УПРАВЛЕНИЕ ФИНАНСОВ АДМИНИСТРАЦИИ ГОРОДА МУРМАНСКА
пр. Ленина,75, г. Мурманск, 183006, тел. (8152) 455652, факс (8152) 458279 E-mail: ufin@citymurmansk.ru
ОКПО 02290226, ОГРН 1025100848904, ИНН 5190800241, КПП 519001001

Инструкция

по установке и использованию ключей электронной подписи, выдаваемых гражданам удостоверяющими центрами ОАО «Ростелеком», в информационной системе управления финансов администрации города Мурманск «Бюджет-Web»

Мурманск
2015

Оглавление

1 Введение

Данная инструкция предназначена для установки и использования ключей электронной подписи, выдаваемых гражданам удостоверяющими центрами ОАО «Ростелеком», в информационной системе управления финансов администрации города Мурманск «Бюджет-Web».

1.1 Общие сведения

В основе формирования Электронной Подписи (ЭП) лежат принципы ассиметричной криптографии, в которой используются пара связанных друг с другом ключей, один из которых называется закрытым (private) и хранится в тайне у владельца, другой же, называемый открытым (public), свободно передается в общем доступе. Предполагается, что пользователь должен владеть известным только ему закрытым ключом из уникальной асимметричной пары ключей. Соответствующий закрытому ключу открытый ключ публикуется в сети для общего доступа. Зная открытый ключ, практически невозможно определить соответствующий ему закрытый.

Для формирования ЭП подписываемый документ подвергается хэшированию (сжатию), а полученный хэш зашифровывается закрытым ключом. По полученному хэшу нельзя восстановить исходный документ, но это и не нужно, поскольку проверка ЭП заключается в сравнении расшифрованной открытым ключом ЭП с хэшем документа. Совпадение гарантирует (с высокой степенью достоверности), во-первых, неизменность (защиту от подделки) документа, и, во-вторых, что его подписал (создал ЭП) владелец закрытого ключа.

Таким образом, ЭП - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Для верификации открытого ключа применяется ***сертификат ключа*** *(сертификат отрытого ключа)* – электронный документ, связывающий открытый ключ с субъектом, правомерно владеющим соответствующим закрытым ключом. Без такой верификации злоумышленник может выдать себя за любого субъекта, подменив открытый ключ.

Для заверения сертификата ключа используется ЭП учреждения, издающего сертификаты – удостоверяющего центра. По набору своих функций удостоверяющий центр – основная компонента инфраструктуры ***открытых ключей*** (PKI - Public key infrastructure). Имея открытый ключ удостоверяющего центра, любой субъект может проверить достоверность изданного удостоверяющим центром сертификата. За достоверность содержащихся в нем данных, идентифицирующих правомерного владельца, отвечает издавший его удостоверяющий центр.

Удостоверяющий центр владеет сертификатом ключа, закрытый ключ которого он использует для заверения издаваемых сертификатов. Также в функции удостоверяющего центра входит ведение списка отозванных (до истечения срока действия) по разным причинам (например, при компрометации закрытого ключа или утрате юридической силы документов, на основании которых он выдан) сертификатов (CRL – Certificate Revocation List). Этот список подписывается ЭП удостоверяющего центра и открыто публикуется. Для каждого отозванного сертификата в списке указываются регистрационный номер, дата и причина отзыва.

Различают подчиненный удостоверяющий центр, сертификат которого издан другим удостоверяющим центром, и корневой удостоверяющий центр, сертификат которого издан им самим. Корневых удостоверяющих центров (независимых друг от друга) может быть несколько.

2 Технические особенности работы ключей ЭП Ростелекома в ИС Бюджет-Web»

Со стороны ИС «Бюджет-Web» предъявляется единственное требование к средствам формирования ЭП – использование криптопровайдеров, совместимых с интерфейсом Microsoft Crypto API 2.0.

Ключи ЭП «Ростелекома» представляют собой электронные USB-носители eToken ГОСТ, выпускаемые компанией «Аладдин», которые изначально предназначены для работы с порталом государственных услуг (http://www.gosuslugi.ru/ru/), но также могут применяться в любых приложениях, использующих технологии инфраструктуры открытых ключей. USB-носитель eToken ГОСТ является персональным устройством, необходимым для формирования ЭП, обеспечивающим гарантированную безопасность операций пользователей за счет применения неизвлекаемых закрытых ключей ЭП и строгой двухфакторной аутентификации.

Ключи ЭП Ростелекома хранят в себе сертификат открытого ключа и закрытый ключ пользователя, выданные Удостоверяющим Центром (УЦ ЭП РТК), являющимся подчиненным корневого Удостоверяющего Центра проекта «Электронное правительство» ОАО «Ростелеком» (УЛ УЦ ЭП РТК).

Для возможности формирования ЭП с использованием ключевой информации, хранящейся на USB-носителе eToken ГОСТ, нужен соответствующий ***криптопровайдер*** – независимый модуль, содержащий библиотеку криптографических функций со стандартизованным интерфейсом. При этом у каждого криптопровайдера есть собственный набор алгоритмов и собственные требования к формату ключей и сертификатов. Помимо этого, для работы с порталом государственных услуг, компания «Ростелеком» записывает ключевую информацию в специализированный контейнер (ГОСТ-апплет), отличный от стандартного места хранения ключевой информации на носителях eToken.

Таким образом, мы получаем ряд требований, предъявляемых к криптопровайдеру, который должен использоваться для формирования ЭП в ИС «Бюджет-Web» с хранимой ключевой информацией на ключах ЭП «Ростелекома», а именно:

- Поддержка интерфейса CryptoAPI 2.0;
- Работа с ключами eToken ГОСТ;
- Возможность работы со специализированным контейнером (ГОСТ-апплетом).

Всем указанным требованиям соответствует криптопровайдер КриптоПРО версии 3.6. Описание настроек КриптоПРО CSP для клиентской части ИС «Бюджет-Web» приведены далее.

3 Рекомендуемая конфигурация рабочих станций

К клиентским местам предъявляются требования (Таблица 1).

Таблица 1

Характеристики рабочих станций

№ п/п	Требования	Параметры
1	Процессор	1.6 ГГц и выше (рекомендуемые требования: 2.2 ГГц и выше)
2	Оперативная память	не менее 512 Мб (рекомендуемые требования: 1024 Мб)
3	Разрешение экрана	Не менее 1024x768
4	Свободное дисковое пространство	Не менее 1Гб
5	Связь	Удаленный доступ: IP соединение, или любое соединение, поддерживающее IP или IPX инкапсуляцию (PPP и т.д.), скорость 14400 bps и выше
	Программное обеспечение	Операционная система: Microsoft Windows XP SP3 и выше, Microsoft Windows Vista SP1 и выше, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows 8.1. Microsoft .NET Framework 3.5 SP1. MS Office 2000 (Word, Excel) и выше или Open Office. КриптоПро CSP 3.6 Драйверы ключей ЭП

4 Настройка программного обеспечения на рабочих станциях пользователей ИС «Бюджет-Web»

Перед выполнением всех операций по настройке программного обеспечения для работы с ЭП и импорту сертификатов ЭП рекомендуется временно отключить работающий на ПК антивирус.

На каждой рабочей станции пользователя ИС «Бюджет-Web» необходимо выполнить следующие настройки:

- проверить правильность настройки браузера для работы клиентской части ИС «Бюджет-Web» в соответствии с «инструкцией по настройке рабочего места пользователя для работы в информационной системе управления финансов администрации города Мурманска «Бюджет-Web»;
- установить драйвер USB-ключа eToken ГОСТ;
- установить криптопровайдер КриптоПРО CSP;
- импортировать сертификаты пользователя;
- проверить формирование ЭП для документов в ИС «Бюджет-Web».

