ГБУ СО «Оператор электронного правительства»
- Μυστρυμμία πο μαστρούμο ΠΚ ππα ραδότει σαπουτρομμού ποππίας μο
Инструкция по настройке ПК для работы с электронной подписью (СКЗИ КриптоПро CSP)
(СКЗИ КриптоПро CSP)

Оглавление

I.	Введение	3
II.	Установка драйвера для носителя ЭЦП (ETOKEN, JACARTA)	3
A.	Установка драйвера JaCarta LT	3
В.	Установка драйвера eToken	6
III.	Установка КриптоПро CSP	8
IV.	Установка корневого сертификата удостоверяющего центра	. 11
v.	Установка личного сертификата пользователя УЦ	. 13
VI.	Смена PIN-кода на доступ к содержимому устройства JaCarta LT	. 16

I. Введение

Документ предназначен для пользователей, осуществляющих самостоятельную настройку ПК для работы с электронной подписью (ЭП) с установленными средствами криптографической защиты информации (СКЗИ) Крипто Про CSP.

В удостоверяющем центре ГБУ СО «Оператор электронного правительства» (далее — УЦ ОЭП) срок действия ключей и сертификата ЭП установлен равным 1 году. При необходимости произвести плановую (скорое истечение срока действия ЭП) или внеплановую (изменение учетных данных владельца ЭП, потеря доступа к ключевому носителю, потеря ключевого носителя и т.д.) смену ЭП необходимо повторно прибыть в УЦ ОЭП по согласованию с менеджером УЦ ОЭП.

Для корректной работы с электронной подписью (ЭП) на различных интернет-порталах (электронные торговые площадки, порталы контролирующих органов, различные федеральные информационные ресурсы и т.д.) в качестве интернет-обозревателя рекомендуется использовать Microsoft Internet Explorer версии 8.0 и выше.

II. Установка драйвера для носителя ЭЦП (ETOKEN, JACARTA)

A. Установка драйвера JaCarta LT

Для корректной работы ключевого носителя JaCarta LT под управлением операционной системы Microsoft Windows необходимо установить программное обеспечение, позволяющее выполнять базовые операции с электронными ключами JaCarta.

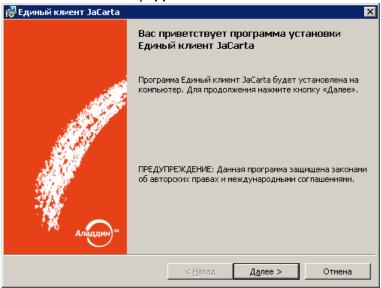
Для получения программного обеспечения актуальной версии необходимо скачать ПО с сайта разработчика: http://aladdin-rd.ru/support/downloads/43987/

Загрузите архив с дистрибутивом в любое место компьютера, распакуйте его и запустите установку утилиты. Выполните установку, следуя инструкциям мастера установки.

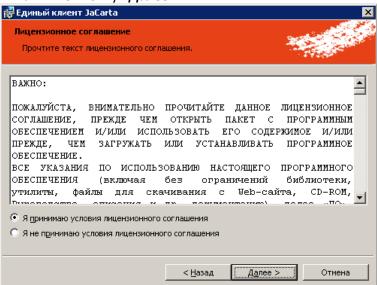
• В первом окне мастера установки нажмите кнопку «Далее» для продолжения установки.



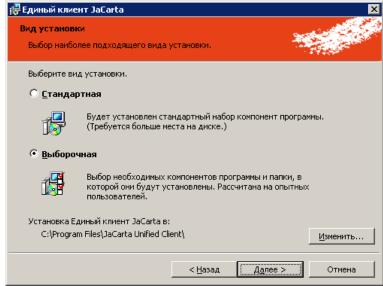
• В окне приветствия нажмите кнопку «Далее».



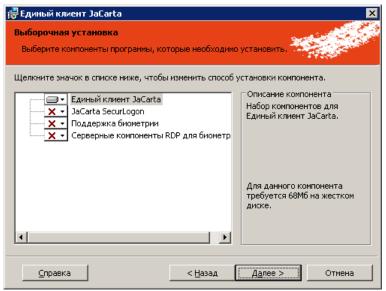
• В окне «Лицензионное соглашение» выберите пункт «Я принимаю условия лицензионного соглашения» и нажмите кнопку «Далее».



