Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра автоматизированных систем управления (АСУ)

ЗНАКОМСТВО С КРИПТОСИСТЕМАМИ

Лабораторная работа №4

по дисциплине

«Информационная безопасность»

Студент гр. 430-2

_____А.А. Лузинсан

«_____»_____2023 г.

Руководитель

Ассистент каф. АСУ

_____ Я.В. Яблонский

«____»_____2023 г.

Томск 2023

Оглавление

1 Цель работы

Цель: освоить процесс создания ключей, распространения открытых и сохранения в тайне закрытых ключей, а также шифрования, расшифрования, создания и подтверждения электронных подписей в криптосистемах.

2 Постановка задачи

Задание по варианту №3: установите программу КриптоАРМ и последовательно выполните следующие шаги:

- Изучите «Руководство пользователю»;
- Ознакомьтесь с работой программы. Внимательно изучите процессы создания ключей, распространения открытых и сохранения в тайне закрытых ключей, схему разделения и сборки ключей.
- Создайте свою собственную пару ключей (открытый и закрытый).
- Распространите свой открытый ключ.
- Получивший открытый ключ пользователь должен проделать следующие действия: подготовить документ (файл), который необходимо переслать другому пользователю, подписать файл цифровой подписью, зашифровать подписанный файл с помощью открытого ключа другого пользователя, передать зашифрованный файл пользователю, чей ключ использовался при шифровании, получатель должен расшифровать файл и проверить достоверность ЭЦП;

3 Алгоритм действий

После изучения «Руководства пользователю» первым делом была проверена информация «О программе». Как видно из рисунка 3.1, версия скачанной криптосистемы является «КриптоАРМ Стандарт Плюс 5». Данная версия является расширенной, в отличие от стандартной версии, так как поддерживает работу с токенами и старт-картами с криптографией «на борту» и неизвлекаемыми ключами. В то время как стандартная версия включает в себя функции подписи и шифрования электронных данных, а также поддерживает российские ГОСТ алгоритмы подписи и шифрования. Функция проверки корректности электронной подписи при работе с криптопровайдером «КриптоПро CSP» включена во все версии КриптоАРМ по-умолчанию.

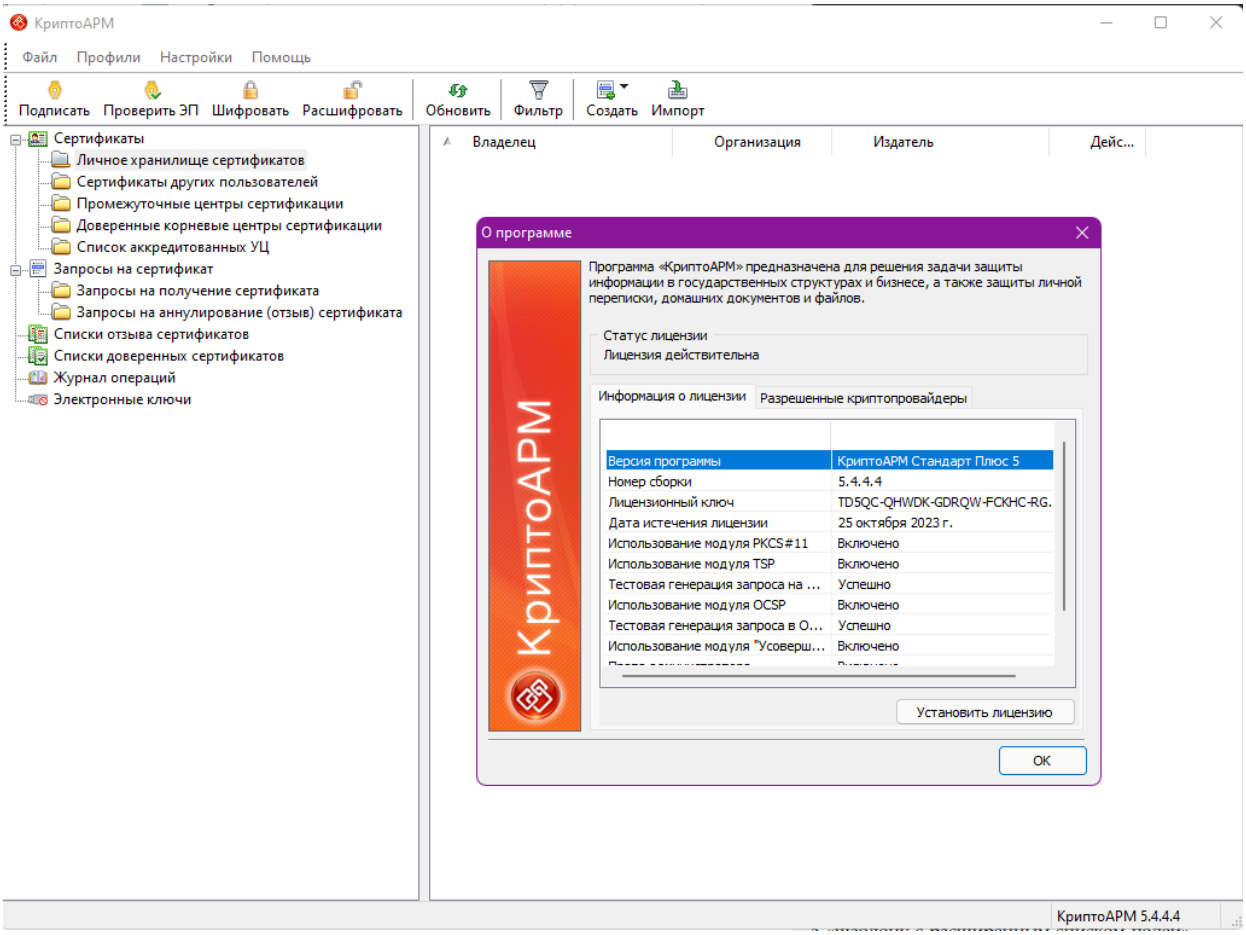

Рисунок 3.1 — Общие сведения о программе

3.1 Создание самоподписанного сертификата

Для того, чтобы создать открытый и закрытый ключи, в криптосистемах используют понятие сертификата.

Самоподписанный сертификат – сертификат, изданный самим пользователем, без обращения к доверенной стороне (Удостоверяющему центру). Самоподписанный сертификат является одновременно личным и корневым (устанавливается в Личное хранилище сертификатов и «Доверенные корневые центры сертификации»). Самоподписанные сертификаты используются для обмена зашифрованными или подписанными документами между людьми, доверяющими друг другу, например, друзьями, коллегами. Обменявшись такими сертификатами между собой, они могут пересылать друг другу подписанные и зашифрованные электронные данные, не беспокоясь при этом, что информация может быть перехвачена, искажена

и использована против их интересов.

Таким образом, для создания самоподписанного сертификата были выполнены следующие действия:

• В дереве элементов главного окна был выбран раздел Сертификаты. Далее правой клавишей мыши было вызвано контекстное меню и выбран пункт Создать > Самоподписанный сертификат, как это показано на рисунке 3.2. Далее открывается Мастер создания самоподписанного сертификата.

• На первом шаге мастера создания самоподписанного сертификата требуется ознакомиться с порядком и требованиями создания самоподписанного сертификата.

• На следующем шаге из выпадающего списка был выбран шаблон «Сертификат КЭП физического лица».

• Далее требовалось указать идентификационную информацию о владельце будущего сертификата в соответствие с шаблоном, выбранным на предыдущем шаге, как это показано на рисунке 3.3. При этом стоит обратить на следующие правила: поля, отмеченные знаком «*» являются обязательными для заполнения, СНИЛС указывается без пробелов и знаков «-».

• После указания данных в разделе «Основная информация» открывается раздел «Параметры ключа», заполнение которого указано на рисунке 3.4. В процессе создания сертификата «с нуля» был отмечен выбор создания нового ключевого набора, что подразумевает генерацию новой ключевой пары и создания сертификата на его основе. Пометка экспортируемости ключей в данном случае является необязательной, так как возвожность экспорта сертификата по умолчанию возможна с открытым ключом, тогда как активация функции позволит экспортировать сертификат ещё и с закрытым ключом, обеспечивая тем самым архивацию сертификата. Таким образом открытый ключ выглядит следующим образом: d196a6dd-c1a8-4887-ae6d-54cc23632930.

• После прохождения вышеупомянутого раздела требовалось подтвердить несколько действий: запрос системы на установку пароля на носитель и подтверждение его, а также запрос системы на установление самоподписанного сертификата в хранилище Доверенных корневых центров сертификации.

Общие сведения о сертификате представлены на рисунке 3.5.

