

**ООО «КИБЕРПЛАТ»**

Россия, 123610, г. Москва, ЦМТ-2,  
Краснопресненская наб., д.12, подъезд №7  
Телефон: 8 (495) 967-02-20 Факс: 8 (495) 967-02-08  
<http://www.cyberplat.ru> Email: [info@cyberplat.ru](mailto:info@cyberplat.ru)

---



**CyberPlat**

Russia, 123610, Moscow, WTC-2,  
Krasnopresnenskaya nab., 12, Entrance #7  
Phone: +7 (495) 967-02-20 Fax: +7 (495) 967-02-08  
<http://www.cyberplat.com> Email: [info@cyberplat.com](mailto:info@cyberplat.com)

---

# Создание ключа подписанта системы CyberFT с помощью программы GenKey

Руководство пользователя

## Аннотация

В настоящем документе описан процесс создания комплекта ключей подписанта, необходимых для документооборота в рамках системы CyberFT. Разработка ООО «КИБЕРПЛАТ».

## Содержание

1	Скачивание программы GenKey .....	3
2	Создание ключей .....	3
2.1	Создание ключей на токене.....	3
2.2	Заполнение параметров сертификата.....	6
2.3	Пример настроек при создании ключей на токене .....	10
2.4	Создание ключей в файле.....	12
3	Установка программы для подписания отправляемых документов.....	15
4	Документация .....	15

## 1 Скачивание программы GenKey

Для работы в системе электронного документооборота сети CyberFT необходимо создать ключи электронной подписи для подписантов документов.

Для создания ключей скачайте с сайта программу генерации ключей GenKey.

Дистрибутив программы можно скачать по данному адресу

<http://download.cyberft.ru/GenKey/GenKey.zip>.

Распакуйте архив в папку C:\...\ GenKey .

Ключи для работы в системе CyberFT могут создаваться на токене, а также в файле на жестком диске компьютера или флеш-носителе. **Хранение ключей на токене более надежно.**

Настоящая инструкция содержит порядок работы при создании ключей с помощью программы GenKey, а также при формировании акта о признании электронной подписи. Подробности работы с программой GenKey вы можете прочитать в [Руководстве пользователя](#) «Генерация ключей с помощью программы GenKey».

**Внимание!** Ключи необходимо выпускать для лиц, обладающих полномочиями подписантов.

## 2 Создание ключей

### 2.1 Создание ключей на токене

В настоящем разделе описано создание ключей криптосистемы RSA **на токене** с помощью программы генерации ключей GenKey. Правила работы с программой описаны в [руководстве пользователя](#) «Генерация ключей с помощью программы GenKey»

Особенности создания ключей **в файле** описаны в разделе «[Создание ключей в файле](#)». Файлы могут размещаться на жестком диске компьютера или на USB флеш-носителе.

Ключи необходимо выпускать для лиц, обладающих **полномочиями подписантов**.

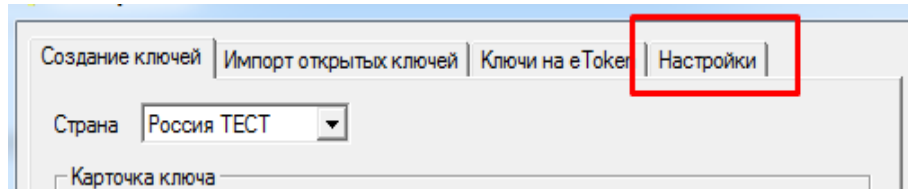
#### **Внимание!**

- Хранение ключей на токене более надежно, чем хранение ключей в файле.
- Разрешенные типы токенов описаны в [руководстве пользователя программы GenKey](#) .
- Перед тем, как создавать ключи на токене, внимательно прочитайте прилагаемую к токену **документацию и установите драйверы**, поставляемые в комплекте с токеном.
- Процедуры **начальной инициализации и установки пароля токена** производятся клиентом самостоятельно при помощи поставляемых с устройством программ.