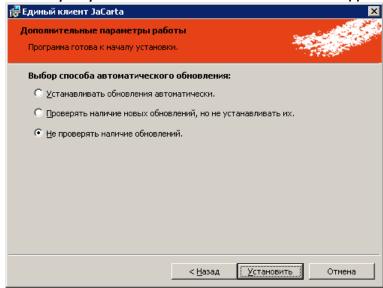
• В окне «Вид установки» выберите «Выборочная» и нажмите «Далее».



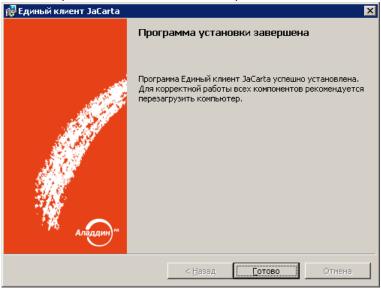
• В окне **«Выборочная установка»** оставьте только пункт **«Единый клиент JaCarta»** и нажмите **«Далее»**.



• Выберите пункт «Не проверять наличие обновлений» и нажмите «Далее».



• Дождитесь окончания установки и нажмите кнопку «Готово».



в. Установка драйвера eToken

Для корректной работы ключевого носителя eToken под управлением операционной системы Microsoft Windows необходимо установить программное обеспечение, позволяющее выполнять базовые операции с электронными ключами eToken.

Для получения программного обеспечения актуальной версии необходимо скачать ПО с сайта разработчика: http://www.aladdin-rd.ru/support/downloads/26037/

Загрузите архив с дистрибутивом в любое место компьютера, распакуйте его и запустите установку утилиты. Выполните установку, следуя инструкциям мастера установки.

В открывшемся окне нажмите «Next».



• В окне «Interface Language» выберите язык «Russian» и нажмите кнопку «Next»



• В открывшейся форме «License Agreement» необходимо ознакомиться с условиями лицензионного соглашения, отметить опцию «I accept the license agreement» и нажать кнопку «Next»



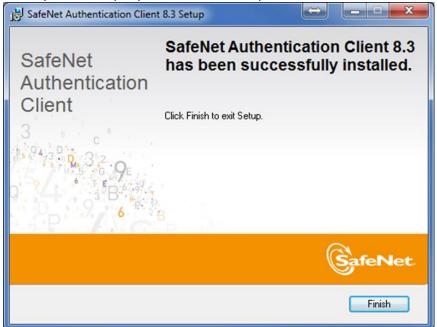
• В окне «Installation Type» выберите «Standard» и нажмите «Next»



• В открывшейся форме «**Destination Folder**» требуется указать каталог установки и нажать кнопку «**Next**»



При успешной установке требуется нажать кнопку «Finish»



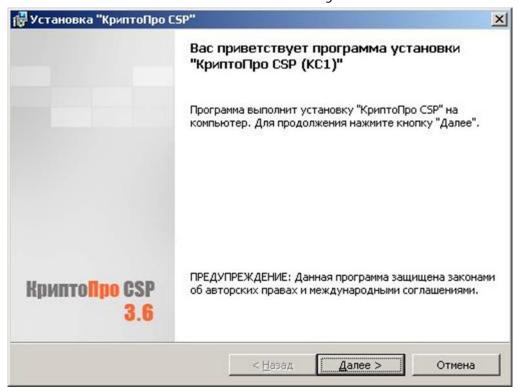
• Перезагрузите компьютер.

III. Установка КриптоПро CSP.

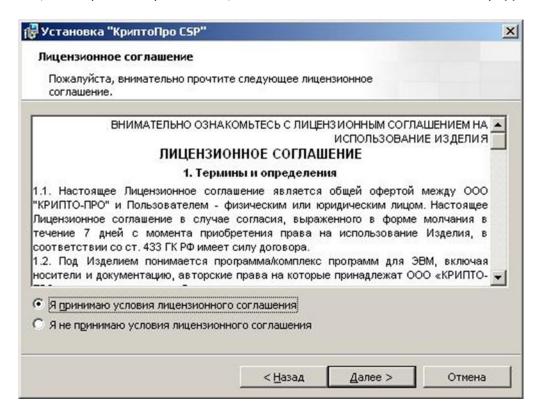
Для установки СКЗИ «КриптоПро CSP» необходимо загрузить дистрибутив: Криптопро CSP 3.6 или Криптопро CSP 3.9. Для штатной эксплуатации средств криптографической защиты информации (СКЗИ), к которым относятся КриптоПро CSP, эти средства должны быть установлены с дистрибутива, полученного у производителя или у официального дилера на материальном носителе.

