

УТВЕРЖДАЮ

Заместитель руководителя
Федерального казначейства

 / Гуральников С.Б. /
« 13 » марта 2015 г.

УТВЕРЖДАЮ

Заместитель руководителя
Федерального казначейства

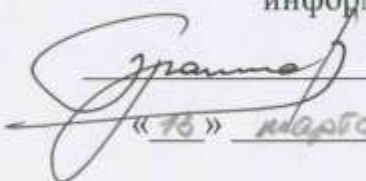
 / Смирнов В.А. /
« 13 » марта 2015 г.

Государственная интегрированная информационная система
управления общественными финансами «Электронный бюджет»

**Руководство по установке и настройке программного
обеспечения автоматизированного рабочего места пользо-
вателя системы «Электронный бюджет»**

СОГЛАСОВАНО

Начальник Управления режима сек-
ретности и безопасности
информации

 / Бражко В.С. /
« 13 » марта 2015 г.

СОГЛАСОВАНО

Начальник Управления интегриро-
ванных информационных систем го-
сударственных финансов

 / Гвоздева Н.В. /
« 13 » марта 2015 г.

СОДЕРЖАНИЕ

АННОТАЦИЯ	3
1. СПИСОК ТЕРМИНОВ И СОКРАЩЕНИЙ.....	4
2. ПОРЯДОК ПОДГОТОВКИ АРМ.....	5
3. ОПИСАНИЕ ОПЕРАЦИЙ.....	6
3.1 Копирование сертификата сервера TLS	6
3.2 Копирование корневого сертификата УЦ Федерального казначейства.....	7
3.3 Установка корневого сертификата в локальное хранилище компьютера	8
3.4 Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя (при необходимости)	11
3.5 Установка ПО «Windows Installer».....	14
3.6 Установка драйвера используемого носителя ключевой информации сертификата пользователя.....	16
3.7 Установка программного обеспечения «Jinn-Admin».....	22
3.8 Установка средства создания защищенного TLS-соединения «Континент TLS Клиент».....	25
3.9 Настройка веб-обозревателя	32
3.10 Установка средства электронной подписи «Jinn-Client»	36
3.11 Установка модуля для работы с электронной подписью «Cubesign»	44
3.11.1 Предварительная установка	44
3.11.2 Установка в процессе инициации процедуры создания заявки в системе согласования и управления доступа.....	48
ЛИСТ СОГЛАСОВАНИЯ	52
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	53

АННОТАЦИЯ

Настоящий документ содержит описание последовательности действий по установке и настройке программного обеспечения автоматизированного рабочего места пользователя системы «Электронный бюджет».

1. СПИСОК ТЕРМИНОВ И СОКРАЩЕНИЙ

В документе используются следующие термины и сокращения:

АРМ – автоматизированное рабочее место пользователя системы «Электронный бюджет»;

ОС – операционная система;

ПО – программное обеспечение;

Пользователь – зарегистрированный в системе «Электронный бюджет» сотрудник организации, которому предоставлен доступ к определенным функциям в системе «Электронный бюджет», в соответствии с заявкой на подключение;

Система «Электронный бюджет» – государственная интегрированная информационная система управления общественными финансами «Электронный бюджет»;

УЦ – Удостоверяющий центр.

2. ПОРЯДОК ПОДГОТОВКИ АРМ

Установка и настройка программного обеспечения автоматизированного рабочего места пользователя должна выполняться под учетной записью пользователя, входящего в группу локальных администраторов операционной системы.

Порядок подготовки АРМ пользователя приведен в таблице (Таблица 1).

Таблица 1. Порядок подготовки АРМ пользователя.

№ п/п	Операция	Раздел
1.	Копирование сертификата сервера TLS в локальную директорию АРМ пользователя.	3.1
2.	Копирование корневого сертификата УЦ Федерального казначейства в локальную директорию АРМ пользователя.	3.2
3.	Установка корневого сертификата УЦ Федерального казначейства в локальное хранилище компьютера.	3.3
4.	Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя (при необходимости).	3.4
5.	Установка ПО «Windows Installer».	3.5
6.	Установка драйвера используемого носителя ключевой информации сертификата пользователя.	3.6
7.	Установка ПО «Jinn-Admin» для генерации запроса к УЦ на получение квалифицированного сертификата пользователя (устанавливается при необходимости).	3.7
8.	Установка и настройка средства создания защищенного TLS-соединения «Континент TLS Клиент».	3.8
9.	Настройка используемого пользователем веб-обозревателя для подключения к системе «Электронный бюджет».	3.9
10.	Установка средства электронной подписи «Jinn-Client».	3.10
11.	Установка модуля для работы с электронной подписью «Cubesign».	3.11

3. ОПИСАНИЕ ОПЕРАЦИЙ

3.1 Копирование сертификата сервера TLS

Для копирования файла сертификата сервера TLS в локальную директорию АРМ пользователя необходимо:

1. Открыть в веб-обозревателе официальный сайта Федерального казначейства, перейдя по адресу в сети Интернет: www.roskazna.ru

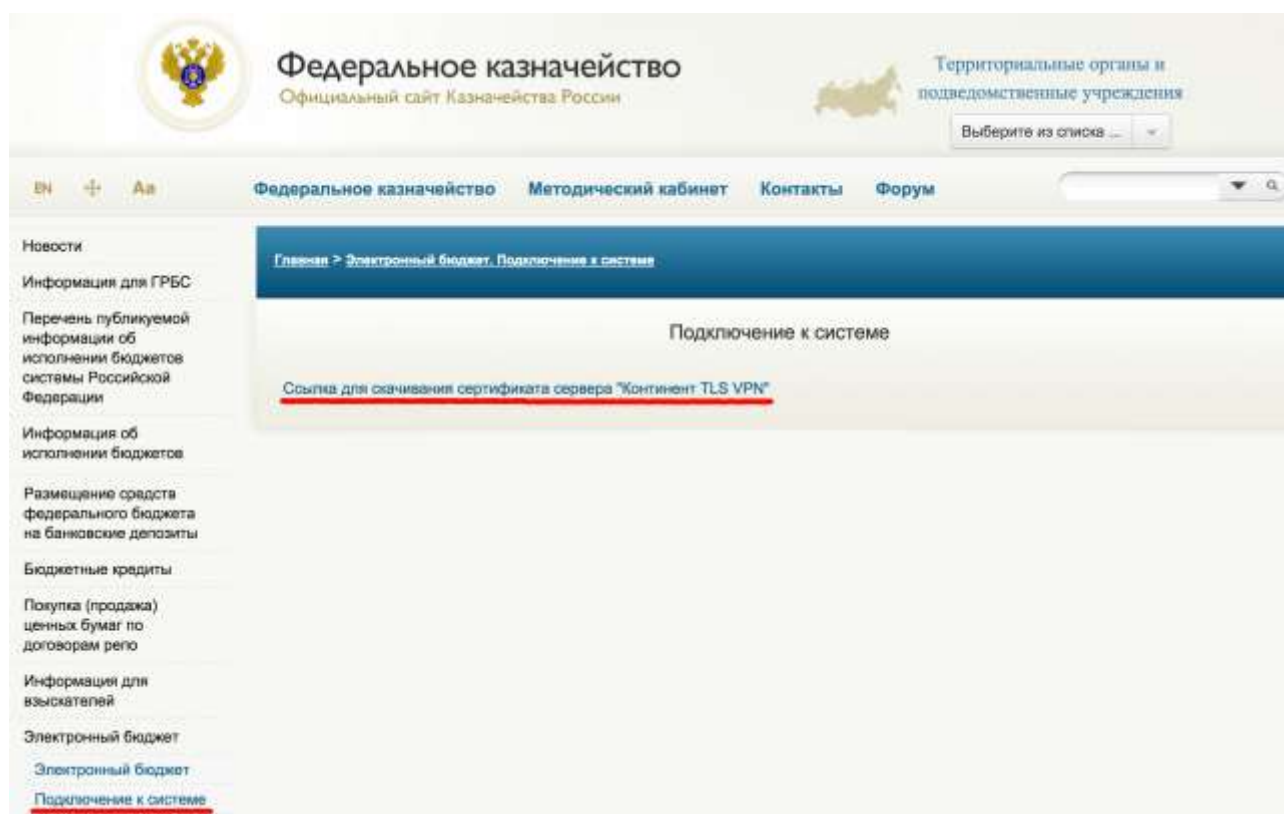


Рисунок 1. Копирование сертификата сервера TLS.

2. Перейти в раздел «Электронный бюджет > Подключение к системе».
3. Активировать ссылку «Ссылка для скачивания сертификата сервера «Континент TLS VPN»».
4. На предложение сохранить файл сертификата «Федеральное казначейство__.cer» выбрать локальную директорию в АРМ пользователя, в которую необходимо сохранить файл.
5. Сохранить файл сертификата сервера TLS.

3.2 Копирование корневого сертификата УЦ Федерального казначейства

Для копирования файла корневого сертификата УЦ Федерального казначейства в локальную директорию АРМ пользователя необходимо:

1. Открыть в веб-обозревателе официальный сайта Федерального казначейства, перейдя по адресу в сети Интернет: www.roskazna.ru

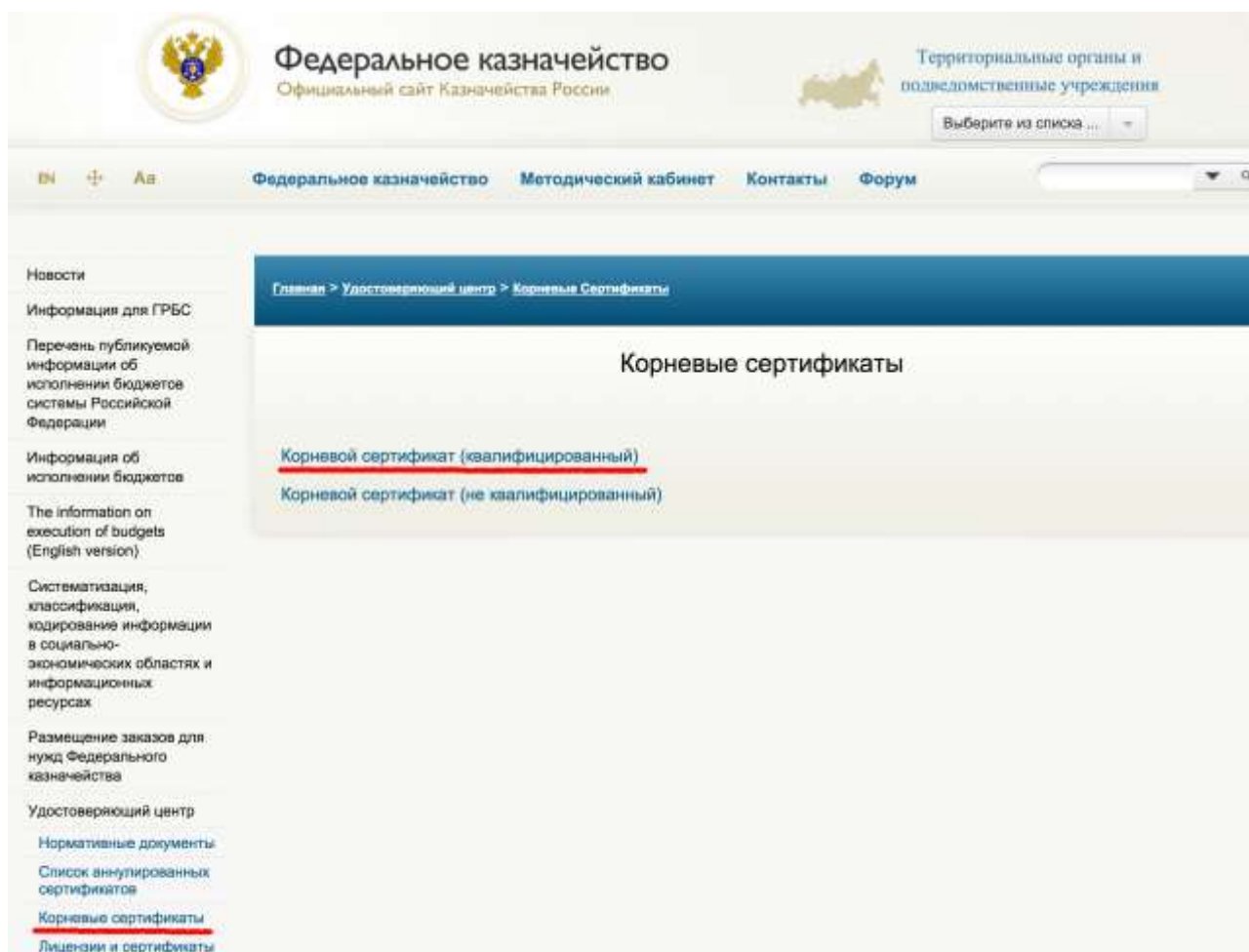


Рисунок 2. Копирование корневого сертификата УЦ Федерального казначейства.

2. Перейти в раздел «Удостоверяющий центр > Корневые сертификаты».
3. Активировать ссылку «Корневой сертификат (квалифицированный)».
4. На предложение сохранить файл сертификата «Корневой сертификат (квалифицированный).cer» выбрать локальную директорию в АРМ пользователя, в которую необходимо сохранить файл.
5. Сохранить файл сертификата сервера TLS.

3.3 Установка корневого сертификата в локальное хранилище компьютера

Для установки корневого сертификата УЦ в хранилище сертификатов компьютера средствами операционной системы семейства Windows необходимо:

1. Через контекстное меню файла корневого сертификата УЦ Федерального казначейства выбрать пункт меню «Установить сертификат».
2. На экране отобразится мастер импорта сертификатов.

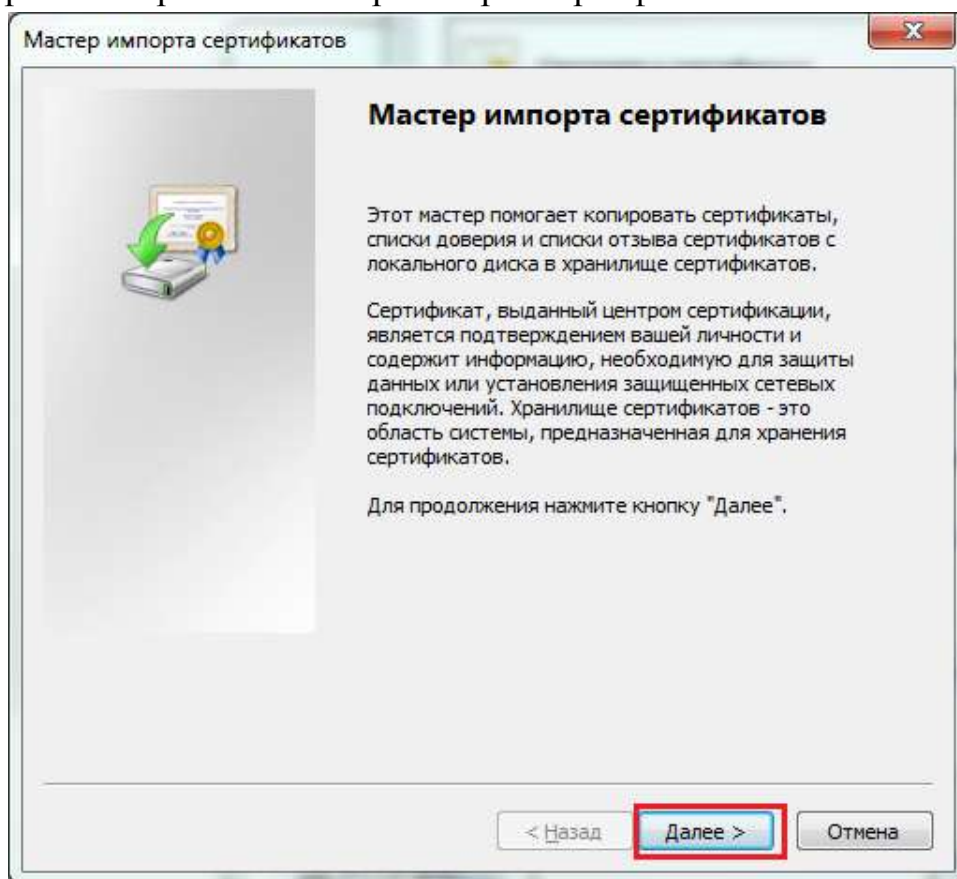


Рисунок 3. Мастер импорта сертификатов.

3. Нажать кнопку «Далее>».

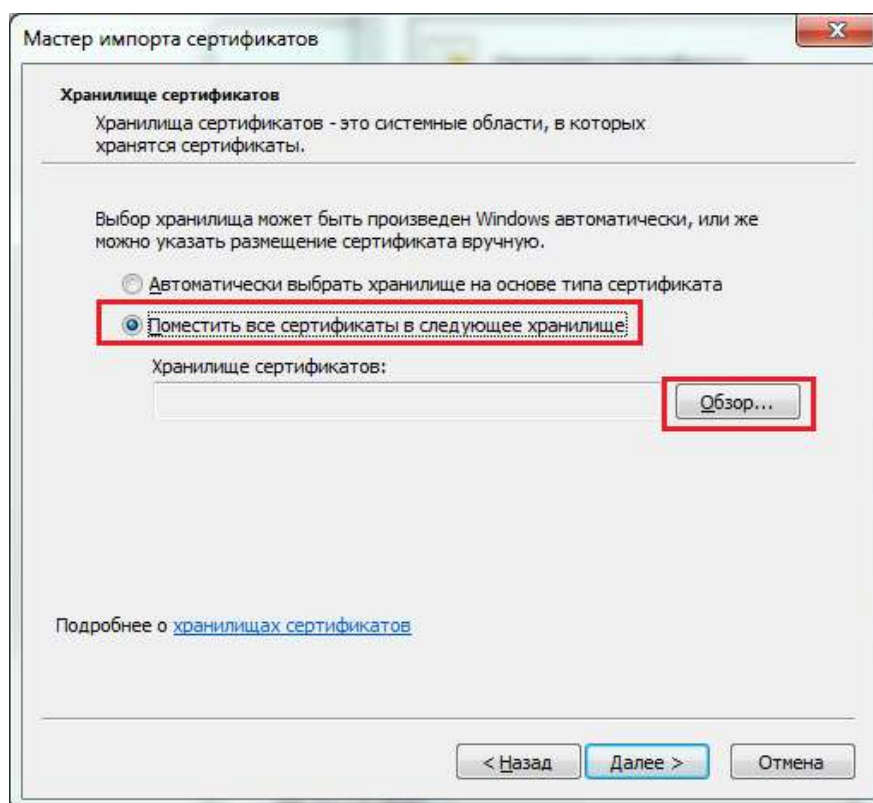


Рисунок 4. Выбор хранилища сертификата.

4. В окне «Хранилище сертификата» выбрать размещение сертификата вручную, указав поле «Поместить сертификаты в следующее хранилище».
5. Нажать кнопку «Обзор...».

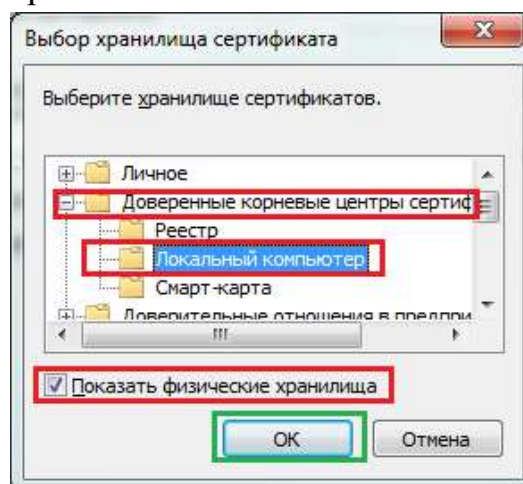


Рисунок 5. Выбор хранилища сертификата. Локальный компьютер.

6. Отметить поле «Показывать физические хранилища».
7. В окне выбора хранилища сертификатов раскрыть контейнер «Доверенные корневые центры сертификации».

8. В контейнере «Доверенные корневые центры сертификации» выбрать вложенный контейнер «Локальный компьютер».
9. Нажать кнопку «Ок».

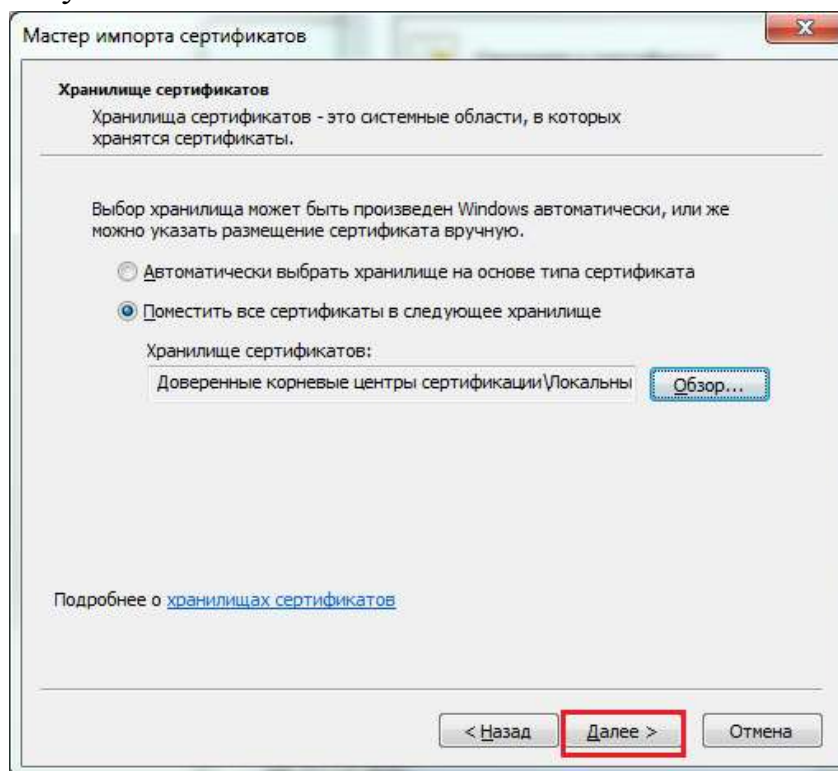


Рисунок 6. Выбор хранилища сертификата. Установка.

