Инструкция по настройке автоматизированного рабочего места для работы в информационной системе Росаккредитации

Листов 12

ООО «Стандарт безопасности»
Ярославль 2013г.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

- Документ предназначен для пользователей, осуществляющих самостоятельную установку программного обеспечения (далее – ПО), необходимого для работы в информационной системе Росаккредитации.

- Для правильной работы необходимо выполнить все пункты данного руководства в указанной последовательности.

- Необходимо обращать особое внимание на примечания помеченные знаком  .

- При несоблюдении данных рекомендаций ООО «Стандарт безопасности» не несет ответственности за корректную работу средств шифрования и ЭП в составе автоматизированного рабочего места (далее – АРМ).

СОСТАВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АРМ

Для настройки АРМ пользователя необходим следующий состав программного обеспечения:

- **Квалифицированная электронная подпись на носителе (eToken GOST, JaCarta GOST, eToken PRO и др.).**
- **Драйвер для работы с соответствующим ключевым носителем (например, eToken PRO).**
- **ПО ViPNet CSP (Допускается использование иного сертифицированного криптопровайдера, например, «КриптоПро CSP»).**
- **ПО ViPNet CryptoFile (Допускается использование другого средства электронной подписи, например, «КриптоАРМ»).**
- **ПО ViPNet Client и файл первичной инициализации абонентского пункта (*.dst) в сети «2936 ФСА»**
- **Специальное ПО (далее – плагин), обеспечивающее работу интернет-обозревателя с Единой системой идентификации и аутентификации (далее – ЕСИА).**

ПОЛУЧЕНИЕ И УСТАНОВКА ViPNet CSP

УСТАНОВКА ДРАЙВЕРОВ ДЛЯ КЛЮЧЕВОГО НОСИТЕЛЯ eToken

НАСТРОЙКА ViPNet CSP ДЛЯ РАБОТЫ С ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Для выполнения этих пунктов, воспользуйтесь инструкцией «Инструкция по настройке рабочего места для работы с ЭП (ViPNet CSP и eToken)», которую необходимо загрузить на сайте www.yarsec.ru в разделе «Удостоверяющий центр» -> «Инструкции» (Рисунок 1)-> «Инструкция по настройке автоматизированного рабочего места для работы с электронной подписью» (Рисунок 2).

