ООО Фирма «ИнфоКрипт»

SberSign-L
11485466.72.21.12.185

Руководство пользователя

2024

Содержание

Введение

Настоящий документ содержит руководство пользователя по работе с программным изделием SberSign-L. Руководство включает в себя справочную информацию по работе программного изделия SberSign-L.

1 Назначение и условия применения

1.1 Назначение системы

Программный продукт SberSign-L предназначен для генерации и проверки электронной подписи (ЭП) файлов на базе алгоритмов, соответствующих стандартам ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012.

SberSign-L использует в качестве СКЗИ модуль криптографических библиотек «Бикрипт 5.0».

В программном продукте SberSign-L реализованы следующие основные функции:

- Генерация ключа ЭП и ключа проверки ЭП в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012. Создание запроса на выпуск сертификата.
- Формирование файла в формате rtf, содержащего ключ проверки ЭП и реквизиты пользователя.
- Поддержка однокомпонентного и двухкомпонентного ключей ЭП.
- Хранение основного и резервного ключа ЭП на ТМ-идентификаторе.
- Формирование и проверка ЭП файлов в соответствии со стандартами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012.
- Формирование ЭП файла с добавлением сертификата ключа ЭП.
- Проверка ЭП файла с использованием справочника ключей проверки ЭП или сертификатов ключей ЭП.
- Контроль целостности справочника (сертификатов) ключей проверки ЭП и справочника ключей проверки ЭП администраторов.
- Проверка ЭП файла с использованием списка отозванных сертификатов.
- Работа в файлах сценариев автоматического выполнения команд (BAT, CMD).
- Ведение системного журнала.

1.2 Условия применения системы

SberSign-L устанавливается на компьютер, удовлетворяющий следующим программным и аппаратным требованиям:

- Программный продукт SberSign-L должен работать под управлением следующих 64-х битных операционных систем: SberLinux (совместим с ОС RedHat 8.6 и выше) и SberOS (совместим с ОС Debian Linux 12 и выше).
- Процессор не ниже Intel Pentium IV.
- Жёсткий диск ёмкостью не менее 1 Гб.
- ОЗУ ёмкостью не менее 1 Гб.
- К компьютеру может быть подключено устройство считывания аутентифицирующих носителей ТМ Infocrypt.

2 Установка SberSign-L

Для того чтобы установить SberSign-L, необходимо выполнить следующие действия:

- создать каталог, в котором должен располагаться SberSign-L;
- скопировать архив ./SberSign-L.deb в созданный каталог;
- выполнить команду

```
sudo dpkg -i ./SberSign-L.deb
```

3 Удаление SberSign-L

- Для того чтобы удалить SberSign-L, следует выполнить команду

```
sudo dpkg -r sbersign
```

4 Описание операций

4.1 Начало работы с программным продуктом SberSign-L

Для начала работы с программным продуктом SberSign-L следует запустить приложение SberSign, щёлкнув соответствующую иконку.

4.2 Настройка параметров SberSign-L

4.2.1 Выбор файлов для БОК, стоп-листа и справочников сертификатов

Для того чтобы задать имена файлов для баз ключей (БОК), стоп-листа и сертификатов, необходимо выбрать пункт меню **Общие параметры** и перейти на вкладку «Ключевые файлы» (см. Рисунок 1).

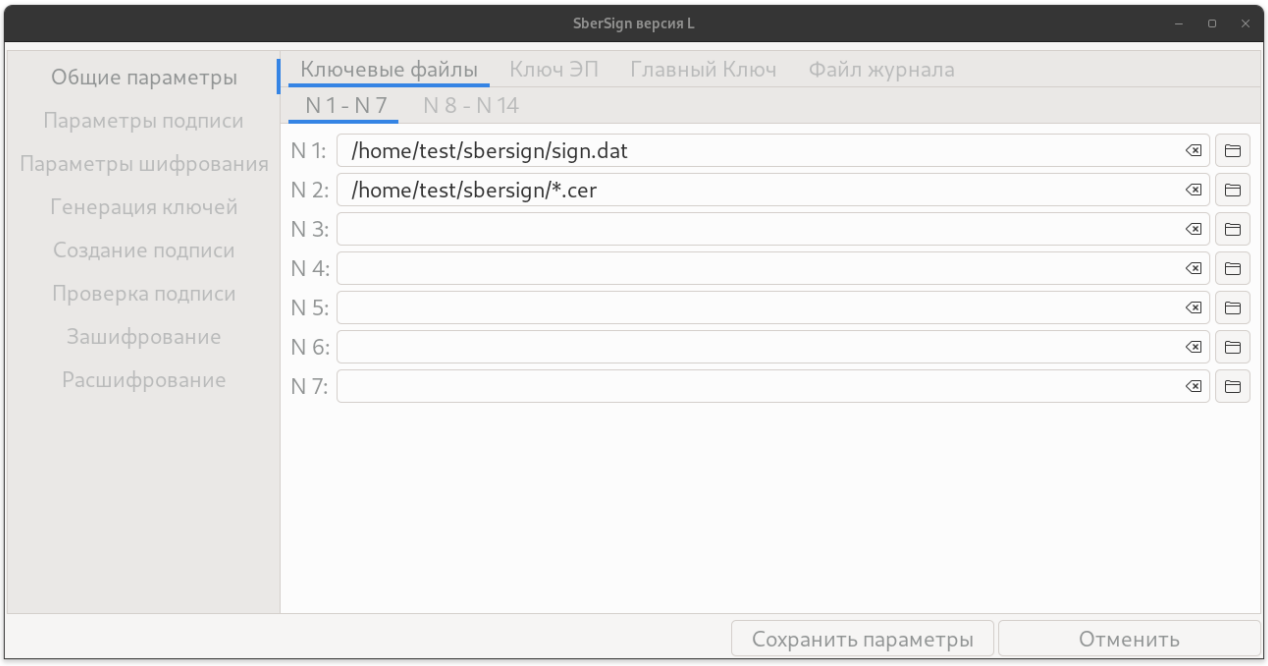

Рисунок 1 – Вкладка «Ключевые файлы»

На этой вкладке можно указать до четырнадцати БОК, стоп-листов или справочников сертификатов. Первые семь строк для имён файлов находятся на вкладке «N 1-7», а вторые семь строк – на вкладке «N 8-14».

Для того чтобы указать расположение нового файла БОК, стоп-листа или справочника сертификатов, следует нажать кнопку  справа от незаполненной строки, затем в открывшемся окне выбрать нужный файл и нажать кнопку **Открыть**.

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить параметры**. Для отказа от произведённых изменений необходимо нажать кнопку **Отменить**.

4.2.2 Выбор места хранения и формата ключа ЭП

Предусмотрено два варианта размещения ключа ЭП:

– на файловой системе по указанному расположению;

– на носителе Touch Memory (TM).

Для того чтобы указать в качестве места хранения ключа ЭП файловую систему, необходимо выбрать пункт меню **Общие параметры** и перейти на вкладку «Ключ ЭП» (см. Рисунок 2) и выбрать вариант «В файле».

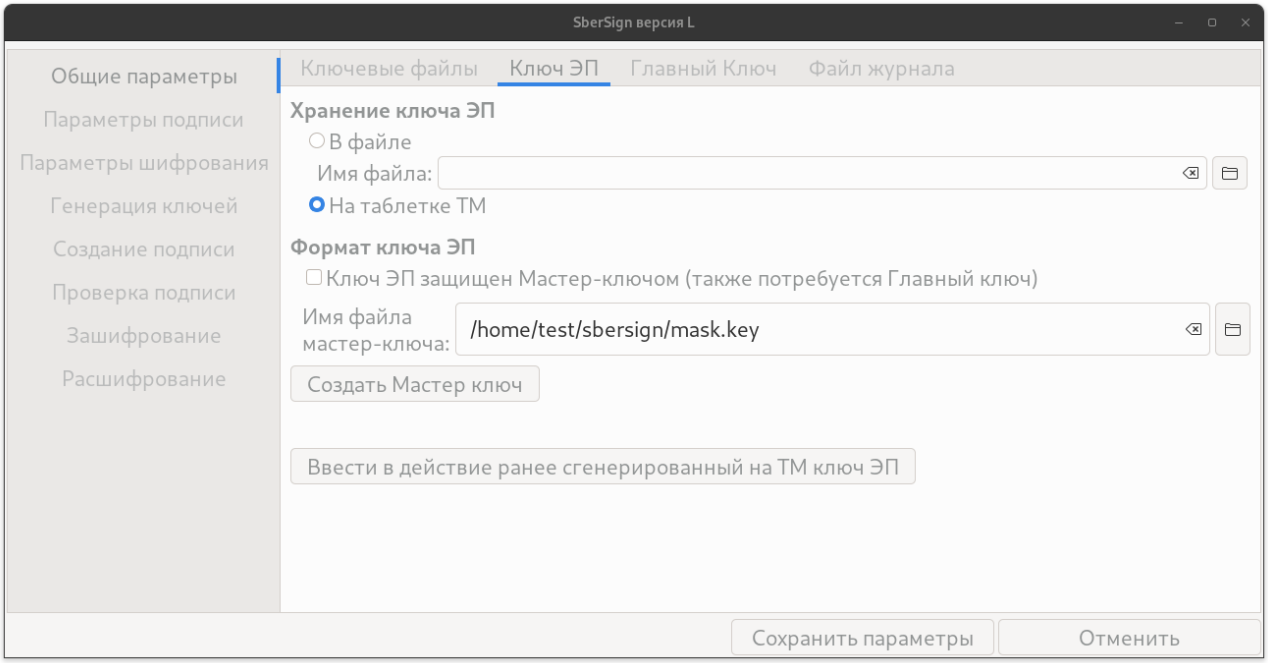

Рисунок 2 – Выбор места хранения и формата ключа ЭП

Справа от поля «Имя файла», следует нажать кнопку , в открывшемся окне выбрать файл, содержащий ключ ЭП, и нажать кнопку **Открыть**.