10. Нажать кнопку «Далее>».

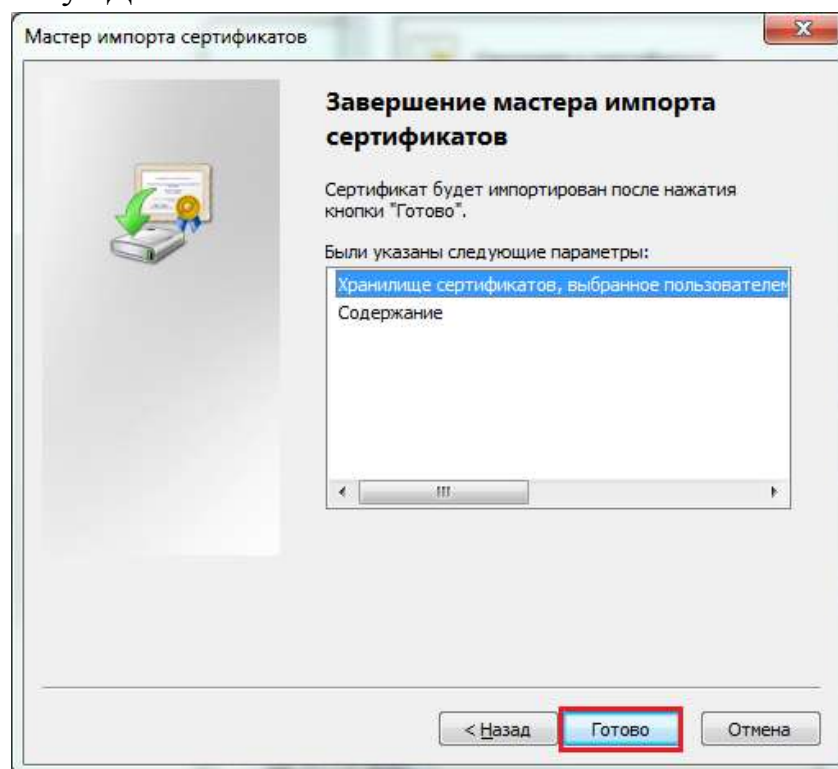


Рисунок 7. Завершение установки.

11. Нажать кнопку «Готово».
12. В случае успешного импорта сертификата отобразится диалог «Импорт успешно выполнен».
13. Нажать кнопку «ОК».

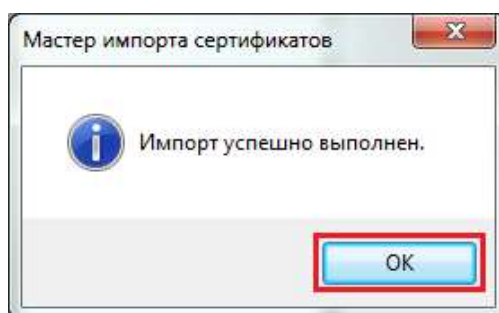


Рисунок 8. Успешный импорт сертификата.

3.4 Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя (при необходимости)

Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя выполняется в случае, если файл сертификата пользователя находится не в контейнере закрытого ключа(в процессе получения в УЦ сертификат в формате «*.cer» был записан на отдельный носитель информации).

Установка сертификата пользователя в хранилище личных сертификатов АРМ пользователя выполняется под учетной записью пользователя, которая будет использоваться в процессе входа в личный кабинет системы «Электронный бюджет».

Для сертификата пользователя в хранилище личных сертификатов АРМ пользователя средствами операционной системы семейства Windows необходимо:

1. Через контекстное меню файла сертификата пользователя выбрать пункт меню «Установить сертификат».
2. На экране отобразится мастер импорта сертификатов.

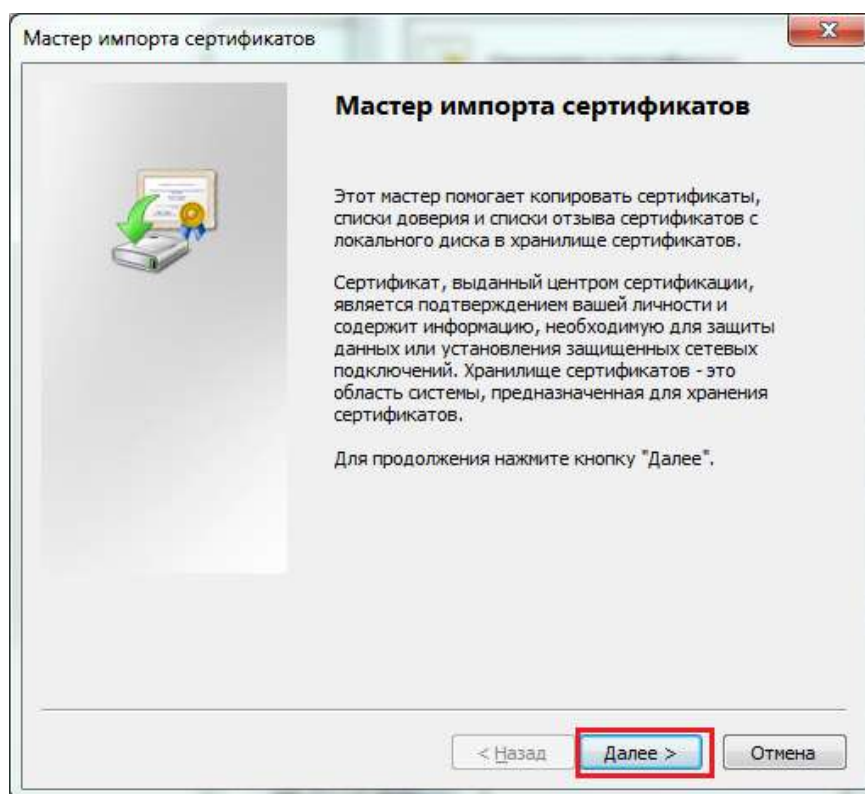


Рисунок 9. Мастер импорта сертификатов.

3. Нажать кнопку «Далее>».

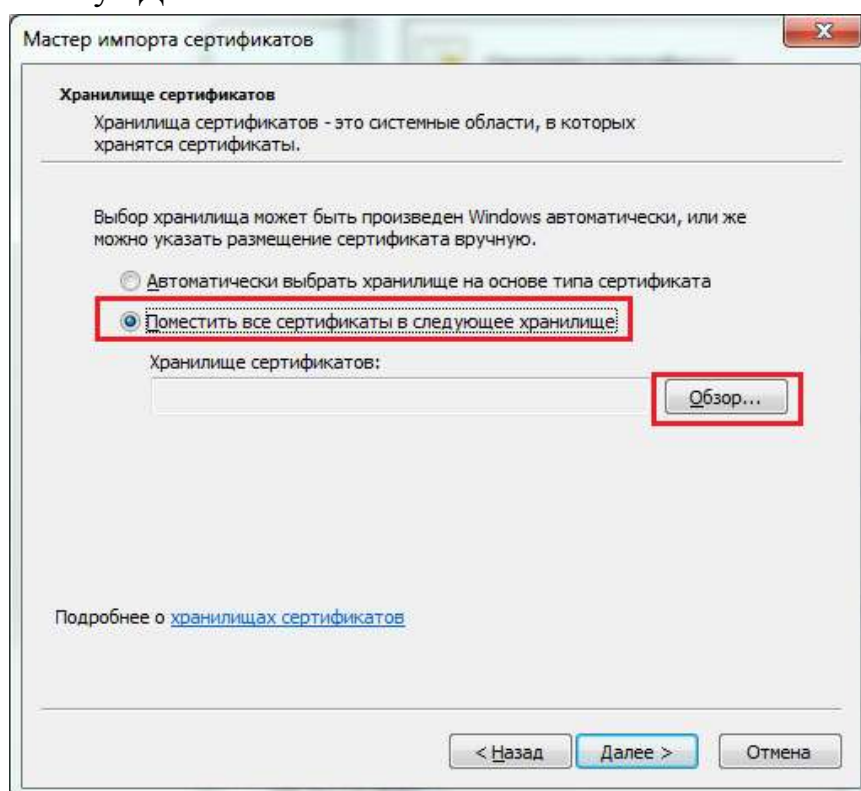


Рисунок 10. Выбор хранилища сертификата.

4. В окне «Хранилище сертификата» выбрать размещение сертификата вручную, указав поле «Поместить сертификаты в следующее хранилище».
5. Нажать кнопку «Обзор...».

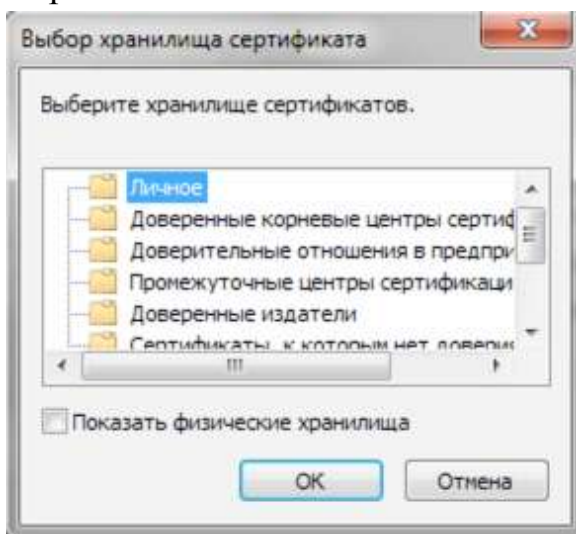


Рисунок 11. Выбор хранилища сертификата. Личное.

6. В окне выбора хранилища сертификатов выбрать контейнер «Личное».
7. Нажать кнопку «ОК».

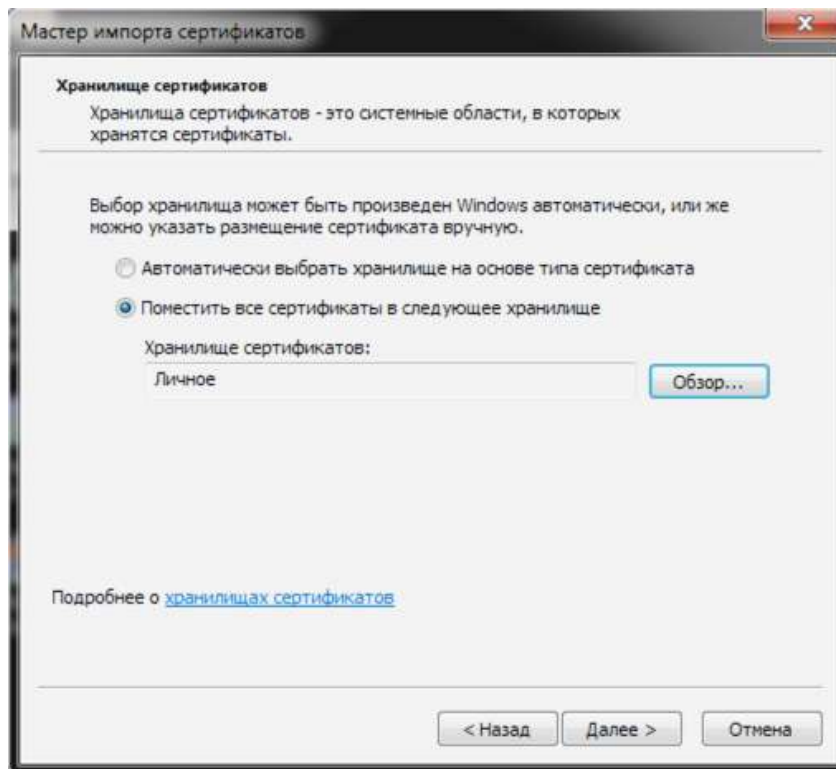


Рисунок 12. Выбор хранилища сертификата. Установка.

8. Нажать кнопку «Далее>».

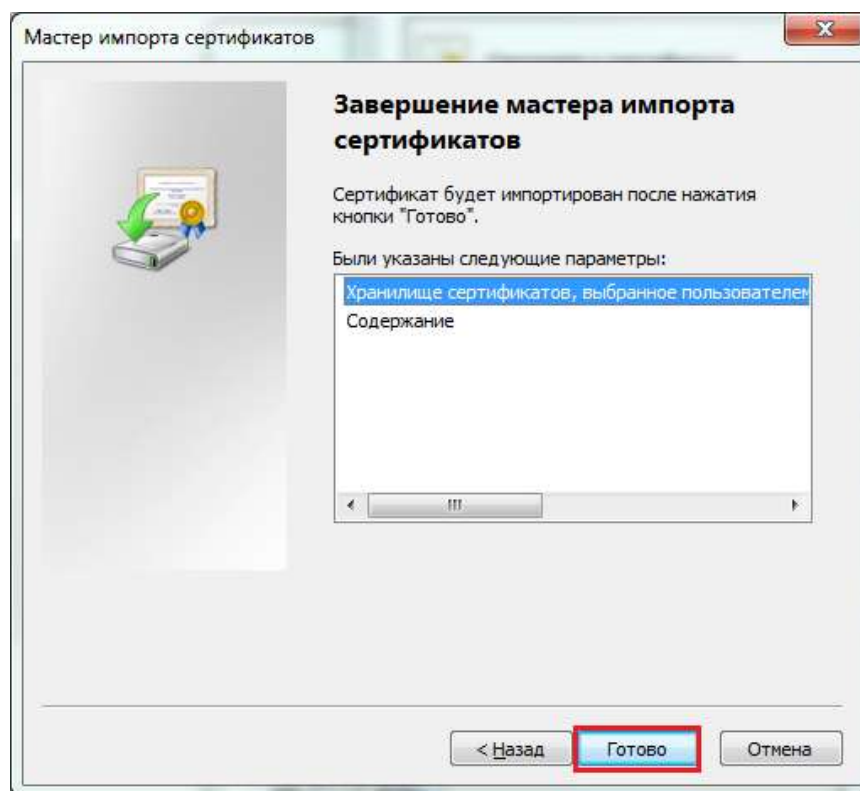


Рисунок 13. Завершение установки.

9. Нажать кнопку «Готово».
10. В случае успешного импорта сертификата отобразится диалог «Импорт успешно выполнен».
11. Нажать кнопку «ОК».

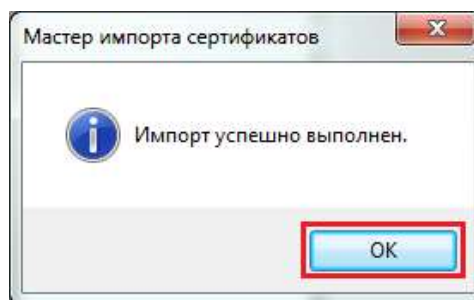


Рисунок 14. Успешный импорт сертификата.

3.5 Установка ПО «Windows Installer»

Необходимость в установке ПО «Windows Installer» может быть определена путем запуска единого меню установщика ПО «Континент TLS Клиент». Для его вызова необходимо осуществить запуск исполняемого файла «ContinentTLSSetup» из состава дистрибутива ПО «Континент TLS Клиент». На экране отобразится окно выбора устанавливаемых компонентов.

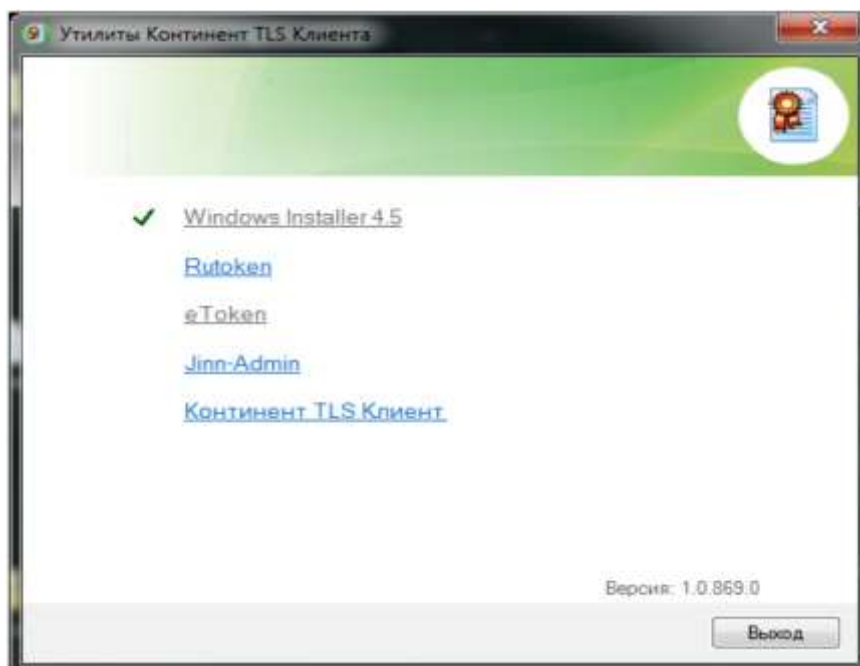


Рисунок 15. Единое меню установщика ПО «Континент TLS Клиент»

В случае, если ПО «Windows Installer» уже установлено в АРМ пользователя, пункт меню данного компонента будет отмечен пиктограммой «✓». В этом случае необходимо перейти к следующему шагу подготовки АРМ пользователя – «Установка драйвера используемого типа носителя ключевой информации сертификата пользователя».

Если ПО не установлено, необходимо:

1. В меню единого установщика ПО «Континент TLS Клиент» активировать ссылку «Windows Installer 4.5». На экране отобразится окно установки компонента.

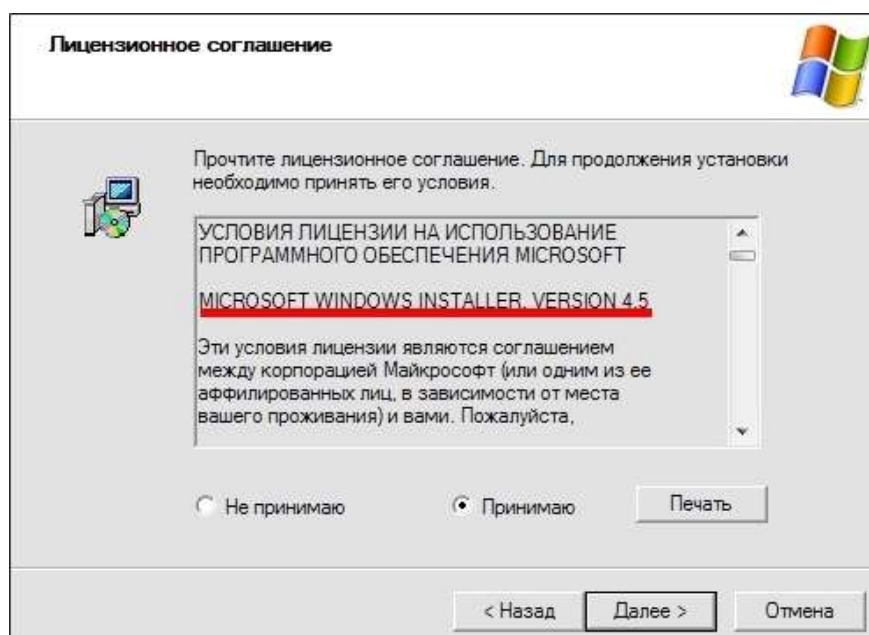


Рисунок 16. Установка ПО «Windows Installer». Лицензионное соглашение.

2. Отметить пункт «Принимаю» и нажать кнопку «Далее». Начнется установка ПО «Windows Installer».
3. По окончании установки нажать кнопку «Завершить».
4. В случае появления диалога о необходимости перезагрузки АРМ пользователя, ответить положительно.

3.6 Установка драйвера используемого носителя ключевой информации сертификата пользователя

Если в качестве носителя ключевой информации сертификата пользователя используется USB флеш-накопитель, установка драйвера данного накопителя осуществляется автоматически средствами ОС в момент первого использования данного накопителя.

Если в качестве носителя ключевой информации сертификата пользователя используется носитель типа eToken или Rutoken, необходимо выполнить установку драйвера соответствующего накопителя в ОС (если ранее не был установлен).

Необходимость в установке драйвера носителя ключевой информации типа eToken или Rutoken может быть определена путем запуска единого меню установщика ПО «Континент TLS Клиент». Для его вызова необходимо осуществить запуск исполняемого файла «ContinentTLSSetup» из состава дистрибутива ПО «Континент TLS Клиент». На экране отобразится окно выбора устанавливаемых компонентов (Рисунок 15).

Если требуемый драйвер уже установлен в АРМ пользователя, пункт меню данного типа носителя ключевой информации будет отмечен пиктограммой «». В этом случае необходимо перейти к следующему шагу подготовки АРМ пользователя – «Установка ПО «Jinn-Admin» для генерации запросов к УЦ на получение квалифицированного сертификата пользователя (устанавливается при необходимости)» либо «Установка средства создания защищенного TLS-соединения «Континент TLS Клиент».

Если необходимый драйвер не установлен, необходимо:

а) Драйвер носителя типа Rutoken

1. Активируйте ссылку Rutoken в едином меню установщика ПО «Континент TLS Клиент». Запустится программа-установщик драйвера Rutoken. Окно приветствия установщика драйверов Rutoken представлено на рисунке (Рисунок 17).