4.1 Проверка настроек браузера

Подробные сведения по настройке браузера содержатся в инструкции пользователя ИС «Бюджет-Web».

Для корректной работы необходимо удостовериться в том, что все необходимые параметры настройки браузера действительны.

4.2 Установка драйвера для USB-носителя eToken ГОСТ

Для возможности работы с USB-ключи eToken ГОСТ в операционной системе семейства Windows требуется установка драйверов. Драйверы доступны для скачивания с сайта производителя – компании «Аладдин» (http://www.aladdin-rd.ru/support/downloads/etoken/) совместно с набором утилит под названием eToken PKI Client.

Внимание! До установки драйвера USB-ключей eToken ГОСТ устанавливать выданные USB-носители eToken в USB-разъем компьютера нельзя.

Существуют версии для 32-х и 64-хбитных систем, которые необходимо устанавливать в зависимости от используемой платформы. Установка драйверов выглядит следующим образом:

- Запустить на выполнение msi-пакет установщика (PKIClient_x32_* или PKIClient_x64_*). В окне приветствия при запуске нажать кнопку **Next>** (Рис. 1):

Рис. 1

- Выбрать язык отображения интерфейса программы «**Russian**» и нажать кнопку **Next>** (Рис. 2):

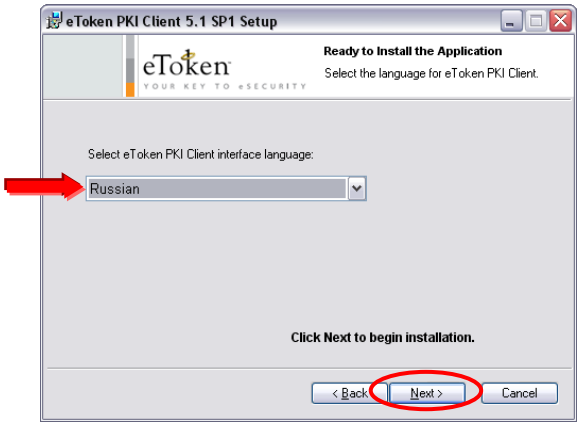


Рис. 2

- Согласиться с лицензионным соглашением, выбрав «**I accept the license agreement**» и нажать кнопку **Next>** (Рис. 3):

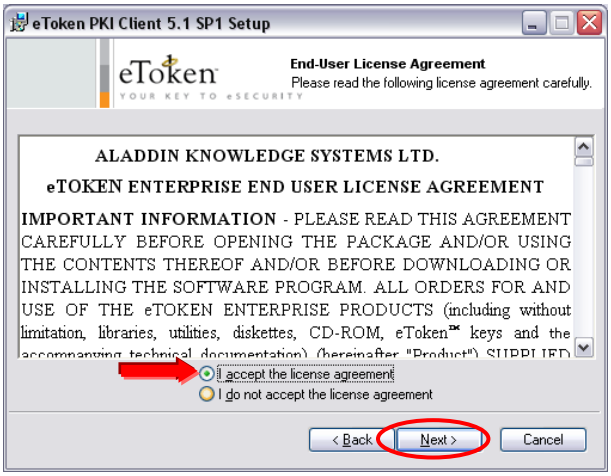


Рис. 3

- Выбрать папку установки или оставить её по умолчанию (рекомендуется) и нажать кнопку **Next>** (Рис. 4):

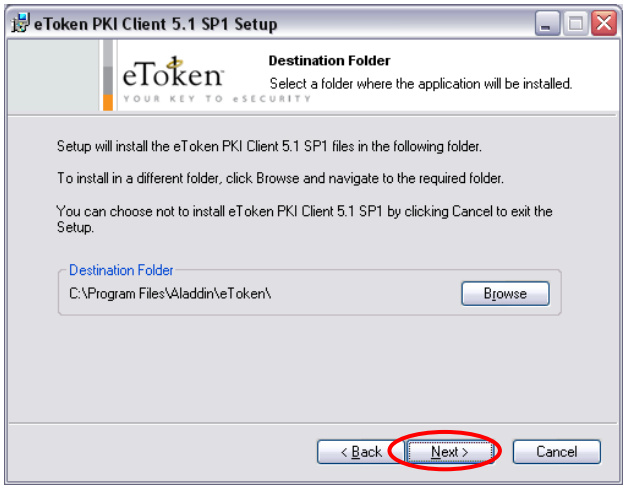


Рис. 4

- По окончании установки нажать кнопку **Finish** (Рис. 5):

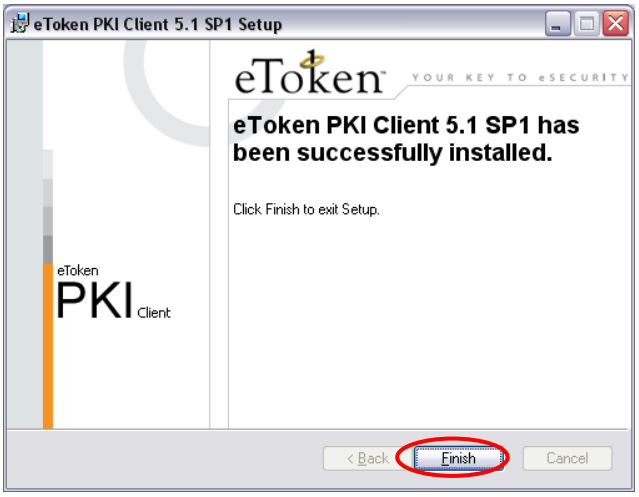


Рис. 5

- После этого можно устанавливать выданный USB-носитель eToken в USB-разъем компьютера. При первом использовании носителя появится окно с запросом на смену пароля для eToken ГОСТ (Рис. 6):

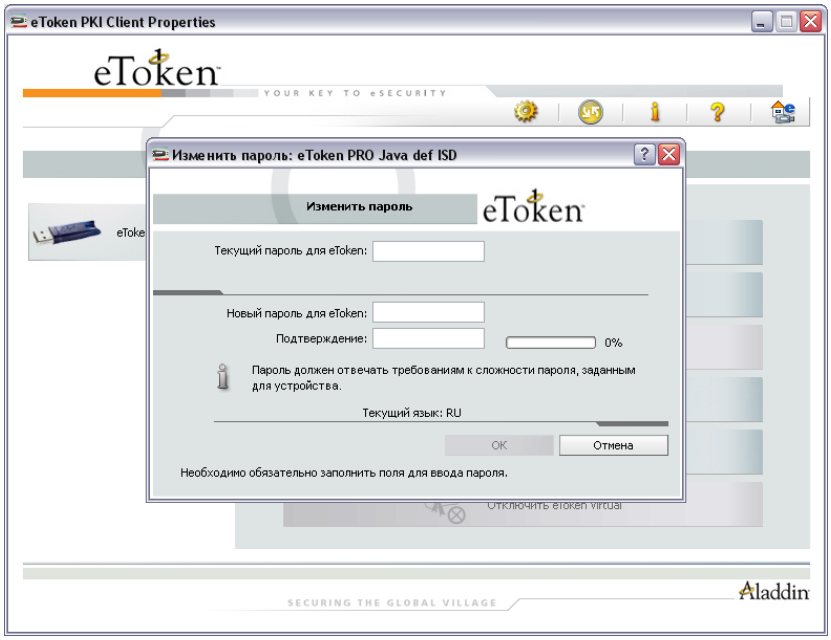


Рис. 6

В случае, если eToken ГОСТ уже использовался для регистрации на сайте государственных услуг (http://www.gosuslugi.ru), то пароль менять нельзя!

