ДАТА СОЗДАНИЯ ДОКУМЕНТА: 8/03/2024

PEM-HEART SIGNATURE РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

CENCERT

ПУБЛИЧНЫЙ ДОКУМЕНТ

СДЕЛАН ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O. 02-230 ВАРШАВА

UL. JUTRZENKI 116 | ТЕЛЕФОН: +48 22 570 57 10 | ФАКС: +48 22 570 57 15

WWW.ENIGMA.COM.PL

ДАТА СОЗДАНИЯ ДОКУМЕНТА: 5/03/2024
ТИП ДОКУМЕНТА: ОБЩЕСТВЕННЫЙ

ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O.
JUTRZENKI 116
02-230 ВАРШАВА
ПОЛЬША

ТЕЛЕФОН: +48 22 570 57 10
ФАКС: +48 22 570 57 15
ВЕБ-САЙТ: WWW.ENIGMA.COM.PL

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

Программное обеспечение PEM-HEART Signature используется для:

- подписывания квалифицированными подписями или электронными печатями на основании сертификатов, выданных Cencert,
- проверки квалифицированных электронных подписей (в том числе подписей на основе сертификатов, выданных в других странах ЕС), в течение срока действия сертификата.

Дополнительно:

- проверка электронной подписи после окончания срока действия сертификата, если подпись находится в архивной форме (см. описание архивной формы в разделе **4.3.1 ПАНЕЛЬ ПРОВЕРКИ**),
- проверка подписей на основании простых (неквалифицированных) сертификатов, выданных Cencert.

PEM-HEART Signature создает электронные подписи в форматах:

- XAdES в соответствии с техническими особенностями ETSI TS 101 903 XML Advanced Electronic Signatures (XadES),
- CAdES CMS в соответствии с техническими особенностями ETSI TS 101 733 Electronic Signature Format (CAdES это аббревиатура от CMS Advanced Electronic Signatures),
- PAdES (стандарт ETSI TS 102 778) - PDF Advanced Electronic Signatures,
- ASiC (стандарт ETSI TS 102 918) - программа создает подпись в виде ASX основной, создавая файл с расширением .asics . (файл содержит базовый контейнер ASiC XadES окружающий).

Эти форматы определяют структуру файла, содержащего подпись. Для выбора конкретного формата требуется программное обеспечение, которое сможет проверить правильность такой подписи.

Производителем решений для Cencert является компания ENIGMA Systemy Ochrony Informacji Sp. z o.o. Основная деятельность ENIGMA — разработка, производство и внедрение инновационных систем защиты информации.

Используя собственные аппаратные и программные решения, обеспечивает лучшую защиту данных в органах государственного и местного самоуправления, финансовых учреждениях и предприятиях. Все продукты ENIGMA обеспечивают полную криптографическую защиту собираемой, обрабатываемой и передаваемой информации. Предлагаемые решения сертифицированы с точки зрения безопасности специализированными подразделениями Службы государственной охраны.

Cencert является зарегистрированным товарным знаком ENIGMA Systemy Ochrony Informacji. Cencert — квалифицированная организация, предоставляющая квалифицированные и неквалифицированные трастовые услуги с 2009 года — в области выдачи сертификатов, квалифицированных меток времени и услуги подтверждения действительности сертификатов (OCSP). Правовой основой предоставления услуг Cencert являются, в частности, eIDAS (Регламент Европейского Парламента и Совета (ЕС) № 910/2014), а также Закон о трастовых услугах и электронной идентификации (Dz. U. 2016 poz. 1579).

2 БЕЗОПАСНОСТЬ ПРОДУКЦИИ

Программу следует использовать на компьютере, находящемся под контролем владельца сертификата. Компьютер должен быть защищен от доступа посторонних лиц, на нем должно быть установлено актуальное антивирусное программное обеспечение и актуальные обновления операционной системы.

Электронные подписи не могут быть созданы на компьютерах, безопасность которых неизвестна (например, компьютеры, доступные для общественности или широкому кругу людей, компьютеры случайных людей и т. д.).

Программу следует использовать в среде, где программный код защищен от изменений операционной системой. Этого можно достичь с помощью операционных систем, предлагающих контроль доступа (Windows, Linux а также MacOSX) или установив права доступа к каталогам с исполняемыми файлами, чтобы пользователь не имел права изменять содержащиеся в них исполняемые файлы.

Программу следует использовать в среде, в которой операционная система защищена от возможности перехвата враждебными системами данных, передаваемых через порты компьютера, а также данных, вводимых с клавиатуры компьютера в окна программы. Этого можно достичь с помощью операционных систем, предлагающих контроль доступа (Windows, Linux а также MacOSX) и обеспечения надлежащего уровня защиты компьютера от авторизованных пользователей (защита путем установления соответствующих прав доступа и постоянного обновления операционной системы), неавторизованных пользователей и атак из компьютерной сети (защита путем постоянного обновления операционной системы и, при необходимости с использованием устройств типа firewall).

Программа, работающая как «защищенное устройство для создания и проверки защищенных электронных подписей», не может использоваться в «публичной среде», то есть в среде, в которой любое физическое лицо может иметь доступ к программному обеспечению при нормальных условиях эксплуатации.

Технический компонент или поставляемые к нему драйверы, которые помимо программы являются частью «защищенного устройства создания и проверки защищенных электронных подписей», имеют функцию уничтожения данных, используемых для создания подписей (т.е. закрытого ключа) при запросе пользователя. Уничтожение осуществляется в такой степени, чтобы предотвратить

реконструкцию этих данных на основе анализа записей в устройствах, в которых они были созданы, сохранены или использованы.

3 УСТАНОВКА

Установочные пакеты доступны через веб-сайт www Cencert:

https://www.cencert.pl/do-pobrania/oprogramowanie-do-podpisu/

3.1 УСТАНОВКА ДЛЯ СИСТЕМЫ WINDOWS

3.1.1 УСТАНОВКА

Установка должна выполняться из-под учетной записи с правами администратора. Перед началом установки рекомендуется закрыть все приложения, кроме тех, которые необходимы для работы операционной системы.

Ниже представлена процедура установки на примере системы Windows 11:

1. Запустите установщик *pemheart-signature.exe*, который отобразит стартовое окно установки.

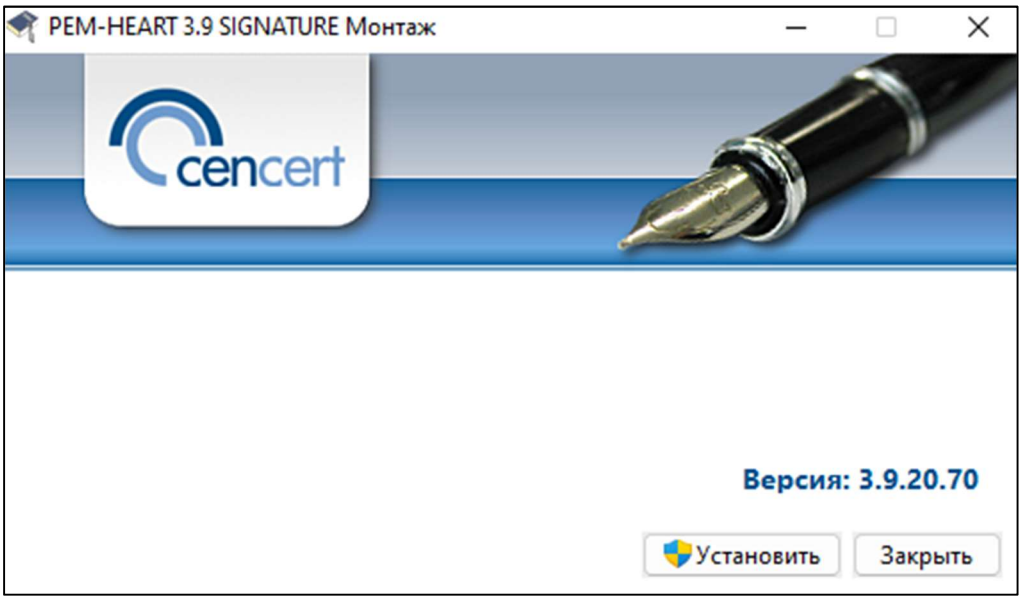


Рис. 1 Стартовое окно мастера установки

2. При нажатии кнопки *Установить* запустится мастер установки продукта *PEM-HEART 3.9 Signature*.

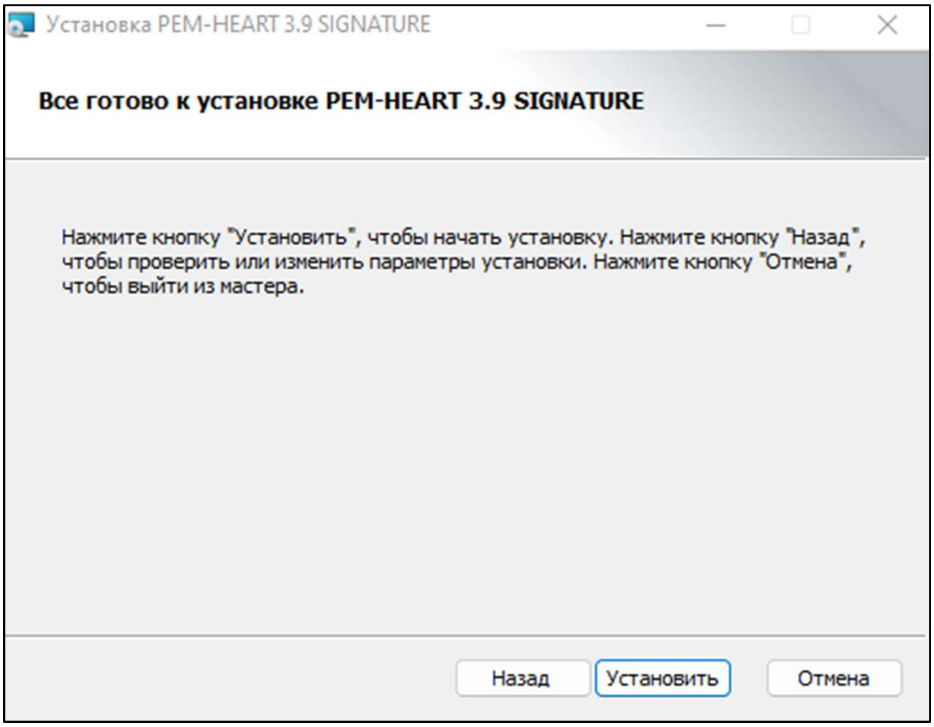


Рис. 2 Окно мастера установки

3. При нажатии кнопки *Установить*, начнется установка программного обеспечения.
4. При нажатии кнопки *Готово* - мастер завершит работу. Это также запустит процесс установки программного обеспечения Thales SafeNet.

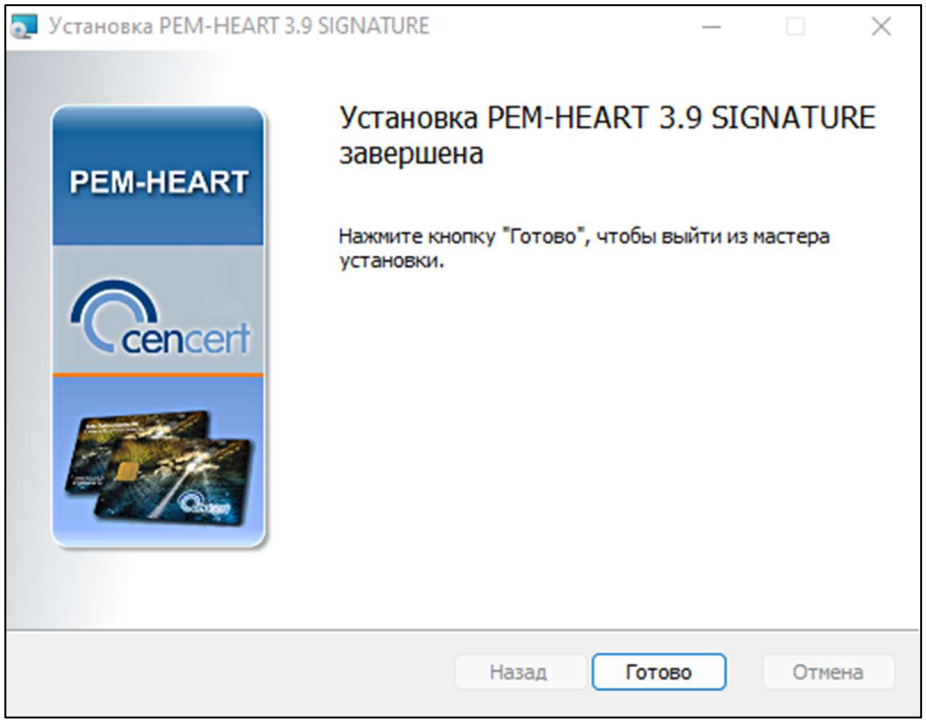


Рис. 3 Окно завершения работы мастера установки

5. Появится мастер установки программного обеспечения Thales SafeNet.

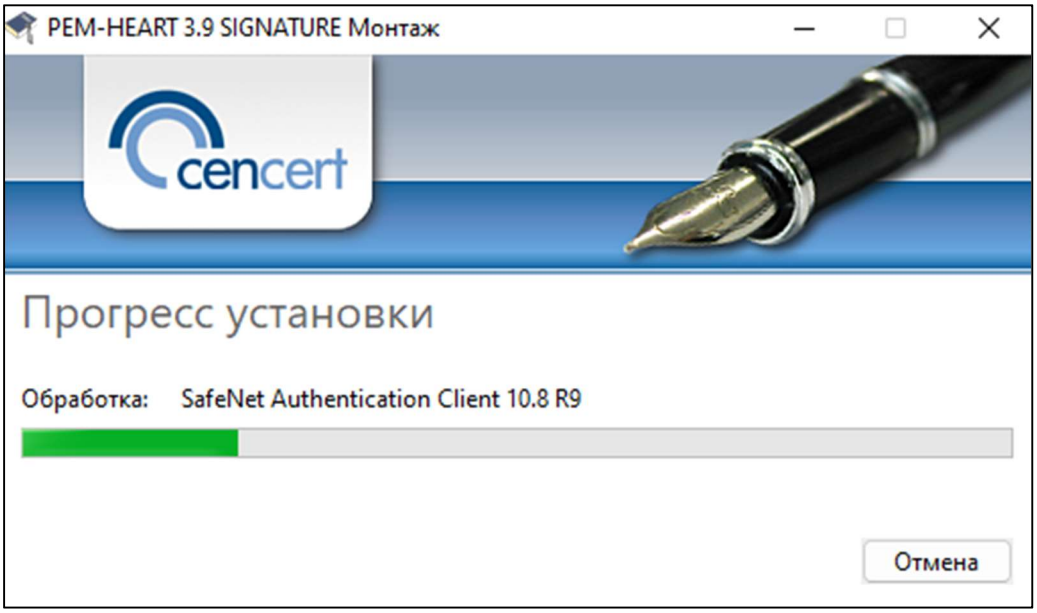


Рис. 4 Установка программы Thales SafeNet

6. Нажмите *Перезагрузить* — это необходимо для начала работы с программой.

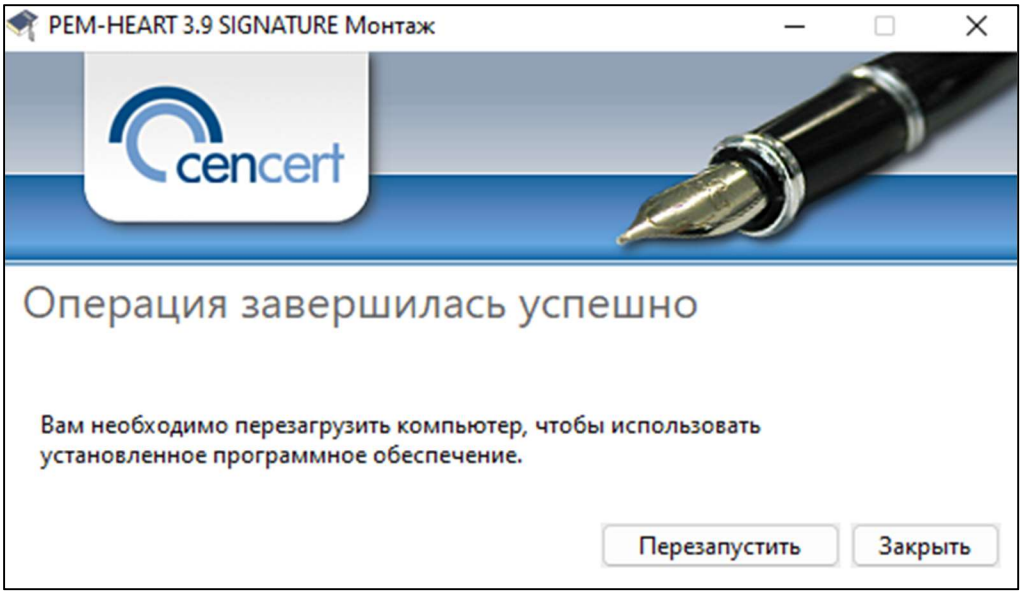


Рис. 5 Окно завершения процесса установки

3.1.2 УДАЛЕНИЕ ПРОГРАММЫ

Программа удаляется путем выбора пакета „PEM-HEART SIGNATURE” из Панели управления Windows: Панель управления\Программы\Программы и компоненты.

1. Запустится мастер установки. Нажмите кнопку *Удалить* — программа начнет процесс удаления программы из ресурсов операционной системы.

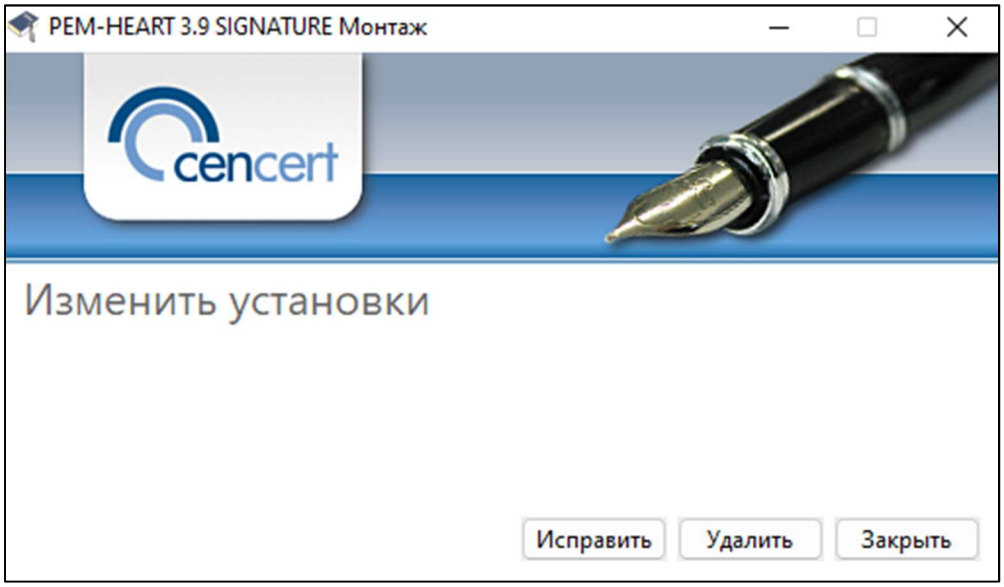


Рис. 6 Варианты модификации установки

2. В ходе процесса появится сообщение с просьбой удалить или сохранить конфигурацию программы SafeNet для карт Thales.

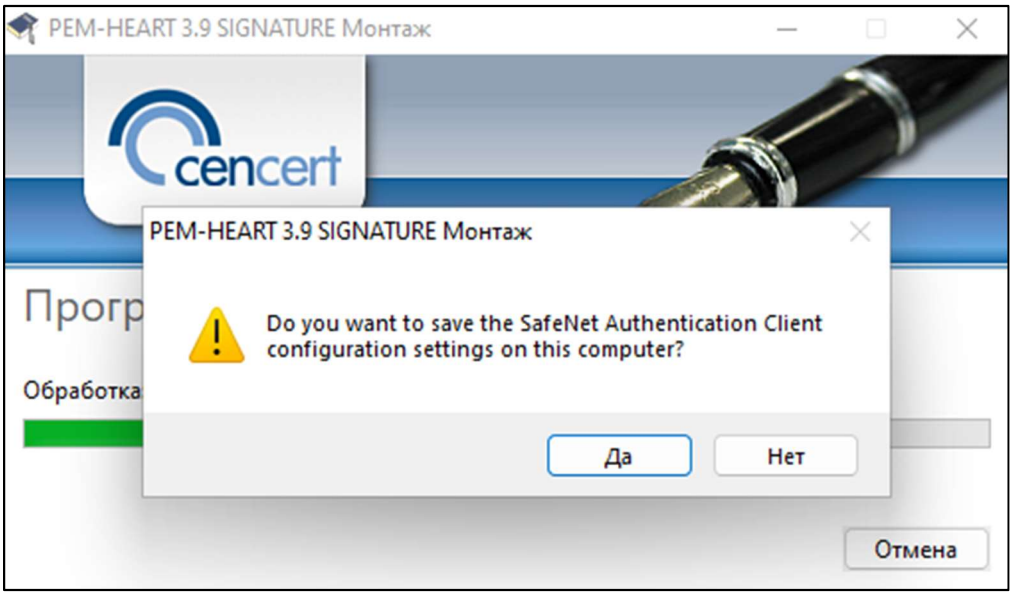


Рис. 7 Удаление программы

3. Мастер установки сообщит вам, что процесс удаления программного обеспечения завершен. Вам необходимо перезагрузить компьютер, нажав *Перезагрузить*.

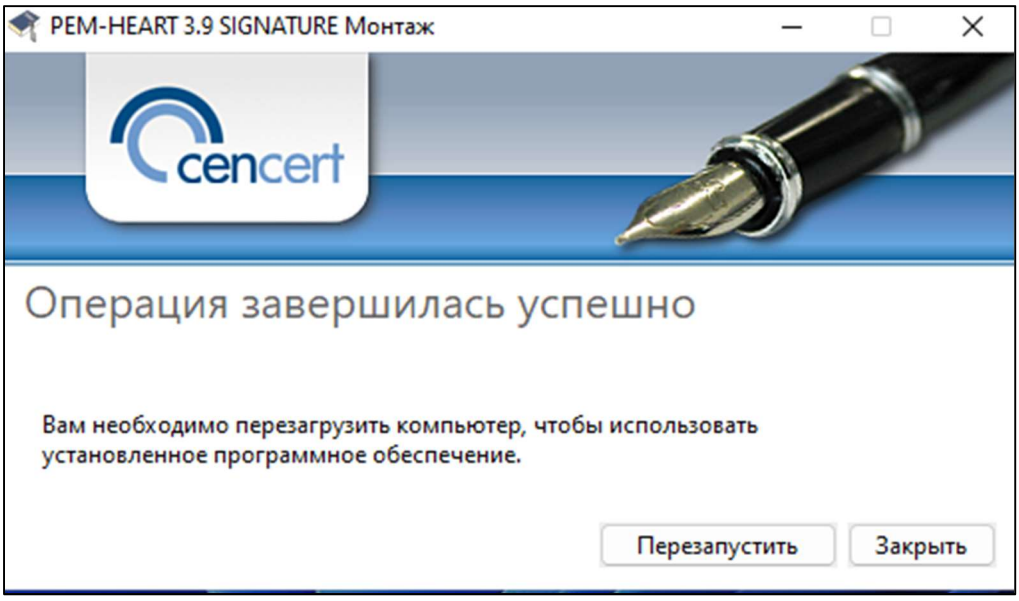


Рис. 8 Подтверждение удаления программы

3.2 УСТАНОВКА ДЛЯ MACOS

Пакет Pem-Heart для MacOS распространяется в формате .dmg — он содержит установочные файлы и программы удаления.

Pem-Heart поддерживает версии macOS 13 (Ventura) и 14 (Sonoma).

Приведенные ниже инструкции основаны на macOS Ventura.

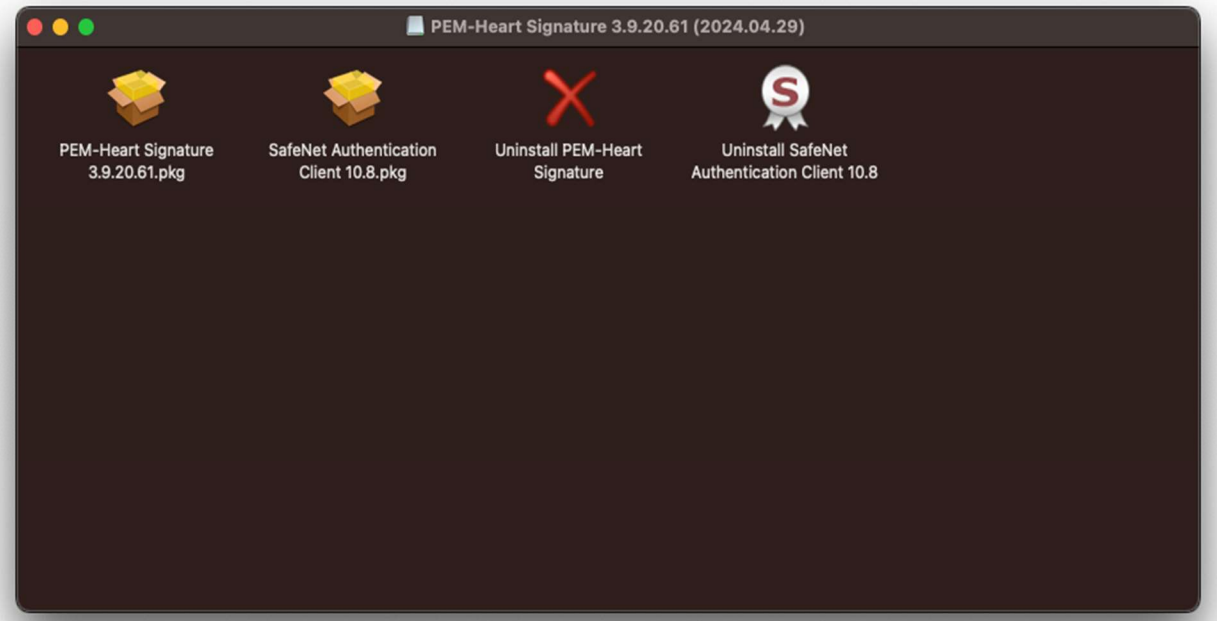


Рис. 9 Пакет Pem-Heart для macOS

3.2.1 УСТАНОВКА ЧЕРЕЗ ФАЙЛОВЫЙ МЕНЕДЖЕР

Установка должна выполняться из-под учетной записи с правами администратора. Перед началом установки рекомендуется закрыть все приложения, кроме тех, которые необходимы для работы операционной системы.