Для того чтобы указать в качестве места хранения ключа ЭП указать устройство Touch Memory, следует на вкладке «Ключ ЭП» выбрать вариант «На таблетке ТМ».

В SberSign-L предусмотрена возможность создания ключевой пары как с однокомпонентным ключом ЭП, так и с двухкомпонентным. Однокомпонентный ключ ЭП создаётся для личного использования, а двухкомпонентный – для использования в автоматизированных системах.

Для того чтобы создавать двухкомпонентные ключи, необходимо установить флажок «Ключ ЭП защищён Мастер-ключом (также потребуется Главный ключ)». Необходимо также указать места хранения мастер-ключа или создать новый мастер-ключ.

Для того чтобы указать место хранения мастер-ключа, следует нажать кнопку справа от поля «Имя файла мастер-ключа» в открывшемся окне выбрать файл, содержащий ключ ЭП, и нажать кнопку **Открыть**.

Для того чтобы создать новый мастер-ключ, необходимо нажать кнопку **Создать Мастер ключ**. При успешном завершении процесса создания мастер-ключа в Терминале появится сообщение «Мастер-ключ сгенерирован успешно!».

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить параметры**. Для отказа от произведённых изменений необходимо нажать кнопку **Отменить**.

4.2.3 Выбор места хранения главного ключа и узла замены

Предусмотрено два варианта поиска главного ключа и узла замены:

– на файловой системе по указанному расположению;
– на носителе Touch Memory (TM).

Для того чтобы указать в качестве места хранения главного ключа и узла замены файловую систему, необходимо выбрать пункт меню **Общие параметры** и перейти на вкладку «Главный ключ» (см. Рисунок 3) и выбрать вариант «В файле».

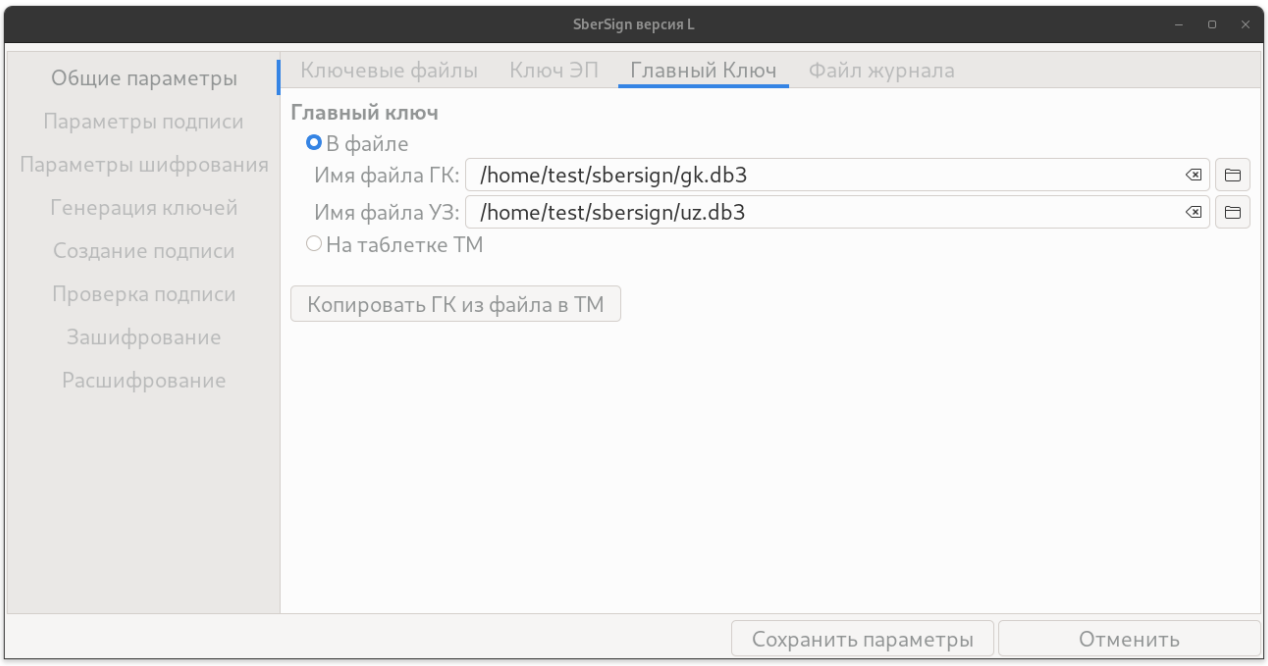

Рисунок 3 – Выбор места хранения главного ключа и узла замены

Для того чтобы указать файл главного ключа, следует справа от поля «Имя файла ГК» нажать кнопку  , в открывшемся окне выбрать нужный файл и нажать кнопку **Открыть**.

Для того чтобы указать файл узла замены, следует справа от поля «Имя файла ГК» нажать кнопку  , в открывшемся окне выбрать нужный файл и нажать кнопку **Открыть**.

Для того чтобы указать в качестве места хранения главного ключа и узла замены устройство Touch Memory, следует на вкладке «Главный ключ» выбрать вариант «На таблетке ТМ».

Если в качестве места хранения главного ключа и узла замены выбран вариант «В файле» и указаны файлы главного ключа и узла замены, имеется возможность скопировать главный ключ и узел замены на ТМ. Для этого необходимо нажать кнопку **Копировать ГК из файла в ТМ** и после появления в Терминале соответствующего предложения приложить ТМ к устройству считывания.

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить параметры**. Для отказа от произведённых изменений необходимо нажать кнопку **Отменить**.

4.2.4 Ведение журнала

В процессе работы SberSign-L может фиксировать в текстовом журнале события, связанные с формированием и проверкой ЭП.

Для того чтобы включить режим ведения журнала, необходимо выбрать пункт меню **Общие параметры** и на вкладке «Файл журнала» (см. Рисунок 4) установить флажок «Вести файл журнала». Для того чтобы выключить режим ведения журнала, необходимо снять флажок «Вести файл журнала».

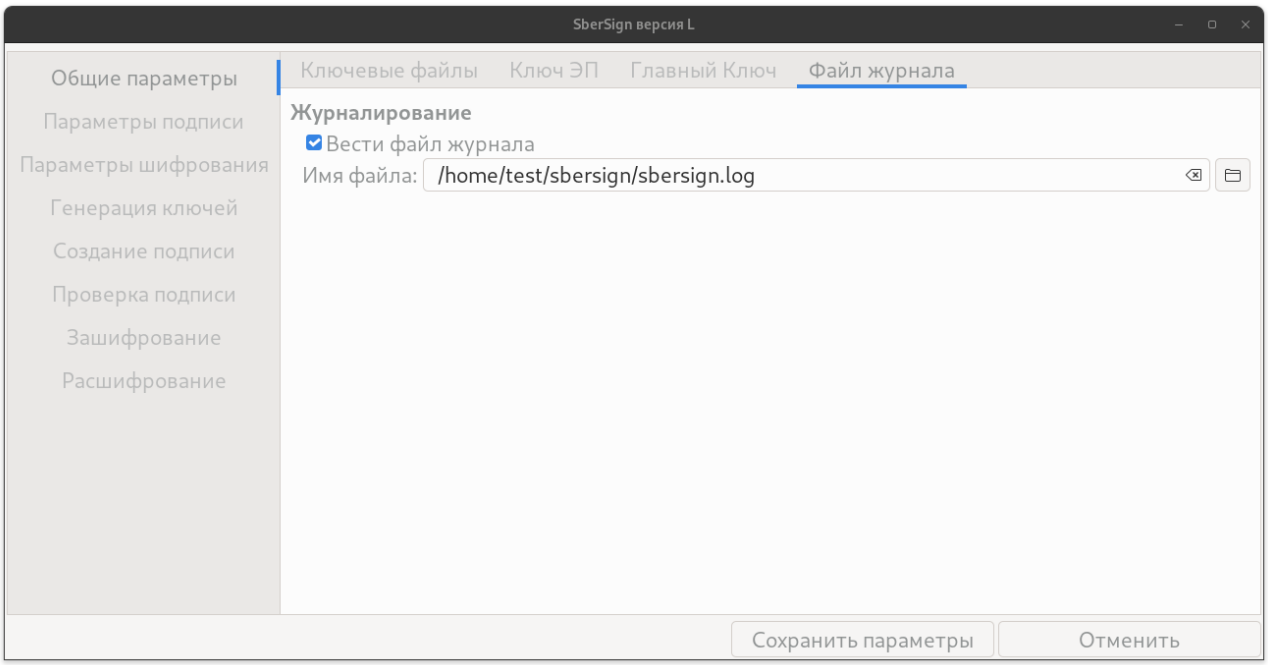

Рисунок 4 – Ведение журнала

Для того чтобы изменить расположение или имя файла журнала, следует нажать кнопку  , затем в открывшемся окне выбрать файл и нажать кнопку **Открыть**.