4.3 Установка криптопровайдера КриптоПРО CSP

Для установки КриптоПро версии 3.6 воспользуйтесь установочным дистрибутивом программы, поставляемым Управлением Федерального казначейства по Мурманской области (http://old.murmansk.roskazna.ru/page/26877). Этот дистрибутив представляет собой стандартную установку Windows-приложений. Для установки криптопровайдера требуется минимум 20 Мбайт свободного места на системном диске. Запустите мастер установки (Рис. 7**Ошибка! Источник ссылки не найден.**), нажмите кнопку **[Далее >]**.

Во избежание проблем с работой криптопровайдера КриптоПро CSP, настоятельно не рекомендуем устанавливать для совместной работы на одном компьютере ViPNet CSP и КриптоПро CSP.
При необходимости использования обоих криптопровайдеров их следует разносить по разным компьютерам, либо использовать средства виртуализации для запуска каждого из криптопровайдеров на своей виртуальной машине.

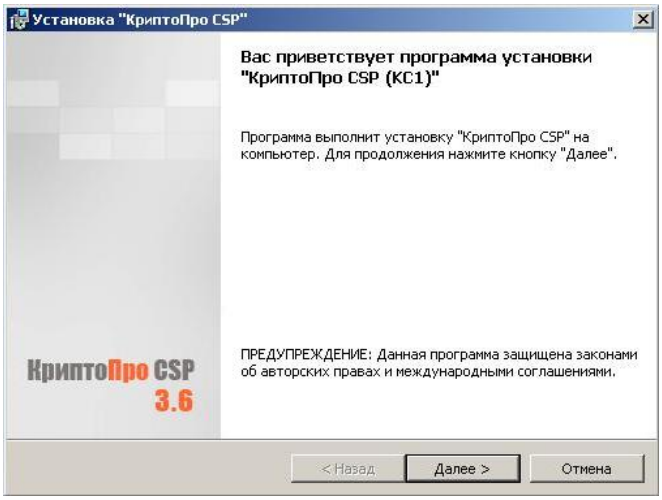


Рис 7. Начало установки СКЗИ «КриптоПро CSP»

В процессе установки введите код лицензии (Рис. 8). При установке программного обеспечения КриптоПро CSP без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия.

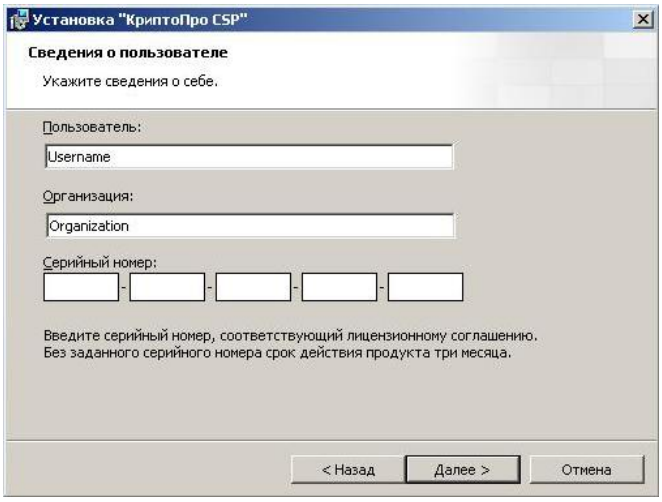


Рис 8. Регистрация информации о лицензионном соглашении

После выбора типа установки «Обычная» в следующем окне нажмите кнопку **[Установить]**.

После окончания установки программы перезагрузите компьютер, чтобы изменения вступили в силу.

4.4 Импорт сертификатов пользователя

Для корректной работы процедур проверки ЭП необходимо выполнить операцию импорта сертификата пользователя:

1. Установить USB-носитель eToken в USB-разъем компьютера.
2. Откройте панель управления компьютером, используя кнопку **Пуск**. В открывшемся окне (Рис. 9) выберите значок **КриптоПро CSP** (Пуск –> Панель управления –> КриптоПро CSP)

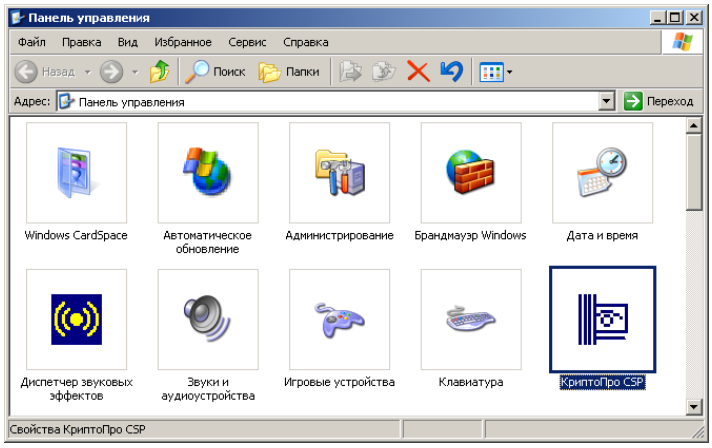


Рис 9. Панель управления

3. Импортировать открытый ключ пользователя:

a. В разделе «**Сервис**» нажать кнопку **Просмотреть сертификаты в контейнере…**(Рис. 10):

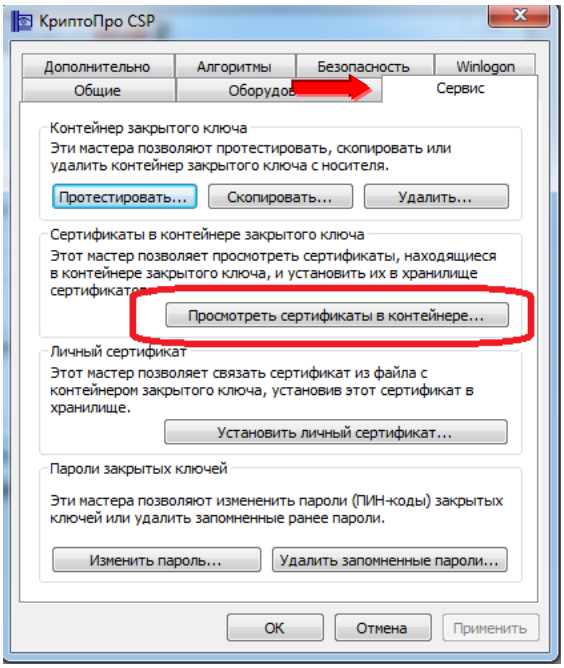


Рис. 10. Выбор контейнера

b. В появившемся окне в разделе «Сертификаты в контейнере закрытого ключа» нажать кнопку **Обзор…** (Рис. 11):

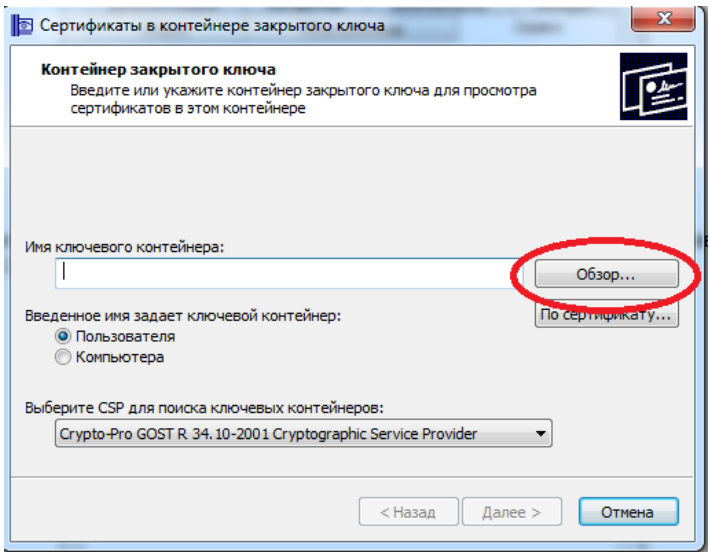


Рис. 11. Выбор закрытого ключа на носителе

c. В открывшемся окне можно увидеть список ключевых контейнеров, подключенных к компьютеру (Рис. 12):

