|  |  |  |
| --- | --- | --- |
| **УТВЕРЖДАЮ:** |  | **УТВЕРЖДАЮ:** |
| Заместитель председателя Федерального фонда обязательного  медицинского страхования |  | Директор  ООО «Атлантико ИТ» |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ю.А. Нечепоренко  «\_\_\_\_» \_\_\_\_\_\_\_\_\_ 2015 г. |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ П.М. Бобнев  «\_\_\_\_» \_\_\_\_\_\_\_\_\_ 2015. |

**УНИФИЦИРОВАННАЯ СИСТЕМА ОБРАБОТКИ ИНФОРМАЦИИ В ФЕДЕРАЛЬНОМ И**

**ТЕРРИТОРИАЛЬНЫХ ФОНДАХ ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ**

полное наименование АС

**УСОИ-М**

сокращенное наименование АС

**Руководство администратора удаленного клиента**

**(работа через веб-интерфейс)**

На 17 листах

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **СОГЛАСОВАНО:** |  | | **СОГЛАСОВАНО:** | |
| От ФОМС  Начальник Управления информационно-аналитических технологий  Федерального фонда обязательного  медицинского страхования  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ В.Г. Алексеев/ | |  | | От ООО «Атлантико ИТ»  Руководитель проекта  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Н.Н. Чаев/ | |
|  | |  | |  | |

# АННОТАЦИЯ

Документ является дополнением к ранее выпущенному документу Руководств администратора удаленного клиента. Документ предназначен для использования администраторами УСОИ в ТФОМС, в филиалах ТФОМС, в СМО и в МО.

Документ содержит сведения, необходимые для обеспечения доступа сотрудников в указанных организациях к сайту УСОИ и установления прав их доступа к отчетным формам.

**СОДЕРЖАНИЕ**

[АННОТАЦИЯ 2](#_Toc437282854)

[ГЛОССАРИЙ 2](#_Toc437282855)

[1. Установка удаленного клиента 2](#_Toc437282856)

[1.1. Требования к системному ПО рабочей станции 2](#_Toc437282857)

[1.2. Установка сертификатов Удостоверяющего Центра ФОМС 2](#_Toc437282858)

[1.3. Установка сертификата подлинности клиента 2](#_Toc437282859)

[1.4. Настройка параметров безопасности браузера Internet Explorer 2](#_Toc437282860)

[2. Получение логина и пароля администратора 2](#_Toc437282861)

[3. Вход в веб-интерфейс УСОИ 2](#_Toc437282862)

[4. Администрирование рабочих мест в Веб-сервисе УСОИ-М 2](#_Toc437282863)

[4.1. Создание ролей 2](#_Toc437282864)

[4.2. Создание учетных записей сотрудников 2](#_Toc437282865)

[5. Приложение 1 Возможные проблемы при установке и их решения. 2](#_Toc437282866)

[5.1. Ответ браузера 403 отказано в доступе. 2](#_Toc437282867)

[5.2. Сервис выдает сообщение об устаревшей версии браузера. 2](#_Toc437282868)

