

## Инструкция по созданию ключа ЭП с использованием программы Admin-PKI.

### Системные требования:

Windows 7 и выше.

**ВАЖНО!** Для MacOS необходимо использовать продукты виртуализации, такие как Parallels Desktop или PlayOnMac.

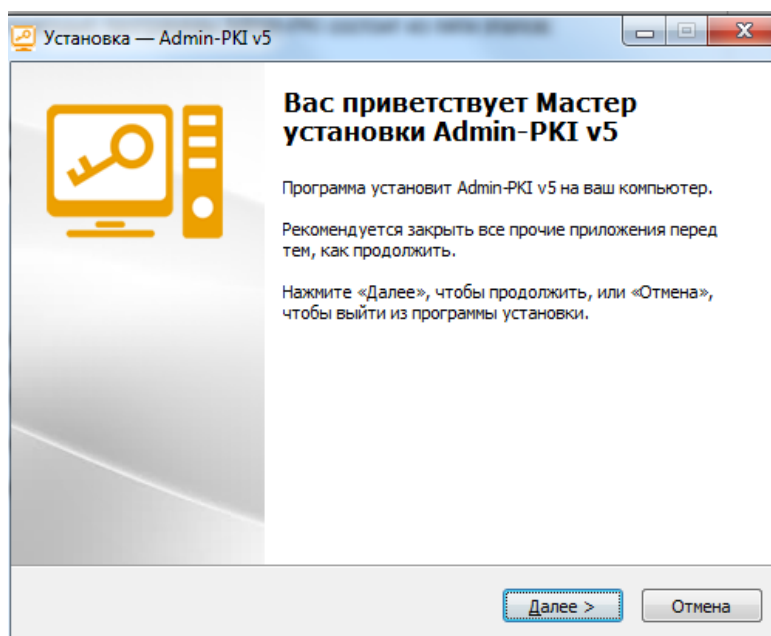
Процедура создания ключа ЭП с помощью программы Admin-PKI состоит из четырёх этапов:

1. Установка программы.
2. Генерация ключа ЭП
3. Передача запроса на сертификат ключа проверки ЭП в Удостоверяющий центр
4. Получение файла сертификата ключа проверки ЭП.

### 1 Установка программы

Для генерации ключа ЭП на Вашем компьютере должна быть установлена программа Admin-PKI. Дистрибутив программы можно скачать по ссылке <https://brokerkf.ru/skzi/> после регистрации.

**!**Извлеките из архива и сохраните оба файла (default\_keygen\_template.tpl и admin-pki-v5.exe) на Ваш ПК.



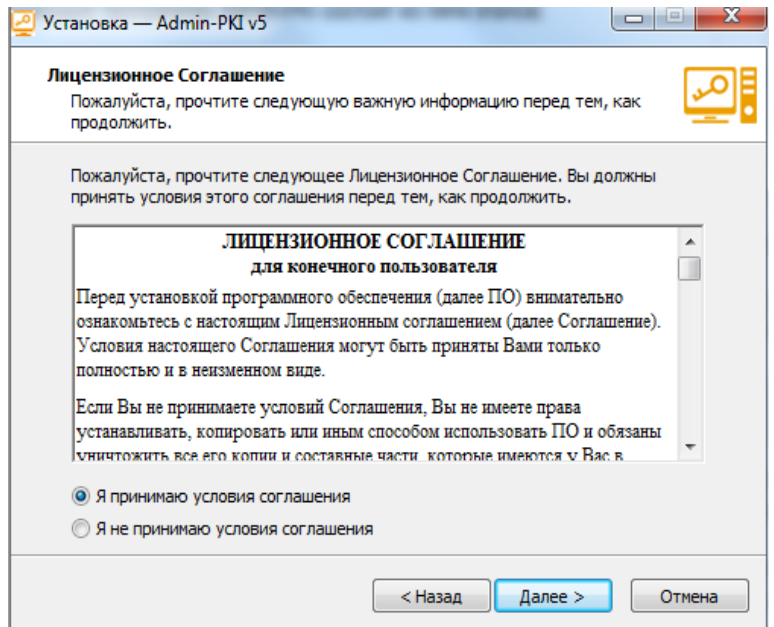
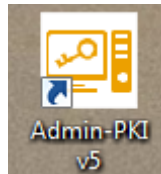
Запустите файл admin-pki-v5.exe.