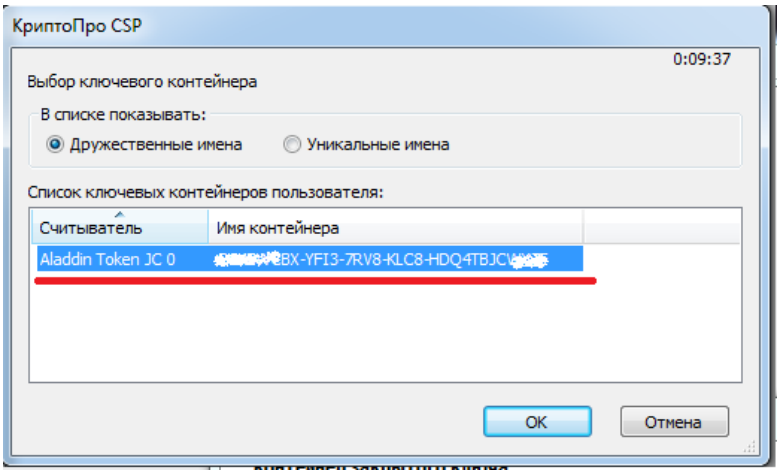


Рис. 12. Список ключевых контейнеров

d. Выбираем контейнер и нажимаем кнопку ОК.

e. Имя ключевого контейнера добавится в соответствующее поле. После этого нажимаем кнопку **Далее** (Рис. 13):

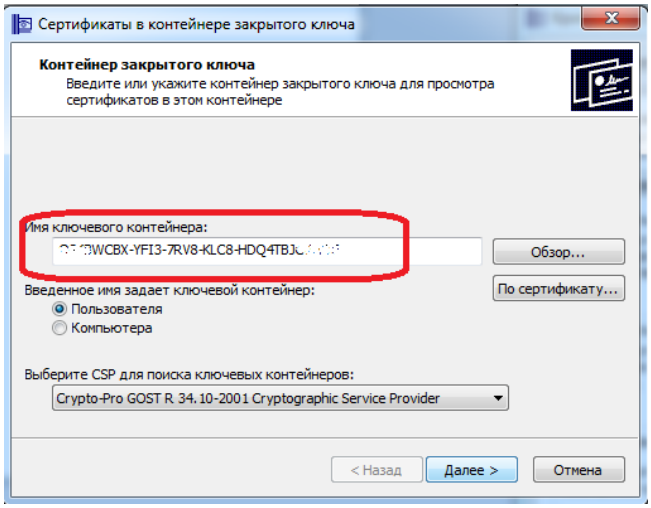


Рис. 13. Имя ключевого контейнера

f. В открывшемся окне запроса ПИН-кода необходимо ввести ПИН-код пользователя-владельца ключа (по умолчанию при выдаче ключа - **1234567890**) и нажать кнопку **ОК.**

g. В следующем окне отображается информация о сертификате в контейнере закрытого ключа. В этом окне нажимаем кнопку **Установить** (рис. 14) и подтверждаем установку:

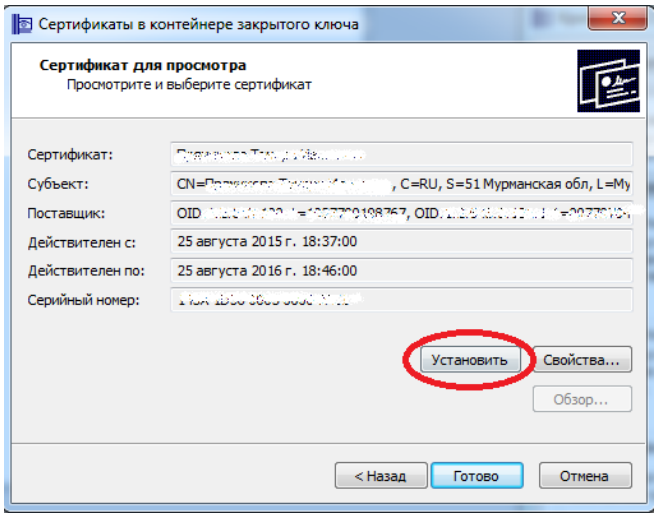


Рис. 14. Установка сертификата

4.5 Проверка формирования ЭП для документов в ИС «Бюджет-Web»

Для подключения ЭП в ИС «Бюджет-Web» необходимо выслать на электронную почту it.murmansk@gmail.com **логин пользователя** в ИС «Бюджет-Web», на которого оформлена электронная подпись, и **наименование соответствующего файла открытого ключа** подписи (имя файла, имеющего расширение .cer)[1]. Форма для заполнения указана в приложении 1.

Простым способом **нахождения наименования файла** открытого ключа является просмотр свойств интернет-обозревателя Internet Explorer после выполнения всех действий, описанных в пп. 3.1-3.3. Сделать это можно следующим образом (на примере Microsoft Windows XP Professional SP3 и Internet Explorer 11):

1. Открыть свойства обозревателя одним из способов:

- через Панель управления Windows (**Пуск→Панель управления→Свойства обозревателя**) (Рис. 15):

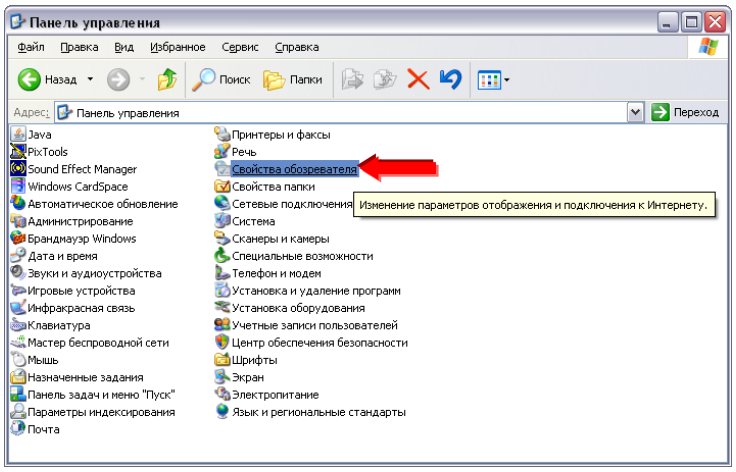


Рис. 15. Свойства обозревателя (Панель управления)

- через меню обозревателя Internet Explorer (**Сервис→Свойства обозревателя**) (Рис. 16):

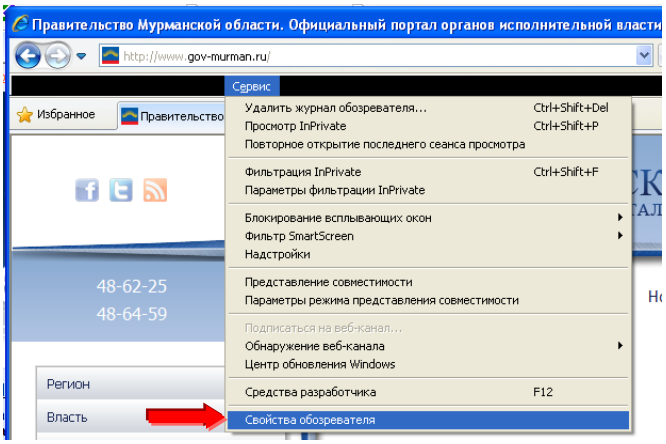


Рис. 16. Свойства обозревателя (меню Internet Explorer)

2. В открывшемся окне «Свойства обозревателя» на вкладке «Содержание» нажать кнопку Сертификаты (Рис. 17):

[1] Необходимо выслать только имя файла. Сам файл открытого ключа высылать не надо!