Рисунок 1

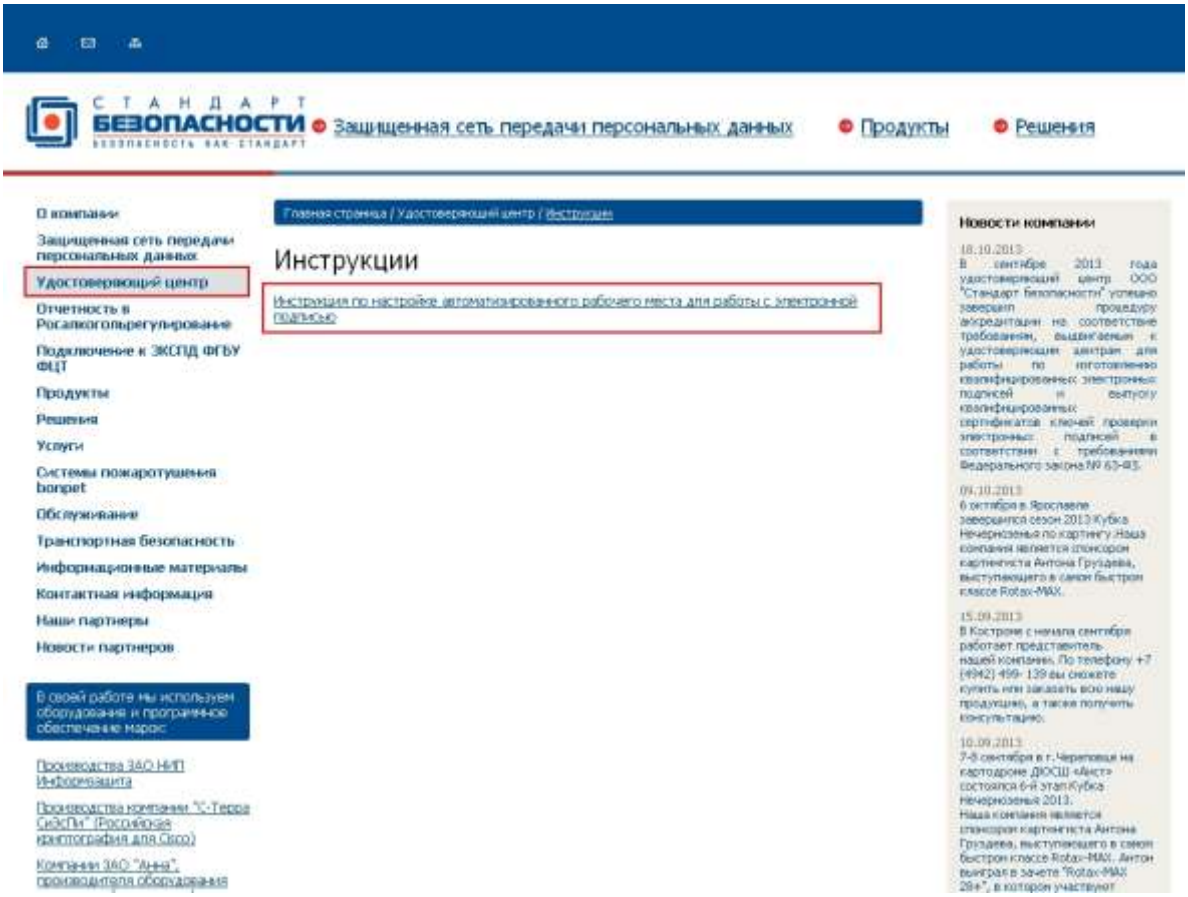


Рисунок 2

Вы должны выполнить все пункты, скаченной инструкции, только после этого продолжить использовать данную инструкцию далее.

РЕГИСТРАЦИЯ В ЕСИА

Для подключения к информационным ресурсам ФГИС Росаккредитации пользователь должен пройти процедуру регистрации в ЕСИА, входящей в инфраструктуру Электронного Правительства.

Для работы с порталом используйте браузер Internet Explorer, входящий в состав Windows, или любой другой (Mozilla Firefox, Google Chrome), скачав его с сайта производителя (Если используется браузер Internet Explorer, следует добавить адрес https://esia.gosuslugi.ru в список надёжных узлов).

Скачайте плагин по ссылке https://esia.gosuslugi.ru/sia-web/htdocs/plugin/CSuserPlugin.exe. Для его установки запустите файл CSuserPlugin.exe и выполните все действия в соответствии с мастером установки (Более подробно этот пункт описан в «Инструкции по настройке автоматизированного рабочего места и работе с квалифицированной электронной подписью на портале Государственных услуг и Государственных закупок», которую можно скачать на сайте www.yarsec.ru в разделе «Удостоверяющий центр» -> «Инструкции» (Рисунок 1).

Ниже описана процедура регистрации в ЕСИА владельца электронной подписи. Подробную информацию по регистрации в ЕСИА можно получить на портале www.gosuslugi.ru или в Росаккредитации (fgis@fsa.gov.ru).

Регистрация пользователей, использующих eToken GOST (JaCarta GOST)

Для прохождения регистрации в ЕСИА достаточно:

- **Вставить ключевой носитель в компьютер;**
- **Зайти на портал http://www.gosuslugi.ru/ и в правой части экрана нажать кнопку «Регистрация» или пройти по адресу https://esia.gosuslugi.ru/sia-web/corp/registration/eds/Index.spr;**
- **Выберите тип регистрируемого лица и нажмите «Далее»;**
- **Подтвердите принятие условий работы с порталом и нажмите «Далее»;**
- **При выборе типа используемого средства электронной подписи выберите пункт «USB-ключ/смарт-карта со встроенным криптопровайдером» (eToken ГОСТ, JaCarta);**
- **Проверьте правильность автоматического заполнения полей из сертификата (при необходимости заполните поля недостающими данными) и нажмите «Далее».**

На этом процедура регистрации завершена. Для входа в личный кабинет используйте кнопку «Вход» на http://www.gosuslugi.ru/, выберите тип авторизации «По USB-ключу/смарт-карте» и введите PIN-код к ключевому носителю (PIN-код для eToken по умолчанию - 123456789).