Доступны версии программы для процессорной архитектуры INTEL и ARM

В файловом менеджере Finder найдите в файловой структуре место с установочным файлом PEM-HEART Signature. Запустите файл, это инициализирует установщик.

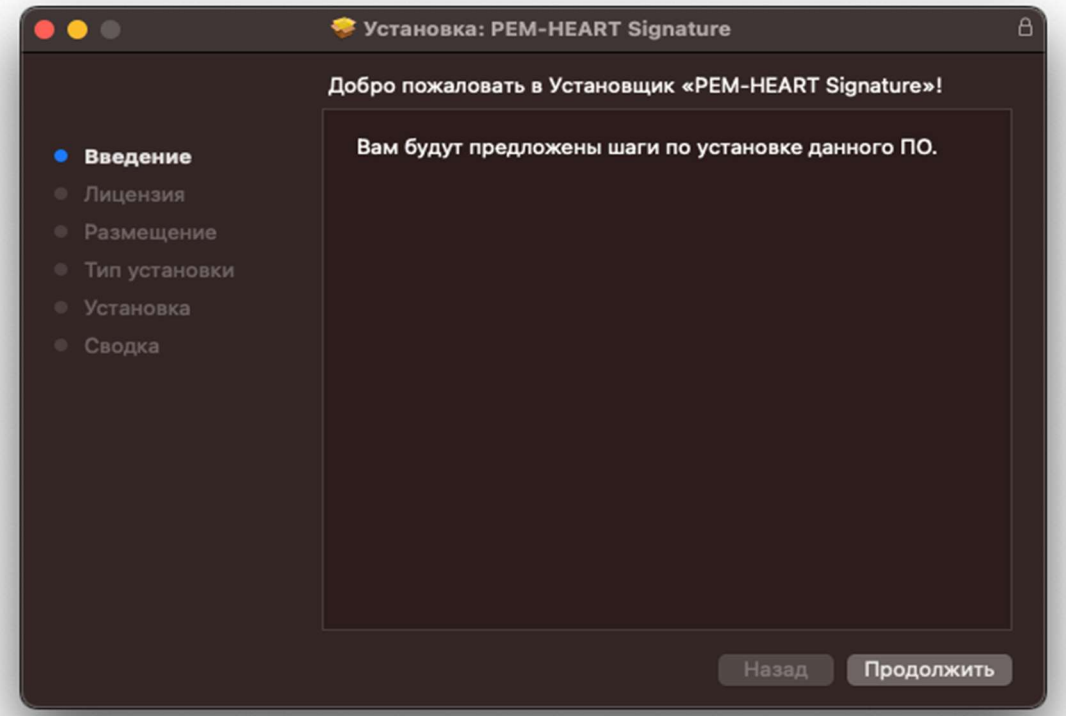


Рис. 10 Установщик пакета Pem-Heart — стартовое окно

1. На первом этапе установки пользователь должен принять лицензионное соглашение.

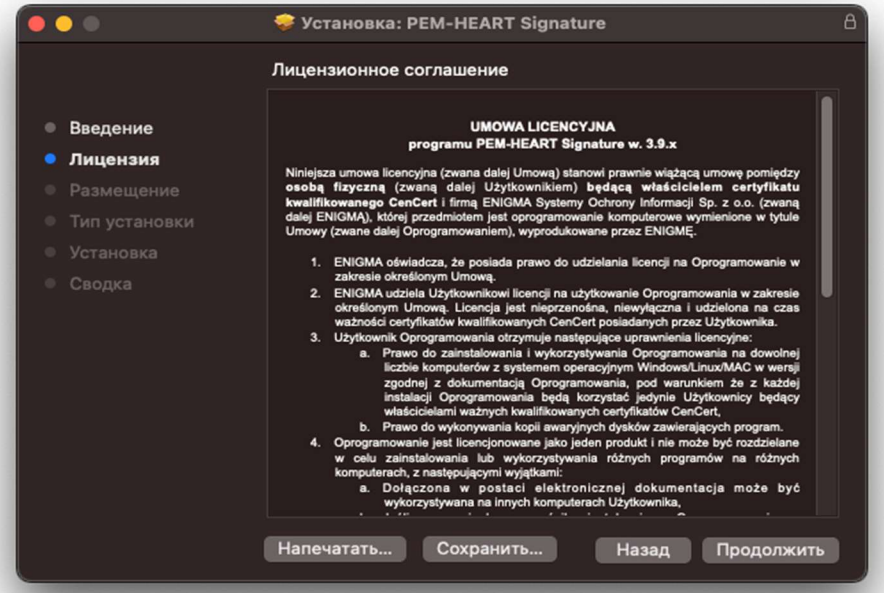


Рис. 11 Установщик пакета Pem-Heart — лицензионное соглашение

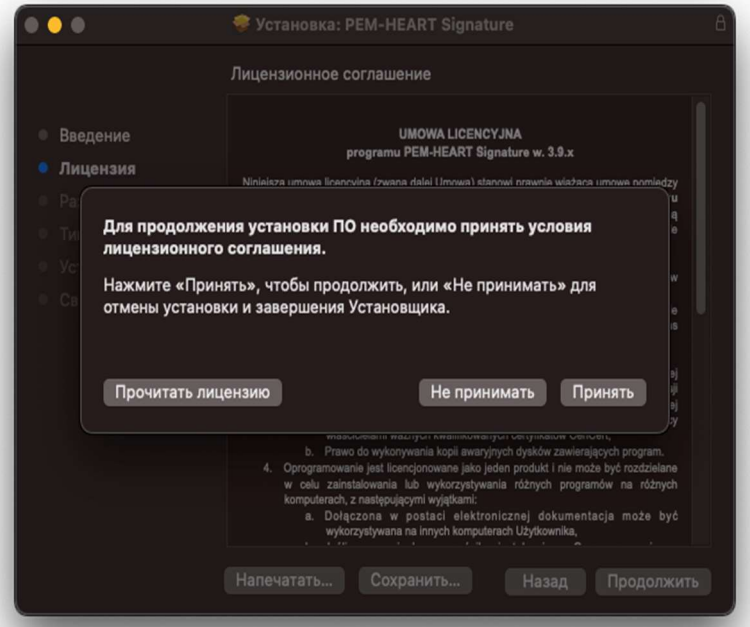


Рис. 12 Установщик пакета Pem-Heart – принятие лицензионного соглашения

2. Затем подтвердите свое намерение установить, нажав кнопку *Установить* и введя пароль учетной записи пользователя – начнется процесс установки. На этом этапе также можно изменить место установки, нажав „Изменить место установки...”.

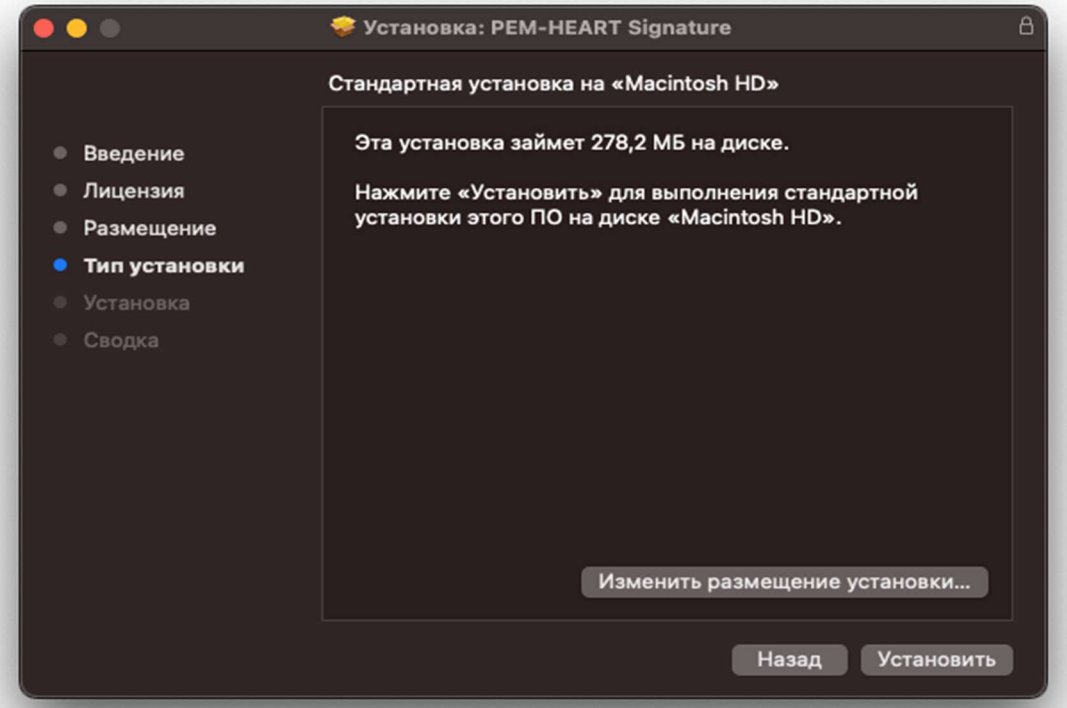


Рис. 13 Установщик пакета Pem-Heart — информация по установке

3. После завершения процесса установки отобразится сводный экран.

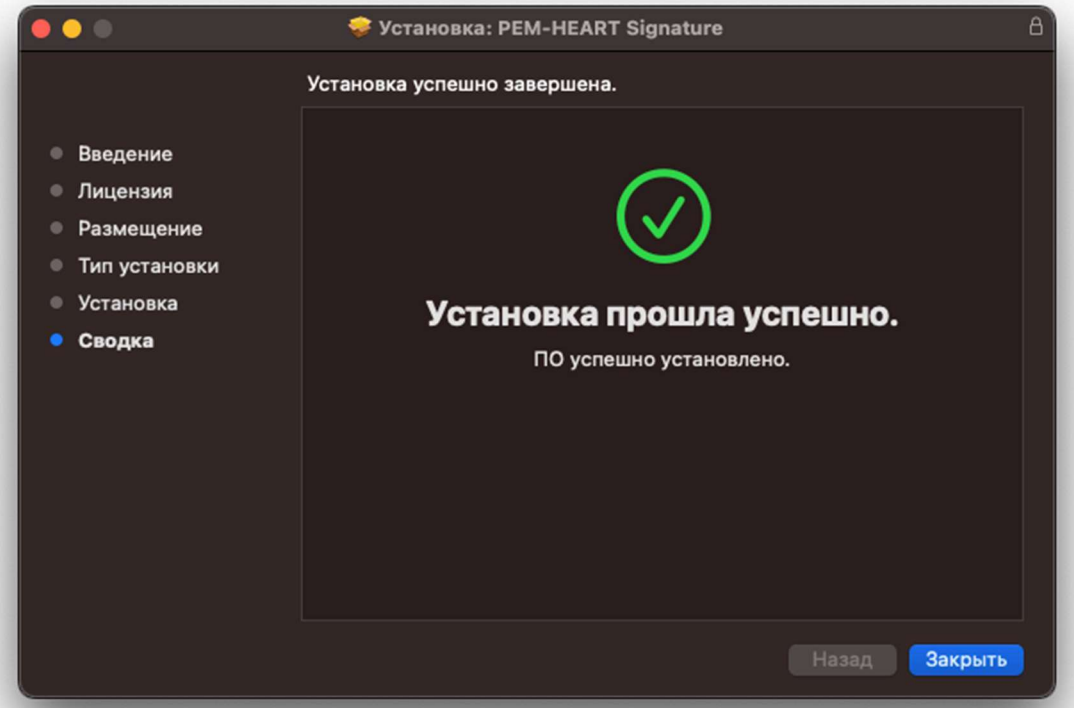


Рис. 14 Установщик пакета Pem-Heart — сводка установки

3.2.2 УСТАНОВКА ПРОГРАММЫ SAFENET CLIENT

Программа SafeNet компании Thales поддерживает карты IDPrime.

Установка должна выполняться из-под учетной записи с правами администратора. Перед началом установки рекомендуется закрыть все приложения, кроме тех, которые необходимы для работы операционной системы.

В файловом менеджере Finder найдите в файловой структуре место с установочным файлом программы SafeNet Authentication Client. Запуск файла приведет к инициализации установщика.

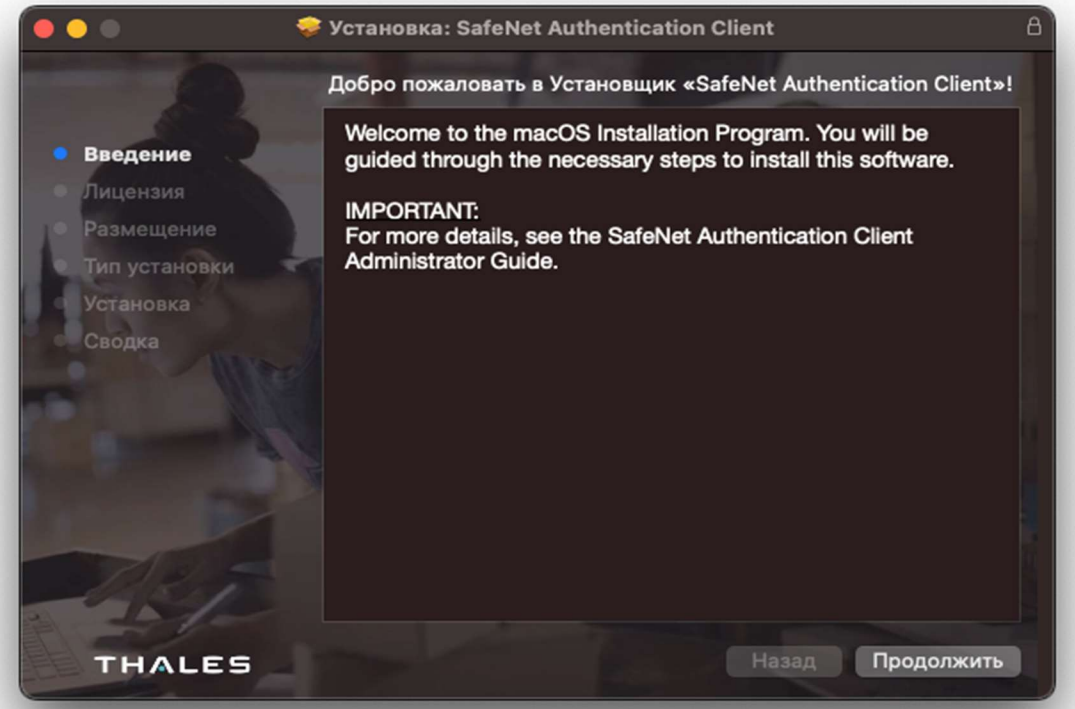


Рис. 15 Установщик пакета SafeNet Authentication Client — стартовое окно

1. На первом этапе установки пользователь должен принять лицензионное соглашение.

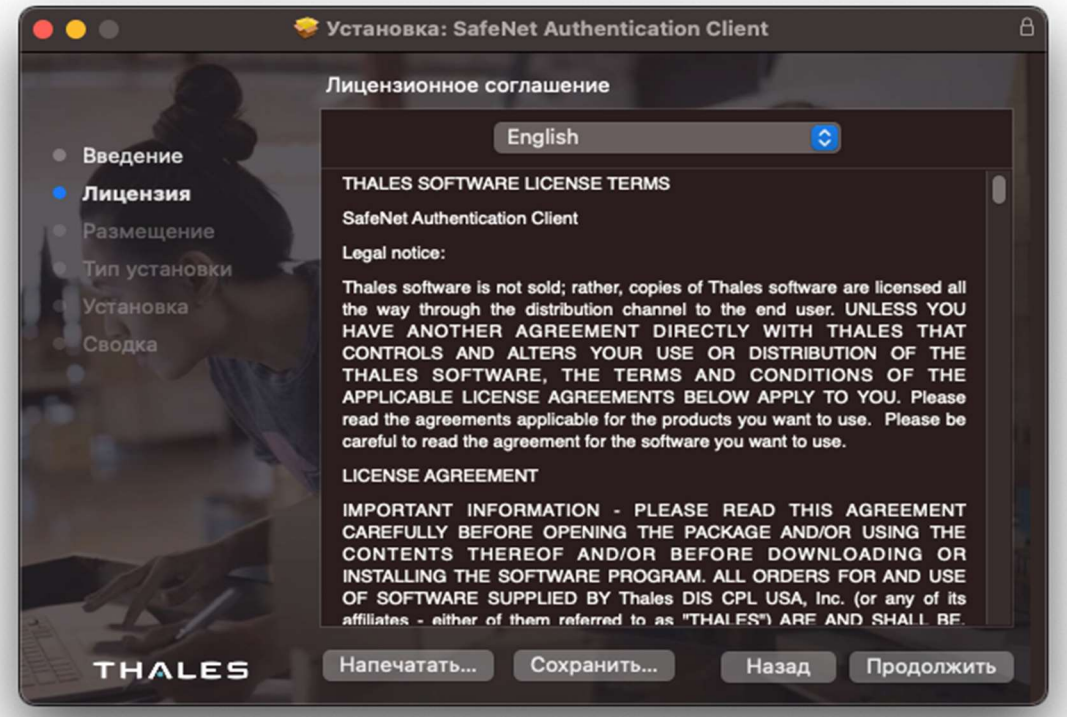


Рис. 16 Установщик пакета SafeNet Authentication Client – лицензионное соглашение

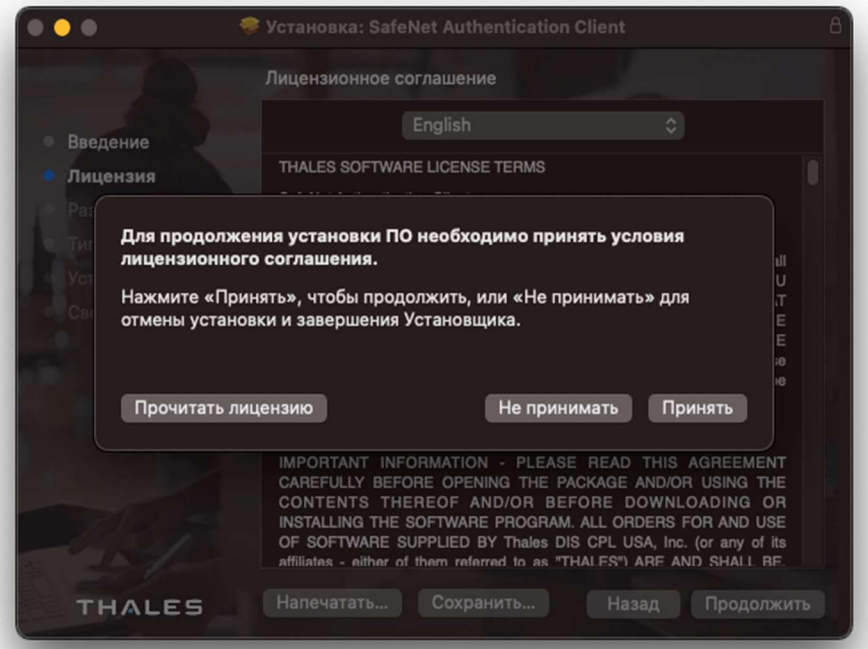


Рис. 17 Установщик пакета SafeNet Authentication Client – принятие лицензионного соглашения

2. Затем подтвердите свое намерение установить, нажав кнопку *Установить* и введя пароль учетной записи пользователя – начнется процесс установки. На этом этапе также можно изменить место установки, нажав „ Изменить место установки...”.

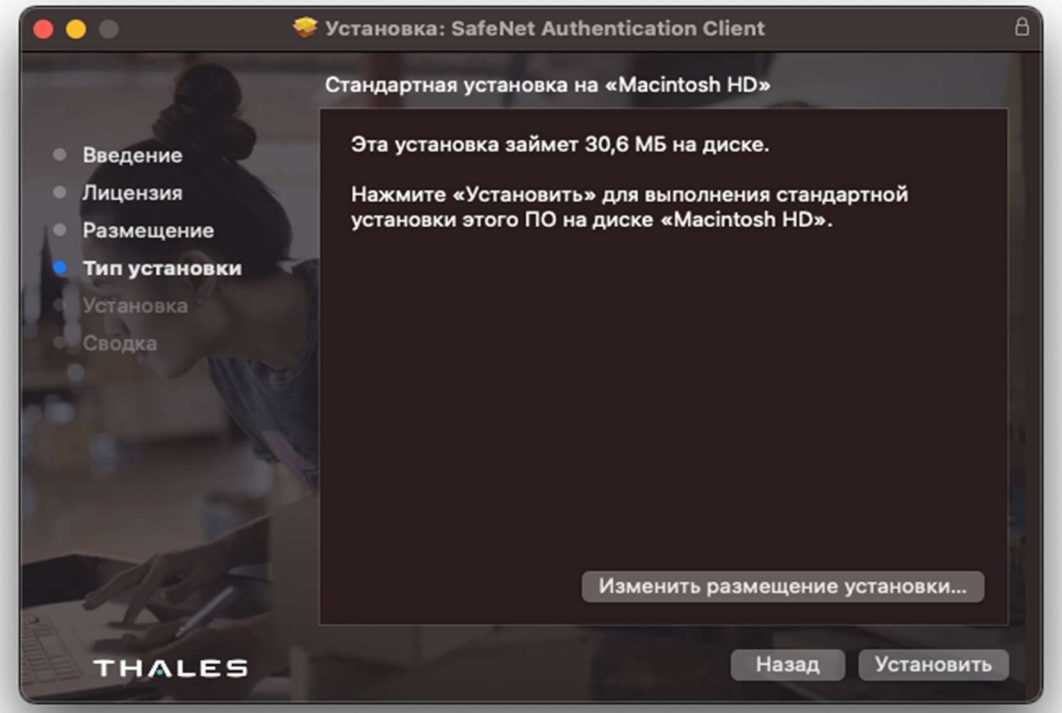


Рис. 18 Установщик пакета SafeNet Authentication Client – информация по установке

3. После завершения процесса установки отобразится сводный экран.

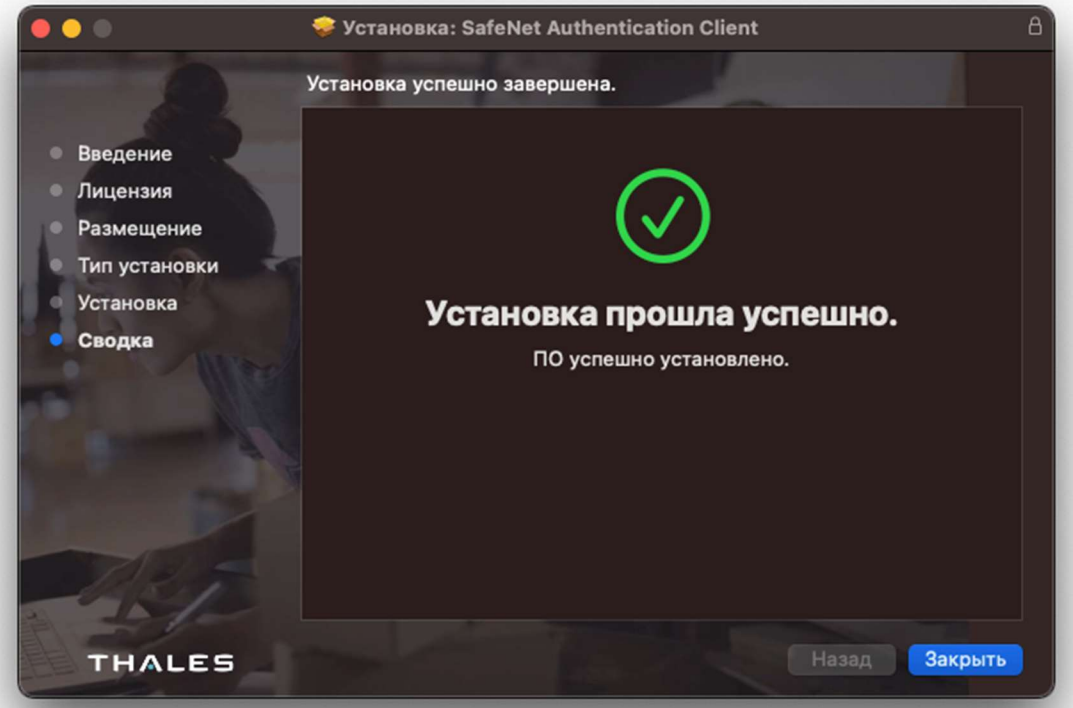


Рис. 19 Установщик пакета SafeNet Authentication Client – сводка установки

3.2.3 УДАЛЕНИЕ ПРОГРАММЫ

Удаление выполняется после запуска программы Uninstall PEM-Heart Signature. Появятся диалоговые окна с просьбой принять удаление:

- Приложение PEM-HEART вместе с отдельными компонентами программного обеспечения,

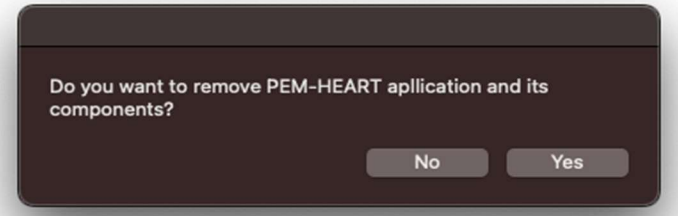


Рис. 20 Сообщение об удалении с просьбой удалить приложение Pem-Heart

- Конфигурация PEM-HEART из каталогов *opt*, *etc* и домашнего каталога,

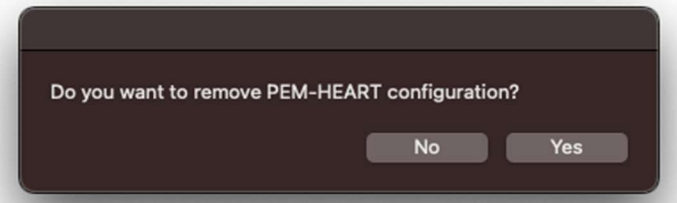


Рис. 21 Сообщение об удалении с просьбой удалить конфигурацию Pem-Heart

- Файлы конфигурации rSign (enigmaCloud.ini).

