

Информационная система
«Конвейер сборки, доставки и
развертывания ПО (CI/CD)».
Руководство по получению доступа к
развернутой инфраструктуре

Всего 12 листов

Оглавление

1	ОБЩИЕ СВЕДЕНИЯ	3
1.1	О ДОКУМЕНТЕ	3
1.2	О ПРОДУКТЕ	3
2	УСЛОВИЯ ПОДКЛЮЧЕНИЯ.....	3
2.1	ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ	4
3	НАСТРОЙКА ПОДКЛЮЧЕНИЯ	4
3.1	ПОЛУЧЕНИЕ ДОМЕННЫХ УЧЕТНЫХ ЗАПИСЕЙ	4
3.2	VPN-СОЕДИНЕНИЕ	5
3.3	ИСПОЛЬЗОВАНИЕ ТОНКОГО КЛИЕНТА.....	5
3.4	ИСПОЛЬЗОВАНИЕ ТОЛСТОГО КЛИЕНТА.....	6
3.5	УСТАНОВКА ДОПОЛНИТЕЛЬНЫХ SSL СЕРТИФИКАТОВ	8
3.6	ПРАВА ДОСТУПА.....	12

1 Общие сведения

1.1 О документе

Настоящий документ представляет собой руководство по получению доступа к развернутому экземпляру продукта. Документ предназначен для специалистов Экспертного совета при Минкомсвязи России, осуществляющим оценку соответствия продукта Правилам формирования и ведения Единого реестра российского ПО.

1.2 О продукте

Информационная система «Конвейер сборки, доставки и развертывания ПО (CI/CD)» (далее, Конвейер (CI/CD)) предназначена для построения автоматизированного процесса разработки, тестирования и развертывания микросервисных приложений.

Для обеспечения процессов непрерывной интеграции и доставки в ИС «Конвейер (CI/CD)» реализован набор пайплайнов. Каждый пайплайн описывает этапы производственного процесса, которые подвергаются автоматизации:

- Разработка
- Тестирование
- Развертывание на требуемых средах
- Взаимодействие с другими информационными системами.

2 Условия подключения

Для проверки продукта на соответствие Правилам формирования и ведения Единого реестра российского ПО, предоставляется удаленный доступ к развернутому экземпляру продукта внутри инфраструктуры изготовителя.

Подключение к информационной системе осуществляется с соблюдением требований информационной безопасности:

- Использование защищенного канала связи посредством VPN-соединения
- Разграничение доступа к компонентам и ресурсам системы на основе ролевой модели
- Двухфакторная аутентификация с привязкой к мобильному номеру телефона пользователя

- Доменная авторизация

Внимание! Данные механизмы работают в штатном режиме и не могут быть отключены на уровне отдельного пользователя. **Изготовитель заинтересован в том, чтобы продукт прошел проверку соответствия, и готов оказать помощь в подключении и проверке системы.**

Ниже приводятся контакты технических специалистов изготовителя, которые могут проконсультировать по вопросам подключения и функциональности продукта в согласованное со специалистами время.

Контактный телефон: +7 (495) 363-05-53 (вн. 7954345)

В случае необходимости изготовитель готов провести демонстрационный показ функциональных возможностей системы.

2.1 Требования к программному обеспечению

Для подключения к развернутому экземпляру проверяемого ПО на компьютере специалиста должно быть установлено и настроено следующее программное обеспечение:

- Браузер (Google Chrome или аналоги)
- Check Point Endpoint Security (VPN-клиент) – рекомендуемая версия E85.20
- Операционная система — Windows 7/8/10, имеются административные права на установку ПО

Важно! Для прохождения двухфакторной аутентификации от специалистов, которые будут проверять продукт, потребуются номера мобильных телефонов. На указанные номера будут приходить SMS-сообщения с проверочными кодами.

3 Настройка подключения

3.1 Получение доменных учетных записей

Для авторизации в компонентах системы используется доменная авторизация. Учетная запись пользователя привязывается к номеру мобильного телефона, на который будут приходить SMS-сообщения с кодами подтверждения.

