# Программный комплекс «Web - Смета»

# Инструкция пользователя по настройке и использованию электронной подписи

Версия 1.01

2019 г.

## Оглавление

1.	Аннотация				
2.	Установка средств криптографической защиты информации4				
2	2.1.	Установ	ка КриптоПро CSP	4	
	2.1.	1. Загр	узка дистрибутива программы КриптоПро CSP	4	
	2.1.2	2. Vcm	ановка КриптоПро CSP	10	
	2.1	3. Уст	ановка корневого сертификата	12	
	2.1.4	4. Vcm	ановка личного сертификата	13	
3.	Уст	ановка пл	агина WorkspaceCrypto	14	
2	3.1.	Установи	ка плагина WorkspaceCrypto и приложения WorkspaceCryptoHost	15	
	3.1.	l. Vcm	ановка из интернет-магазина	15	
	3.1.2	2. Офд	рлайн установка	16	
3	3.2.	Установ	ка приложения WorkspaceCryptoHost	17	
3	3.3.	Обновле	ние приложения WorkspaceCryptoHost	19	
4.	Про	верка фун	акционирования механизмов электронной подписи	21	
5.	Исп	ользовани	ие электронной подписи	22	
5	5.1.	Формиро	ование электронной подписи	22	
5	5.2.	Аутенти	фикация с помощью электронной подписи		

#### 1. Аннотация

Настоящий документ «Инструкция пользователя по настройке и использованию электронной подписи» (далее - Инструкция) предназначен для администраторов безопасности и операторов, осуществляющих работу с предметными решениями, разработанными ООО «НПО «Криста» на основе Web-Сметы (далее, Платформа).

В документе описывается порядок действий пользователя направленный на формирование окружения и обеспечение условий работы модуля «Электронная подпись» (далее, МЭП) в предметных решениях (далее, Система).

Функционал МЭП позволяет:

- Создавать/проверять электронную подпись данных в Системе;
- Аутентифицировать пользователей Системы по сертификату ключа электронной подписи.

Для работы с МЭП в общем случае потребуется выполнение следующих действий:

- Скачивание и установка СКЗИ КриптоПро CSP 4.0;
- Скачивание и установка в соответствующие хранилища корневых и промежуточных сертификатов удостоверяющего центра, где была получена подпись;
- Подключение ключевого носителя к компьютеру и установка личного сертификата;
- Скачивание и установка плагина WorkspaceCrypto;
- Установка приложения WorkspaceCryptoHost.

МЭП функционирует в среде Windows/Linux и поддерживается работа в следующих браузерах: применим в следующих браузерах: Mozilla Firefox, Opera, Google Chrome.

#### 2. Установка средств криптографической защиты информации

Для использования МЭП, на рабочем месте должно быть установлено средство криптографической защиты информации (далее, СКЗИ).

Платформа поддерживает работу СКЗИ КриптоПро CSP (см. Установка КриптоПро CSP).

СКЗИ обеспечивает выполнение следующих функций:

- авторизация и обеспечение юридической значимости электронных документов при обмене ими между пользователями посредством использования процедур формирования и проверки электронной подписи;
- обеспечение конфиденциальности и контроля целостности информации;
- создание и управление ключевой информацией.

## 2.1. Установка КриптоПро CSP

#### 2.1.1. Загрузка дистрибутива программы КриптоПро CSP

- 1. Открыть главную страницу сайта ООО КРИПТО-<br/>ПРО <a href="https://www.cryptopro.ru/">https://www.cryptopro.ru/;</a>
- 2. Авторизоваться на сайте, введя в форму аутентификации e-mail (логин) и пароль пользователя (См. Рисунок 1):

Вход						
E-mail: *						
Пароль / Pass	Пароль / Password: *					
Вход	Регистрация Забыли пароль?					

#### Рисунок 1. Форма аутентификации КриптоПро

Если пользователь не зарегистрирован, то необходимо выполнить процедуру регистрации на сайте ООО КРИПТО-ПРО.