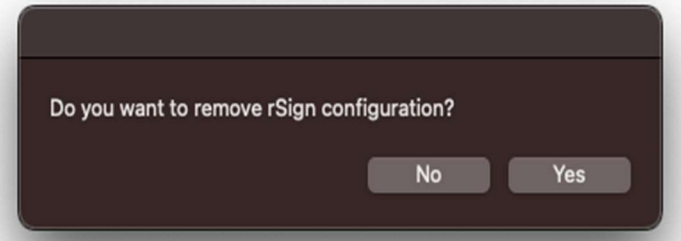


Рис. 22 Сообщение об удалении с просьбой удалить конфигурацию rSign

По окончании процесса появится окно с подтверждением удаления:

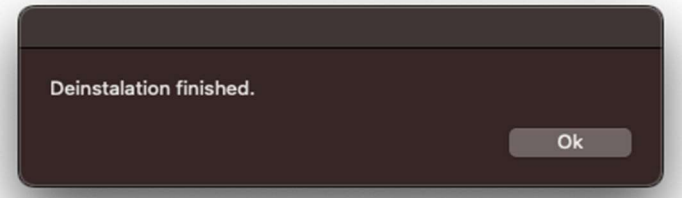


Рис. 23 Подтверждение удаления программы

3.2.4 УДАЛЕНИЕ SAFENET CLIENT

Удаление программного обеспечения для управления картами Thales осуществляется из Панели управления, в разделе *Программы и компоненты*, где необходимо выбрать программу из доступного списка и выбрать опцию *Удалить* или *Удалить/изменить*.

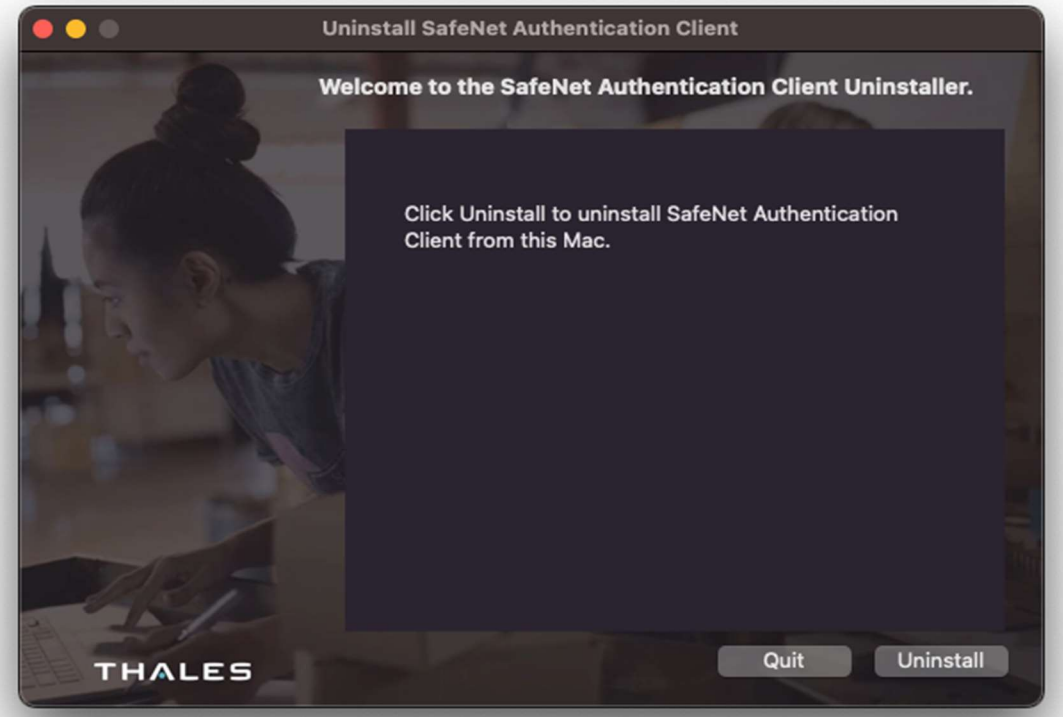


Рис. 24 Программа удаления программного обеспечения SafeNet Authentication Client – окно запуска

В окне мастера удаления нажмите *Удалить* и введите свой пароль. Появится подтверждение процесса.

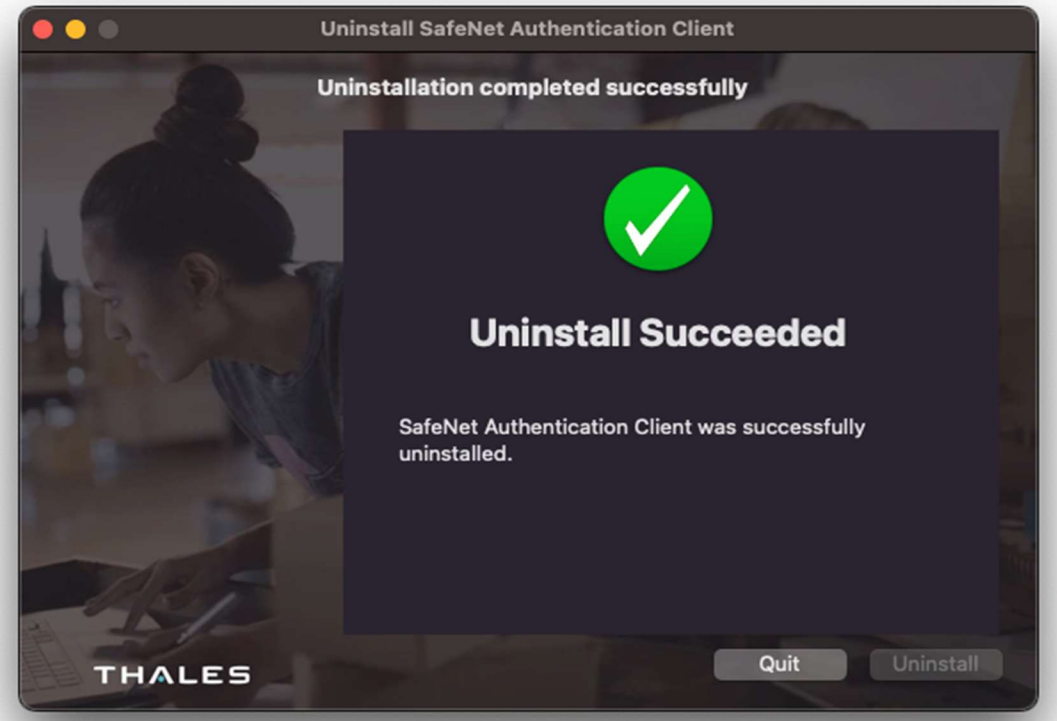


Рис. 25 Deinstalator SafeNet Authentication Client – сводная информация об удалении

3.3 УСТАНОВКА ДЛЯ СИСТЕМЫ LINUX

Установка должна выполняться из-под учетной записи с правами администратора. Перед началом установки рекомендуется закрыть все приложения, кроме тех, которые необходимы для работы операционной системы.

Следующий порядок установки представлен на примере системы Ubuntu 20.04 LTS, в менеджере пакетов системы (например, Ubuntu Software) и через терминал из командной строки.

Операции установки пакета должна предшествовать установка необходимых пакетов: pcscd и libncurses5. Это можно сделать с помощью команд:

sudo apt-get install pcscd

sudo apt-get install libncurses5

3.3.1 УСТАНОВКА ЧЕРЕЗ ФАЙЛОВЫЙ МЕНЕДЖЕР

В диспетчере найдите в файловой структуре место, где находятся установочные файлы PEM-HEART Signature. Установка осуществляется запуском (двойным щелчком мыши) заданного файла. Затем откроется связанный по умолчанию менеджер пакетов. После нажатия кнопки *Установить* PEM-HEART Signature устанавливается в систему.

После завершения установки появится соответствующее сообщение и окно установщика можно будет закрыть. Наконец, вам необходимо установить клиент аутентификации Safenet, чтобы использовать все доступные карты. Установочный файл можно скачать с сайта cencert.pl.

Safenet Authentication Client во время установки требуется, чтобы в системе был установлен пакет libgdk-pixbuf2.0-0. После установки доступ к программе возможен через контекстное меню файлов или через системное меню программ.

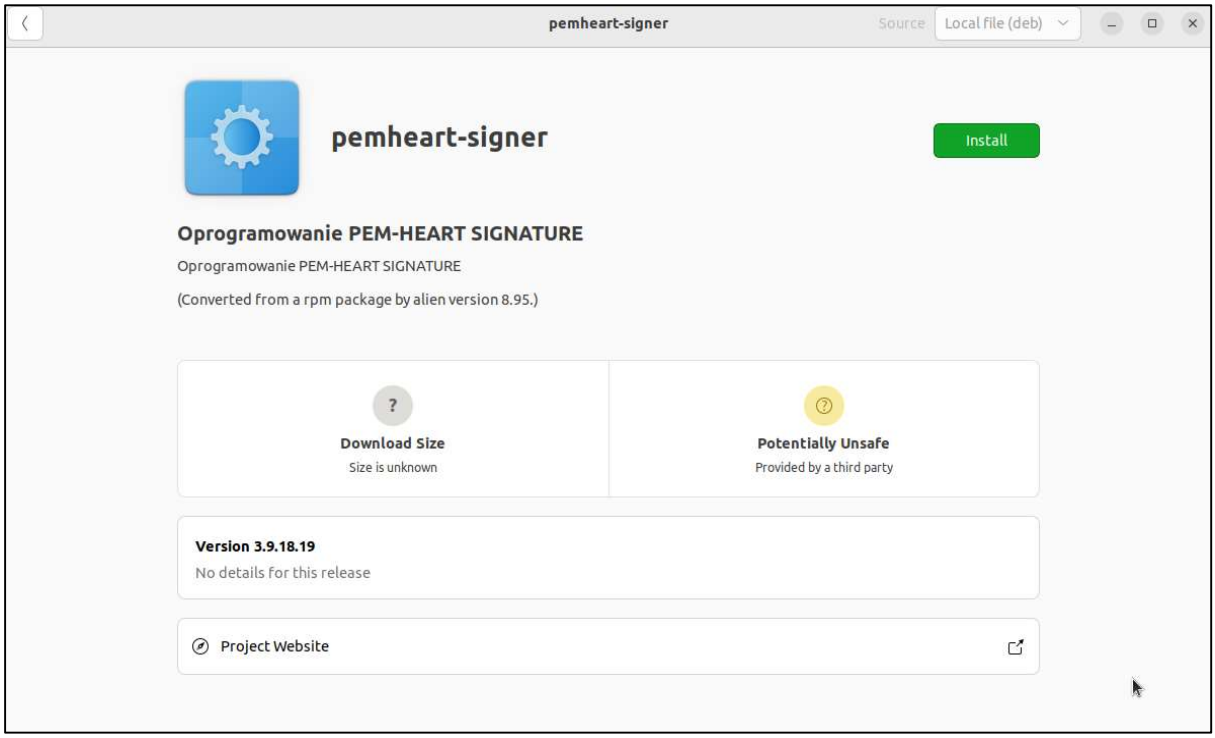


Рис. 26 Установка программы для системы Linux через файловый менеджер

Для установки нажмите зеленую кнопку в правом верхнем углу *Install*.

3.3.2 УСТАНОВКА ЧЕРЕЗ КОМАНДНУЮ СТРОКУ

Вариант установки PEM-HEART Signature через командную строку показан ниже.

После запуска окна терминала найдите место в файловой структуре, где расположены установочные файлы. Программное обеспечение распространяется в виде установочного пакета (файл с расширением .deb). Чтобы установить пакет «PEM-HEART Signature» в Ubuntu (здесь, в версии 20.4 LTS), выполните команду:

sudo dpkg -i PH-3.9.X.X_amd64.deb

где X.X это номер выпущенной версии программного обеспечения.

3.3.3 УДАЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Чтобы удалить программное обеспечение из системы, вы можете использовать терминал с командной строкой или запустить менеджер пакетов.

- Удалить через командную строку

Удаление PEM-HEART Signature производится с помощью двух консольных программ:

sudo apt-get purge pemheart-signer или

sudo apt remove pemheart-signer

- Удаление через файловый менеджер

После запуска менеджера пакетов (в примере использовалось программное обеспечение Ubuntu) найдите на вкладке «Установлено» в pemheart-signer, а затем нажмите на красную корзину (***Рис.27 Удаление программы для системы Linux через файловый менеджер***)

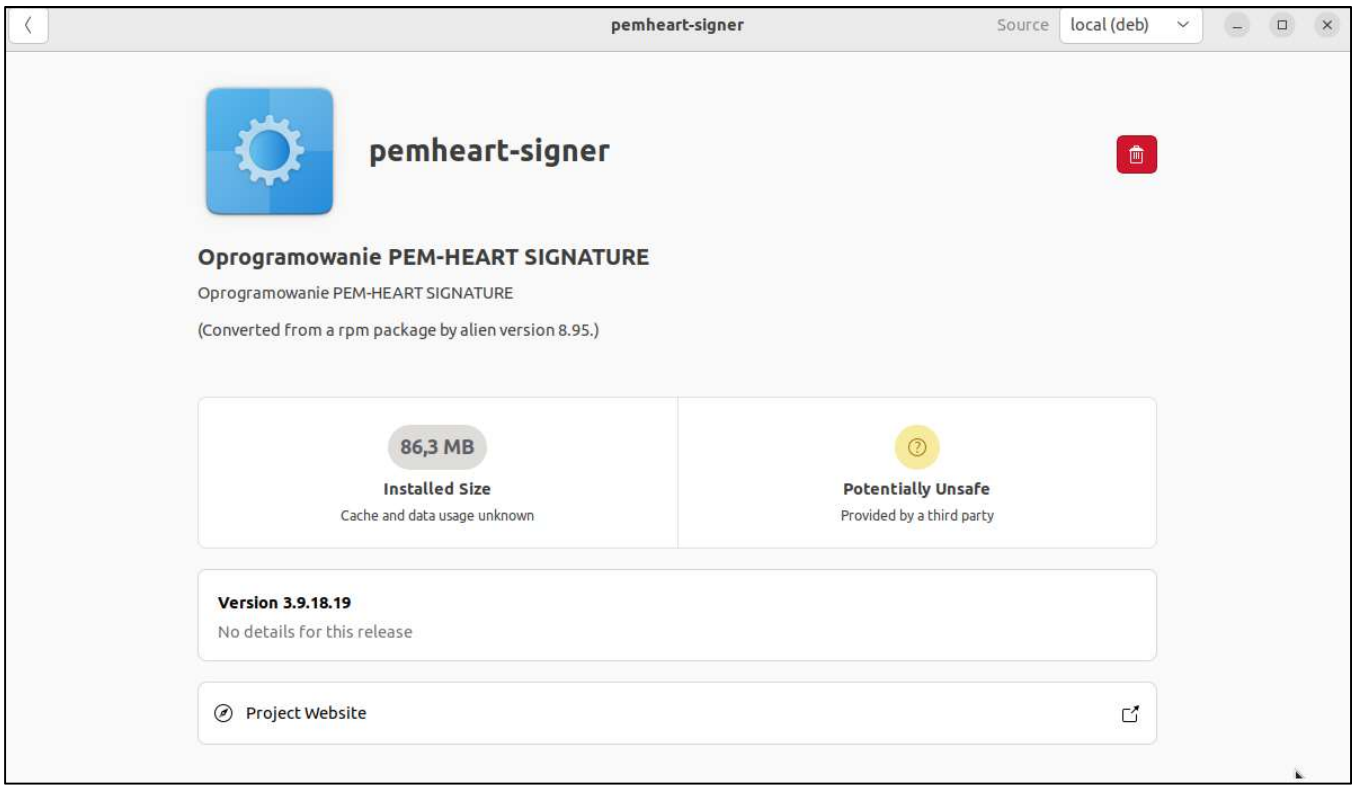


Рис. 27 Удаление программы для системы Linux через файловый менеджер

4 ОПЕРАЦИИ С ФАЙЛАМИ

Пользователь может выполнить некоторые операции без непосредственного запуска программы – щелкнув правой кнопкой мыши (PPM) по файлу. Из контекстного меню доступны различные функции, в том числе: проставление подписи или проверка подписи. В зависимости от типа файла набор опций может различаться.

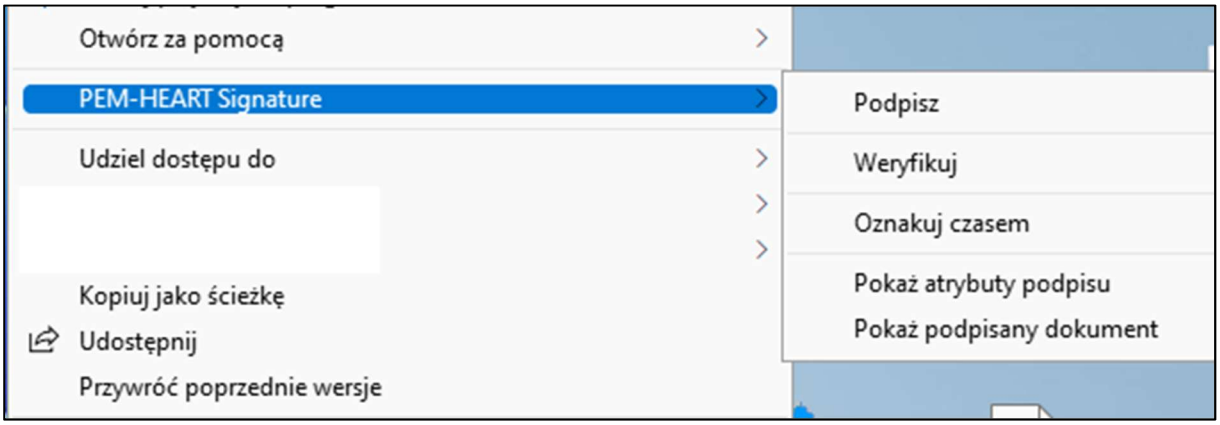


Рис. 28 Пример функций PPM для файла PDF

4.1 ПОДПИСАНИЕ – ПОДПИСЬ НА КАРТЕ ИЛИ USB-ТОКЕНЕ

Чтобы подписать, вставьте карту Cencert (токен в USB-порт USB-считывателя), а затем щелкните правой кнопкой мыши (PPM) по файлу, который необходимо подписать, чтобы развернуть контекстное меню - выберите *PEM-HEART Signature -> Подпиши* (для многих приложений этот параметр может находиться в разделе *Показать дополнительные параметры*). Операция также выполняется на уровне работающего приложения PEM-HEART Signature (описание деятельности представлено в **5.2.1 Подписание – подпись на карте или USB-токене, стр. 41**)

Программа автоматически выберет рекомендуемый формат подписи и запросит ПИН-код карты.

Комментарии:

- Дополнительные параметры, такие как изменение формата подписи, подпись в отдельном файле, отметка времени и другие настройки, доступны под кнопкой «Параметры...». Измененные таким образом настройки

применяются к конкретной подписи и не запоминаются для дальнейшего использования. См. также главу **8.1 ИЗМЕНЕНИЕ ПАРАМЕТРОВ ПОДПИСИ**.

- В зависимости от формата подписи она будет сохранена в том же файле без изменения имени или в новом файле с измененным расширением.
- Если выбрать «подпись в отдельном файле», подпись будет сохранена в отдельном файле. Выбор этой опции требует последующей отправки получателю двух файлов: исходного файла и подпись.
- Если подпись должна включать метку времени и/или ответ OCSP, во время подписи требуется подключение к Интернету. Вам также может потребоваться приобрести услугу штамповки времени.

4.2 ПОДПИСАНИЕ – ПОДПИСЬ RSIGN (ОБЛАЧНАЯ ПОДПИСЬ)

Для подписания щелкните правой кнопкой мыши (PPM) по подписываемому файлу, чтобы развернуть контекстное меню – выберите следующие параметры: *PEM-HEART Signature -> Подпиши (для многих приложений этот параметр может находиться в разделе Показать дополнительные параметры).* Операция также выполняется на уровне работающего приложения PEM-HEART Signature (описание деятельности представлено в **5.2.2 ПРЕДСТАВЛЕНИЕ ПОДПИСИ – ПОДПИСЬ RSIGN (ОБЛАЧНАЯ ПОДПИСЬ)**)

Программа автоматически выберет рекомендуемый формат подписи. Затем нажмите *Далее* и введите свой PIN-код для подписи (пользователю будет предложено его ввести). Следующий шаг требует запуска приложения *rSign by Cencert* на вашем мобильном устройстве, с которого вам необходимо считать с экрана код „ АКТИВНЫЙ PIN ДЛЯ ПОДПИСИ ” – вам следует ввести его в приложение на вашем компьютере и нажать ОК. Далее необходимо подтвердить намерение подписания в приложении rSign, после чего программа выполнит подпись.

Внимание! Рекомендуем настроить параметры в приложении *Настройки -> PIN -> Запомните свой PIN на определенный период времени*, при этом время установлено на 3 минуты. Это позволит вам подписать с отметкой времени или даже несколько раз (если программа выбрала несколько файлов для подписи) без необходимости утверждать каждую операцию подписи на телефоне. Если вы установите для подписи значение «Запрашивать PIN каждый раз», создание подписи с отметкой времени потребует двойного подтверждения подписи на телефоне (подпись под документом, подпись под запросом отметки времени).

Комментарии:

- Дополнительные параметры, такие как изменение формата подписи, подпись в отдельном файле, отметка времени и другие настройки, доступны под кнопкой «Параметры...». Настройки, измененные таким образом, применяются к конкретной подписи и не запоминаются для дальнейшего использования. См. также главу **8.1 ИЗМЕНЕНИЕ ПАРАМЕТРОВ ПОДПИСИ**.
- В зависимости от формата подписи подпись будет сохранена в том же файле без изменения имени или в новом файле с измененным расширением.
- Если выбрать «подпись в отдельном файле», подпись будет сохранена в отдельном файле. Выбор этой опции требует последующей отправки получателю двух файлов: исходного файла и подписи.
- Для подписания требуется подключение к Интернету.

4.3 ПРОВЕРКА ПОДПИСИ

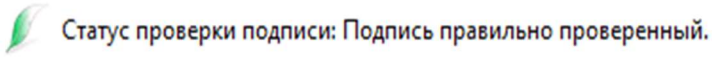
Чтобы проверить подпись, щелкните правой кнопкой мыши (PPM) в файле, который необходимо подписать, затем выберите команду *PEM-HEART Signature -> Проверить* (для многих приложений эта опция может находиться под *Показать больше вариантов*). После этого откроется окно проверки подписи. Затем нажмите кнопку *Проверить*. Программа проверит сохраненные в документе подписи и отобразит результат проверки. Операция также выполняется из работающего приложения PEM-HEART Signature (описание деятельности представлено в **5.3 ПРОВЕРКА ПОДПИСИ В ПРОГРАММЕ**)

Если подпись была отмечена временной меткой – момент, для которого проверена подпись, берется из временной метки (любой последующий отзыв сертификата не повлияет на результат проверки такой подписи).

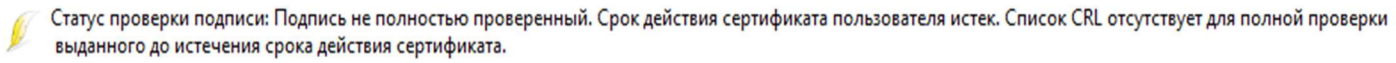
Если подпись не имеет временной метки – подпись проверяется в текущий момент или в другой момент, введенный вручную в программу («проверить за указанное время: ...»). Если вручную вводить момент проверки подписи, то ответственность за правильность времени (и, возможно, доказуемость) полностью лежит на пользователе.

Результат проверки отмечается цветными символами, чтобы его можно было четко отличить:

- Зеленый цвет означает правильную проверку подписи.



- Желтый цвет означает неполную проверку — подпись математически правильна, но подтвердить, был ли сертификат действителен на момент подписания, пока невозможно. В этом случае вам следует повторить проверку позже — например, через несколько часов или на следующий день.



- Красный цвет означает сбой проверки подписи (например, математическое несоответствие, т. е. нарушение целостности документа или объявление сертификата недействительным).

4.3.1 ПАНЕЛЬ ПРОВЕРКИ

После проверки подписи в верхнем меню доступны различные дополнительные действия, в том числе:

- *Представить документ* - отображение исходного (подписанного) документа, если в системе установлена программа для отображения данного типа документов.
- *Открыть каталог* – открытие просмотра каталога на диске, где сохранен документ.
- *Атрибуты подписи* - показ дополнительных данных, прикрепленных к подписи.
- *Показать сертификат* - отображение сертификата с реквизитами лица, подписавшего документ. Здесь вы можете экспортировать сертификат в следующем формате *.crt* через кнопку *Экспорт*.
- *Показать отчет xml* – показ XML-отчета в окне программы.
- *Создать отчет в формате PDF* - сохранение читаемого отчета (в формате PDF) на диске, подтверждающего проверку подписи.
- *Показать помощь* – будет отображено руководство пользователя в формате pdf.

После правильной проверки подписи можно создавать расширенные формы подписи. [1]:

- *Создать архивного персонажа* - обеспечение возможности корректной проверки подписи на срок действия временной метки (практически примерно 7-10 лет). Для создания архивной формы требуется доступ к Интернету и загрузка, среди прочего, две временные метки. Возможно, вам придется приобрести пакет меток времени.

Срок действия архивной формы подписи может продлеваться любое количество раз (путем добавления еще одной отметки времени), каждый раз на последующие 7-10 лет.

