	disableLn	Прекращение действия ЛН	https://docs.fss.ru/WSLnCryptoV11/FileOperationsLnPort?WSDL	Активен
2	getExistingLNNumRange	getExistingLNNumRange	https://docs.fss.ru/WSLnCryptoV11/FileOperationsLnPort?WSDL	Активен
3	getLNData	getLNData	https://docs.fss.ru/WSLnCryptoV11/FileOperationsLnPort?WSDL	Активен
4	getNewLNNumRange	Получение пула новых номеров листов нетрудоспособности	https://docs.fss.ru/WSLnCryptoV11/FileOperationsLnPort?WSDL	Активен
5	prParseFileInIpu	prParseFileInIpu	https://docs.fss.ru/WSLnCryptoV11/FileOperationsLnPort?WSDL	Активен

Для настройки системных опций ФСС перейдите на вкладку «Опции» (Рисунок 5).

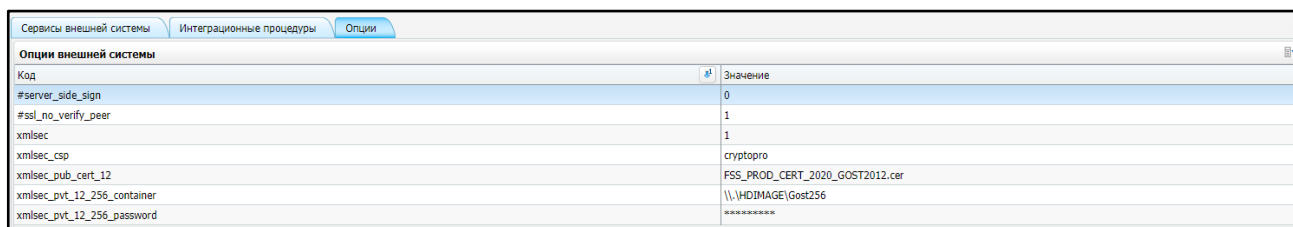


Рисунок 5 – Окно настройки внешних систем. Вкладка «Опции»

Вызовите контекстное меню и выберите пункт «Добавить» (Рисунок 6). Заполните поля данными из таблицы (Таблица 2).

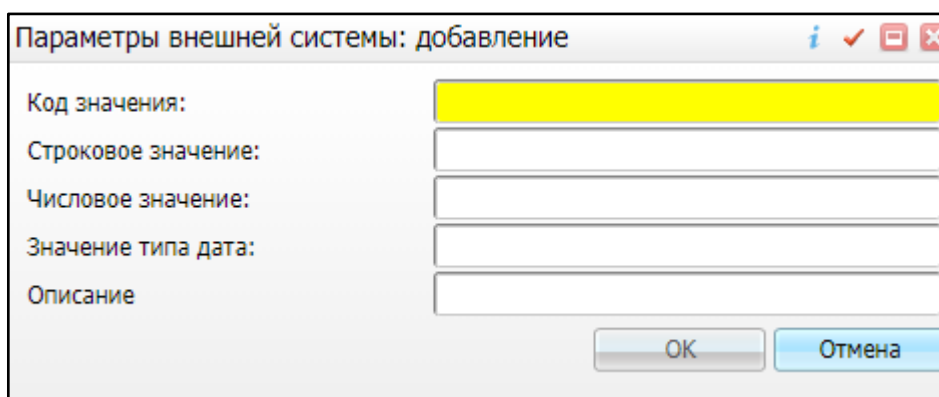


Рисунок 6 – Окно «Параметры внешней системы: добавление»

Таблица 2 – Опции ФСС

Код	Значение
#ssl_no_verify_peer	Отключить верификацию ssl-сертификата: – «0» – нет;

Код	Значение
	– «1» – да
#server_side_sign	Подписание запросов перед отправкой в ФСС: – «0» – на стороне пользователя; – «1» – на сервере
xmlsec_csp	Криптопровайдер (openssl, cryptopro) По умолчанию «cryptopro»
xmlsec	Шифрование данных ЭРС: – «1» – включить; – «0» – выключить
xmlsec_pub_cert	Путь к сертификату ФСС (относительно директории Etc)
xmlsec_pvt_container	Имя ключевого контейнера
xmlsec_pvt_password	Пароль от ключевого контейнера



### 3 Настройка интеграции через СМЭВ 3

Возможность передачи сведений ЭРС через СМЭВ 3 регулируется настройкой внешней системы «smev3/fss». Если сервис приостановлен, передача происходит напрямую через сервисы ФСС (внешняя система fss). Если сервис не приостановлен, передача происходит через СМЭВ 3.