# ГЛОССАРИЙ

|  |  |
| --- | --- |
| **Термин** | **Содержание термина** |
| Абонент | организация или подразделение организации, обязанное предоставлять определенные виды отчетности в систему УСОИ-М. Абонентами могут быть территориальные фонды ОМС и их филиалы, филиалы страховых медицинских организаций или сами страховые медицинские организации, действующие в субъектах РФ, а также лечебно-профилактические (медицинские) организации, действующие в субъектах РФ |
| Веб-интерфе́йс УСОИ | интерфейс, посредством которого пользователь взаимодействует с веб-сайтом УСОИ через браузер Интернет. |
| Форма | отчетный документ регламентированной формы и способа заполнения, имеющий установленные сроки и периодичность его представления Абонентом в УСОИ\_М в электронном виде. |
| Сотрудник | пользователь, выполняющий заполнение электронных отчетных (входных) форм Абонентов. Удаленный пользователь может вводить сведения одного или несколько абонентов в соответствии с правами, предоставленными ему администратором системы. Помимо ввода отчетных данных, удаленный пользователь может изменять некоторые идентификационные данные Абонентов, такие как фамилия руководителя организации, контактные телефоны и т.д. |
| Администратор | Сотрудник, имеющий полномочия на управления полномочиями сотрудников своей организации. |
| Токен | компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удаленного доступа к информационным ресурсам и т.д. Как правило, это физическое устройство, используемое для упрощения аутентификации. |
| ПО | аббревиатура, обозначающая - программное обеспечение. Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ |
| ЭЦП | аббревиатура, обозначающая - электронная цифроваяподпись. Электронная подпись предназначена для идентификации лица, подписавшего электронный документ, и является полноценной заменой (аналогом) собственноручной подписи в случаях, предусмотренных законом |

# Установка удаленного клиента

## Требования к системному ПО рабочей станции

На рабочих станциях должны быть установлены:

* MS Windows XP SP3 / Vista SP1; Windows 7 или выше;
* MS Office 2003 или выше;
* MS Internet Explorer 8.0 или выше;
* ЭЦП и действующие X.509 сертификаты открытых подписей, выданные УЦ ФФОМС или записанные на внешний носитель совместимый с CryptoPro CSP (Token, дискета и т.д.);
* обеспечен Интернет доступ к удостоверяющему центру;
* Adobe Reader 9.0 и выше;
* Криптопровайдер, работающий со стандартом ГОСТ 34.10-2001. Проверена работа криптопровайдера КриптоПро CSP версии 3.6 R4 (7777). Пробную лицензию можно скачать по адресу <http://www.cryptopro.ru/downloads>.
* В случае, если предполагается простановка электронной подписи на документах, необходимо, чтобы на Вашем компьютере был разрешен запуск приложений ActiveX. Проверить это можно в Свойствах обозревателя Intenet Explorer;
* КриптоПро ЭЦП Browser plug-in для Windows. Его можно скачать по адресу <http://www.cryptopro.ru/products/cades/plugin/downloads>;
* Сертификаты подлинности УЦ ФОМС и промежуточного центра сертификации ФОМС.

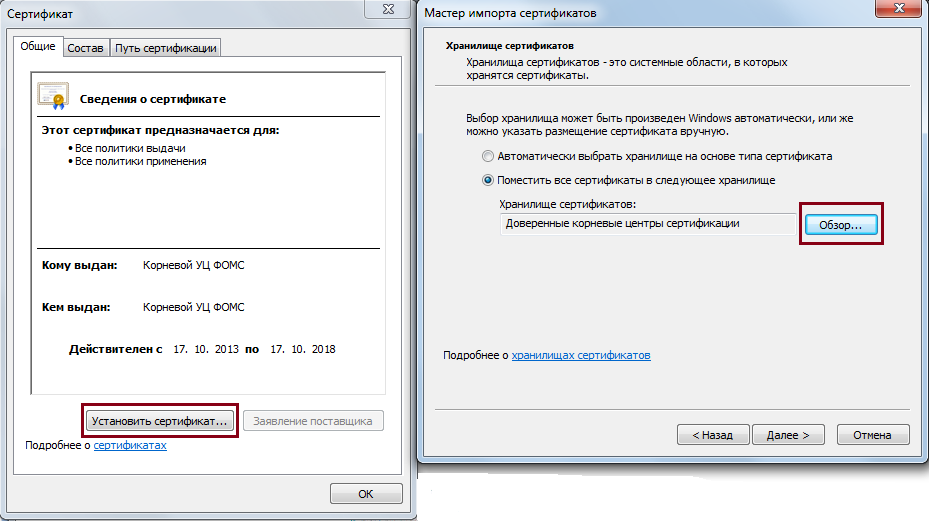
## Установка сертификатов Удостоверяющего Центра ФОМС

Получение и установку сертификатов Удостоверяющего Центра (УЦ) ФОМС и промежуточного центра сертификации следует проводить на каждом рабочем месте, предназначенном для работы с УСОИ-М через ВЕб-сервис.