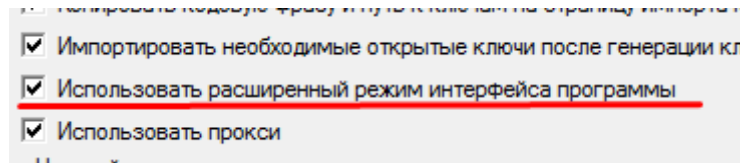
## Порядок действий

1. При создании ключей на токене до запуска программы **GenKey** **подключите токен** к компьютеру через USB-порт.
2. Запустите программу создания ключей **Genkey.exe**.
3. Перейдите на вкладку **Настройки**.

**Обратите внимание**, что вкладка **Ключи на eToken** будет отображаться на экране, если на вашем компьютере установлен драйвер токена.



4. Установите отметку **Использовать расширенный режим интерфейса программы**.

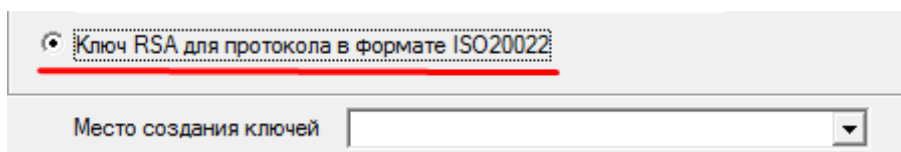


Также рекомендуется установить отметку **Запоминать и восстанавливать путь к последней папке с ключами**. Это может помочь при поиске ключа на компьютере, если путь к папке с ключами был утерян.

5. Вернитесь на вкладку **Создание ключей**.

The screenshot shows the 'GenKey 4.12.8' application window. The main menu includes 'Создание ключей', 'Импорт открытых ключей', 'Ключи на eToken', and 'Настройки'. The 'Страна' dropdown is set to 'Россия ТЕСТ'. Under the 'Карточка ключа' section, the 'Получить карточку ключа с сервера КиберПлат' option is selected, with empty 'Логин' and 'Пароль' fields. The 'Загрузить из файла' option is also present with a file path 'C:\Users\maksimov\Desktop' and a folder icon. The 'Ключ RSA для протокола в формате ISO20022' option is selected. Below this, 'Место создания ключей' is set to 'eToken [Maksimov Pjotr]'. The 'Сохранить сертификат' field contains 'C:\Users\maksimov\Desktop\Место сохранения' with a folder icon. The 'Параметры сертификата' button is labeled 'Настроить'. The 'Длина создаваемого ключа' dropdown is set to '2048'. The 'Кодовая фраза токена' field is empty. At the bottom, the 'Имя ключа в тонком клиенте' checkbox is checked, and the field contains 'Ключ [January 14, 2019 12:45:31]'. The bottom bar features the 'CyberPlat' logo and three buttons: 'Создать', 'Выход', and 'Справка'.

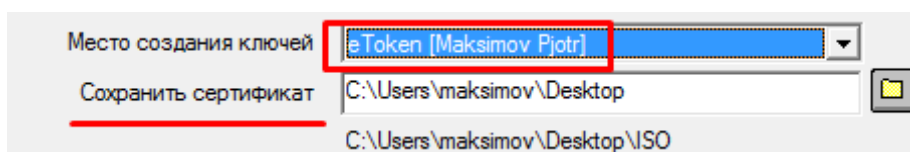
6. Установите отметку *Ключ RSA для протокола в формате ISO20022*.



7. Выберите место создания **место создания ключей**: «eToken» либо «файл». **Обратите внимание**, что надежнее хранить ключи на токене.

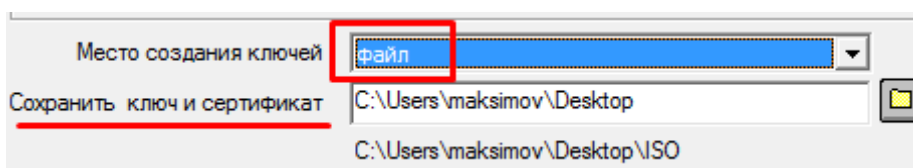
Если ключ создается на токене, предварительно убедитесь, что токен подключен к компьютеру.

