Работа с утилитой "Генератор запросов сертификатов для Рутокен ЭЦП 2.0 и 3.0"

Общая информация

Эту инструкцию можно использовать, если вы работаете с устройствами:

- Рутокен ЭЦП 2.0 2100;
- Рутокен ЭЦП 2.0;
- Рутокен ЭЦП 2.0 micro;
- Рутокен ЭЦП 2.0 Touch;
- Рутокен ЭЦП 2.0 Flash;
- Рутокен ЭЦП 2.0 Type-C;
- Рутокен ЭЦП 2.0 3000;
- Рутокен ЭЦП 3.0 NFC.

У каждого устройства Рутокен есть PIN-код Пользователя и PIN-код Администратора.

PIN-код Пользователя является паролем, который используется для реализации основных функций устройства Рутокен. Его значение по умолчанию — 12345678.

PIN-код Администратора является паролем, который используется для доступа к административным функциям устройства Рутокен. Его значение по умолчанию — 87654321.

Процесс создания сертификата квалифицированной электронной подписи состоит из следующих этапов:

1 этап. Создание запроса на сертификат квалифицированной электронной подписи и сохранение его на компьютере.

2 этап. Подписание запроса на сертификат квалифицированной электронной подписи.

3 этап. Создание сертификата квалифицированной электронной подписи и сохранение его на компьютере.

4 этап. Запись сертификата на устройство Рутокен ЭЦП 2.0 и 3.0.

Утилита "Генератор запросов сертификатов для Рутокен ЭЦП 2.0 и 3.0" предназначена:

- для создания запроса на сертификат квалифицированной электронной подписи;
- для записи готового сертификата на устройство Рутокен.

Запрос на сертификат используется для указания всей необходимой информации для сертификата квалифицированной электронной подписи.

Доступ к утилите возможен из Панели управления Рутокен, которая входит в состав комплекта "Драйверы Рутокен для Windows".

Установка комплекта "Драйверы Рутокен для Windows"

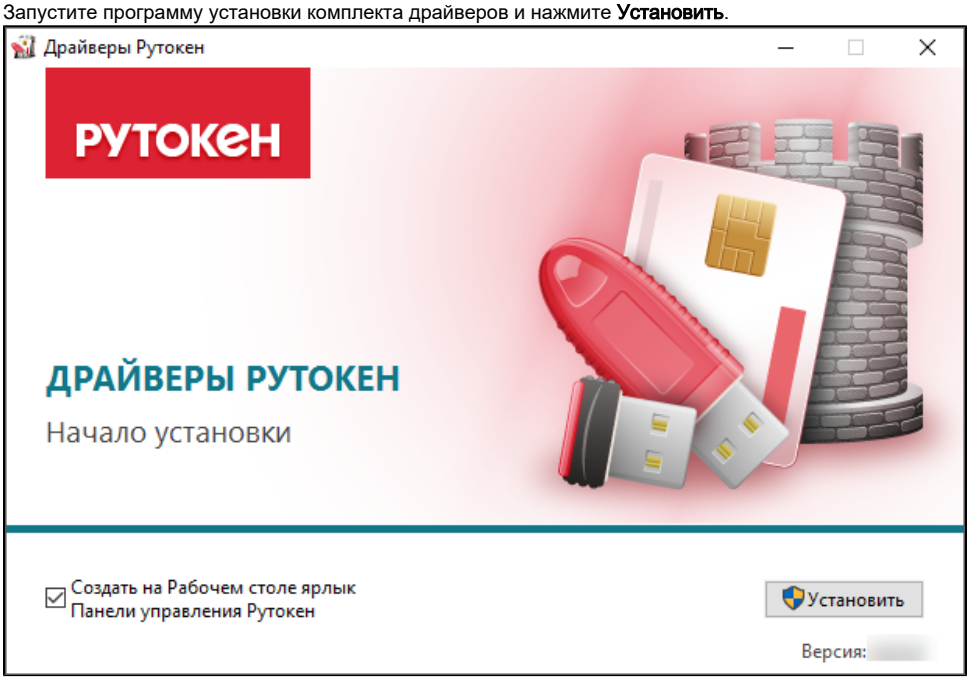
Актуальная версия комплекта драйверов доступна по ссылке:

https://www.rutoken.ru/support/download/drivers-for-windows/

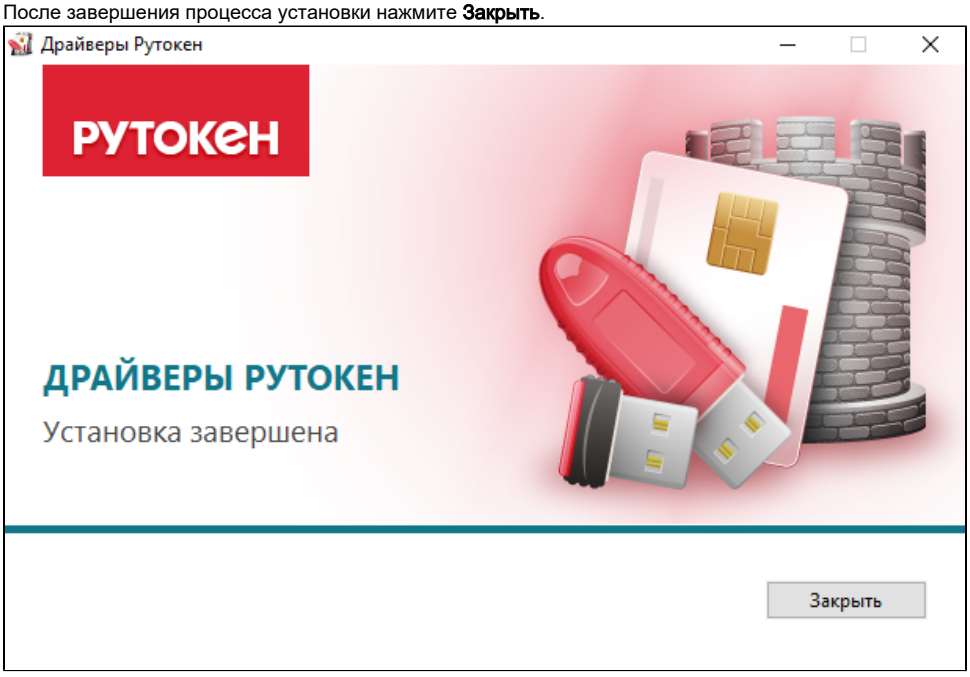
Перед началом установки комплекта драйверов рекомендуется закрыть все работающие приложения и отключить Рутокен от компьютера. Для установки комплекта драйверов необходимы права администратора системы.