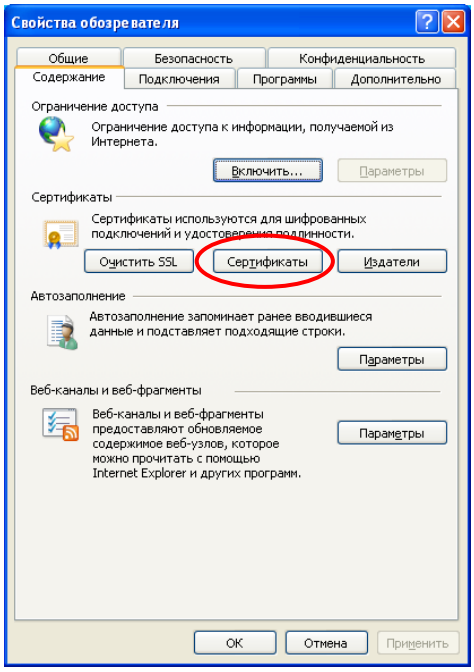


Рис. 17. Свойства обозревателя, вкладка «Содержание»

3. В окне «Сертификаты» на вкладке «Личные» в поле «Кому выдан» содержится необходимая информация о наименовании необходимого сертификата (Рис. 18):

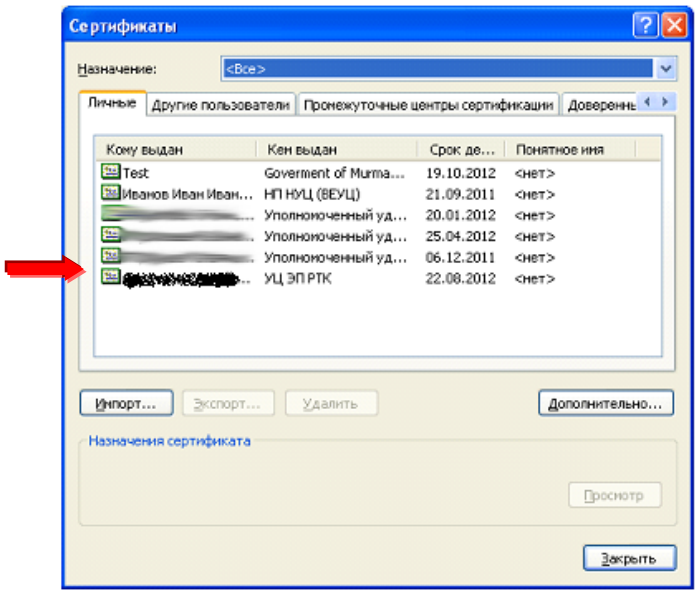


Рис. 18 Информация о сертификатах

Для пересылки необходимо выбрать из этого поля полное наименование сертификата (**как правило, оно совпадает с Фамилией Именем Отчеством владельца сертификата подписи**). Регистр букв при этом учитывается.

Если для сотрудника, имеющего полномочия подписывать документы в ИС «Бюджет-Web» и на которого оформлена электронная подпись, отсутствует соответствующая учетная запись (логин) в ИС «Бюджет-Web», необходимо вместе с пересылкой наименования открытого ключа подписи подать заявку на выдачу такой учетной записи сотруднику.

Каждая электронная подпись сопоставляется конкретной учетной записи пользователя в ИС «Бюджет-Web».

Для проверки функционирования ключей ЭП «Ростелекома» в ИС «Бюджет-Web» необходимо выполнить операцию подписания и проверки ЭП.

Безошибочное выполнение операций подписания и проверки ЭП будет служить проверкой правильности работы ключей ЭП «Ростелекома» в ИС «Бюджет-Web».

- При включенной настройке «Использовать ЭЦП» на панелях инструментов списков документов становится доступен режим подписания документов электронной подписью (Рис. 19):

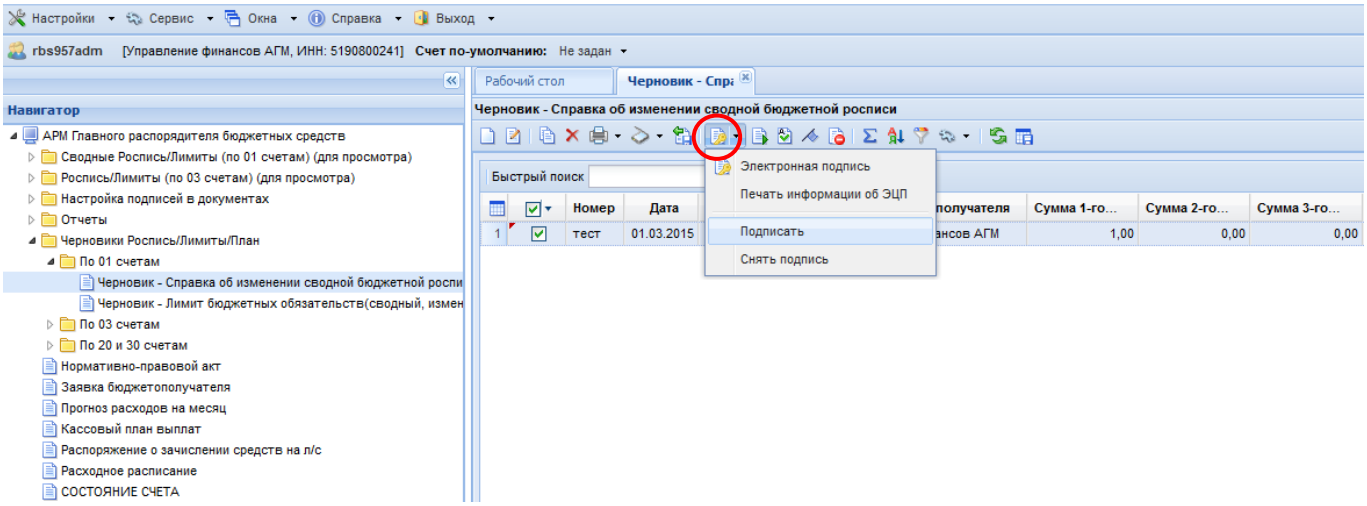


Рис. 19. Установка ЭП в режиме списка документов ИС «Бюджет-Web»

- После нажатия кнопки **Подписать** (в раскрывающемся списке значка ), в случае, если на компьютере пользователя установлено несколько сертификатов, появляется окно выбора сертификатов (Рис. 20), в котором указывается необходимый сертификат подписи. Если на компьютере пользователя установлен только один сертификат, то программа автоматически переходит к процессу подписи документа данным сертификатом.