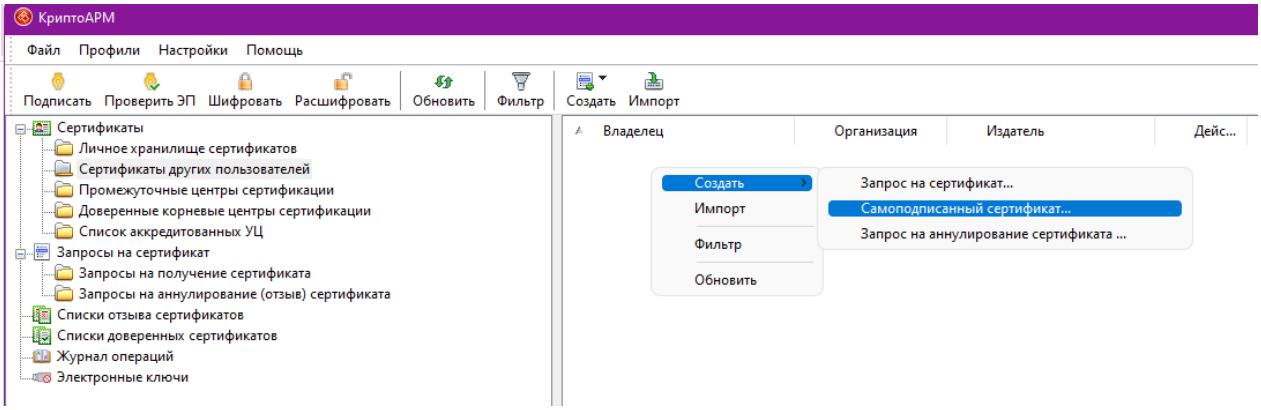

Рисунок 3.2 — Вызов контекстного меню для создания самоподписанного сертификата

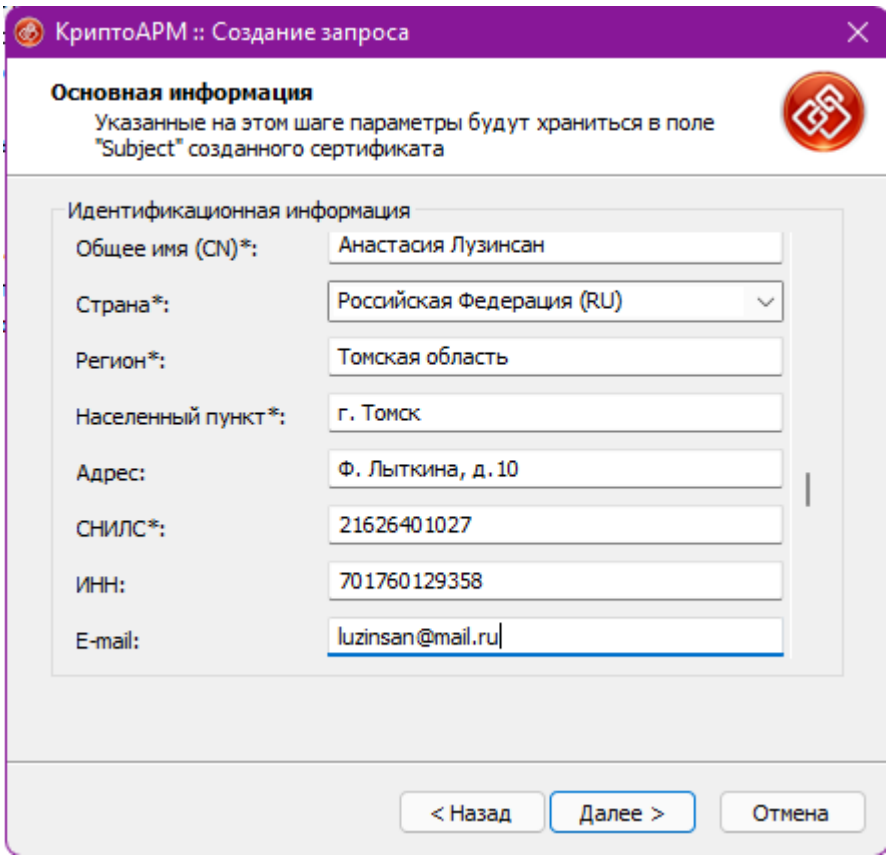

Рисунок 3.3 — Внесение идентификационной информации о владельце

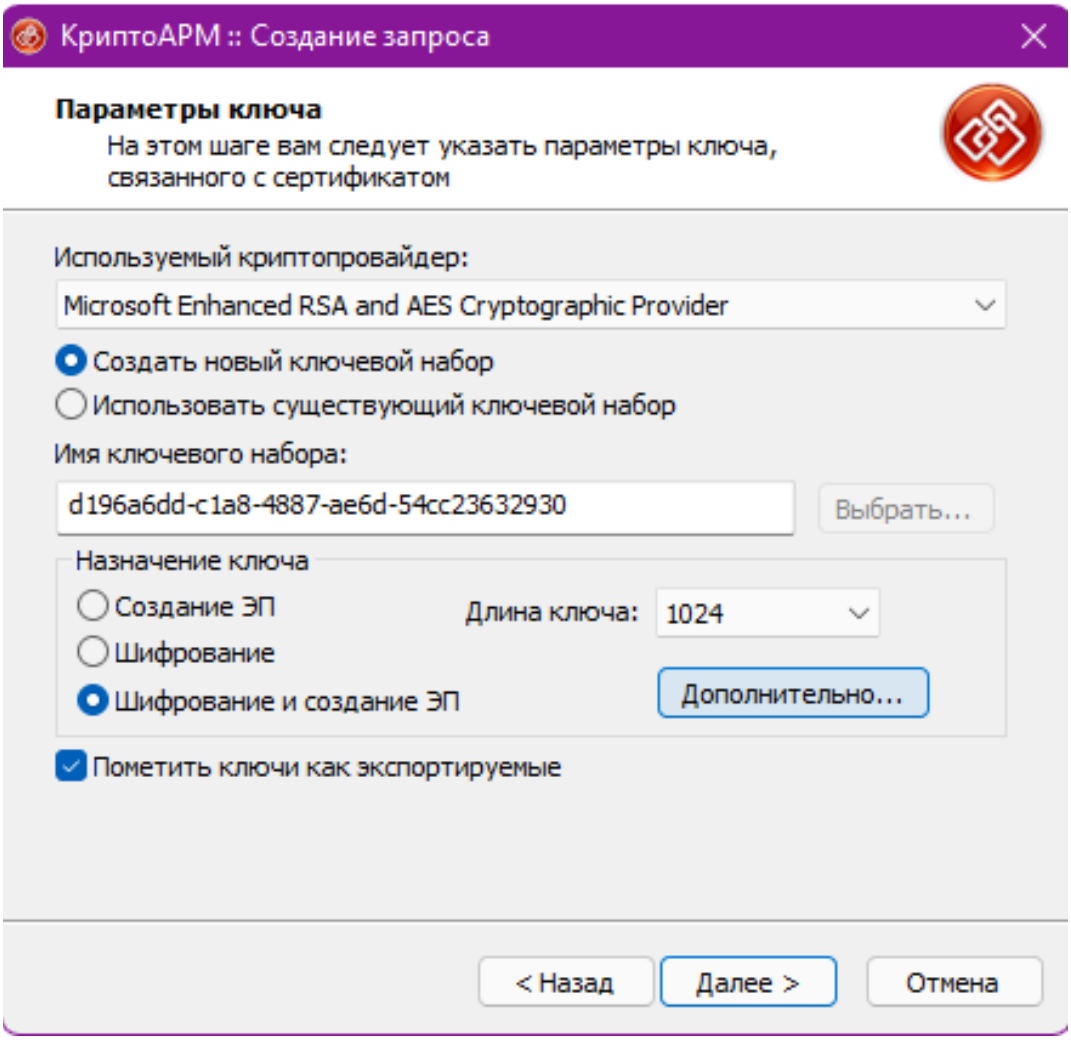

Рисунок 3.4 — Указание параметров ключа

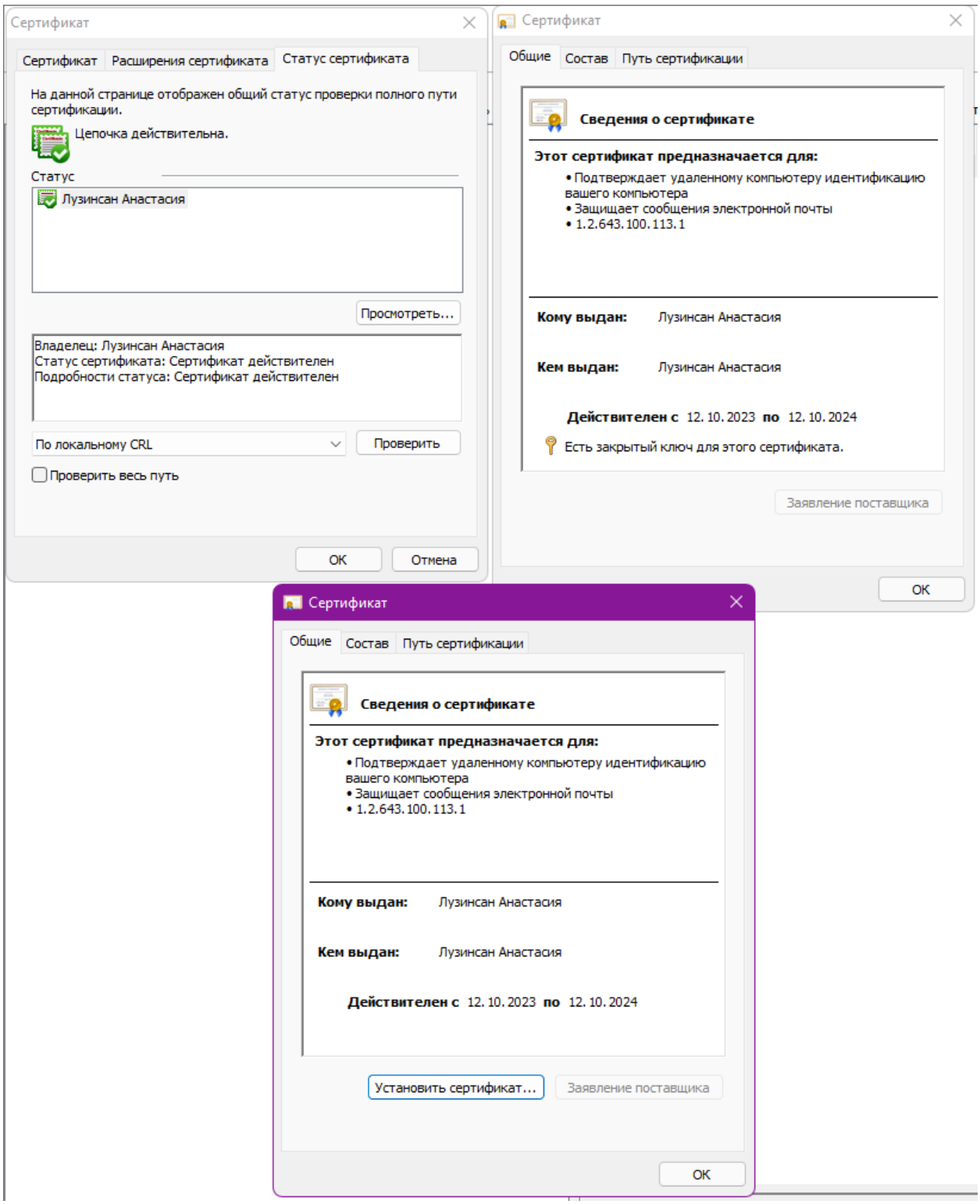

Рисунок 3.5 — Общие сведения о сертификате

3.2 Распространение открытого ключа

3.2.1 Экспортирование сертификата

Для того, чтобы смоделировать ситуацию передачи зашифрованного текста с невозможностью расшифровать данные, необходимо экспортировать сертификат без закрытого ключа. Экспорт сертификатов в криптосистеме КриптоАРМ осуществляется «Мастером экспорта сертификатов», как это показано на рисунке 3.6. При этом для наших целей необходимо указать пункт «Нет, не экспортировать закрытый ключ».