8. А. При генерации ключа на токене заполните поле *Сохранить сертификат*.



Укажите путь к папке, где будет сохранен **сертификат ключа**.

- Б. При генерации ключа в файле заполните поле *Сохранить ключ и сертификат*.



Укажите путь к папке, где будет сохранен **сертификат открытого ключа**.

## 2.2 Заполнение параметров сертификата

Для настройки параметров сертификата открытого ключа на вкладке *Создание ключей* в поле *Параметры сертификата* нажмите кнопку *Настроить*.

*Создание*

Вы перейдете на страницу следующего вида.

Настройки сертификата		
Период действия	Серийный номер	Алгоритм
Действует с 10.08.2018 по 10.08.2019	9	RSA\sha256
Владелец сертификата		
Обязательные поля		
Код страны (C)	RU (Россия)	
Населенный пункт (L)	Moscow	
Организация (O)	Test Org Ltd	
Общее имя (CN)	Test Org	
Фамилия (SN)	Ivanov	
Имя и Отчество (G)	Ivan Ivanovich	
Пример заполнения		
	RU (Россия)	
	Moscow	
	Test Org Ltd	
	Test Org (для контролера: BITBWER@AXX)	
	Ivanov	
	Ivan Ivanovich	

**Период действия** – укажите период действия ключа, максимальная длина периода – 12 месяцев.

**Действует с** – дата начала действия сертификата;

**По** – дата окончания действия сертификата. Начальная и конечная даты входят в период.

**Срок действия сертификата устанавливается не более 12 месяцев.**

**Серийный номер** – серийный номер сертификата, целое число; при настройке параметров очередного сертификата номер автоматически увеличивается на 1.

Заполните параметры в панели **Владелец сертификата**.

### **Обратите внимание!**

- Необходимо заполнить только первый блок **Обязательные поля**.
- **Рекомендуемые поля** заполнять необязательно.
- **Названия всех полей заполняются только на латинице.**

Правила заполнения полей панели **Владелец сертификата/ Обязательные поля**.

**Код страны (C)** – наименование страны.

**Населенный пункт (L)** – для юридических лиц укажите населенный пункт, которому принадлежит юридический адрес организации владельца ключа. Для физических лиц укажите населенный пункт регистрации.

**Организация(O)** - введите наименование организации.

Если ключ создается для юридического лица, укажите наименование организации.

Если ключ создается для физического лица, укажите полностью ФИО физического лица, которое является владельцем ключа.

**Общее имя (CN)** – поле можно не заполнять или заполните это поле так же, как и поле **Организация (O)**.

**Фамилия (SN)** – фамилия владельца ключа.

**Имя и Отчество (G)** – укажите имя и отчество владельца ключа.

После заполнения всех обязательных полей нажмите кнопку **ОК**.

### Примеры заполнения реквизитов владельца сертификата

Юридическое лицо.

Обязательные поля	
Код страны (C)	RU (Россия)
Населенный пункт (L)	Moscow
Организация (O)	ООО Cyberplat
Общее имя (CN)	ООО Cyberplat
Фамилия (SN)	Maksimov
Имя и Отчество (G)	Petr Alekseevich

Физическое лицо.

Обязательные поля	
Код страны (C)	RU (Россия)
Населенный пункт (L)	Moscow
Организация (O)	Maksimov Petr Alekseevich
Общее имя (CN)	Maksimov Petr Alekseevich
Фамилия (SN)	Maksimov
Имя и Отчество (G)	Petr Alekseevich

Вернитесь на вкладку **Создание ключей**.

В поле **Длина создаваемого ключа** укажите значение **2048**.

параметры сертификата	настроить
Длина создаваемого ключа	2048

При создании ключа **на токене** придумайте и введите **Кодовую фразу токена**.

Кодовая фраза токена
*****

При создании ключа **в файле** введите **единый пароль** в следующие четыре поля.