1 В формате подписи PAdES невозможно добавить к подписи временную метку, если она не была добавлена сразу при создании подписи

- *Создать форму long* - обеспечение возможности корректной проверки подписи на срок действия OCSP и метки времени (практически примерно 5-10 лет). Создание персонажа *long* требует доступа в Интернет и загрузки, среди прочего, временной метки. Возможно, вам придется приобрести пакет меток времени..

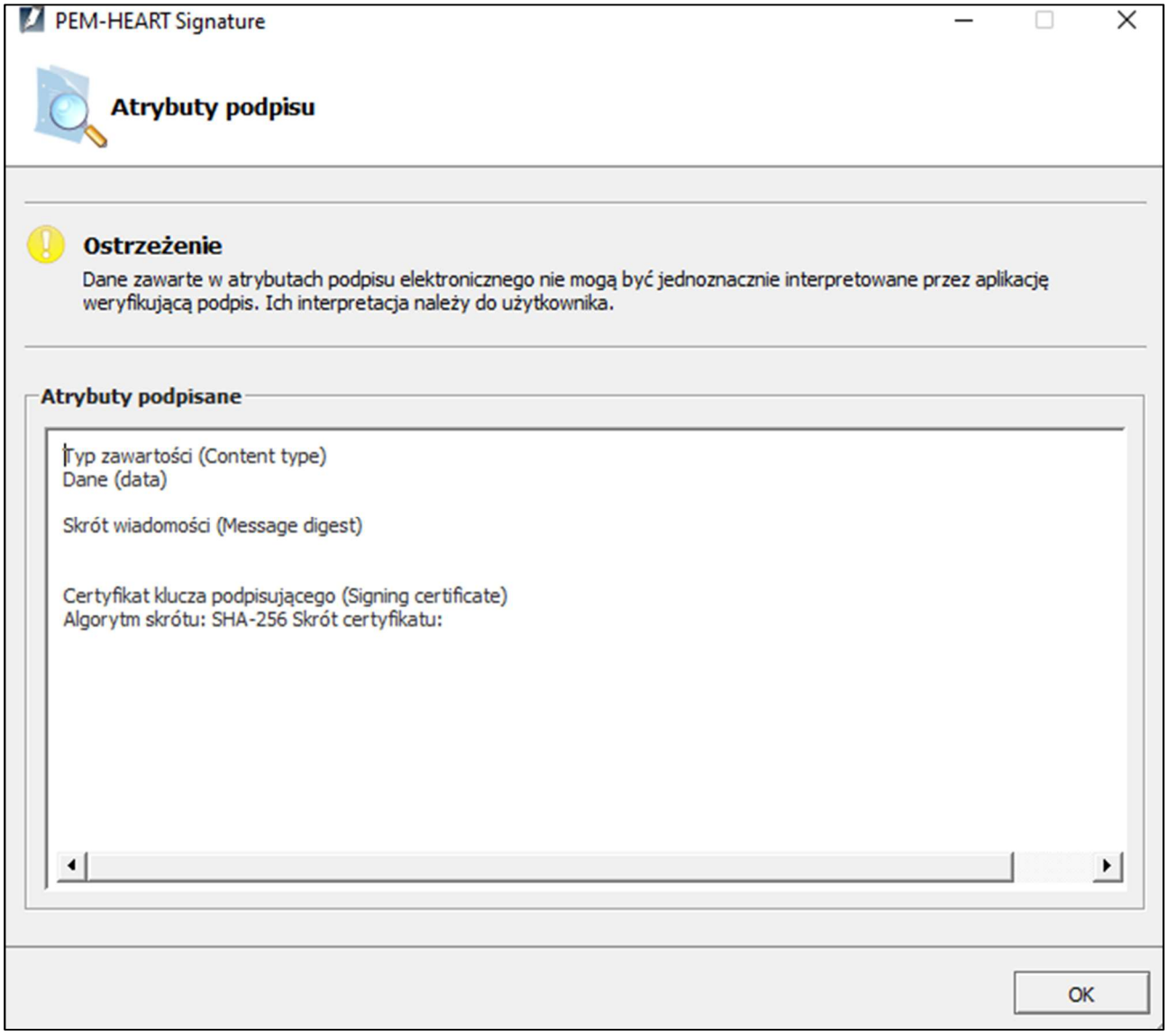


Рис. 29 Окно с атрибутами подписи

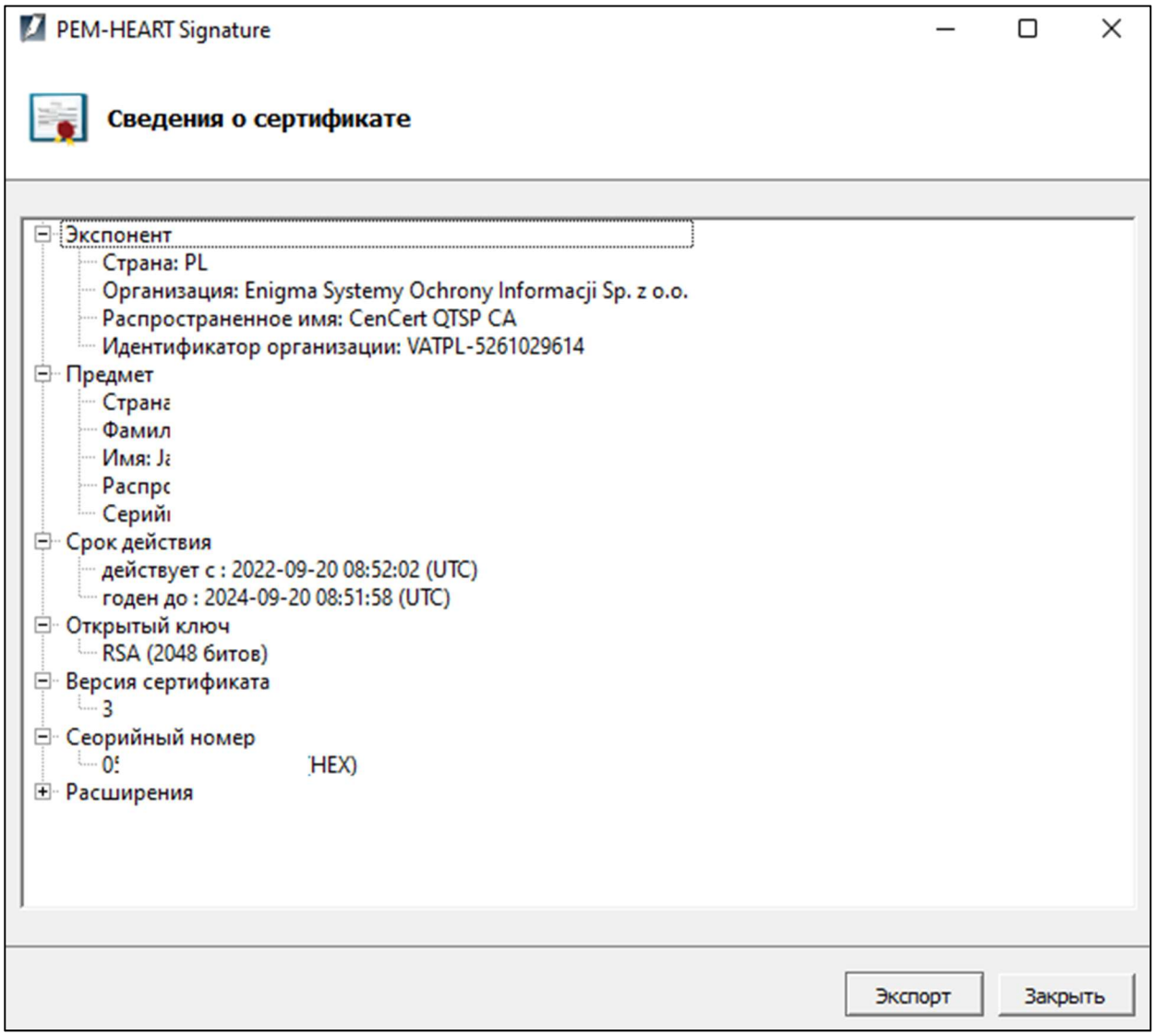


Рис. 30 Окно с подробной информацией о сертификате

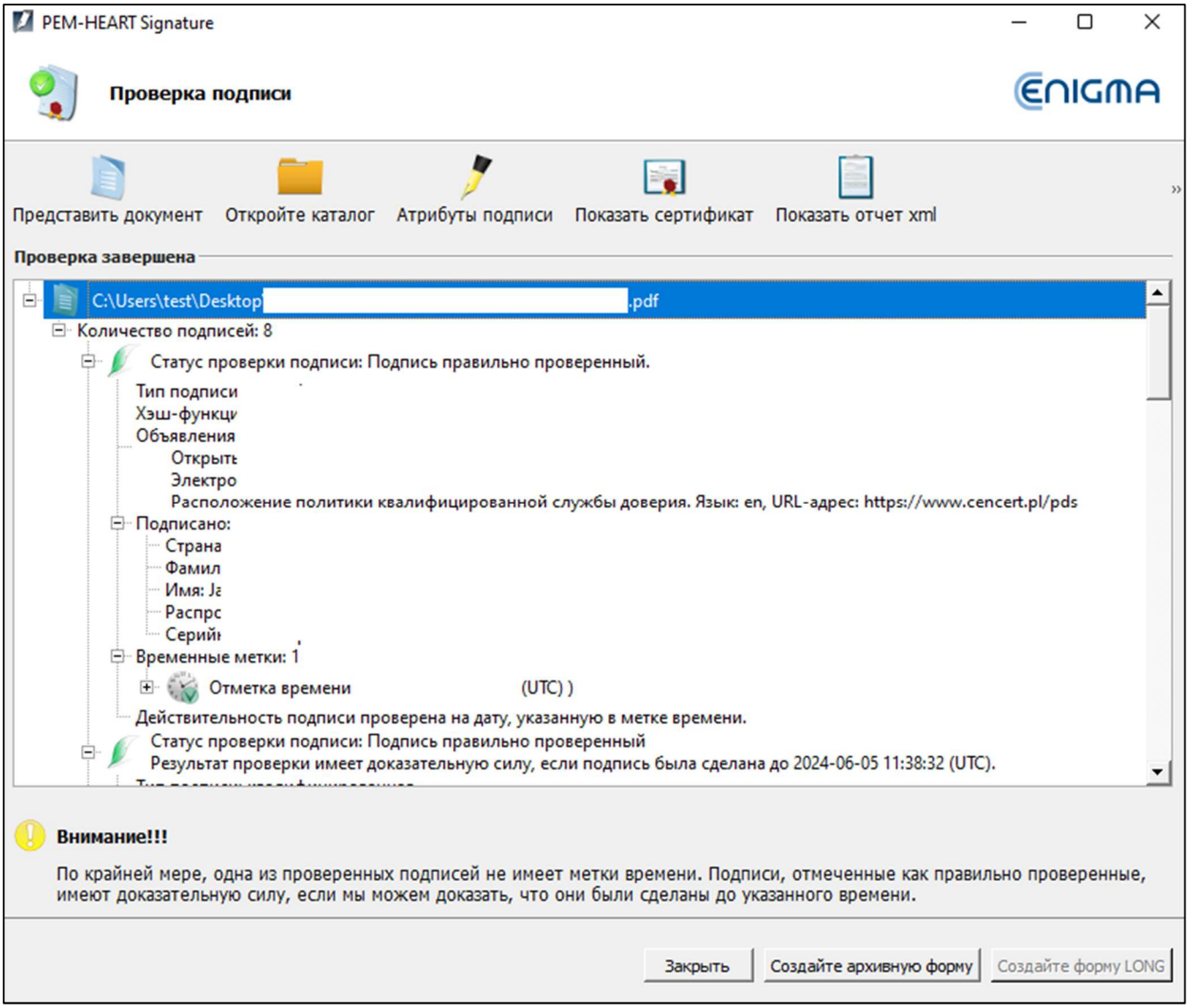


Рис. 31 Статус подписи после проверки

5 ОСНОВНЫЕ ФУНКЦИИ

5.1 ЗАПУСК ПРОГРАММЫ

Все функции программы доступны после запуска программы *PEM-HEART Signature* из меню *Start* (Windows) или через значок на рабочем столе. В других операционных системах запустите программу способом, соответствующим вашей системе. Внешний вид программы такой же, как в системе Windows.

5.2 ПОДПИСАНИЕ В ПРОГРАММЕ

5.2.1 ПОДПИСАНИЕ – ПОДПИСЬ НА КАРТЕ ИЛИ USB-ТОКЕНЕ

Чтобы подписать после запуска программы, нажмите значок *Подписать* (в левой части окна, на панели *Основные функции*). Откроется окно, позволяющее выбрать файлы для подписи. Здесь вы можете добавить файл или файлы для подписи (кнопка *Добавить файл*) или перетащить файл в окно списка файлов. Если указан весь каталог (кнопка *Добавить каталог*), все файлы из этого каталога и его подкаталогов будут добавлены в список подписываемых файлов. После добавления всех файлов в подпись нажмите *Далее*. Если к операционной системе подключен один считыватель с сертификатом, программа запросит ПИН карты. Если считывателей с сертификатами будет больше, программа выдаст окно с выбором токена. После корректной работы подпись будет создана.

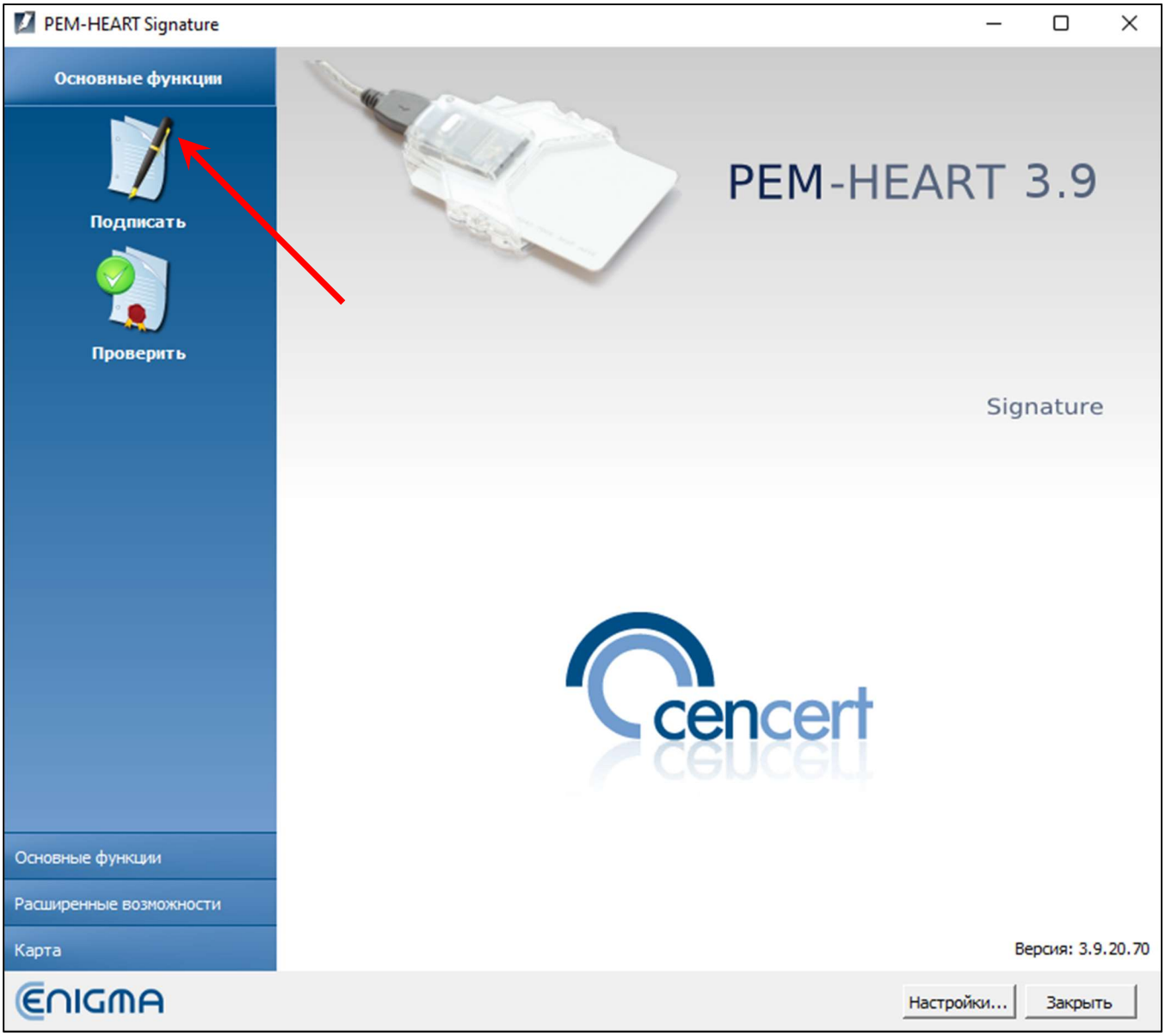


Рис. 32 Главное меню приложения PEM-HEART Signature – выбор опции «Подписать»

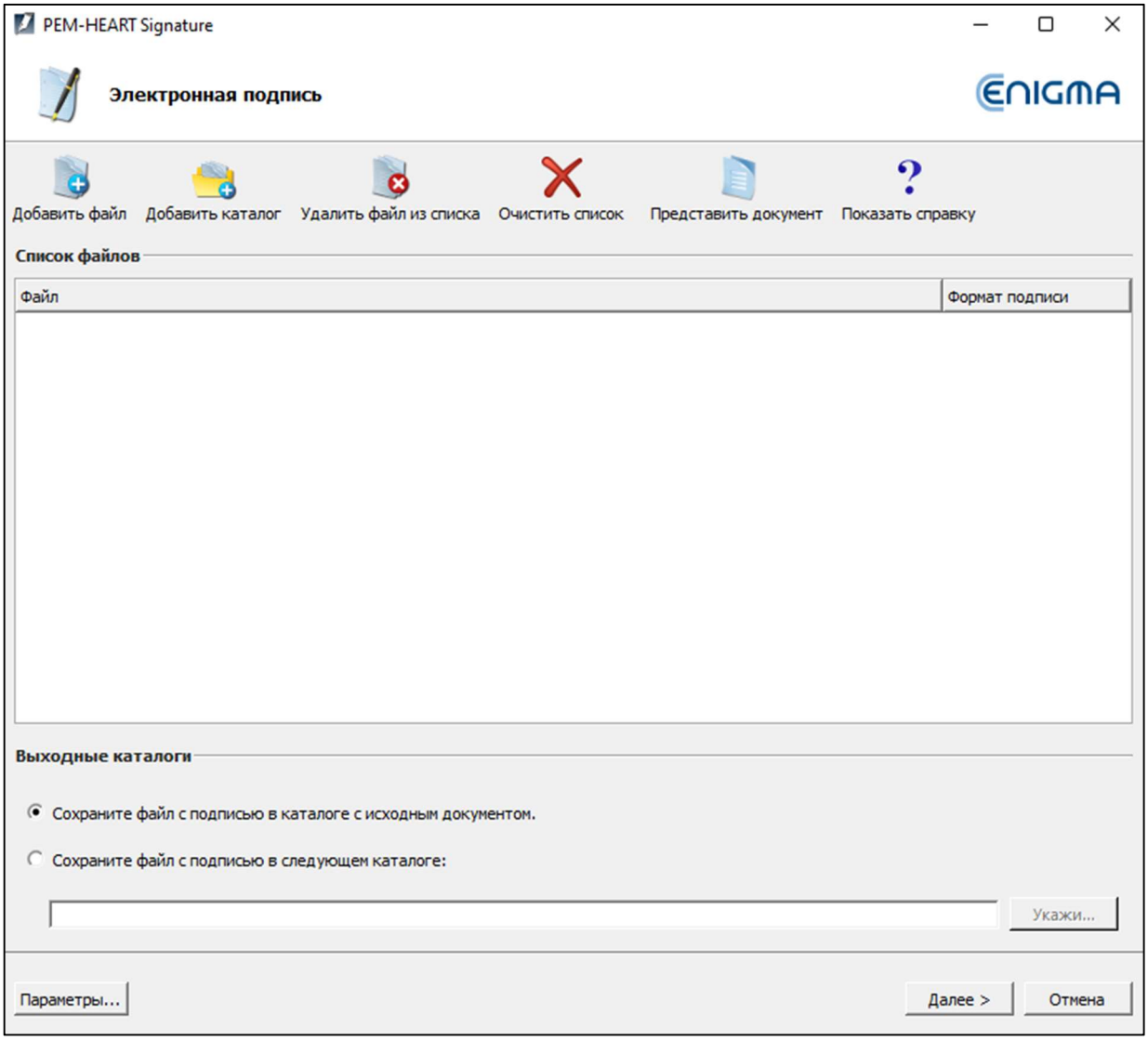


Рис. 33 Окно подачи электронной подписи

Комментарии:

1) 1) Дополнительные параметры, такие как изменение формата подписи, подпись в отдельном файле, отметка времени и другие настройки, доступны под кнопкой *Параметры ...* . Измененные таким образом настройки применяются к конкретной подписи и не запоминаются для дальнейшего использования. См. также главу **8.1 ИЗМЕНЕНИЕ ПАРАМЕТРОВ ПОДПИСИ**.

2) В зависимости от формата подписи, подпись будет сохранена в том же файле без изменения имени или в новом файле с измененным расширением.

3) Если выбрать «подпись в отдельном файле», подпись будет сохранена в отдельном файле. В этом случае получателю необходимо предоставить два файла: исходный файл и файл подписи.

4) Если подпись должна включать метку времени и/или ответ OCSP, во время подписи требуется подключение к Интернету. Вам также может потребоваться приобрести услугу отметки времени.

5.2.2 ПРЕДСТАВЛЕНИЕ ПОДПИСИ – ПОДПИСЬ RSIGN (ОБЛАЧНАЯ ПОДПИСЬ)

Чтобы подписать rSign, после запуска программы нажмите значок *Подписать* (в левой части окна, на панели *Основные функции*). Откроется окно, позволяющее выбрать файлы для подписи. Здесь вы можете добавить файл или файлы для подписи (кнопка *Добавить файл*) или перетащив файл в окно списка файлов. Если указан весь каталог (кнопка *Добавить каталог)*, все файлы из этого каталога и его подкаталогов будут вставлены в список подписываемых файлов. После добавления всех файлов в подпись нажмите кнопку *Далее*. После добавления всех файлов в подпись нажмите кнопку *Далее*. Если к операционной системе подключен один считыватель с сертификатом, программа запросит ПИН для подписи. Если считывателей с сертификатами будет больше, программа выдаст окно с выбором токена. После корректной работы подпись будет создана.

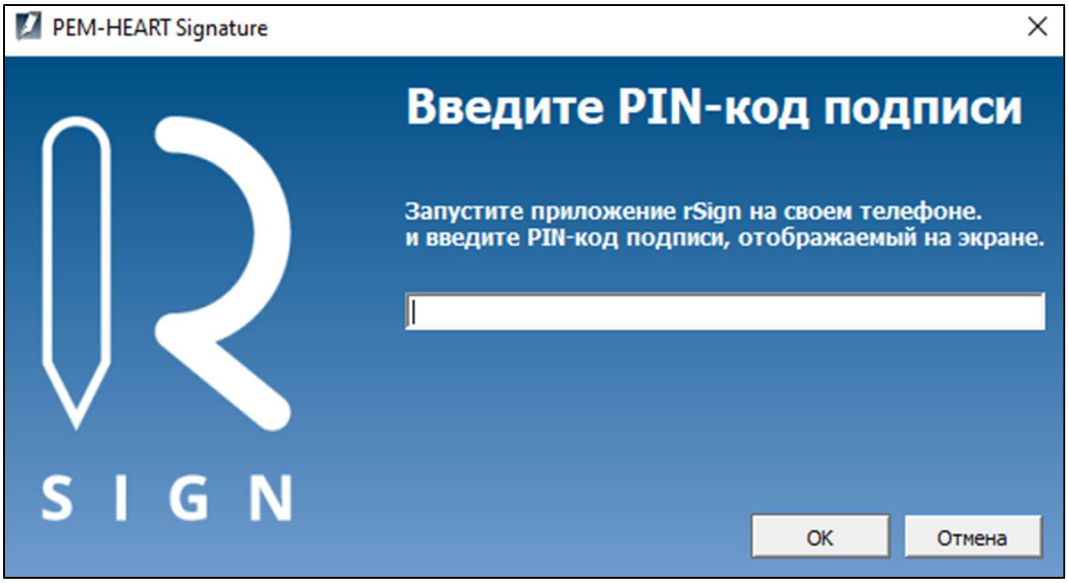


Рис. 34 Сообщение об использовании приложения rSign на телефоне

Теперь запустите мобильное приложение *rSign by Cencert*, а затем прочитайте *Активный ПИН подписи,* скопируйте его в программу на своем компьютере и подтвердите, нажав *OK*. Намерение подписать необходимо подтвердить в заявке rSign.