Для генерации учетной записи:

- Сформируйте заявку на предоставление доступа по следующей форме

Таблица 1 Форма заявки на получение прав доступа к ИС (отправляется по e-mail)

Адресаты	(предоставляется по запросу)
Тема письма	Экспертный совет. Реестр отеч. ПО. Заявка на доступ
Сообщение	<p>Добрый день!</p> <p>В рамках проверки соответствия ИС «Конвейер (CI/CD)» на соответствие Правилам формирования и ведения Единого реестра российского ПО прошу предоставить доступ к проверяемой системе специалисту(ам) (<i>перечислить списком</i>):</p> <ul style="list-style-type: none"> • Ф.И.О.: • Номер мобильного телефона, используемый для авторизации: • Должность: <p>_____</p> <p>(корпоративная подпись)</p>

- Отправьте заявку по e-mail на указанные в письме адреса
- После обработки заявки на e-mail отправителя придут авторизационные данные — логин/пароль, ссылки на ресурсы и другая важная информация.

3.2 VPN-соединение

Для организации защищенного соединения используется Check Point Endpoint Security. С помощью данного VPN-клиента организуется доступ к проверяемой системе. Check Point Endpoint Security может использоваться как тонкий, так и толстый клиент:

- При работе в браузере — режим тонкого клиента
- При установке дистрибутива на ПК — режим толстого клиента

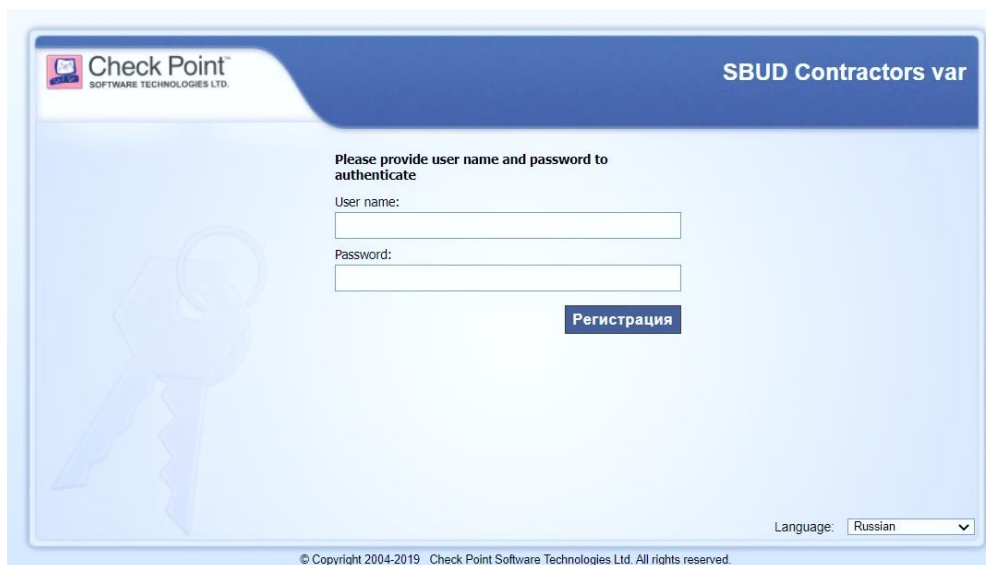
Важно! Для работы с ИС «Конвейер (CI/CD)» рекомендуется использовать Check Point Endpoint Security в режиме толстого клиента.

3.3 Использование тонкого клиента

Для авторизации и использования Check Point Endpoint Security в качестве тонкого клиента:

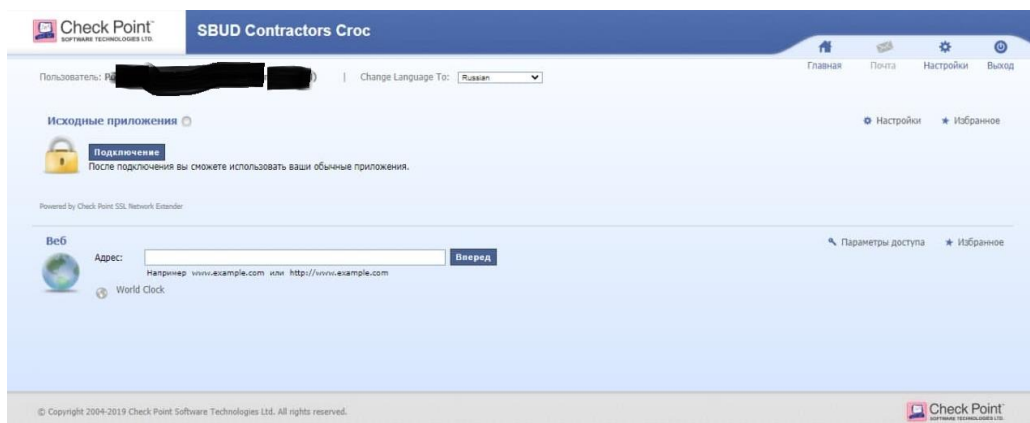
- Откройте браузер, в адресной строке введите адрес сервиса авторизации (*предоставляется в ответном письме — см. п.3.1*)
- В открывшемся окне укажите логин/пароль из письма, далее нажмите **Регистрация**