Получение дистрибутивов возможно после предварительной регистрации на сайте производителя http://www.cryptopro.ru/downloads/howto?destination=node%2F148

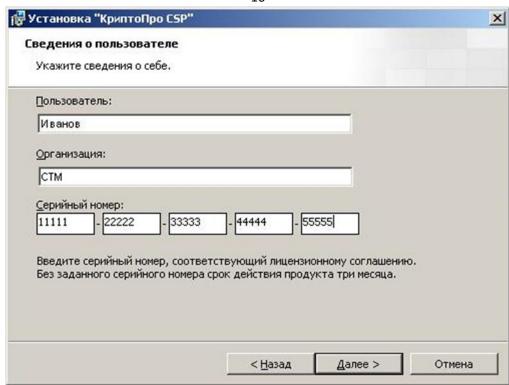
1. При запуске файла дистрибутива откроется окно установки, в котором требуется нажать кнопку «Далее»



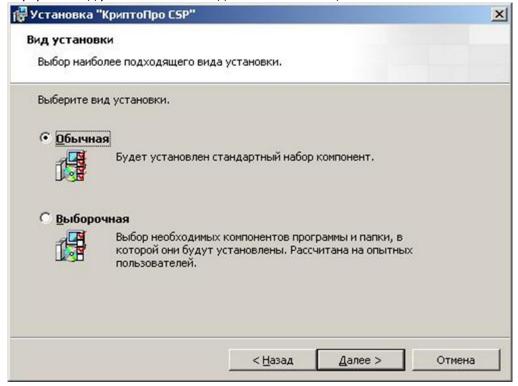
2. В форме «Лицензионное соглашение» требуется ознакомиться с лицензионным соглашением, отметить опцию «Я принимаю условия лицензионного соглашения» и нажать кнопку «Далее»



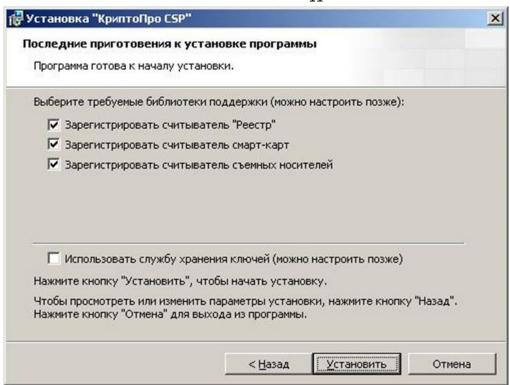
3. В форме «Сведения о пользователе» необходимо указать имя пользователя; организацию; серийный номер (Без указания серийного номера программа будет работать в демонстрационном режиме от одного до трех месяцев).



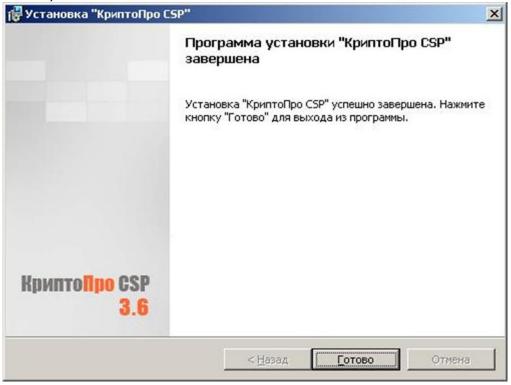
4. В форме «Вид установки» необходимо отметить опцию «Обычная» и нажать кнопку «Далее»



5. В форме «Последние приготовление к установке программы» требуется отметить необходимые опции и нажать кнопку «**Установить**»



6. При успешной установке откроется окно «Установка КриптоПРО CSP», в котором требуется нажать кнопку «**Готово**»



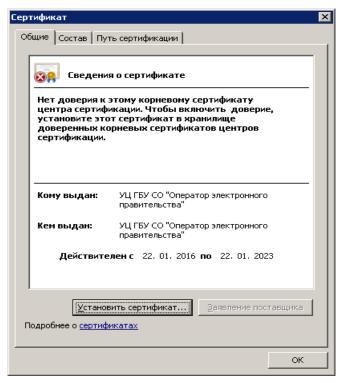
7. После установки «КриптоПро CSP» необходимо перезагрузить компьютер.