Для возможности передачи сведений через СМЭВ 3 необходимо сначала отправить заявку на регистрацию в тестовой версии СМЭВ 3 в СТП СМЭВ. Подключение к продуктивной версии СМЭВ 3 возможно только после предоставления отчета о тестировании СТП СМЭВ.

Для добавления внешней системы «smev3/fss» выберите в главном меню пункт «Система/ Интеграция/ Настройка внешних систем». В разделе «Внешние системы» вызовите контекстное меню и выберите пункт «Добавить» (Рисунок 7).



Рисунок 7 – Выбор пункта контекстного меню «Добавить» в разделе «Внешние системы»

В открывшемся окне «Внешние системы: Добавление» (Рисунок 8) заполните следующие поля:

- «Код» – введите «smev3/fss»;
- «Наименование» – введите «СМЭВ3 / Фонд социального страхования»;
- «Сервис приостановлен» – для передачи сведений ЭРС через СМЭВ 3, укажите значение «Нет». При выборе значения «Да» передача сведений будет осуществляться через сервис ФСС.

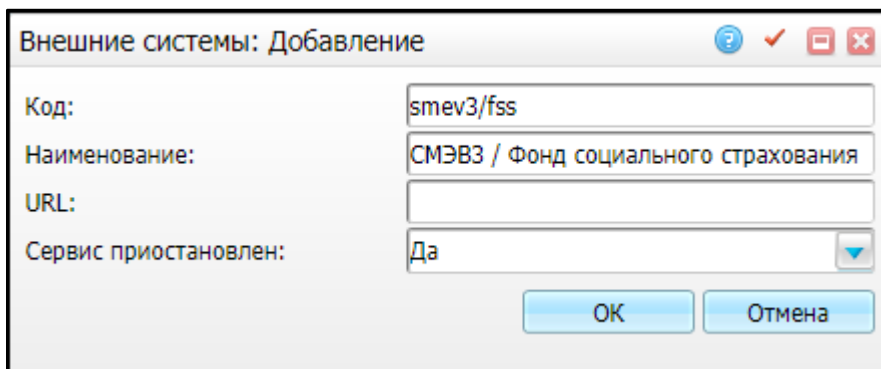


Рисунок 8 – Окно «Внешние системы: Добавление»

Нажмите кнопку «ОК».

Для внешней системы «smev3/fss» добавьте сервисы. Для этого в разделе «Сервисы внешних систем» вызовите контекстное меню и выберите пункт «Добавить» (Рисунок 9).

