МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«16» 05 2024 г.

Методы и средства защиты информации в системах электронного документооборота

Методические указания по выполнению лабораторных работ по дисциплине «Методы и средства защиты информации в системах электронного документооборота» для студентов направления подготовки 10.04.01 «Информационная безопасность»

Курск 2024

УДК 004

Составители: Таныгин М.О

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Методы и средства защиты информации в системах электронного документооборота: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. – Курск, 2024. – 70 с.: Библиогр.: с. 70.

Содержат сведения по вопросам формирования у студентов знаний в области методов и средств защиты информации в системах электронного документооборота, а также развития в процессе обучения системного мышления, необходимого для решения задач управления в области информационной безопасности.

Методические указания по выполнению лабораторных работ по дисциплине «Методы и средства защиты информации в системах электронного документооборота» предназначены для студентов направления подготовки 10.04.01 «Информационная безопасность».

Текст печатается в авторской редакции
Подписано в печать 16.05.24 . Формат 60x84 1/16.
Усл. печ.л. 4,2 Уч. –изд.л. 4,1. Тираж 50 экз. Заказ 408
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Лабораторная работа № 1. Механизмы обеспечения информационной безопасности электронных документов

1. Теоретические сведения

Техническое обеспечение электронной цифровой подписи основано на использовании методов криптографии.

Любой документ можно рассматривать как уникальную последовательность символов. Изменение хотя бы одного символа в последовательности будет означать, что в результате получится уже совсем другой документ, отличный от исходного.

Чтобы последовательность символов, представляющих документ, могла, во-первых, идентифицировать ее отправителя, а во-вторых, подтвердить ее неизменность с момента отправления, она должна обладать уникальными признаками, известными только отправителю и получателю сообщения. Для этого используются различные средства шифрования, создаваемые и изучаемые наукой криптографией.

Для шифрования и дешифрования информации необходимо знать **метод** и **ключ шифрования**.

Метод шифрования — это формальный алгоритм, описывающий порядок преобразования исходного сообщения в результирующее.

Ключ шифрования — это набор параметров (данных), необходимых для применения метода. Так, например, буквы любой последовательности символов можно заменить на соответствующие комбинации цифр — это метод шифрования. А конкретное указание, какую букву заменить на какую последовательность цифр, является ключом.

Существуют **симметричные** и **асимметричные** методы шифрования.

Симметричный метод шифрования состоит в том, что партнер создает ключ шифрования, который передает другому партнеру. Сообщение шифруется и дешифруется **одним** ключом. Этот алгоритм трудно напрямую использовать, например, в электронной коммерции, так как возникает проблема идентификации удаленного партнера.

Несимметричная (асимметричная) криптография использует специальные математические методы. В результате применения этих методов создается пара ключей: то, что зашифровано одним ключом, может быть дешифровано другим, и наоборот. Владелец ключей один оставляет у себя, а другой может распространить, например, прямой рассылкой через Интернет. Ключ, оставленный у владельца, называется закрытым или личным (ключ электронной подписи), другой — открытым или публичным (ключ проверки электронной подписи)

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи (Ст. 2. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи").

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи) (Ст. 2. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи").

Закрытый ключ может быть скомпрометирован различными способами:

- хищение ключа путем копирования в результате несанкционированного доступа к оборудованию (прямого или удаленного), на котором он хранится;
- получение ключа путем ответа на запрос, использованный с признаками мошенничества или подлога;
- хищение ключа в результате хищения оборудования, на котором он хранится;
- хищение ключа в результате сговора с лицами, имеющими право на его использование (даже рядовой факт увольнения сотрудника, имевшего доступ к закрытому ключу организации, рассматривается как компрометация ключа).

Незаконность данных традиционных методов компрометации обеспечивает законодательство.