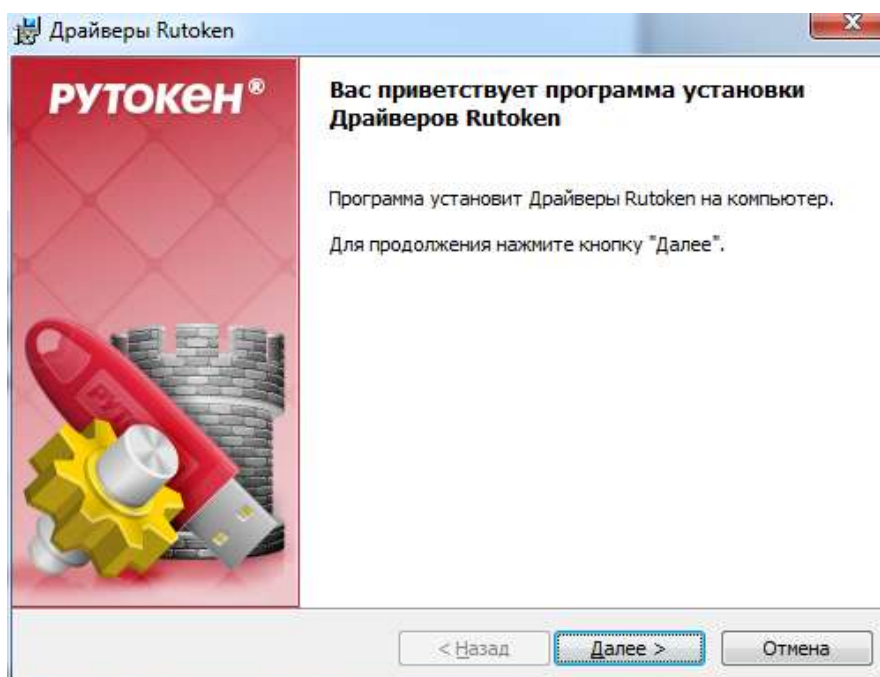


Рисунок 17. Экранная форма приветствия установщика драйвера Rutoken

2. Нажмите кнопку «Далее». На экране отобразится диалог о готовности к выполнению установки драйверов.

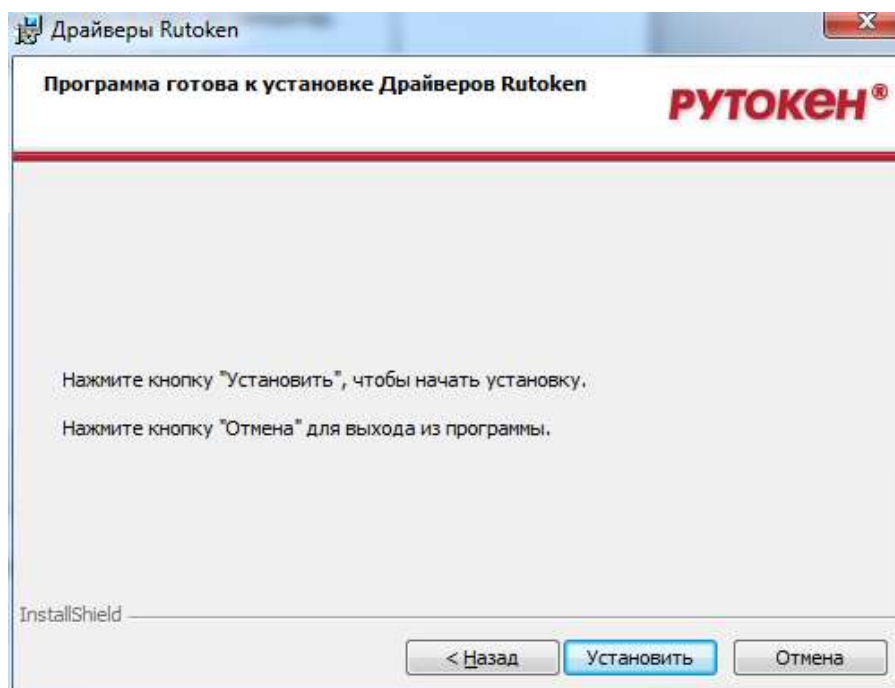


Рисунок 18. Сообщение о готовности к выполнению установки драйверов.

3. Нажмите кнопку «Установить». Начнется установка драйверов Rutoken на АРМ пользователя. Установка может занять несколько минут, информация о прогрессе установки выводится в окне, представленном на рисунке (Рисунок 19).

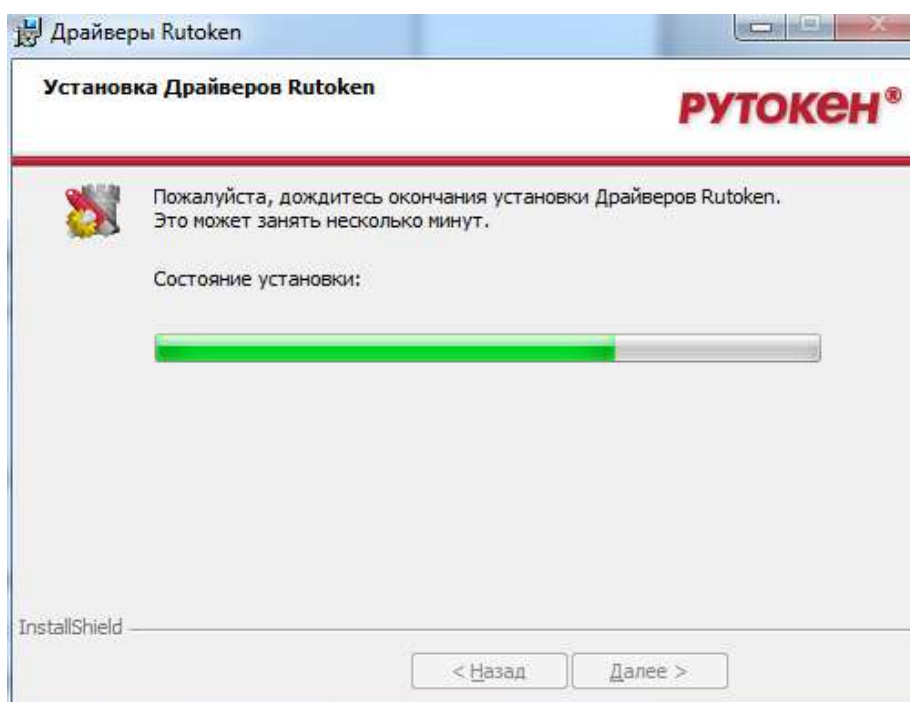


Рисунок 19. Окно, информирующее о прогрессе установки драйверов Rutoken

После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 20).

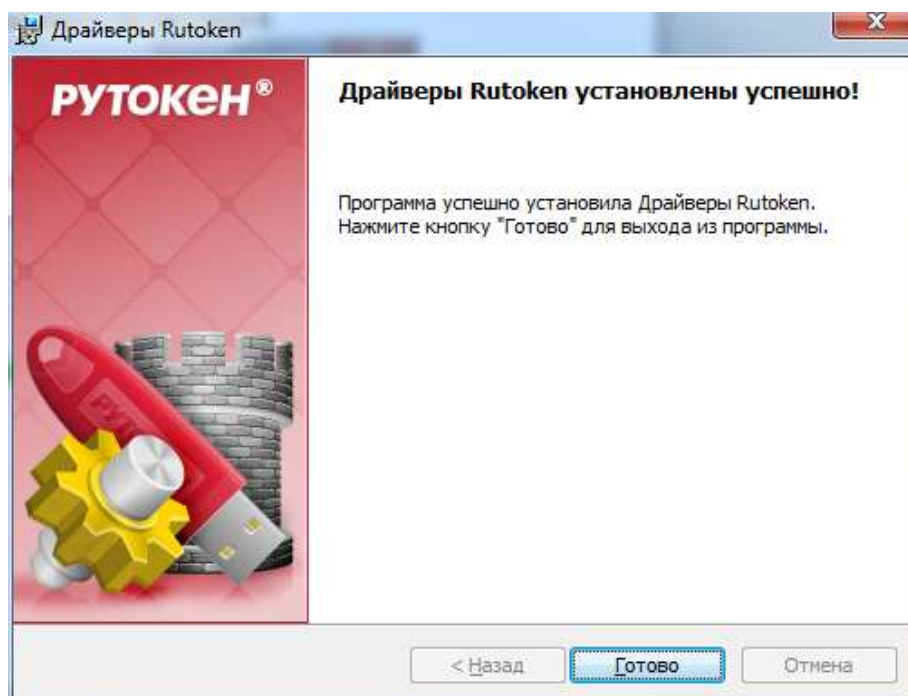


Рисунок 20. Сообщение об успешной установке драйверов Rutoken.

4. Нажмите кнопку «Готово». Окно установщика драйверов Rutoken будет закрыто.

5. В случае появления диалога о необходимости перезагрузки АРМ Пользователя, ответить отрицательно.

б) Драйвер носителя типа eToken

1. Активируйте ссылку eToken в едином меню установщика ПО «Континент TLS Клиент» (см. Рисунок 15). Запустится программа-установщик драйвера eToken. Окно приветствия установщика драйвера eToken представлено на рисунке (**Рисунок 21**).



Рисунок 21. Экранная форма приветствия установщика драйверов eToken

2. Нажмите кнопку «Next». На экране появится диалог выбора языка, который будет использован в устанавливаемом ПО (**Рисунок 22**).



Рисунок 22. Окно выбора языка программы, управляющей ключевыми носителями eToken

3. Так как для решения задач, возникающих при работе в системе «Электронный бюджет», данное ПО не будет использоваться пользователями системы, то выбор языка можно пропустить, нажав кнопку «Next». На экране появится диалог лицензионное соглашение (**Рисунок 23**).

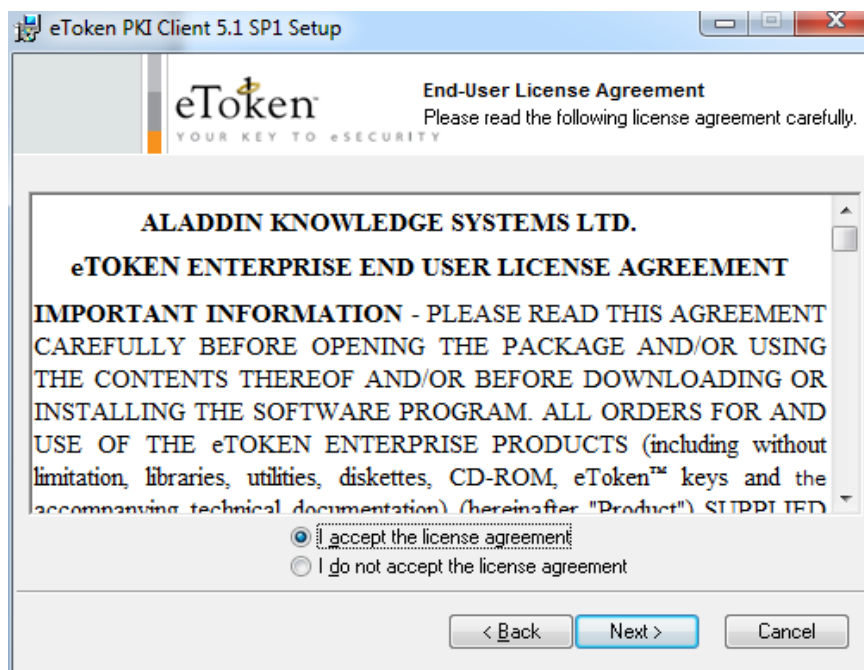


Рисунок 23. Окно просмотра лицензионного соглашения

4. Выберите пункт «I accept the license agreement» и нажмите кнопку «Next». На экране появится диалог выбора пути установки компонентов устанавливаемого ПО (**Рисунок 24**).

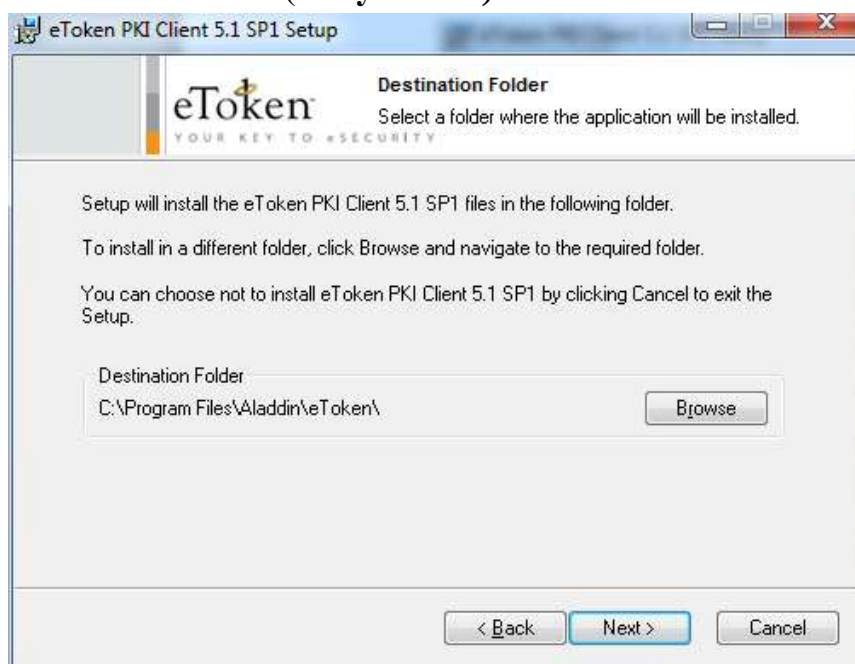


Рисунок 24. Окно выбора пути для установки программы

5. Оставьте путь установки по умолчанию либо измените на необходимый. Нажмите кнопку «Next».

Начнется установка программы и драйверов. Диалог процесса установки представлено на рисунке (Рисунок 25).

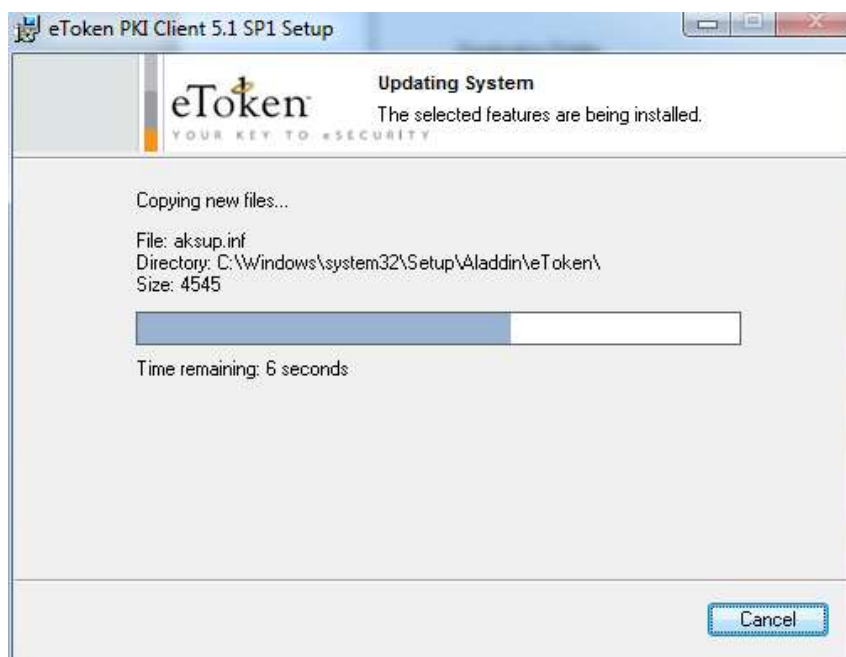


Рисунок 25. Прогресс установки драйверов eToken

После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 26).

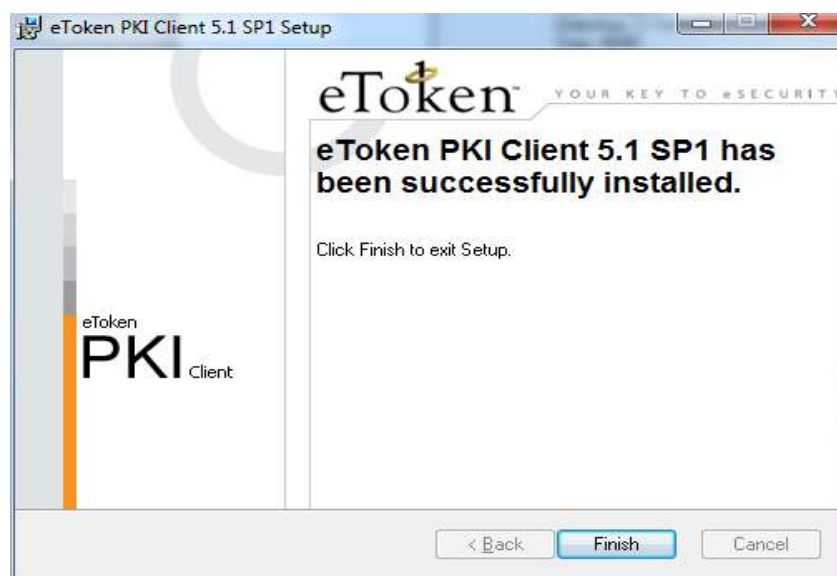


Рисунок 26. Сообщение об успешной установке драйверов Rutoken

6. Нажмите кнопку «Finish». Окно установщика драйверов будет закрыто.
7. В случае появления диалога о необходимости перезагрузки АРМ пользователя, ответить отрицательно.

3.7 Установка программного обеспечения «Jinn-Admin»

Установка ПО «Jinn-Admin» осуществляется по желанию пользователя, для генерации запроса к УЦ на получение квалифицированного сертификата пользователя в случае, если получение сертификата будет осуществляться не в УЦ Федерального казначейства.

Для установки необходимо:

1. В меню единого установщика ПО «Континент TLS Клиент» активировать ссылку «Jinn-Admin» (см. Рисунок 15).
2. На экране отобразится стартовое окно установки ПО «Jinn-Admin». Нажмите кнопку «Далее».

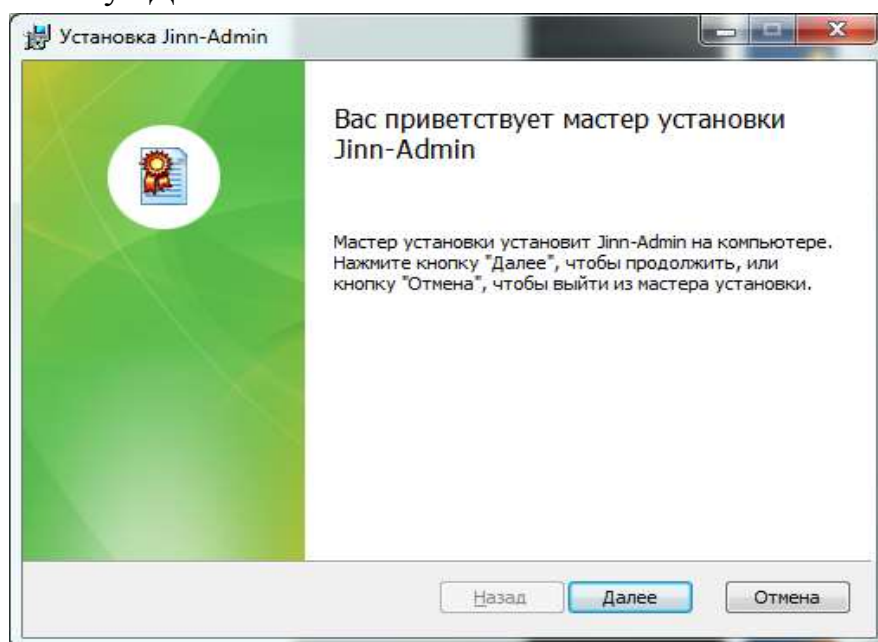


Рисунок 27. Окно приветствия ПО «Jinn-Admin»

3. На экране отобразится диалог с лицензионным соглашением. Отметьте значение «Я принимаю условия лицензионного соглашения» и нажмите кнопку «Далее».

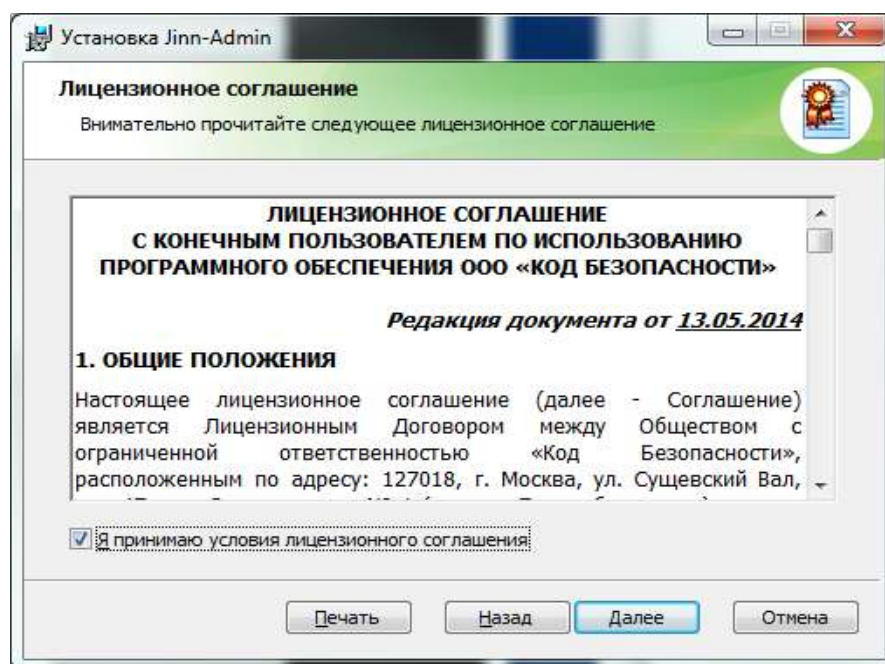


Рисунок 28. Окно лицензионного соглашения ПО «Jinn-Admin»

4. На экране отобразится диалог для ввода лицензионного ключа продукта, поставляемого вместе с дистрибутивом ПО «Jinn-Client» в электронном или печатном виде.