Рисунок 1



- На указанный в заявке номер мобильного телефона придет SMS-сообщение с кодом авторизации. Введите код в открывшееся окно и нажмите **Enter**.
- После успешной авторизации откроется окно для подключения к инфраструктурным сервисам системы

Рисунок 2



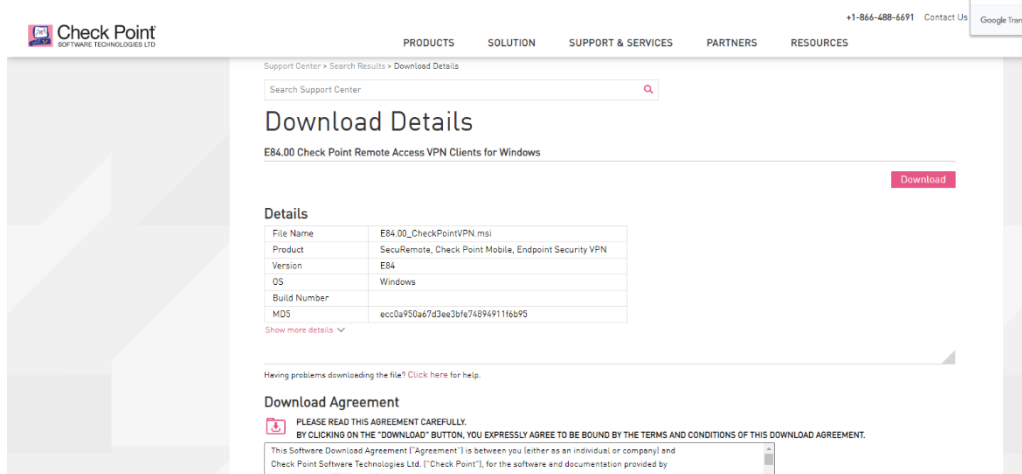
- Для активации VPN-соединения нажмите **Подключение**

3.4 Использование толстого клиента

Установка клиента Check Point Endpoint Security на ПК является рекомендуемым способом соединения. Чтобы настроить соединение:

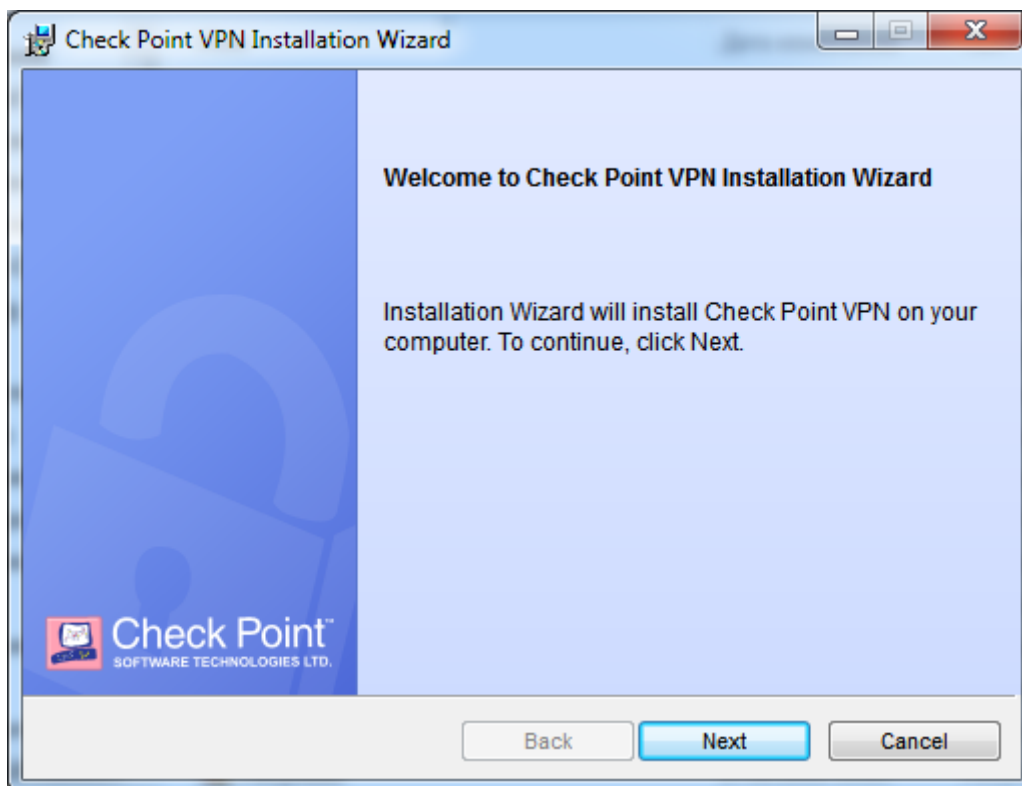
- Скачайте дистрибутив [Check Point Endpoint Security](#)