**Требования к паролю:** длина не менее 8 символов, пароль должен содержать латинские буквы в верхнем и нижнем регистре, цифры, спецсимволы из списка (!@#%).

**Внимание!** При создании ключа в файле пароль необходимо обязательно заполнить и сохранить. Так как в случае утраты пароля он не подлежит восстановлению и ключ потребует пере выпуска.

При создании ключа в файле в поле *Привязывать ключи к компьютеру* установите отметку **Нет**.

Поле *Имя ключа в тонком клиенте* пользователь не заполняет, оно формируется программой Genkey и далее не используется. (Если отметка *Имя ключа в тонком клиенте* установлена, то в данном поле автоматически отображается значение, созданное программой Genkey).

Проверьте, что все параметры конфигурации заполнены правильно, и нажмите кнопку **Создать**.

**Генерация ключей завершена.**

В результате генерации будут созданы:

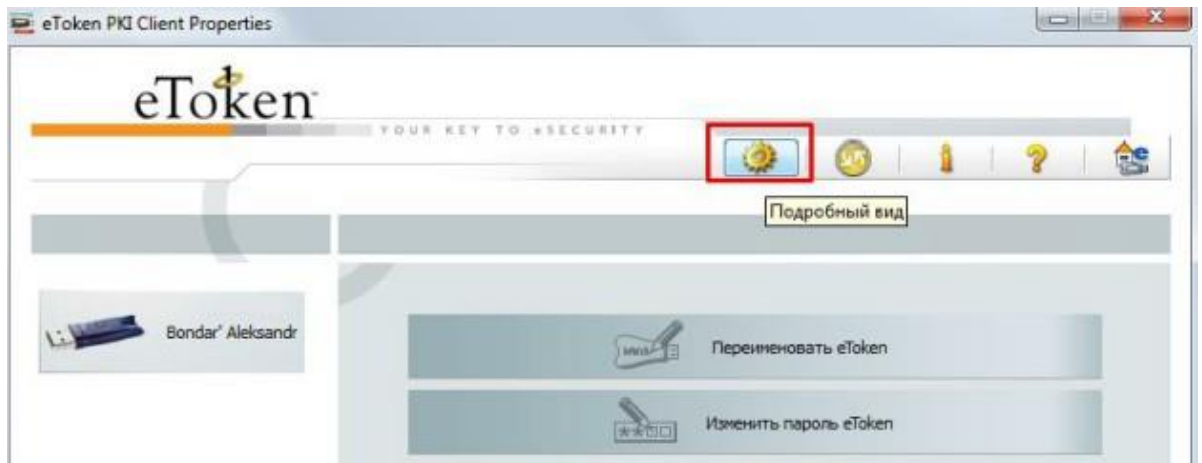
**сертификат открытого ключа** – файл **certificate.pem** будет создан в файле на диске компьютера,

на токене будут созданы **закрытый ключ и rfx-контейнер**, содержащий архив с закрытым ключом и сертификатом ключа.