Работа по получению и установке должна проводиться только через Internet Explorer версии не ниже 8.0.

Первым действием должно быть обращение по адресу <http://ffoms.ru/system-oms/Certification/>. В нижней части страницы, открывшейся по данной ссылке, расположены кнопки для работ с указанными сертификатами. Далее следует:

1. нажать ссылку **Сертификат корневого УЦ** В открывшемся окне нажать кнопку «**Открыть**»**.**
2. В открывшемся окне «Сертификат» нажать кнопку «**Установить сертификат**».
3. В открывшемся окне «Мастер импорта сертификатов» нажимать кнопку «**Далее**» до появления окна с информацией о выборе хранилища (см. снимок ниже). В окне выбрать опцию «**Поместить все сертификаты в следующие хранилища**». Нажать кнопку «**Обзор**» и в списке выбрать пункт «**Доверенные центры сертификации**». Нажать кнопку «**Далее**» и, затем, кнопку «**Готово**».
4. На появившемся сообщении об опасной операции нажать ОК.
5. После появления сообщения об успешном импорте сертификата нажать ОК произойдет возврат в окно «**Сертификат».** Нажать ОК**.**



После нажатия ОК в окне Сертификат произойдет возврат на страницу выбора ссылок на сертификаты.

Далее выбирается ссылка «**Сертификат промежуточного УЦ**» и повторяются все действия, аналогичные описанным выше, с той оговоркой, что вместо пункта «**Доверенные центры сертификации**» следует выбрать пункт «**Промежуточные центры сертификации**».

Следует отметить, что указанные сертификаты привязываются к рабочему месту (компьютеру), но не к сотруднику. Каждый сотрудник должен для работы в УСОИ-М дополнительно иметь личный сертификат подлинности клиента, выданный Удостоверяющим Центром ФОМС. Порядок выдачи и установки такого сертификата описывается ниже.

## Установка сертификата подлинности клиента

Сертификат подлинности клиента необходим только для аутентификации сотрудника при входе в УСОИ-М. Он не влияет на состав функций и прав, открытых для работы внутри этой системы.

Выдача сертификатов подлинности клиента УСОИ-М выполняется в каждом регионе РФ его территориальным фондом ОМС. В территориальном фонде эту функцию выполняет сотрудник, выступающий как представитель УЦ ФОМС, то есть, как лицо, наделенное правами выдачи таких сертификатов.

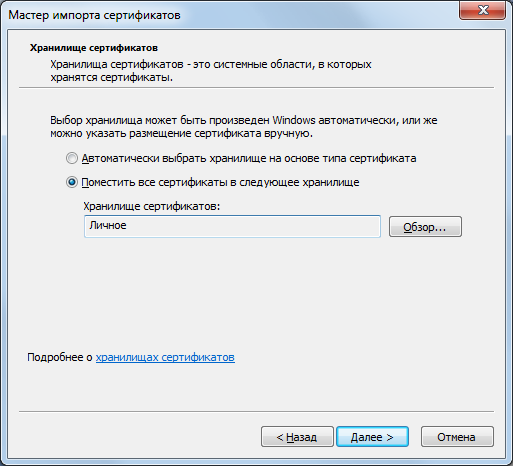
Существуют две формы выдачи сертификата:

* на физическом носителе, к примеру на eToken;
* в виде файла формата «\***.pfx**» (контейнера).