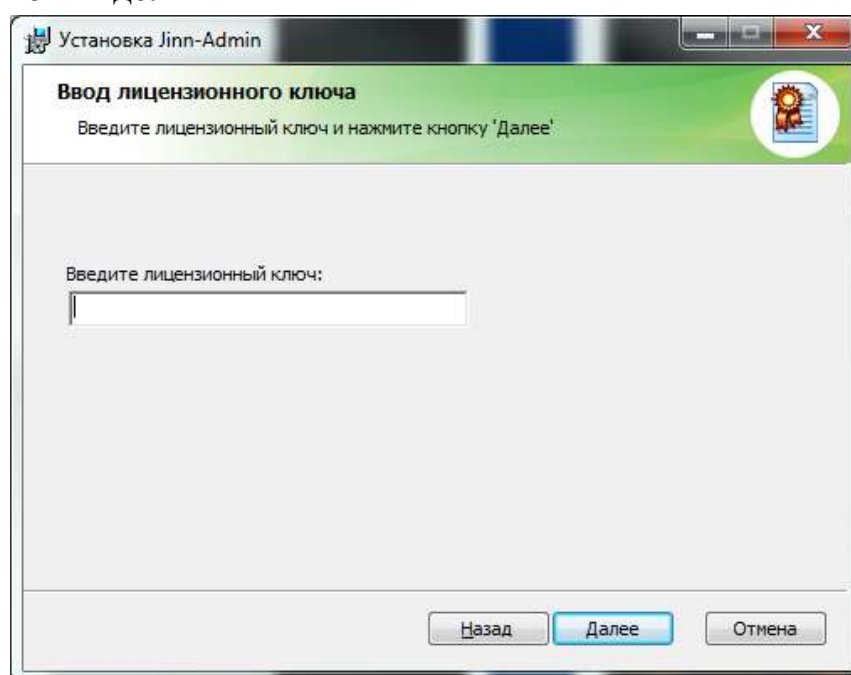


Рисунок 29. Окно ввода лицензионного ключа ПО «Jinn-Admin»

5. Введите регистрационный ключ и нажмите кнопку «Далее».
6. На экране отобразится диалог выбора папки для размещения файлов ПО.

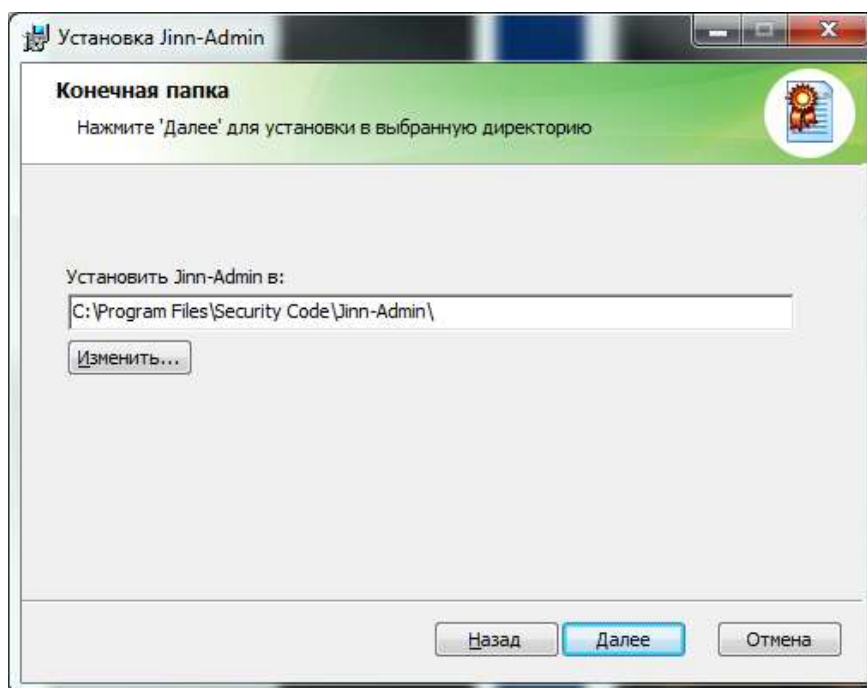


Рисунок 30. Диалог выбора папки для размещения файлов ПО «Jinn-Admin»

7. При необходимости укажите другую папку. Нажмите кнопку «Далее».
8. На экране отобразится диалог с сообщением о готовности к установке. Нажмите кнопку «Установить».

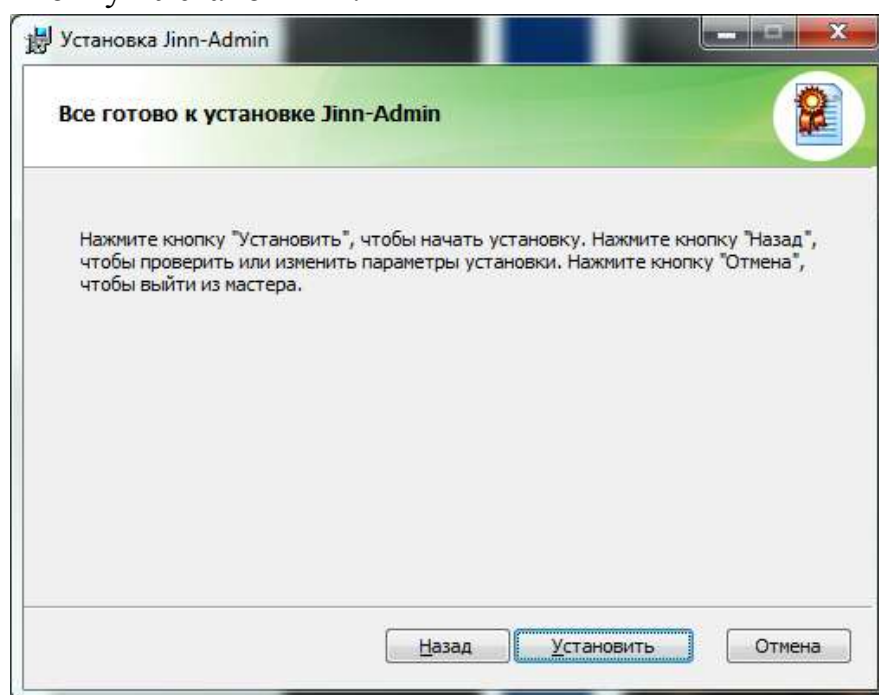
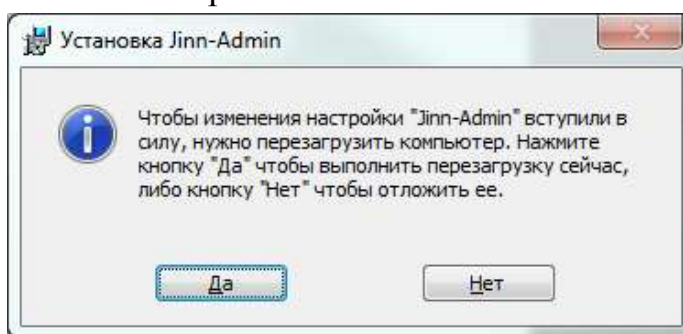


Рисунок 31. Диалог готовности к установке ПО «Jinn-Admin»

9. Программа установки приступит к копированию файлов. Ход процесса установки отображается в виде индикатора прогресса. По завершении установки на экране появится заключительный диалог программы установки.

10. Нажмите кнопку «Готово». На экране отобразится диалог о необходимости перезагрузки компьютера.



- Рисунок 32. Диалог о необходимости перезагрузки АРМ Пользователя
11. Нажать кнопку «Нет».

3.8 Установка средства создания защищенного TLS-соединения «Континент TLS Клиент»

Для установки ПО «Континент TLS Клиент» необходимо:

1. Активируйте ссылку «Континент TLS Клиент» в едином меню установщика ПО «Континент TLS Клиент» (см. Рисунок 15). На экране отобразится стартовое окно мастера установки компонента.

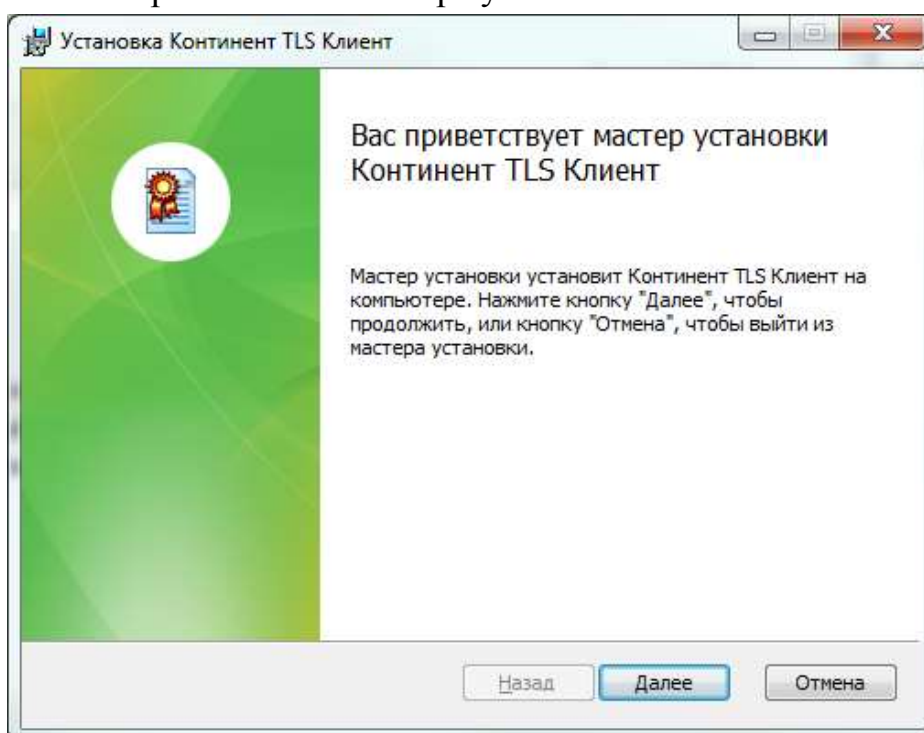


Рисунок 33. Стартовое окно мастера установки ПО «Континент TLS Клиент».

2. Нажать кнопку «Далее». На экране появится окно лицензионного соглашения.

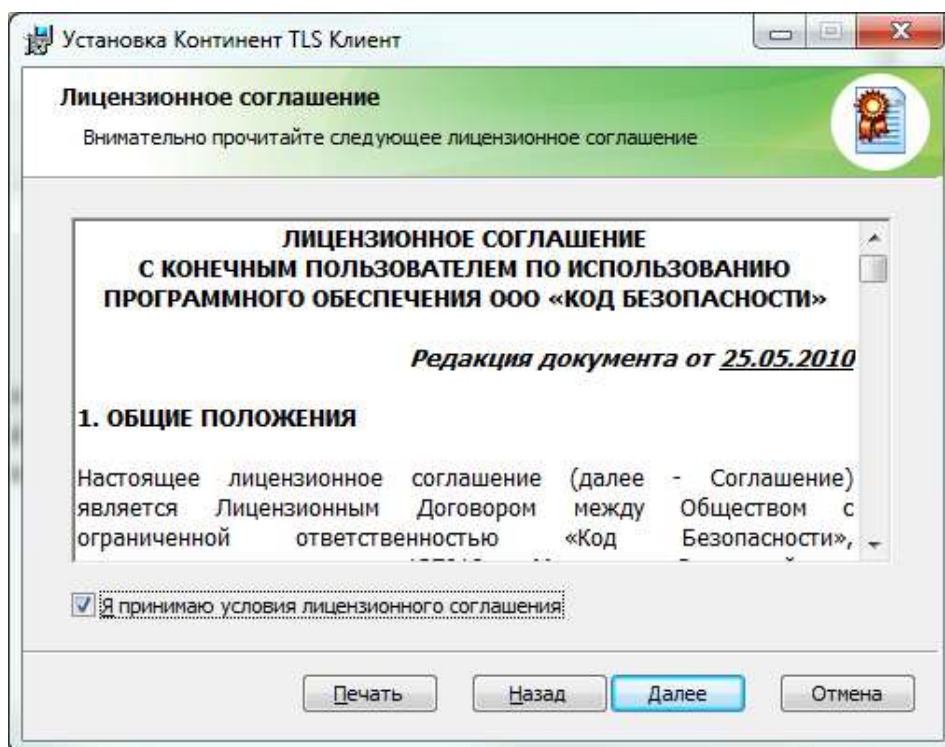


Рисунок 34. Окно лицензионного соглашения ПО «Континент TLS Клиент».

3. Поставьте отметку в поле «Я принимаю условия лицензионного соглашения» и нажмите кнопку «Далее». На экране появится окно ввода лицензионного ключа, поставляемого с ПО «Континент TLS Клиент» на бумажном или электронном носителе.

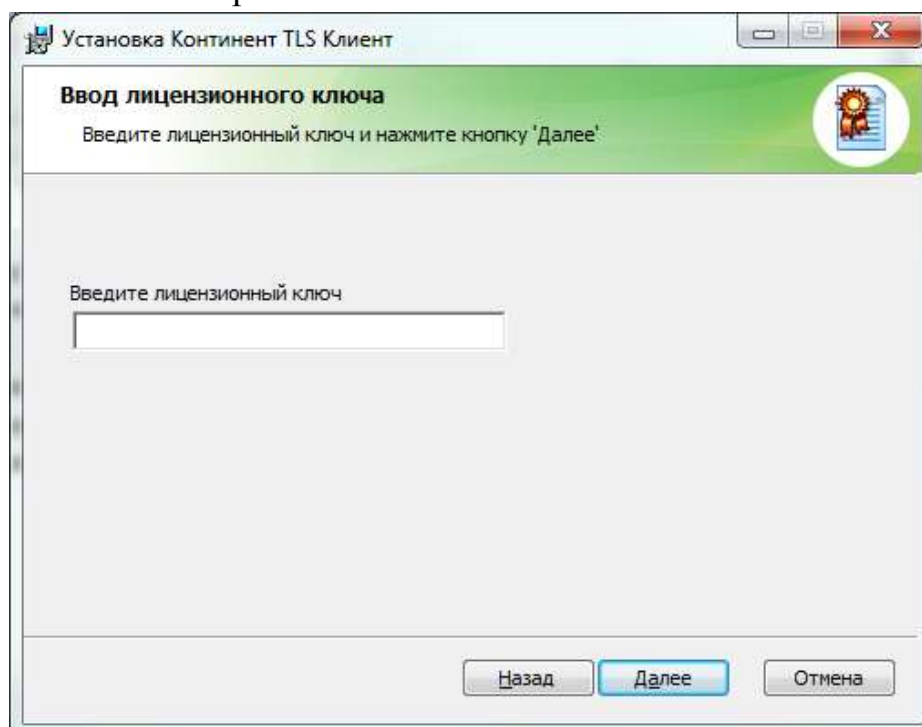


Рисунок 35. Окно ввода лицензионного ключа ПО «Континент TLS Клиент».

4. Введите лицензионный ключ и нажмите кнопку «Далее». На экране появится диалог выбора пути установки ПО «Континент TLS Клиент».

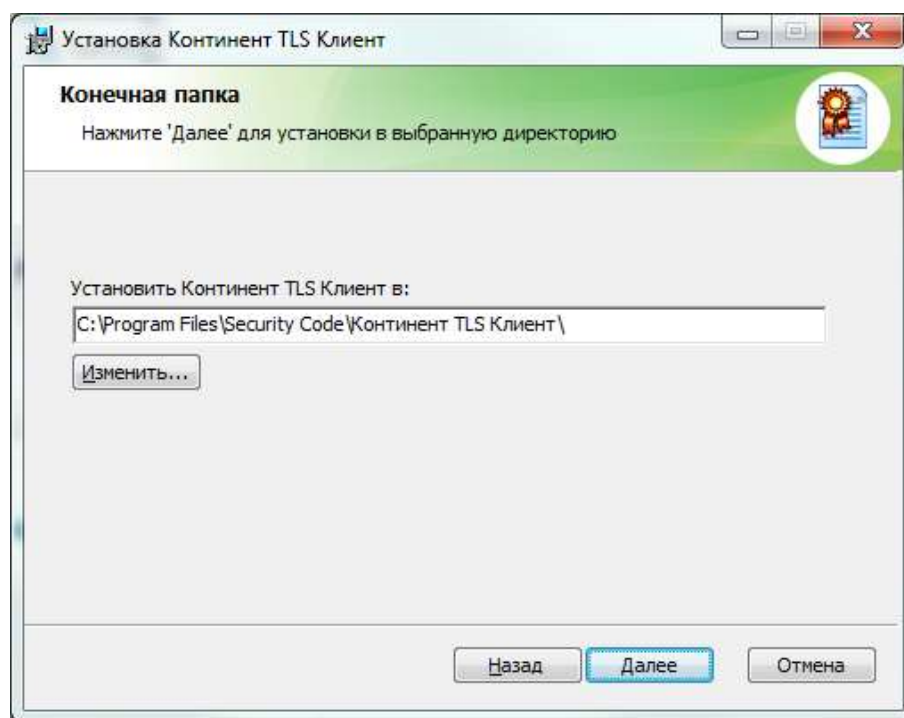


Рисунок 36. Окно выбора пути установки ПО «Континент TLS Клиент».

5. Оставьте путь установки по умолчанию. Нажмите кнопку «Далее». На экране появится диалог «Запуск configurатора».

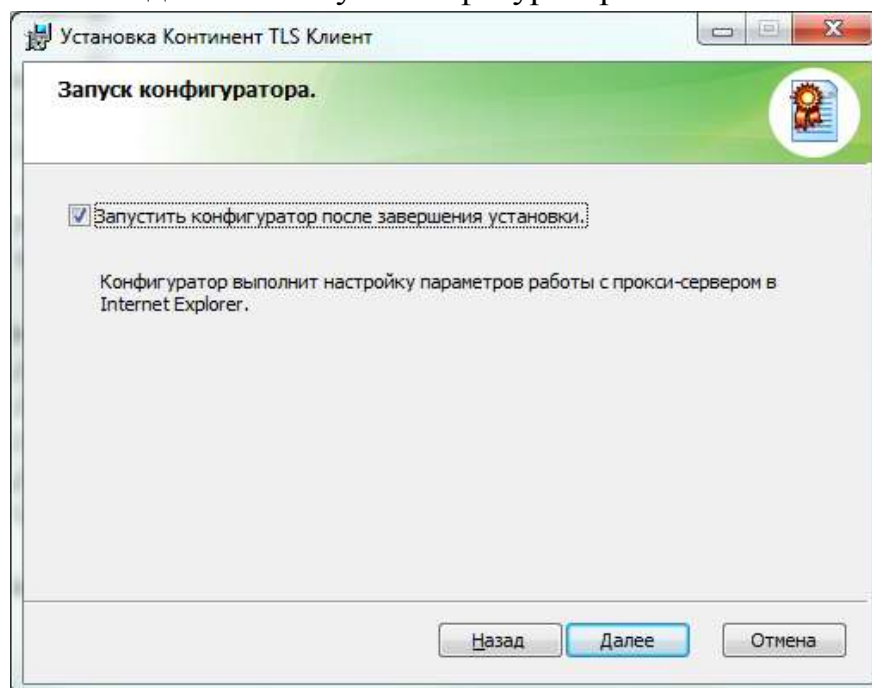


Рисунок 37. Окно запуска configurатора ПО «Континент TLS Клиент».

6. Установите отметку в поле «Запустить конфигуратор после завершения установки».
7. Нажмите кнопку «Далее». На экране появится окно с сообщением о готовности к установке.

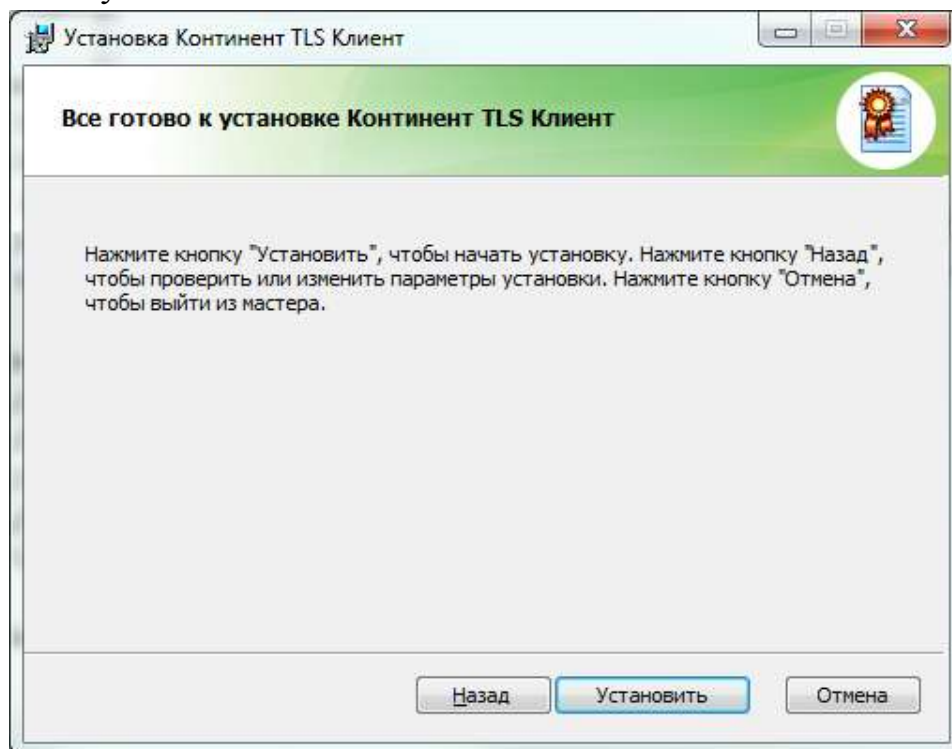


Рисунок 38. Окно готовности к установке ПО «Континент TLS Клиент».