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить параметры**. Для отказа от произведённых изменений необходимо нажать кнопку **Отменить**.

4.3 Генерация ключей ЭП

4.3.1 Настройка параметров генерации ключей ЭП

Для того чтобы изменить значения параметров генерации ключей ЭП, необходимо выбрать пункт меню **Генерация ключей** (см. Рисунок 5).

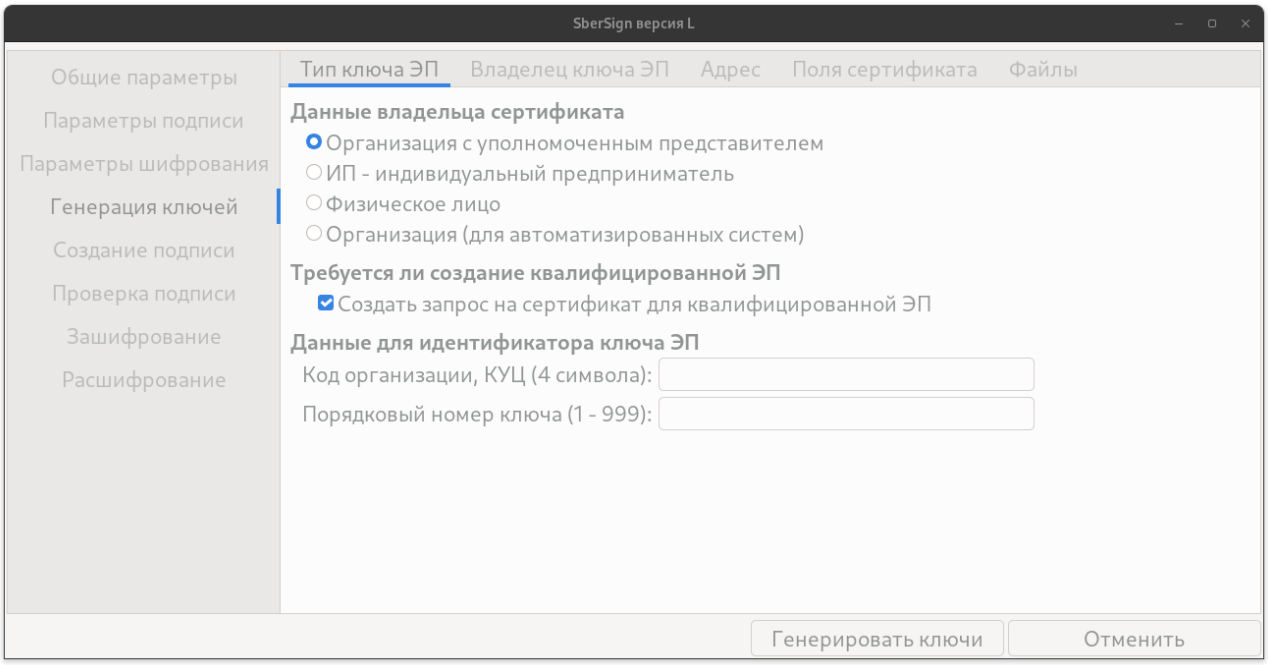

Рисунок 5 – Настройка параметров генерации ключей ЭП

На вкладке «Тип ключа ЭП» в секции «Данные владельца сертификата» следует выбрать тип владельца сертификата для создаваемого ключа ЭП.

Если требуется создать запрос на квалифицированный сертификат, необходимо установить флажок «Создать запрос на сертификат для квалифицированной ЭП», если требуется создать запрос на неквалифицированный сертификат, необходимо этот флажок снять.

В поле «Код организации, КУЦ (4 символа)» необходимо ввести уникальный четырехразрядный буквенно-цифровой код организации - клиента Сбербанка России, присваиваемый автоматизированной системой корневого Удостоверяющего центра ОАО «Сбербанк России». В поле «Порядковый номер ключа» необходимо ввести четырехразрядный порядковый номер ключа ЭП для данного владельца, который не должен использоваться повторно даже в случае перегенерации ключа.

Затем на вкладке «Владелец ключа ЭП» (см. Рисунок 6) необходимо заполнить данными владельца ключа поля: «Фамилия», «Имя», «Отчество», «Организация». Заполнение поля «Должность» не является обязательным.

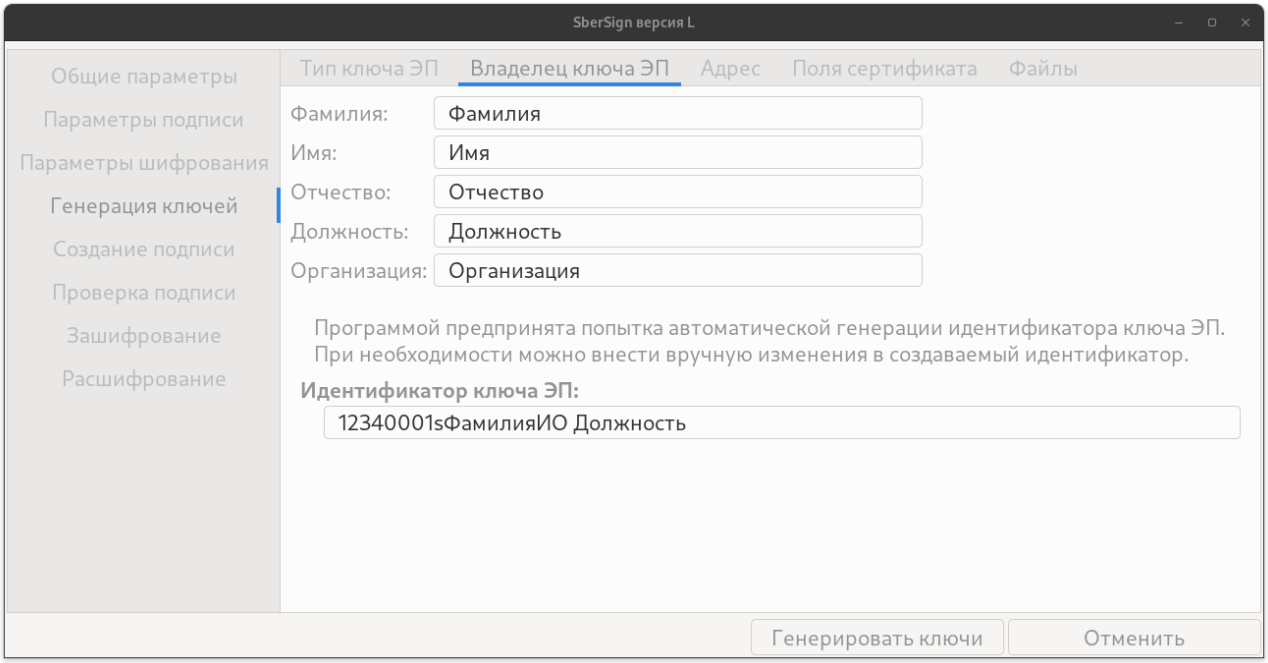

Рисунок 6 – Вкладка «Владелец ключа ЭП»

На основании введённых данных автоматически формируется идентификатор ключа ЭП. При необходимости этот идентификатор может быть изменён.

Идентификатор ключа ЭП не может состоять более чем из 32 символов (включая пробелы) и должен соответствовать формату: **YYYYNNNNsФамилияИО Должность**, где **YYYY** – КУЦ (уникальный четырехразрядный буквенно-цифровой код организации - клиента Сбербанка России, присваиваемый автоматизированной системой корневого Удостоверяющего центра ПАО Сбербанк); **NNNN** – уникальный для каждого Участника системы ЭДО четырехразрядный порядковый номер ключа ЭП, который не должен использоваться повторно даже в случае перегенерации ключа; **s** – признак принадлежности ключа ЭП организации, являющейся клиентом Сбербанка.

Далее на вкладке «Адрес» (см. Рисунок 7) необходимо заполнить данными владельца ключа поля: «Страна», «Регион», «Населённый пункт» и «Адрес». Заполнение полей «Почтовый индекс» не является обязательным.