Для установки комплекта драйверов:

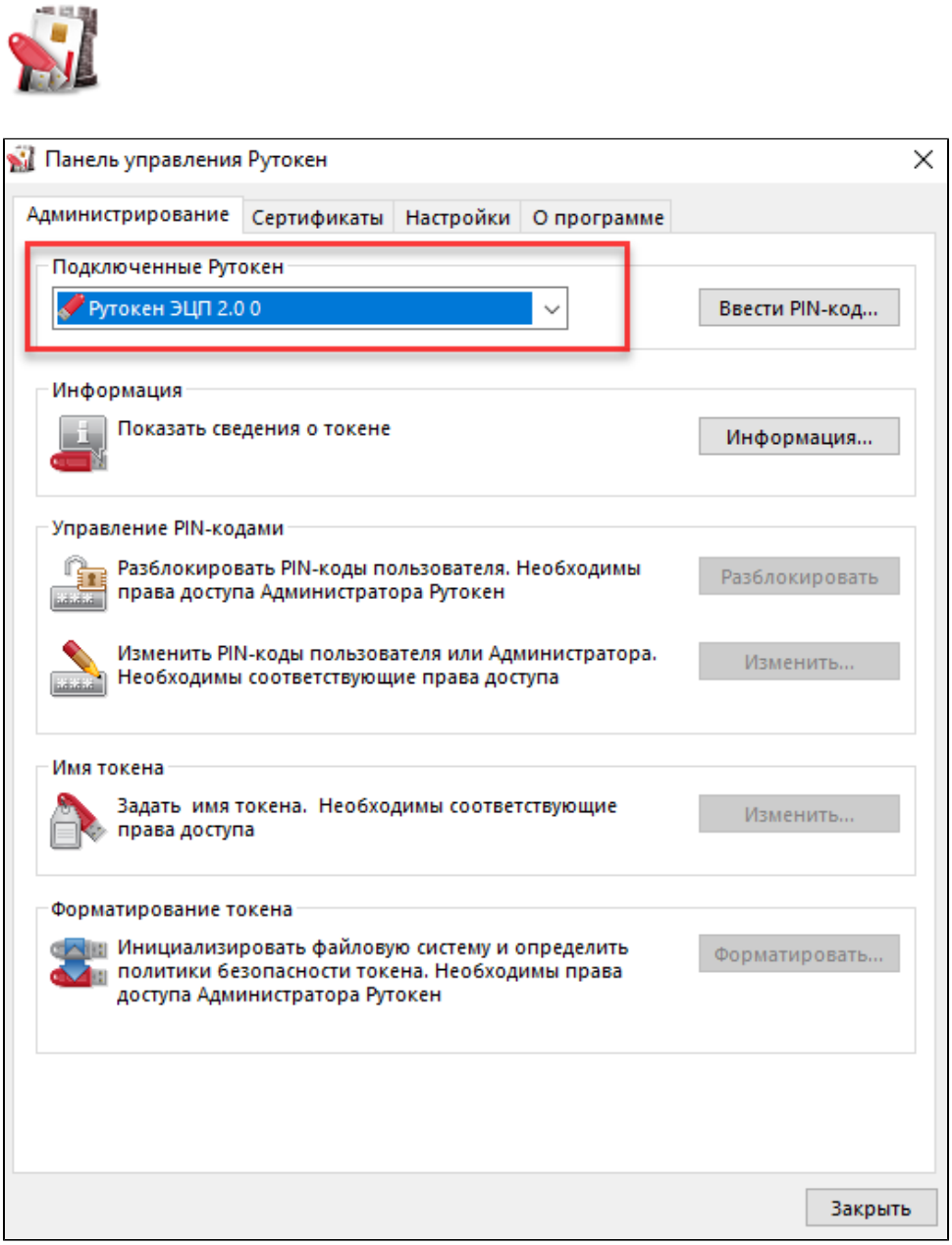
1. Запустите программу установки комплекта драйверов и нажмите **Установить**.



2. В окне с запросом на разрешение изменений на компьютере нажмите **Да**. В результате запустится процесс установки комплекта драйверов.
3. После завершения процесса установки нажмите **Закрыть**.



4. Подключите Рутокен к компьютеру.
5. Запустите **Панель управления Рутокен**. В результате откроется главное окно панели управления и в поле **Подключенные Рутокен** отобразится название подключенного устройства.



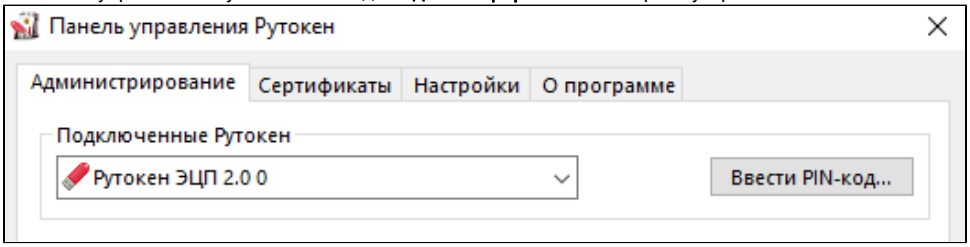
Запуск утилиты "Генератор запросов сертификатов для Рутокен ЭЦП 2.0 и 3.0"

Чтобы генератор запросов стал доступен в Панели управления Рутокен необходимо ввести PIN-код Администратора.

Если вы не знаете PIN-кода Администратора, то обратитесь к тому, кто выдал вам устройство Рутокен.

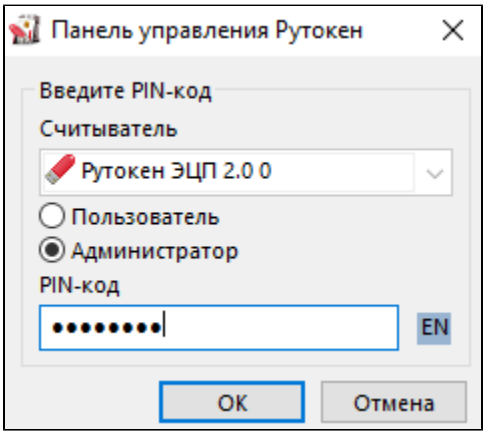
Чтобы запустить утилиту:

1. В Панели управления Рутокен на вкладке **Администрирование** выберите устройство.