Рисунок 3



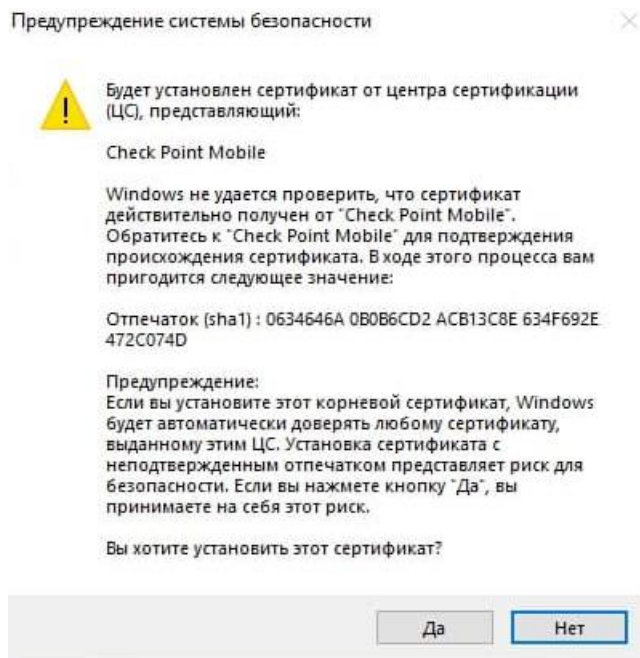
- Запустите установку. Пользователь, от имени которого запускается установка, должен иметь права администратора ОС или иметь права на установку ПО

Рисунок 4



- В окне выбора продукта поставьте чекбокс напротив *Endpoint Security VPN*, далее нажмите **Next** и следуйте штатному алгоритму установки.
- В процессе установки система предложит установить SSL-сертификат. Для его установки нажмите **Да**

Рисунок 5



- В случае успешной установки в системном древе (правый нижний угол панели задач) появится значок клиента
- Для настройки VPN-соединения нажмите на значок клиента правой кнопкой мыши > **Connect**
- Система предложит настроить новое соединение, нажмите **Yes**
- В поле *Server address or Name* введите адрес сервиса авторизации (*предоставляется в ответном письме — см. п. 3.1*), нажмите **Next**
- В случае успешной настройки откроется окно подключения.
- Для активации VPN-соединения укажите логин/пароль, полученные на этапе регистрации учетной записи, далее нажмите **Connect**.
- В случае успешного соединения программа выведет сообщение в древе «*Connected*».