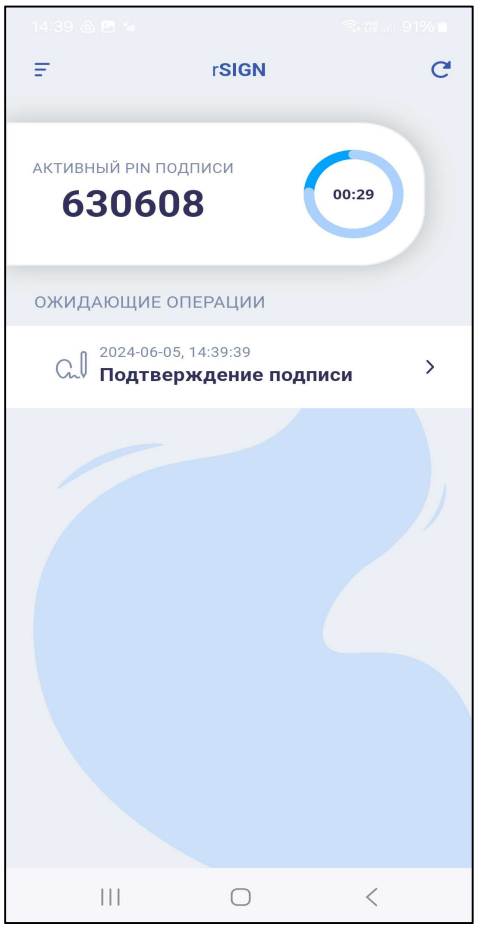


Рис. 35 Экран приложения rSign с Активным PIN подписи

В заявке необходимо подтвердить свое желание подписать, нажав кнопку *Подтверждение подписи* в разделе *ОЖИДАЮЩИЕ ОПЕРАЦИИ* чуть ниже отображаемого Активного ПИН подписи (**Рис. 35 Экран приложения rSign с Активным PIN подписи**). Если данные верны, на следующем этапе необходимо подтвердить операцию, нажав кнопку *ПОДТВЕРДИТЬ* (**Рис. 36 Подтверждение проведения операции электронной подписи**)

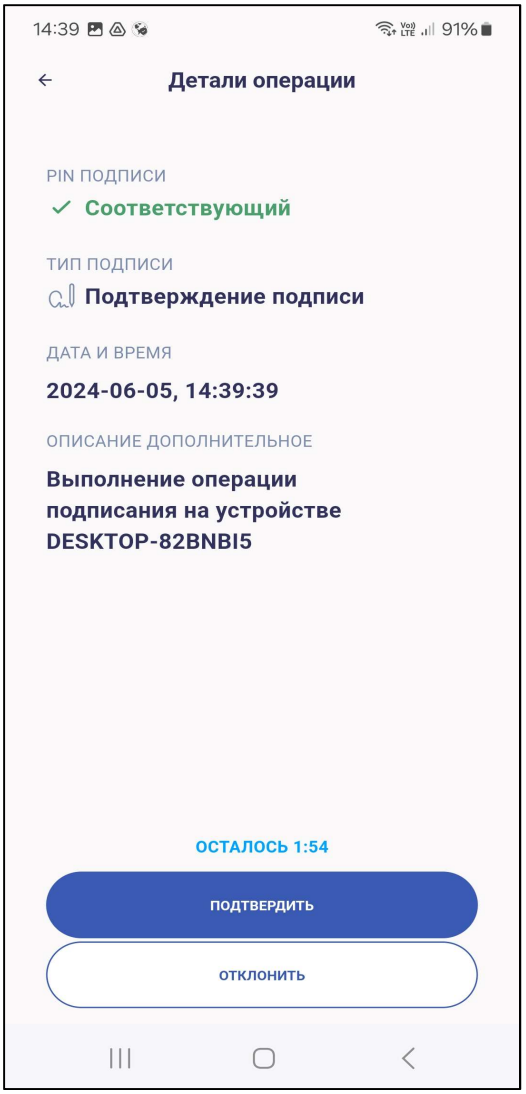


Рис. 36 Подтверждение проведения операции электронной подписи

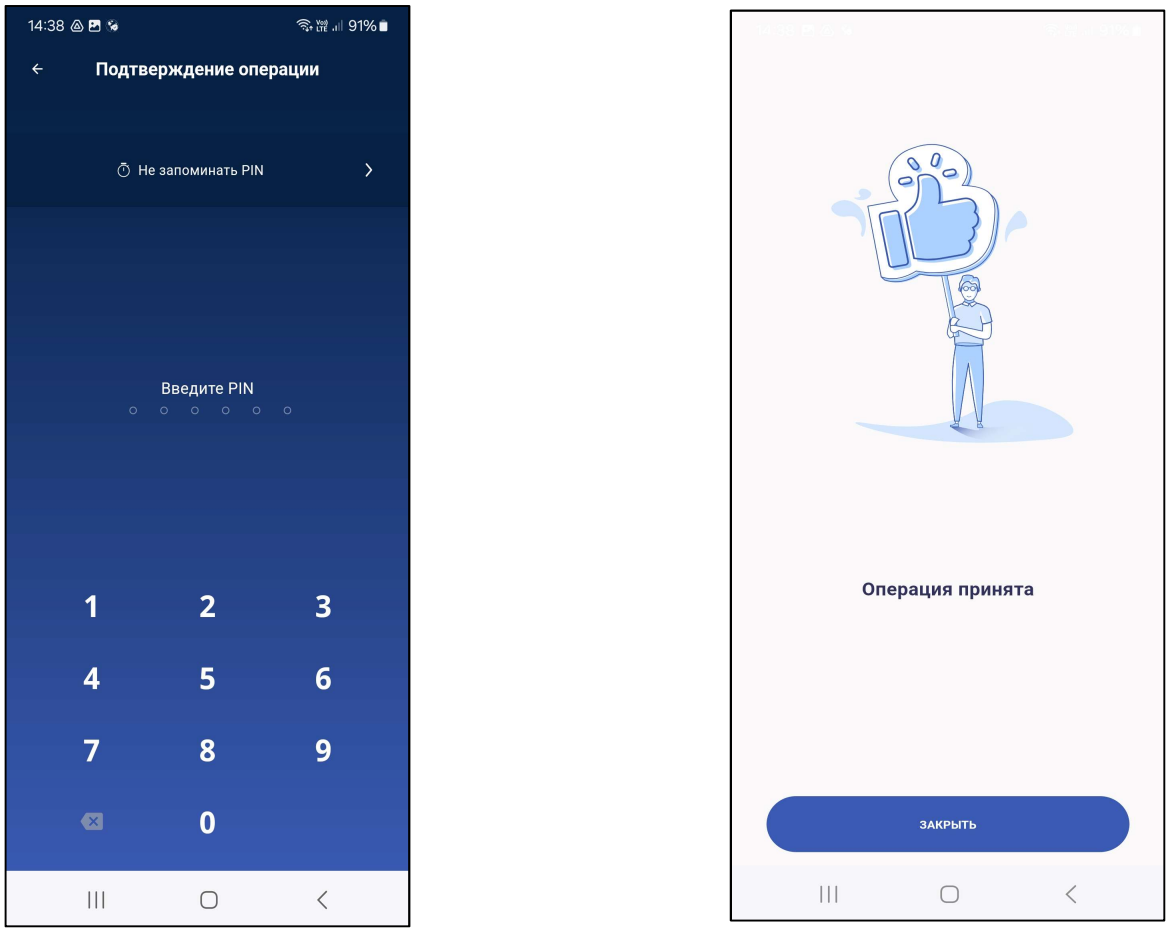


Рис. 37 Окно ввода PIN и подтверждения операции подписи (телефон)

Отобразится экран ввода ПИН-кода. После его ввода дождитесь подтверждения операции – если код введен правильно, процедура будет принята и появится окно, как показано на **Окно ввода PIN и подтверждения операции подписи (телефон)**.

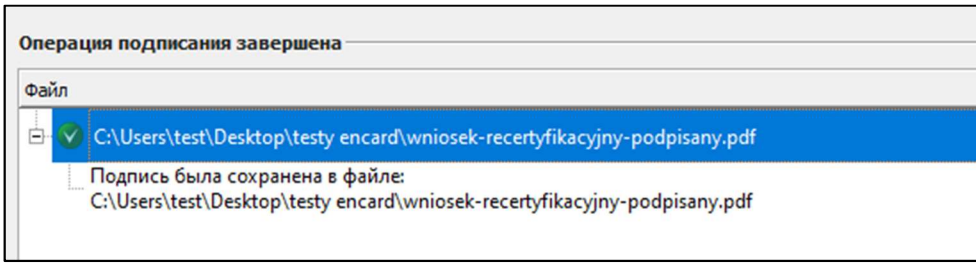


Рис. 38 Подтверждение операции подписи (компьютер)

Компьютерная программа выведет информацию о правильности подписания документа (**Рис. 38 Подтверждение операции подписи (компьютер)**).

5.3 ПРОВЕРКА ПОДПИСИ В ПРОГРАММЕ

Чтобы проверить подпись, после запуска программы нажмите значок *Проверить* (в левой части окна, на панели *Основные функции*).

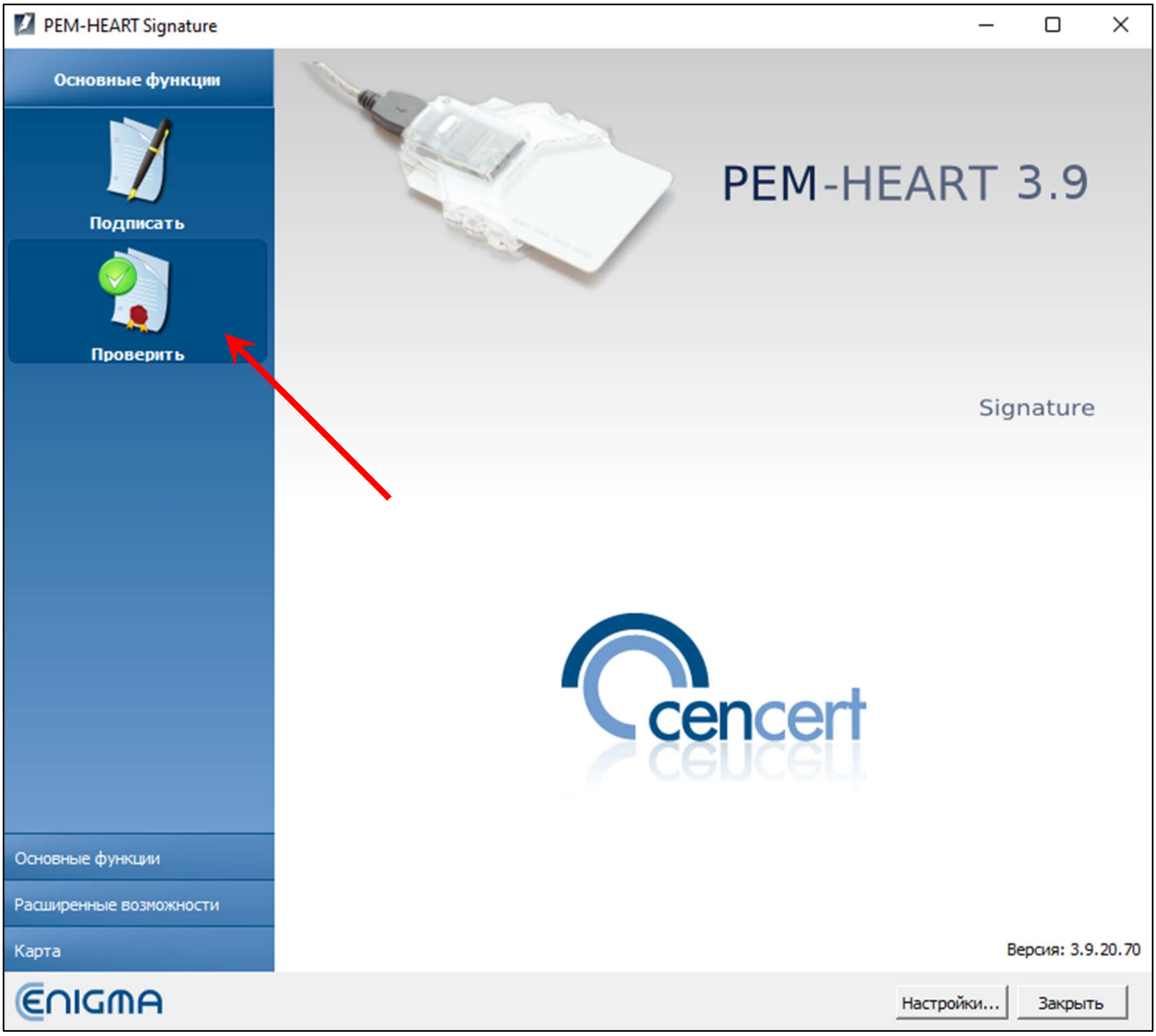


Рис. 39 Главное меню приложения PEM-HEART Signature — выбор опции Проверить

Откроется окно, позволяющее выбрать файлы для проверки. Вы можете добавить один или несколько файлов для проверки (кнопка *Добавить файл*) или перетащить файл в окно списка файлов. Если выбрать весь каталог (кнопка *Добавить каталог*), программа включит все файлы из этого каталога и его подкаталогов в список проверяемых файлов. После добавления всех файлов нажмите кнопку *Проверить*.

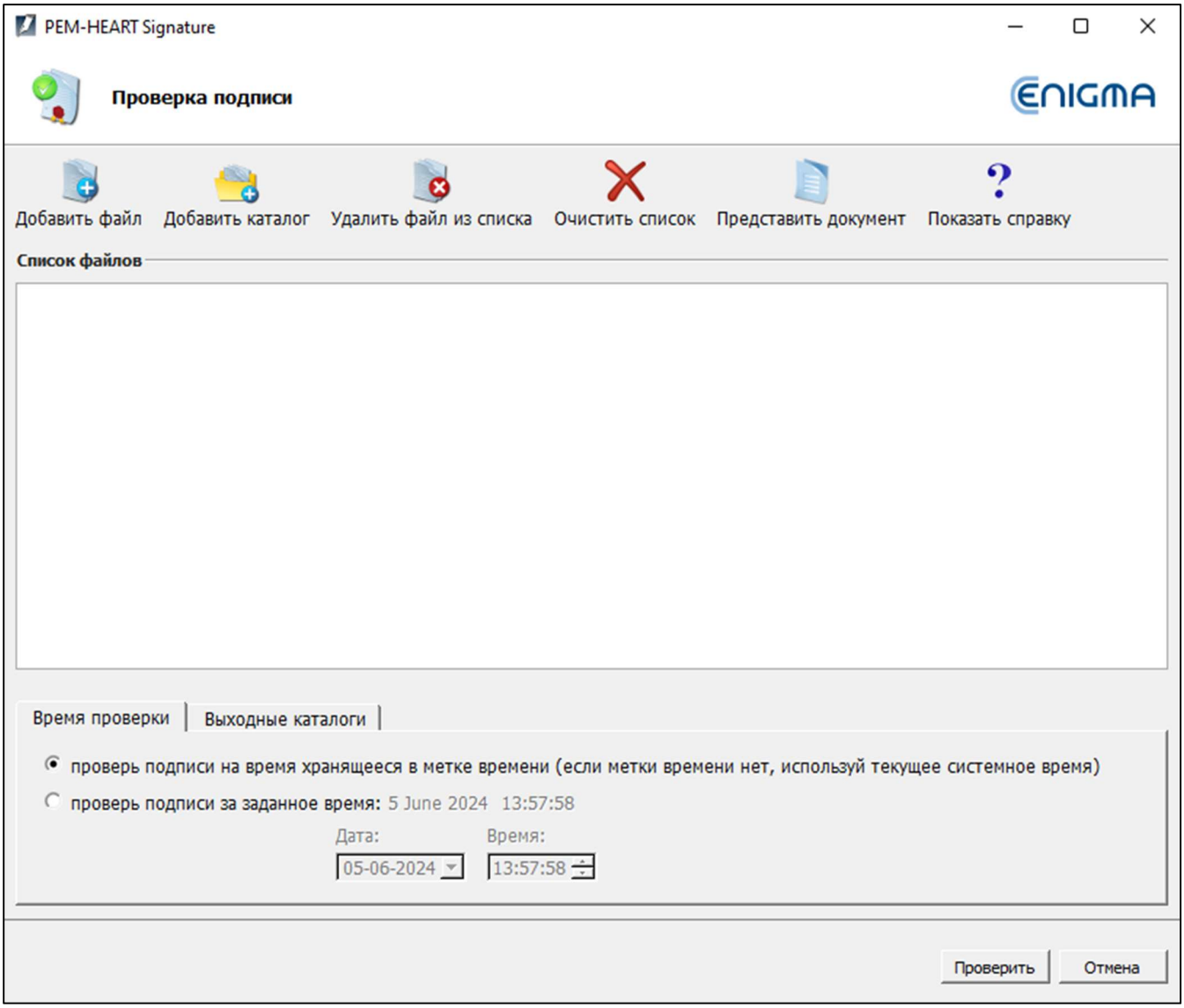


Рис. 40 Окно проверки электронной подписи

Программа проверит сохраненные в документе подписи и отобразит результат проверки.

Более подробную информацию о проверке можно найти в **4.3 ПРОВЕРКА ПОДПИСИ**.

6 РАСШИРЕННЫЕ ВОЗМОЖНОСТИ

Рис. 41 Главное меню приложения PEM-HEART Signature – расширенные возможности

6.1 КОНТРПОДПИСЬ

Контрподпись — особый способ подписания, при котором подпись технически ставится не под самим документом, а под предыдущими подписями (документ подписывается косвенно). Этот тип подписи предотвращает удаление предыдущих подписей из документа. В случае стандартных множественных подписей технически возможно удалить одну из предыдущих подписей из документа, сохранив при этом действительность остальных подписей («Контрподпись» делает это невозможным).

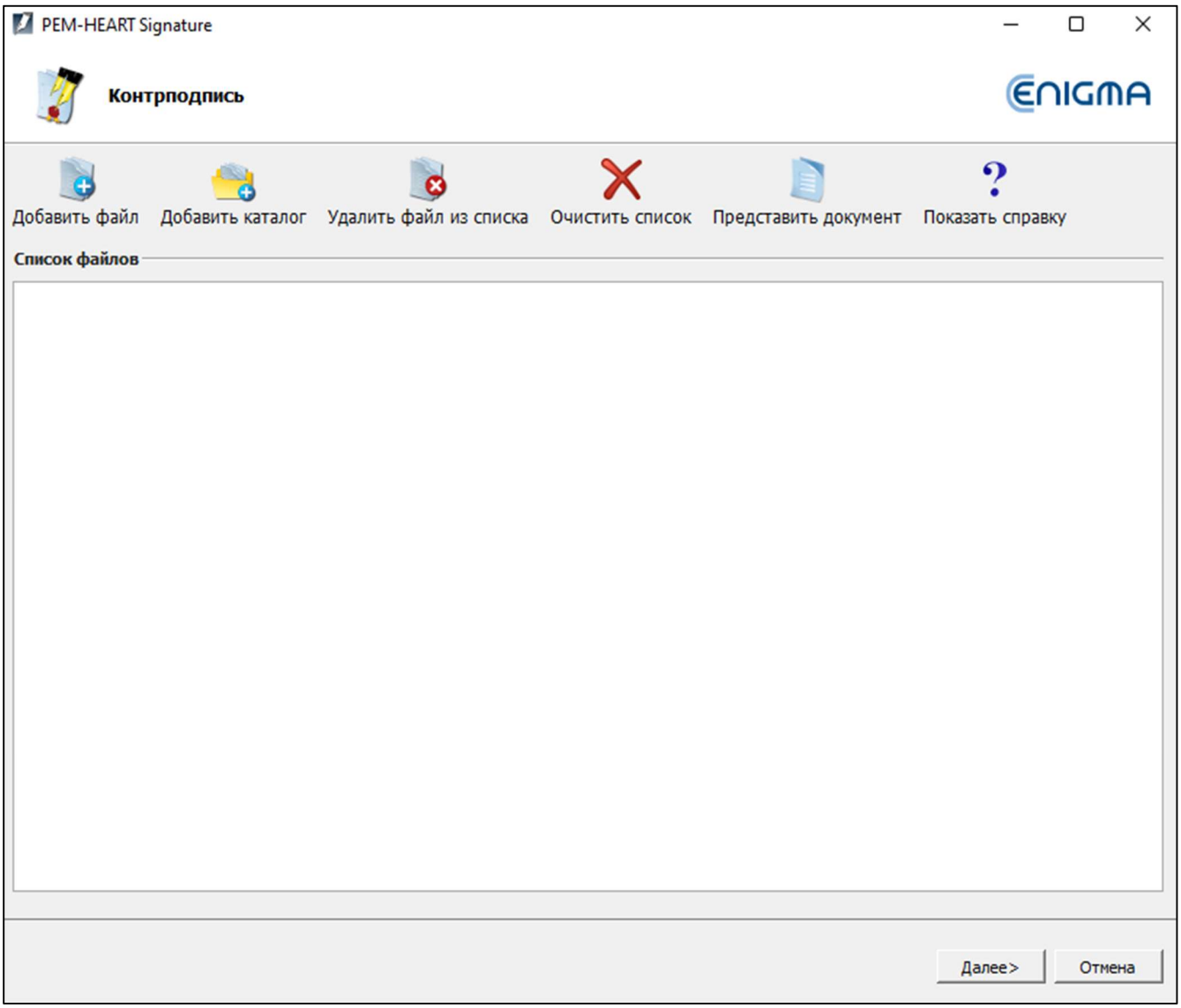


Рис. 42 Окно подачи контрподписи

Термин «контрподпись» в приведенном выше значении не следует путать с этим же термином, используемым в законном обороте. Предоставление электронной подписи в качестве «контрподписи» (в смысле, описанном выше) не разрешено законодательными положениями, касающимися электронных подписей. В целом применяются положения, касающиеся электронных подписей. В юридическом смысле «контрподпись», описанная в этом документе, действует на тех же принципах, что и любая другая электронная подпись..

6.2 ОТМЕТКА ВРЕМЕНИ

Квалифицированная временная метка свидетельствует о существовании документа в данный момент времени. В польском законодательстве судебное

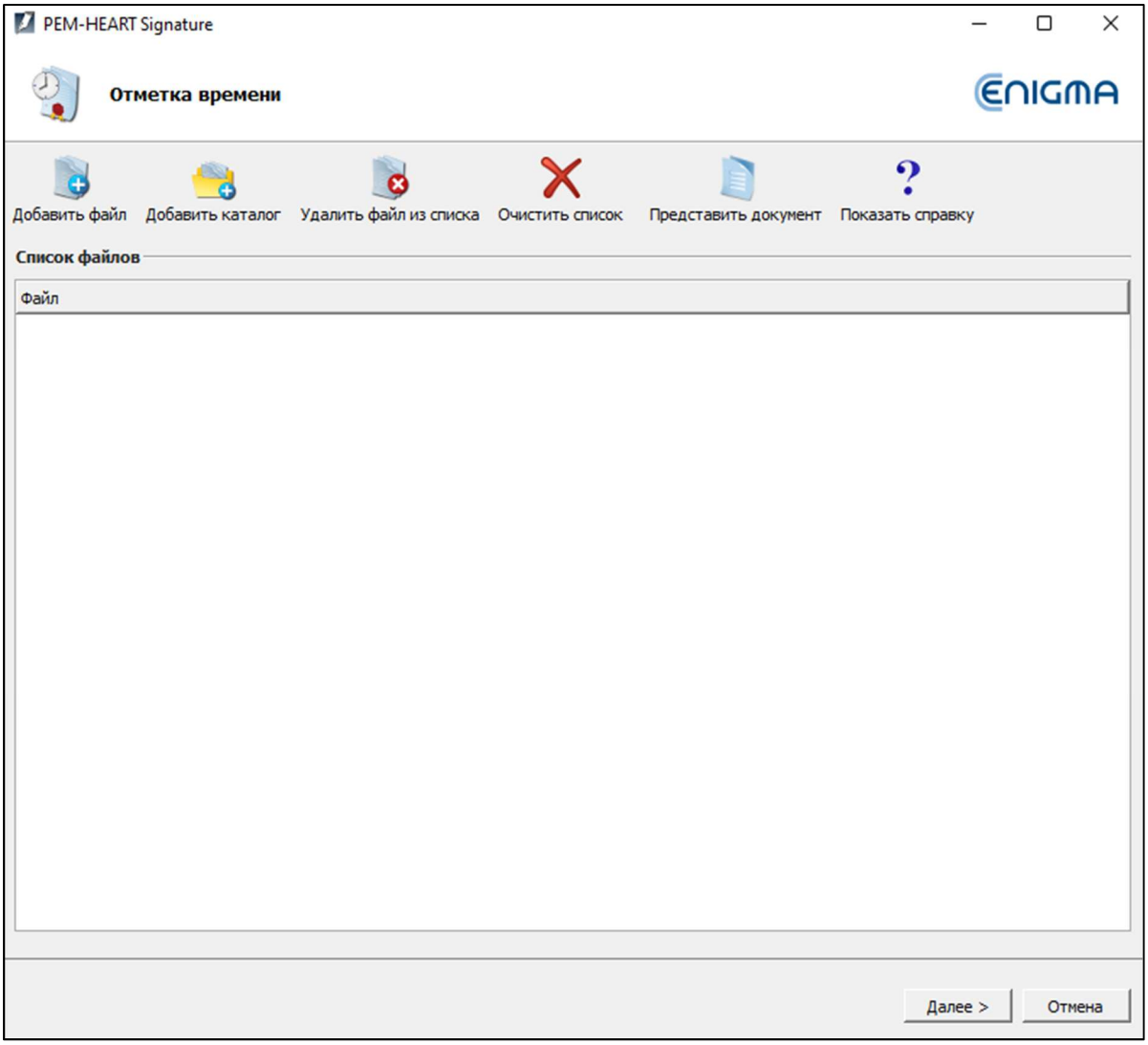


Рис. 43 Окно применения временной метки к электронной подписи

действие с определенной отметкой времени имеет «определенную дату». На всей территории ЕС (согласно регламенту eIDAS) квалифицированная электронная отметка времени имеет презумпцию точности даты и времени, которые она указывает, а также целостности данных, с которыми связаны указанные дата и время.

Если для подписи используется временная метка, она удостоверяет не только существование подписанного документа, но и саму подпись, что защищает от юридических последствий последующего отзыва сертификата, использованного для подписи.

Временная метка может быть прикреплена к подписи и позже, даже получателем документа (на самом деле, получатель документа зачастую больше заинтересован в возможности длительной корректной проверки подписи). Также стоит рассмотреть более совершенные формы подписи – т.е. *long* и *архивную* (см. Главу **4.3.1 ПАНЕЛЬ ПРОВЕРКИ**). Эти формы также могут использовать временные метки, но они дополняют их другими данными, необходимыми для проверки.

В меню выберите *Расширенные возможности* (панель в левой части главного окна) и нажмите значок *Отметка времени*.

Появится окно, позволяющее указать файлы и/или каталоги, как при подписании, так и при проверке подписи. После выбора файлов и нажатия кнопки *Далее* программа запрашивает ПИН-код карты (чтобы подписать запрос отметки времени) или ПИН-код rSign, затем добавляет временную метку к каждой подписи, содержащейся в этом файле.

Внимание: Для загрузки меток времени может потребоваться приобретение пакета меток времени.