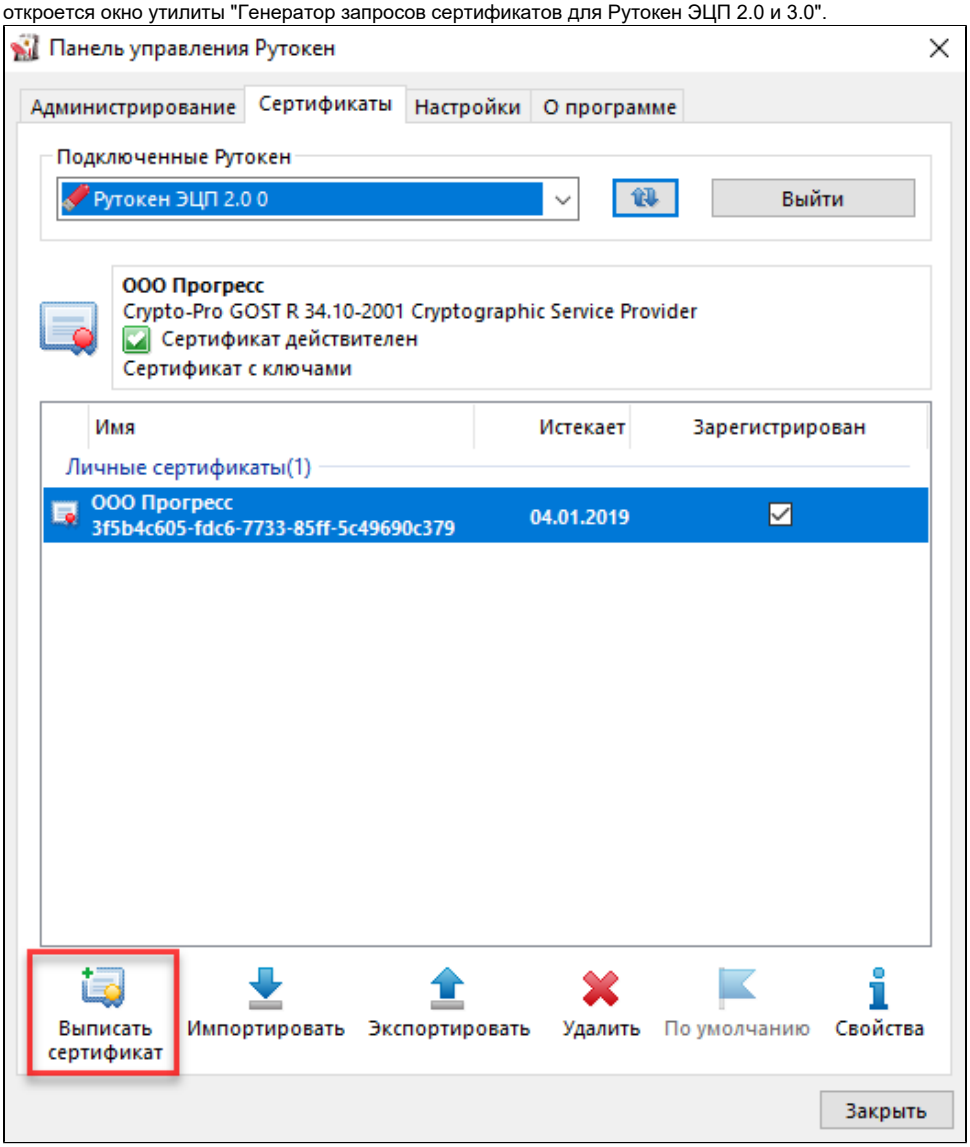


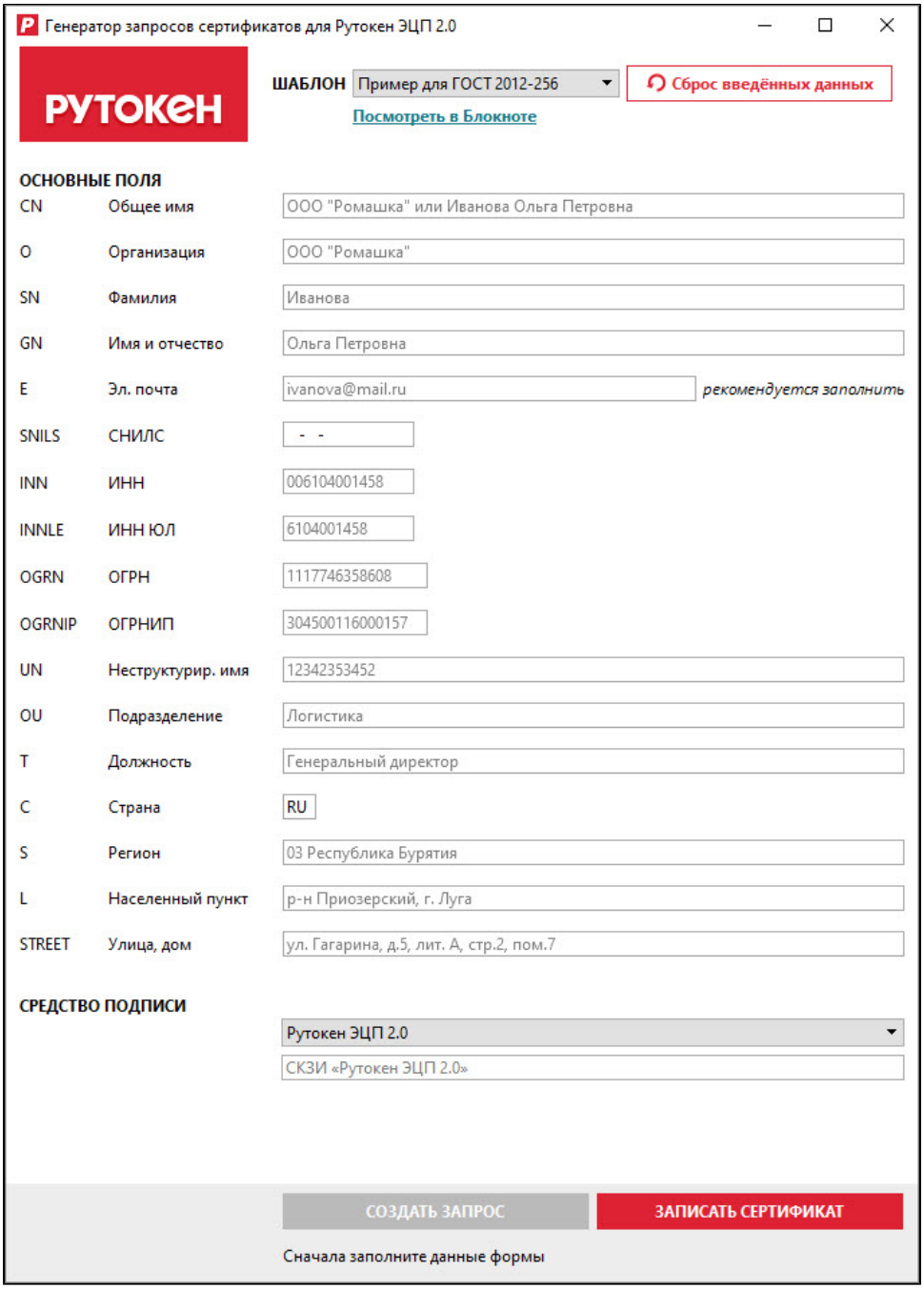
2. Нажмите **Ввести PIN-код**.