Это не относится к нетрадиционным методам реконструкции закрытого ключа по исходным данным, полученным вполне легально, в частности по открытому ключу. Возможность реконструкции определяется тем, что открытый и закрытый ключи связаны определенными математическими соотношениями. Теоретически знание открытого ключа дает возможность восстановить закрытый ключ. Однако на практике это связано с наличием специальных программных и аппаратных средств и огромными затратами вычислительного времени. Существует специальная отрасль науки, называемая криптоанализом, которая позволяет воспроизводить зашифрованную информацию и оценить степень защиты информации.

Поскольку от алгоритмов, на основе которых действует средство ЭП, зависит надежность и устойчивость документооборота, к средствам ЭП предъявляются специальные требования.

Средства электронной подписи - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи (Ст. 2. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи").

2. Задание на лабораторную

Для сдачи данной практической работы необходимо оформить отчет в формате .doc. В отчете необходимо представить подтверждение выполнения следующих действий в виде скриншотов:

1. Установить приложение Kleopatra:

- пользователи **Windows** найдут инструкции по установке и использованию программы Kleopatra в следующих разделах данной книги

- пользователи **MacOS** могут скачать методические указания по ссылке

- пользователи **Linux** могут скачать методические указания по ссылке

2. Сгенерировать в Kleopatra новую пару ключей (открытый + закрытый) по алгоритму RSA

3. Экспортировать открытый ключ в файл и передать его партнеру (одногруппнику (-це)) по электронной почте

4. Получить открытый ключ партнера (файл с расширением .asc) и импортировать его в Kleopatra, заверить своим закрытым ключом.

5. Создать файл формата .doc/.docx/.txt с текстом

6. Используя открытый ключ партнера, зашифровать для него созданный файл в Kleopatra и передать по его электронной почте

7. Расшифровать зашифрованный файл (сначала без подписи, затем с подписью) партнера своим закрытым ключом

8. Созданный в п.5 текстовый документ подписать своей электронной подписью и отправить партнеру два файла: сам документ и файл с подписью (***.sig).

9. Проверить электронную подпись партнера.

10. Изменить содержание документа и проверить электронную подпись повторно. Написать ответ на вопрос: почему после изменения содержания документа электронная подпись оказывается неверной.

3. Загрузка и установка приложения для шифрования и электронной подписи

1. Необходимо зайти на интернет-сайт GnuPG по ссылке (https://www.gpg4win.org/)
2. С помощью кнопки **Download Gpg4win** зайдите на страницу загрузки приложения GnuPG (рис .1).

Рис. 1. Главная страница сайта Gpg4win

3. Откроется страница для загрузки приложения. Здесь можно выбрать на свое усмотрение размер и способ вознаграждения разработчиков. Нажмите на кнопку **Download** для загрузки установочного файла приложения на компьютер.

4. Выберите необходимую директорию для загрузки установочного файла на компьютер.

5. Запустите установочный файл gpg4win-3.1.5.exe. Появится окно установки (рис. 3).