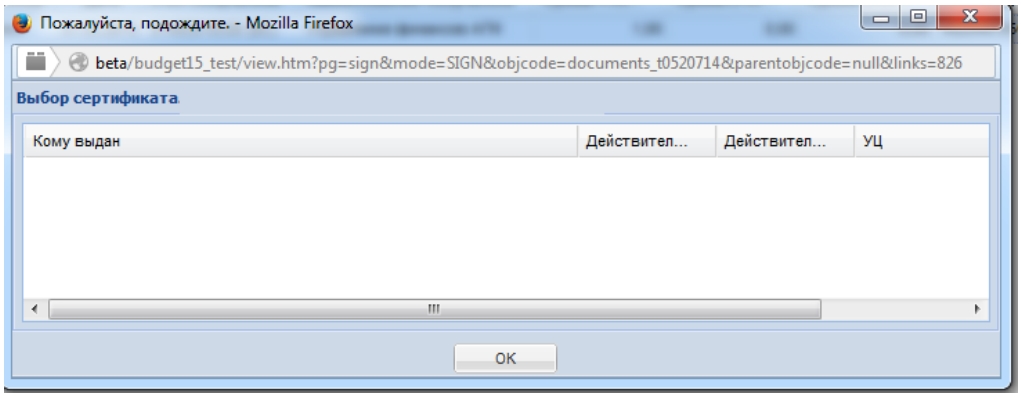


Рис. 20. Окно, отображающее выбор сертификатов пользователя

- Для работы с ЭП в браузере предусмотрен специальный плагин **«XCrypt»**. В случае, если плагин не установлен, программа выдаст соответствующий протокол и предложит его скачать (Рис. 21):

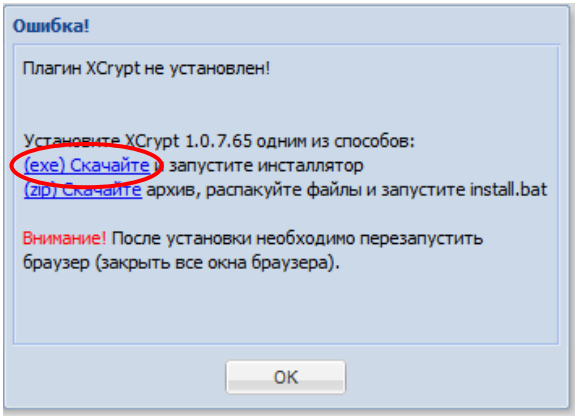


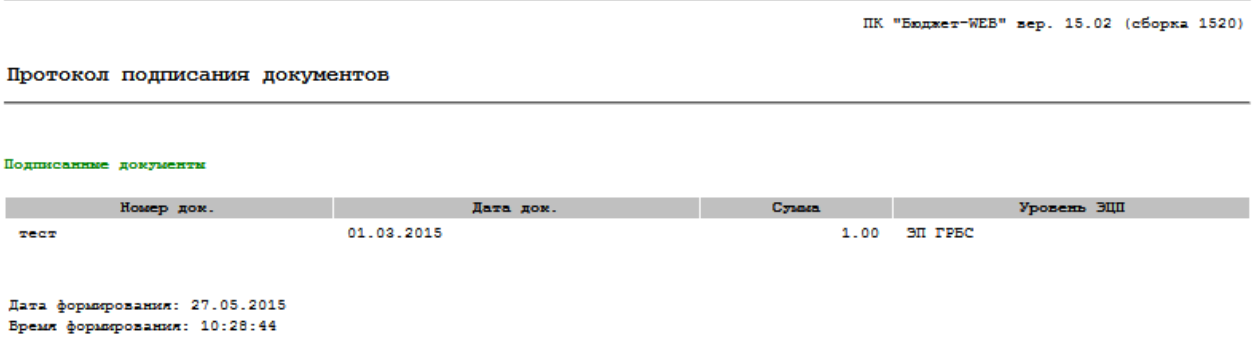
Рис. 21. Окно, отображающее скачивание компонента «XCrypt»

После скачивания плагина «XCrypt» необходимо запустить его установку с правами Администратора (в противном случае плагин не установится) (Рис. 22):

Рис. 22. Установка плагина «XCrypt»

После установки «XCrypt», необходимо перезапустить браузер и разрешить использование данного плагина.

- Процесс подписания может занимать достаточно продолжительное время (в зависимости от количества и структуры подписываемых документов).
- При успешном завершении программа выдаст протокол подписания документов (Рис. 23)



ПК "Бюджет-WEB" вер. 15.02 (сборка 1520)

Протокол подписания документов

Подписанные документы

Номер док.	Дата док.	Сумма	Уровень ЭЦП
тест	01.03.2015	1.00	ЭП ГРБС

Дата формирования: 27.05.2015
Время формирования: 10:28:44

Рис. 23. Завершение процесса подписания

- О том, что соответствующий документ подписан, свидетельствует запись в поле **«Аналитический признак»** соответствующего документа. Иногда для отображения актуального состояния документа требуется обновить список соответствующей кнопкой (Рис. 24):

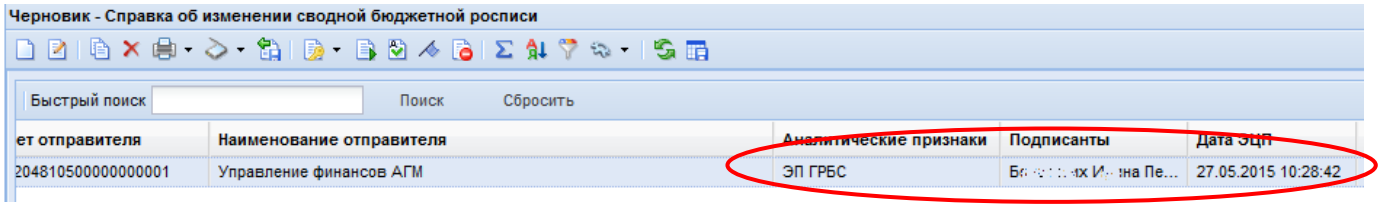
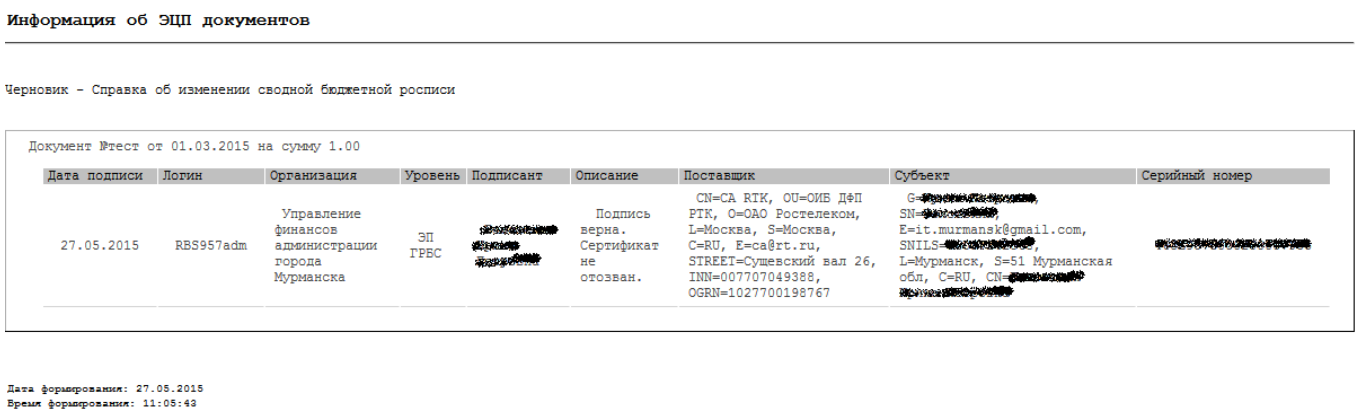


Рис. 24. Отображение подписанных документов в ИС «Бюджет-Web»

- Информацию об электронной подписи можно проверить в режиме **«Печать информации об ЭЦП»** в раскрывающемся списке значка (Рис. 25):



Информация об ЭЦП документов

Черновик - Справка об изменении сводной бюджетной росписи

Документ №тест от 01.03.2015 на сумму 1.00

Дата подписи	Логин	Организация	Уровень	Подписант	Описание	Поставщик	Субъект	Серийный номер
27.05.2015	RBS957adm	Управление финансов администрации города Мурманска	ЭП ГРБС	[redacted]	Подпись верна. Сертификат не отозван.	CN=CA RTK, OU=ОИБ ДФП РТК, O=ОАО Ростелеком, L=Москва, S=Москва, C=RU, E=ca@rt.ru, STREET=Сущевский вал 26, INN=007707049388, OGRN=1027700198767	G=[redacted] SN=[redacted] E=it.murmansk@gmail.com, SNILS=[redacted], L=Мурманск, S=51 Мурманская обл, C=RU, CN=[redacted]	[redacted]