3. Установите переключатель в положение **Администратор** и введите PIN-код Администратора.
4. Нажмите **ОК**.



5. Перейдите на вкладку **Сертификаты**.
6. Нажмите **Выписать сертификат** (эта кнопка станет активной, если вы ввели корректный PIN-код Администратора). В результате откроется окно утилиты "Генератор запросов сертификатов для Рутокен ЭЦП 2.0 и 3.0".





В полях отображаются примеры значений для каждого поля.

После этого вы можете работать с утилитой.

Краткое описание работы с утилитой

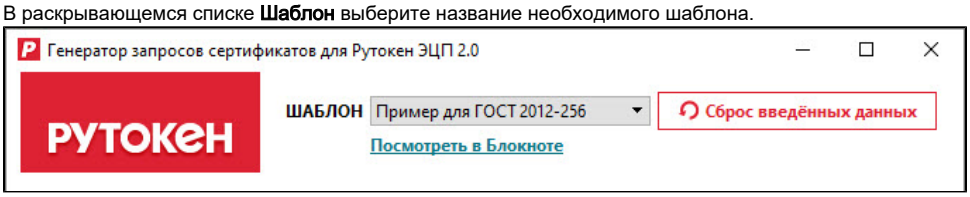
Создание запроса на сертификат квалифицированной электронной подписи

Перед запуском утилиты отключите от компьютера все лишние устройства Рутокен. Оставьте только устройство, на которое необходимо записать сертификат квалифицированной электронной подписи.

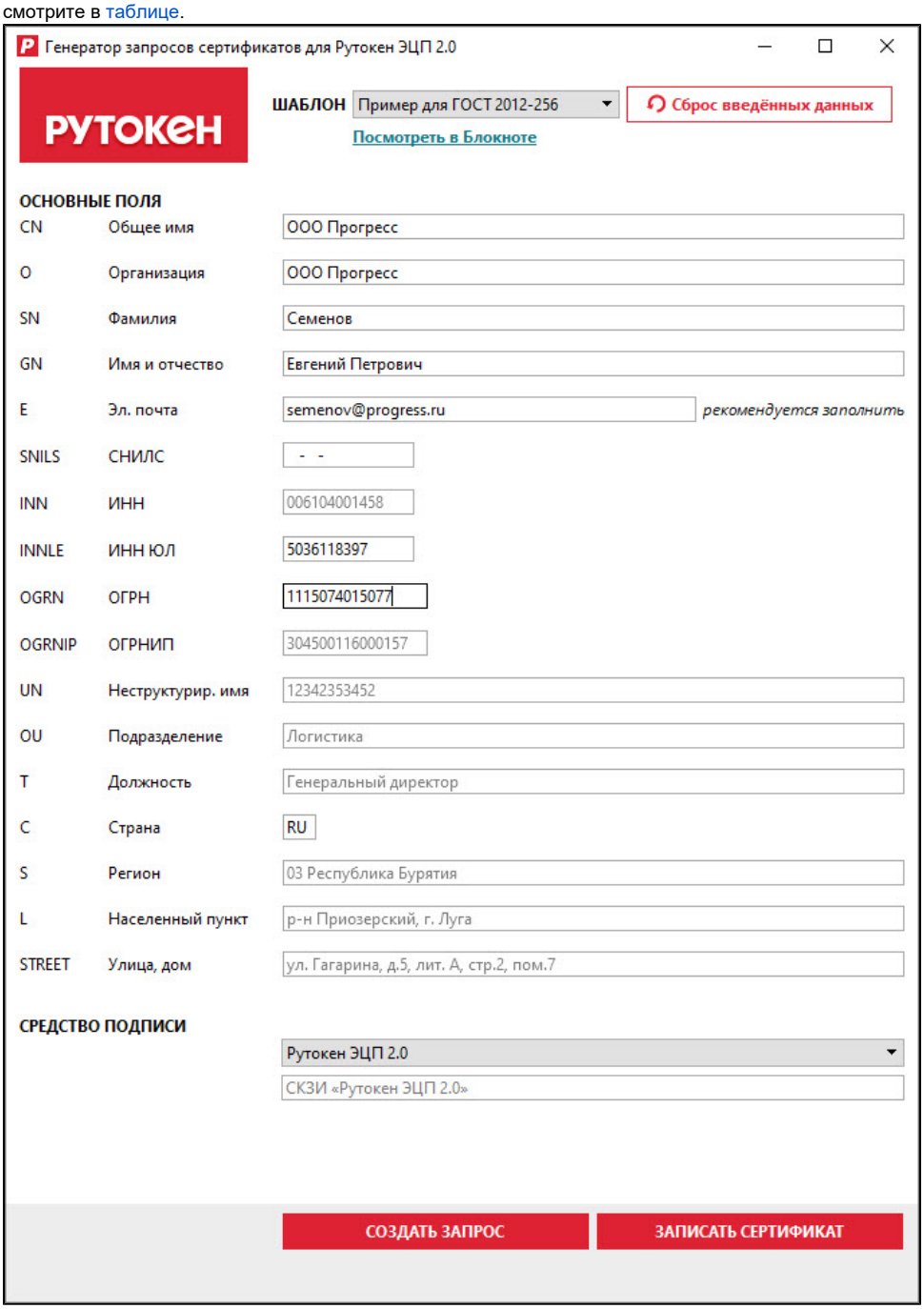
Для **создания запроса** на сертификат квалифицированной электронной подписи:

1. Запустите утилиту.

2. В раскрывающемся списке **Шаблон** выберите название необходимого шаблона.

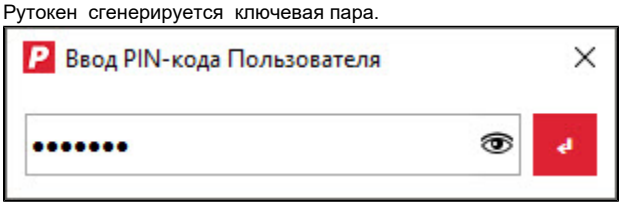


3. Введите необходимые значения полей запроса (все поля заполняются согласно Приказу ФСБ РФ от 29.01.2021 № 31 "О внесении в приказ ФСБ России от 27.12.2011 № 795 "Об утверждении требований к форме квалифицированного сертификата ключа проверки электронной подписи"). Требования к данным, указанным в запросе на сертификат квалифицированной электронной подписи смотрите в таблице.