IV. Установка корневого сертификата удостоверяющего центра.

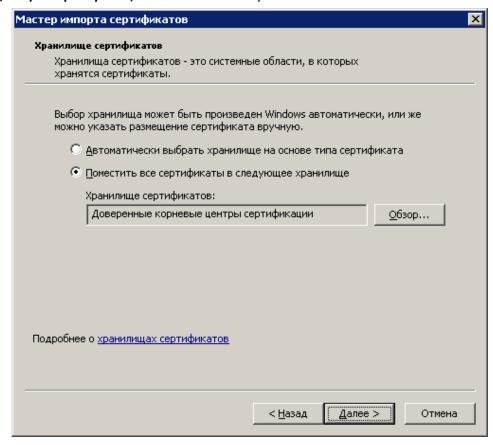
- 1. Для получения корневого сертификата Удостоверяющего центра ГБУ СО «Оператор электронного правительства» перейдите по ссылке https://egov66.ru/ca/cdp/ca-2015.cer
- 2. Откройте сертификат непосредственно из окна Web-браузера, нажав кнопку «*Открыть*» или сохраните сертификат на жесткий диск компьютера и откройте его двойным щелчком левой



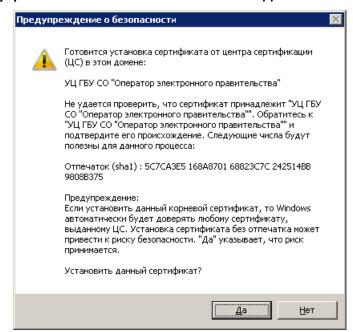
3. В открывшемся окне нажмите кнопку «Установить сертификат».



4. Выполните установку корневого сертификата удостоверяющего центра, следуя инструкциям мастера установки. На шаге выбора «Хранилища сертификатов» укажите: «Поместить все сертификаты в следующее хранилище» нажмите кнопку «Обзор...», укажите раздел «Доверенные корневые центры сертификации» нажмите кнопку «ОК».



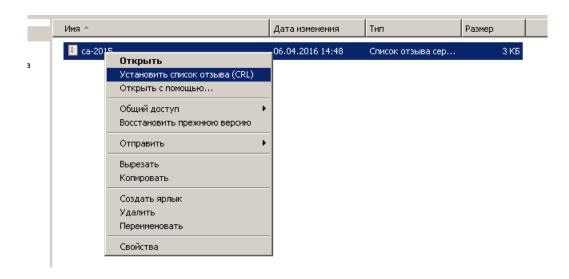
5. В окне **«Предупреждение о безопасности»** нажмите **«Да»**.



- 6. Далее получите список отозванных сертификатов Удостоверяющего центра ГБУ СО «Оператор электронного правительства» перейдите по ссылке https://egov66.ru/ca/cdp/ca-2015.crl
- 7. Сохраните список отозванных сертификатов на жесткий диск компьютера.



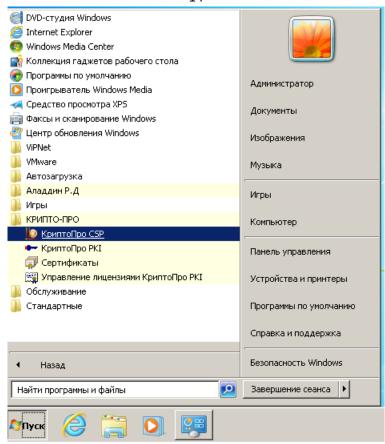
8. Найдите в папке сохранения файл са-2015.crl и нажмите на нем правой кнопкой мыши. В появившемся меню выберите пункт «Установить список отзыва (CRL)».



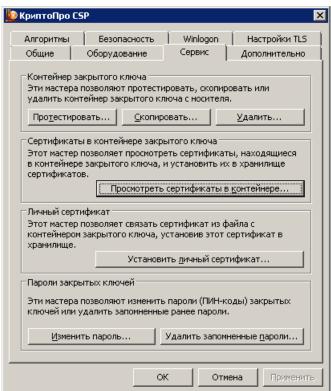
9. Выполните установку списка отозванных сертификатов удостоверяющего центра, следуя инструкциям мастера установки.

V. Установка личного сертификата пользователя УЦ.

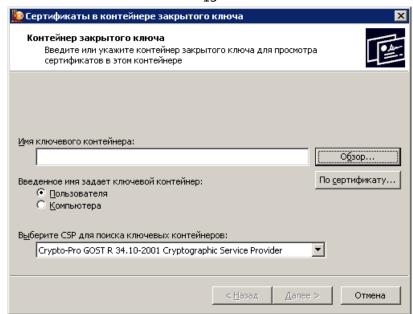
Запустите КриптоПро CSP.