3. Открыть «Центр загрузки КриптоПро».

(!)

**Примечание.** Страница «Центра загрузки КриптоПро» находится на сайте ООО КРИПТО-ПРО, доступна по адресу: <u>https://www.cryptopro.ru/downloads</u>



**Примечание.** Функционал работы с «Центром загрузки КриптоПро» доступен после авторизации на сайте ООО КРИПТО-ПРО - <u>https://www.cryptopro.ru/</u>.

4. Выбрать пункт «КриптоПро CSP»

КРИПТОПРО	Ключевое сл	тоПро	рмации
О компании   Продукты	Услуги	Партнёры	Поддержка
<sup>главная</sup> Центр загрузки			
Перейти к загрузке файлов > <u>КриптоПро CSP</u>	а для указа	нного продукта	a:
КриптоПро УЦ			

Рисунок 2. Страница «Центр загрузки»

Будет выполнен переход на страницу с лицензионным соглашением для продукта КриптоПро CSP.

5. После ознакомления с лицензионным соглашением для продолжения загрузки дистрибутива необходимо нажать кнопку «Я согласен с Лицензионным соглашением. Перейти к загрузке»:

Использование программного обеспечения регламентируется приведенным ниже Лицензионным соглашением с ООО "КРИПТО-ПРО": ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ С ЛИЦЕНЗИОННЫМ СОГЛАШЕНИЕМ НА ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ 1. Исключительные права на программу для ЭВМ, включая документацию в электронном виде, (далее - Изделие) принадлежат ООО «КРИПТО-ПРО», далее -Правообладатель. 2. Настоящее соглашение является офертой ООО «КРИПТО-ПРО» к физическому или юридическому лицу, далее - Пользователь. 3. Пользователь в соответствии с настоящим соглашением получает право использовать Изделие на территории Российской Федерации. 4. Установка Изделия в память ЭВМ рассматривается как безусловное согласие Пользователя с условиями настоящего соглашения. 5. В случае несогласия с каким-либо из условий настоящего соглашения Пользователь не имеет права продолжать установку Изделия в память ЭВМ, а в Ŧ случае установки Изделия в память ЭВМ обязан удалить Изделие из ЭВМ. Я согласен с Лицензионным соглашением. Перейти к загрузке.

Рисунок 3. Лицензионное соглашение продукта КриптоПро CSP

6. После нажатия на кнопку «Я согласен с Лицензионным соглашением. Перейти к загрузке» будет осуществлен переход на страницу с перечнем дистрибутивов доступных для загрузки:



Рисунок 4. Страница с перечнем дистрибутивов для загрузки

7. Необходимо выбрать последнюю сертифицированную версию КриптоПро CSP, соответствующую операционной системе установленной на рабочем месте пользователя (Windows, либо Linux). После выбора версии дистрибутив программы будет загружен на компьютер пользователя.

**Примечание.** При выборе ссылки «Windows» будет загружен исполняемый файл «CSPSetup.exe». При выборе Linux в зависимости от установленного менеджера пакетов и разрядности ОС (32-разрядная или 64-разрядная) необходимо загрузить либо \*.deb (x86/x64) либо \*.rpm (x86/x64). После выбора установочного пакета будет загружен архив. Пример загружаемого файла 64-разрядной системы с менеджером пакетов dpkg: linux-amd64\_deb.tgz **Примечание.** Установка дистрибутива КриптоПро CSP должна производиться пользователем, имеющим права администратора.