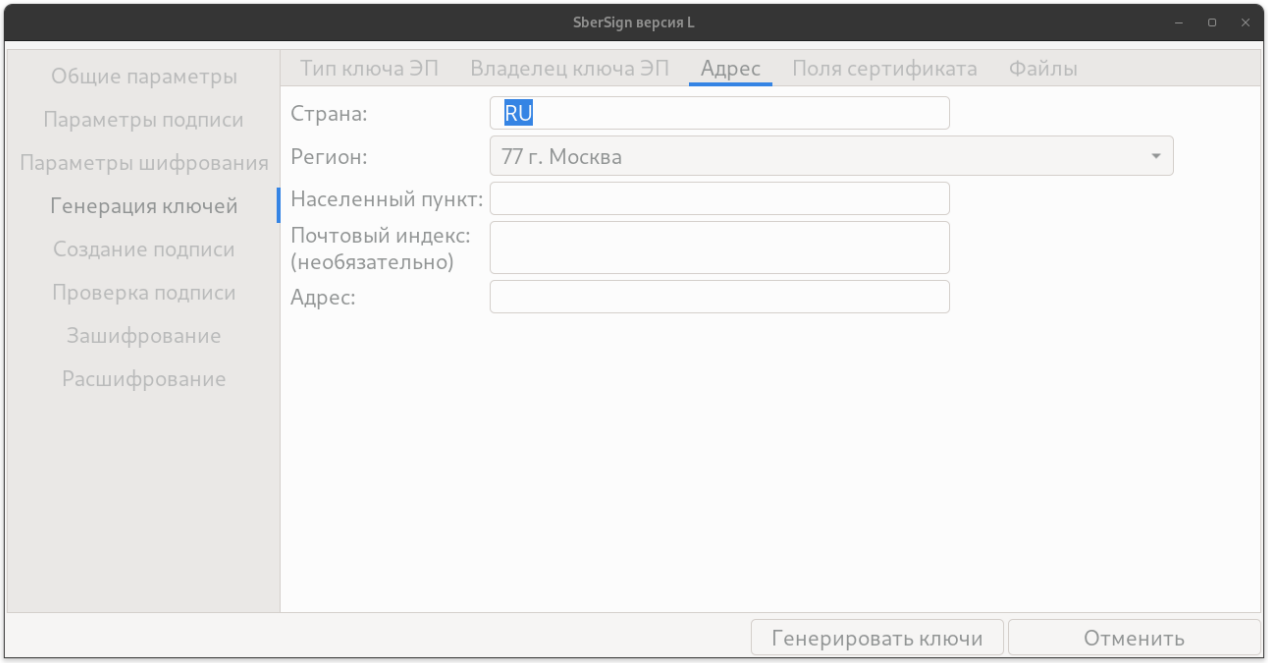

Рисунок 7 – Вкладка «Адрес»

Далее на вкладке «Поля сертификата» (см. Рисунок 8) необходимо заполнить данными владельца ключа поля: «Подразделение», «ОГРН» и «СНИЛС».

Если в качестве типа владельца сертификата выбрано «Физическое лицо», необходимо также заполнить поле «ИНН ФЛ». Для других типов владельца сертификата необходимо заполнить поле «ИНН ЮЛ». Заполнение поля ««E-mail» не является обязательным.

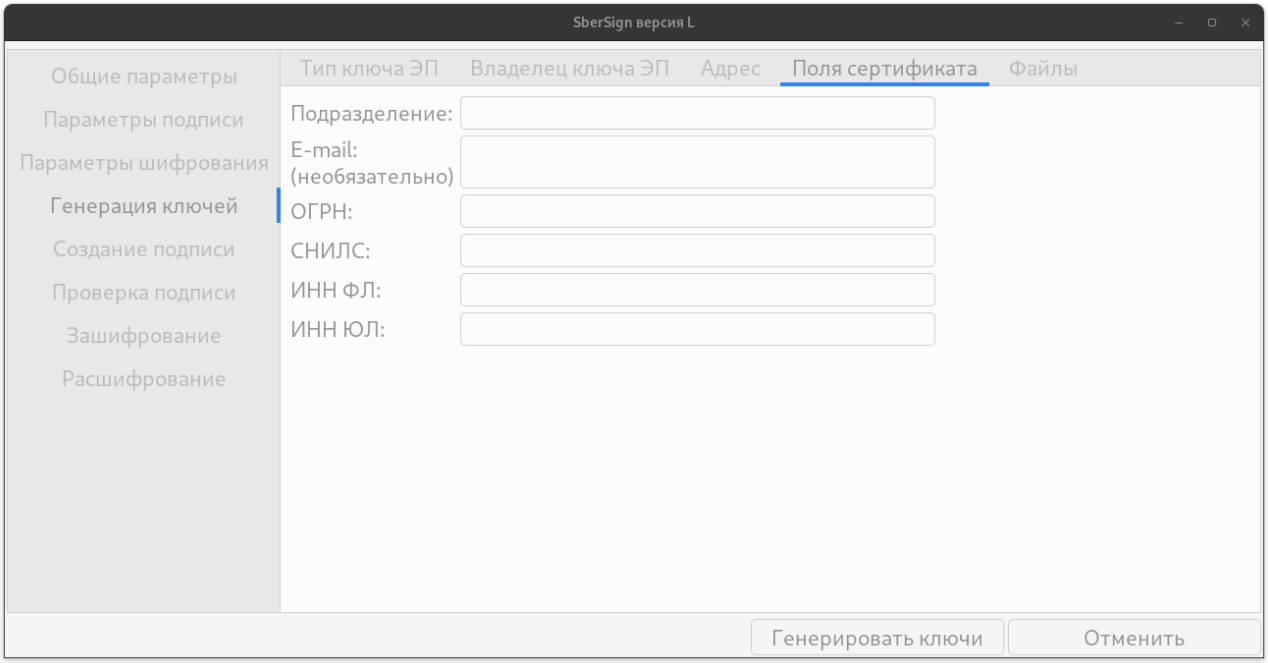

Рисунок 8 – Вкладка «Поля сертификата»

Далее на вкладке «Файлы» (см. Рисунок 9) необходимо выбрать место, куда будут записаны ключ проверки ЭП, запрос на создание сертификата в формате p10 и заявление на изготовление сертификата ключа проверки ЭП в формате rtf.

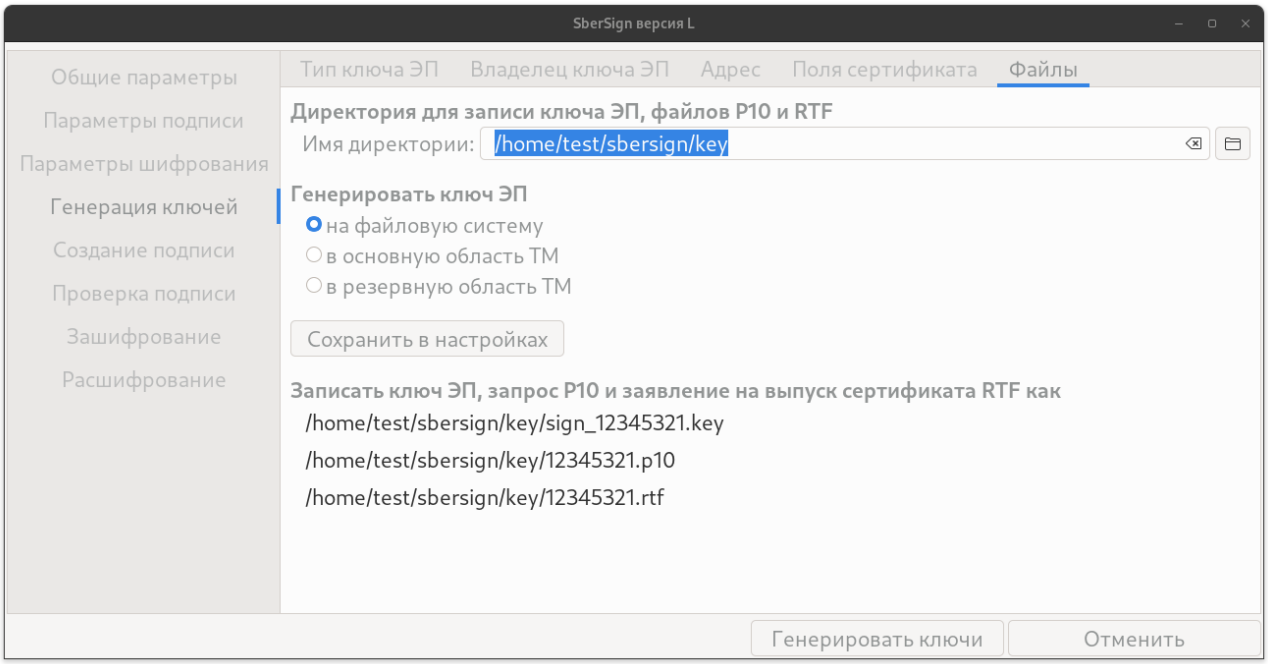

Рисунок 9 – Вкладка «Файлы»

Для этого следует нажать кнопку  , в открывшемся окне выбрать нужную директорию и нажать кнопку **Открыть**.

Для того чтобы указать в качестве места хранения создаваемого ключа ЭП файловую систему, необходимо в секции «Генерировать ключ ЭП» выбрать вариант «на файловую систему».

Для того чтобы указать в качестве места хранения создаваемого ключа ЭП устройство ТМ, необходимо в секции «Генерировать ключ ЭП» выбрать один из вариантов «в основную область ТМ» или «в резервную область ТМ» в зависимости от того, в какую область ТМ следует записать создаваемый ключ.

4.3.2 Генерация ключевой пары

Для того чтобы создать новую ключевую пару и запрос на сертификат ключа проверки электронной подписи, необходимо настроить параметры генерации ключей ЭП (см. подраздел 4.3.1) и нажать кнопку **Генерировать ключи**.

В открывшемся окне (см. Рисунок 10) следует проверить правильность сформированного идентификатора ключа ЭП и нажать кнопку **Да** для подтверждения создания ключевой пары или кнопку **Нет** для отказа от создания ключевой пары с данным идентификатором.