6.3 ПОДПИСАНИЕ XML-ДОКУМЕНТА С ВЛОЖЕНИЯМИ

По умолчанию, когда программа подписывает XML-документ заверенной подписью *(XAdES enveloped),* она помещает подпись в конец структуры документа. В подавляющем большинстве случаев такое поведение программы является достаточным и соответствует требованиям систем, использующих подписи. Однако если есть необходимость разместить подпись внутри документа по-другому, воспользуйтесь опцией Подписать XML-документ с вложениями. Использование этой опции предназначено для опытных пользователей и требует знания структуры XML-файлов, в частности знания документации *XML Pointer Language (XPointer).*

Выберите вкладку *Расширенные возможности* в меню (панель в левой части главного окна) и нажмите значок *Подписать XML-документ с вложениями*. Когда программа отобразит окно добавления файлов в подпись, выберите XML-файл (в файле опционально могут быть указаны вложения). Если подпись должна быть размещена не в конце файла, то необходимо указать соответствующее место в структуре XML-документа. В таком случае пользователь должен выбрать опцию Добавить новое... в разделе Место подписи, после чего отобразится окно настройки места подписи.

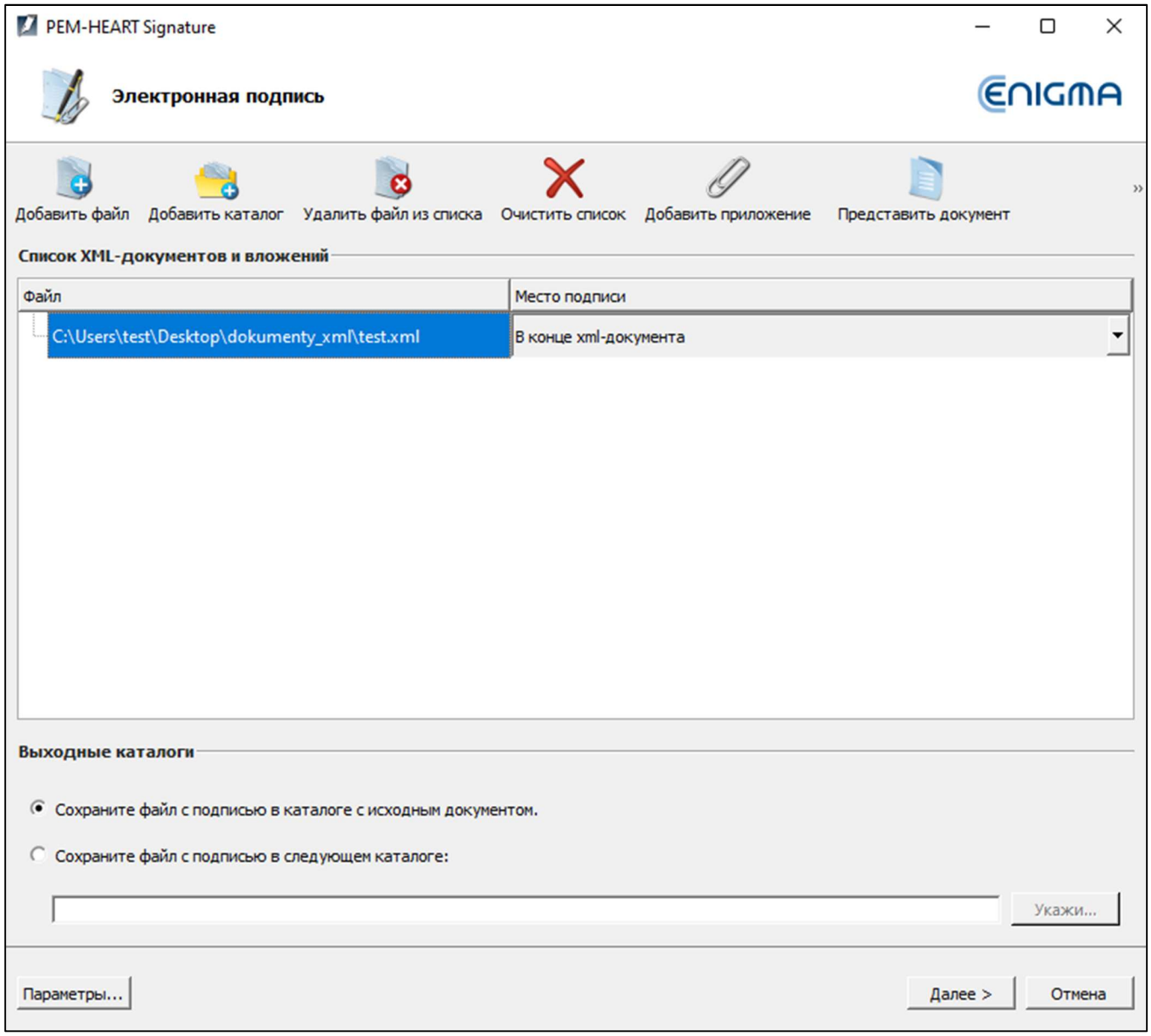


Рис. 44 Подписание XML-документа с вложениями – переходим к настройке места подписи

Затем в следующем окне нажмите кнопку, введите имя вашей конфигурации, укажите структуру xpointer и, при необходимости, описание заданной конфигурации. Структура *xpointer* определяется в виде: xpointer([*указывающий на узел XML*]). Доступные формы указания этого места описаны в документации *XML Pointer Language (XPointer),* доступной, среди прочего, по адресу: на страницах http://www.w3.org/TR/WD-xptr.

После завершения подписания появится сводное окно. Создание подписи в формате конверта XAdES *(XAdES enveloped)* не меняет расширение XML-файла или его структуру.

7 ПОДДЕРЖКА КРИПТОГРАФИЧЕСКИХ КАРТ В ПРОГРАММЕ

7.1 СМЕНИТЬ PIN-КОД

(Функция недоступна для rSign) Чтобы изменить ПИН-код карты, выберите вкладку *Карта* в главном меню (панель в левой части главного окна) и нажмите значок *Сменить PIN-код*.

Рис. 45 Главное меню приложения PEM-HEART Signature – выбор вкладки «Карта»

Далее необходимо указать токен, для которого необходимо изменить PIN.

Внимание:

- Для карт IDEMIA: объекты, относящиеся к квалифицированной подписи, всегда помещаются в первый жетон сверху; оставшиеся жетоны можно использовать для других целей, например, для электронной печати.
- Для карт IDPrime: объекты, относящиеся к квалифицированной подписи, всегда размещаются на втором жетоне сверху – он называется „Digital Signature PIN”.

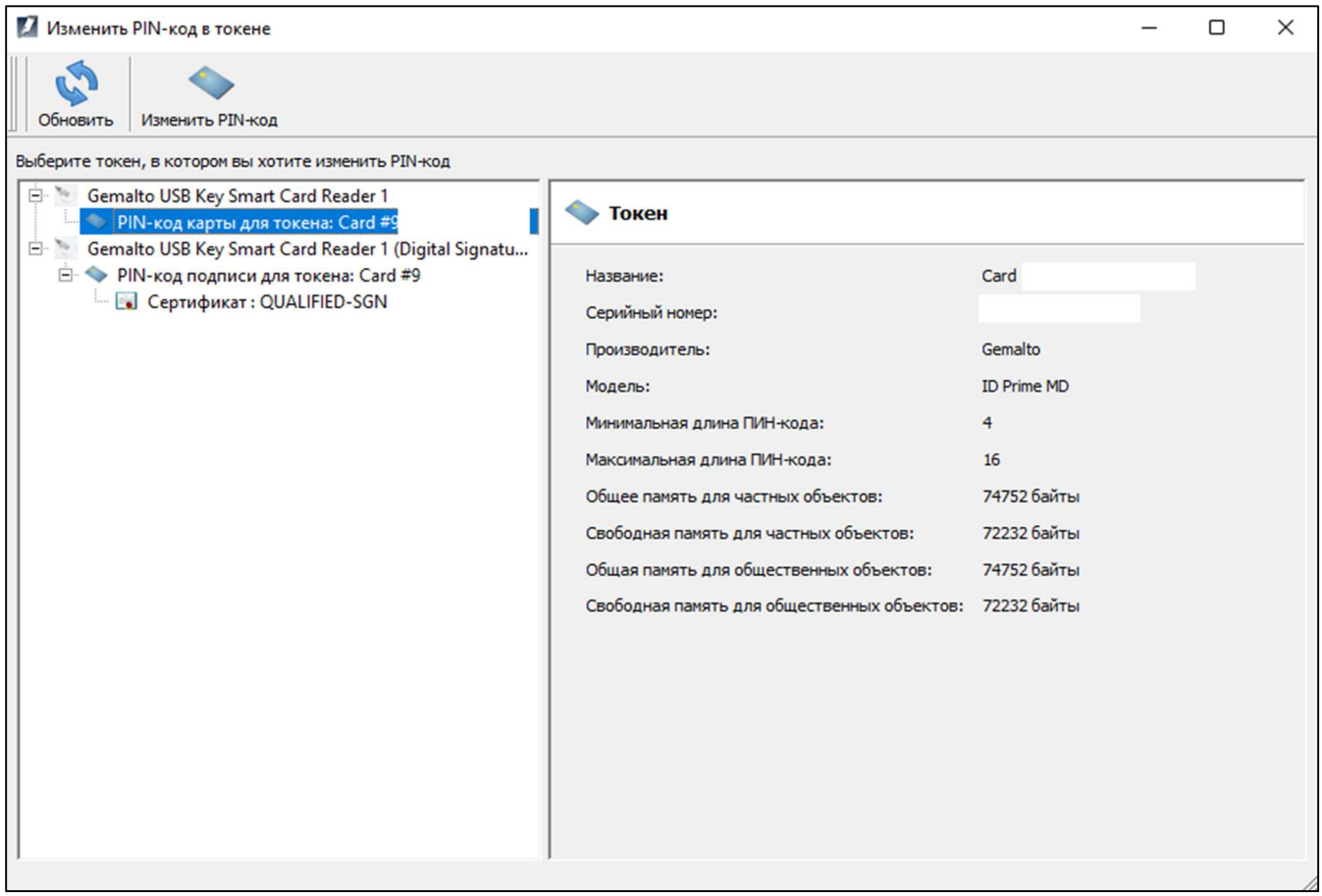


Рис. 46 Пример экрана программы для карты Thales типа A

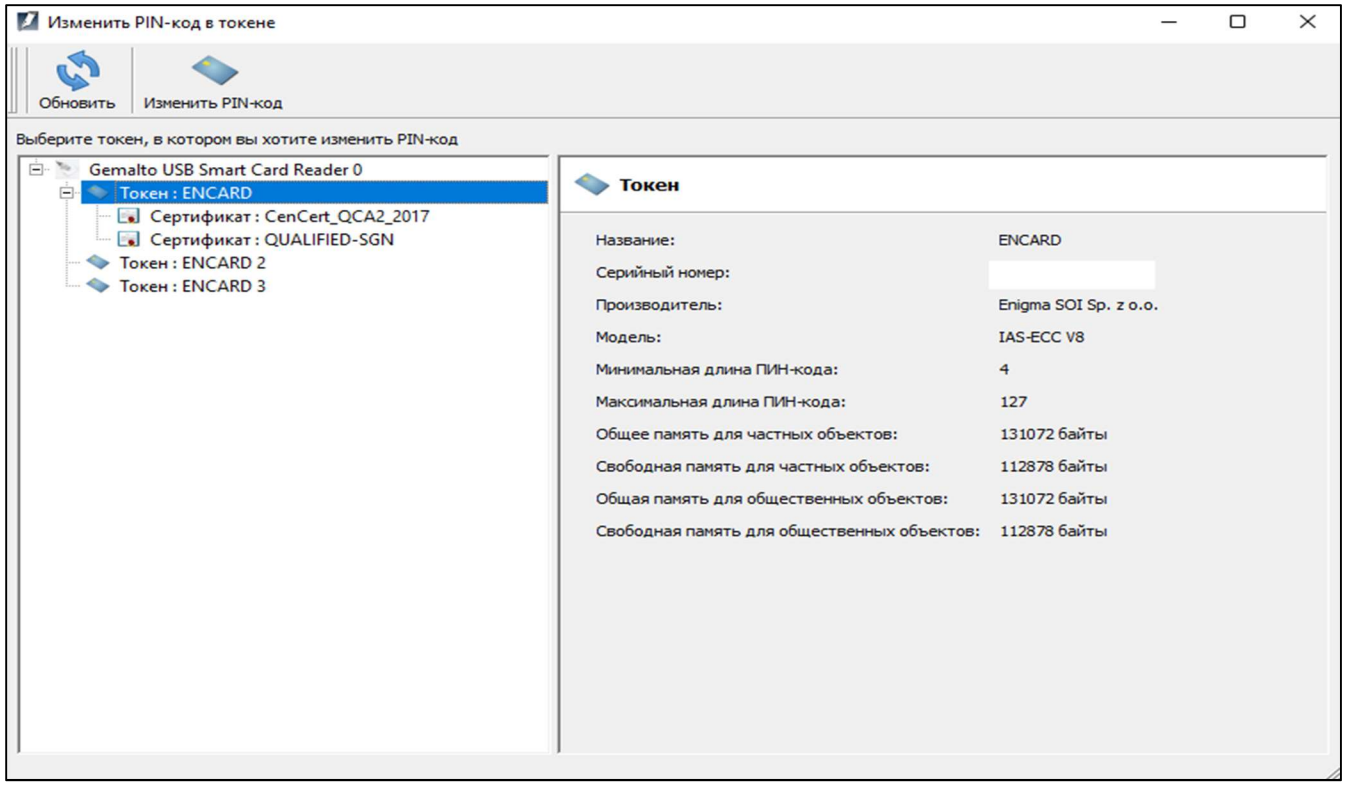


Рис. 47 Пример экрана программы для карты IDEMIA Encard

Чтобы внести изменения, пользователь выбирает опцию «Сменить PIN-код», расположенную над списком токенов. Чтобы изменить код, необходимо ввести правильный текущий ПИН-код и дважды ввести новый код. Не рекомендуется использовать в качестве ПИН-кода польские буквы или другие символы, которые могут быть неправильно введены из-за разных языковых настроек клавиатуры компьютера (карта блокируется после 3-х попыток ввода неправильного кода). Рекомендуется записать ПИН-код в надежном месте (отдельно от карты), исключением является ПИН-код для карт thales (первый токен), в этом случае он будет заблокирован после 5 попыток.

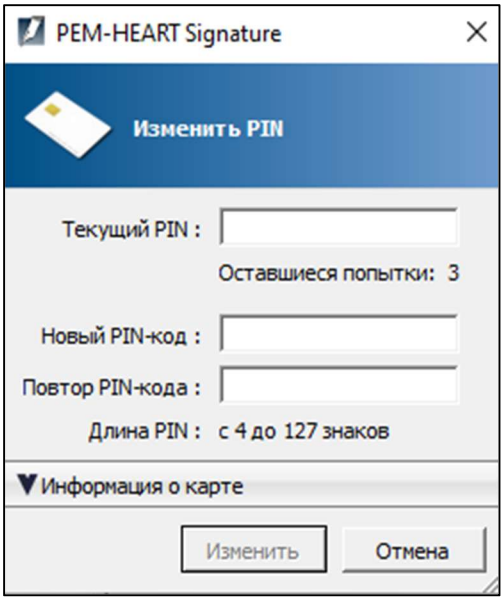


Рис. 48 Экран смены PIN-кода карты IDEMIA

Внимание! Если PIN-код заблокирован, разблокировать карту можно только с помощью PUK-кода.

PIN/PUK-коды присваиваются пользователем при активации карты. Cencert не имеет PIN/PUK-кодов и невозможно разблокировать карту из-за неправильного PIN/PUK-кода.

7.2 РАЗБЛОКИРОВКА КАРТЫ

(Функция недоступна для rSign) Если карта заблокирована после ввода слишком большого количества неправильных PIN-кодов, ее можно разблокировать с помощью PUK-кода. PUK-код присваивается пользователем при активации карты. После использования кнопки *Разблокировать* карту откроется окно с выбором токенов.

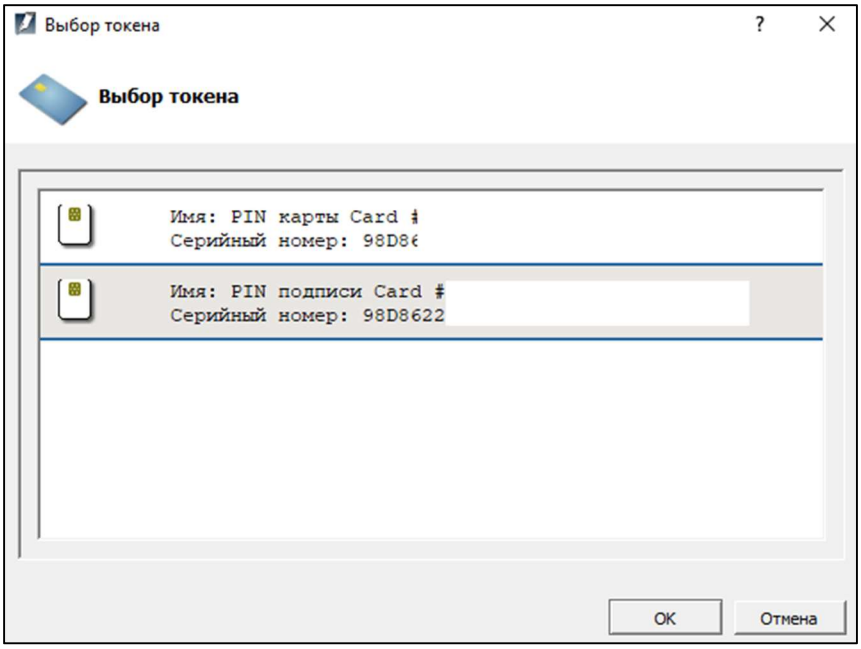


Рис. 49 Разблокировка карты - выбор токена - карта IDPrime

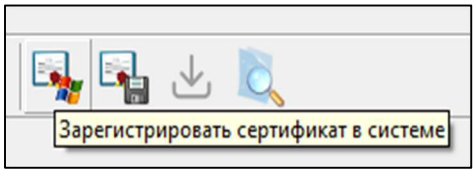
После правильного ввода PUK-кода можно будет установить новый PIN-код и карта будет разблокирована.

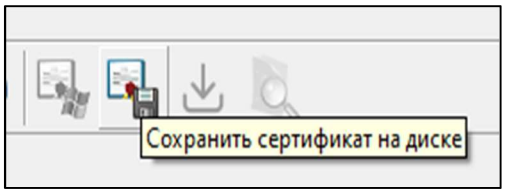
Внимание!! Количество попыток разблокировки карты с помощью PUK-кода ограничено. При неправильном заполнении данных при каждой попытке карта блокируется навсегда и дальнейшее ее использование невозможно.

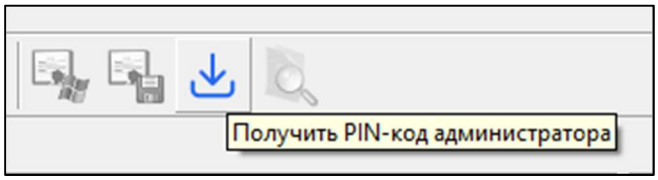
PIN/PUK-коды присваиваются пользователем при активации карты. Centert не имеет PIN/PUK-кодов и не может помочь, если ваша карта заблокирована из-за неправильного PIN/PUK-кода.

7.3 ДИАГНОСТИКА

Панель *Диагностика* отображает дополнительную информацию о данных сертификата, позволяет сохранить сертификат в файл, зарегистрировать его в Windows, загрузить PIN-код администратора (только для карт IDPrime) и включить ведение журнала (только для карт IDEMIA и rSign – функция описана в **10.1 ЖУРНАЛЫ РАБОТЫ КАРТЫ ДЛЯ СИСТЕМ WINDOWS**).







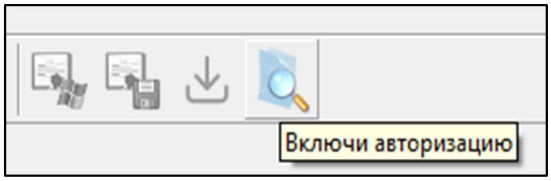


Рис. 50 Дополнительные параметры на экране Диагностика

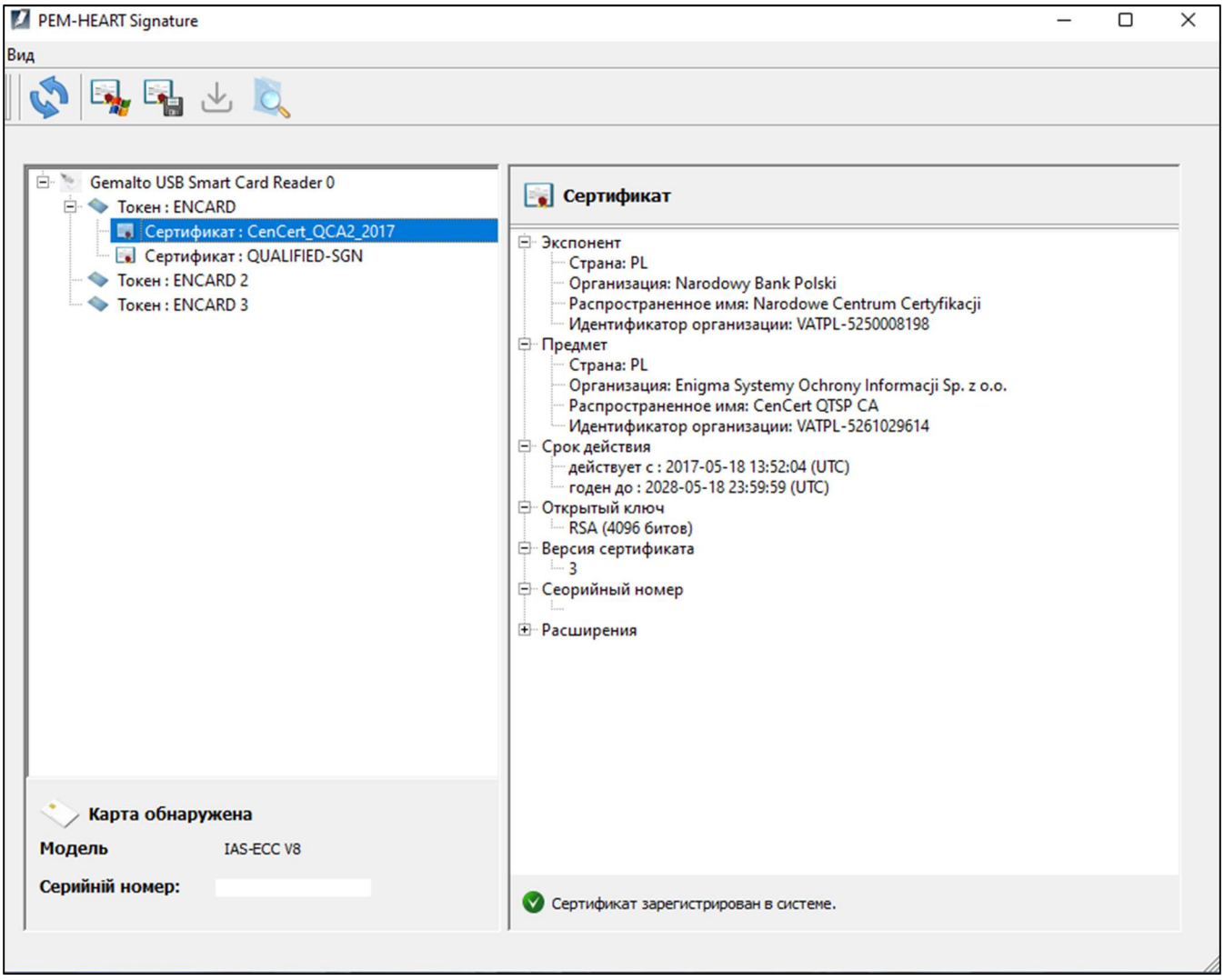


Рис. 51 Вид открытой панели Диагностики - отображение токена с карты и rSign

7.4 ДОПОЛНИТЕЛЬНЫЕ ОПЦИИ

7.4.1 ПРОДЛЕНИЕ СЕРТИФИКАТА

Вы будете перенаправлены и откроете программу продления сертификата PEM-HEART. Ссылка на страницу руководства пользователя: https://www.cencert.pl/poradnik-uzytkownika/

7.4.2 КОНФИГУРАЦИЯ RSIGN

Программа конфигурации PEM-HEART rSign перенаправляется и открывается.

8 НАСТРОЙКИ ПРОГРАММЫ

Внимание!

Все операции по изменению параметров будут сохранены в памяти программы после их сохранения с помощью кнопки *Сохранить* в правом нижнем углу меню программы.

8.1 ИЗМЕНЕНИЕ ПАРАМЕТРОВ ПОДПИСИ

Чтобы изменить параметры подписи, нажмите кнопку в главном окне программы **Настройки** (находится в правом нижнем углу экрана приложения, рядом с кнопкой **Закрыть**). Появится новое окно настроек с открытой вкладкой **Подписание**. Все параметры, определяющие формат подписи (XAdES, CAdES, PAdES, ASiC) будет применено к файлам с расширением, выбранным в данный момент в списке *расширений*. Все файлы с расширениями *.* (поэтому все файлы, кроме тех, которые указаны в списке под этим расширением), будут подписаны в формате по умолчанию XAdES в отдельном файле. При этом файлы *.PDF и *.XML имеют свои собственные форматы подписи по умолчанию, которые будут видны после выбора в списке строки *.PDF или *.XML соответственно.