Регистрация пользователей, использующих eToken PRO или любой другой носитель

Для регистрации необходимо:

- **Вставить ключевой носитель в компьютер;**
- **Зайти на портал http://www.gosuslugi.ru/ и в правой части экрана нажать кнопку Регистрация или пройти по адресу https://esia.gosuslugi.ru/sia-web/corp/registration/eds/Index.spr;**
- **Выберите тип регистрируемого лица и нажмите «Далее»;**
- **Подтвердите принятие условий работы с порталом и нажмите «Далее»;**
- **При выборе типа используемого средства электронной подписи выберите пункт «Средство электронной подписи с программным криптопровайдером» (КриптоПро CSP, LISSI-CSP, ViPNet CSP, Магистра CSP);**
- **В окне выбора сертификата выберите сертификат, выданный УЦ ИИТ, для работы в информационной системе Росаккредитации;**
- **Проверьте правильность автоматического заполнения полей из сертификата (при необходимости заполните поля недостающими данными) и нажмите «Далее».**

На этом процедура регистрации завершена. Для входа в личный кабинет используйте кнопку «Вход» на http://www.gosuslugi.ru/, выберите тип авторизации «Через криптопровайдер / УЭК» и введите PIN-код к ключевому носителю (PIN-код для eToken по умолчанию - 123456789).

Дополнительную информацию по регистрации на портале государственных услуг (в ЕСИА) юридических и физических лиц, а также добавлению сотрудников организации (юридического лица) вы можете получить в отдельном руководстве, размещенном по адресу: http://www.iitrust.ru/downloads/manual/uc/Manual_ESIA_ARM.pdf.

ЭКСПОРТ СЕРТИФИКАТА ЭЛЕКТРОННОЙ ПОДПИСИ ДЛЯ ПЕРЕДАЧИ ВО ФГИС РОСАККРЕДИТАЦИИ.

Для передачи сертификата электронной подписи во ФГИС Росаккредитации необходимо:

- Запустить ViPNet CSP;
- Перейти на вкладку «Контейнеры»;
- Выбрать соответствующий контейнер и нажать «Свойства»;
- В открывшемся окне выделить контейнер и нажать «Сертификат»;
- В окне просмотра сертификата перейдите на вкладку «Состав» и нажмите «Копировать в файл» (Рисунок 3).