1. Установка КриптоПро CSP начинается с запуска, скачанного на предыдущем шаге дистрибутива программы. Перед запуском мастера установки выводится диалоговое окно, в котором доступен выбор уровня защищенности (параметр Дополнительные опции):

	×
😥 КриптоПро CSP 4.0.9963	
Благодарим за выбор КриптоПро CSP.	
Продолжая установку, вы принимаете условия Лицензионного соглашения.	
Продукт будет установлен с временной лицензией на 3 месяца.	
http://www.cryptopro.ru	
Установить (рекомендуется)	
Продукт будет установлен в конфигурации КС1 и языком операционной системы с настройками по умолчанию.	
→ Дополнительные опции	
Позволяет выбрать конфигурацию КС и язык.	
🗹 Установить корневые сертификаты	

Рисунок 5. Страница мастера установки в ОС Windows 10

Укажите требуемый уровень безопасности, если он отличается от значения по умолчанию.

Для Linux необходимо распаковать архив и установить компоненты. Пример порядка установки для Ubuntu:

sudo dpkg -i ./lsb-cprocsp-base\_4.0.9963-5\_all.deb sudo dpkg -i ./lsb-cprocsp-rdr-64\_4.0.9963-5\_amd64.deb sudo dpkg -i ./lsb-cprocsp-kc1-64\_4.0.9963-5\_amd64.deb sudo dpkg -i ./lsb-cprocsp-capilite-64\_4.0.9963-5\_amd64.deb sudo dpkg -i ./lsb-cprocsp-kc2-64\_4.0.9963-5\_amd64.deb sudo dpkg -i ./cprocsp-rdr-gui-gtk-64\_4.0.9963-5\_amd64.deb

Подробно процесс установки дистрибутива описан в документации КриптоПро CSP:

- ЖТЯИ.00087-03 92 01. КриптоПро CSP. Инструкция по использованию СКЗИ под управлением ОС Windows. 2018. С. 5;
- ЖТЯИ.00087-03 91 03. СКЗИ КриптоПро СЅР. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux. 2018. С. 7.

**Примечание.** Документация КриптоПро CSP доступна по адресу: <u>https://www.cryptopro.ru/products/csp/downloads</u> и содержится в разделе соответствующей версии приложения выбранного пользователем.

**Примечание.** При установке программного обеспечения «КриптоПро CSP» без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер с бланка лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).

(!)

**Пример.** Установка лицензии в Linux: Перейти в рабочий каталог программы: cd /opt/cprocsp/sbin/amd64/ Установить лицензию: ./cpconfig -license -set XXXXX-XXXXX- XXXXX- XXXXX-XXXXX

#### 2.1.3. Установка корневого сертификата

В зависимости от принятой в организации политики безопасности в целях обеспечения контроля доверенности сертификатов открытых ключей, при использовании СКЗИ под управлением ОС Windows/Linux, может потребоваться установка корневого сертификата в доверенное хранилище.

Корневой сертификат предоставляется соответствующим удостоверяющим центром, выбранным для формирования электронной подписи.

Для Windows установка сертификатов осуществляется с помощью мастера импорта сертификатов.

Для Linux пример установки корневого сертификата, промежуточных сертификатов и списка отзывов:

Переходим в рабочий каталог: cd /opt/cprocsp/bin/amd64 ./certmgr -inst -file [path\_to\_file]/certnew.cer -store uRoot ./certmgr -inst -all -file [path\_to\_file]/certnew.p7b -store uRoot ./certmgr -inst -crl -store uRoot -file [path\_to\_file]/certcrl.crl

Подробнее порядок установки корневого сертификата описан в документе:

- Для ОС Windows ЖТЯИ.00087-03 92 01. КриптоПро CSP. Инструкция по использованию, ч. 4.3., С. 56;
- Для ОС Linux ЖТЯИ.00087-03 93 02. Приложение командной строки для работы с сертификатами, ч. 2., С. 7.



**Примечание.** Корневые и промежуточные сертификаты устанавливаются автоматически в соответствующие хранилища, если на этапе «Установка личного сертификата» сертификат устанавливается с помощью панели управления СКЗИ КриптоПро CSP, при условии что они содержатся в контейнере закрытого ключа.

#### 2.1.4. Установка личного сертификата

Для работы с МЭП необходимо установить пользовательский сертификат в локальное хранилище и создать ссылку, которая будет однозначно связывать сертификат с личным ключом пользователя.