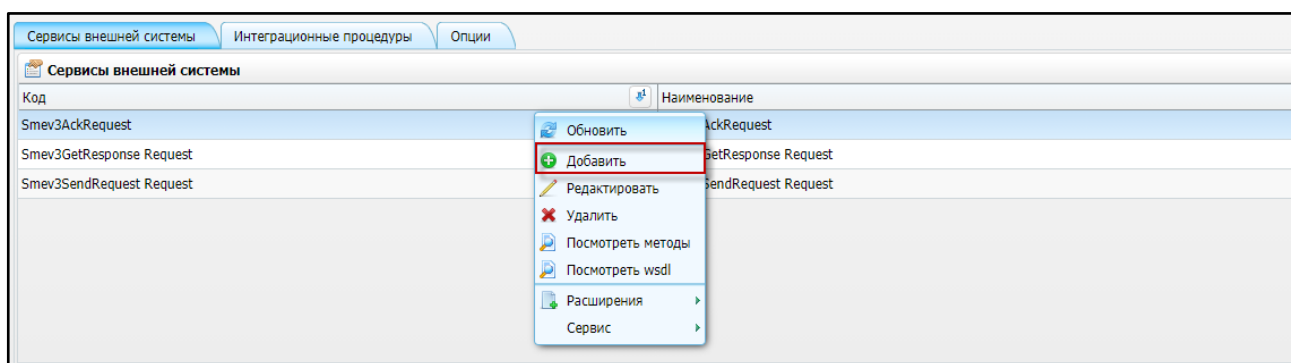


Рисунок 9 – Выбор пункта контекстного меню «Добавить»

В открывшемся окне «Сервис интеграции: добавление» (Рисунок 10) заполните поля данными из таблицы (Таблица 3).

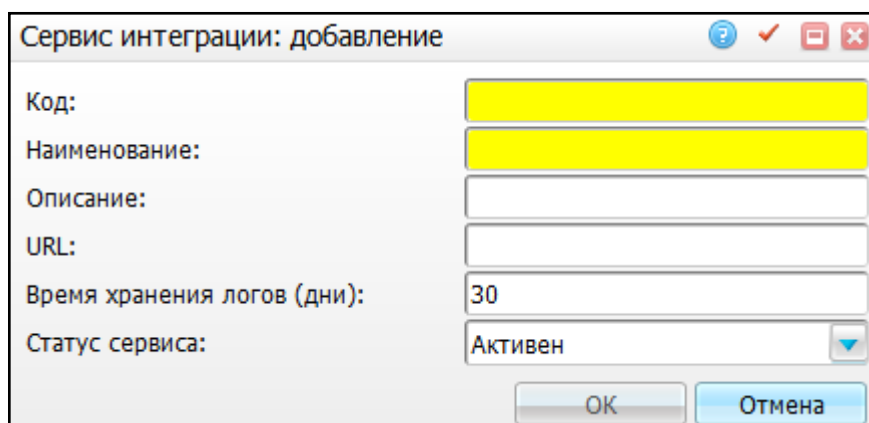


Рисунок 10 – Окно «Сервис интеграции: добавление»

Таблица 3 – Сервисы ФСС

№	Код	Наименование	URL	Статус
1	Smev3AckRequest	Smev3AckRequest	http://smev3-n0.test.gosuslugi.ru:7500/ws?wsdl	Активен
2	Smev3GetResponseRequest	Smev3GetResponseRequest	http://smev3n0.test.gosuslugi.ru:7500/ws?wsdl	Активен
3	Smev3SendRequestRequest	Smev3SendRequestRequest	http://smev3n0.test.gosuslugi.ru:7500/ws?wsdl	Активен

Для настройки системных опций «smev3/fss» перейдите на вкладку «Опции» (Рисунок 11).

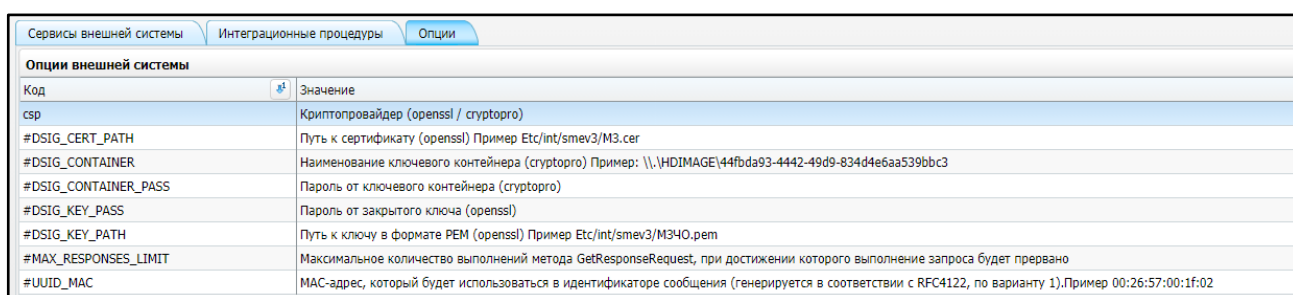


Рисунок 11 – Окно настройки внешних систем. Вкладка «Опции»

Вызовите контекстное меню и выберите пункт «Добавить» (Рисунок 12) и заполните поля данными из таблицы (Таблица 4).