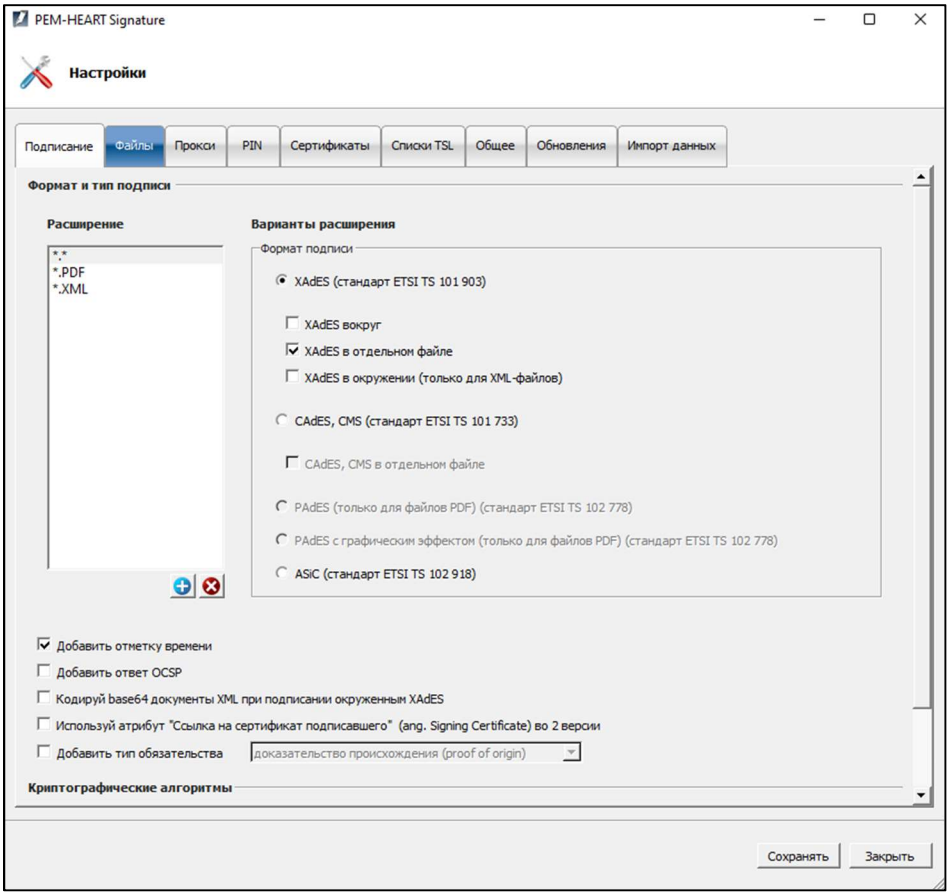


Рис. 52 Окно изменения настроек подписи

Здесь вы можете добавить (или удалить) расширения файлов (с помощью значков и), для которых должен использоваться другой формат подписи по умолчанию. Например, добавив новый элемент «*.docx» и определив, что для этих файлов должна быть сделана подпись, например CAdES и CMS, в отдельном файле, а затем для того, чтобы инициировать подпись для каждого файла с документом Ms Word. (*.docx), программа по умолчанию предложит подпись в форматах CAdES и CMS в отдельном файле.

В разделе ниже, посвященном выбору расширения и настройке формата подписи для данного расширения, есть дополнительные параметры подписей. Эти настройки применяются ко всем подписям — независимо от имени файла.

Опция *Добавить временную метку* означает, что к каждой подписи будет добавлена временная метка (**Внимание!** Для правильной работы вам может потребоваться приобрести пакет временных меток).

Параметр *Добавить ответ OCSP* означает, что помимо отметки времени (флажок *Добавить временную метку* разблокирует опцию *Добавить ответ OCSP*) к подписи

будет добавлена информация о статусе сертификата, используемого для подписи (при этом создается подпись long — см. также глава **4.3.1 ПАНЕЛЬ ПРОВЕРКИ**).

Параметр *Кодировать документы xml в формате base64* при создании подписи вокруг XAdES необходим в определенных ситуациях, когда система, проверяющая подписанные документы, имеет ограниченные возможности для проверки различных форматов подписей и требует этого.

Параметр Использовать атрибут *Сертификат подписи* в версии 2 помещает ссылку на сертификат в подпись в формате, совместимом с новыми версиями стандартов ETSI в отношении формата подписи. Выберите этот вариант, если этого требует система проверки подписи, использующая только новые форматы.

При выборе опции *Добавить тип обязательства* добавляется подписанный атрибут, указывающий цель (в какой роли) подписывающая сторона (например, «официальное одобрение» или «подтверждение получения» и т. д.).

Параметр *Алгоритм хеширования* указывает криптографический алгоритм хеширования, используемый для выдачи подписи. Программа позволяет вам выбирать только из хороших алгоритмов, которые гарантируют адекватную безопасность (когда данная версия программы актуальна).

8.2 ФАЙЛЫ

Вкладка содержит параметры настройки каталогов вывода обрабатываемых документов. По умолчанию программа обрабатывает документы в том же каталоге, где находится документ. Можно определить другие каталоги, в которых будут сохраняться подписанные или проверенные документы.

Чтобы определить каталог, установите флажок перед описанием опции, после чего будет активирована кнопка *Указать*, с помощью которой можно указать данный каталог в файловой системе.

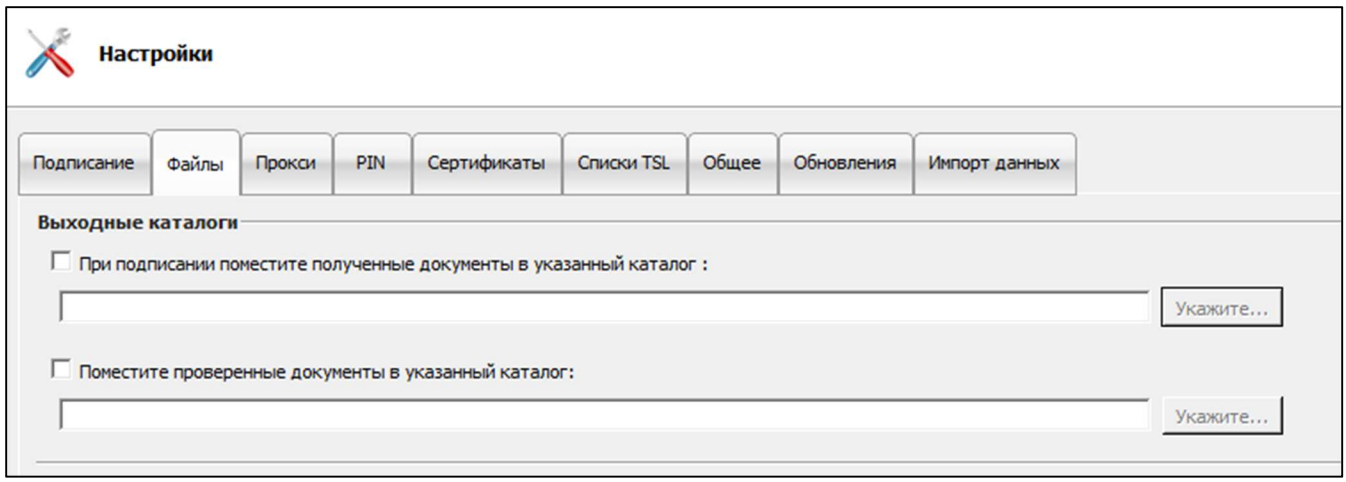


Рис. 53 Определение выходных каталогов для обработанных документов

8.3 ПРОКСИ

Вкладка используется для определения подключения к прокси-серверу. Есть две возможные конфигурации на выбор:

- *Использовать системные настройки* (только для систем Windows) – вариант по умолчанию, конфигурация загружается из настроек системы (реестра)

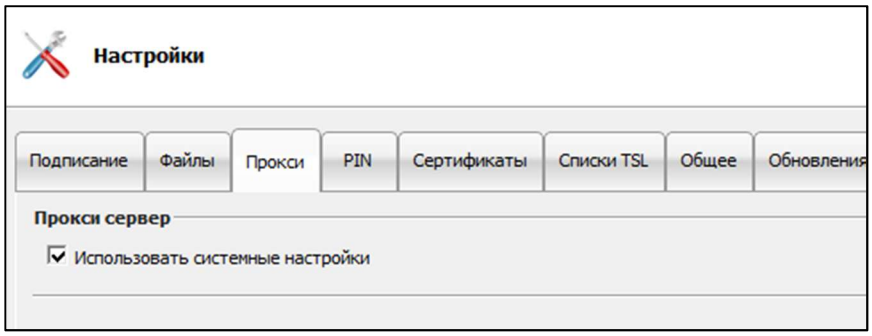


Рис. 54 Прокси-сервер – настройки системы

- *Настроить прокси* – ручная настройка конфигурации, указание адреса порта и/или аутентификационных данных. Пожалуйста, заполните все обязательные поля для данного прокси-сервера. Активация настроек подтверждается кнопкой *Сохранить* в правом нижнем углу программы. *Аутентификация* прокси-сервера здесь является дополнительной версией и не требуется.

Неправильная конфигурация сервера приводит к тому, что программа не имеет доступа к Интернету (невозможно скачать временную метку, возможно, не удастся проверить подписи).

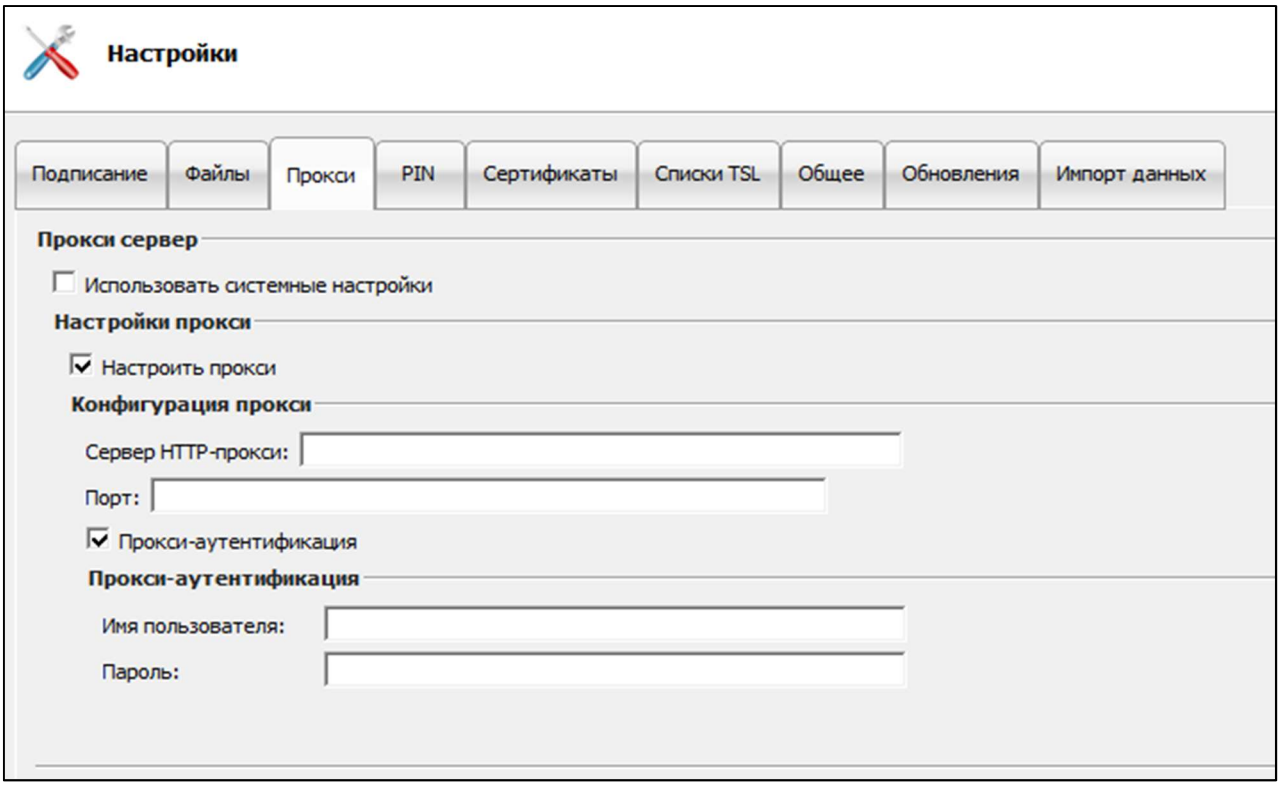


Рис. 55 Прокси-сервер – ручные настройки

8.4 PIN

Вкладка PIN предназначена для настройки возможности запоминания

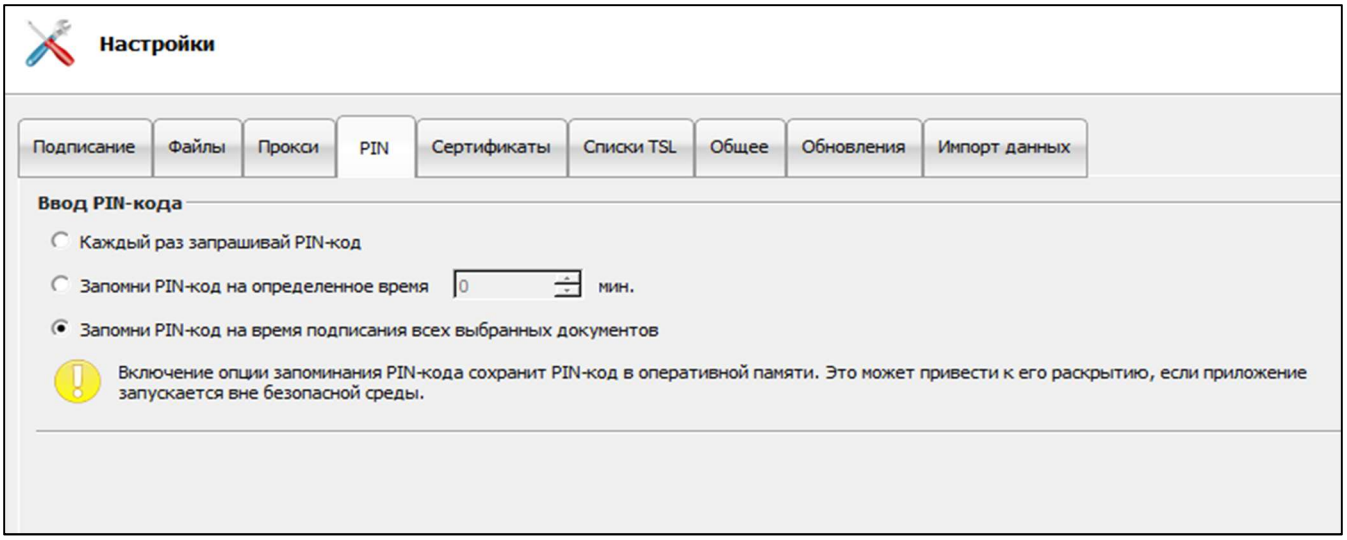


Рис. 56 Настройки PIN-кода

программой PIN-кода криптографической карты.

Внимание! Эта опция не применяется к подписям rSign (в облаке). Для этого типа подписи настройки настраиваются в мобильном приложении.

По умолчанию PIN-код запоминается на время подписи всех документов в окне подписи. Чтобы подписать все файлы в окне программы, вам нужно ввести PIN-код только один раз - после подписания повторный выбор файлов для подписи (даже без закрытия программы) означает, что вам нужно будет ввести PIN-код еще раз. Также можно установить другие параметры: PIN-код всегда будет предоставляться для каждого отдельного документа или он будет сохраняться в памяти компьютера в течение определенного периода времени.

8.5 СЕРТИФИКАТЫ

Вкладка касается представления, регистрации в системе и экспорта сертификата пользователя. Если в считыватель вставлена карта, программа автоматически прочитает с нее данные и они отобразятся в окне. Если сертификат не читается, проверьте размещение карты и воспользуйтесь кнопкой *Загрузить*. Если токен rSign установлен в системе, он также будет отображаться в списке после действия *Загрузить*.

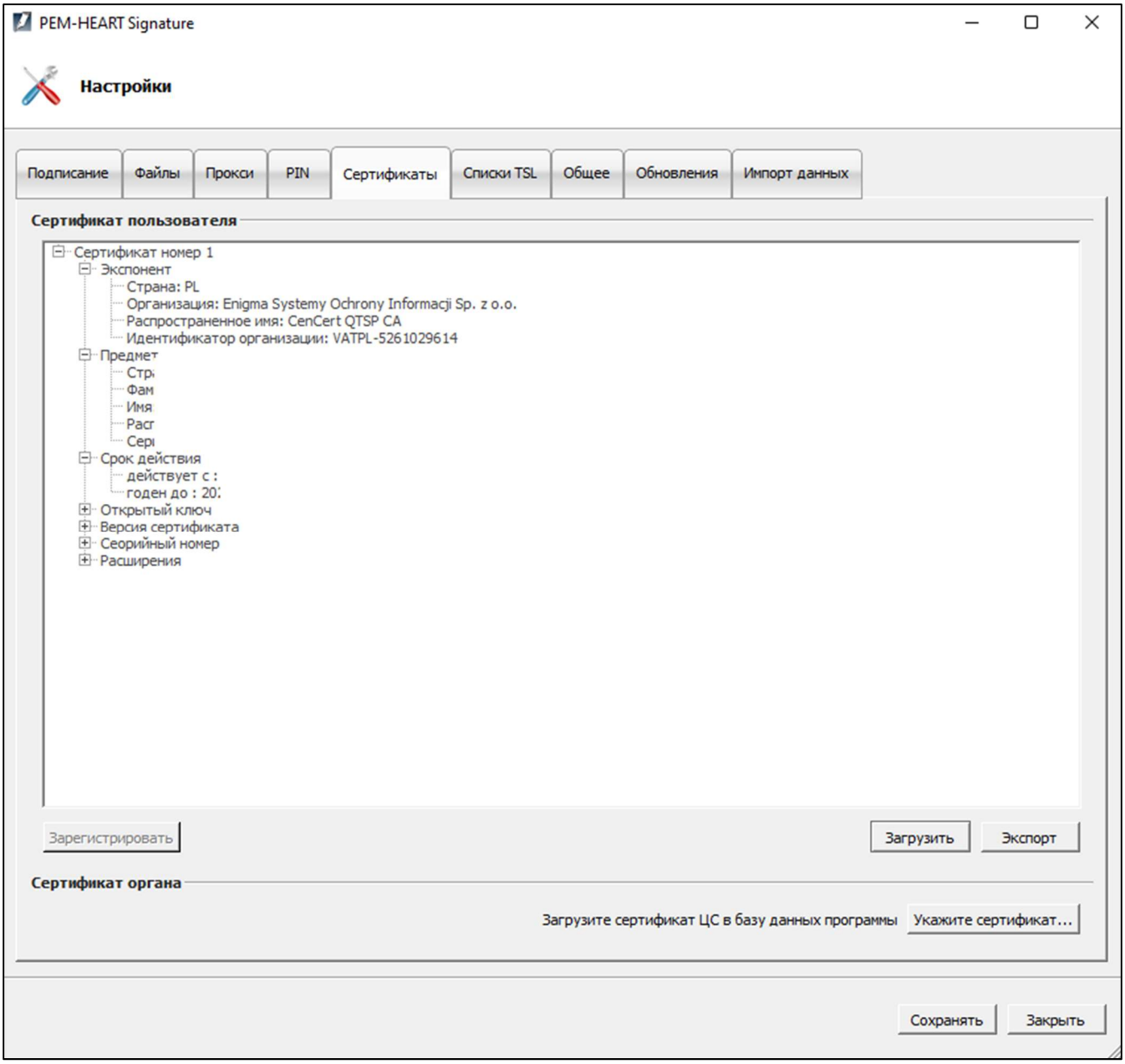


Рис. 57 Настройки сертификата пользователя

Кнопка *Зарегистрировать* предназначена для регистрации считанного с носителя сертификата в системном хранилище. Экспортировать сертификат в файл можно с помощью кнопки *Экспорт*. Раздел *Сертификат центра* используется для указания и загрузки такого сертификата поставщика услуг доверия в базу данных программы. Опция используется в специфических ситуациях, касающихся неквалифицированных подписей - когда у программы нет в базе данных действующего сертификата *промежуточного органа* поставщика услуг доверия.

8.6 СПИСКИ TSL

Списки TSL содержат все необходимые данные о квалифицированных поставщиках трастовых услуг в ЕС (включая польских). Они позволяют проверять подписи, сделанные с использованием квалифицированных сертификатов, выданных польскими и другими поставщиками трастовых услуг ЕС.

На вкладке отображается текущий статус списков TSL, доступных в программе. Также предусмотрена возможность ручной загрузки текущих списков TSL, выпущенных в отдельных странах (однако для нормальной работы загрузка вручную не требуется, поскольку программа автоматически загружает новые

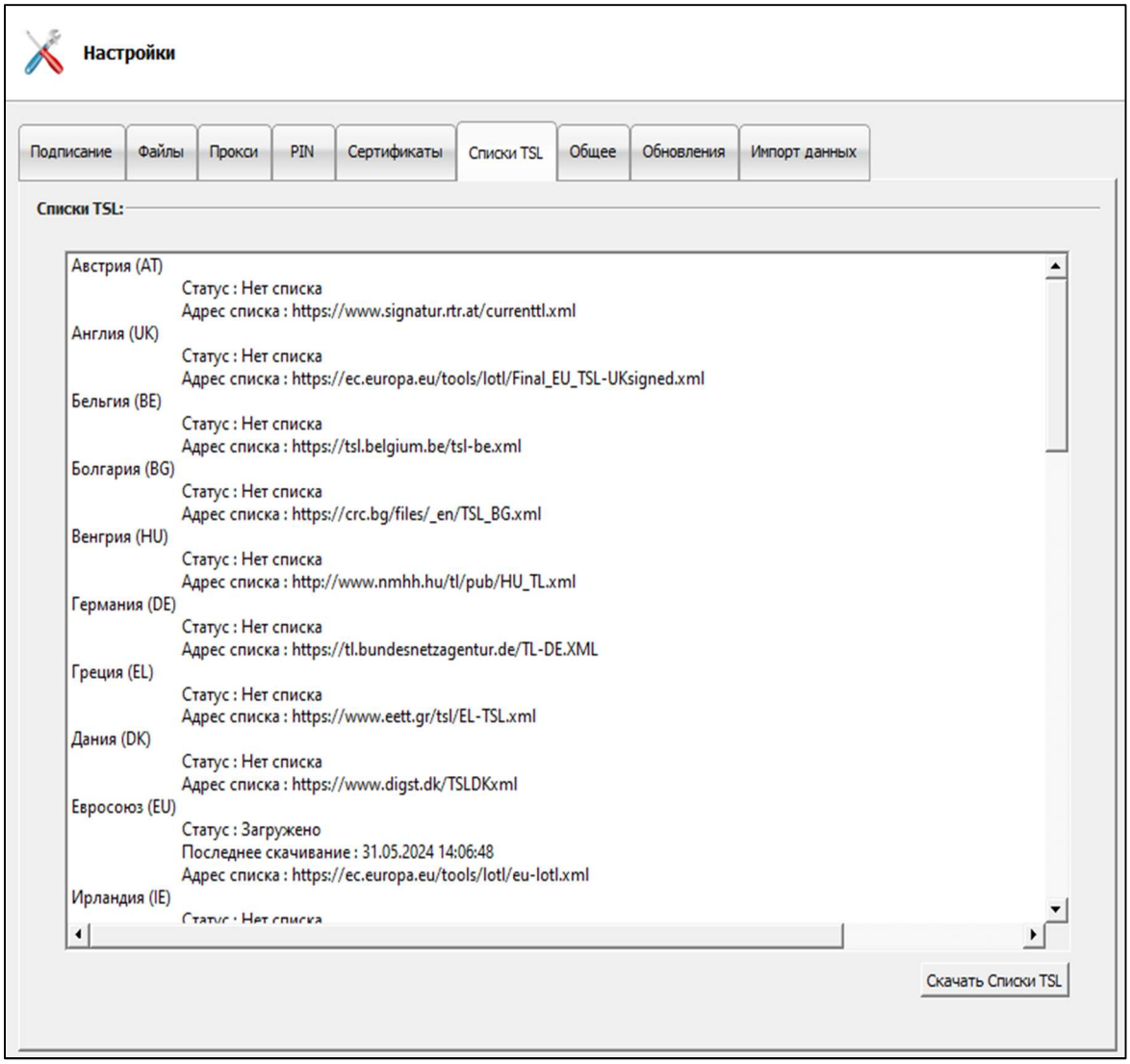


Рис. 58 Настройки – списки TSL

списки TSL, если при проверке подписи она встречает сертификат, который невозможно проверить на основании списков TSL, доступных на данный момент программе). Чтобы загрузить списки TSL, нажмите кнопку *Загрузить списки TSL*.

8.7 НАСТРОЙКИ ЯЗЫКА

Изменить язык программы можно через вкладку *Общие* панели *Настройки*. Языки на выбор: *польский, английский, украинский, русский*.

Параметр *Использовать встроенные окна выбора файлов* используется для изменения внешнего вида окон, появляющихся при выборе файла, например для подписи.

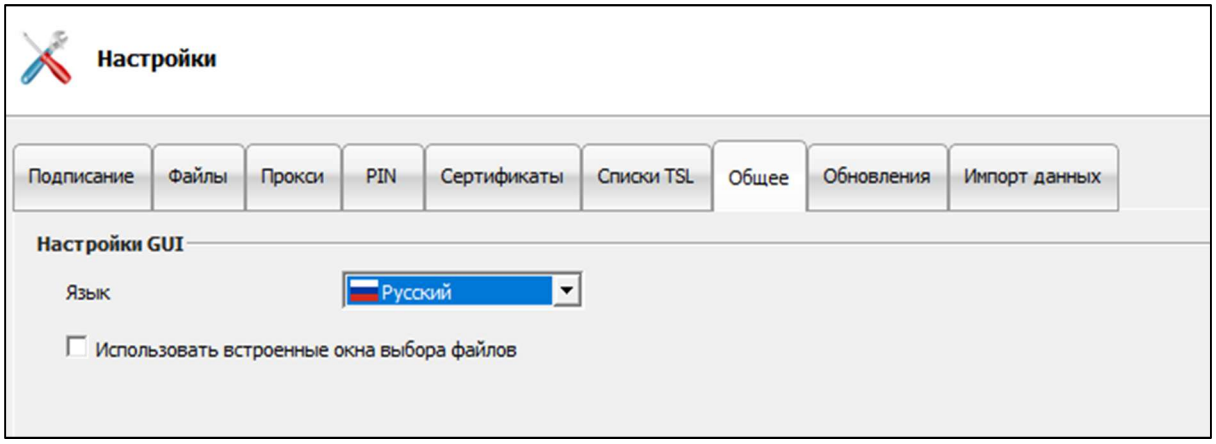


Рис. 59 Выбор языка, используемого в программе

8.8 ОБНОВЛЕНИЯ

Версия программы отображается в главном окне (правый нижний угол) PEM-HEART Signature. Дополнительно во вкладке *Обновления* вы можете проверить, есть ли новая версия. Информацию о доступных обновлениях можно предоставить вручную, нажав кнопку *Проверить наличие обновлений*, либо установить параметры автоматической проверки при запуске программы. Если будет обнаружена новая версия программного обеспечения, отобразятся сообщения.