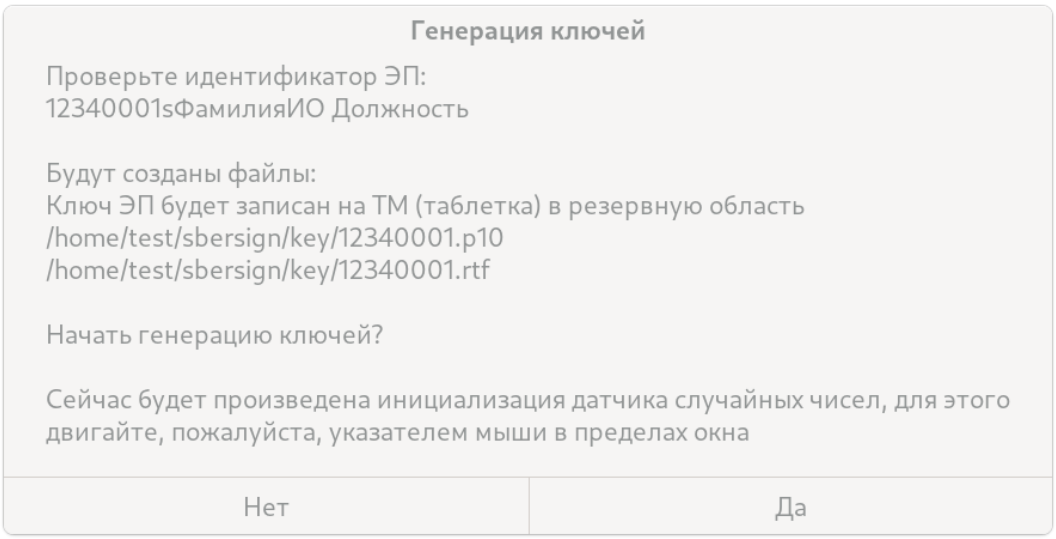

Рисунок 10 – Подтверждение создания ключевой пары

В открывшемся окне инициализации ПДСЧ (см. Рисунок 11) необходимо перемещать указатель мыши в пределах этого окна, многократно меняя направление движения по горизонтальной оси. Когда необходимое количество данных будет получено, окно закроется. Для отмены процесса инициализации ПДСЧ следует нажать кнопку **Отмена**.

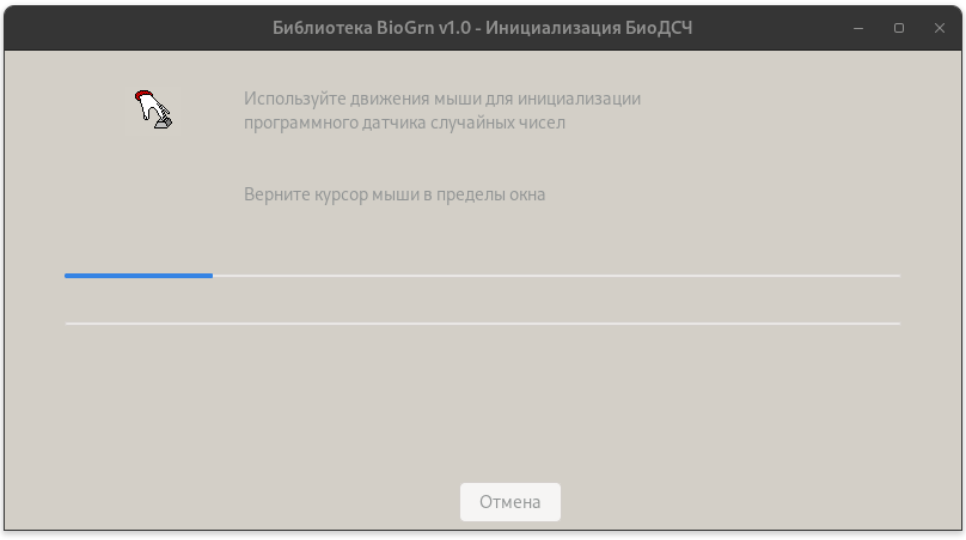

Рисунок 11 – Окно инициализации ПДСЧ

Если в качестве места хранения однокомпонентного ключа ЭП была выбрана файловая система (см. подраздел 4.3.1), по завершении процесса формирования ключа ЭП в Терминале будет предложен пароль для доступа к созданному ключу, состоящий из шести символов и включающий буквы английского алфавита и цифры.

Если пароль не устраивает, следует нажать клавишу Esc. Можно нажимать клавишу Esc несколько раз до тех пор, пока не появится приемлемая комбинация.

Выбранный пароль необходимо запомнить (сохранить в надёжном месте). Для подтверждения выбранного пароля его необходимо ввести в Терминале.

Если в качестве места хранения ключа ЭП было выбрано устройство ТМ, после появления в Терминале соответствующего предложения необходимо приложить ТМ к устройству считывания.

При успешном завершении процесса создания ключевой пары в Терминале появится сообщение «Ключи ЭП созданы!».

4.4 Создание ЭП

4.4.1 Настройка параметров создания ЭП

Для того чтобы изменить параметры ключа ЭП, необходимо выбрать пункт меню **Параметры подписи**.

4.4.1.1 Выбор формата ЭП

Для выбора формата ЭП необходимо перейти на вкладку «Формат подписи» (см. Рисунок 12).

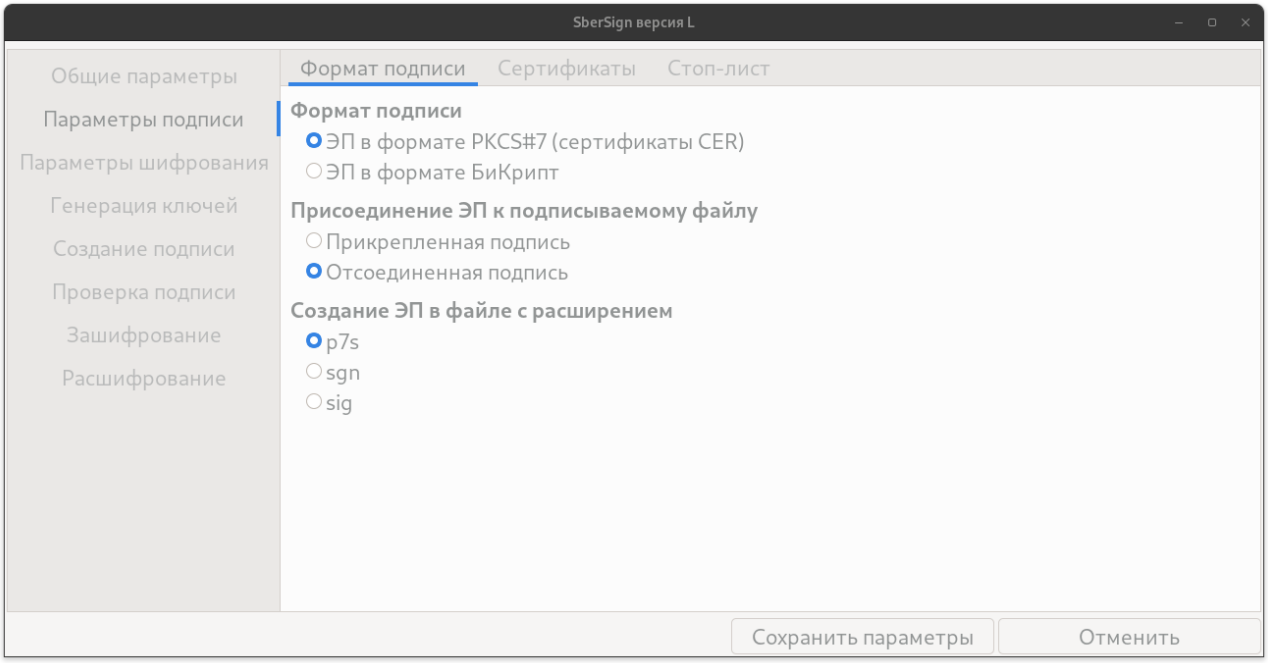

Рисунок 12 – Выбор формата ЭП

В SberSign-L предусмотрено два формата электронной подписи: Бикрипт и PKCS#7. Для того чтобы электронная подпись создавалась в формате Бикрипт, необходимо в секции «Формат подписи» выбрать вариант «ЭП в формате БиКрипт».

Для того чтобы электронная подпись создавалась в формате PKCS#7, необходимо в секции «Формат подписи» выбрать вариант «ЭП в формате PKCS#7 (сертификаты CER)».

По умолчанию электронная подпись в формате PKCS#7 записывается в отдельный файл. Для того чтобы электронная подпись в формате PKCS#7 добавлялась в подписываемый файл (и проверялась из подписанного файла), в секции «Присоединение ЭП к подписываемому файлу» необходимо выбрать вариант «Прикрепленная подпись». При этом необходимо учитывать, что при таких настройках размер подписываемого файла не должен превышать 300 Мбайт.

По умолчанию электронная подпись в формате PKCS#7 записывается в отдельный файл с расширением p7s. Для того чтобы ЭП записывалась в файл с другим расширением (sgn или sig), необходимо выбрать его в секции «Создание ЭП в файле с расширением».

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить параметры**. Для отказа от произведённых изменений необходимо нажать кнопку **Отменить**.

4.4.1.2 Выбор присоединяемой к ЭП цепочки сертификатов

В SberSign-L предусмотрена возможность присоединения сертификата ключа ЭП к подписи файла в формате PKCS#7. Поддерживаются сертификаты ключей ЭП в формате X.509.

Для того чтобы присоединять сертификат к подписи файла, необходимо выбрать пункт меню **Параметры подписи** и перейти на вкладку «Сертификаты» (см. Рисунок 13).