3.5 Установка дополнительных SSL сертификатов

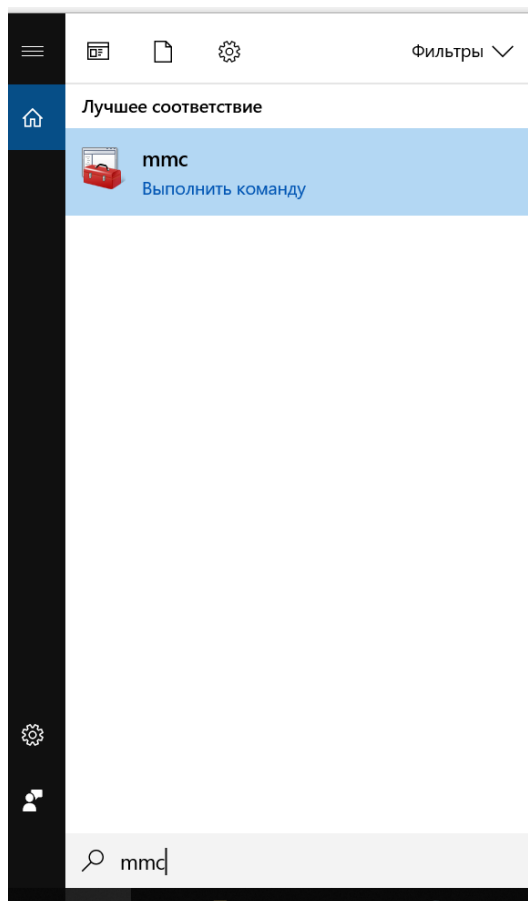
Ко всем ресурсам доступ осуществляется по протоколу HTTPS (TLS), поэтому для доступа требуется использовать цепочку SSL-сертификатов:

- Корневой сертификат — *предоставляется в ответном письме — см. п. 3.1.*
- Промежуточный сертификат — *предоставляется в ответном письме — см. п. 3.1.*

Для того, чтобы установить SSL-сертификаты:

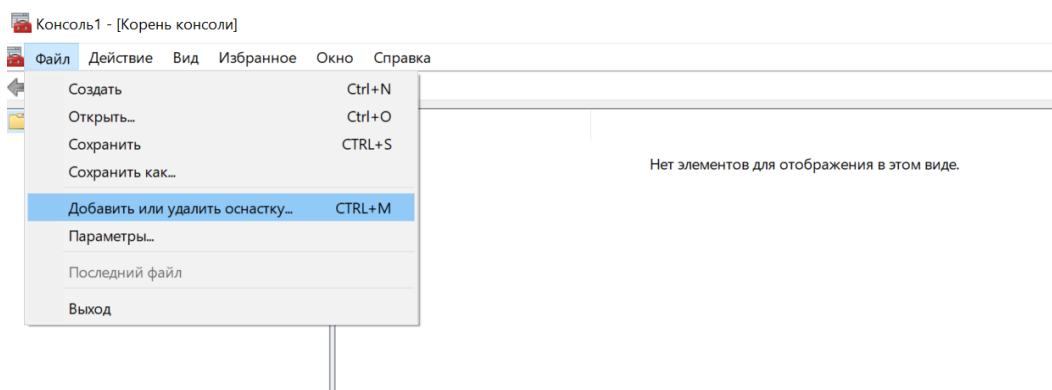
- Нажмите **Win**, в открывшемся меню введите **mmc**, далее выберите *Выполнить команду*

Рисунок 6



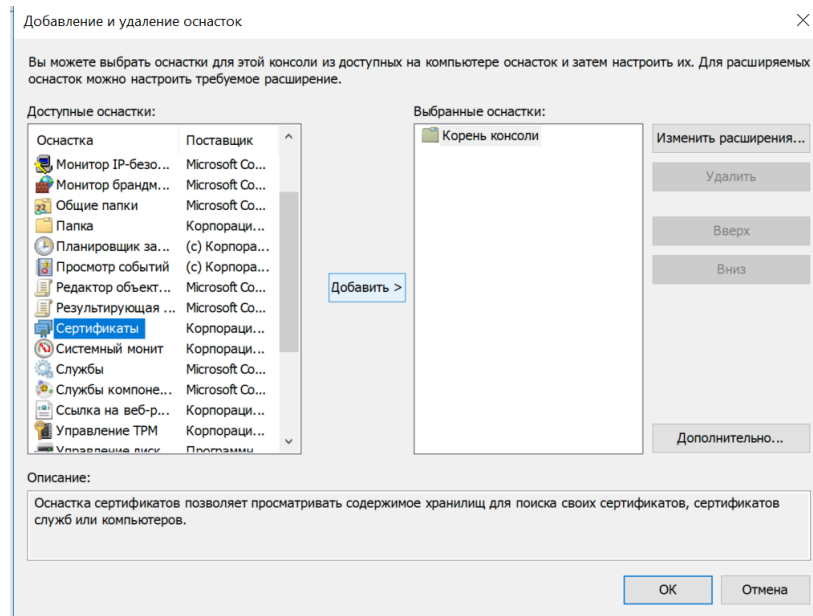
- В открывшейся программе выберите *Файл > Добавить или удалить оснастку*