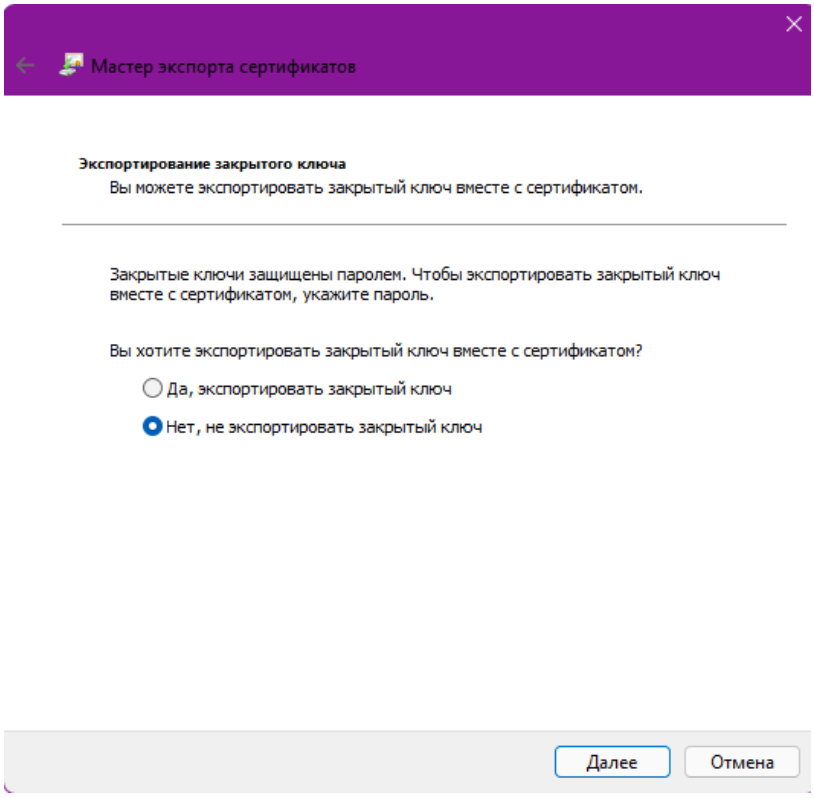

Рисунок 3.6 — Экспорт сертификата без закрытого ключа

Далее открывается раздел с указанием формата экспортируемого файла, как показано на рисунке 3.7. В качестве такого расширения был выбран «Стандарт Cryptographic Message Syntax — сертификаты PKCS #7 (.p7b)». Общая информация об экспортировании сертификата указана на рисунке 3.8.

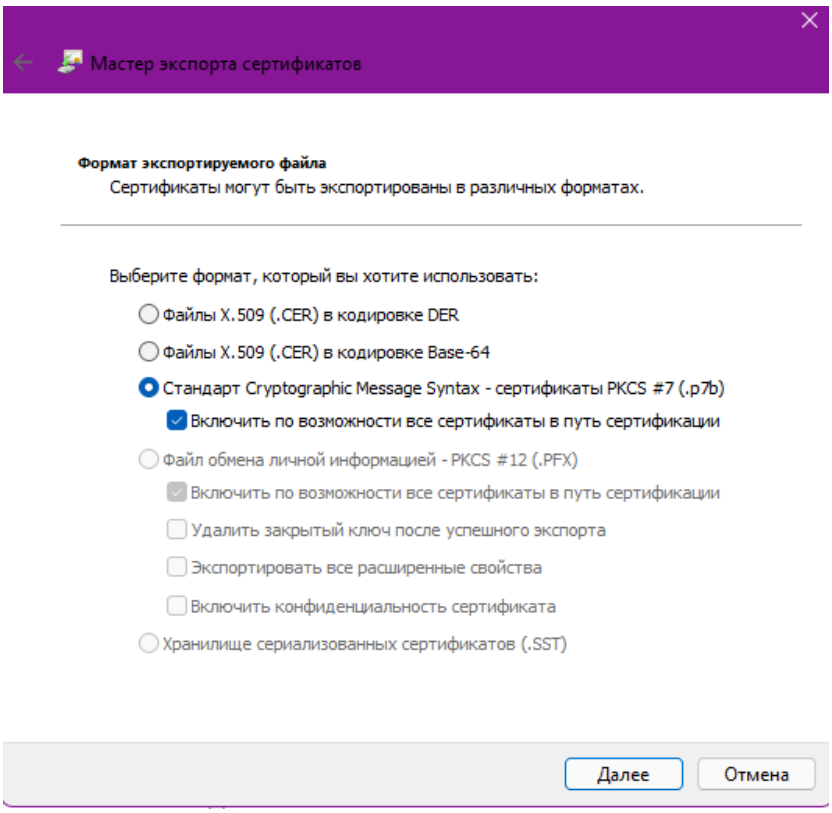

Рисунок 3.7 — Указание формата экспортируемого файла

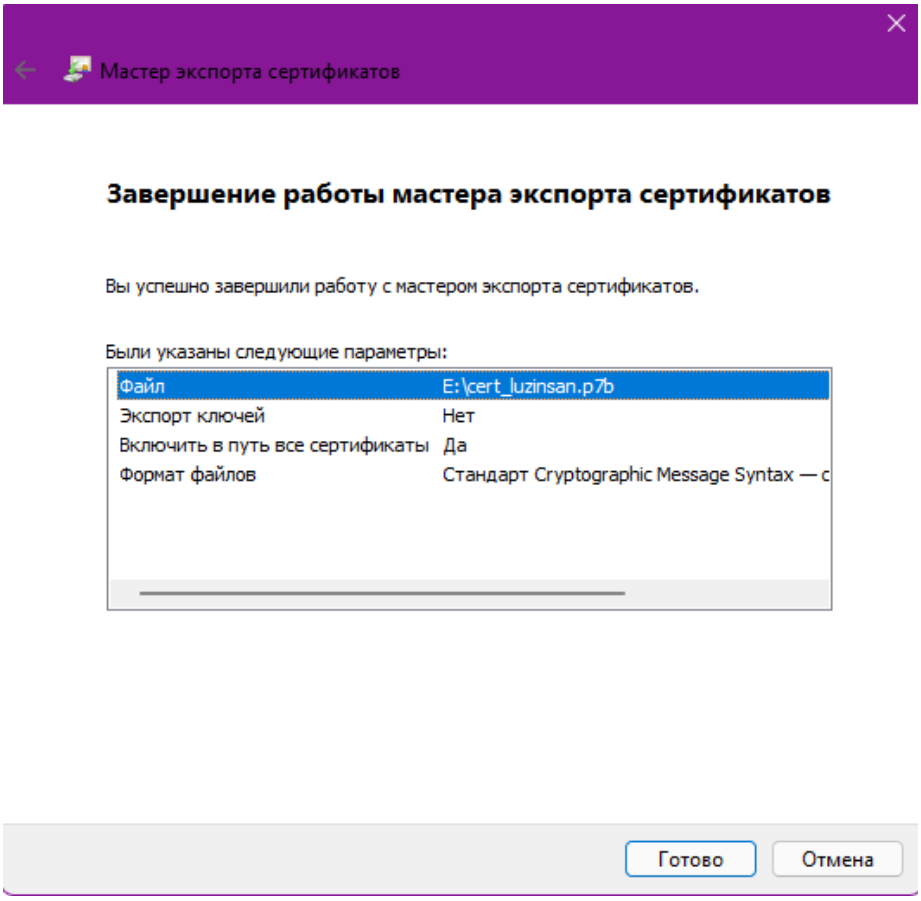

Рисунок 3.8 — Завершение работы мастера экспорта сертификатов

3.2.2 Импортирование сертификата

Переходя на стадию создания электронной подписи и шифрования данных с помощью открытого ключа получателя, предварительно необходимо импортировать сертификат получателя в список доверенных корневых центров сертификации.

Для этого в меню выбирается функция «Импортировать», после чего вызывается окно «Установка сертификатов, CRL и CTL». Переходя в раздел «Выбор файла сертификата, CRL или CTL», был указан путь до файла сертификата, полученный через flash-носитель от пользователя-получателя, как это показано на рисунке 3.9. Так как данный сертификат не содержится в списке доверенных сертификатов, то его статус на данном этапе будет отображаться как «недействительный».

Так как в приветственном окне не был установлен флаг «Установить личный сертификат», то система на следующем шаге предложила указать хранилище, в котором будет храниться импортируемый сертификат. Для данного сертификата было указано хранилище «Доверенные корневые центры сертификации».

В результате проделанных действий в хранилище доверенных сертификатов пользователя-отправителя добавится сертификат получателя, содержащий его открытый ключ.