Дата формирования: 27.05.2015
Время формирования: 11:05:43

Рис. 25. Информация об электронной подписи

- После подписания документы будут открываться только в режиме просмотра (Рис. 26)

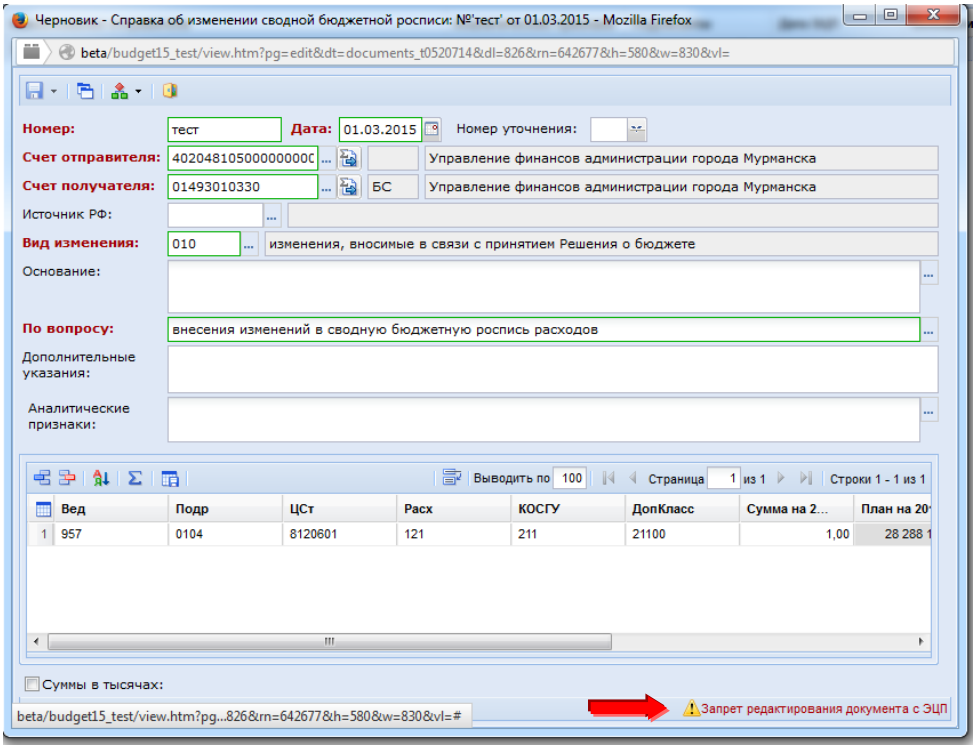


Рис. 26. Запрет изменения подписанного документа

- ИС «Бюджет-Web» поддерживает возможность подписания документа несколькими ЭП разного уровня в соответствии с полномочиями подписывающего. Программа допускает наличие до пяти уровней ЭП, каждому уровню сопоставляются определенные пользователи, которые будут иметь доступ к простановке ЭП данного уровня.
- Для обеспечения возможности редактирования подписанного документа необходимо сначала снять с него электронную подпись. Для этого необходимо выделить в списке документов соответствующую строку и нажать кнопку **«Снять подпись»** в раскрывающемся списке значка  .

Работа с вложениями к документам

ИС «Бюджет-Web» предусматривает возможность прикреплять произвольные электронные файлы к документу. Для этого не панели инструментов предусмотрена кнопка **«Оправдательные документы»** (Рис. 27)

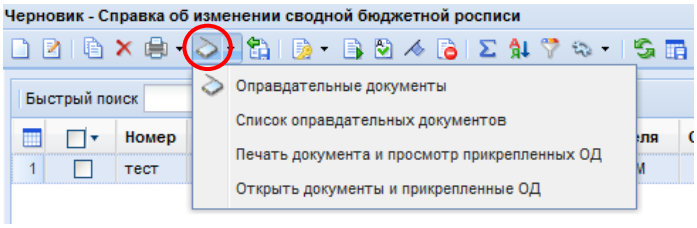


Рис. 27. Режимы работы с оправдательными документами в ИС «Бюджет-Web»

После нажания на кнопку **«Оправдательные документы»** открывается окно работы с вложенными файлами (Рис. 28).

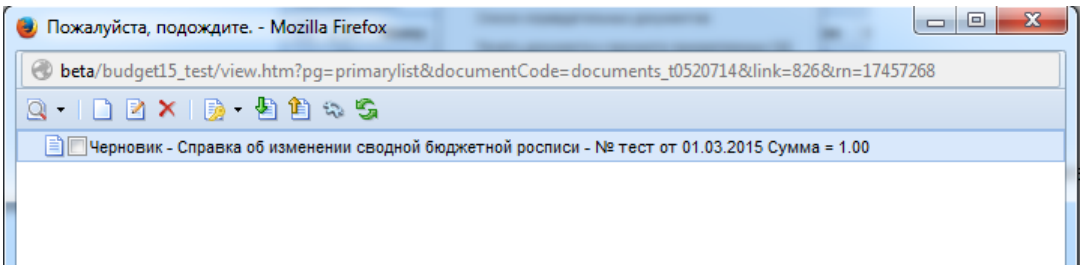


Рис. 28. Работа с оправдательными документами в ИС «Бюджет-Web»

Отметив указанный в списке электронный документ, необходимо нажать кнопку **«Создать…** » на панели инструментов. Далее откроется окно поиска файла, где, путем нажатия на значок , указывается месторасположение прикрепляемого файла и, при необходимости, заполняется комментарий к нему (Рис. 29).

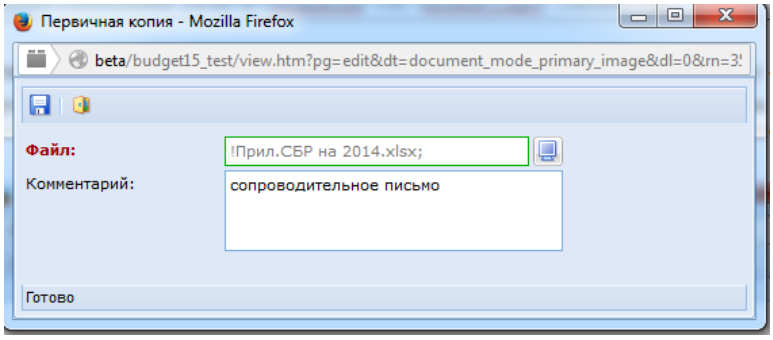


Рис. 29. Работа с оправдательными документами в ИС «Бюджет-Web»

Для прикрепления выбранного файла на панели инструментов нажимается кнопка **«Сохранить** ». После завершения процесса загрузки файла, программа выдаст соответствующий протокол, затем окно поиска файлов можно закрыть. В окне работы с вложенными файлами отобразится загруженный файл (Рис. 30). Для прикрепления следующего файла процедура повторяется аналогично.

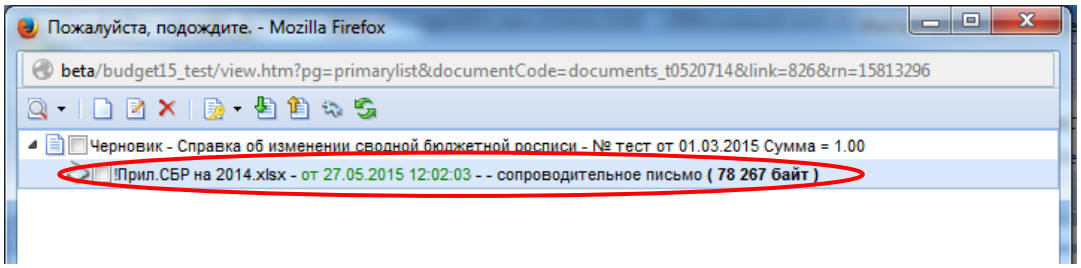


Рис. 30. Загруженное вложение

Размер каждого из прикрепляемых файлов не должен превышать 10 Мб.