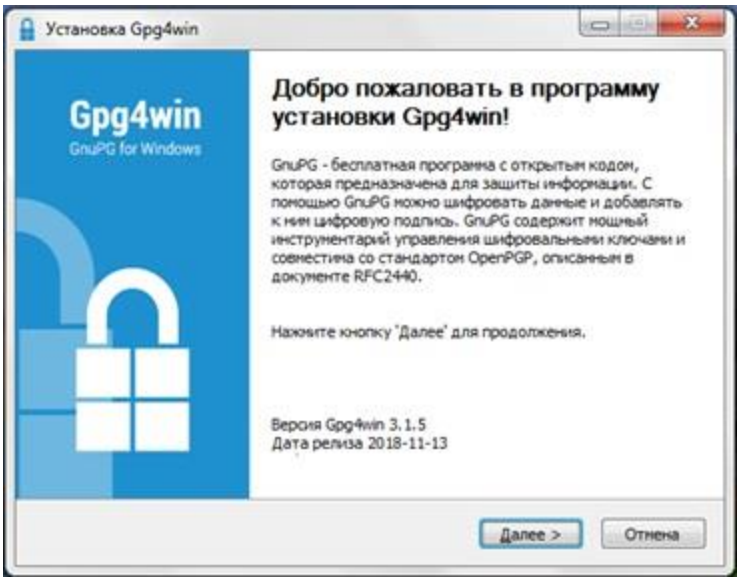


Рис. 3. Установка приложения GnuPG

6. Для выполнения заданий, предусмотренных данной практической работой необходимо из компонентов программы выбрать приложение Kleopatra (рис. 4). Вы можете ознакомиться с описанием остальных компонентов, и при необходимости их установить дополнительно.

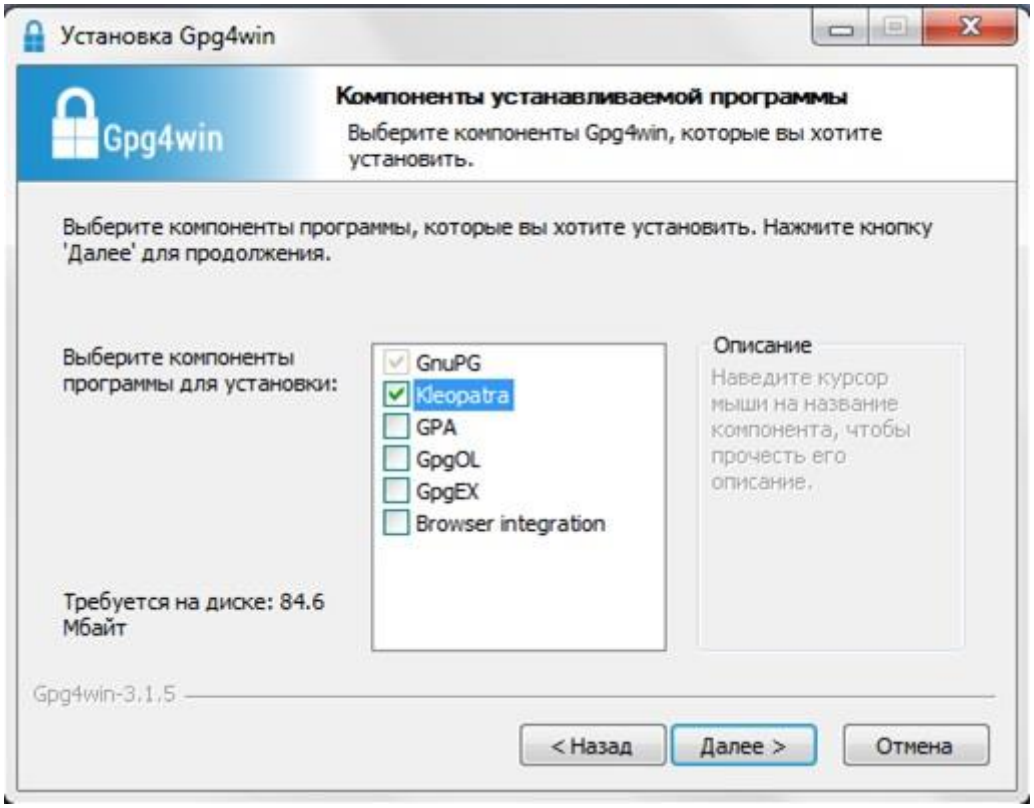


Рис. 4. Выбор компонентов устанавливаемого приложения

7. Выберите папку для установки приложения GnuPG (рис.5)