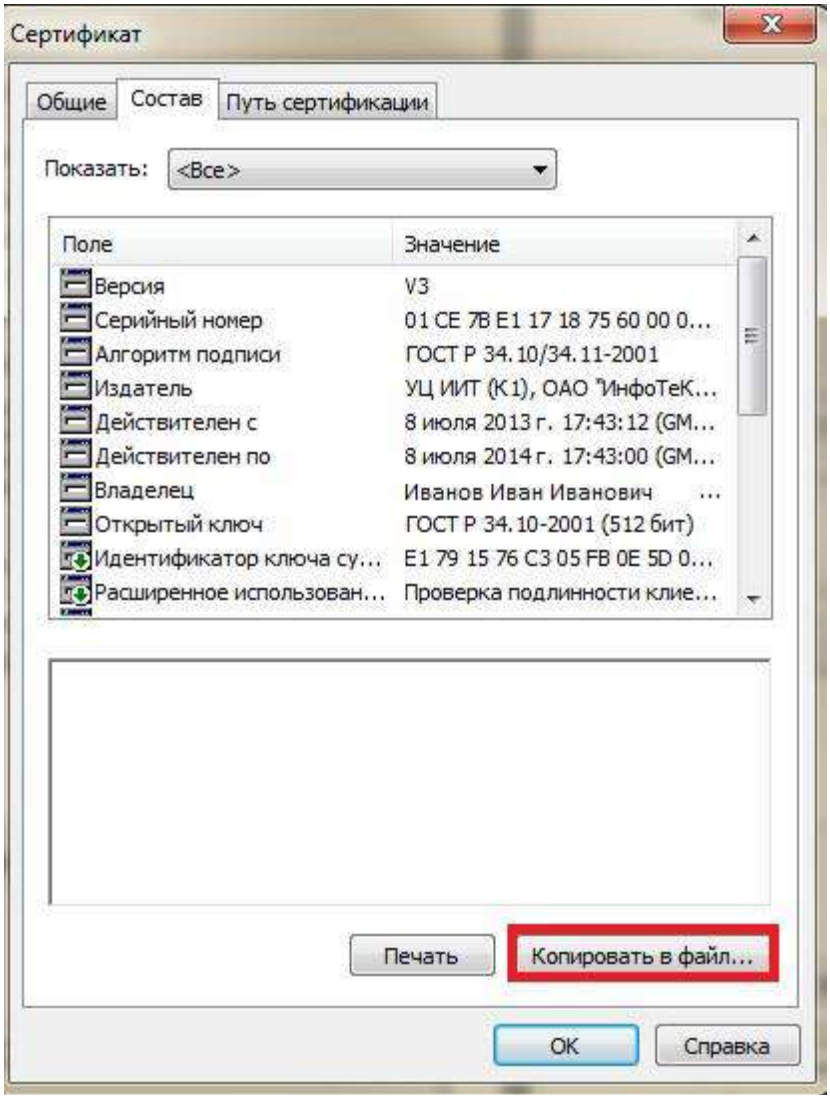


Рисунок 3

- Следуйте инструкциям мастера экспорта сертификатов;
- Сохраните файл сертификата в папку на диске компьютера.

Внимание! Полученный файл сертификата квалифицированной электронной подписи (файл с расширением *.cer) необходимо заархивировать (формат *.zip или *.rar) и отправить на адрес электронной почты fgis@fsa.gov.ru. Название темы письма должно содержать номер аттестата аккредитации и словосочетание «сертификат ЭП». Содержание письма, отправляемого на указанный адрес электронной почты, должно соответствовать заполняемым полям формы запросов http://fsa.gov.ru/public/uploads/usr/Zapros_connect_FGIS.docx, указанных в п. 4.5 Порядка получения доступа информационным ресурсам ФГИС Росаккредитации. В письме так же необходимо указать информацию о количестве рабочих мест, на которых будет устанавливаться легально приобретённое ПО «ViPNet Client 3.x (КС3)».

В ответ на отправленное письмо пользователь должен получить зашифрованный на его сертификате файл(ы) первичной инициализации абонентского пункта (*.dst) в сети «2936 ФСА».

ПОЛУЧЕНИЕ И УСТАНОВКА ViPNet CryptoFile

Для расшифрования полученного от Росаккредитации файла первичной инициализации абонентского пункта (*.dst) в сети «2936 ФСА» рекомендуется использовать ПО ViPNet CryptoFile.

- Загрузите дистрибутив ViPNet CryptoFile по ссылкам

http://iitrust.ru/downloads/cryptofile/ViPNet_CryptoFile_4x86.zip - для установки на 32-х разрядную ОС Windows;

http://iitrust.ru/downloads/cryptofile/ViPNet_CryptoFile_4x64.zip - для установки на 64-х разрядную ОС Windows;

- Запустите установку ViPNet CryptoFile из файла setup_x86.msi или setup_x64.msi;
- Следуйте инструкциям мастера установки;
- После успешной установки ПО – запустите его с рабочего стола или из меню «Пуск»;
- Добавьте полученный от ФГИС Росаккредитации файл в список ViPNet CryptoFile (Рисунок 4)

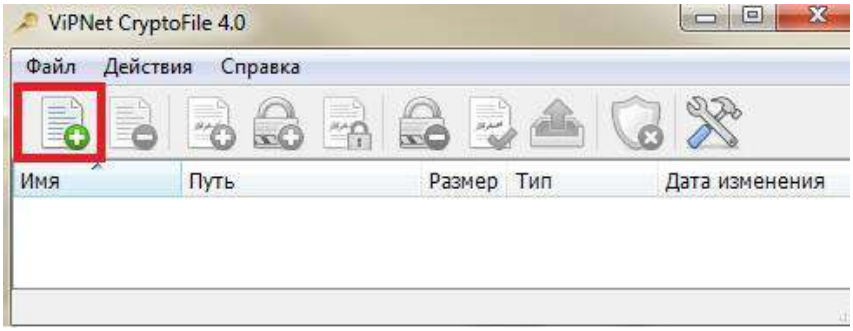
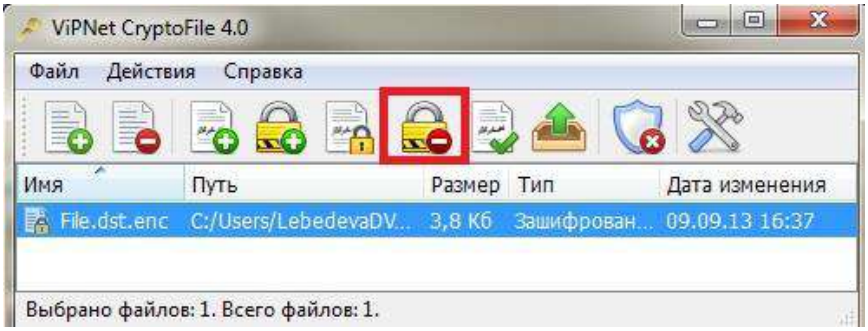