ИС «Бюджет-Web» поддерживает работу со всеми типами вложений. Наиболее распространенные типы файлов следующие:

- текстовые: документы MS Word, MS Excel, MS PowerPoint, OpenOffice и др.;
- графические: .JPEG, .PNG, .BMP, .GIF, .TIF, .DIB и др.;
- архивы: .ZIP, .RAR и др.;
- универсальные: .PDF, .XML, .HTML и др.

После загрузки всех вложений на них необходимо наложить электронную подпись. Для этого все файлы вложений помечаются «галкой» и на панели инструментов в раскрывающемся меню кнопки **«Электронная подпись** » жмется **«Подписать»** (Рис. 31). Процесс подписания файлов вложений не отличается от процесса подписания электронных документов, рассмотренных ранее в инструкции.

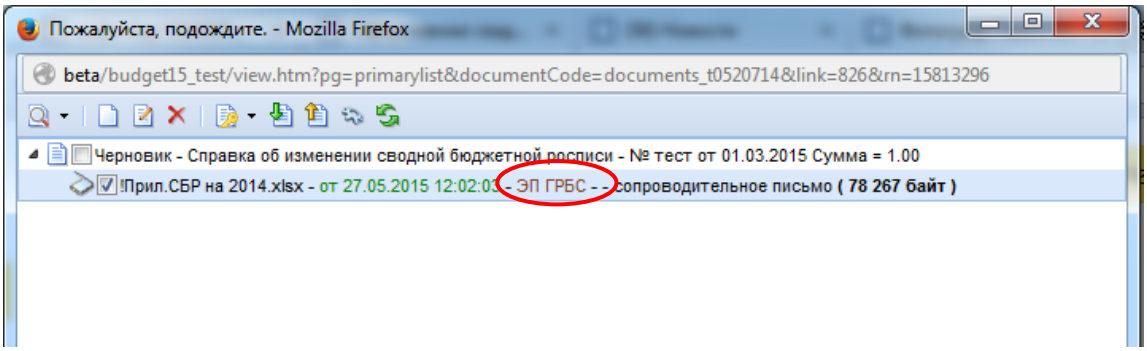


Рис. 31. Подпись вложений

5 Возможные проблемы и пути их решения

Для минимизации возможных проблем при установке и использовании электронной подписи следует четко и грамотно выполнить требования настоящей инструкции, а также инструкции пользователя ИС «Бюджет-Web». В частности, следует проверить выполнение следующих мероприятий:

1. Обеспечение лицензионной чистоты операционной системы Windows и наличия всех необходимых ее обновлений.
2. Настройки сетевых соединений должны позволять беспрепятственно скачивать и устанавливать любые компоненты с сервера ИС «Бюджет-Web».
3. Установку всех средств ЭП следует производить в режиме администратора ПК. Для операционных систем Windows Vista, Windows 7, Windows 8 установку следует производить при отключенном контроле учетных записей (UAC), либо с разрешением выполнения действия.
4. Перед началом установки криптопровайдера КриптоПро CSP необходимо полностью удалить с ПК другие криптопровайдеры. Полное удаление, включая чистку системного реестра, следует производить с помощью соответствующих системных утилит.
5. Регистрация ПО КриптоПро CSP обязательна! Без регистрации работа ЭП не гарантируется.

5.1 Не виден контейнер электронной подписи или не виден сертификат электронной подписи в контейнере

Проблема может проявляться при просмотре контейнера на ключе eToken (Рис. 23-26).

Возможные причины:

1. Время ожидания отображения ещё не истекло.
2. Некорректно установлено ПО КриптоПро CSP.
3. Неисправен носитель (ключ) или на нём физически отсутствует необходимый контейнер (сертификат).

Порядок решения проблемы:

1. При вставке носителя с контейнером необходимо подождать несколько минут, пока контейнер с сертификатом будет опознан.
2. При наличии другого носителя с ключом следует проверить его взамен того, что не опознается. Если другой ключ работает нормально, тогда следует обратиться в удостоверяющий центр по поводу замены неисправного носителя или записи отсутствующего ключа.
3. Если контейнер по-прежнему не виден, следует установить КриптоПро CSP снова, предварительно полностью удалив его существующую установку. При новой установке более тщательно проверить версию ПО КриптоПро CSP, а также **прохождение регистрации** этого продукта.

5.2 При подписании документов в ИС «Бюджет-Web» возникает ошибка модуля XCrypt

Проблема проявляется при попытке подписания документов (Рис. 36-37).

Возможные причины:

1. Некорректно установлено ПО КриптоПро CSP.
2. При работе с ИС «Бюджет-Web» используются неверные настройки интернет-браузера и/или брандмауэра.
3. Как следствие причины 1 и/или 2, в системе отсутствует компонент **XCrypt**, отвечающий за использование ЭП в ИС «Бюджет-Web».

Порядок решения проблемы:

1. Выполнить настройки сетевых соединений и интернет-браузера таким образом, чтобы было возможно беспрепятственно скачивать и устанавливать любые компоненты с сервера ИС «Бюджет-Web» (информация содержится в руководстве пользователя). В частности, в настройках Internet Explorer для безопасных узлов должна быть выбрана настройка **«Загрузка неподписанных элементов ActiveX» - «Разрешить».**
2. Установить КриптоПро CSP снова, предварительно полностью удалив его существующую установку. При новой установке более тщательно проверить версию ПО КриптоПро CSP, а также **прохождение регистрации** этого продукта.
3. Скачать и разархивировать файл **XCrypt.xxxx.exe** из прилагаемого архива и произвести его установку с правами Администратора
4. Перезагрузить компьютер.

ВАЖНОЕ НАПОМИНАНИЕ:

Для подключения ЭП в ИС «Бюджет-Web» необходимо выслать на электронную почту it.murmansk@gmail.com логин пользователя в ИС «Бюджет-Web», на которого оформлена электронная подпись, и наименование соответствующего файла открытого ключа подписи (имя файла, имеющего расширение .cer). Форма для заполнения указана в приложении 1.

Приложение 1

Форма привязки наименования открытого ключа электронной подписи к учетной записи пользователя в ИС «Бюджет-Web»

1. Таблица для заполнения привязки наименования открытого ключа к уже имеющимся учетным записям пользователя:

№ п/п	ФИО уполномоченного лица	Должность	Контактный телефон	Адрес электронной почты	Логин в системе «Бюджет-Web»	Наименования открытого ключа ЭП[1]	Примечание
1							
2							
…							

2. Таблица для заполнения привязки наименования открытого ключа к пользователям, для которых необходимо создание новых логинов в системе «Бюджет-Web»[2]:

№ п/п	ФИО уполномоченного лица	Должность	Контактный телефон	Адрес электронной почты	Наименования открытого ключа ЭП[1]	Примечание
1						
…						

[1] – при заполнении данного поля таблицы необходимо руководствоваться инструкцией по установке и использованию ключей ЭП «Ростелекома» в ИС «Бюджет-Web» (стр. 15, пункт 3.5). Как правило, наименование сертификата совпадает с Фамилией Именем Отчеством владельца сертификата подписи.

[2] – заполняется только при необходимости

После заполнения указанной формы необходимо отправить ее по адресу электронной почты *it.murmansk@gmail.com* с указанием темы письма «Привязка наименований сертификатов – [Наименование ГРБС]». В случае заполнения информации в Таблице 2 данного приложения, новые учетные записи пользователей (пара Логин/Пароль) будут присланы на тот же адрес электронной почты, с которой производилась отправка.