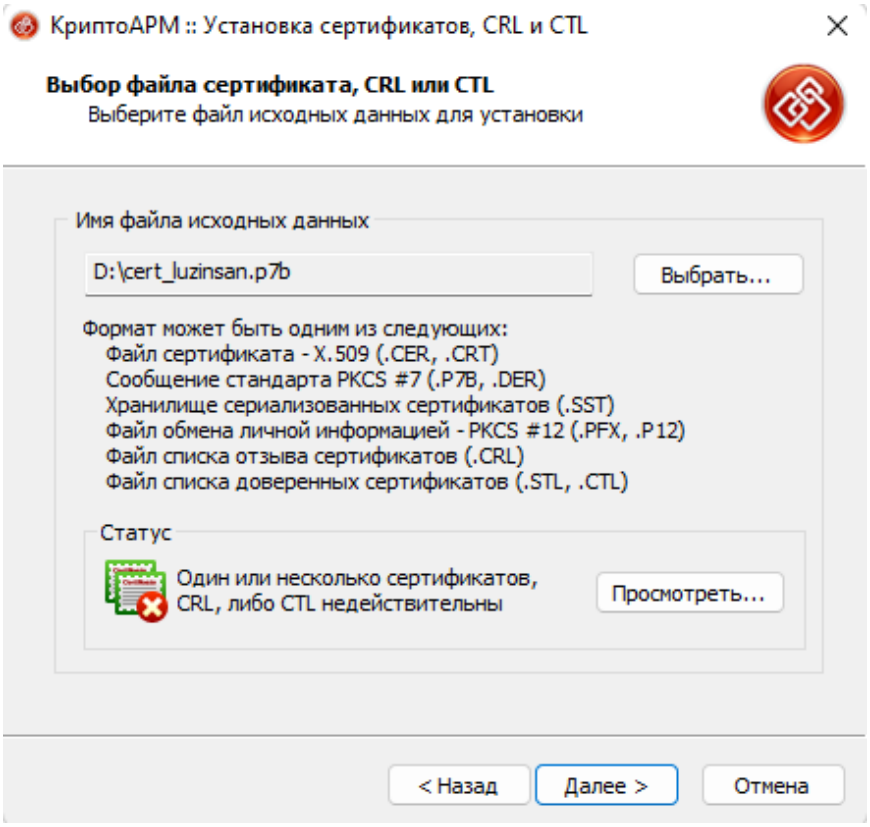

Рисунок 3.9 — Выбор файла сертификата для импортирования

3.3 Создание электронной подписи и шифрование сообщения

Предварительно у пользователя-отправителя должен существовать сертификат. Если этого не было сделано, но осуществляются все те же действия, которые были описаны в пункте 3.1.

В результате проделанных действий на машине отправителя был получен результат, представленный на рисунке 3.10.

Далее, для того чтобы подписать и зашифровать сообщения в одном диалоговом окне, был вызван мастер подписи и шифрования посредством ниспадающего списка из панели меню, как указано на рисунке 3.11.

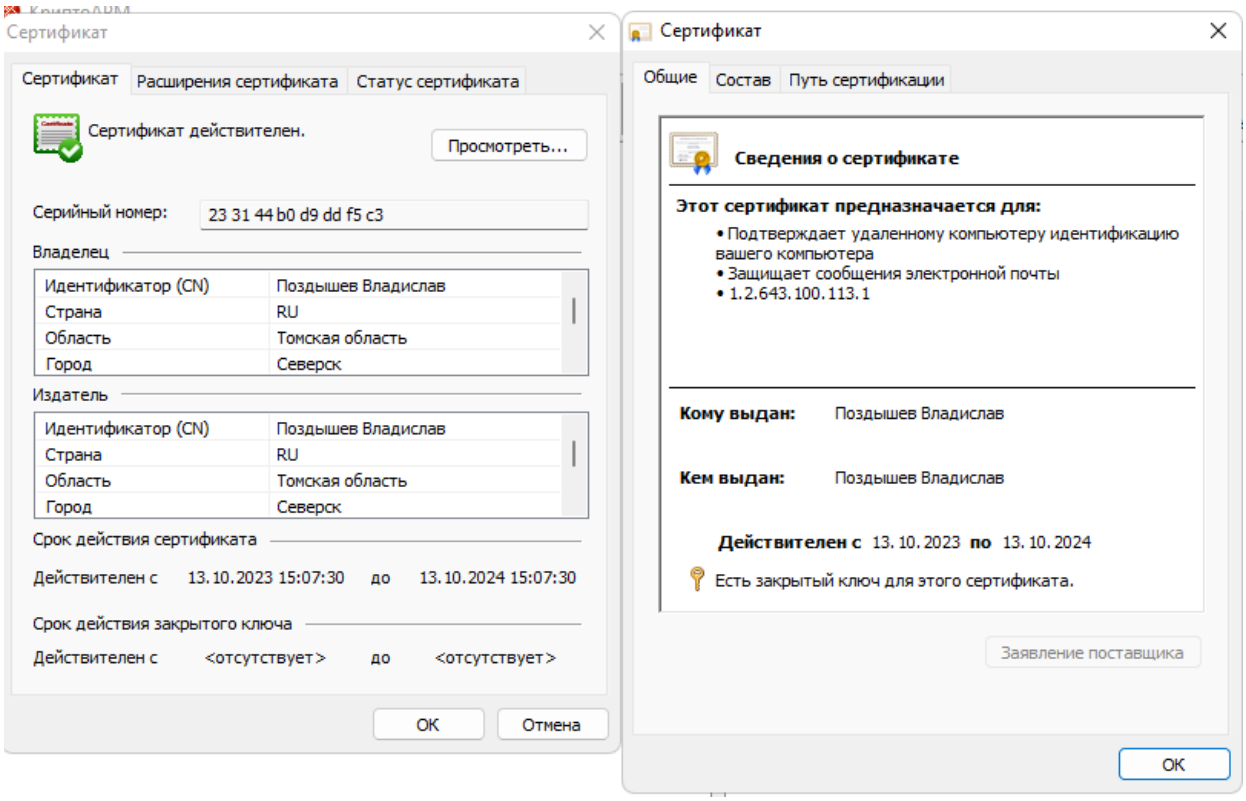

Рисунок 3.10 — Общие сведения сертификата отправителя

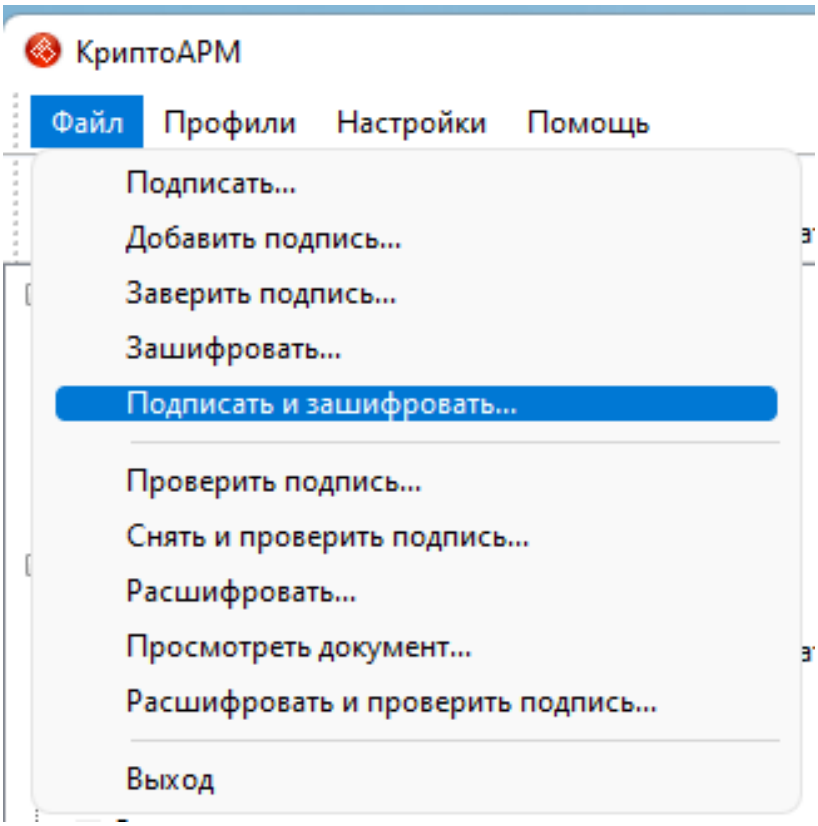

Рисунок 3.11 — Активация мастера подписи и шифрования

3.3.1 Создание электронной подписи

Открыв мастер выполнения операции подписи и шифрования, программа предлагает выбрать файлы и папки, которые необходимо зашифровать и подписать. После добавления документов открывается раздел «Выходной формат», в котором указываются параметры для создания электронной подписи данных. В качестве кодировки и расширения выходного файла был выбран Base64 encoded X.509 с расширением подписанного файла *.sig, как изображено на рисунке 3.12.

В следующем разделе под названием «Параметры подписи» устанавливаются непосредственно параметры подписи. Заполнение этого раздела представлено на рисунке 3.13.

Нажимая кнопку «Далее», мастер предлагает указать сертификат для создания подписи. От имени пользователя-отправителя в качестве личного сертификата для подписи был указан основной сертификат пользователя-отправителя. Хеш-алгоритм, который был выбран на данном этапе, стал SHA-1, как показано на рисунке 3.14.