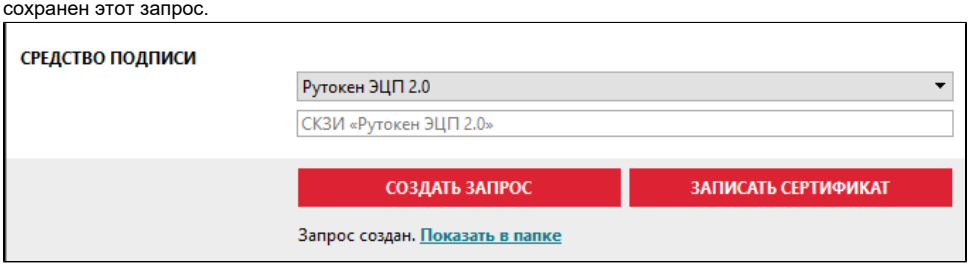


4. Нажмите **Создать запрос.**
5. Выберите на компьютере папку для сохранения файла запроса и нажмите **Сохранить**.
6. Укажите PIN-код Пользователя устройства Рутокен.

7. Нажмите на кнопку . В результате на компьютере сохранится файл запроса, а на устройстве Рутокен сгенерируется ключевая пара.



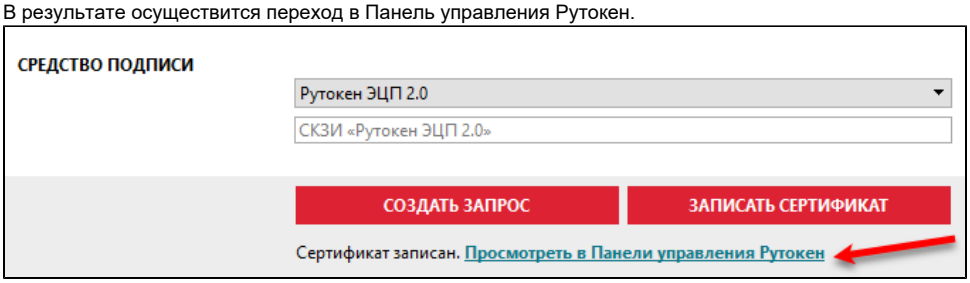
8. Чтобы убедиться в том, что запрос создан, щелкните по ссылке **Показать в папке**. В результате откроется папка, в которой сохранен этот запрос.



Запись сертификата квалифицированной электронной подписи на устройство Рутокен

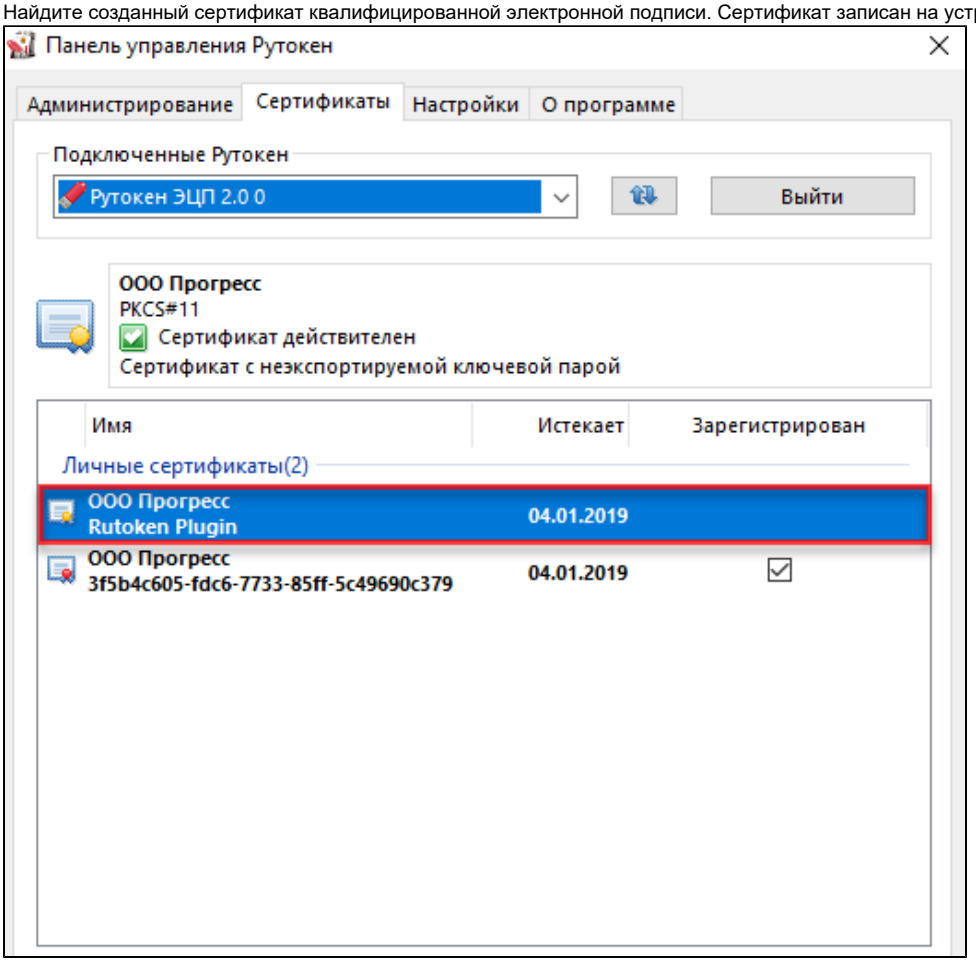
Для **записи** сертификата квалифицированной электронной подписи на устройство Рутокен ЭЦП 2.0 и 3.0:

1. Нажмите **Запись сертификата**.
2. Выберите на компьютере файл с сертификатом и нажмите **Открыть**. В результате сертификат запишется на устройство Рутокен.
3. Для просмотра сертификата, записанного на устройство Рутокен, щелкните по ссылке **Просмотреть в Панели управления Рутокен.** В результате осуществится переход в Панель управления Рутокен.



4. Перейдите на вкладку **Сертификаты** и нажмите на кнопку .

5. Найдите созданный сертификат квалифицированной электронной подписи. Сертификат записан на устройство Рутокен.



Дополнительные возможности утилиты

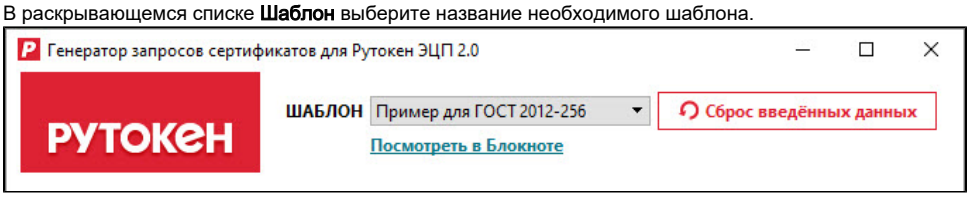
Пользователям утилиты доступны следующие возможности для работы с шаблонами:

- изменение параметров шаблона;
- сохранение нового шаблона на компьютере;
- использование существующего или нового шаблона.