Рисунок 4



Выделите данный файл в списке и нажмите «Расшифровать» (Рисунок 5)

Рисунок 5

- Введите ПИН-код к eToken;
- Убедитесь в успешном завершении операции и нажмите «Закрыть»;
- Расшифрованный файл будет сохранен в той же папке, что и зашифрованный файл.

Внимание! Зашифрованный файл является файлом первичной инициализации абонентского пункта (*.dst) в сети «2936 ФСА», который потребуется для работы с ViPNet Client.

УСТАНОВКА И ИНИЦИАЛИЗАЦИЯ ViPNet Client

Для подключения АРМ пользователей к ФГИС Росаккредитации используется ПО «ViPNet Client 3.x (КС3)».

Для установки ViPNet Client необходимо выполнить следующие действия:

- Запустите файл setup.exe;
- Выполните установку ViPNet Client, следуя инструкциям мастера установки;
- В окне выбора Типа установки выберите Типичная;
- Продолжите установку, следуя инструкциям мастера;
- После окончания установки появится сообщение об успешном завершении установки;
- По результату успешной установки рекомендуется перезагрузить компьютер.

После установки ViPNet Client и перезагрузки компьютера ViPNet Client [Монитор] еще не готов к работе, поскольку еще не установлен набор ключей (dst-файл). Для инициализации ViPNet Client [Монитор] выполните следующее:

- Запустите ViPNet Client [Монитор];
- В окне ввода пароля в правой части кнопки Настройка выберите Первичная инициализация;
- В окне выбора местонахождения дистрибутива ключей нажмите кнопку Обзор и укажите путь к файлу ключевой информации (*.dst).
- Далее следуйте инструкциям мастера установки.

После установки и инициализации ViPNet Client проверьте функционирование защищенного канала связи для подключения к ФГИС Росаккредитации.

Для этого в Интернет-обозревателе введите адрес: http://10.250.4.13/. Страница (Рисунок 6) должна быть доступна (открыться).

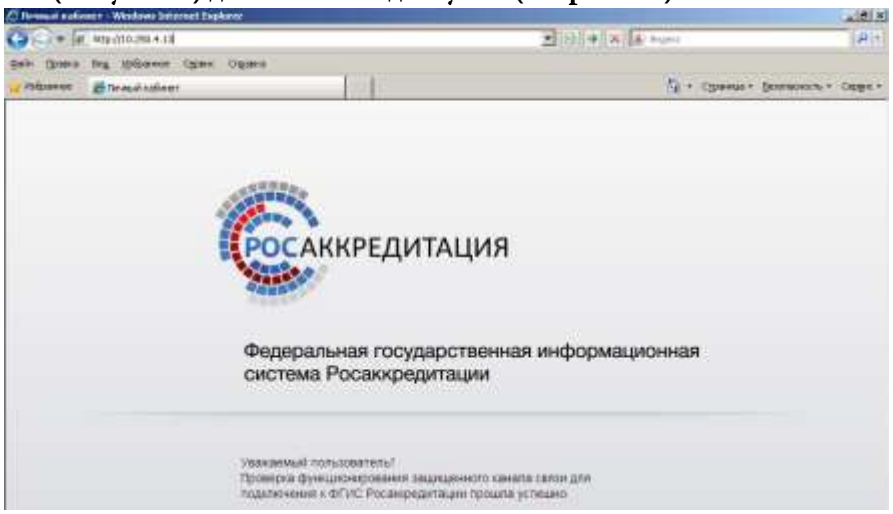


Рисунок 6

Для более подробной информации об установке и настройке ViPNet Client воспользуйтесь «Инструкцией по установке, запуску и первоначальной настройке ПО ViPNet Client», входящей в состав эксплуатационной документации ViPNet.

При необходимости дополнительных настроек ViPNet Client, отвечающих за функционирование абонентского пункта в сети «2936 ФСА» используйте «ViPNet Client [Монитор]. Руководство пользователя», входящей в состав эксплуатационной документации ViPNet.