Рисунок 7



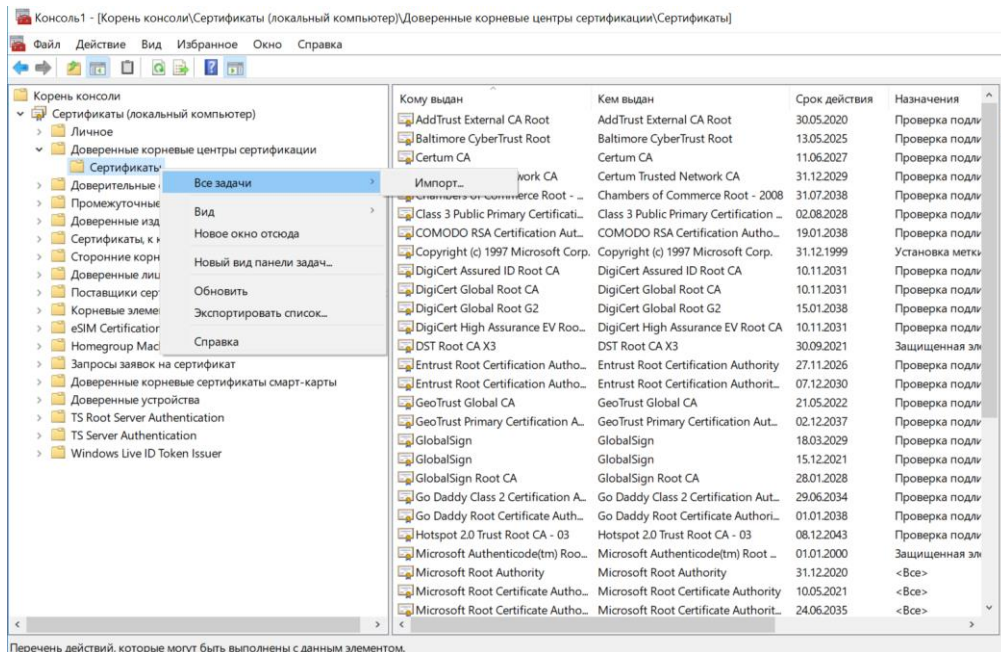
- В открывшемся окне *Доступные оснастки* найдите *Сертификаты*, далее нажмите **Добавить > ОК**

Рисунок 8



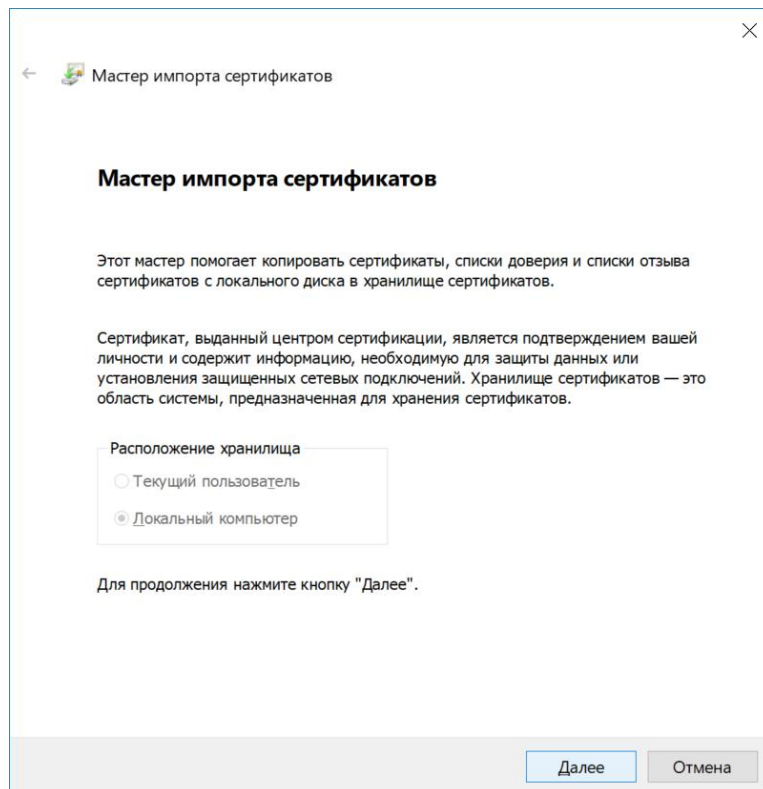
- В корне консоли раскройте список *Доверенные корневые центры сертификации*, кликните правой кнопкой мыши на *Сертификаты*