8. Нажмите кнопку «Установить». Начнется установка компонента.

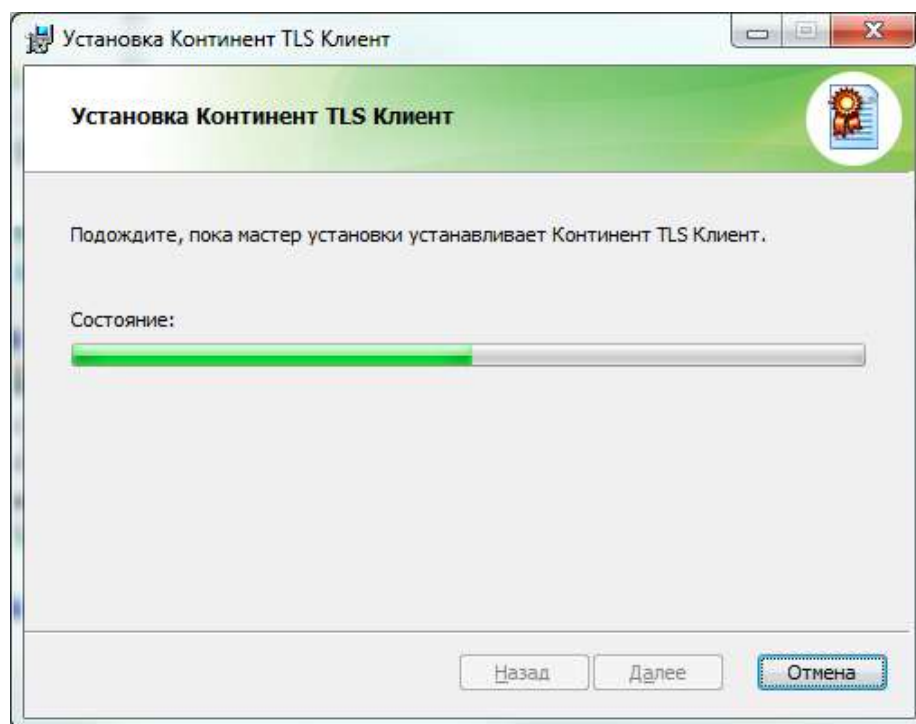


Рисунок 39. Процесс установки ПО «Континент TLS Клиент».

9. На экране отобразится диалог настройки ПО «Континент TLS Клиент».

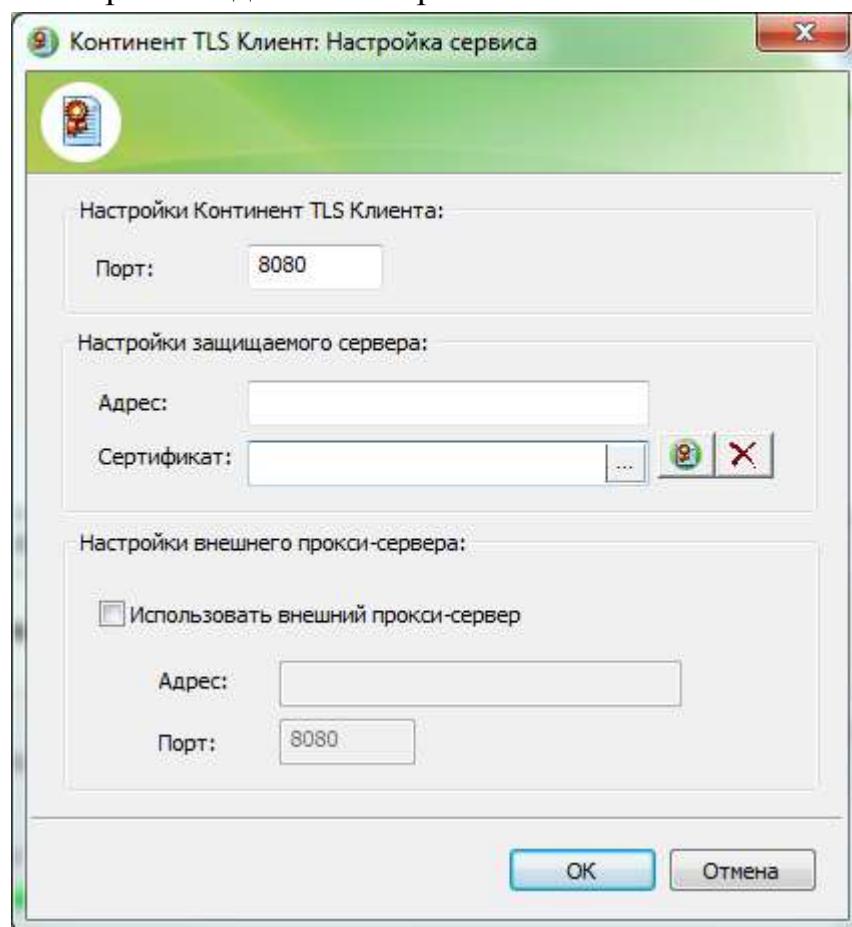


Рисунок 40. Настройка ПО «Континент TLS Клиент».

Для настройки ПО необходимо:

- а) В разделе «Настройки Континент TLS Клиента» значение «Порт» оставить по умолчанию, равное 8080.
- б) В разделе «Настройки защищаемого сервера» в поле «Адрес» задать имя сервера TLS: lk.budget.gov.ru.
- с) В разделе «Настройки защищаемого сервера» в поле «Сертификат» указать файл сертификата сервера TLS, скопированный в локальную директорию в п.3.1 настоящего Руководства.

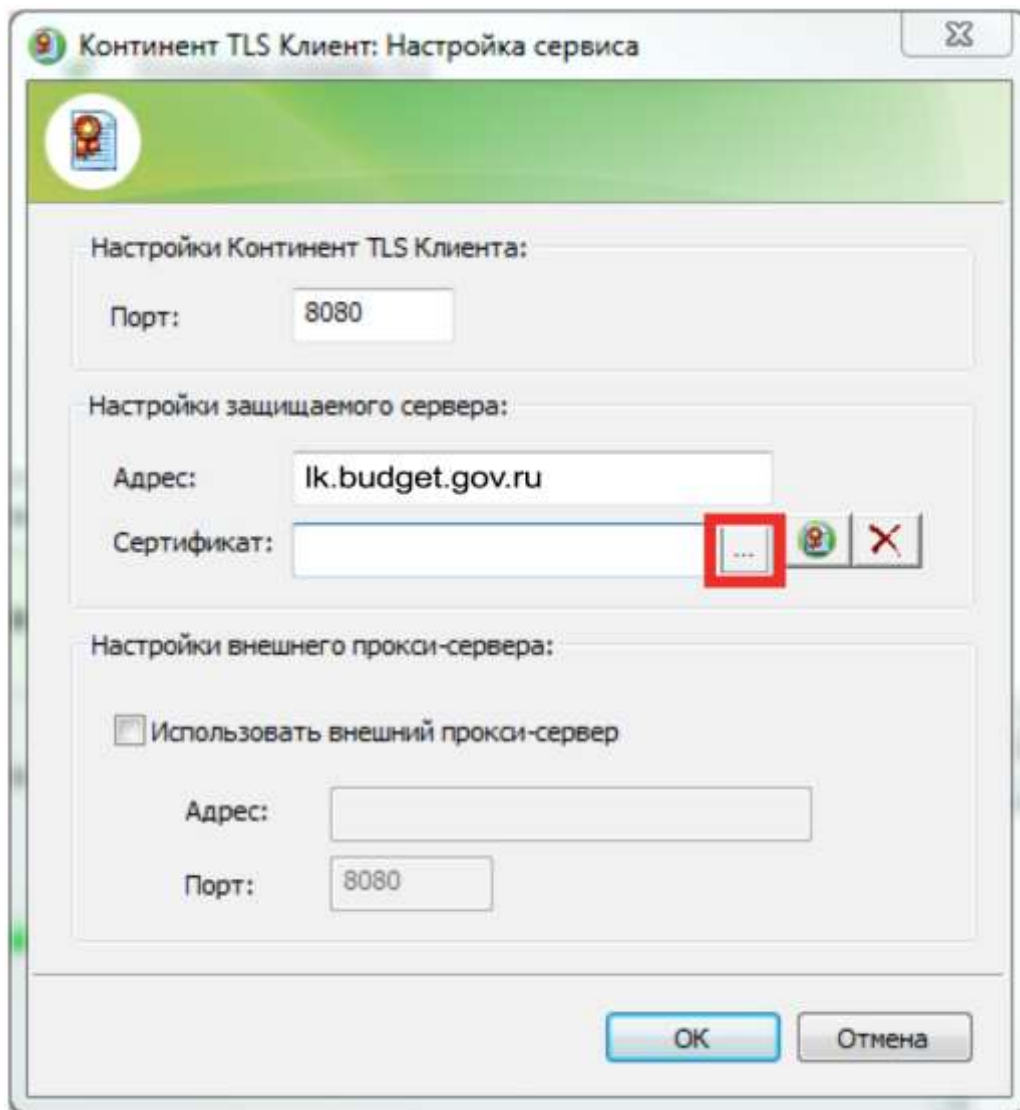


Рисунок 41. Настройка ПО «Континент TLS Клиент». Выбор сертификата.

- д) Если в АРМ пользователя не используется внешний прокси-сервер, нажать кнопку «ОК».
- е) В противном случае, указать адрес и порт используемого внешнего прокси-сервера организации.

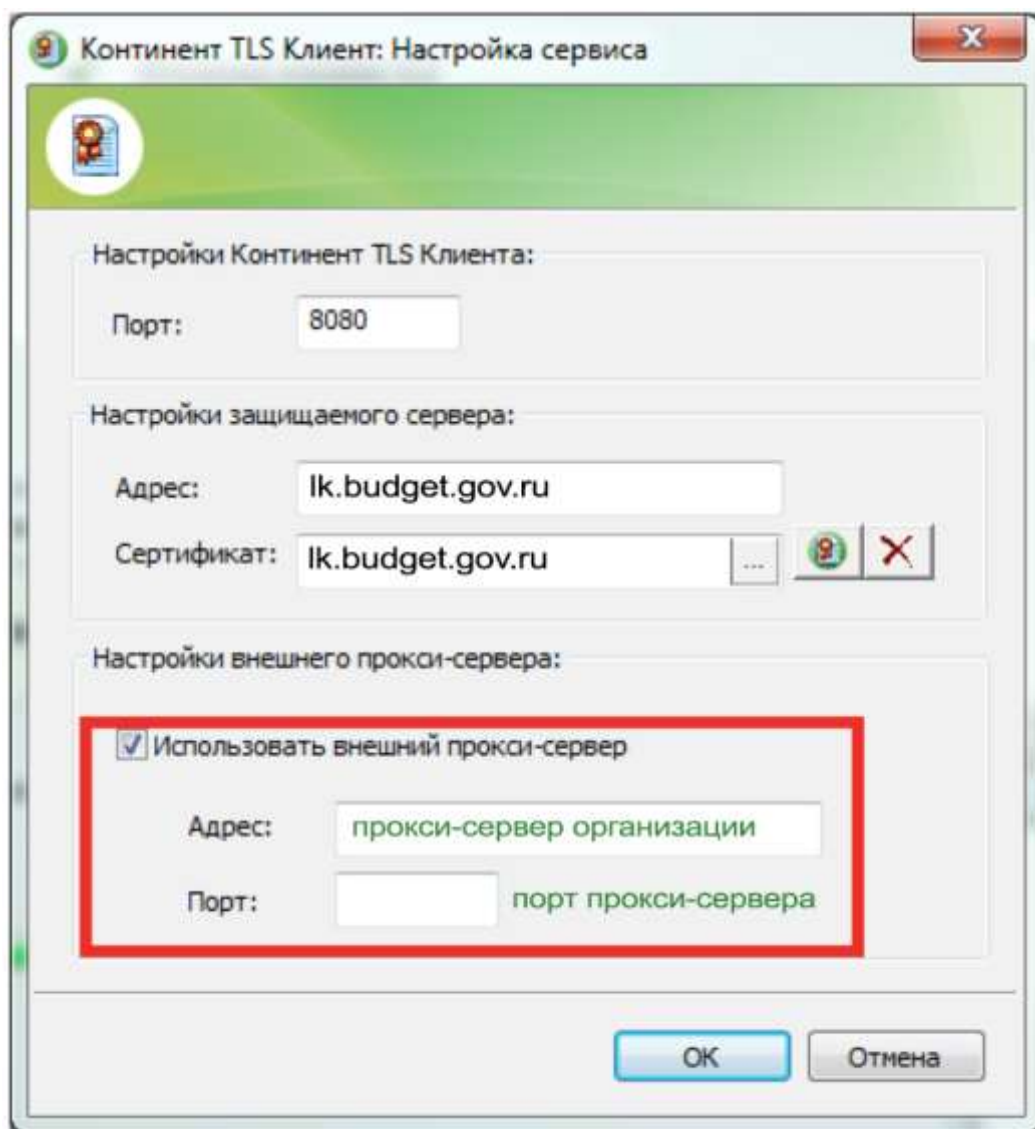


Рисунок 42. Настройка сервиса ПО «Континент TLS Клиент».
Настройка внешнего прокси-сервера.

f) Нажать кнопку «ОК».

10. На экране отобразится диалог завершения установки ПО «Континент TLS Клиент».

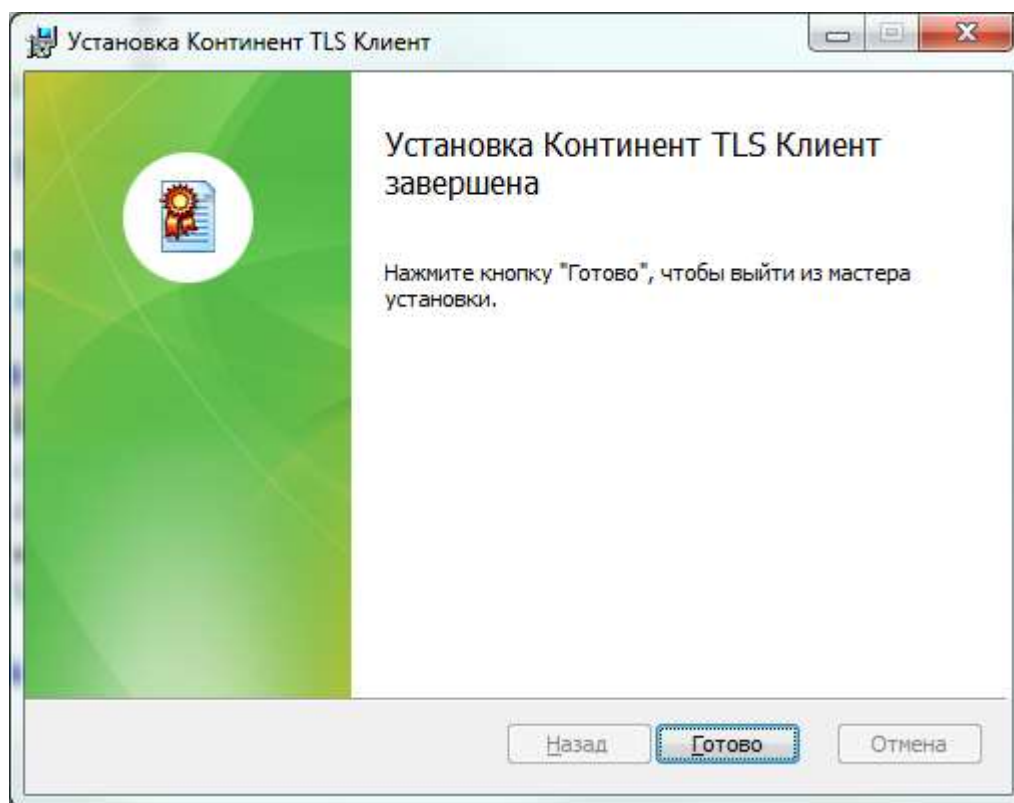


Рисунок 43. Диалог завершения установки ПО «Континент TLS Клиент».

11. Нажать кнопку «Готово».

12. На экране отобразится диалог о необходимости перезагрузки АРМ пользователя.

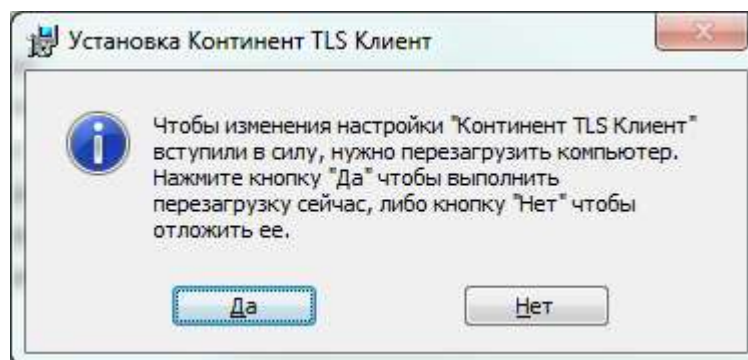


Рисунок 44. Диалог о необходимости перезагрузки АРМ Пользователя.

13. Нажать кнопку «Нет».

3.9 Настройка веб-обозревателя

Настройка веб-обозревателя для подключения к системе «Электронный бюджет» зависит от используемого пользователем типа веб-обозревателя.

a) Internet Explorer

1. Открыть свойства веб-обозревателя.
2. Перейти на вкладку «Подключения».
3. Нажать кнопку «Настройка сети».
4. В разделе «Прокси-сервер» задать поля Адрес: 127.0.0.1, Порт: 8080.

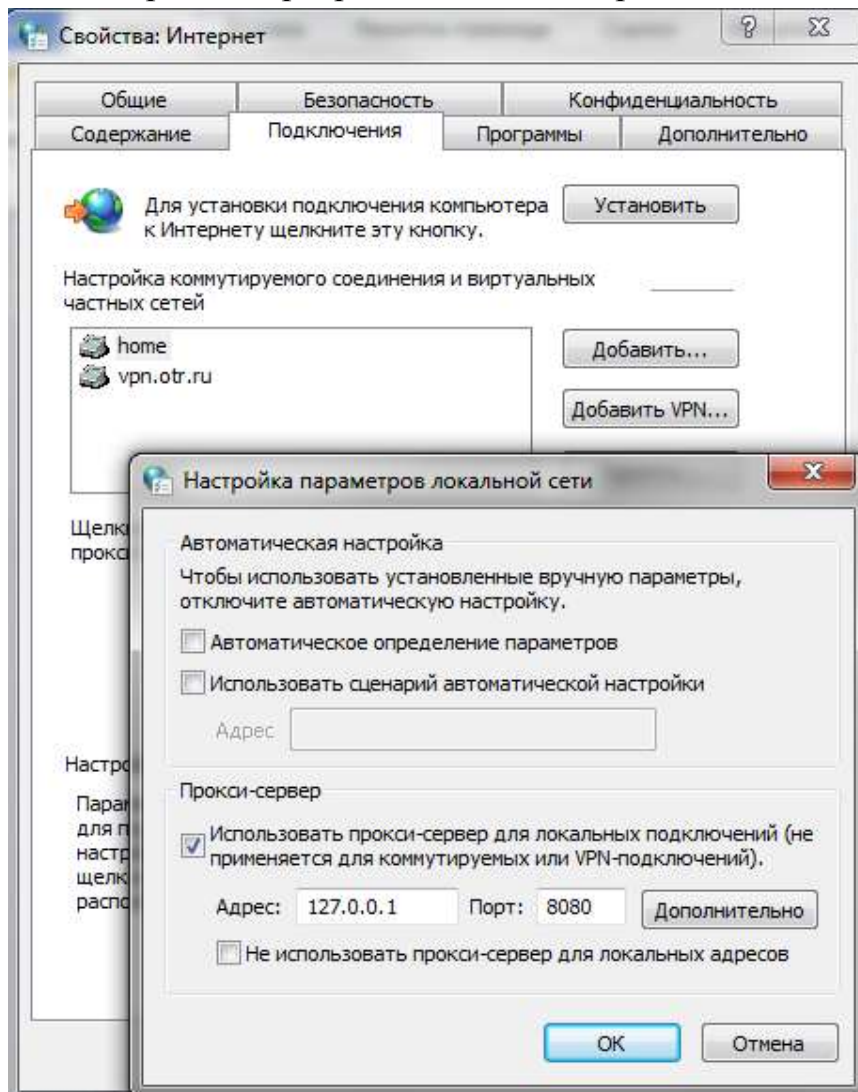


Рисунок 45. Диалог настройки прокси-сервера

5. Нажать кнопку «ОК».
6. Перейти на вкладку «Безопасность».