Для Windows установка личного сертификата осуществляется через панель управления СКЗИ КриптоПро CSP.

Для Linux пример установки личного сертификата:

Пример для тестового контейнера и HDIMAGE: Скачиваем тестовый контейнер сертификат УШ и с тестового (https://www.cryptopro.ru/certsrv/) и распаковываем. Копируем контейнер с закрытым ключем в HDIMAGE: cp ./le-820ae.000 -R /var/opt/cprocsp/keys/\$USER/ Переходим в рабочий каталог: cd /opt/cprocsp/bin/amd64 Связываем сертификат и контейнер (пароль для контейнера 12345678): ./certmgr -inst store uMy -file [path\_to\_file]/And.cer -cont '\\.\HDIMAGE\le-820aed1b-8eb2-4d3b-a02e-9b65f7682ac5' Смотрим список сертификатов хранилища Му: ./certmgr -list -store иМу

Порядок установки личного сертификата описан в документе:

- Для ОС Windows ЖТЯИ.00087-03 92 01. КриптоПро CSP. Инструкция по использованию, ч. 2.5.2., С. 33;
- Для ОС Linux ЖТЯИ.00087-03 93 02. Приложение командной строки для работы с сертификатами, ч. 2., С. 7.

## 3. Установка плагина WorkspaceCrypto

WorkspaceCrypto является плагином для веб-браузера, благодаря которому у пользователя появляется возможность подписывать документы электронной подписью. Плагин обеспечивает возможность аутентифицироваться в приложении по сертификату ключа электронной подписи.

Плагин WorkspaceCrypto применим в следующих браузерах:

- Mozilla Firefox
- Opera
- Google Chrome

Плагин WorkspaceCrypto загружается из интернет-магазина соответствующего браузера. В исключительных ситуациях, когда плагин не доступен в интернетмагазине, загрузка осуществляется: https://www.ssksoft.ru/public/WorkspaceCrypto/latest/browser-extensions.zip.

Установка плагина будет выполнена на примере браузера Google Chrome. Установка плагина на других браузерах происходит аналогичным образом с учетом специфики этих браузеров.

WorkspaceCrypto использует нативное приложение WorkspaceCryptoHost для взаимодействия для Windows CryptoAPI. WorkspaceCryptoHost – это хост-приложение, которое обеспечивает подписание ЭП посредством провайдеров Крипто-про CSP и VipNet CSP. Реализует поддержку алгоритмов цифровой подписи «XMLDSig» и «CMS detached». Для корректной работы приложения необходимо наличие установленного в системе крипто-провайдера (КриптоПро).

**Примечание.** Если плагин WorkspaceCrypto и приложение WorkspaceCryptoHost установлено, то необходимо перейти в раздел 4. Наличие установленных плагинов проверяется в браузере на странице «Расширения». Наличие установленных приложений в «Параметры Windows» в разделе «Приложения и возможности» для OC Windows 8+ или в меню «Программы и компоненты» для более ранних версий OC Windows.

## 3.1. Установка плагина WorkspaceCrypto и приложения WorkspaceCryptoHost

#### 3.1.1. Установка из интернет-магазина

Для установки плагина необходимо выполнить следующие шаги:

- 1. Запустить браузер.
- 2. Открыть интернет-магазин:
  - a. для Google Chrome <u>https://chrome.google.com/webstore/</u>
  - b. для Mozilla Firefox https://addons.mozilla.org/ru/firefox/
  - с. для Opera <u>https://addons.opera.com/ru/</u>
- 3. В строке поиска расширений ввести название плагина WorkspaceCrypto. Выполнить поиск. В результате поиска будет найдено расширение WorkspaceCrypto.
- 4. На странице будет доступна кнопка добавления расширений в браузер

Установить . Для установки плагина нажимаем кнопку «Установить», далее браузер без участия пользователя установит расширение. После установки в меню браузера будет добавлена кнопка . Восклицательный знак в красном треугольнике означает, что на РМ не установлено приложение WorkspaceCryptoHost. Порядок установки приложения описан в разделе 3.2. Установка приложения WorkspaceCryptoHost.