Нажмите **«Далее»**, чтобы продолжить установку ПО

Выберите пункт «**Я принимаю условия соглашения**», и нажмите «**Далее**»

Во всех следующих окнах нажимайте также «**Далее**»

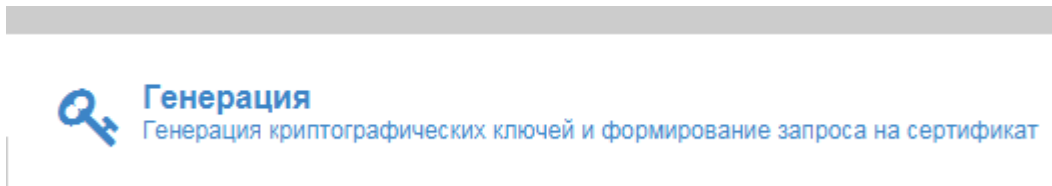
На Вашем компьютере появится новый ярлык:



## 2 Генерация ключа ЭП

Запустите программу двойным щелчком левой кнопкой мыши.

Выберите пункт «Генерация»:



Укажите диск (каталог ключевого носителя), где будет храниться Ваш секретный ключ (например, создайте новую папку на флэшке: L:\ключ2022). **Запомните указанный путь.**

### Параметры ключевого контейнера

В этом разделе Вам необходимо указать параметры ключевого контейнера для генерации криптографических ключей.

Опцию [Задать файл ключа ЭП (закрытого ключа)...] используйте для формирования запроса на сертификацию уже существующего ключа ЭП (закрытого ключа) или для генерации нового ключа ЭП (закрытого ключа) с именем или каталогом хранения, отличными от заданных по умолчанию.

#### Каталог ключевого контейнера

Задать файл ключа ЭП (закрытого ключа).

В следующем окне выберите пункт «Защитить на пароле».

## Защита на пароле

В этом разделе Вы можете установить пароль для доступа к ключевому контейнеру.

**Защитить на пароле**

Требования к паролям

Далее заполните необходимые поля Вашими данными:

## Сведения о владельце сертификата

В этом разделе для генерации криптографических ключей и формирования запроса на сертификат необходимо заполнить поля формы.

### Заполнить поля формы по сертификату

Заполнить по сертификату...

Очистить

**Ф.И.О. (CommonName):**

ФИО полностью

Организация (OrganizationName):

для ЮЛ

**Подразделение (OrganizationUnitName):**

номер договора

Должность (Title):

для ЮЛ

**Адрес электронной почты (E-Mail):**

your@e-mail.ru

**Страна (CountryName):**

RU

**Город (LocalityName):**

город

В поле «**Файл запроса**» укажите, где программой будет сохранен файл с запросом на сертификат созданного ключа ЭП. В качестве имени файла укажите **номер своего договора**, расширение – обязательно **“.pem”**.

## Файл запроса

В этом разделе Вам необходимо указать путь к файлу для сохранения запроса на сертификацию ключа проверки ЭП (открытого ключа). Вы можете выбрать опцию просмотра и печати сформированного запроса.

### Файл запроса

L:\ключ2022\Недоговора.pem

Обзор

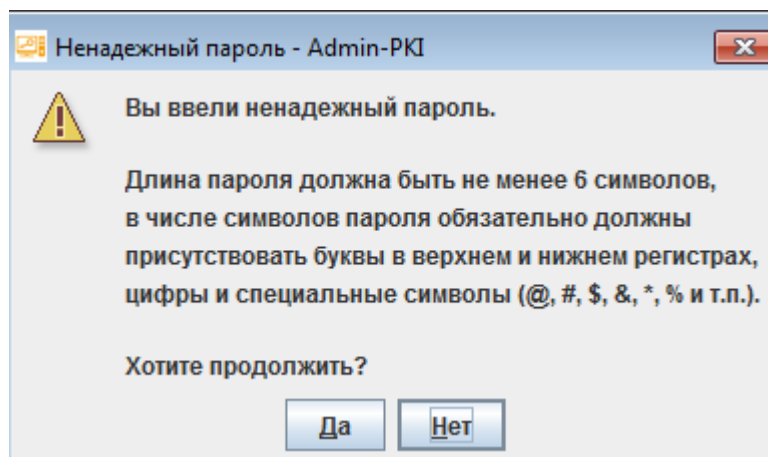
Администратору УЦ по электронной почте

НАЖМИТЕ «Далее»

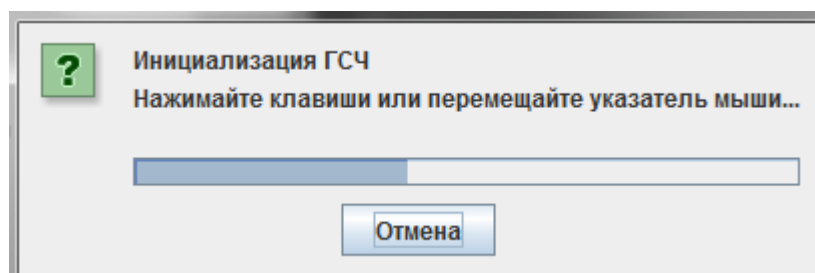
При необходимости установите пароль (не менее 6 символов) на создаваемый ключевой контейнер.