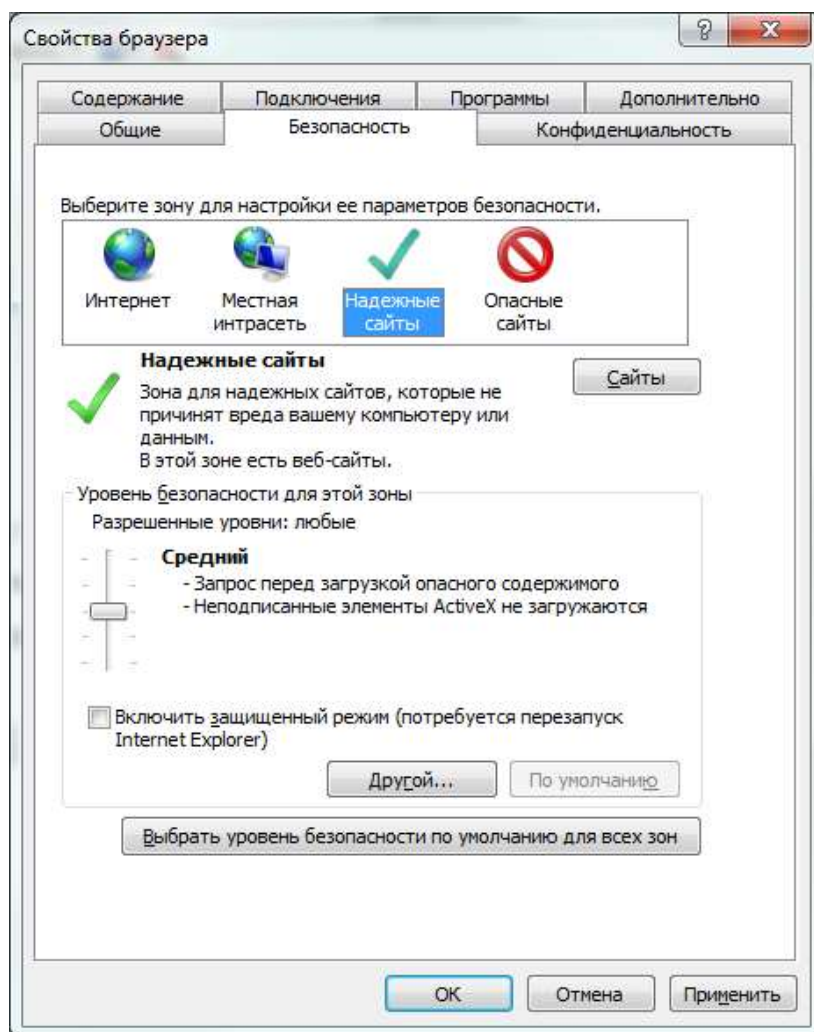


Рисунок 46. Диалог настройки безопасности браузера.

7. Выбрать зону для настройки «Надежные узлы».
8. Нажать кнопку «Сайты».

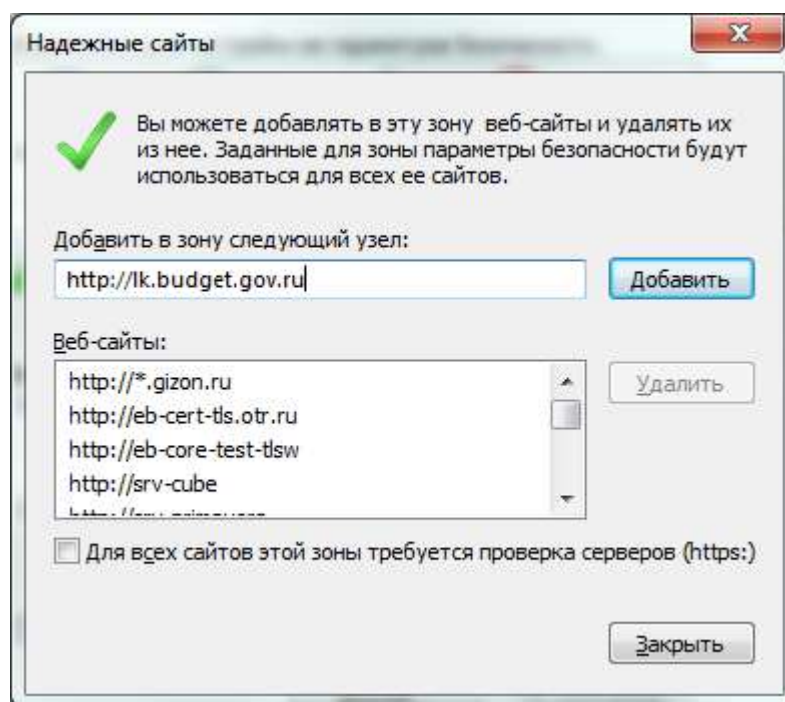


Рисунок 47. Диалог настройки доверенных узлов.

9. В окне «Надежные сайты» снять отметку с поля «Для всех сайтов этой зоны требуется проверка серверов (https:)».
10. В поле «Добавить в зону следующий узел» задать значение «http://lk.budget.gov.ru» и нажать кнопку «Добавить».
11. В окне «Надежные сайты» нажать кнопку «Закреть».
12. В окне «Свойства браузера» нажать кнопку «ОК».

b) Google Chrome

1. Открыть настройки веб-обозревателя.
2. Перейти вниз окна настроек и активировать ссылку «Показать дополнительные настройки».
3. Нажать кнопку «Изменить настройки прокси-сервера».
4. Повторить п.4-12 раздела «a) Internet Explorer».

c) Mozilla Firefox

1. Откройте меню «Инструменты» и выберите пункт «Настройки».
2. Перейти в раздел «Дополнительные» на вкладку «Сеть».
3. В секции настроек «Соединение» нажать кнопку «Настроить...».
4. В открывшемся окне параметров соединения установить значение «Ручная настройка сервиса прокси».
5. Задать значения полей HTTP-прокси: 127.0.0.1; Порт: 8080.
6. Нажать кнопку «ОК».

7. В окне «Настройки» нажать кнопку «Ок».

d) Opera

1. Откройте меню «Настройка\Общие настройки».
2. Перейти на вкладку «Расширенные», выбрать раздел настроек «Сеть».
3. Нажать кнопку «Прокси-серверы...».
4. В открывшемся окне параметров соединения установить значение «Конфигурировать прокси-сервер вручную».
5. Для протокола HTTP задать значения полей прокси-сервер: 127.0.0.1; Порт: 8080.
6. Установить значение «Использовать прокси-сервер для всех протоколов».

3.10 Установка средства электронной подписи «Jinn-Client»

Для установки ПО «Jinn-Client» необходимо:

1. В АРМ пользователя вставить носитель информации, содержащий дистрибутив ПО «Jinn-Client».
2. В составе дистрибутива ПО «Jinn-Client» осуществить запуск исполняемого файла «Setup». На экране отобразится меню единого установщика ПО «Jinn-Client».

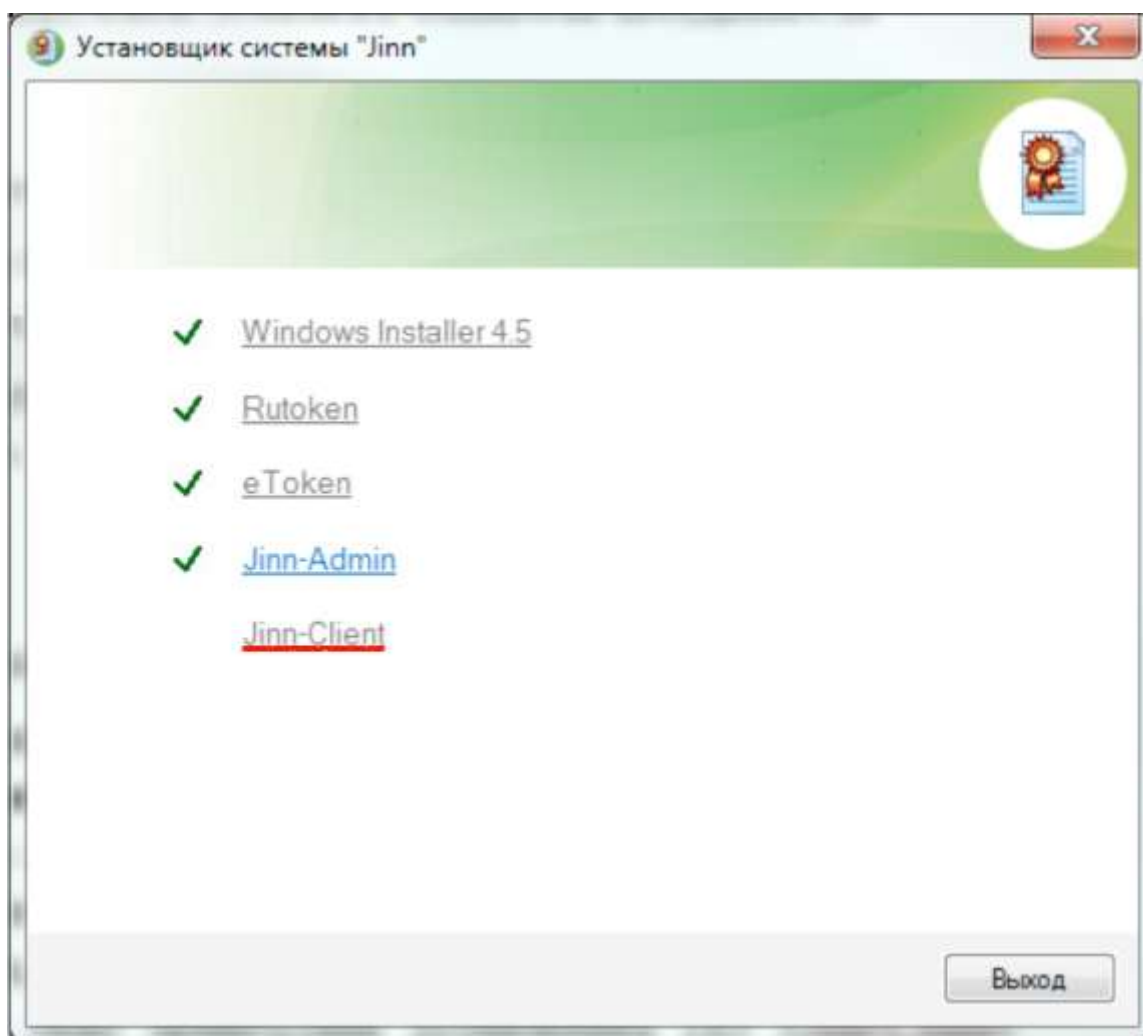


Рисунок 48. Меню единого установщика ПО «Jinn-Client»

3. В меню установщика ПО «Jinn-Client» активировать ссылку «Jinn-Client».

На экране отобразится диалог приветствия установщика ПО «Jinn-Client» (Рисунок 49)

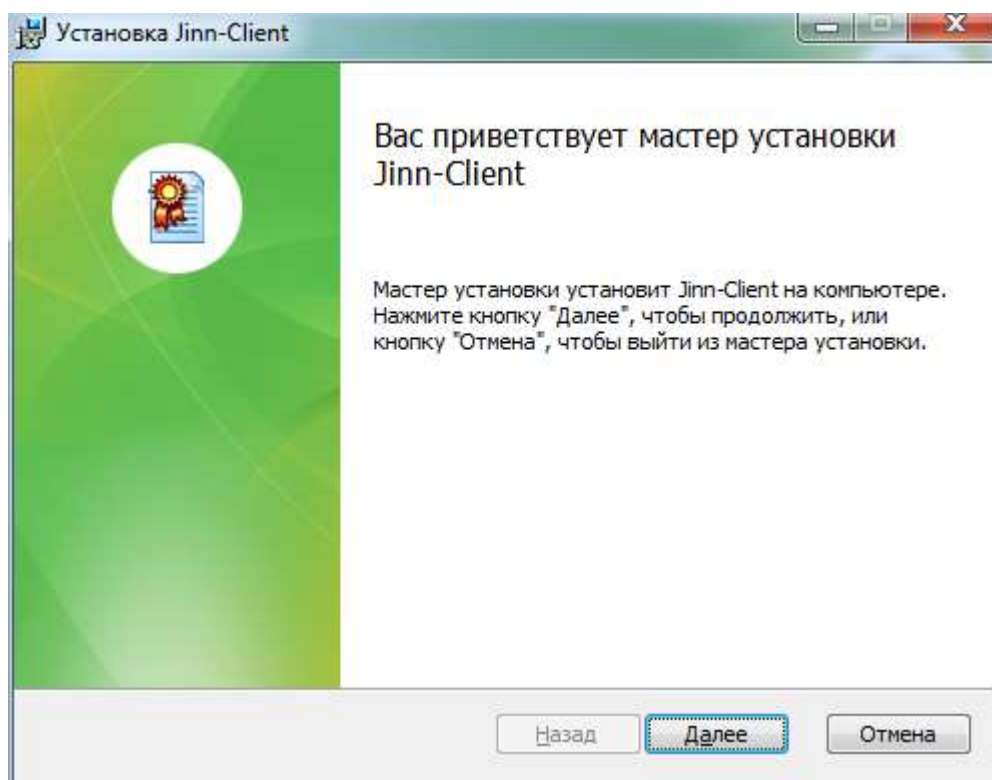


Рисунок 49. Окно приветствия установщика Jinn-Client

4. Для продолжения установки нажмите кнопку «Далее».
5. В появившемся диалоге лицензионного соглашения отметить пункт «Я принимаю условия лицензионного соглашения» (**Рисунок 50**) и нажать кнопку «Далее».

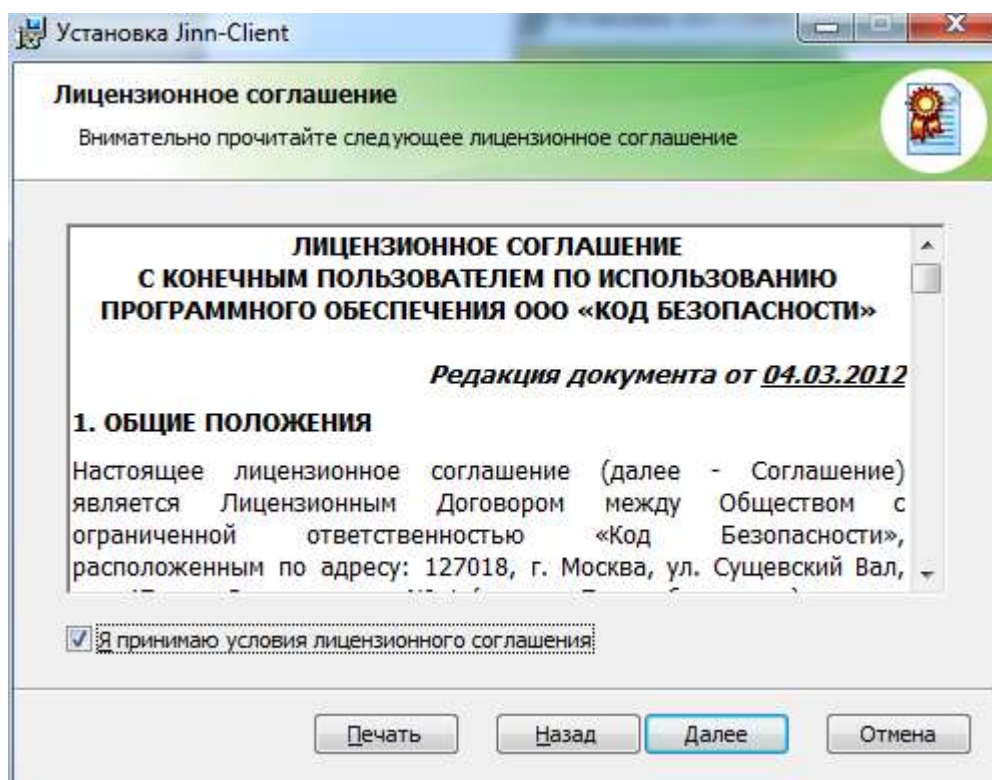


Рисунок 50. Окно просмотра лицензионного соглашения

На экране отобразится диалог ввода лицензионного ключа (**Рисунок 51**), поставляемого вместе с дистрибутивом ПО «Jinn-Client» в электронном или бумажном виде.

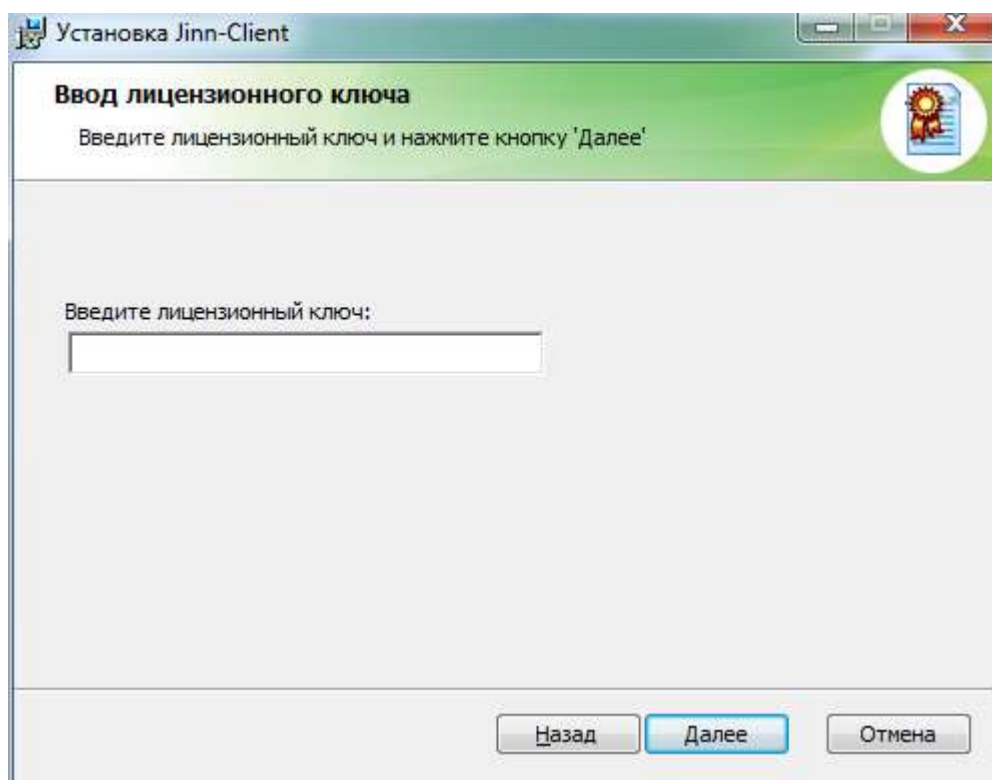


Рисунок 51. Окно ввода лицензионного ключа

6. Введите лицензионный ключ и нажмите кнопку «Далее».

На экране отобразится диалог выбора пути установки ПО «Jinn-Client» (Рисунок 52).

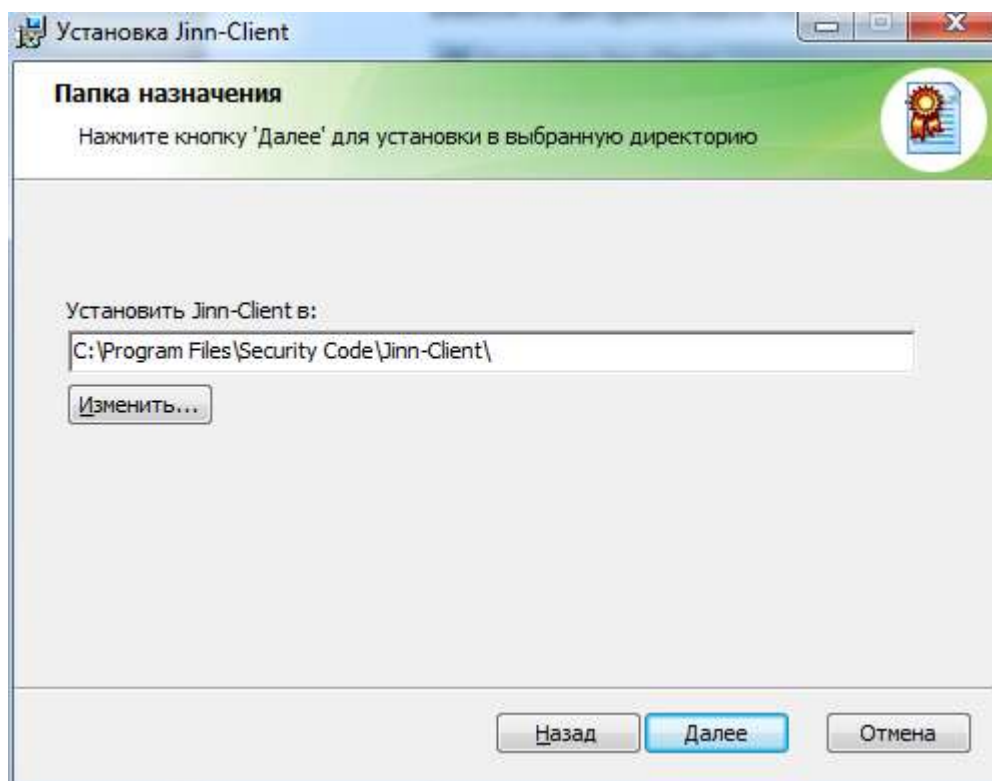


Рисунок 52. Окно выбора пути установки Jinn-Client

7. Оставьте путь установки по умолчанию либо измените на требуемый. Нажмите кнопку «Далее».
8. В диалоге настройки параметров Jinn-Client (Рисунок 53) ничего не изменяя нажмите кнопку «Далее».