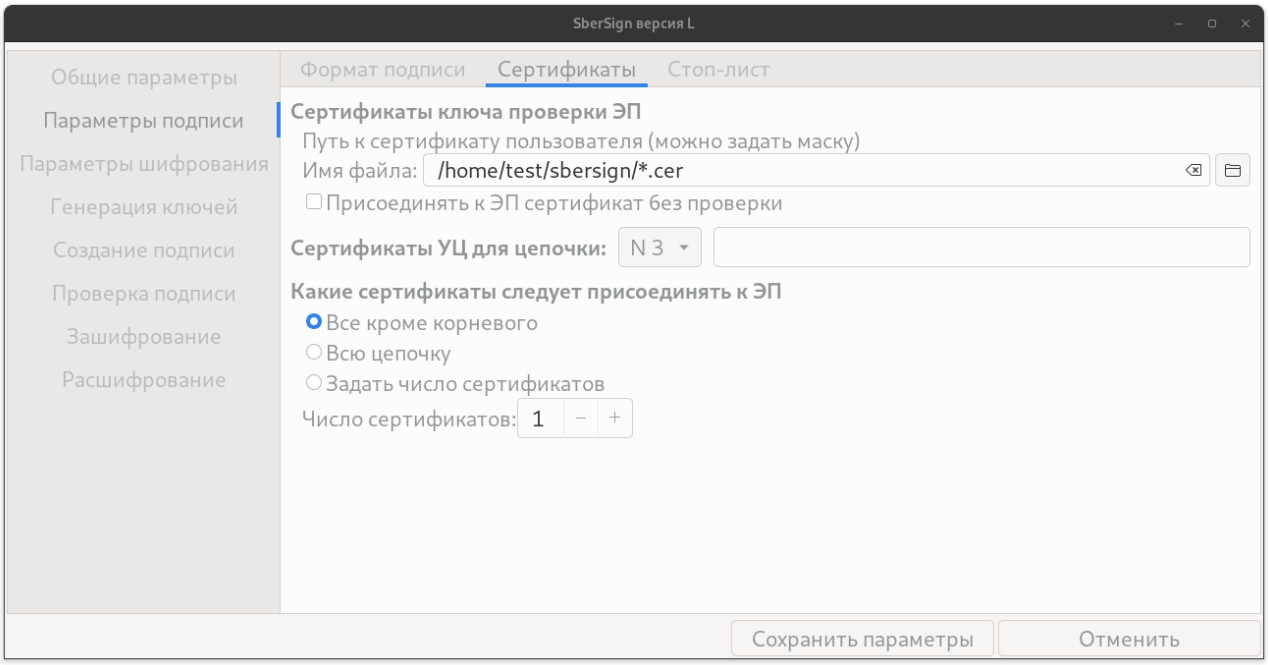

Рисунок 13 – Выбор цепочки сертификатов

Для того чтобы присоединять сертификат к подписи файла, необходимо секции «Сертификаты ключа проверки ЭП» в поле «Путь к сертификату пользователя (можно задать маску)» указать расположение файла сертификата. Для этого следует нажать кнопку  справа от поля «Имя файла», в открывшемся окне выбрать файл, содержащий сертификат, и нажать кнопку **Открыть**.

Для того чтобы для выбранного сертификата при присоединении к подписи файла не производилась проверка цепочки сертификатов, необходимо установить флажок «Присоединять к ЭП сертификат без проверки».

Для того чтобы присоединять к подписи файла цепочку сертификатов, необходимо указать расположение файлов сертификатов, входящих в цепочку. Для этого следует щёлкнуть стрелку в правой части поля «Сертификаты УЦ для цепочки» и выбрать из выпадающего списка номер нужной директории сертификатов на вкладке «Ключевая информация» (см. подраздел 4.2.1).

По умолчанию к подписи файла в формате PKCS#7 присоединяется вся цепочка сертификатов кроме корневого.

Для того чтобы присоединять к подписи файла всю цепочку сертификатов, включая корневой сертификат, необходимо в секции «Какие сертификаты следует присоединять к ЭП» выбрать вариант «Всю цепочку».

Для того чтобы присоединять к подписи файла цепочку сертификатов определённой длины, необходимо выбрать вариант «Задать число сертификатов» и в поле «Число сертификатов» указать длину цепочки сертификатов.

Для того чтобы не присоединять сертификаты к подписи файла, необходимо выбрать вариант «Задать число сертификатов» и в поле справа задать значение 0.

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить параметры**. Для отказа от произведённых изменений необходимо нажать кнопку **Отменить**.

4.4.1.3 Ввод в действие ключа ЭП

Если при генерации ключей ЭП в качестве места для записи ключа ЭП был выбран вариант «в резервную область ТМ», то для использования этого ключа ЭП его необходимо ввести в действие.

Для того чтобы ввести в действие ранее созданный ключ ЭП, следует выбрать пункт меню **Общие параметры** и на вкладке «Ключ ЭП» (см. Рисунок 2) нажать кнопу «Ввести в действие ранее сгенерированный на ТМ ключ ЭП».

После появления в Терминале соответствующего предложения необходимо приложить ТМ к устройству считывания. При успешном завершении процесса ввода ключа в действие в Терминале появится сообщение «Ключ ЭП с идентификатором YYYYNNNNsФамилияИО Должность успешно введен в действие».

4.4.1.4 Выбор списка отозванных сертификатов для ЭП в формате PKCS#7

Для выбора списка отозванных сертификатов (стоп-листа) для ЭП в формате PKCS#7 необходимо выбрать пункт меню **Параметры подписи** и перейти на вкладку «Стоп-лист» (см. Рисунок 14).

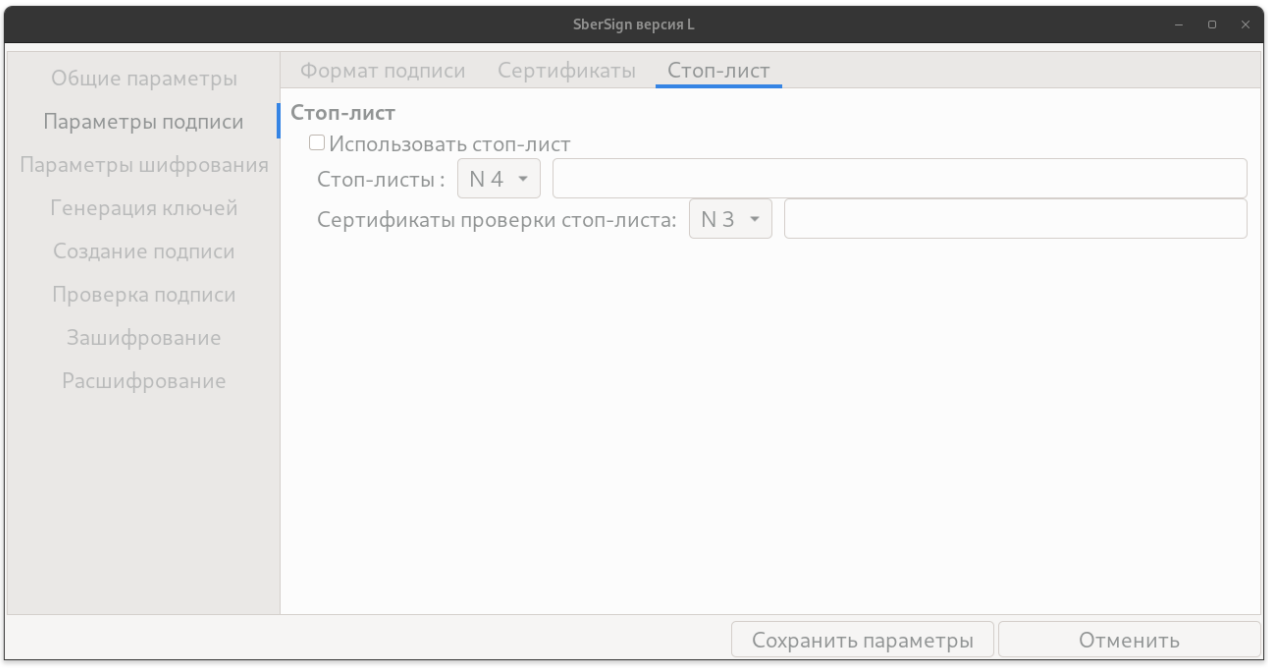

Рисунок 14 – Вкладка «Стоп-лист»

Для того чтобы сертификаты проверялись с помощью списка отозванных сертификатов из файла, необходимо указать этот файл в списке на вкладке «Ключевые файлы» (см. раздел 4.2.1).

Для того чтобы указать файл стоп-листа, необходимо установить флажок «Использовать стоп-лист:» и, щёлкнув стрелку слева от поля «Стоп-листы», выбрать из выпадающего списка номер ячейки соответствующего списка отозванных сертификатов на вкладке «Ключевые файлы».

Далее необходимо указать директорию, где находятся сертификаты, с помощью которых можно проверить электронную подпись под стоп-листом. Для этого следует щёлкнуть стрелку в правой части поля «Сертификаты проверки стоп-листа», выбрать из выпадающего списка номер нужной директории сертификатов на вкладке «Ключевые файлы».

4.4.2 Формирование ЭП файлов

Для того чтобы сформировать ЭП файла, необходимо выбрать пункт меню **Создание подписи** (см. Рисунок 15).