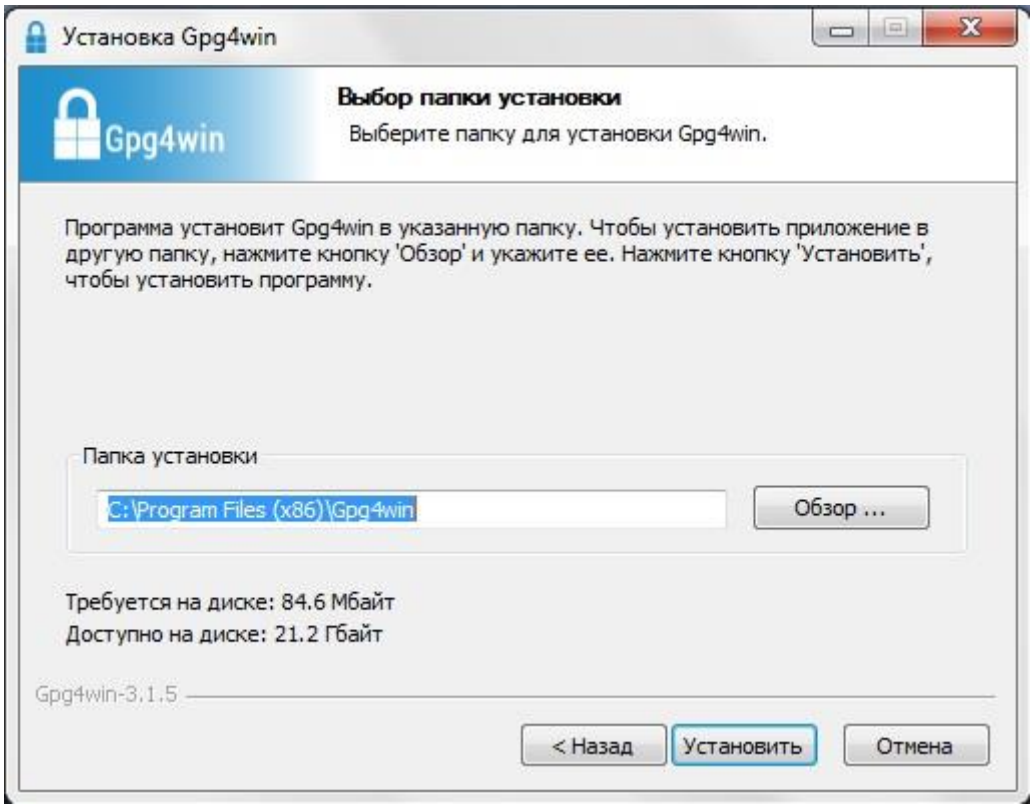


Рис. 5. Выбор папки для установки приложения GnuPG

8. Нажмите кнопку «Установить». После установки нажмите кнопку «Далее» для продолжения, затем Готово (рис. 6).

Рис. 6. Завершение установки приложения GnuPG

4. Создание пары ключей для шифрования и электронной подписи

1. Запустите приложение Kleopatra (рис. 7)

Рис. 7. Интерфейс приложения Kleopatra

2. Нажмите кнопку «Создать новую пару ключей». Появится окно «мастер создания пары ключей» (рис. 8). Введите свои регистрационные данные:

- Фамилия Имя (Отчество - необязательно)
- Адрес электронной почты

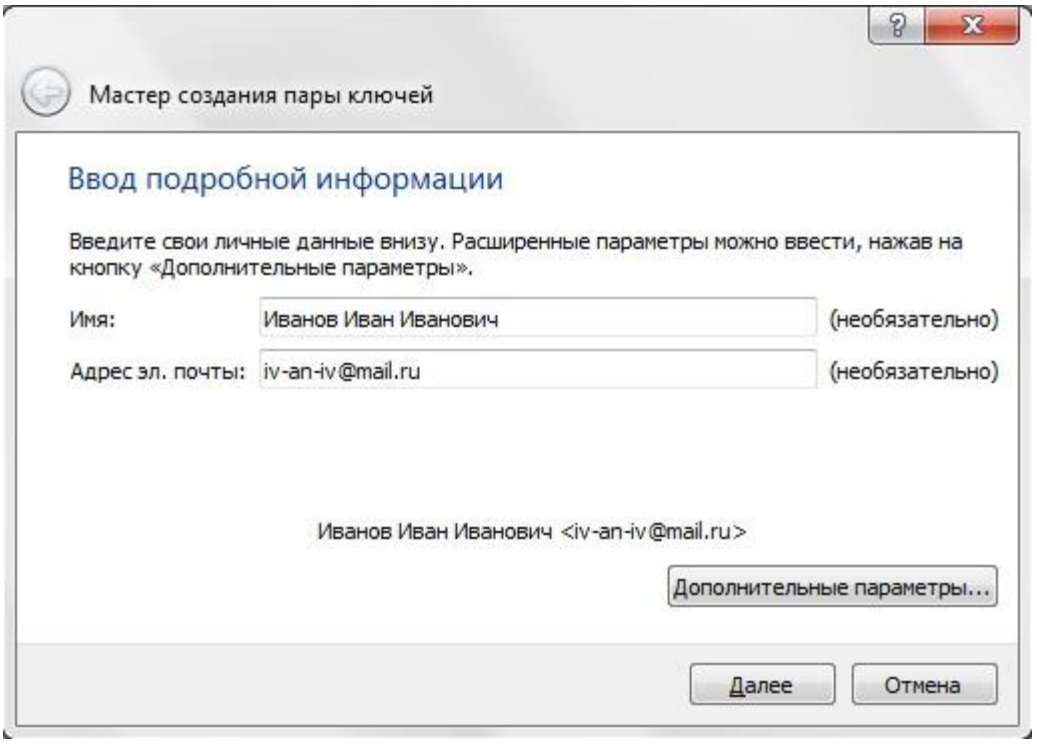


Рис. 8. Мастер создания пары ключей

3. Нажав кнопку «Дополнительные параметры» выйдет окно «Дополнительные параметры» (рис. 9), с помощью которого имеется возможность выбрать:

a) алгоритм шифрования (RSA, DSA, ECDSA/EdDSA)

b) длину ключа (2048, 3072, 4096 бит)