Различия между указанными формами следующие:

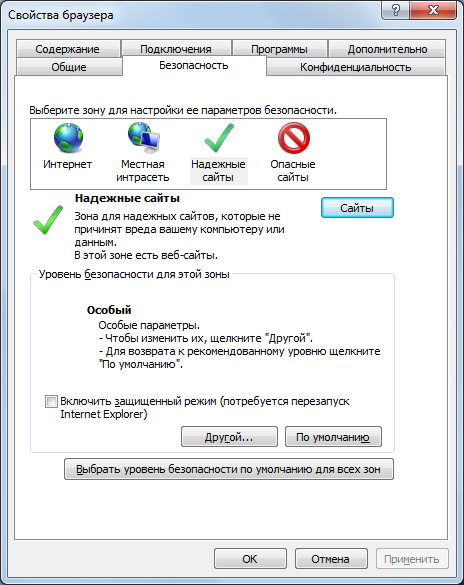
* Внешний носитель можно использовать на любой рабочей станции (он независим от компьютера). Перед работой этот носитель просто вставляется в компьютер и может быть извлечен по её окночании.
* Сертификат, установленный из файла формата «\***.pfx**», привязывается к компьютеру. Тем самым, привязывается к компьютеру и сотрудник. Формально, сертификат из контейнера можно установить (привязать) на нескольких компьютерах, но это не рекомендуемый вариант.

Установке сертификата из файла формата «\***.pfx**» инициируется открытием этого файла в системе Windows. Откроется окно Мастера импорта сертификатов, аналогичное рассмотренному выше. Необходимо выполните те же действия, которые были описаны выше, но при указании хранилища сертификатов необходимо указать хранилище «**Личное**».

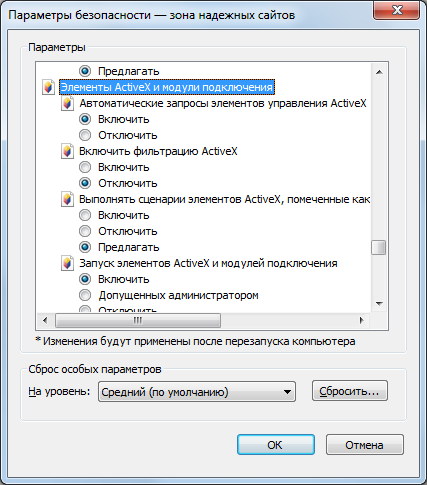


## Настройка параметров безопасности браузера Internet Explorer

Для функционирования электронной подписи документов необходимо разрешить использование элементов ActiveX. Необходимо запустить Internet Explorer и далее выбрать пункт меню **«Сервис»** –>**«Свойства обозревателя».** В открывшемся окне перейдите на вкладку **«Безопасность».**



После этого выберите зону «**Надежные узлы**», нажмите кнопку «**Сайты»** и в открывшемся окне добавьте узел «https://91.226.250.25/», введя этот адрес в верхнее поле. Затем нажмите кнопку «**Добавить»** и «**Закрыть**»**.** Далее в закладке «**Безопасность»** нажмите кнопку «**Другой**». В древовидном списке найдите пункт «**Элементы ActiveX и модули подключения**».



В пунктах «**Выполнять сценарии элементов ActiveX, помеченные как безопасные**» и «**Выполнять сценарии элементов ActiveX, не помеченные как безопасные для использования**» выбрать «**Предлагать**». В пункте «**Запуск элементов ActiveX и модулей подключения**» выбрать «**Включить**». Нажать «**ОК**» и закрыть свойства браузера.

# Получение логина и пароля администратора

Учетная запись нового абонента (организации) одновременно является учетной записью администратора этого абонента. Она создается автоматически при заведении этого абонента в базу данных администратором вышестоящего уровня..

Для администраторов ТФОМС их учетные записи это существующие учетные записи их фондов в УСОИ с их логинами и паролями.

Администраторы филиалов ТФОМС, СМО или МО после ввода их организаций в список абонентов администратором вышестоящего уровня должны, в настоящее время, обратиться за получением логина и пароля к разработчикам. Впоследующем эти сведения им сможет сообщать администратор, добавивший нового абонента в список..