Рисунок 9



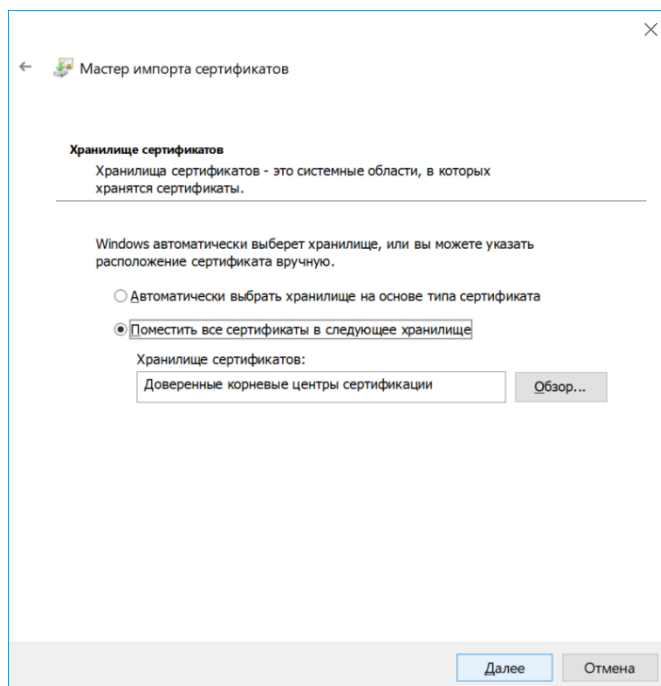
- В открывшемся окне выберите *Все задачи > Импорт*
- Откроется мастер импорта сертификатов

Рисунок 10



- В поле *Имя файла* укажите путь к сертификату, нажав **Обзор**, затем нажмите **Далее**
- В окне *Хранилище сертификатов* поставьте чекбокс напротив *Поместить все сертификаты в следующее хранилище*

Рисунок 11



- Укажите путь к хранилищу, нажав **Обзор**
- Для завершения настройки следуйте инструкциям.

Аналогичные действия нужно совершить со всеми устанавливаемыми сертификатами.

3.6 Права доступа

Учетной записи пользователя предоставляются пользовательские права на работу с системой «Конвейер (CI/CD)». Для проверки на соответствие Правилам формирования и ведения Единого реестра российского ПО пользовательским учетным записям предоставлен доступ к тестовым репозиториям, позволяющим проверить основные функциональные возможности продукта.

Важно! Учетная запись имеет полные функциональные права на работу с продуктом, кроме административных. Это означает, что из-под предоставленной учетной записи не могут быть совершены действия, которые могут повредить или повлиять на работоспособность системы или ее отдельно взятых компонент.

В случае необходимости ознакомиться с системой с точки зрения администратора — обратитесь с запросом на проведение демонстрационного показа специалистом изготовителя.

Учетные записи, зарегистрированные для проверки соответствия, имеют доступ к следующим web-интерфейсам системы:

- Gitlab (*ссылка предоставляется в ответном письме — см. п. 3.1*):
 - Тестовые репозитории (права **developer**), для которых настроены Gitlab CI и Gitlab Runner
- Nexus (*ссылка предоставляется в ответном письме — см. п. 3.1*):
 - Артефакты тестовых репозиториях
- Портал App.Farm с документацией (*ссылка предоставляется в ответном письме — см. п. 3.1*)
- Сервис статического анализа кода на уязвимости (*ссылка предоставляется в ответном письме — см. п. 3.1*):
 - Отчеты по тестовым проектам
- Сервисы проверки безопасности DevSecOps (AppSec.Hub):
 - Отчеты по тестовым репозиториям.