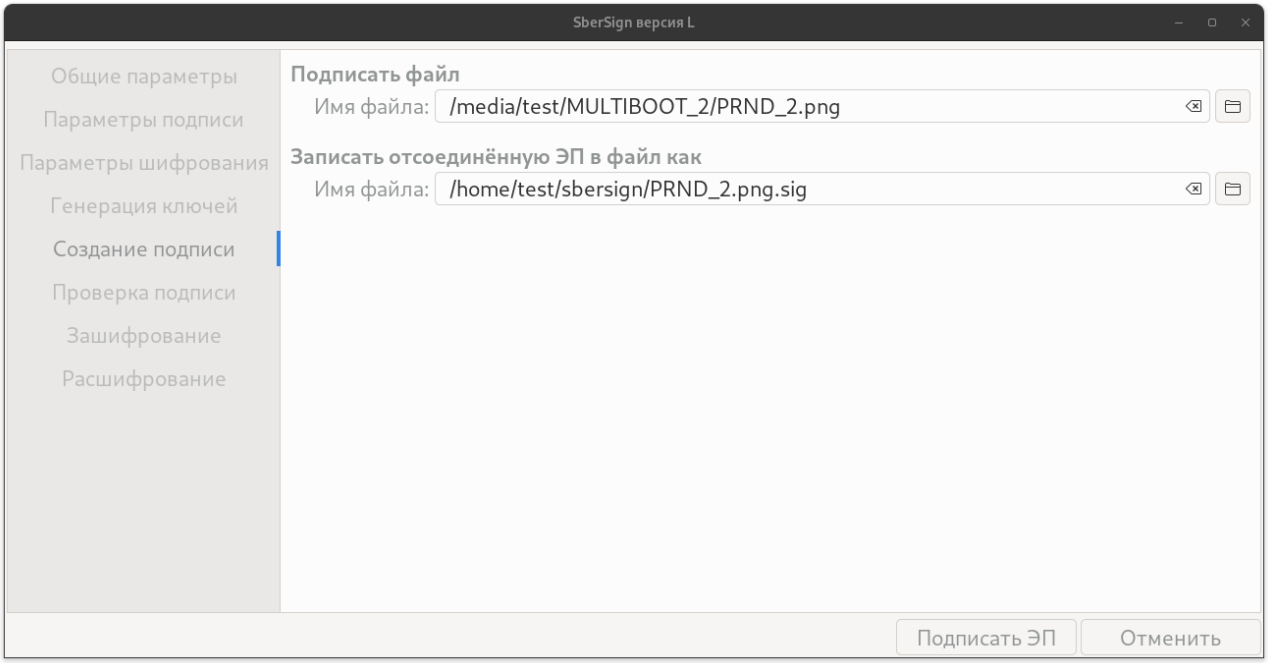

Рисунок 15 – Формирование ЭП

В секции «Подписать файл» следует нажать кнопку  справа от поля «Имя файла», в открывшемся окне выбрать файл, который следует подписать, и нажать кнопку **Открыть**.

Если в параметрах создания ЭП (см. подраздел 4.4.1.1) указано, что подпись должна записываться в отдельный файл, то в секции «Записать откреплённую ЭП в файл как» в поле «Имя файла» появится имя файла, в который будет записана подпись.

Для подписания файла необходимо нажать кнопку **Подписать ЭП**. Для отказа от подписания следует нажать кнопку **Отменить**.

После появления в Терминале соответствующего предложения необходимо приложить ТМ к устройству считывания. При успешном завершении процесса создания ЭП в Терминале появится сообщение «Ключи ЭП созданы!».

4.5 Проверка ЭП

4.5.1 Настройка параметров проверки ЭП

Параметры проверки ЭП совпадают с параметрами создания ЭП (см. подраздел 4.4.1).

4.5.2 Проверка подписи

Для того чтобы проверить ЭП, необходимо выбрать пункт меню **Проверка подписи** (см. Рисунок 16).

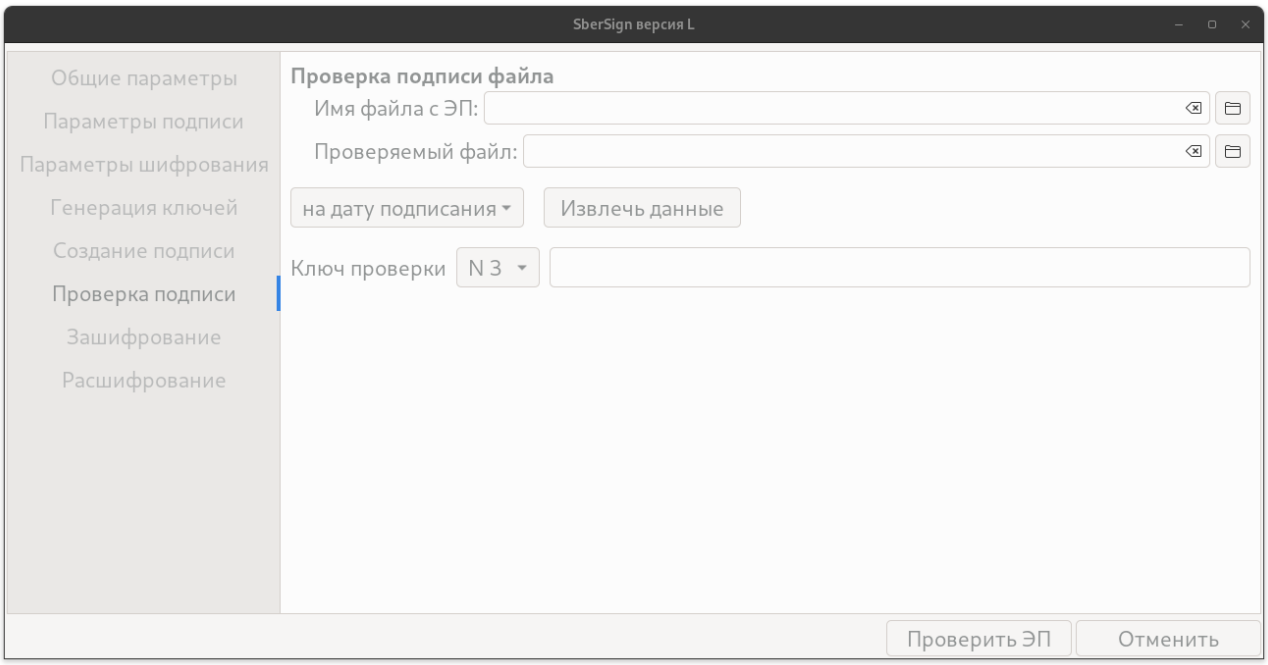

Рисунок 16 – Настройка параметров проверки ЭП

В секции «Проверка подписи файла» следует нажать кнопку  справа от поля «Имя файла с ЭП», в открывшемся окне выбрать файл, в котором находится проверяемая подпись, и нажать кнопку **Открыть**.

Если подпись находится в отдельном файле, необходимо нажать кнопку  справа от поля «Проверяемый файл» и выбрать файл, который подписан выбранной подписью.

Для выбора ключа проверки ЭП необходимо щёлкнуть стрелку слева от поля «Ключ проверки» и выбрать из выпадающего списка номер ячейки соответствующего ключа на вкладке «Ключевые файлы» (см. Рисунок 1).

Если ЭП сформирована в формате PKCS#7 (см. подраздел 4.4.1.1), то её можно проверить как на текущую дату, так и на дату подписания. Выбрать нужный вариант можно нажав стрелку ниже поля «Проверяемый файл».

Если ЭП присоединена к подписываемому файлу, для восстановления первоначального вида файла без подписи необходимо нажать кнопку **Извлечь данные**.

Для проверки выбранной подписи файла необходимо нажать кнопку **Проверить ЭП**. Для отказа от проверки следует нажать кнопку **Отменить**.

4.6 Зашифрование и расшифрование файлов

4.6.1 Выбор режима шифрования

В SberSign-L предусмотрено два режима шифрования файлов: шифрование с помощью сертификатов X.509 и шифрование с помощью сетевых ключей. Для того чтобы установить режим шифрования файлов с помощью сертификатов X.509, необходимо выбрать пункт меню **Параметры шифрования** (см. Рисунок 17) и на вкладке «Формат шифрования» выбрать вариант «Шифруем на сертификатах CER». Для того чтобы установить режим шифрования файлов с помощью сетевых ключей, необходимо выбрать вариант «Шифруем на сетевых ключах NKL».