#### 3.1.2. Оффлайн установка



**Примечание.** Для плагина WorkspaceCrypto установленного оффлайн не доступно автоматическое обновление. В таком случае обновление производится пользователем вручную, в соответствии с инструкциями, описанными в текущем разделе.

Для установки плагина необходимо выполнить следующие шаги:

1. Скачатьархивсдистрибутивамиплагина:https://www.ssksoft.ru/public/WorkspaceCrypto/latest/browser-extensions.zip.

(!)

Примечание. В архиве содержится несколько файлов:

workspacecrypto-1.0-chrome.crx — файл установки для браузера Chrome workspacecrypto-1.0-firefox.zip — архив с файлами установки для браузера FireFox workspacecrypto-1.0-opera.crx - файл установки для браузера Chrome

- 2. Запустить браузер.
- 3. Открыть страницу «Расширения» (chrome://extensions/).
- 4. Включить «Режим разработчика»:



Рисунок 6. Флаг-галка включения параметра «Режим разработчика»

- 5. Распаковать apxub browser-extensions.zip полученный на шаге 1.
- 6. Перетащить файл workspacecrypto-1.0-chrome.crx на страницу расширений браузера и подтвердить установку приложения:



Рисунок 7. Окно подтверждения установки приложения

После установки в меню браузера будет добавлена кнопка « Восклицательный знак в красном треугольнике означает, что на РМ не установлено приложение WorkspaceCryptoHost. Порядок установки приложения описан в разделе 3.2. Установка приложения WorkspaceCryptoHost.

## 3.2. Установка приложения WorkspaceCryptoHost

1. После установки плагина осуществляется автоматическая проверка на наличие установленного приложения WorkspaceCryptoHost. Если приложение не установлено, то пользователю будет предложено установить его:



Рисунок 8. Ссылка на дистрибутив приложения WorkspaceCryptoHost

- 2. Далее, в окне уведомления необходимо нажать кнопку **ок**, после чего будет загружена последняя версия приложения WorkspaceCryptoHost.
- 3. Запустить загруженный инсталлятор WorkspaceCryptoHost.exe. Откроется окно мастера установки:

🕞 Установка — WorkspaceCryptoHost	_			×
Выбор папки установки В какую папку вы хотите установить WorkspaceCryptoHost?				
Программа установит WorkspaceCryptoHost в следующу	ую п	апку.		
Нажмите «Далее», чтобы продолжить. Если вы хотите выбрать нажмите «Обзор».	» дру	гую г	апку,	
WorkspaceCryptoHost		<u>О</u> бз	op	]
требуется как минимум 4,4 Mb свободного дискового пространс	тва.			
<u>Д</u> алее	>		Отме	на

Рисунок 9. Окно мастера установки приложения WorkspaceCryptoHost

В мастере установки все параметры принимаются по умолчанию. После установки приложения WorkspaceCryptoHost кнопка приложения в меню браузера должна принять следующий вид «

## 3.3. Обновление приложения WorkspaceCryptoHost

Для обновления установленного приложения WorkspaceCryptoHost необходимо выполнить следующие шаги:

1. Удалить хост-приложение с компьютера через панель управления: Панель управления\Программы\Программы и компоненты:



Рисунок 10. Программы и компоненты. Удаление хост-приложения.

2. Выбрать в контекстном меню плагина пункт «Скачать хост-приложение»:



Рисунок 11. Контекстное меню плагина

Выполнится автоматическая загрузка инсталлятора последней версии приложения WorkspaceCryptoHost.

3. После того как будет выгружен инсталлятор приложения WorkspaceCryptoHost необходимо вернуться к шагу «3» пункта «3.2. Установка приложения WorkspaceCryptoHost» Инструкции.