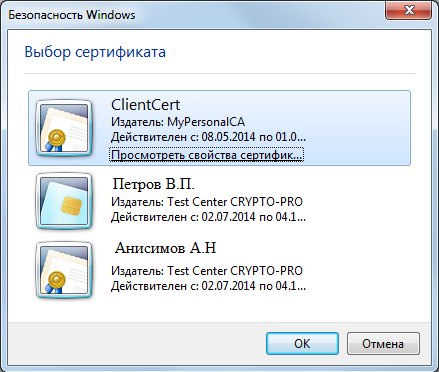
# Вход в веб-интерфейс УСОИ

Обращение любого пользователя, в том числе администратора ТФОМС, происходит одинаковым образом:

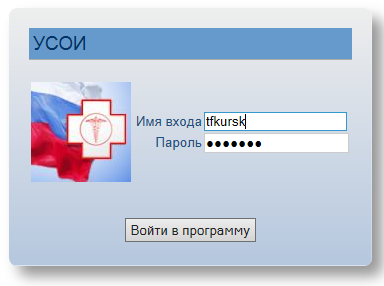
1. Запускается Internet Explorer
2. Если используется eToken, то он должен быть вставлен в компьютер;
3. В поле адреса Интернет набирается строка:

<https://91.226.250.25/>

1. Интернет браузер отобразит диалоговое окно, в котором будут представлены все доступные сертификаты подлинности клиента. Нужно выбрать сертификат, выданный УЦ ФОМС для работы с Веб-интерфе́йсом УСОИ-М.

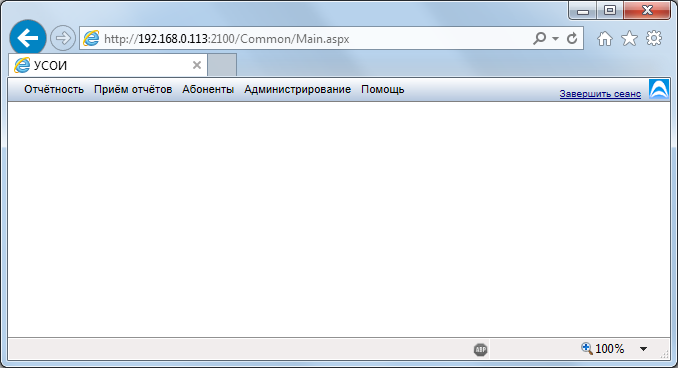


1. Если сертификат прошел проверку, то откроется страница Веб-интерфе́йса УСОИ.



После ввода логина и пароля нажимается кнопка «**Войти в программу**».

При успешном соединении возникает окно основной рабочей области удаленного пользователя УСОИ-М:



Появление данного окна свидетельствует об успешном подключении администратора к УСОИ-М.

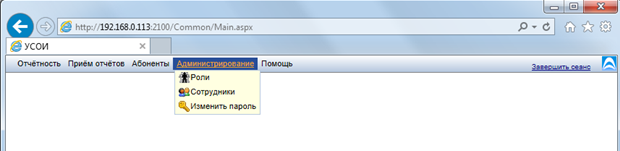
# Администрирование рабочих мест в Веб-сервисе УСОИ-М

Администрирование рабочих мест через веб-сервис производится по единой технологии:

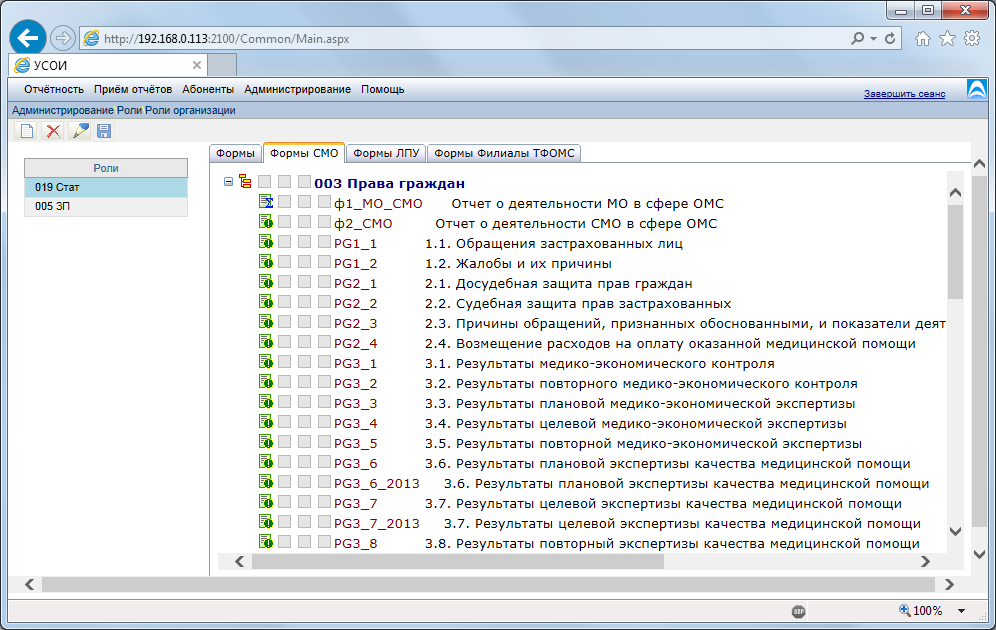
* Создание ролей своей организации;
* Создание учетных записей сотрудников своей организации и указание их прав доступа в системе.

## Создание ролей

Создание или редактирование свойств ролей производится в разделе «**Администрирование – Роли»:**

****

При выборе пункта Роли открывается окно:



В списке ролей, находящемся в правой части окна, можно создавать необходимые роли и указывать им права доступа к разделам видов отчетности или к отдельным формам в этих разделах.

В системе есть предопределенная по правам роль «**Администратор**», которая в списке ролей не указывается..

В целях удобства работы формы разделены на четыре закладки. Первая закладка содержит все формы, в остальных показываются формы, используемые, соответственно, в СМО, ЛПУ и филиалах ТФОМС. Доступ имеет три степени допуска: «**Разрешить чтение формы**», «**Разрешить редактирование формы**» и «**Запретить выходные формы**».

* Запретить выходные формы – полный запрет на работу с формами (запрет на создание и просмотр документов по формам);
* Разрешить редактирование формы – разрешение чтения и редактирования входных форм;
* Разрешить чтение формы – разрешение просмотра входных форм.

Для создания новой роли следует нажать на кнопку  «**Добавить новую роль**». Новой роли можно сразу же указать права работы с документами по формам.

В режиме редактирования роли (по кнопке  «**Редактировать роль**») можно изменить название роли (для этого нужно дважды кликнуть мышью по полю наименования) или. Указать права на формы установкой флажков в дереве форм рядом с именем каждой формы. Если никакие флажки не установлены , то доступ к форме закрыт.

Информация о типе квадратика для установки флажка появляется при наведении курсора мыши на него.

Изменения следует сохранить кнопкой  «**Сохранить изменения**».