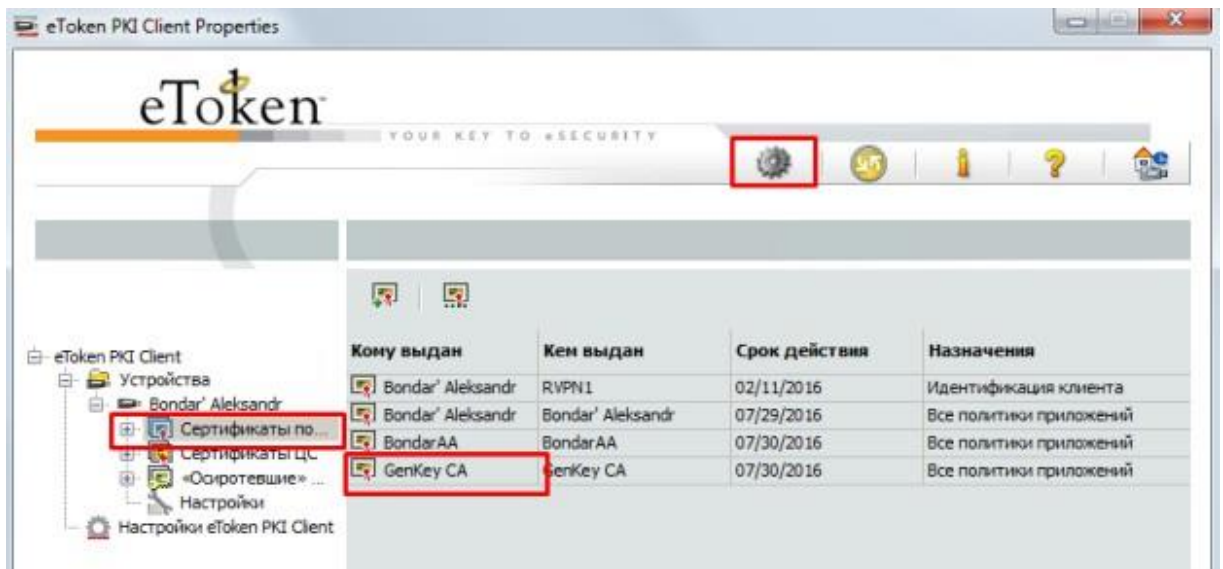
При создании ключа на токене следует удостовериться, что **новый ключ успешно записался на токен**.

Необходимо выполнить следующие действия.

- откройте программу **PKI Client** ;
- войдите в пункт главного меню **Подробный вид**;