# 4. Проверка функционирования механизмов электронной подписи

Проверить корректную установку окружения необходимого для работы электронной подписи можно на тестовой странице: https://www.ssksoft.ru/workspacecryptotest/

На странице отображается следующая информация:

- Сведения о плагине: установлен/не установлен/версия плагина.
- Установлено или нет хост-приложение и его версию.
- Установлен или нет СКЗИ.
- Какие установлены сертификаты.

Реализована возможность подписания данных с помощью личного сертификата.

Если все настройки были выполнены корректно, то результат проверки на странице будет следующий:

Workspace Сгурто Проверка функционирования электронной подписи
Добро пожаловать!
Страница предназначена для проверки работы WorkspaceCrypto.
Убедитесь, выполнены ли все настройки.
Ваша операционная система: Windows Ваш браузер: Chrome
Плагин включен: Да. Версия 1.0
Хост-приложение установлено: Да. Версия 1.0
Криптопровайдер: Установлен
Установленные сертификаты: 120036986F466FF7DA413BD5EF00010036986F;Установлен;CMS;31.05.2019;31.08.2019

Рисунок 12. Успешное прохождение проверок на тестовой странице

Тестовая страница позволяет определить, на каком этапе возникли проблемы с настройкой окружения.

Пример интерфейса страницы, если плагин не установлен:

Workspace Crypto Проверка функционирования электронной подписи
Добро пожаловать!
Страница предназначена для проверки работы WorkspaceCrypto. Убедитесь, выполнены ли все настройки.
Ваша операционная система: Windows
Ваш браузер: Chrome
Плагин включен: Нет, скачать из <u>магазина приложений</u> или <u>офлайн</u>

Рисунок 13. Интерфейс тестовой страницы: плагин не установлен.

## 5. Использование электронной подписи

## 5.1. Формирование электронной подписи

Формирование электронной подписи осуществляется на запущенном экземпляре Системы. Необходимо открыть интерфейс, для которого включен параметр «Использовать цифровую подпись».



**Примечание.** Интерфейсы, для которых включен параметр «Использовать цифровую подпись» выделяются от остальных тем, что у таких интерфейсов на панели кнопок

будет доступна кнопка 🙎 «Цифровая подпись».

Для наложения электронной подписи необходимо выполнить следующие шаги:

R

1. Для вызова интерфейса «Подпись» необходимо нажать на кнопку «Цифровая подпись».

2. Откроется интерфейс «Новая подпись», на котором отображается информация о подписываемом документе в xml-формате. Для формирования

электронной подписи необходимо нажать кнопку

Подпись	Подпись				
Новая под	пись Текущие подписи				
Описание:	/четная карточка мероприя	ятия №1940 от 23.01.2019	Подп	исать	
Образец до	кумента для подписи:				
xml vers<br <Учетнаяк <Поля> <Дата> <Номер <Номер <ТипМе <ДатаС <Номер <Колич <ДатаН <ДатаО <Ответ <ДатаН <ДатаО <ФондР <Колич <Форма <Класс: Поля <Информ <Записа Поля<br <ДатаС <Лоля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лаля <Лала	on="1.0" encoding="window арточка version="xml-1"> 23.01.2019 Дата >1940 Номер (M>9998/3.2 НомерКМ роприятия>Совместное Т<br изданияЗаписиУК>23.01.20 Плана>9998/00 НомерПл-<br нованиеКМУК>м6 Наимен<br роприятия>Экспертное В<br учалаПроверкиУК>08.01.20 сончанияПроверкиУК>08.01.20 сончанияПроверкиУК>08.01.20 сончанияПроверкиУК>08.01.20 сончанияПроверкиУК>08.01.20 сончанияПроверкиУК>08.01.20 сончанияПроверкиУК>08.01.20 сончанияПроверкиУК>08.01.20 сончанияПроверкиУК>08.01.20 сончанияПроверкиУК>08.01.20 сончанияПроверкиУК>08.01.20 сончанияПроверкиУК>08.01.20 сончанияПроверки золаПроверкиУК>08.01.20 сончанияПроверки Зоо1 Класс ацияОбУстраненииНаруше 1> создания>31.05.2019 Дата аСоздания>31.05.2019 Дата асоздания>31.05.201	vs-1251"?> ГипМероприятия> 19 ДатаСозданияЗаписиУК ана> нованиеКМУК> идМероприятия> 19 ДатаНачалаПроверкиУК 1.2019 ДатаОкончанияПроверкиУК вовая инспекция ОтветственнаяИнспекци<br иода>27.01.2019 ДатаНачалаПроверяемогоП<br иода>27.01.2019 ДатаОкончанияПроверя<br РабочегоВремени> твоЧеловек> e ФормаМероприятия ний> атаСоздания>	яУК> ериода> емогоПериода>		
			Закр	ыть	