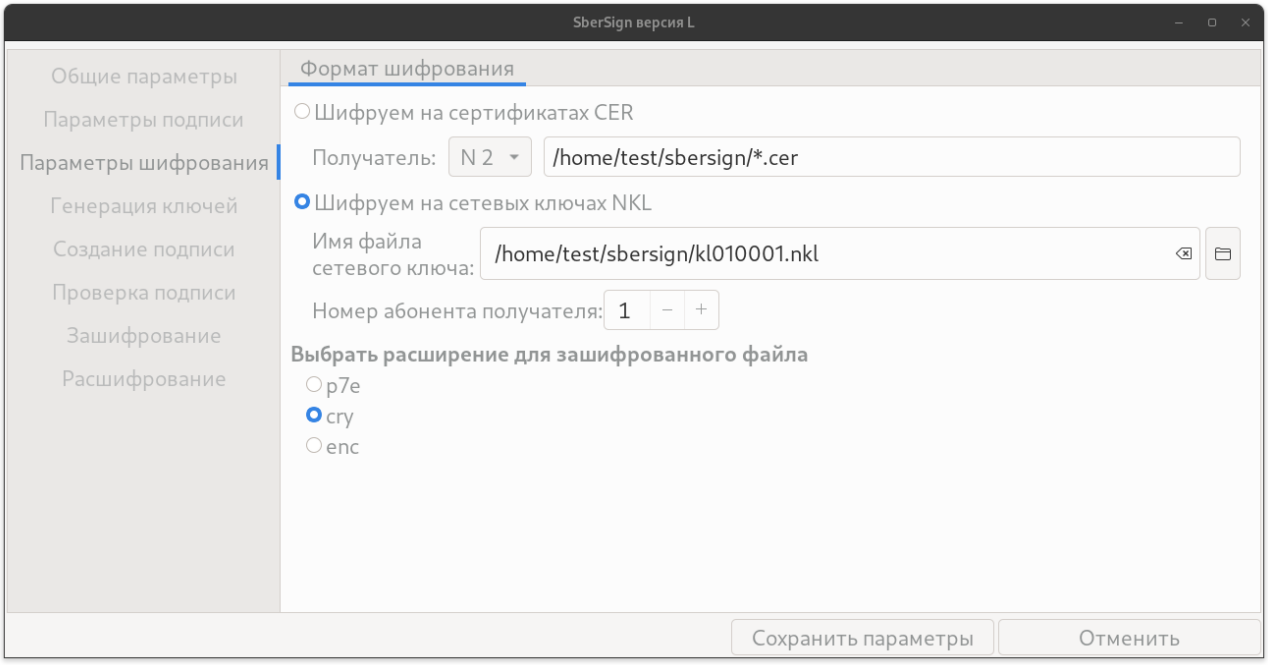

Рисунок 17 – Настройка параметров шифрования

Если выбран режим шифрования с помощью сетевых ключей, необходимо нажать кнопку  справа от поля «Имя файла сетевого ключа», в открывшемся окне выбрать файл, в котором находится сетевой ключ, и нажать кнопку **Открыть**.

Для того чтобы указать абонента, в адрес которого будут зашифровываться все файлы, необходимо в поле «Номер абонента получателя» (см. Рисунок 17) с помощью знаков «+» и «-» указать номер нужного абонента. Если зашифрование будет

производиться в адрес центра, то в качестве номера абонента получателя следует указать 1.

В секции «Выбрать расширение для зашифрованного файла» можно выбрать вариант p7e, cry или enc. При расшифровании файла в расшифрованной копии данное расширение будет удалено.

Для подтверждения произведённых изменений необходимо нажать кнопку **Сохранить параметры**. Для отказа от произведённых изменений необходимо нажать кнопку **Отменить**.

4.6.2 Зашифрование файлов

Предварительно необходимо настроить параметры шифрования (см. подраздел 4.6.1).

Для того чтобы зашифровать файл, необходимо в меню выбрать пункт **Зашифрование** (см. Рисунок 18).

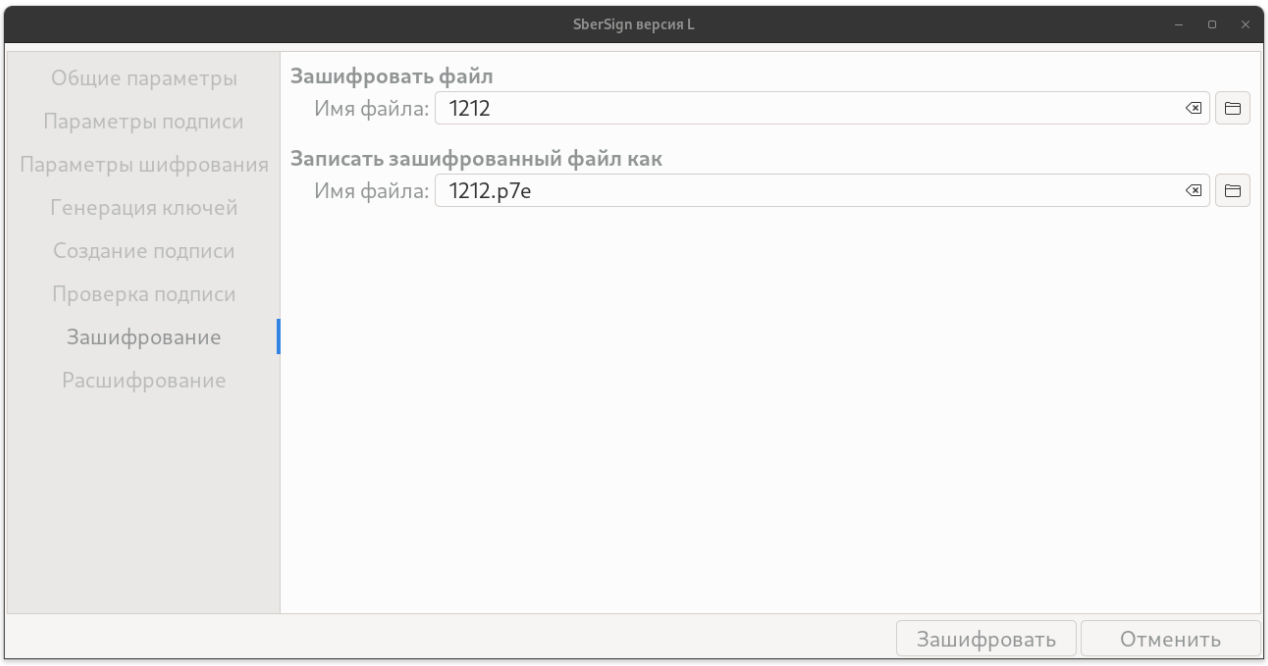

Рисунок 18 – Зашифрование файла

В секции «Зашифровать файл» следует нажать кнопку  справа от поля «Имя файла», в открывшемся окне выбрать файл, который следует зашифровать, и нажать кнопку **Открыть**.

В секции «Записать зашифрованный файл как» при необходимости можно изменить имя и расположение зашифрованного файла.

Для подписания выбранного файла необходимо нажать кнопку **Зашифровать**. Для отказа от подписания следует нажать кнопку **Отменить**.

При успешном завершении процесса шифрования в Терминале появится сообщение «Файл зашифрован».

4.6.3 Расшифрование файлов

Для того чтобы расшифровать файл, необходимо в меню выбрать пункт **Расшифрование** (см. Рисунок 19).

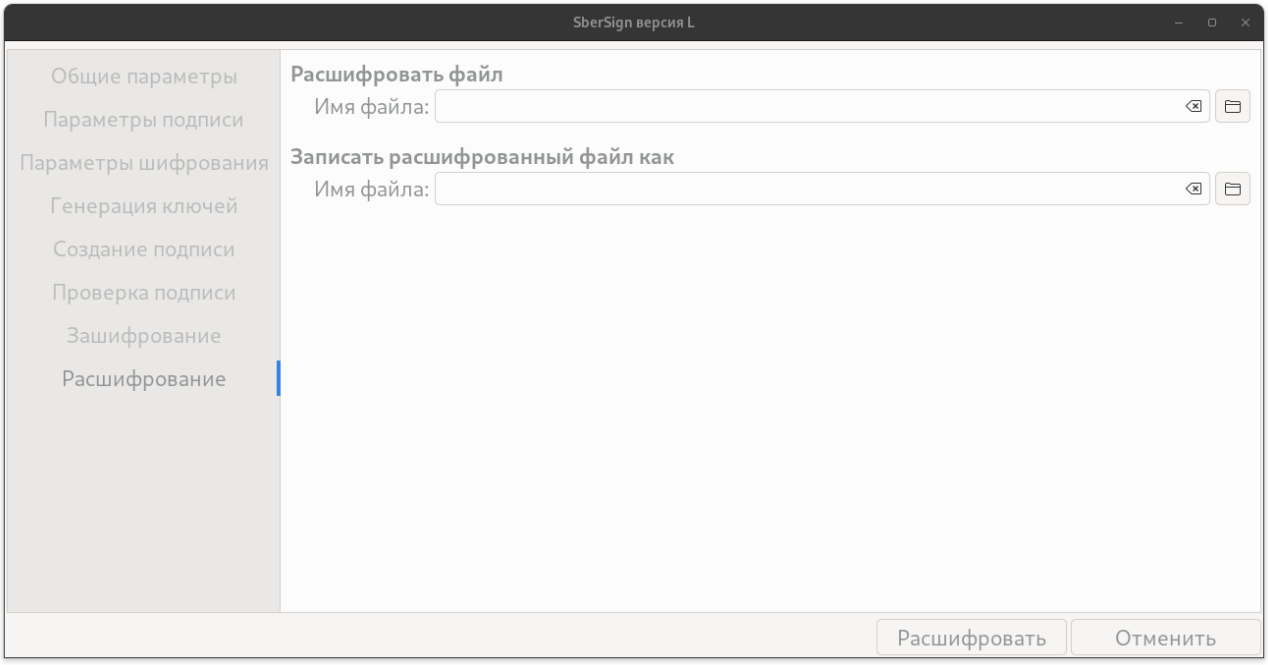

Рисунок 19 – Расшифрование файла

В секции «Расшифровать файл» следует нажать кнопку  справа от поля «Имя файла», в открывшемся окне выбрать файл, который следует расшифровать, и нажать кнопку **Открыть**.

В секции «Записать расшифрованный файл как» при необходимости можно изменить имя и расположение расшифрованного файла.

Для расшифрования выбранного файла необходимо нажать кнопку **Расшифровать**. Для отказа от подписания следует нажать кнопку **Отменить**.