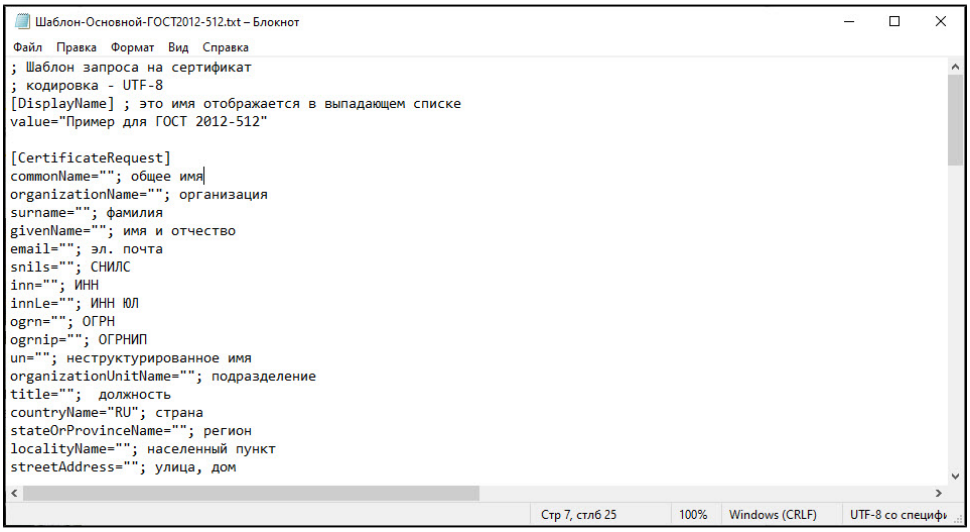
Изменение параметров шаблона запроса на сертификат квалифицированной электронной подписи

Для изменения параметров шаблона:

1. Запустите **Панель управления Рутокен**.
2. Запустите утилиту.
3. В раскрывающемся списке **Шаблон** выберите название необходимого шаблона.



4. Щелкните по ссылке "Просмотреть в Блокноте". Откроется окно шаблона.

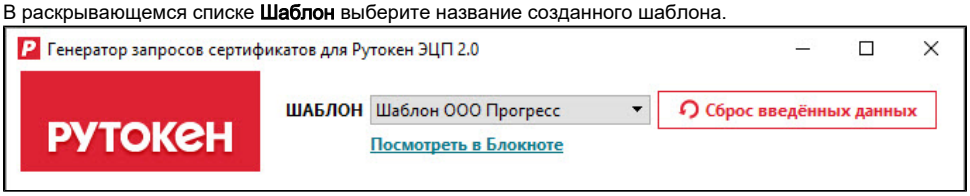


5. Измените необходимый параметр запроса.
6. В окне шаблона выберите пункт **Файл** и подпункт **Сохранить как**.
7. Выберите папку для сохранения шаблона на компьютере.
8. Укажите имя файла.
9. Нажмите **Сохранить**.

Использование нового шаблона запроса на сертификат квалифицированной электронной подписи

Для использования нового шаблона запроса на сертификат квалифицированной электронной подписи:

1. Запустите **Панель управления Рутокен**.
2. Запустите утилиту.
3. В раскрывающемся списке **Шаблон** выберите название созданного шаблона.



4. Следуйте инструкции по созданию запроса на сертификат квалифицированной электронной подписи.

Структура кода шаблона запроса на сертификат квалифицированной электронной подписи

Код шаблона запроса на сертификат квалифицированной электронной подписи состоит из блоков, у каждого из которых есть свое назначение.

Блок **[DisplayName]** используется для указания названия шаблона, которое отобразится в раскрывающемся списке в окне **Генератор запросов сертификатов для Рутокен ЭЦП 2.0 и 3.0**.

Блок **[CertificateRequest]** используется для указания информации о владельце сертификата. Параметры запроса данного блока описаны в **Таблице 1**.

Таблица 1

Название поля (параметр запроса)	**Требования к данным**
Общее имя (`commonName`)	• для физического лица — имя, фамилия и отчество владельца сертификата • для юридического лица — наименование организации владельца сертификата
Организация	• наименование организации владельца сертификата

(organizationName)	
Фамилия (surname)	• фамилия владельца сертификата с большой буквы в одно слово (без пробелов)
Имя и отчество (givenName)	• имя и отчество владельца сертификата
Эл. почта (email)	• адрес электронной почты владельца сертификата (используются только латинские буквы и цифры)
СНИЛС (snils)	• строка, состоящая из 11 цифр • для физического лица — СНИЛС владельца сертификата • для юридического лица — СНИЛС организации владельца сертификата
ИНН (inn)	ИНН физического лица, строка, состоящая из 12 цифр
ИНН ЮЛ (innLe)	ИНН юридического лица, состоящая из 10 цифр
ОГРН (ogrn)	• строка, состоящая из 13 цифр • ОГРН организации владельца сертификата
ОГРНИП (ogrnip)	• строка, состоящая из 15 цифр • ОГРНИП владельца сертификата
Неструктурир. имя (un)	• КПП организации владельца сертификата (для ЕГАИС)
Подразделение (organizationUnitName)	• подразделение или отдел, в котором работает владелец сертификата
Должность (title)	• должность владельца сертификата
Страна (countryName)	• для физического лица — краткое наименование страны, в которой проживает владелец сертификата • для юридического лица — краткое наименование страны, в которой находится организация владельца сертификата
Регион (stateOrProvinceName)	• для физического лица — название региона, в котором проживает владелец сертификата • для юридического лица — название региона, в котором находится организация владельца сертификата
Населенный пункт (localityName)	• для физического лица — название населенного пункта, в котором проживает владелец сертификата • для юридического лица — название населенного пункта, в котором находится организация владельца сертификата
Улица, дом	

(streetAddress)	• для физического лица — адрес, по которому проживает владелец сертификата • для юридического лица — юридический адрес организации владельца сертификата

Блок **[KeyUsage]** используется для указания области использования сертификата. Значения, которые можно указать в данном блоке указаны в **Таблице 2**.

Таблица 2

Название	Описание
digitalSignature	электронная цифровая подпись
nonRepudiation	неотрекаемость от авторства
keyEncipherment	шифрование ключей
dataEncipherment	шифрование данных
keyAgreement	согласование ключей
keyCertSign	электронная цифровая подпись сертификатов ключей подписи
crlSign	электронная цифровая подпись списков отозванных сертификатов
encipherOnly	зашифровывание
decipherOnly	расшифровывание

Блок **[ExtendedKeyUsage]** используется для указания параметров расширенного использования сертификата. Здесь указываются идентификаторы необходимых операций, классов пользователей и устройств. Примеры значений смотрите в **Таблице 3**. В данном блоке вы можете задавать и свои значения.