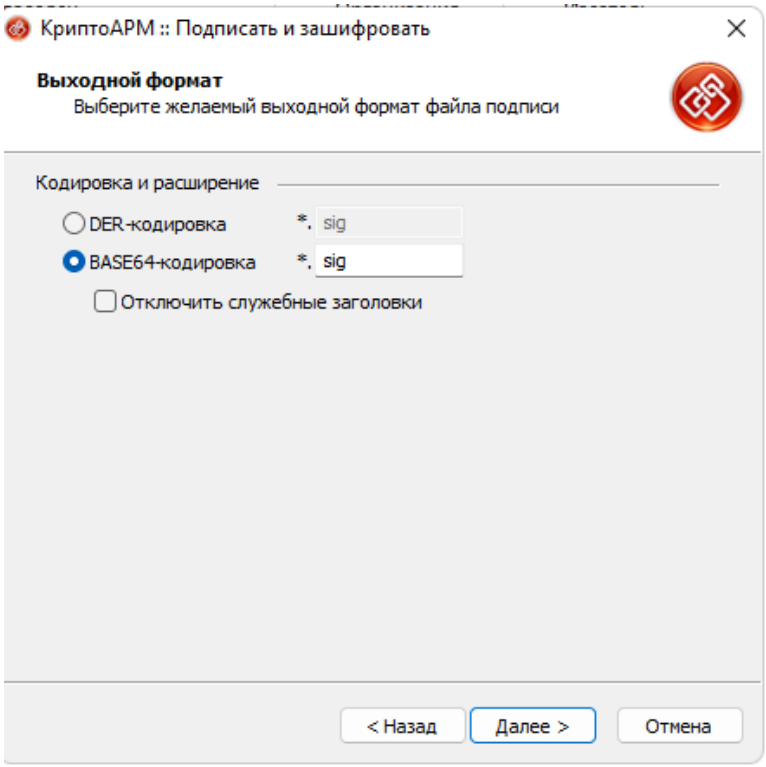

Рисунок 3.12 — Указание кодировки при создании электронной подписи отправителя

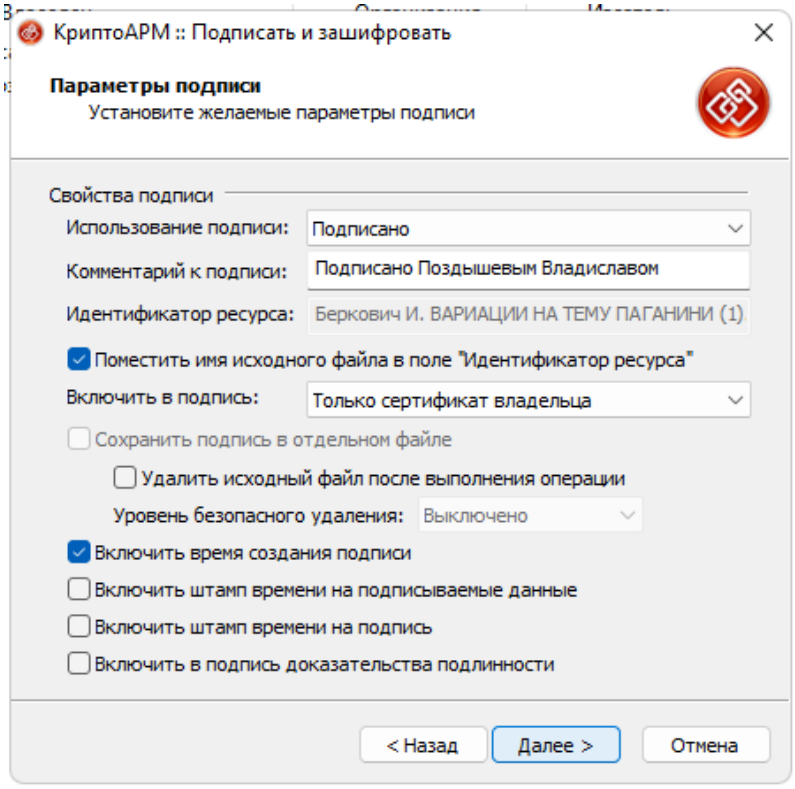

Рисунок 3.13 — Настройка параметров подписи отправителя

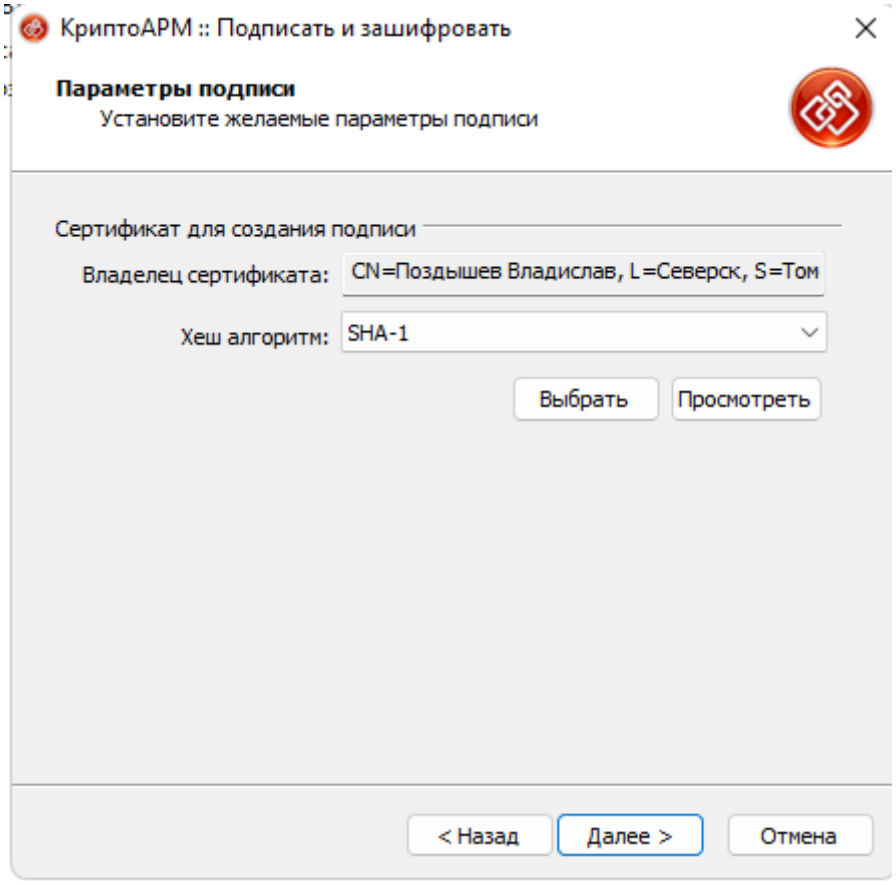

Рисунок 3.14 — Продолжение настройки параметров подписи отправителя

3.3.2 Шифрование сообщения

В том же самом мастере выполнения операции подписи и шифрования после нажатия на кнопку «Далее» мастер переходит к части с настройкой параметров непосредственно шифрования данных.

Подобно созданию подписи, в разделе «Выходной формат файла» на данном этапе указываются настройки выходного формата файла, а именно: кодировка и расширение, флаг архивирвоания, путь для выходных файлов, настройка сохранения структуры вложенности каталогов и отправка зашифрованного письма по электронной почте. Таким образом указанные для нашего случая настройки изображены на рисунке 3.15.

Далее открывается раздел с настройкой свойств шифрования. В данном разделе необходимо указать режим шифрования для отправителя сообщения.

В качестве криптопровайдера был выбран Microsoft Enhanced RSA and AES Cryptoprovider и алгоритм шифрования AES 128, как можно понять из рисунка 3.16.

На следующем шаге мастер предлагает выбрать сертификаты получателей шифруемого файла, используя кнопку «Добавить». Так как мы уже предваритель добавляли сертификат получателя в доверенный список сертификатов, то теперь не доставит труда указать данный сертификат в список получателей шифруемого файла. Результат представлен на рисунке 3.17.

После завершения сбора параметров для выполнения шифрования возникает окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был зашифрован файл и сертификат получателя (-ей). Для продолжения была нажата кнопка «Готово».

Далее возникает окно «Результат выполнения операции» со статусом завершения операции. Для просмотра детальной информации о результатах шифрования и используемых параметров, необходимо нажать кнопку «Детали». Далее «Менеджер сообщения», в котором можно просмотреть сертификаты получателей. Детали операции «Подписи и Шифрования» представлены на рисунке 3.18.