**Не забывайте пароль - впоследствии он будет использоваться при подключении к QUIK и подписи поручений в Личном кабинете.**

При появлении такого окна нажмите ДА

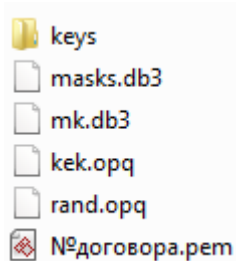


Появится окно «Инициализация генератора случайных чисел». Перемещайте мышью или нажимайте любые клавиши клавиатуры до тех пор, пока шкала не заполнится синими кубиками полностью. Окно «Инициализация ГСЧ» закроется автоматически.



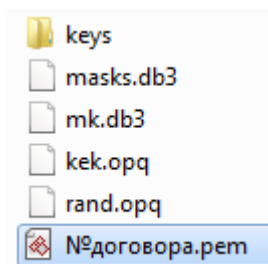
Последним будет сообщение о том, что ключи успешно сформированы.

**Убедитесь, что на указанном Вами носителе появились все файлы ключевого контейнера:**



### 3 Передача запроса на сертификат ключа проверки ЭП в Удостоверяющий центр

Запрос на сертификат ключа проверки ЭП необходимо передать в Удостоверяющий центр по электронной почте по адресу [uc@brokerkf.ru](mailto:uc@brokerkf.ru).



**Будьте внимательны:** отправлять нужно только один файл – с расширением **.pem**. Это файл запроса на сертификат ключа проверки ЭП (он не секретный).

После отправки в Удостоверяющий центр файла запроса (.pem), в течение трёх рабочих дней Вы получите обратным письмом документ:

- Сертификат ключа проверки ЭП

При получении первого сертификата необходимо распечатать документ на одном (отдельном) листе бумаги, подписать и передать в Компанию одним из следующих способов:

- непосредственно в офис Компании
- через офис Агента Компании (<https://brokerkf.ru/about/contacts/offices/>)
- направить подписанный документ почтовым отправлением в адрес Компании (191119, Россия, город Санкт-Петербург, улица Марата, дом 69-71).

При смене сертификата документы в Компанию можно передать без визита в офис:

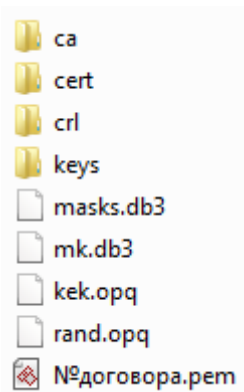
- через Личный кабинет (модуль WebBank, используйте пункт «Документы – Отправить новый», выбрав тип документа «Сертификат электронной подписи»).

### 4 Получение файла сертификата ключа проверки ЭП

После отправки в Удостоверяющий центр файла запроса (.pem), в течение трёх рабочих дней Вы также получите обратным письмом файл Вашего сертификата, а также корневой сертификат Удостоверяющего центра и список отозванных сертификатов.

Их необходимо скопировать на Ваш ключевой носитель (флэш-карту, где сохранены ранее созданные файлы).

В результате у Вас должен быть каталог с ключами следующего вида:



После получения от Вас подписанных документов, Компания регистрирует сертификат ключа проверки ЭП.

Срок действия ключа ЭП – 1 год. По истечении этого срока ключ будет автоматически отозван Системой. При истечении срока действия ключа Вам потребуется создать новый ключ ЭП.

Предварительно Вы получите уведомление о скором истечении срока действия сертификата и необходимости получения нового.

***Создание резервной копии – необходимый этап в процессе генерации ключа.***

При порче основного ключевого носителя, Вы всегда сможете продолжить работу, используя запасную копию.

В Компании копии Вашего ключа ЭП нет.

Для создания резервной копии, помимо ключевого носителя с текущим ключом ЭП, Вам потребуется еще один носитель информации.

Содержимое папки ключевого контейнера скопируйте на второй (резервный) ключевой носитель.

Хранить ключевой носитель с резервной копией необходимо в условиях, исключающих доступ к нему третьих лиц (например, использовать для хранения личный сейф).

**Соблюдайте правила безопасности при работе с ключевым носителем:**

- Не передавайте носитель с ключами ЭП третьим лицам
- Не оставляйте носитель с ключами ЭП в открытом доступе (например, на столе) при отсутствии на рабочем месте
- Извлекайте носитель с ключами ЭП из компьютера каждый раз после завершения его использования
- Не оставляйте носитель с ключами ЭП установленным в компьютер при неактивности