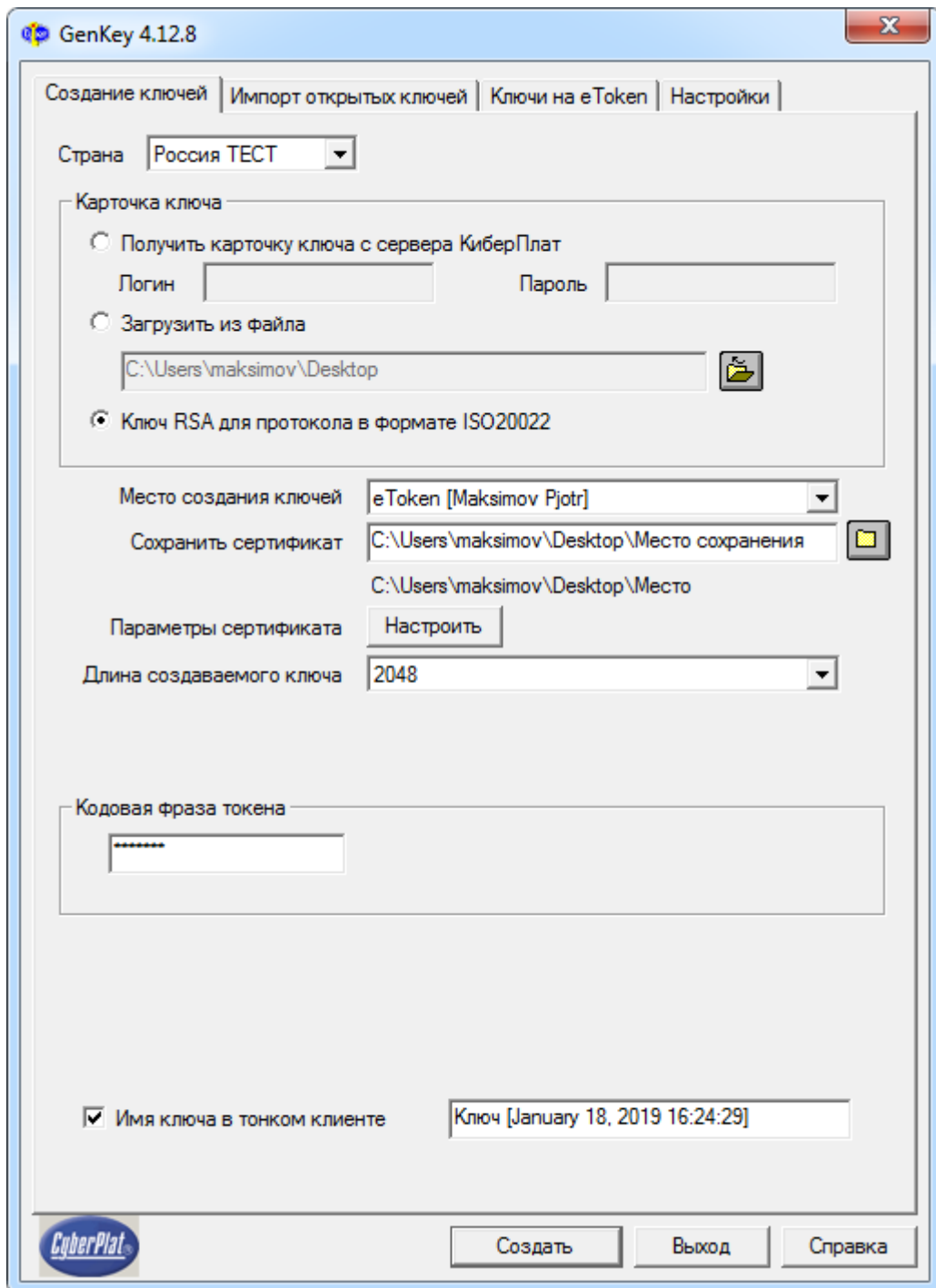


- Проверьте наличие созданного сертификата.



### 2.3 Пример настроек при создании ключей на токене

На следующем рисунке приведен пример заполнения настроек сертификата при создании ключей на токене.



В поле *Сохранить сертификат* указано значение **D:\** .

Пусть в настройках сертификата указано название организации **CN= Test Org 2** и дата создания ключей **10.08.2018**.

Тогда сертификат открытого ключа будет создан на диске компьютера в папке **D:\Test Org 2\_180810**. Это название отображается ниже поля *Сохранить сертификат*.

**Имена созданных файлов:**

**Test Org 2\_180810\_certificate.pem** – файл сертификата открытого ключа, сохраняется в созданной папке;

**Test Org 2\_180810\_certificate.pfx** – файл хранилища сертификата, сохраняется на токене;

**Test Org 2\_180810\_private\_key.pem** – файл закрытого ключа, сохраняется на токене.

## 2.4 Создание ключей в файле

Ключи необходимо выпускать для лиц, обладающих **полномочиями подписантов**.

Порядок создания ключей на токене описан в одноименном [разделе](#).

Порядок создания ключей в файле аналогичен порядку создания ключей на токене. Ключи могут размещаться на **жестком диске компьютера** или на **флеш-носителе**. В файлах сохраняются сертификат открытого ключа и закрытый ключ.

### Порядок работы при создании ключей в файле

1. Запустите программу генерации ключей GenKey.
2. Заполните параметры, отмеченные на рисунке красной рамкой.

Установите отметку **RSA**.

**Место создания ключей** – выберите значение «файл».

В поле **Сохранить ключи и сертификат** укажите путь к папке, куда будут сохраняться ключи. Название создаваемой папки с ключами отображается ниже поля.

4.17.7.0

Создание ключей | Импорт открытых ключей | Ключи на Token | Настройки

Формат ключа  
IPRIV по карточке ключа

Площадка Россия

Получить карточку ключа с сервера КиберПлат  
Логин  Пароль

Загрузить из файла

RSA

Для ISO20022, CyberFT

Место создания ключей файл

Сохранить ключ и сертификат   
D:\Test Org\_180810

Параметры сертификата Настроить

Длина создаваемого ключа 2048

Кодовая фраза закрытого ключа  
 Повтор

\*Пароль соответствует условиям

Кодовая фраза pfx  
 Повтор фразы

\*Пароль соответствует условиям

Привязывать ключи к компьютеру  Нет  Да

Имя ключа в тонком клиенте

Создать | Выход | Справка

3. В поле **Параметры сертификата** нажмите кнопку **Настроить**, откроется следующее окно.