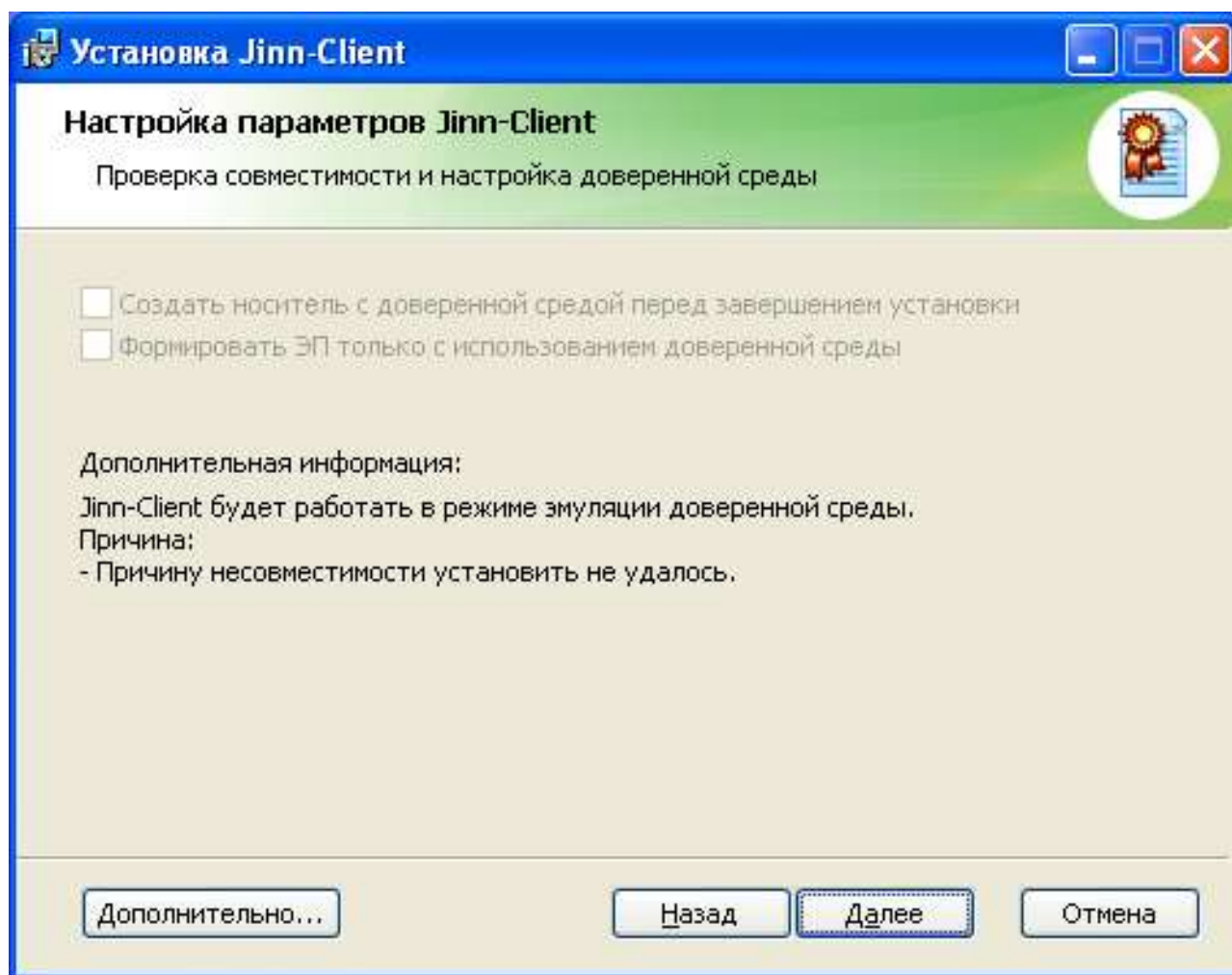


Рисунок 53. Окно настройки параметров Jinn-Client

В случае появления комментария «Процессор не совместим с доверенной средой» выполнять какие-либо действия от пользователя не требуется. Данный комментарий означает, что работа в ПО «Jinn-Client» будет осуществляться без использования режима доверенной среды, процесс установки ПО «Jinn-Client» при этом прерывать не нужно.

Далее пользователю будет выведено информационное сообщение о готовности к установке ПО «Jinn-Client» (**Рисунок 54**).

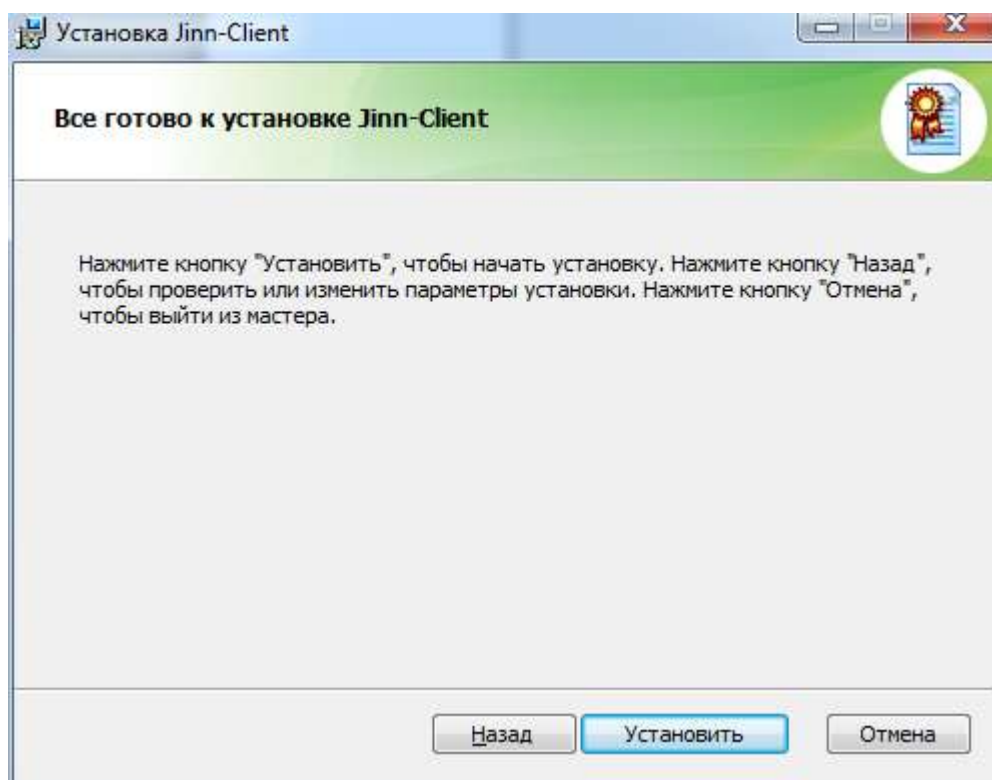


Рисунок 54. Сообщение о готовности к установке Jinn-Client

9. Нажмите кнопку «Установить».

На экране отобразится диалог процесса установки ПО «Jinn-Client» (Рисунок 55).

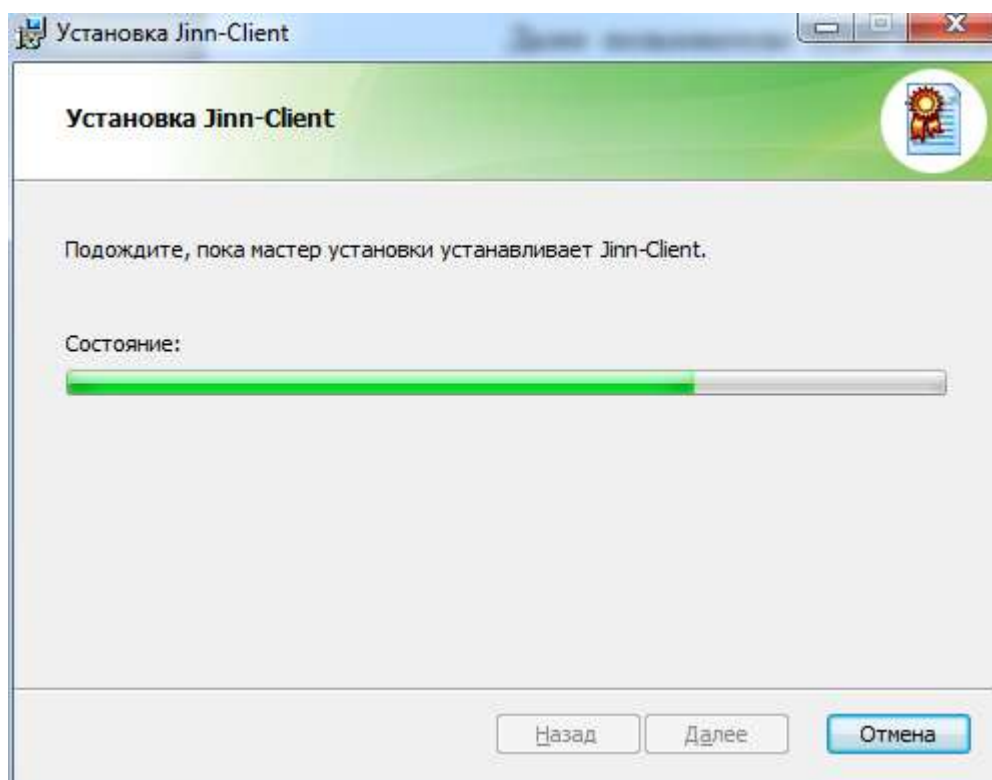


Рисунок 55. Окно, информирующее пользователя о прогрессе в процессе установки Jinn-Client

По завершению установки на экран будет выведен диалог об успешном завершении установки (**Рисунок 56**).

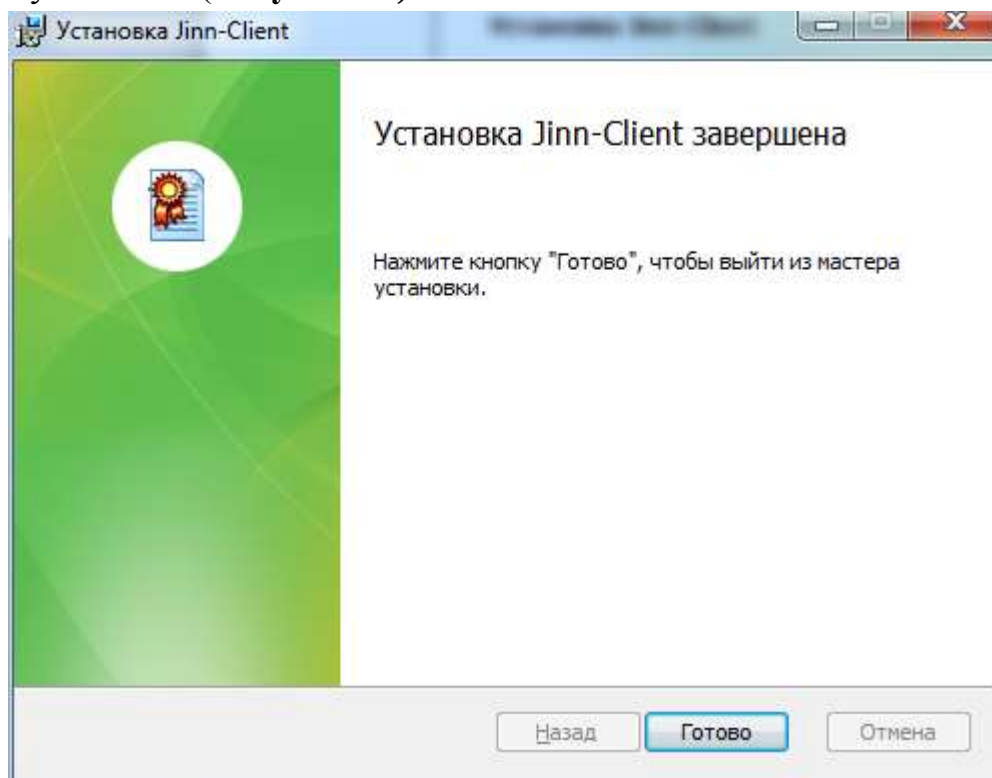


Рисунок 56. Сообщение об успешном завершении установки Jinn-Client

10.Нажмите кнопку «Готово».

11.На экране отобразится диалог о необходимости перезагрузки АРМ пользователя.

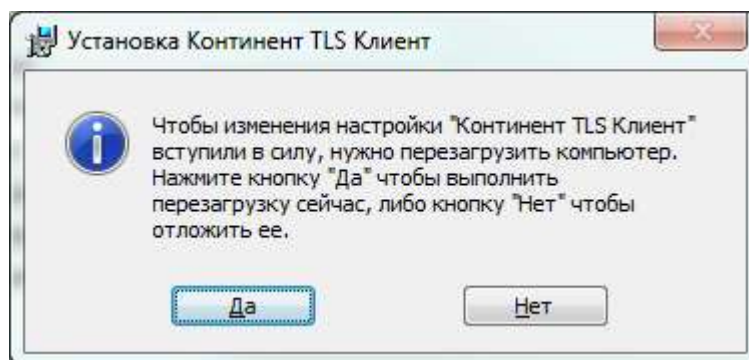


Рисунок 57. Диалог о необходимости перезагрузки АРМ Пользователя.

12.Нажать кнопку «Нет».

После установки ПО «Jinn-Client» дополнительных действий в части настройки данного ПО не требуется.

3.11 Установка модуля для работы с электронной подписью «Cubesign»

3.11.1 Предварительная установка

Для установки модуля для работы с электронной подписью «Cubesign» необходимо выполнить следующие действия:

1. В АРМ пользователя вставить носитель информации, содержащий дистрибутив ПО «Jinn-Client».
2. В составе дистрибутива ПО «Jinn-Client» осуществить запуск исполняемого файла «Cubesign».

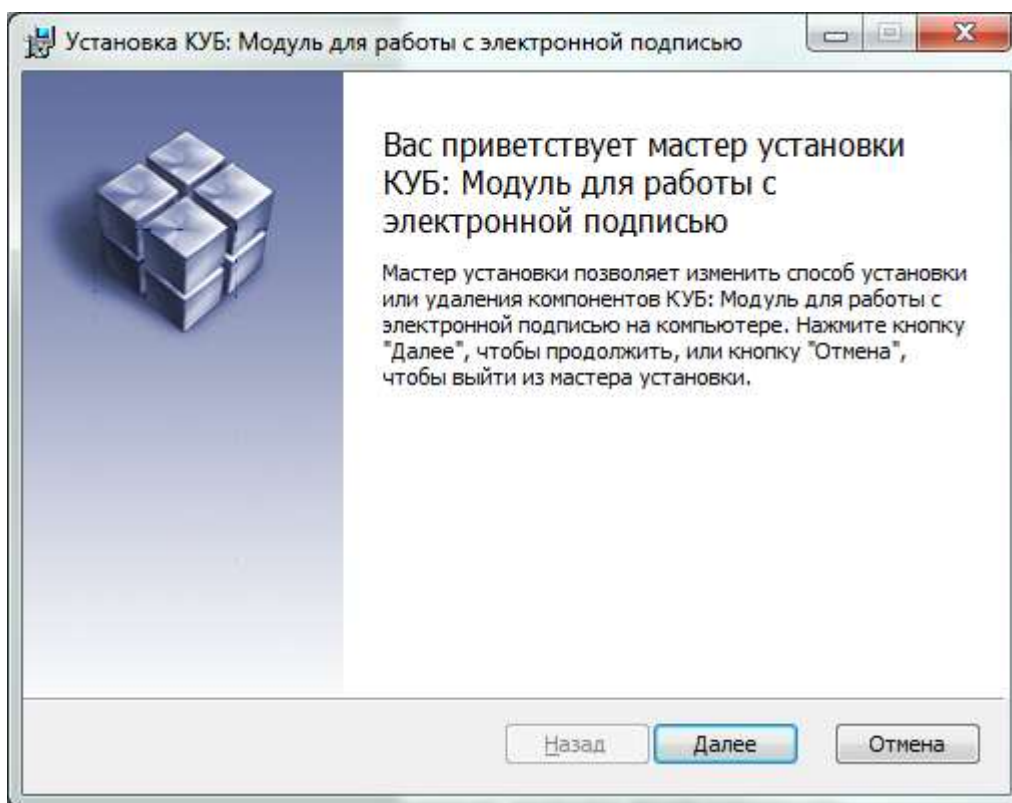


Рисунок 58. Диалог приветствия установщика модуля

3. На экране отобразится диалог приветствия установщика модуля. Нажать кнопку «Далее».
4. На экране отобразится окно лицензионного соглашения.

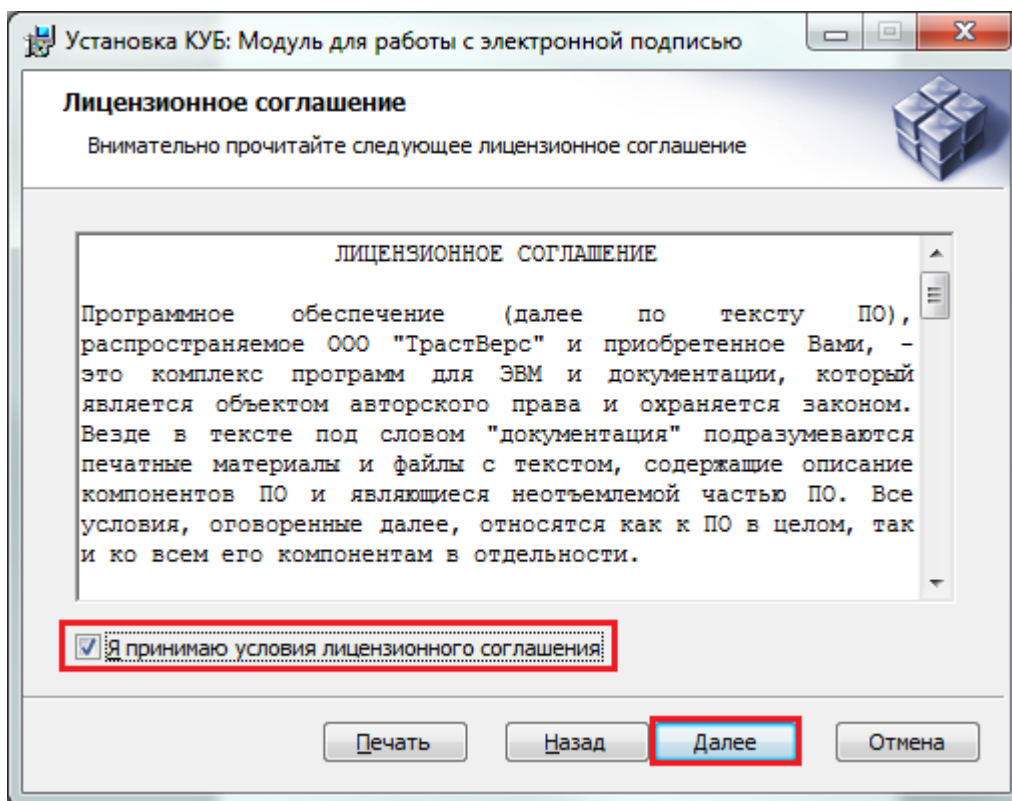


Рисунок 59. Принятие лицензионного соглашения

5. Принять условия лицензионного соглашения поставив галочку в соответствующем поле и нажмите «Далее».

На экране отобразится диалог расположения файлов установки модуля.

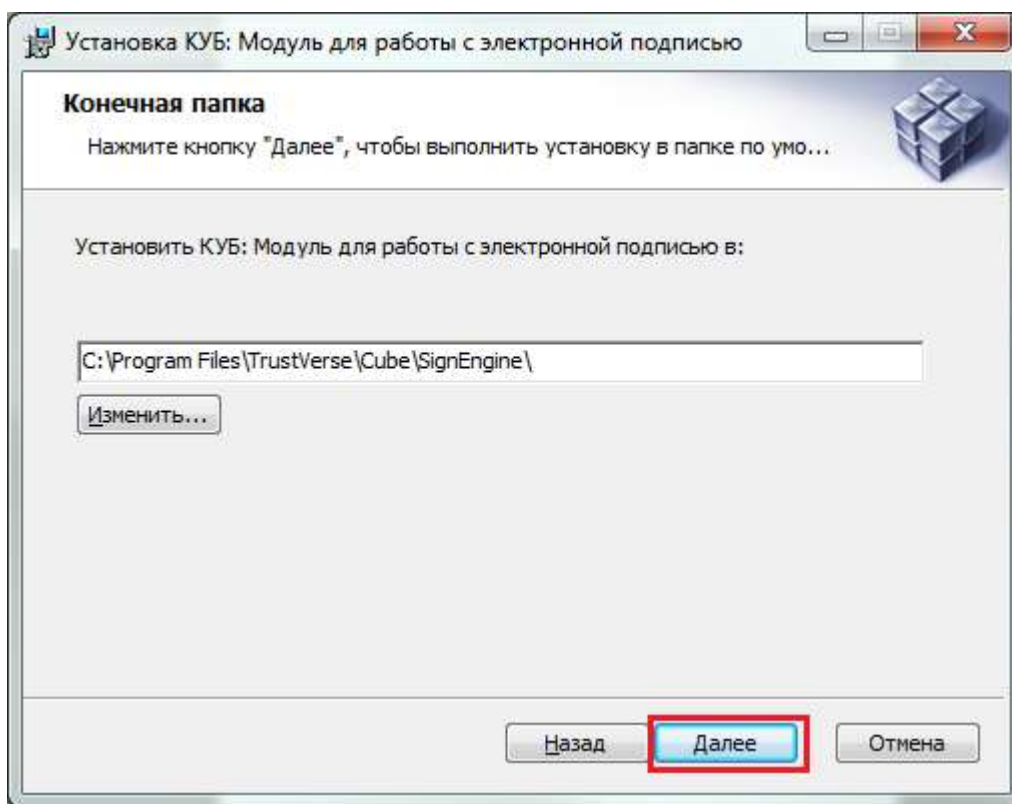


Рисунок 60. Выбор папки для установки

6. Установить компонент средства подписи в папку предложенную по умолчанию и нажмите «Далее».
7. Подтвердить начало установки, нажав кнопку «Установить».