#### Рисунок 14. Интерфейс «Новая подпись»

3. В окне выбора сертификата для подписи документа необходимо выбрать соответствующий пользователю сертификат.

Бе	Безопасность Windows X					
В	Выберите сертификат					
Д	пя подписи документа					
	CMS					
- L	Издатель: CRYPTO-PRO Test Center 2					
	Действителен с: 31.05.2019 по 31.08.2019					
	Просмотреть свойства сертификата					
Больше вариантов						
	ОК Отмена					

Рисунок 15. Модальное окно выбора сертификата для подписи ДОКУМЕНТА

4. После выбора сертификата для подписи документа будет выведено диалоговое окно, в котором необходимо указать пароль от контейнера с закрытым ключом:

指 Крипт	×	
£	Введите пароль для контейнера "CMS"	0:09:58
		RU
	Пароль:	
🗌 Запом	нить пароль	
	ОК Отмена	

Рисунок 16. Диалоговое окно КриптоПро CSP для ввода пароля от контейнера с закрытым ключом

Для просмотра сведений о подписи документа необходимо открыть закладку «Текущие подписи»:

Подпись	Подпись					
Новая подпись Текущи	е подписи					
$\mathbb{B} \times   \mathbf{g}$						
Время подписи	Пользователь	Описание				
31.05.2019 16:39:27		Учетная карточка мероприятия №1940 от 23.01.2019				
Содержимое подписи		Результат проверки подписи				
Поле	Значение	Проверка подписи прошла успешно				
Действителен с	2019.05.31 11:34:53					
Действителен до	2019.08.31 11:44:53					
Ключ подписи	120036986F466FF7DA413BD5EF0001	0036986F				
Дата подписи	2019.05.31 16:39:28					
Владелец подписи	CMS					
OID алгоритма подписи	1.2.643.7.1.1.2.2					
Состав подписи Ошибки образа						
		Закрыть				

#### Рисунок 17. Интерфейс «Текущие подписи» положительный результат проверки ЭП

В заголовке окна отображается список подписей. Для каждой подписи выводятся сведения о времени подписи, о пользователе Системы выполнившем операцию «Подписать» и сведения о подписанном документе. В детализации «Состав подписи» отображаются сведения о содержимом подписи и результат проверки подписи. В случае успешного подписания документа в параметре «Результат проверки подписи»: «Проверка подписи прошла успешно». Если в результате проверки подписи будут возвращены ошибки, то появится соответствующее сообщение:

Подпись				×		
Новая подпись Текущ	ие подпи	си				
$\mathbb{B} \times \mathcal{C}$						
Время подписи		Пользователь	Описание			
31.05.2019 16:47:52		Caracity (10.0.000)	Учетная карточка мероприятия №1940 от 23.01.2019			
31.05.2019 16:39:27		11-4 (a [10, a.o.2 21]	Учетная карточка мероприятия №1940 от 23.01.2019			
Содержимое подписи				Результат проверки подписи		
Поле	Значен	не		Ошибка проверки подписи: Оригинал документа не соответствует подписанному.		
Действителен с	2019.0	5.31 11:34:53				
Действителен до	2019.0	)8.31 11:44:53				
Ключ подписи	120036	6986F466FF7DA413BD5EF00010036986F				
Дата подписи 2019.05.31 16:47:5		5.31 16:47:51				
Владелец подписи СМS						
Состав подписи Ошибки образа						
				Закрыть		