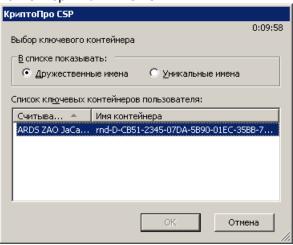
1. Перейдите в раздел **«Сервис».** Затем нажмите кнопку **«Просмотреть сертификаты в контейнере...»**.



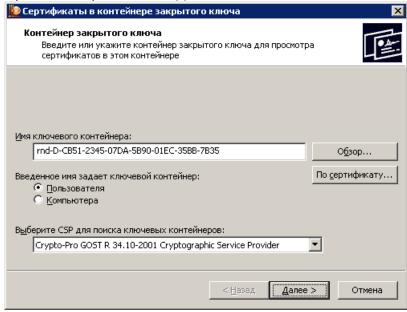
2. В окне выбора контейнера закрытого ключа нажмите *«Обзор»*.



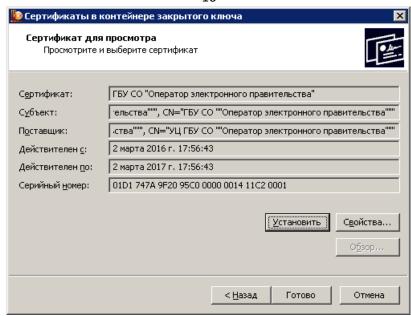
3. Выберите нужный контейнер и нажмите «ОК».



4. После выбора контейнера нажмите «Далее».



5. В окне просмотра сертификата нажмите **«Установить»**.

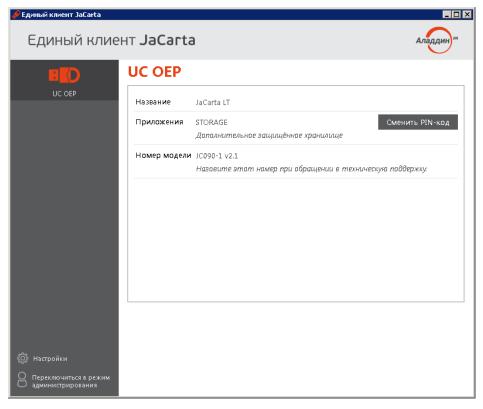


На этом установка личного сертификата завершена.

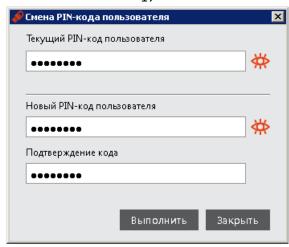
Для работы с СКП в информационных системах могут понадобиться дополнительные настройки рабочего места, требуемые параметры необходимо узнавать для каждой информационной системы.

VI. Смена PIN-кода на доступ к содержимому устройства JaCarta LT.

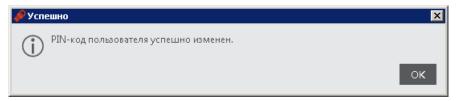
- 1. Вставьте JaCarta LT, на котором необходимо сменить PIN-код пользователя, в USB- порт компьютера.
- 2. Откройте Единый клиент JaCarta.
- 3. Если к компьютеру подсоединено несколько электронных ключей, в левой панели Единого клиента JaCarta выберите нужный электронный ключ.



- 4. В главном окне нажмите кнопку «Сменить PIN-код».
- В поле «Текущий PIN-код» введите текущий PIN-код пользователя.



- 6. В полях **«Новый PIN-код пользователя»** и **«Подтверждение PIN-код пользователя»** введите новый PIN-код пользователя.
- 7. Нажмите кнопку *«Выполнить»*. При успешной установке нового PIN-кода пользователя появится соответствующее сообщение.



Количество ввода неправильного пароля (PIN-кода) для доступа к ключам электронной подписи на JaCarta LT ограничено (по умолчанию 10), после чего доступ к информации на JaCarta LT блокируется. Блокировка доступа к информации на JaCarta LT является необратимой аппаратной функцией. Никогда не используйте для решения технических проблем, возникающих при использовании JaCarta LT, процедуру инициализации JaCarta LT. Необходимо учитывать, что инициализация JaCarta LT ведет к потере всей информации в памяти ключа.

Внимание! Для работы с электронной подписью настоятельно рекомендуем использовать браузер Internet Explorer, в частных случаях, где у порталов используются свои плагины для работы с электронной подписью Google Chrome.