Таблица 3

Значение	Описание
1.3.6.1.5.5.7.3.2	проверка подлинности клиента
1.3.6.1.5.5.7.3.4	защищенная электронная почта
1.2.643.2.2.34.6	пользователь Центра Регистрации, HTTP, TLS клиент
1.2.643.2.2.34.26	пользователь службы актуальных статусов
1.2.643.2.2.34.25	пользователь службы штампов времени

Блок **[CustomExtension]** используется для указания расширений сертификата не предусмотренных в других блоках.

Расширения сертификата — это информационные поля, которые содержат дополнительные сведения о сертификате.

Расширения сертификата задаются следующими параметрами:

- oid — идентификатор расширения;
- value — данные этого расширения в DER-кодировке.
- criticality — критичность наличия данного расширения.

Блок **[Criticality]** используется для указания критичности наличия параметров сертификата, указанных в блоках **[KeyUsage]** и **[ExtendedKeyUsage]**.

Способ идентификации заявителя (**IdentificationKind**, OID=1.2.643.100.114) задается в этом блоке.
Значение с 0 (личное присутствие) - по умолчанию добавляется.
В описании шаблона есть другие значения:

Таблица 4

Значение IdentificationKind oid=1.2.643.100.114	**Описание**
`@ByteArray(\x02\x01\x00)`	Личное присутствие (0)
`@ByteArray(\x02\x01\x01)`	По действующей КЭП (1)
`@ByteArray(\x02\x01\x02)`	Загранпаспорт с электронным носителе (2)
`@ByteArray(\x02\x01\x03)`	ЕСИА / ЕБС (3)

Дополнительная информация об утилите

Изменение значения поля запроса на сертификат квалифицированной электронной подписи

Для изменения параметра запроса на сертификат квалифицированной электронной подписи необходимо выполнить следующие действия:

1. Запустите **Панель управления Рутокен**.
2. Запустите утилиту.
3. Выберите название шаблона.
4. Щелкните по ссылке "Просмотреть в блокноте". Откроется окно **Шаблон-Основной**.
5. Поставьте курсор мыши в необходимой строке между кавычками и укажите значение параметра.
6. В окне шаблона выберите пункт **Файл** и подпункт **Сохранить как**.
7. Выберите папку для сохранения шаблона на компьютере.
8. Укажите имя файла.
9. Нажмите **Сохранить**.

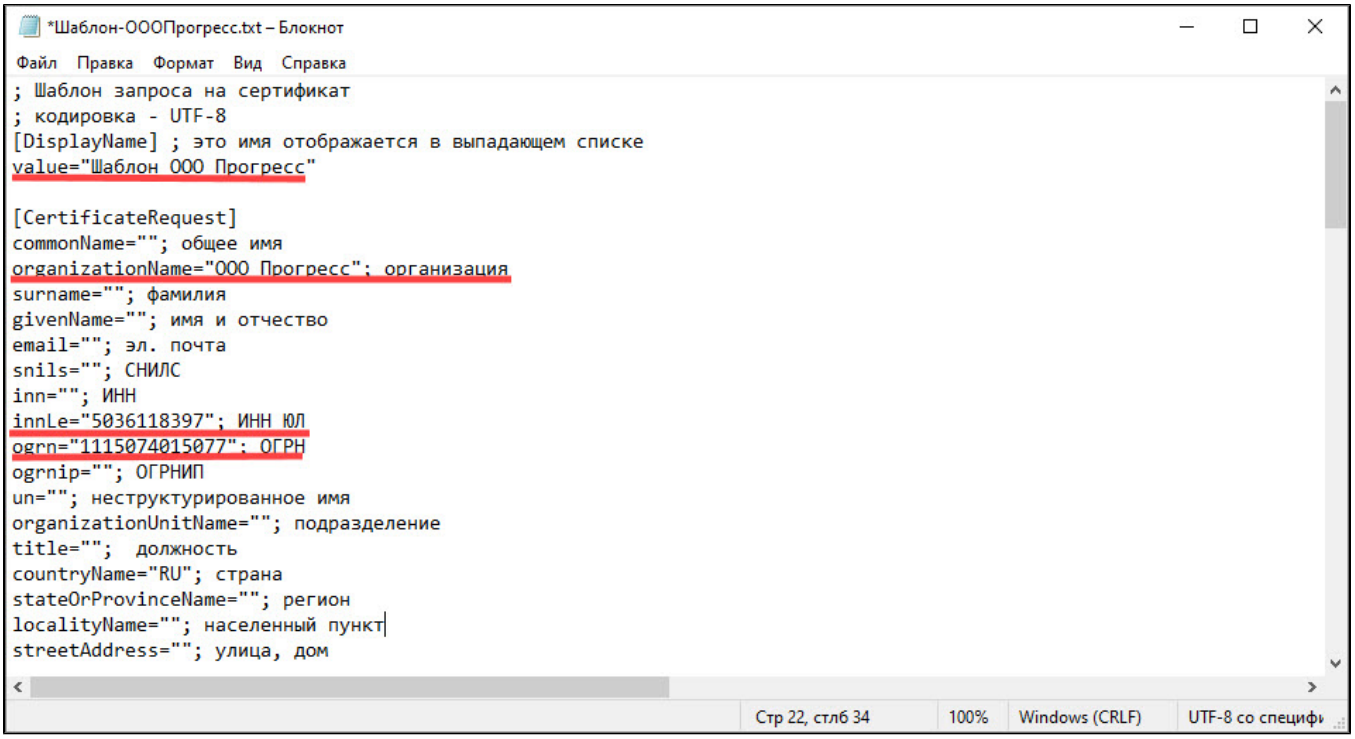
Примеры работы с шаблонами запросов

Пример 1:

Изменения в блоке **[CertificateRequest]**.

1) Изменим следующие параметры запроса на сертификат квалифицированной электронной подписи:

- value;
- organizationName;
- innLe;
- ogrn.

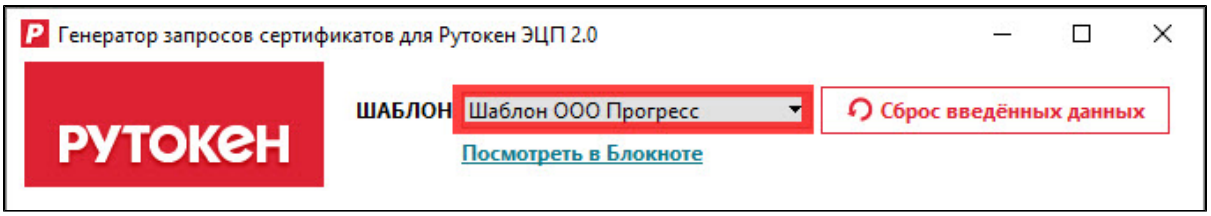


2) Сохраним новый шаблон на компьютере и назовем его **Шаблон ООО Прогресс**.