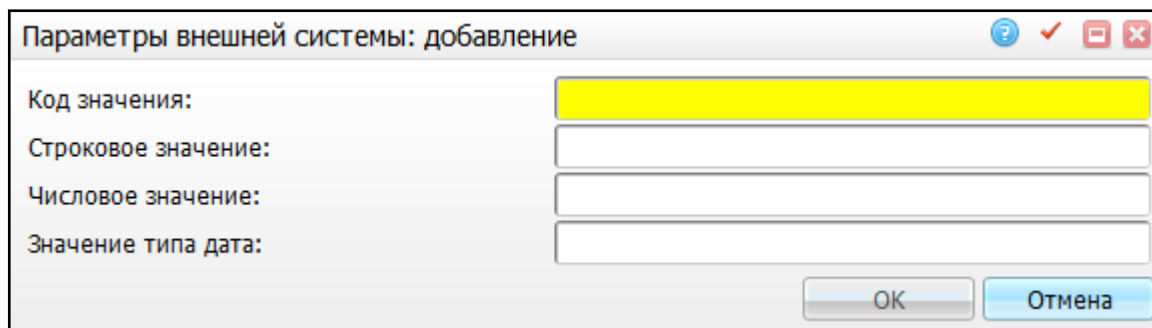


Рисунок 12 – Окно «Параметры внешней системы: добавление»

Таблица 4 – Опции СМЭВ

Код	Значение
csp	Криптопровайдер (openssl / cryptopro)
#UUID_MAC	MAC-адрес, который будет использоваться в идентификаторе сообщения (генерируется в соответствии с RFC4122, по варианту 1).Пример 00:26:57:00:1f:02
#MAX_RESPONSES_LIMIT	Максимальное количество выполнений метода GetResponseRequest, при достижении которого выполнение запроса будет прервано

Код	Значение
#DSIG_KEY_PATH	Путь к ключу в формате PEM (openssl) Пример Etc/int/smev3/M3ЧО.pem
#DSIG_KEY_PASS	Пароль от закрытого ключа (openssl)
#DSIG_CERT_PATH	Путь к сертификату (openssl) Пример Etc/int/smev3/M3.cer
#DSIG_CONTAINER	Наименование ключевого контейнера (cryptopro) Пример: \\.\HDIMAGE\44fbda93-4442-49d9-834d4e6aa539bbc3
#DSIG_CONTAINER_PASS	Пароль от ключевого контейнера (cryptopro)

Настройте системную опцию «Region». Для этого перейдите в пункт меню «Система/ Настройка системных опций/ Системные опции (Администратор)». В окне «Системные опции» вызовите контекстное меню и выберите пункт «Добавить».

Откроется окно «Системные опции: добавление» (Рисунок 13).

Рисунок 13 – Окно добавления системной опции. Вкладка «Реквизиты»

На вкладке «Реквизиты» заполните поля:

- «Раздел» – введите «GEOGRAFY»;
- «Код опции» – введите «Region»;
- «Наименование опции» – введите «Код региона»;
- «Уровень запрета переопределение» – из выпадающего списка выберите значение «До системного».

Перейдите на вкладку «Тип данных» (Рисунок 14).