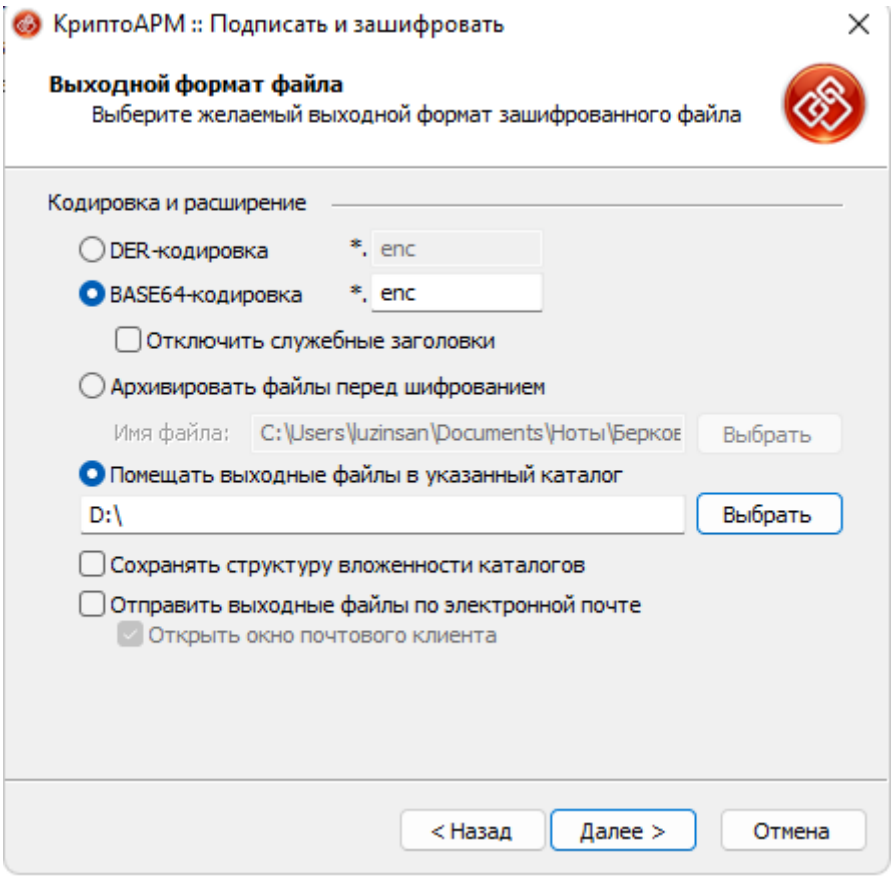

Рисунок 3.15 — Указание выходного формата файла

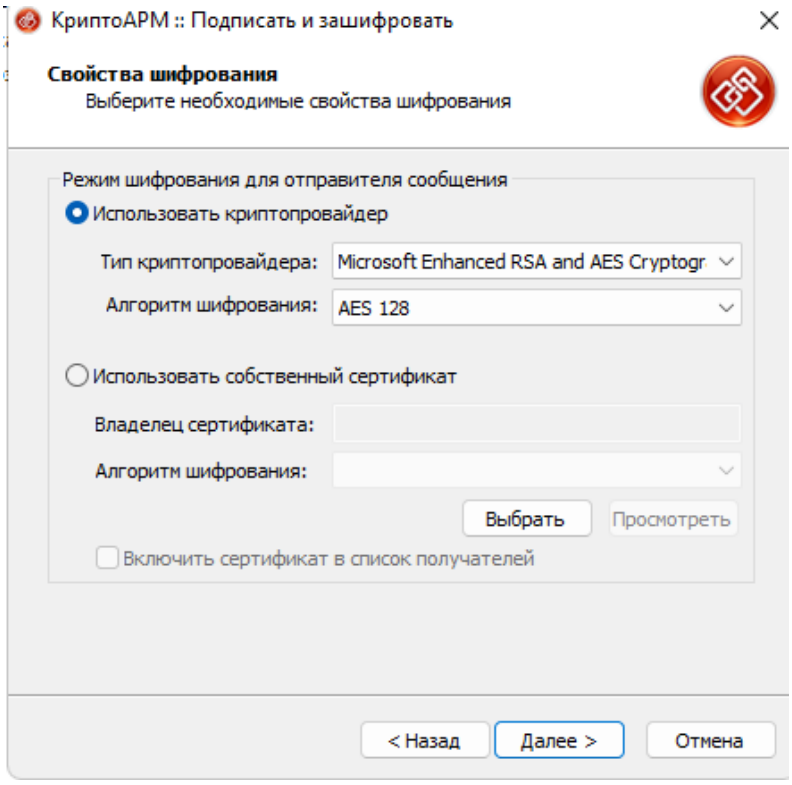

Рисунок 3.16 — Настройка свойств шифрования сообщения

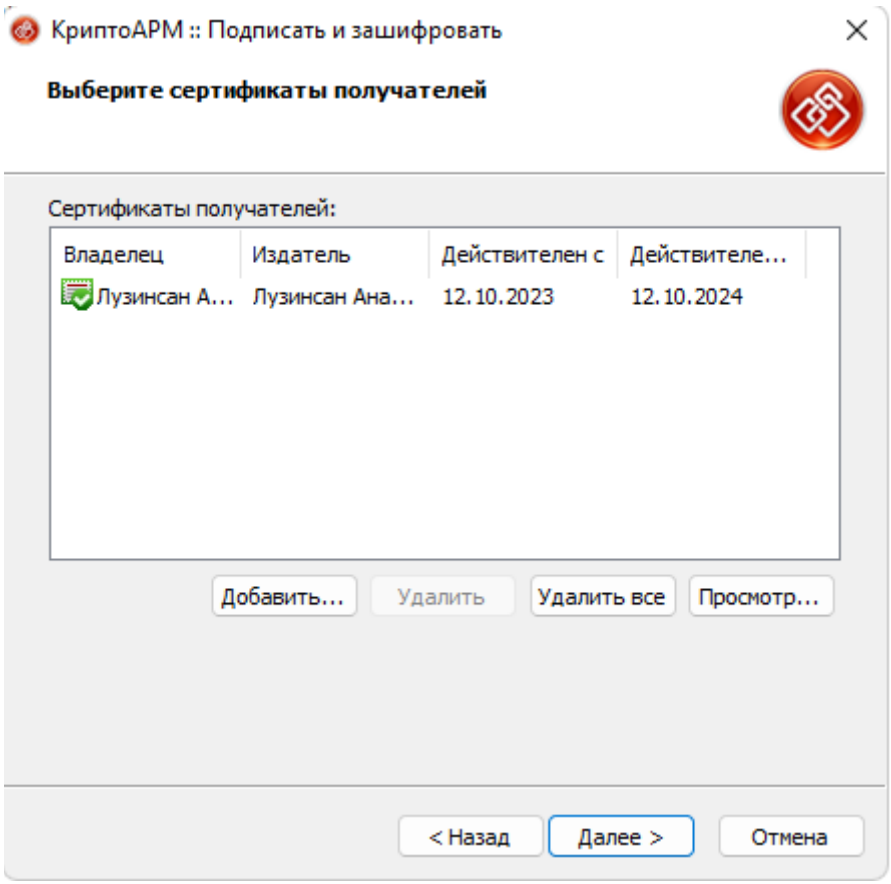

Рисунок 3.17 — Добавление сертификатов получателей

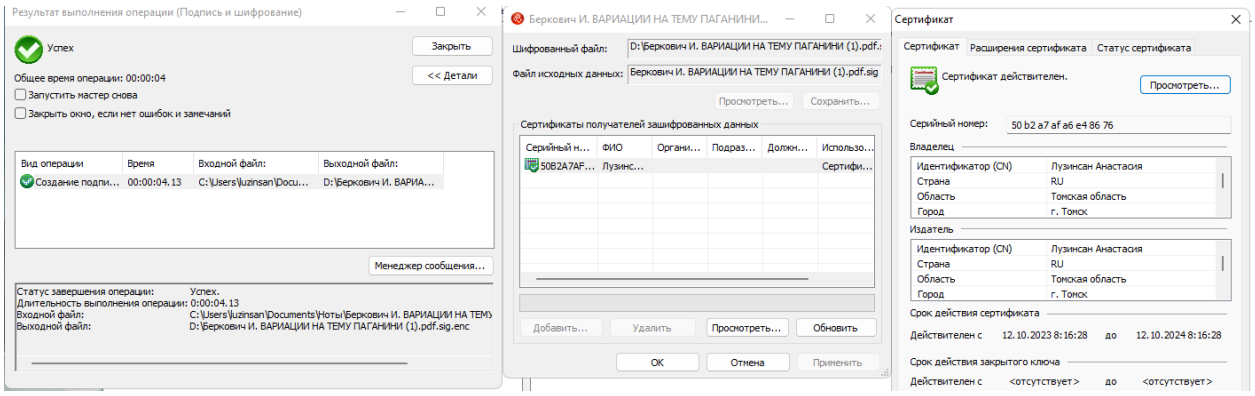

Рисунок 3.18 — Результат шифрования

3.4 Расшифрование и проверка подписи

С помощью программы «КриптоАРМ» пользователь-получатель можете расшифровать и проверить ЭП отдельного файла или группы файлов, папку с файлами (при этом каждый файл, входящий в указанную папку, будет расшифрован и проверена подпись) или расшифровать архивы.

После открытия мастера операции «Расшифрования и проверка подписи» и выбора настройки по-умолчанию, открывается раздел для выбора файлов с зашифрованными и подписанными данными. Выбрав соответствующие файлы, как показано на рисунке 3.19, матер переходит в раздел с настройкой сертификатов расшифрования, то есть именно того сертификата, в котором содержится закрытый ключ для расшифрования.

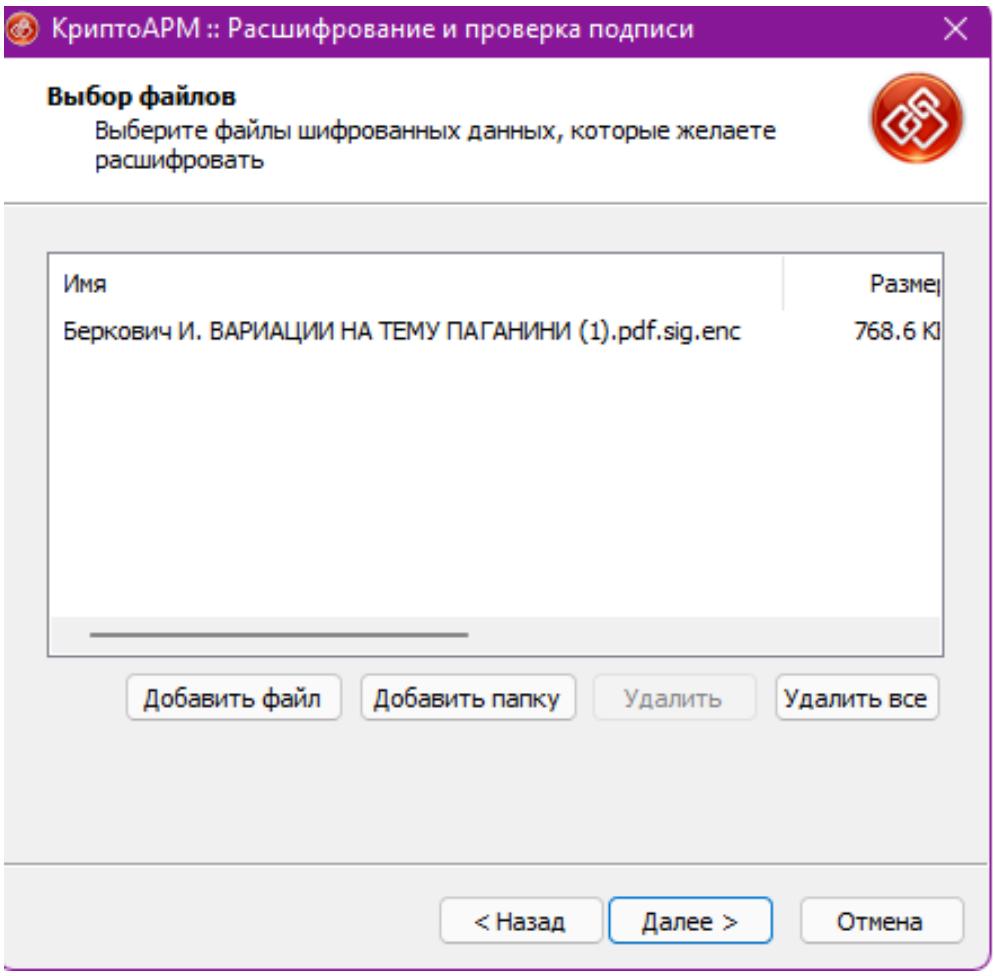

Рисунок 3.19 — Выбора файлов для расшифрования получателем

В данном разделе также содержатся настройки режима сохранения расшифрованных файлов, в том числе указание пути сохранения файла. Итоговые настройки показаны на рисунке 3.20.