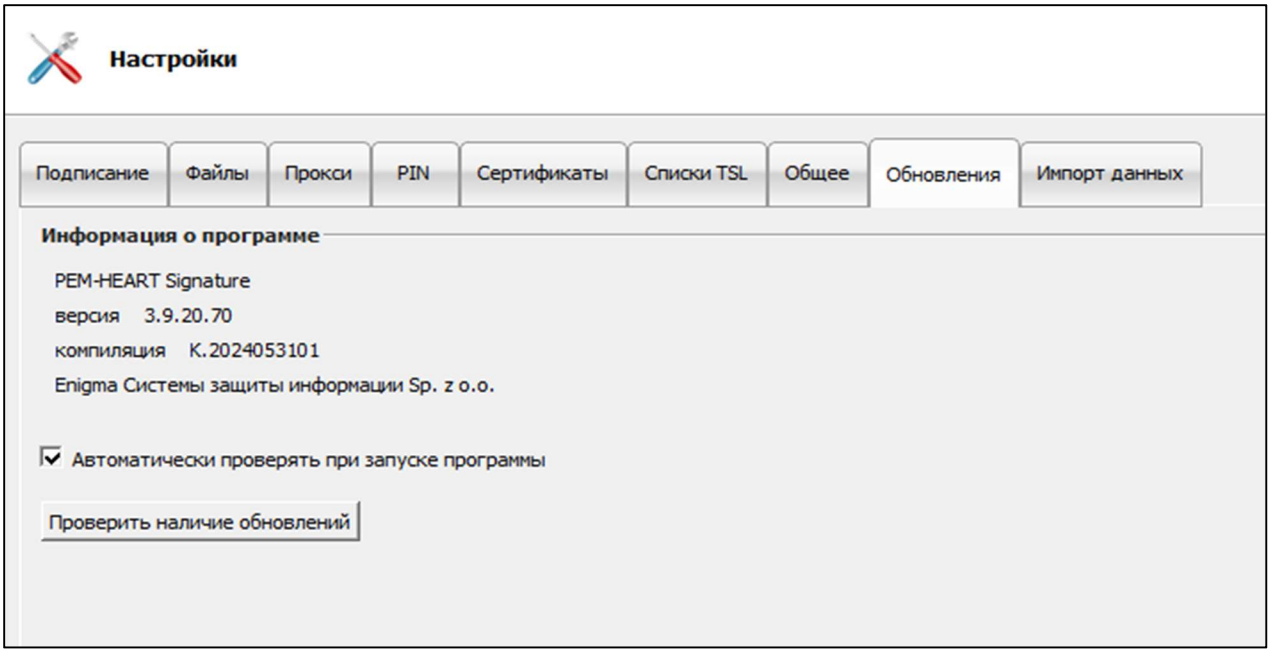


Рис. 60 Окно с информацией о версии ПО

8.9 ИМПОРТ ДАННЫХ

Опции импорта данных используются для того, чтобы программа могла функционировать в среде, где нет доступа в Интернет. Добавление временных меток и проверка статуса сертификата на основе OCSP в такой ситуации невозможны, но подписание и проверка подписи все равно возможны при условии наличия в программе актуальных списков TSL и CRL - которые в этом случае необходимо перенести и загрузить в программу вручную.

Внимание! Создание подписей rSign (в облаке) всегда требует доступа в Интернет.

Чтобы загрузить файл с CRL или TSL, нажмите кнопку *Точка* рядом с соответствующим списком (после чего необходимо выбрать соответствующий файл на диске), а затем кнопку *Добавить CRL* или *Добавить TSL* соответственно.

Рис. 61 Настройки – импорт данных списков CRL и TSL

8.9.1 ОЧИСТКА КЕША

Кнопка «Очистить кэш» удаляет базу данных PEM-HEART Signature. Это следует попробовать в определенных случаях, например, при возникновении ошибки базы данных. База данных содержит данные кэша (например, текущий список CRL), удаление которых не имеет негативных последствий, поскольку программа автоматически загрузит недостающие данные из сетевых ресурсов.

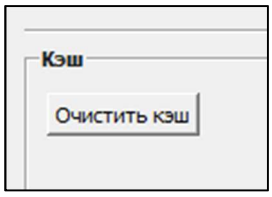


Рис. 62 Возможность очистки

9 ПОДПИСЬ RSIGN

9.1 КОНФИГУРАЦИЯ НА КОМПЬЮТЕРЕ

9.1.1 ДОБАВЛЕНИЕ ТОКЕНА RSIGN

Чтобы использовать rSign на конкретном компьютере (учетной записи Windows), необходимо настроить подпись на каждом таком компьютере (учетной записи).

Цели этой операции двоякие - во-первых, приступая к созданию подписи, программа должна знать, кто будет подписывать (каким сертификатом будет подписана подпись). Во-вторых, важной целью является повышение безопасности вашей подписи — rSign можно подписать только на том компьютере, который вы ранее признали доверенным.

Чтобы настроить подпись rSign, запустите программу *PEM-HEART Signature -> Карта -> Конфигурация rSign* или из меню Windows *PEM-HEART Конфигурация rSign*. Затем выберите кнопку *Активация*

Рис. 63 Конфигурация подписи rSign

Затем введите идентификатор ключа rSign из приложения на своем мобильном телефоне.

Рис. 65 Окно мобильного приложения с идентификатором ключа

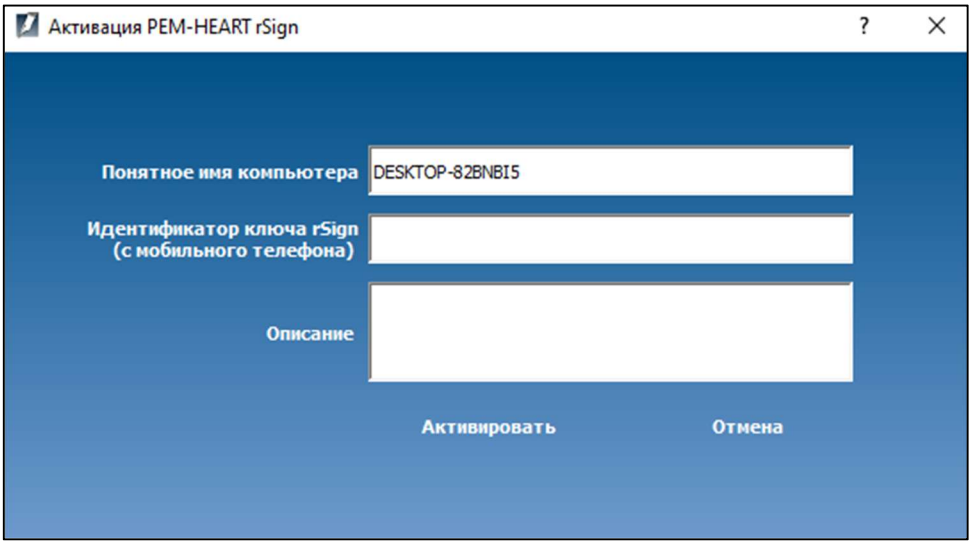


Рис. 64 Окно активации подписи rSign

9.1.2 УДАЛЕНИЕ ТОКЕНА RSIGN

Если есть необходимость удалить токен rSign с компьютера, такую операцию можно выполнить через программу *PEM-HEART Конфигурация rSign*. После запуска программы нажмите кнопку *Удалить токен*. Затем отобразится активный токен rSign в конфигурации и данные сертификата.

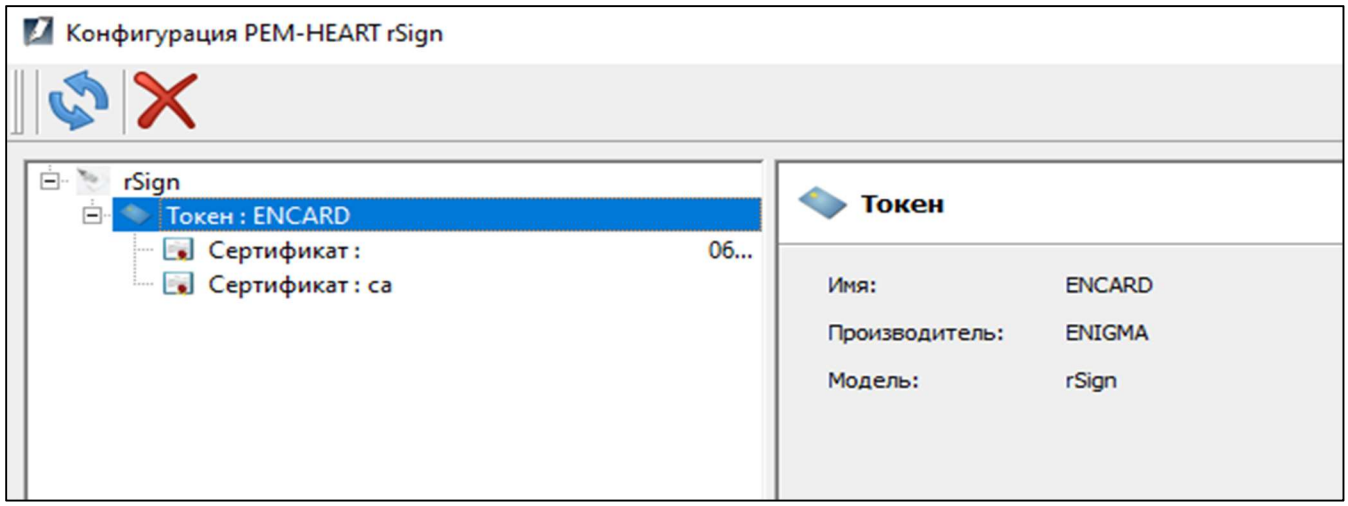


Рис. 66 Просмотр активного токена rSign с данными сертификата

Затем нажмите в левом окне на *Токен: ENCARD*, который активирует  кнопку на верхней панели – его выбор запустит процесс удаления токена. Пользователь должен подтвердить удаление в отдельном окне:

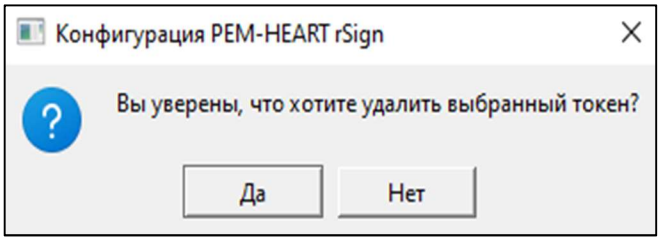


Рис. 67 Подтверждение удаления токена rSign

Нажатие *Да* удалит токен.

9.2 КОНФИГУРАЦИЯ МОБИЛЬНОГО ПРИЛОЖЕНИЯ

9.2.1 УСТАНОВКА

Приложение доступно для скачивания в AppStore и Google Play.

9.2.2 ОСНОВНОЙ ЭКРАН

После запуска приложения по умолчанию отображается экран с активным PIN-кодом для подписи. В представлении Пользователь видит PIN -код, таймер, задающий время его использования, и очередь ожидающих операций. Кроме того, в правом верхнем углу есть значок  , использование которого обновляет вид уведомлений и значок в левом верхнем углу  , значок, при выборе которого будут отображаться параметры: *Операции (отображаются по умолчанию при запуске приложения), Key ID, Настройки*.

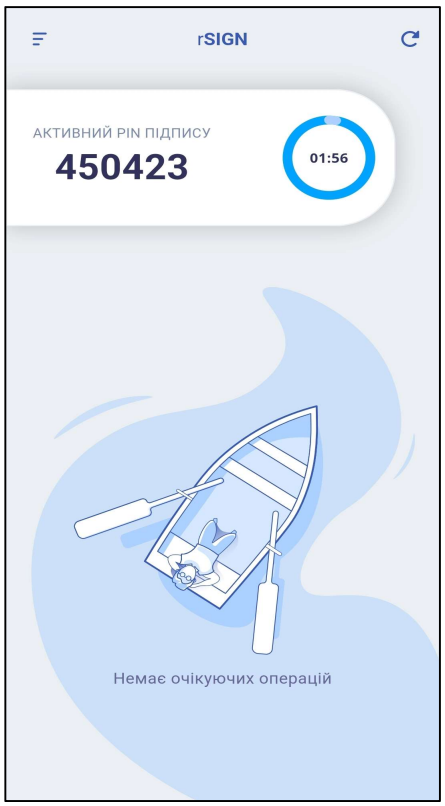


Рис. 68 Основной экран мобильного приложения rSign

9.2.3 ИДЕНТИФИКАТОР КЛЮЧА

При выборе опции *Идентификатор ключа* отобразится экран с используемым идентификатором ключа, среди прочего: чтобы настроить использование rSign на вашем компьютере. Однако прежде чем Пользователь сможет его увидеть, программа сначала запросит PIN-код — только если он введен правильно и подтвержден, будет отображен идентификатор ключа.

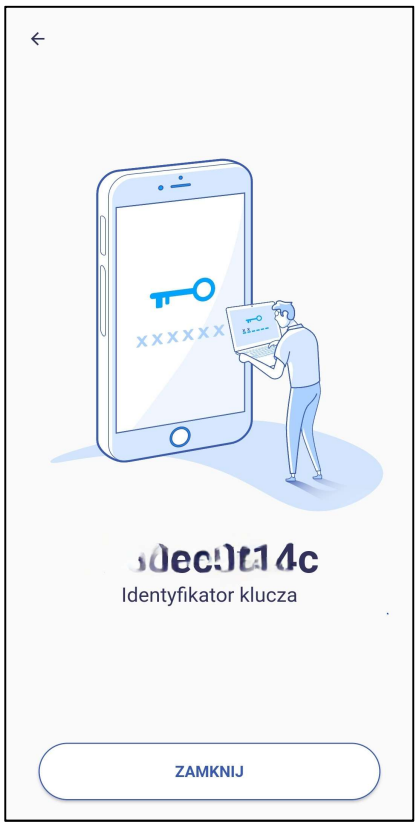


Рис. 69 Экран приложения после выбора опции идентификатор ключа

9.2.4 НАСТРОЙКИ

При выборе *Настройки* отобразится экран со списком доступных настроек приложения. Это:

- *Запоминание PIN-кода для подписи* – опция, позволяющая запомнить введенный ПИН-код на период времени, указанный Пользователем. Доступны четыре варианта — три предопределенных: 3, 5 и 10 минут и любой от 1 до 60 минут.
- *Изменение PIN-кода* – опция, позволяющая изменить PIN-код.
- *Связанный номер телефона* – здесь Пользователь вводит номер телефона, привязанный к учетной записи.
- *Резервное копирование* – позволяет создать резервную копию для активации rSign на любом устройстве.
- *Деактивировать устройство* – опция, позволяющая удалить данные активации rSign с устройства.
- *Язык* – позволяет изменить язык в приложении. Языки на выбор: польский, английский, русский, украинский.

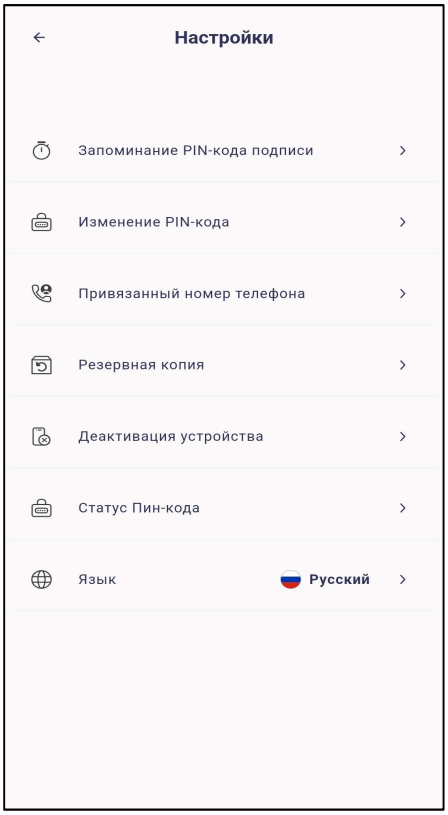
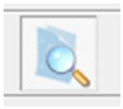


Рис. 70 Экран приложения после выбора опции

10 АДМИНИСТРИРОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ PEM-HEART

10.1 ЖУРНАЛЫ РАБОТЫ КАРТЫ ДЛЯ СИСТЕМ WINDOWS

Программное обеспечение позволяет включить вход в систему для операций, совершаемых с использованием карты, например, подписания документа. Есть два способа включить эту функцию:

- Щелкнув значок увеличительного стекла на панели Диагностика, активируемая расширенными функциями.
-  - значок, указывающий на то, что функция включена – при первом использовании перезапустите программу PEM-HEART Signature для сохранения изменений,

   - значок, указывающий на то, что функция отключена – при первом включении необходимо перезапустить программу PEM-HEART Signature для сохранения изменений.

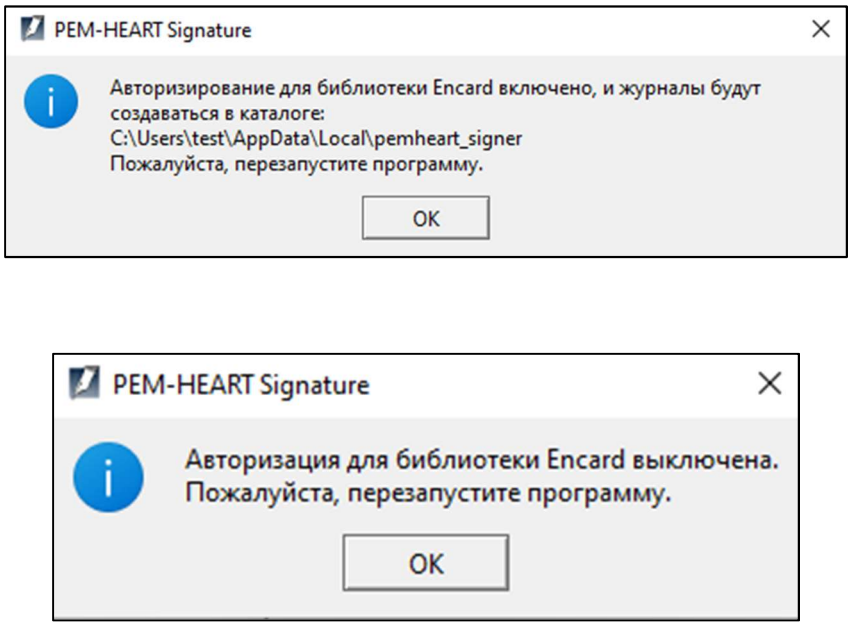


Рис. 71 Сообщение после включения и отключения входа на карты IDEMIA

- Более расширенная настройка вызывается через окна конфигурации библиотеки PKCS#11. Выберите меню «Пуск»->Программы->ENCARD->Конфигурация ENCARD PKCS#11. Выбор опции конфигурации откроет окно конфигурации библиотеки PKCS#11.

Выбор опции *Сохранить вызываемые функции в файл* (она же является названием первого раздела) используется для настройки записи всей информации в файл журнала, в частности содержимого приватных объектов. Введенные PIN не сохраняются - при входе команды на карту заменяются на XX символы.

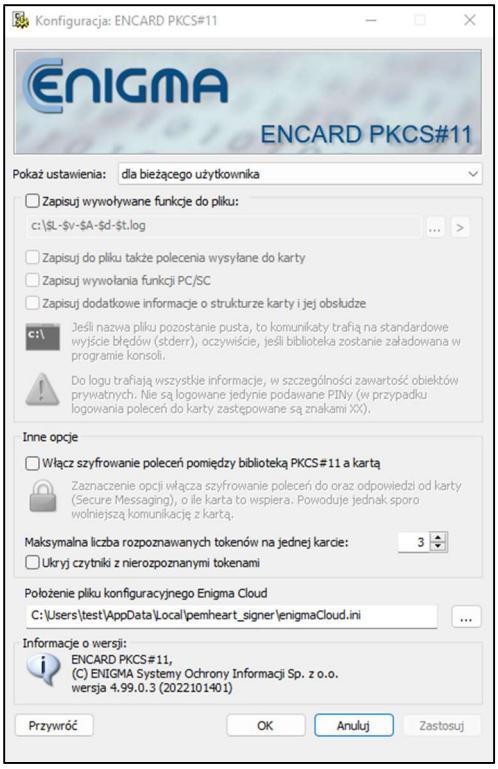


Рис. 72 Экран конфигурации библиотеки PKCS#11

Кнопка используется для определения местоположения и имени файла журнала. ... Если имя файла оставить пустым, сообщения перейдут в стандартную ошибку (stderr), если библиотека загружена в консольную программу.

Библиотека принимает в имени файла специальные макросы, позволяющие вести запись в разные файлы журналов в зависимости от загружающего его приложения, текущего времени и даты, версии библиотеки и других. При нажатии кнопки > рядом с именем файла журнала отображается диалоговое окно конфигурации, содержащее список всех макросов:

- $A - имя файла приложения, загружающего библиотеку (без пути и расширения).
- $L - имя файла загруженной библиотеки (без пути и расширения).
- $l - внутреннее название библиотеки.
- $D - дата загрузки библиотеки в виде YYYY-MM-DD.
- $d - дата загрузки библиотеки в виде YYYYMMDD.
- $T - время загрузки библиотеки в виде hh-mm-ss.
- $t - время загрузки библиотеки в виде hhmmss.

- $K - номер сборки библиотеки (np. 2008080901).
- $V - основная версия библиотеки (np. 2.0).
- $v - полная версия библиотеки (np. 2.01.2.2).
- $$ - знак $.

При записи вызываемых функций в файл пользователь может выбрать другую информацию для добавления в журнал дополнительной информации. Дополнительные опции включают в себя:

- *Сохранение в файл команды, отправленной на карту*
- *Журнал вызовов функций ПК/SC*
- *Запись дополнительной информации о структуре карты и ее работе*

Второй раздел окна настройки библиотеки PKCS#11 позволяет добавить шифрование в соединении между библиотекой PKCS#11 и картой, что осуществляется установкой флажка *Включить шифрование команд* между библиотекой PKCS#11 и картой. Кроме того, вы можете указать максимальное количество распознанных токенов на одной карте и скрыть считыватели с нераспознанными токенами.

Чуть ниже второго раздела находится место для указания пути к файлу конфигурации Enigma Cloud и информации о программном обеспечении для настройки.

Все изменения сохраняются при нажатии кнопки *Применить*. Выбор *ОК* также сохраняет изменения и закрывает открытое окно конфигурации. Любые изменения опций можно отменить, выбрав *Отмена* (закрытие окна конфигурации без сохранения изменений) или *Восстановить* (восстановление настроек с момента сразу после запуска конфигуратора, без закрытия программы).

11 ПОИСК НЕИСПРАВНОСТЕЙ

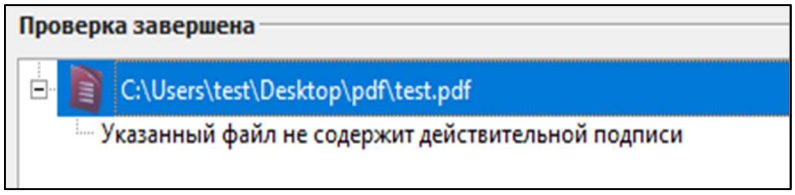


Рис. 73 Сообщение об отсутствии действительной подписи в файле

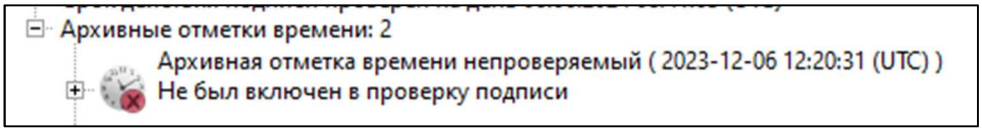


Рис. 74 Сообщение о непроверяемой временной метке архива

УСТАНОВКА		
Проблема	**Причина**	**Решение**
Операция не удалась	Пользователь отменил процесс установки программы	Перезапустите установщик

ПОДПИСАНИЕ		
Проблема	**Причина**	**Решение**
Временную метку не удалось получить ни с одного из серверов.	С сертификатом не связан пакет меток времени	- повторите попытку на следующий день или - приобрести пакет штампов времени (подробности: http://www.cencert.pl), или - отключить опцию отметки времени для подписей (см. Главу **6.2 ОТМЕТКА ВРЕМЕНИ**)
	У программы нет доступа к интернету или запрос не	- проверьте подключение к Интернету - проверьте настройки прокси

	одобрен в приложении rSign	(если вы используете прокси-сервер) - см. Главу **8.3 ПРОКСИ**)
Функциональность недоступна для текущего носителя !!!	Нет реализованной функции поддержки проверки данного файла, подпись сделана в неподдерживаемом стандарте	Заявка в Cencert

ПРОВЕРКА		
Проблема	**Причина**	**Решение**
Укажите местонахождение документов. Не все отключенные документы были найдены ...	Программа не нашла подписанный файл в каталоге подписи.	Укажите файл, который был подписан (соответствует проверяемой подписи)
Ошибка открытия входного файла	Файл поврежден или открыт в другой программе	Закройте другую программу и попробуйте снова открыть файл в PEM-HEART Signature.
	Файл уже открыт в другой программе	
	У программы нет доступа к местоположению файла	Проверьте, действительно ли файл существует в указанном месте
Ни один из файлов не содержит действительной подписи	Файл поврежден или подписан в формате, не поддерживаемом PEM-HEART SIgnature	Указание другого файла или отчет в Cencert

12 УКАЗАТЕЛЬ РИСУНКОВ