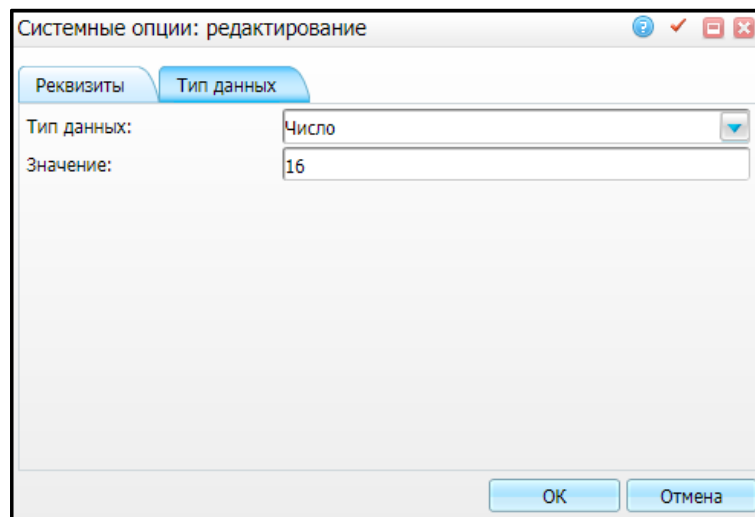


Рисунок 14 – Окно добавления системной опции. Вкладка «Тип данных»

Заполните поля:

- «Тип данных» – из выпадающего списка выберите значение «Число»;
- «Значение» – введите код нужного региона.

Нажмите кнопку «ОК».

## 4 ФСС ЭРС: Шифрование и подписание сообщений

Для обеспечения юридически значимого документооборота используется ЭП следующих участников:

- ЭП уполномоченного лица МО:
  - ЭП руководителя МО;
  - ЭП главного бухгалтера МО.
- ЭП юридических лиц:
  - ЭП МО;
  - ЭП ФСС.

Электронные подписи уполномоченных лиц аналогичны собственноручным подписям данных лиц и подтверждают факт формирования электронного документа конкретным участником.

ЭП МО подписывается любой запрос от МО к Системе учета ЭРС, включая:

- запрос на получение номера ЭРС (формирование ЭРС);
- запрос на получение данных по сформированному ЭРС;
- запросы на предоставление данных по Талонам 1, 2, 3-1 и 3-2 ЭРС от МО в Систему;
- ЭП МО накладывается на совокупность данных по одному Талону ЭРС, при этом сообщение, отправляемое в Систему, может одновременно содержать сведения по нескольким Талонам ЭРС и в этом случае необходимо наличие нескольких подписей МО в сообщении, каждая из которых будет соответствовать данным отдельного Талона;
- запрос на предоставление данных по платежным документам от МО в Систему. В данном случае одна ЭП МО накладывается на совокупность данных по одному счету и связанном с ним реестром Талонов;
- запрос на предоставление данных о постановке ребенка (детей) на учет в детской поликлинике от МО в Систему;
- запрос на получение данных по статусу счета;
- запрос на получение данных по переданным ранее Талонам, находящимся в определенном статусе;
- запрос на закрытие ЭРС.

При предоставлении сведений по каждому Талону ЭРС и платежным документам (счет и реестр Талонов) от МО в Систему должны быть предоставлены подписи уполномоченных лиц МО:

- ЭП Руководителя МО (для Талонов и документов на оплату: счет и реестр Талонов);
- ЭП бухгалтера (для счета).

При этом ЭП МО и ЭП руководителя МО действуют на весь набор предоставляемых сведений по одному Талону и документу на оплату, а ЭП главного бухгалтера только на сведения по Счету. Таким образом, со сведениями по одному Талону поступает одна ЭП МО и одна ЭП уполномоченного лица. По сведениям по документу на оплату (счет с включенным в него реестром Талонов) поступает одна ЭП МО и две ЭП уполномоченных лиц.

За достоверность ЭП уполномоченных лиц (руководитель МО, главный бухгалтер) при передаче сведений от МО в Систему отвечает сторона МО.

ЭП ФСС подписывается любое ответное сообщение от Системы в результате взаимодействия с МО:

- текущее состояние ЭРС в системе учета ЭРС или отказ в предоставлении сведений, формируемые как ответ Системы на соответствующий запрос данных сформированного ЭРС;
- номер ЭРС или отказ в предоставлении сведений, формируемые как ответ Системы на соответствующий запрос на предоставление номера ЭРС (формирование ЭРС);
- данные переданных ранее Талонов, находящихся в определенном статусе, или отказ в предоставлении сведений, формируемые как ответ Системы на соответствующий запрос на предоставление данных по переданным ранее Талонам, находящимся в определенном статусе;
- служебное сообщение, содержащее статус приема информации по Талонам ЭРС, данным о постановке ребенка (детей) на учет в детской поликлинике, документам на оплату, формируемое в ответ на предоставление данных по Талонам ЭРС, данным о постановке ребенка (детей) на учет в детской поликлинике и документам на оплату от МО.