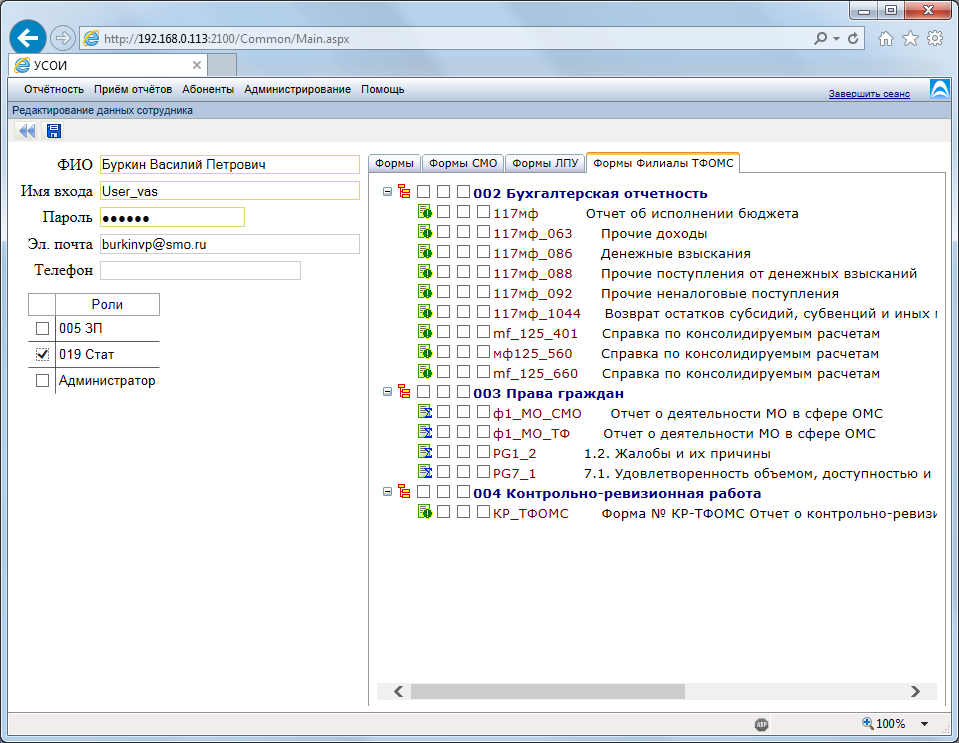
## Создание учетных записей сотрудников

Создание или редактирование записей сотрудников производится в разделе «**Администрирование – Сотрудники».** Список сотрудников представлен в виде таблицы с краткой информацией (тут не приводится).

Запись сотрудника создается нажатием кнопки  «**Добавление нового сотрудника**». В открывшейся форме следует заполнить поля с личными данными и присвоить роль. Ролей может быть несколько в зависимости от поля деятельности сотрудника. Если сотрудник должен иметь индивидуальный доступ, более широкий, чем прав доступа какой-либо роли, то ему, помимо роли, можно выдать дополнительный доступ в древе форм. Данная операция аналогична выдаче прав для роли.

Аналогичные действия выполняются по кнопке  «**Редактирование данных сотрудника**».

Для сохранения данных сотрудника следует нажать кнопку  «**Сохранить изменения**».



Учетная запись сотрудника должна соответствовать следующим требованиям

* ФИО сотрудника должны быть заполнены;
* Имя входа должно быть уникальным;
* Длина пароля не может быть менее 7 знаков;
* Поля «**Электронная почта**» и «**Телефон**» необязательны для заполнения.

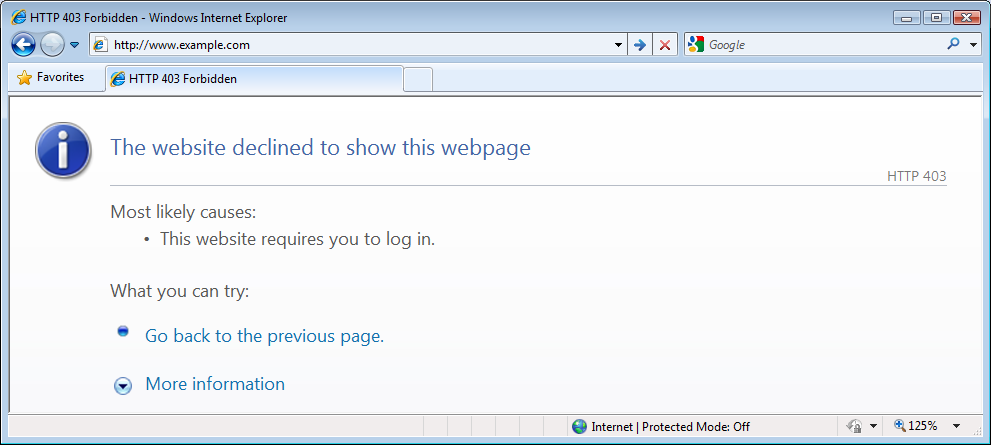
Логин (имя входа) и пароль сотрудника должны быть сообщены ему администратором, установившим их значения.