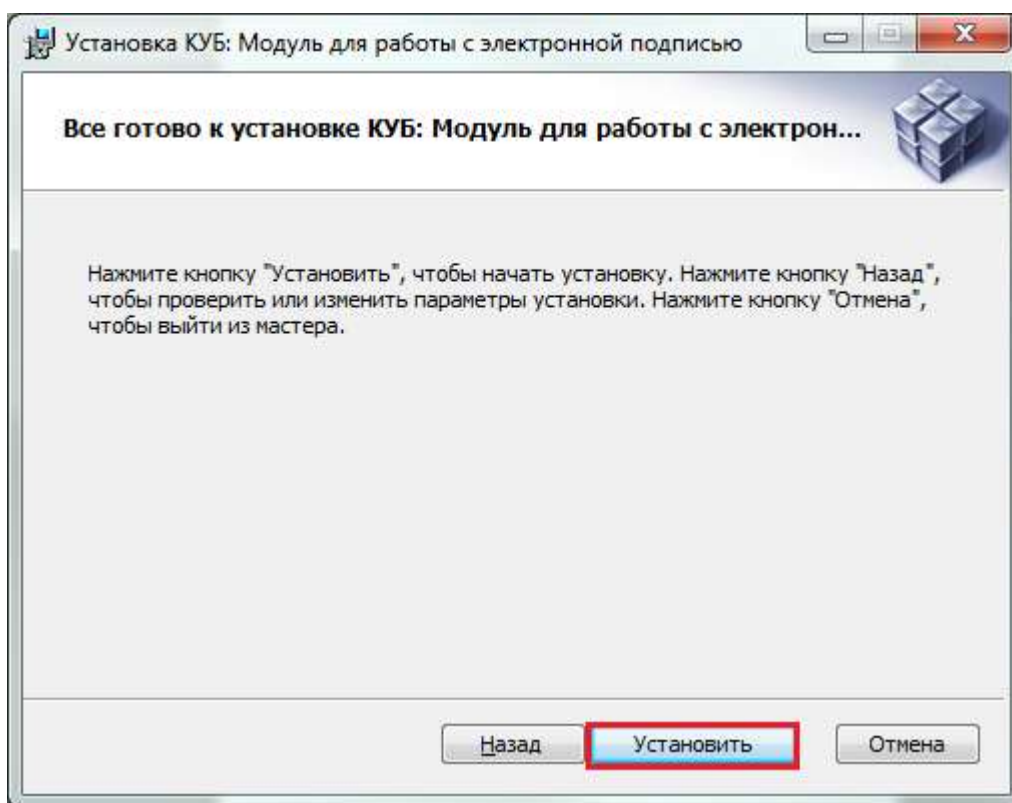


Рисунок 61. Подтверждение установки

8. Дождитесь окончания процесса установки.

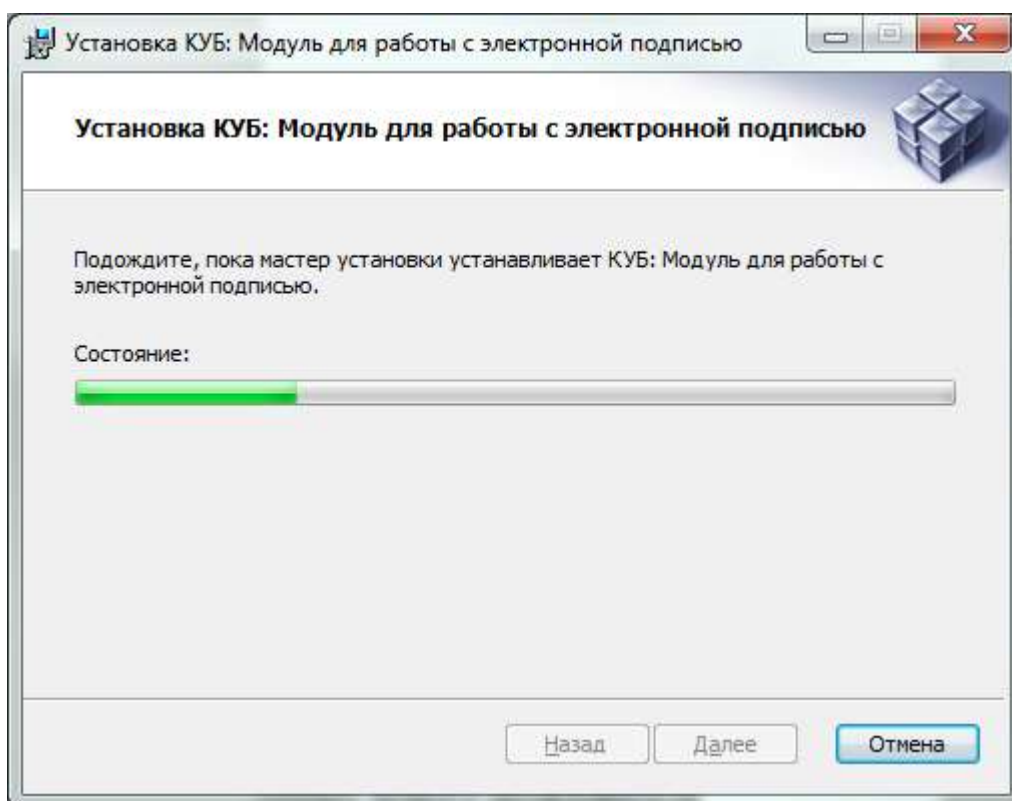


Рисунок 62. Установка компонента средства подписи

9. Завершите установку компонента средства подписи, нажав «Готово»

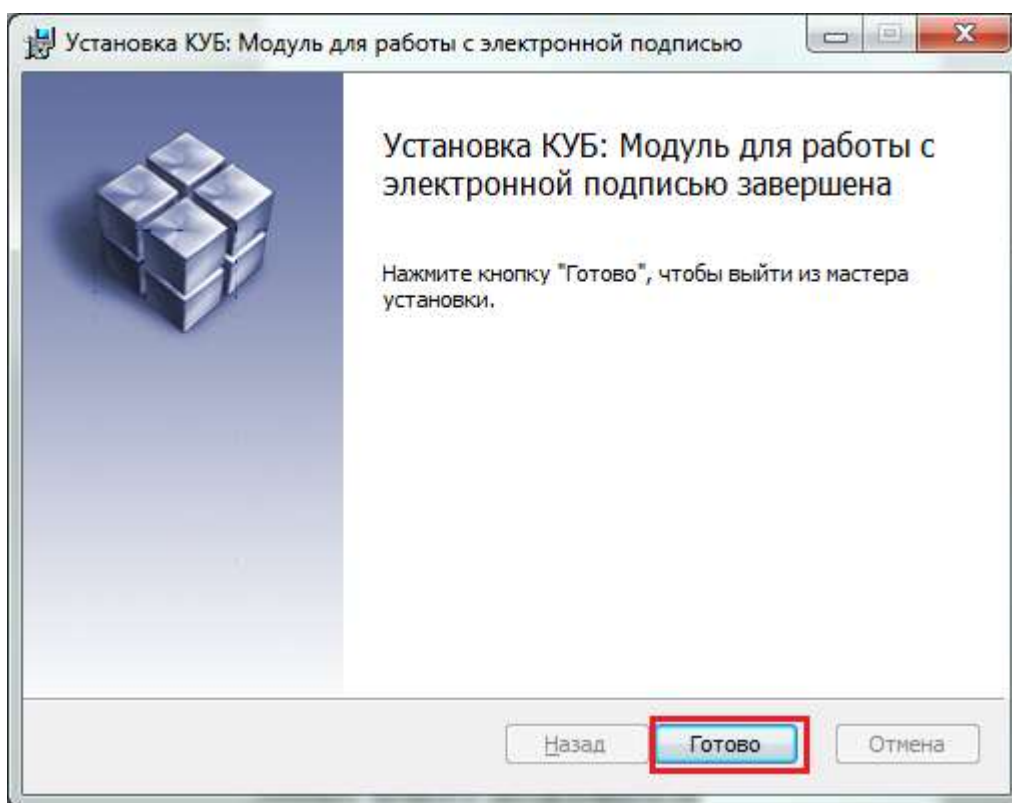


Рисунок 63. Завершение установки

10.Перезагрузите АРМ пользователя.

3.11.2 Установка в процессе инициации процедуры создания заявки в системе согласования и управления доступа

1. Выполнить вход в личный кабинет пользователя.
2. На главной странице личного кабинета активировать ссылку «Вход в Систему согласования и управления доступом».

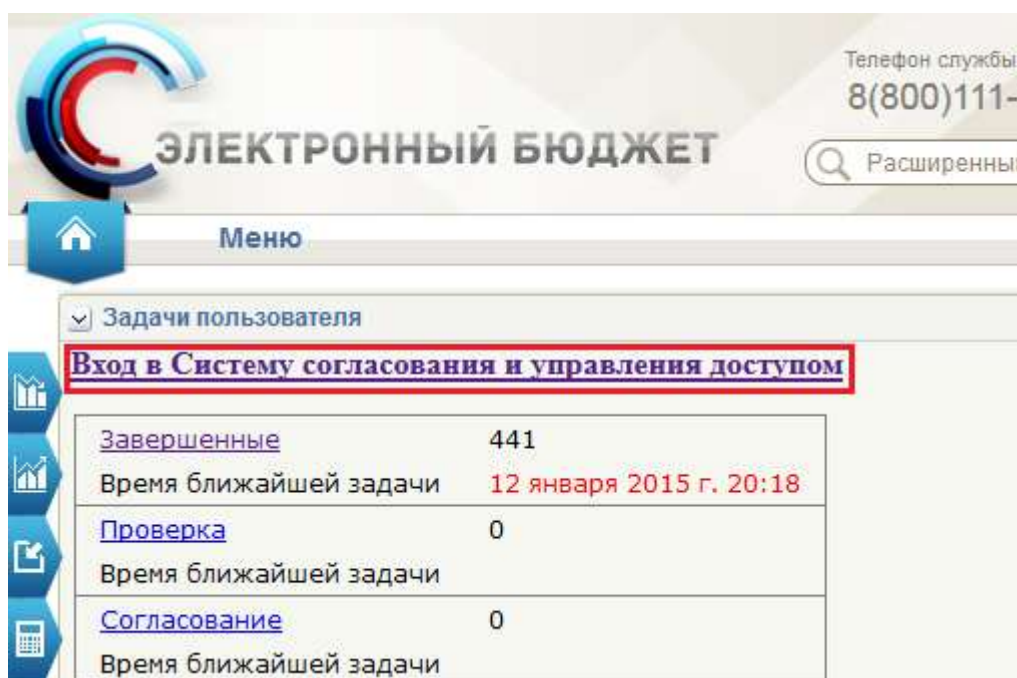


Рисунок 64. Личный кабинет пользователя

3. На главной странице системы согласования и управления доступом в разделе «Создать заявку» активировать любой доступный тип заявки, например, в группе «Кадровые процедуры» активировать ссылку «Прием на работу сотрудника».

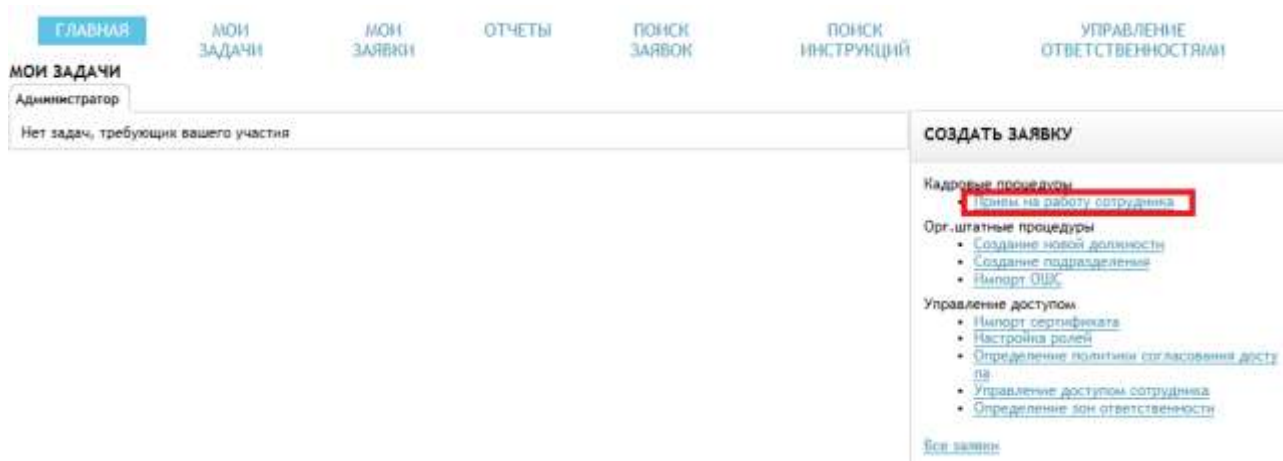


Рисунок 65. Переход к регистрации данных нового пользователя

4. На главной странице системы согласования и управления доступом в разделе «Создать заявку» активировать любую доступный тип заявки, например, в группе «Кадровые процедуры» активировать ссылку «Прием на работу сотрудника».

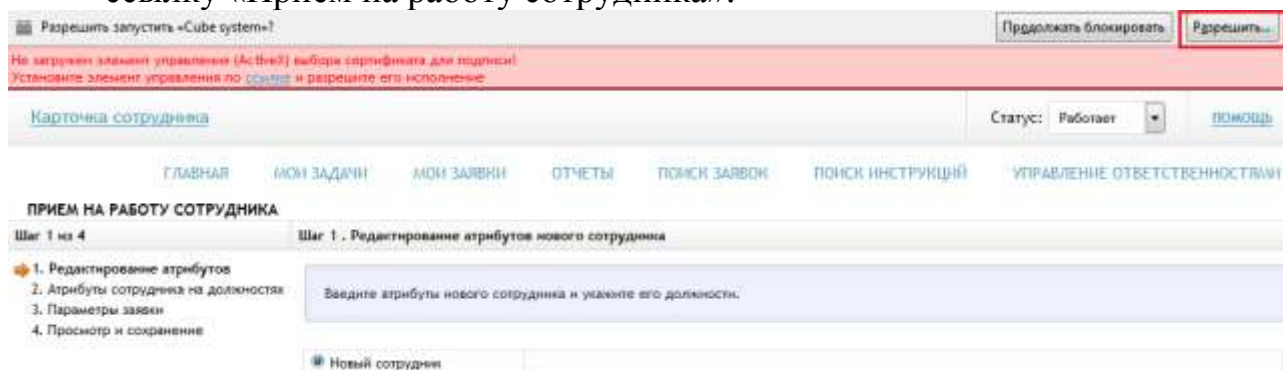


Рисунок 66. Разрешение активного содержимого личного кабинете

5. В случае появления диалога о блокировке активного содержимого личного кабинета, в правом верхнем углу нажать кнопку «Разрешить...».
6. Во всплывающем диалоге нажать кнопку «Разрешить и запомнить».

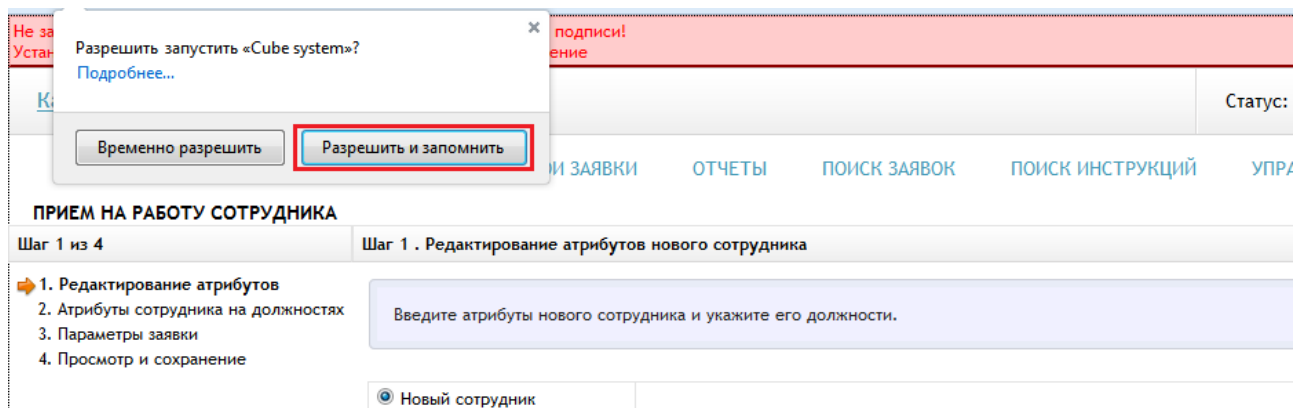


Рисунок 67. Разрешение активного содержимого личного кабинета

7. В верхней части окна в предупреждающем сообщении о незагруженном элементе управления активировать предлагаемую ссылку.

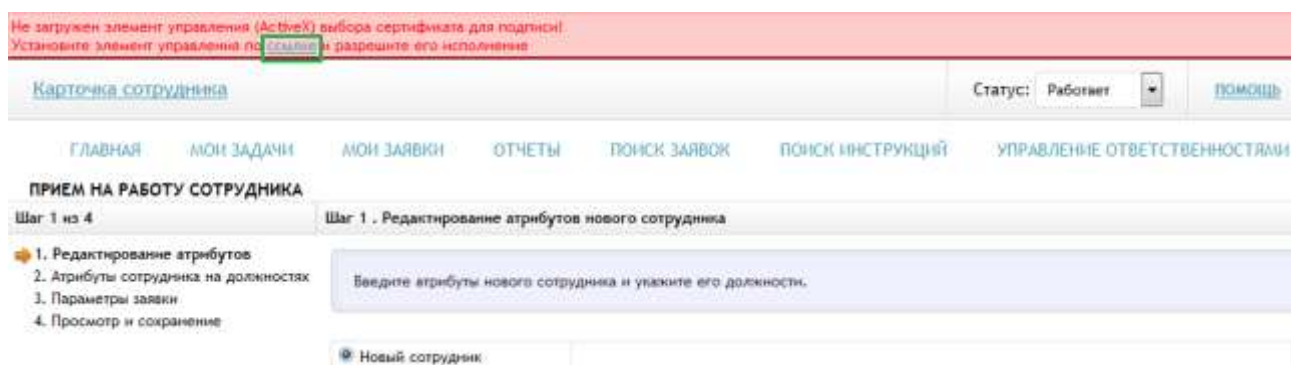


Рисунок 68. Копирование модуля «cubesign» в локальную директорию АРМ пользователя

8. В диалоге сохранения файла нажать кнопку «Сохранить файл».

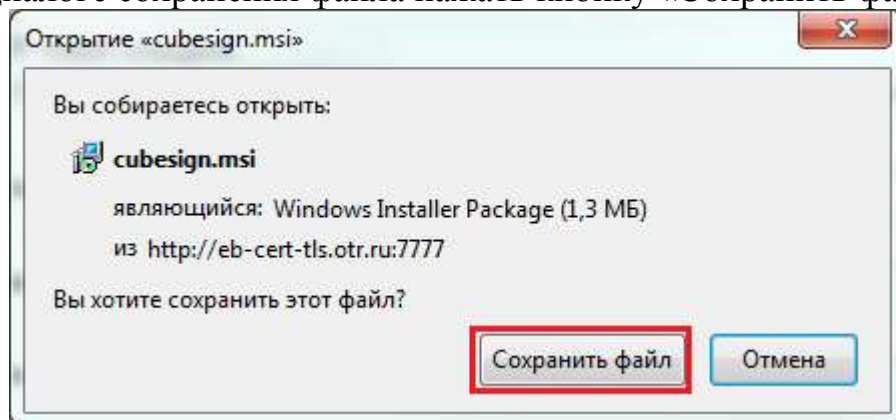
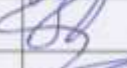


Рисунок 69. Копирование модуля «cubesign» в локальную директорию АРМ пользователя

9. Выполнить запуск сохраненного файла «cubesign.msi».
10. Повторить шаги 3 - 9 раздела 3.11.1 настоящего Руководства.

11. Выполнить перезапуск веб-обозревателя либо перезагрузку АРМ пользователя, если она не выполнялась после установки ПО «Jinn-Client» и «Континент TLS Клиент».

ЛИСТ СОГЛАСОВАНИЯ

Наименование организации, предприятия	Фамилия, имя, отчество	Должность	Подпись	Дата
УШССТФ	Баркова И.Ч.	Нач. отдела		
УРС. Вн	Табришова М.Б.	ЗНО		
УРС. БИ	Федосимов Б.И.	Заместитель ООМБСД		
УРС. БЧ	Мамедов А.И.	Заместитель отряда		
УРС. БЧ	Медведев А.Б.	ЗНУ		
УРС	Федорова Л.В.	Зам. нач. ОЗПТО		
	Талиев И.	Нач. от.		
	Мамедов И. И.	Нач. от.		
	Заваров В.И.	Зам. нач. Упр.		
	Певнев С.Г.	Нач. Упр. - 5		

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер версии документа	Дата изменения (дд.мм.гггг)	Автор изменения (ФИО)	Комментарии к изменениям
1.0	16.01.2015	Пляцидевский А.Н	Первоначальная версия документа