На стороне Системы учета ЭРС производится проверка всех ЭП внешних к Системе участников взаимодействия, предоставляющих сведения в Систему или запрашивающих сведения из Системы.

На стороне МО производится проверка ЭП ФСС, передаваемой вместе со сведениями, генерируемыми Системой в ответ на обращение к Системе.

#### **4.1 Шифрование данных**

Для обеспечения конфиденциальности данных при взаимодействии с сервисом применяется шифрование информации в соответствии со следующими стандартами и алгоритмами:

- XML Encryption Syntax and Processing (W3C) – спецификация, описывающая процедуру шифрования данных в формате XML, а также итоговую структуру данных, в которую сохраняется зашифрованный документ.
- шифрование сессионного ключа и данных происходит по алгоритму ГОСТ 28147-89.

Механизм шифрования выглядит следующим образом:

- генерируется сессионный ключ;
- сессионным ключом шифруется тело сообщения;
- сессионный ключ шифруется открытым ключом публичного сертификата получателя сообщения;
- зашифрованный сессионный ключ включается в тело сообщения.

Расшифровка выполняется следующим образом:

- получатель расшифровывает сессионный ключ своим закрытым ключом;
- получатель сессионным ключом расшифровывает тело зашифрованного сообщения.

При взаимодействии с Системой учета ЭРС и МО все сообщения должны быть зашифрованы по указанным стандартам и алгоритмам. Система учета ЭРС принимает на вход зашифрованные сообщения, содержащее внутри себя смысловые сообщения с учетом обеспечения юридической значимости.

##### **4.1.1 Структура зашифрованного сообщения**

Каркас сообщения определен стандартом SOAP и представляет собой следующий XML-документ:

```
<soapenv:Envelope
xmlns:soapenv=«http://schemas.xmlsoap.org/soap/envelope/»>
  <soapenv:Header></soapenv:Header>
  <soapenv:Body></soapenv:Body>
</soapenv:Envelope>
```



Для передачи зашифрованного сообщения в системы учета ЭРС, необходимо, чтобы оно соответствовало структуре SOAP-сообщения. Для этого зашифрованное сообщение поместите внутрь блока Body нового сообщения SOAP.

В соответствии со спецификацией XML Encryption Syntax and Processing (W3C) внутри блока Body формируется следующая структура данных:

```
<xenc:EncryptedData
  xmlns:xenc=«http://www.w3.org/2001/04/xmlenc#»
  Type=«http://www.w3.org/2001/04/xmlenc#Content»
  xmlns:ds=«http://www.w3.org/2000/09/xmldsig#»
  xmlns:sch=«http://gost34.ibs.ru/WrapperService/Schema»
  xmlns:wsse=«http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd»
  xmlns:wsu=«http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd»>
  <xenc:EncryptionMethod
    Algorithm=«urn:ietf:params:xml:ns:cpxmlsec:algorithms:gost28147» />
  <ds:KeyInfo>
    <xenc:EncryptedKey
      xmlns:xenc=«http://www.w3.org/2001/04/xmlenc#»>
      <xenc:EncryptionMethod
        Algorithm=«urn:ietf:params:xml:ns:cpxmlsec:algorithms:transport-gost2001» />
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>...
        </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </xenc:EncryptedKey>
  <xenc:CipherData>
    <xenc:CipherValue>.</xenc:CipherValue>
  </xenc:CipherData>
</xenc:EncryptedData>undefined</SOAP-ENV:Body>undefined</SOAP-ENV:Envelope>
```

**Лист регистрации изменений**

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	Измененных	замененных	новых	аннулированных					