Сотрудник может поменять свой пароль с помощью раздела **«Администрирование - Изменить пароль».**

Следует отметить, что для каждого типа организации существуют предопределенные в ФОМС группы форм. Администраторы организаций могут присваивать доступ к формам для сотрудников только в рамках этих групп.

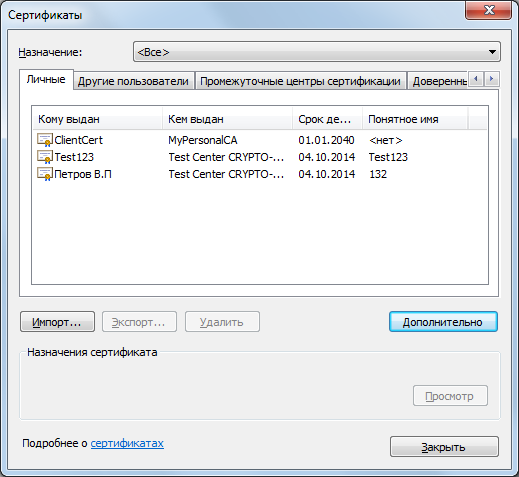
# Приложение 1 Возможные проблемы при установке и их решения.

## Ответ браузера 403 отказано в доступе.



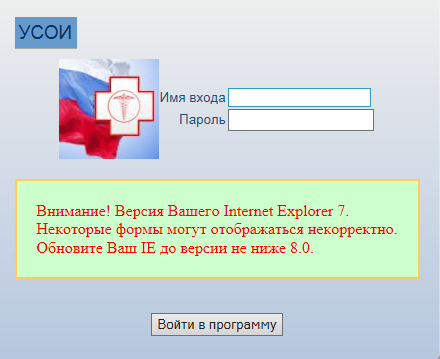
Если возникает такая ошибка при попытке соединения с сервисом, то следует выполнить следующие действия.

1. Убедится, что сертификат попал в раздел личное. Для этого откройте «**Сервис**» - «**Свойства Браузера**». В появившемся окне откройте закладку «Содержимое». В закладке нажать на кнопку «**Сертификаты**». Сертификат, который предполагается использовать для взаимодействия с сервисом должен быть виден в закладке «**Личное**». Если его там нет, то он установлен не правильно.



1. Убедится, что у сертификата есть закрытый ключ. Если сертификат был поставлен в виде файла-контейнера, нужно проверить расширение файла. Закрытый ключ может содержаться только в файле формата «\*.**pfx**». Другие форматы не подходят, и следует обратиться в ТФОМС региона за правильным файлом.
2. Если формат поставки был в виде контейнера формата «\*.**pfx**» или на съемном носителе, то необходимо проверить наличие закрытого ключа в нем. Для этого воспользуйтесь программой «CryptoPro CSP». В ней в закладке «**Сервис**» протестируйте контейнер с сертификатом. В окне результата при положительном результате будет написано о наличии закрытого ключа. В противном случае ключа нет, следует обратиться в ТФОМС региона для получения закрытого ключа. Подробная инструкция по работе с «**CryptoPro CSP**» доступна на сайте КриптоПро или на диске поставки ПО.

## Сервис выдает сообщение об устаревшей версии браузера.



Если при входе в систему выдается такое сообщение, а версия браузера подходит под требования системы, то может стоять режим совместимости. Для его отключения нажмите «**F12**» на клавиатуре и выберите режим отображения «**EDGE»** и режим представления на последнюю версию вашего браузера.