#### Рисунок 18. Интерфейс «Текущие подписи» ЭП не прошла проверку

Детальная информация об ошибке содержится в детализации «Ошибки образа»:

Подпись				
Новая подпись Текущие подпис	си			
$\mathbb{B} \times \mathcal{C}$				
Время подписи	Пользователь	Описание		
31.05.2019 16:47:52	warm [	Учетная карточка мер	ооприятия №1940 от 23.01.2019	
31.05.2019 16:39:27	Garanas [10:40 - 11]	Учетная карточка мер	ооприятия №1940 от 23.01.2019	
Название узла	Новое значение		Подписанное значение	
Root\УчетнаяКарточка\ОбъектыПро	оверки Узлов: 1		Узлов: 2	
Состав подписи Ошибки образа	a			

#### Рисунок 19. Детализация «Ошибки образа»

## 5.2. Аутентификация с помощью электронной подписи

Для входа в Систему с помощью МЭП необходимо выполнить следующие шаги:

- 1. Загрузить страницу аутентификации Системы.
- 2. Нажать на кнопку «Войти по сертификату»:

Войти по сертификату				
Единая точка входа				
——— или ———				
1.5.drx	$\sim$			
lifet#	~			
Организация:	$\sim$			
Конфигуратор	$\sim$			
Пароль:				
Войти				
Запомнить меня				
1.5.5 CIVE CHOT 20100521 1010 (D.D.S.SOR. 14 JOINNI)	s			

Рисунок 20. Страница аутентификации Системы

3. В окне выбора сертификата необходимо выбрать соответствующий пользователю сертификат.

Безопасн	Безопасность Windows			
Выберите сертификат				
Для подписи документа				
E	CMS			
Издатель: CRYPTO-PRO Test Center 2				
	Действителен с: 31.05.2019 по 31.08.2019			
	Просмотреть свойства сертификата			
Больше вариантов				
	OK	Отмена		

Рисунок 21. Модальное окно выбора сертификата для подписи документа

4. После выбора сертификата будет выведено диалоговое окно, в котором необходимо указать пароль от контейнера с закрытым ключом:



Рисунок 22. Диалоговое окно КриптоПро CSP для ввода пароля от контейнера с закрытым ключом

5. Далее Система выполняет проверку соответствия выбранного сертификата с данными модуля «Безопасность», в котором содержатся сведения о пользователе и его сертификате. После успешного завершения проверки будет открыт интерфейс Системы в соответствии с выбранным рабочим местом на странице аутентификации.

**Примечание.** Для аутентификации в Системе с помощью ЭП необходимо, что бы на интерфейсе «Пользователи» в модуле «Безопасность» на закладке «Ключ ЭП» для соответствующего пользователя был загружен личный сертификат и включен флаггалка «Доступ разрешен».

🖺 Сохранить + Добавить + 🗡 Удалить +				
Общие настройки Ключ ЭП (	Смета			
Выбрать сертификат				
Серийный номер:	120036986f466ff7da413bd5ef00010036986f			
Владелец (общее имя):	CMS			
Владелец:	C=RU, CN=CMS			
Поставщик (общее имя):	CRYPTO-PRO Test Center 2			
Поставщик:	CN=CRYPTO-PRO Test Center 2, O=CRYPTO-			
Не действителен до:	31.05.2019 11:34:53			
Не действителен после:	31.08.2019 11:44:53			
Отпечаток:	66c9cacc17ce9eab4e356dab469be9bdbff001a			
Доступ разрешен:				

Рисунок 23. Настройка доступа к Системе по ЭП для пользователя в модуле «Безопасность»