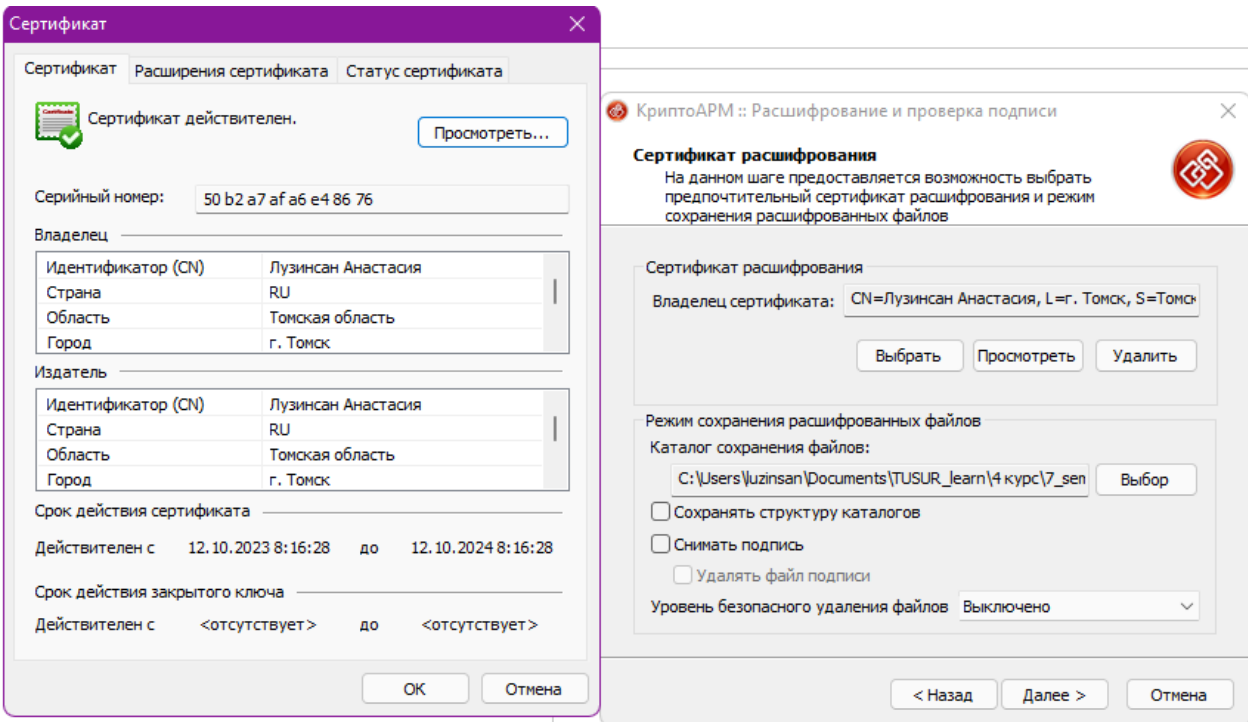

Рисунок 3.20 — Настройки сертификата расшифрования и режима сохранения расшифрованных файлов

Далее мастер переходит в обзорный раздел, в котором указаны все данные, как показано на рисунке 3.21.

Нажимая на кнопку «Готово», мастер выполняет расшифрование и отображает результат, как показано на рисунке 3.22.

Переходя в «Менеджер сообщения» можно просмотреть статус подписи сертификатом отправителя, как показано на рисунке 3.23. Как видно из изображения, статус сертификата и подписи «подтверждён». В этом же окне можно сохранить расшифрованный документ.