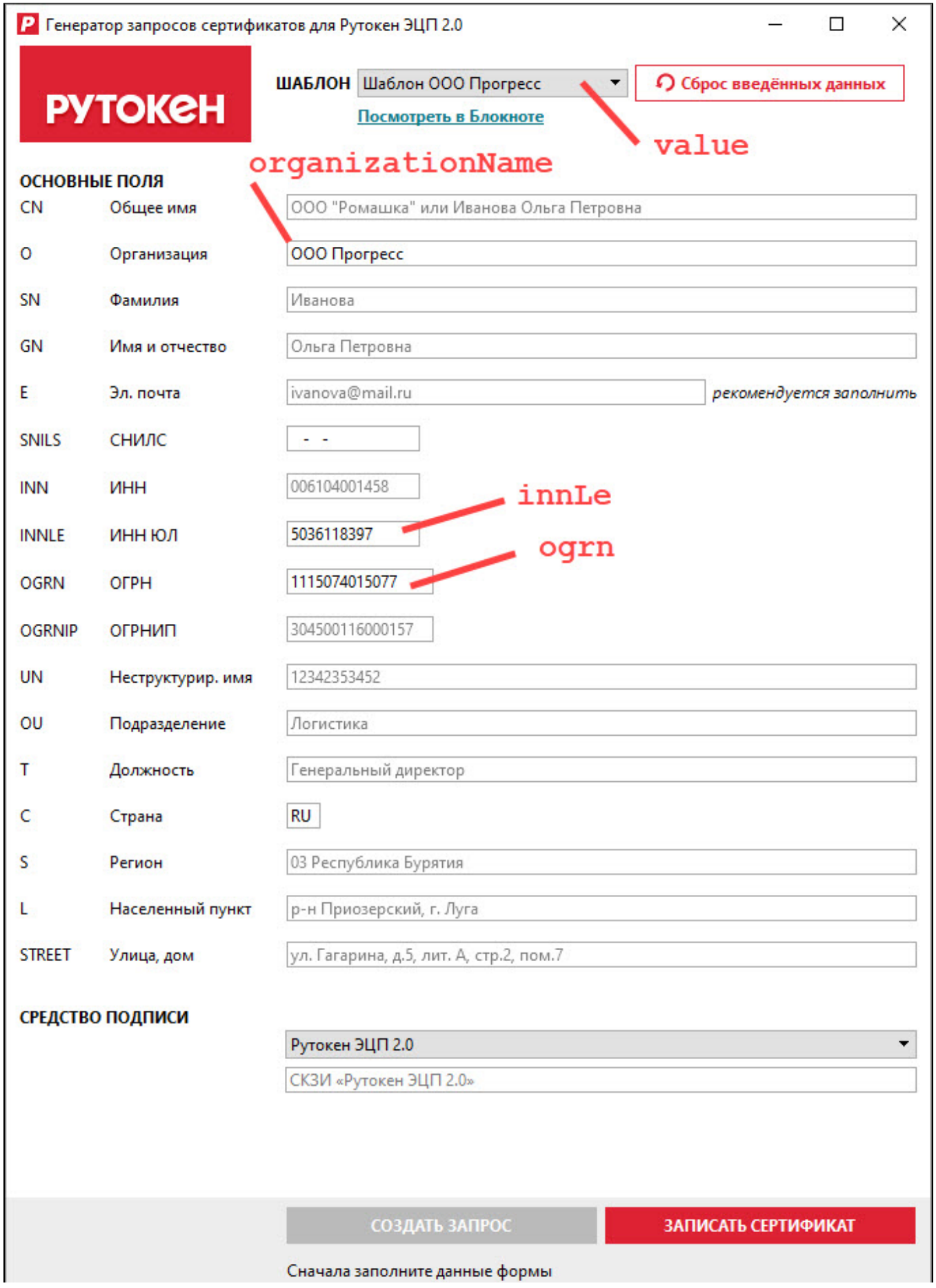
3) Запустим **Панель управления Рутокен**.

4) Откроем утилиту.

5) В раскрывающемся списке выберем название шаблона.



6) Заданные параметры отобразятся в окне **Генератор запросов сертификатов для Рутокен ЭЦП 2.0**.


Генератор запросов сертификатов для Рутокен ЭЦП 2.0
РУТОКЕН
ШАБЛОН
Шаблон ООО Прогресс
Сброс введённых данных
Посмотреть в Блокноте
value
organizationName
ОСНОВНЫЕ ПОЛЯ
CN Общее имя
ООО "Ромашка" или Иванова Ольга Петровна
O Организация
ООО Прогресс
SN Фамилия
Иванова
GN Имя и отчество
Ольга Петровна
E Эл. почта
ivanova@mail.ru
рекомендуется заполнить
SNILS СНИЛС
INN ИНН
006104001458
innLe
INNLE ИНН ЮЛ
5036118397
ogrn
OGRN ОГРН
1115074015077
OGRNIP ОГРНИП
304500116000157
UN Неструктурир. имя
12342353452
OU Подразделение
Логистика
T Должность
Генеральный директор
C Страна
RU
S Регион
03 Республика Бурятия
L Населенный пункт
р-н Приозерский, г. Луга
STREET Улица, дом
ул. Гагарина, д.5, лит. А, стр.2, пом.7
СРЕДСТВО ПОДПИСИ
Рутокен ЭЦП 2.0
СКЗИ «Рутокен ЭЦП 2.0»
СОЗДАТЬ ЗАПРОС
ЗАПИСАТЬ СЕРТИФИКАТ
Сначала заполните данные формы

Пример 2:

Изменения в блоке **[CustomExtension]**.

1) Добавим следующие расширения для сертификата:

- `1\oid=1.3.6.1.4.1.311.21.7`
- `1\value=@ByteArray(\x30\x0D\x06\x08\x2A\x85\x03\x02\x02\x2E\x00\x08\x02\x01\x01)`
- `1\criticality=non critical`

```
[CustomExtensions]
1\oid=1.3.6.1.4.1.311.21.7
1\value=@ByteArray(\x30\x0D\x06\x08\x2A\x85\x03\x02\x02\x2E\x00\x08\x02\x01\x01)
1\criticality=non critical
size=1
```

Каждое расширение для сертификата может быть обозначено, как критическое или некритическое (параметр criticality). Сертификат должен быть отвергнут при отсутствии критических расширений (если параметр у расширения criticality=critical).

Отсутствие некритических расширений может быть проигнорировано (если параметр у расширения criticality= non critical).

2) Сохраните шаблон на компьютере. В результате для сертификата будет задано следующее расширение:

```
SEQUENCE {
 OBJECTIDENTIFIER 1.2.643.2.2.46.0.8
 INTEGER 1
 }
```