**Настройки сертификата** ✕

<b>Период действия</b>		<b>Серийный номер</b>	<b>Алгоритм</b>		
Действует с	10.08.2018	по	10.08.2019	9	RSA\sha256

<b>Владелец сертификата</b>		<b>Пример заполнения</b>
<b>Обязательные поля</b>		
Код страны (C)	RU (Россия)	RU (Россия)
Населенный пункт (L)	Moscow	Moscow
Организация (O)	Test Org Ltd	Test Org Ltd
Общее имя (CN)	Test Org	Test Org (для контролера: BITBWER@A××× )
Фамилия (SN)	Ivanov	Ivanov
Имя и Отчество (G)	Ivan Ivanovich	Ivan Ivanovich
<b>Рекомендуемые поля</b>		
Регион (S)	77 Moscow	77 Moscow
Подразделение (OU)	Board of Directors	Board of Directors
Адрес (STREET)	Testovaya ul., 12, office 123	Testovaya ul., 12, office 123
Должность (T)	Director	Director
Email (E)	dir@testorg.com	dir@testorg.com
Описание (Description)	OGRN 1234567890123; INN 123456789012	OGRN 1234567890123; INN 123456789012

**Примечание**

- Для обеспечения возможности использования сертификата в международном обмене рекомендуется заполнять поля латиницей, для обмена только в пределах РФ можно использовать кириллицу.
- При заполнении полей сертификата не рекомендуется использовать следующие символы: кавычки («»'), апостроф ('), прямая и обратная косая черта (^).

OK

Заполните *Период действия* ключей.

**Внимание!**

Максимальный срок действия ключа **12 месяцев**.

Надо **заполнить все обязательные поля** владельца сертификата, как это описано в разделе [«Заполнение параметров сертификата»](#).

4. Вернитесь на вкладку *Создание ключей*. Установите длину ключа **2048 бит**.

Установите длину ключа **2048 бит**.

В параметре *Привязывать ключи к компьютеру* установите отметку **«Нет»**.

5. Далее необходимо указать **одинаковые кодовые фразы** (пароли) для закрытого ключа и для хранилища ключа PFX.

**Внимание!** Кодовую фразу необходимо сохранить. Так как в случае утраты пароль не подлежит восстановлению, ключ потребуется перевыпускать.

6. После заполнения параметров нажмите кнопку *Создать*.

7. В папке, путь к которой указан в поле *Сохранить файл и сертификат*, появится новая папка с файлами, перечисленными ниже.

Название папки формируется из значения поля *Общее имя (CN)* в настройках сертификата и даты создания ключей в формате ГГММДД.

**Пример.** CN= Test Org, дата создания ключей 10.08.2018.

Имя созданной папки: **Test Org\_180810**

Имена файлов, сохраняемых в созданной папке:

**Test Org\_180810\_certificate.pem** – файл сертификата открытого ключа;

**Test Org\_180810\_certificate.pfx** – файл хранилища сертификата открытого ключа;

**Test Org\_180810\_private\_key.pem** – файл закрытого ключа.

**Внимание!** Обязательно сохраните созданные файлы. Они необходимы для подписания отправляемых документов.

### 3 Установка программы для подписания отправляемых документов.

Далее необходимо установить программу **CyberSignService** подписания отправляемых документов.

Скачайте установочный файл здесь:

<http://download.cyberft.ru/CyberSignService/> .

Программа устанавливается пользователем с правами администратора компьютера.

Инструкцию по настройке программы можно на сайте <https://www.cyberft.ru/> в разделе Главная/ Документы и ПО/ Программное обеспечение

(<https://cyberft.ru/downloads/soft>) по ссылке «[Руководство «Сервис подписания в сети CyberFT»](#)».

### 4 Документация

Ссылки на документацию ПО «Терминал CyberFT» вы найдете здесь: <https://cyberft.ru/downloads/soft> .