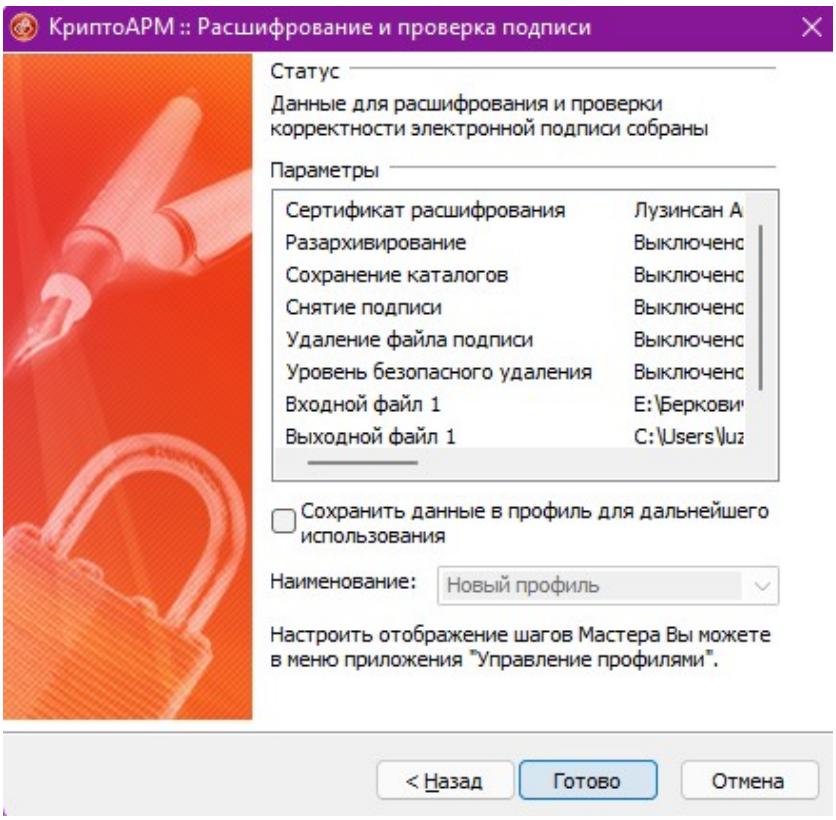

Рисунок 3.21 — Общие сведения настройки расшифрования и проверки подписи

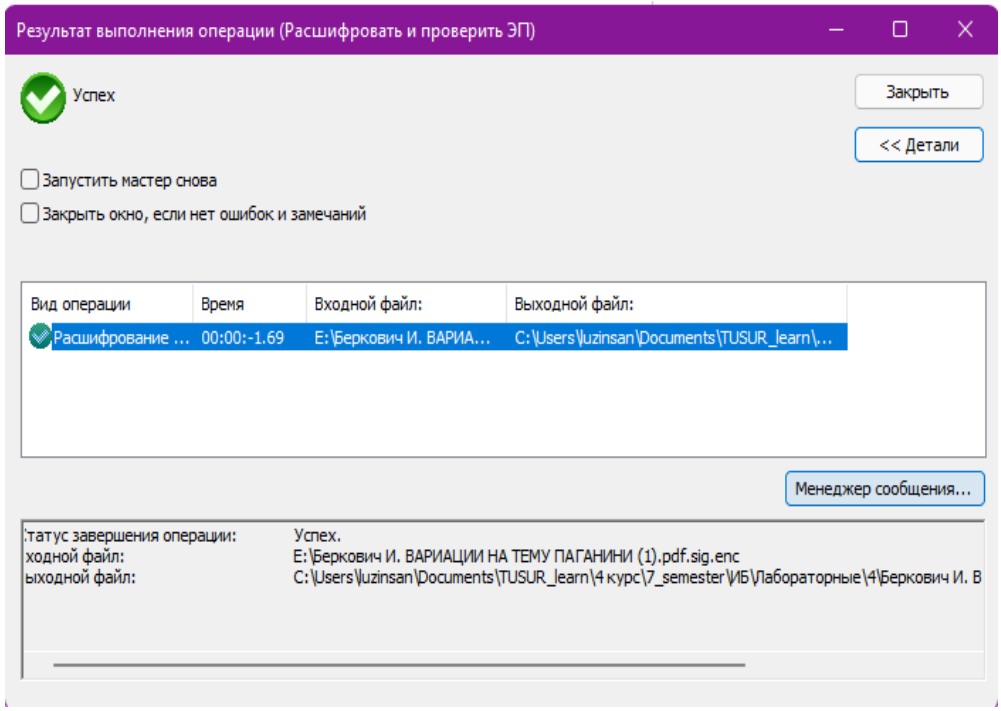

Рисунок 3.22 — Результат расшифрования файла

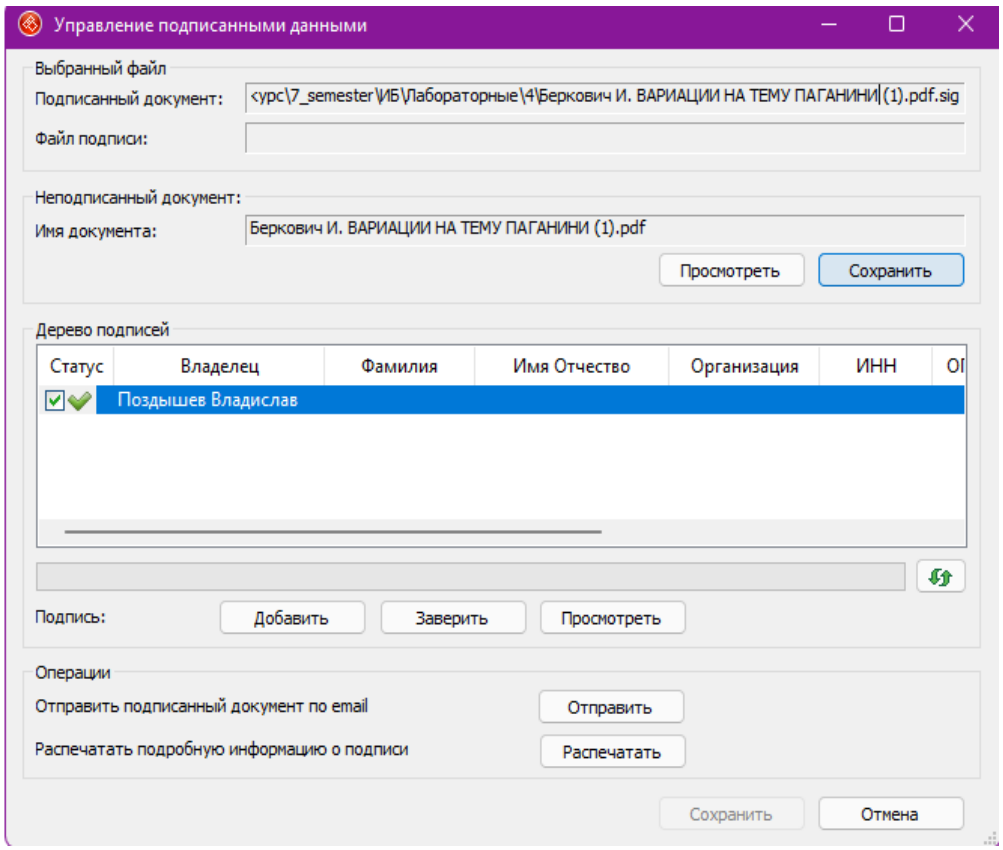

Рисунок 3.23 — Проверка подписи сертификата отправителя

4 ПОЛУЧЕННЫЕ В РЕЗУЛЬТАТЕ РАБОТЫ ФАЙЛЫ

В результате шифрования данным отправителем был получен подписанный и зашифрованный файл: *Беркович И. ВАРИАЦИИ НА ТЕМУ ПАГАНИНИ.pdf.sig*. Расширение этого файла «.sig» означает, что данный файл был подписан с помощью Base64 encoded X.509, в свою очередь расширение .enc означает, что данный файл зашифрован. Часть содержимого зашифрованного файла можно посмотреть на рисунке 4.2.

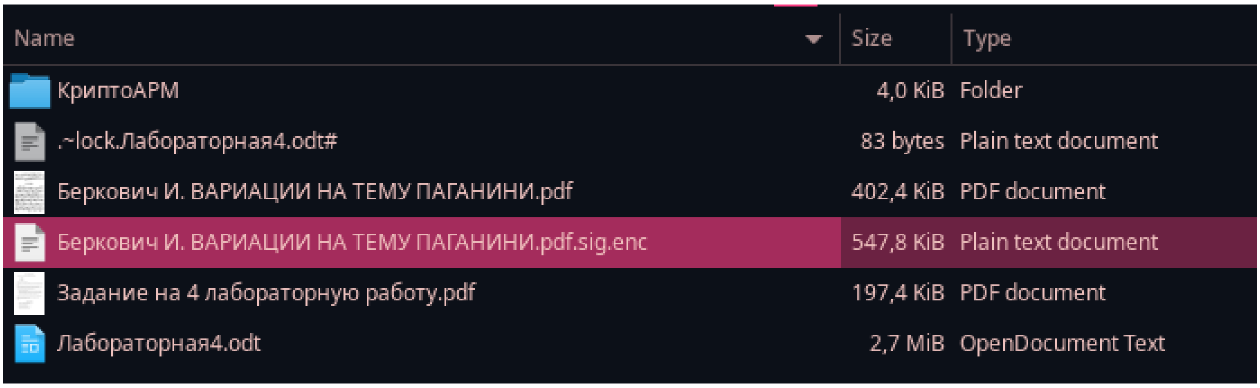

Рисунок 4.1 — Наличие подписанного и зашифрованного файла в каталоге получателя

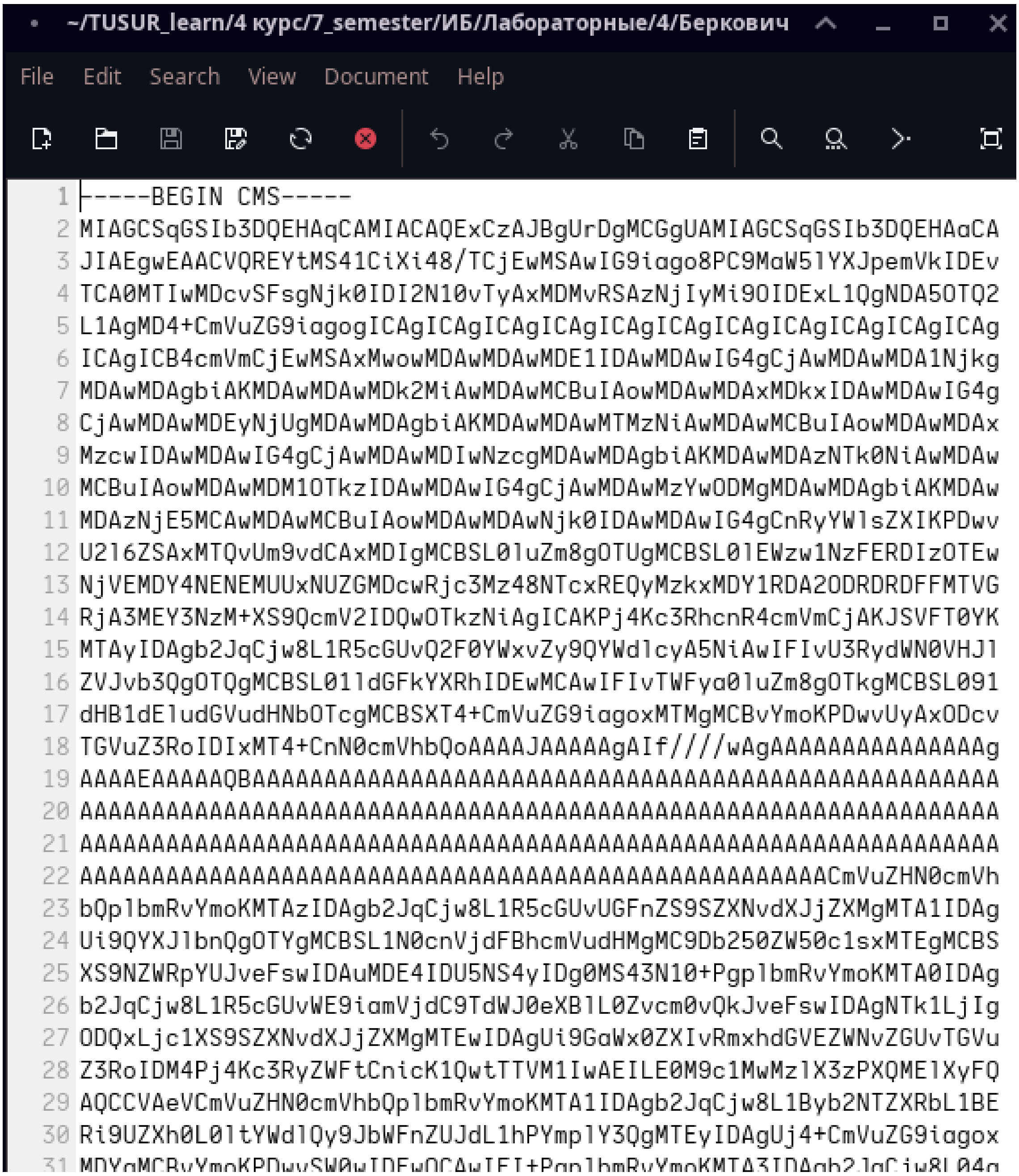

Рисунок 4.2 — Содержимое зашифрованного файла

5 ОТВЕТЫ НА ВОПРОСЫ С ПОЯСНЕНИЯМИ

1. Что такое – электронная цифровая подпись?

Электронная цифровая подпись - это криптографический метод аутентификации и обеспечения целостности данных. Она позволяет подписывающей стороне (обычно отправителю) создать уникальную цифровую подпись для документа или сообщения с использованием своего закрытого ключа. Эта подпись может быть проверена другими сторонами с использованием открытого ключа подписывающей стороны, чтобы убедиться в том, что данные не были изменены и их отправитель действительно является тем, за кого себя выдаёт

2. Основное назначение сертификата открытого ключа?

Основное назначение сертификата открытого ключа - это удостоверение подлинности открытого ключа, принадлежащего конкретной сущности (например, лицу или организации). Сертификаты открытых ключей используются в инфраструктуре открытых ключей (PKI) для обеспечения доверия к открытым ключам, используемым в процессе шифрования, аутентификации и проверки электронных подписей.

3. Что включает в себя сертификат?

Сертификат включает в себя информацию о владельце открытого ключа, сам открытый ключ, срок его действия и цифровую подпись удостоверяющего центра, который подтверждает подлинность этого сертификата.

4. Что привело к необходимости создания PKI.

Необходимость создания PKI вызвана необходимостью обеспечения безопасности и доверия в электронных коммуникациях. С использованием PKI можно эффективно управлять открытыми ключами, обеспечивать аутентификацию, конфиденциальность и целостность данных, а также

создавать электронные цифровые подписи.

5. Какие задачи позволяет решать PKI.

• Аутентификацию - подтверждение подлинности участников коммуникации.

• Конфиденциальность - защита данных от несанкционированного доступа.

• Целостность - гарантированное отсутствие изменений данных в процессе передачи.

• Невозможность отказа - возможность доказать, что конкретная сторона создала электронную подпись.

• Управление ключами - безопасное управление ключами шифрования и подписи.

6. Основные компоненты PKI и их функции включают:

• Удостоверяющий центр (CA): Выпускает сертификаты открытых ключей, подтверждая их подлинность.

• Регистрационный центр (RA): Проверяет подлинность запросов на сертификацию и передает их CA.

• Серверы директории: Хранят и распространяют сертификаты.

• Субъекты: Лица или устройства, использующие сертификаты для аутентификации и обеспечения безопасности.

PKI обеспечивает инфраструктуру для создания и управления сертификатами открытых ключей, что позволяет обеспечить безопасность электронных коммуникаций и аутентификацию в цифровом мире.

6 Вывод о проделанной работе

В результате выполнения лабораторной работы я освоила процесс создания ключей, распространения открытых и сохранения в тайне закрытых ключей, а также шифрования, расшифрования, создания и подтверждения электронных подписей в криптосистемах.