c) срок действия сертификата электронной подписи

d) и другие параметры

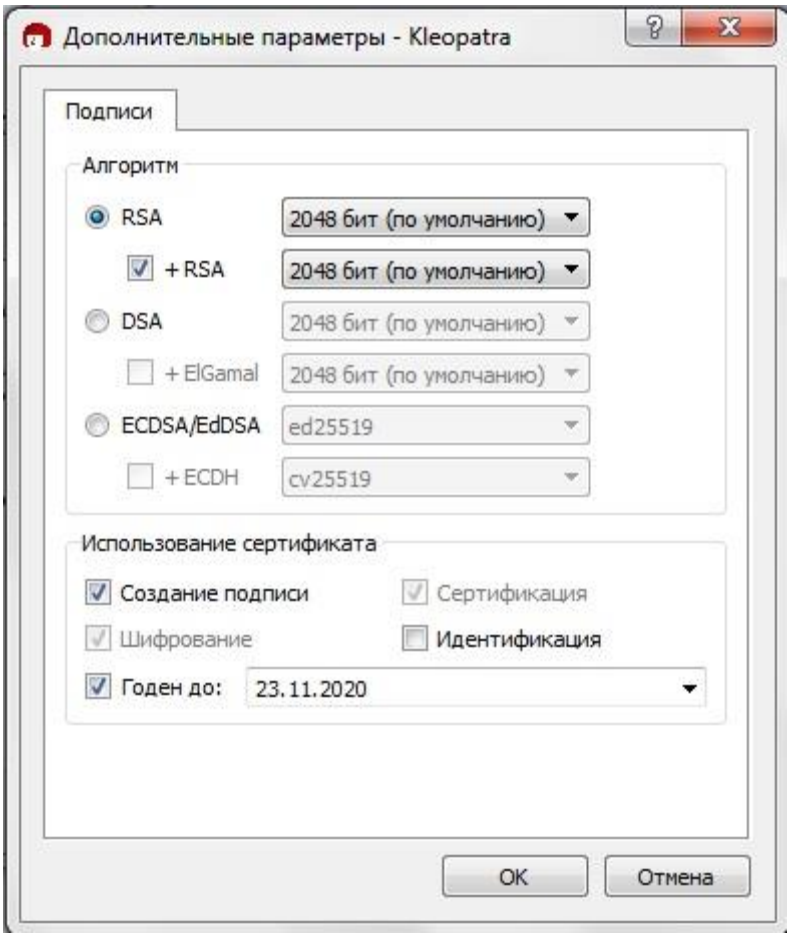


Рис. 9. Дополнительные параметры

4. Не изменяя настроек нажмите кнопку «Отмена» и выйдите из окна «Дополнительные параметры». Нажмите «Далее»

5. Откроется окно «Обзор параметров», в котором можно проверить введенные данные перед созданием пары ключей. Нажмите кнопку «Создать».

6. Программа попросит ввести фразу-пароль для защиты нового ключа. Введите фразу-пароль и подтвердите ее. Нажмите «ОК» (рис. 10).

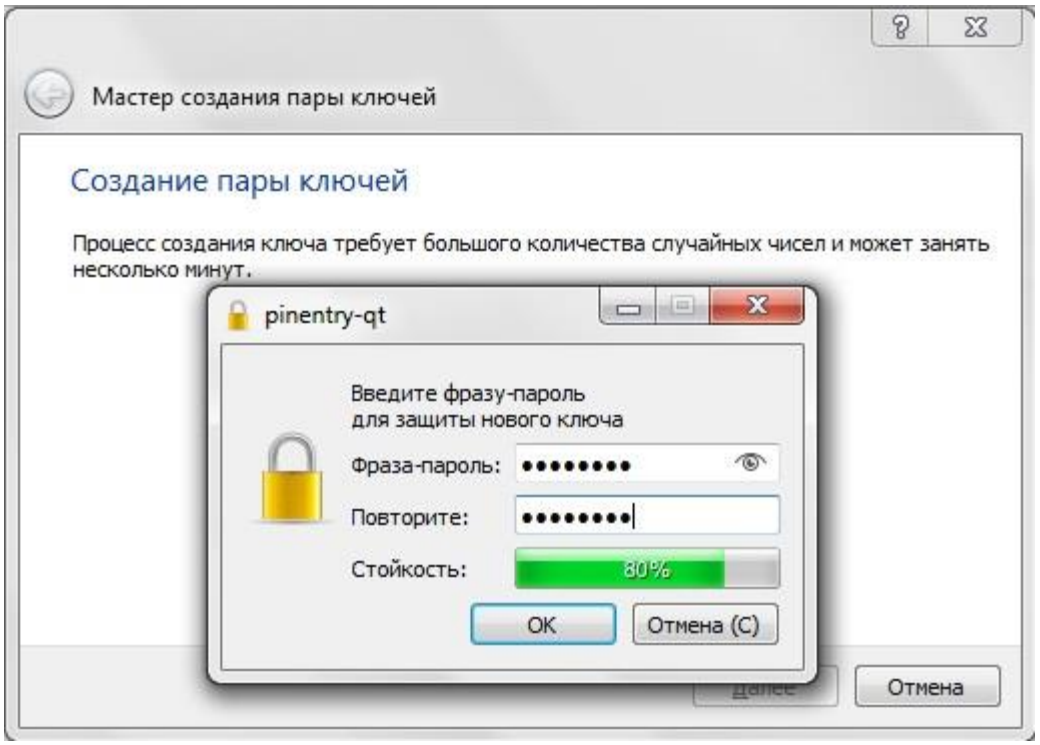


Рис. 10 Ввод фразы-пароля для защиты новых ключей

7. Об успешном создании новой пары ключей программа оповещает следующим окном (рис. 11). Нажмите кнопку «Завершить».

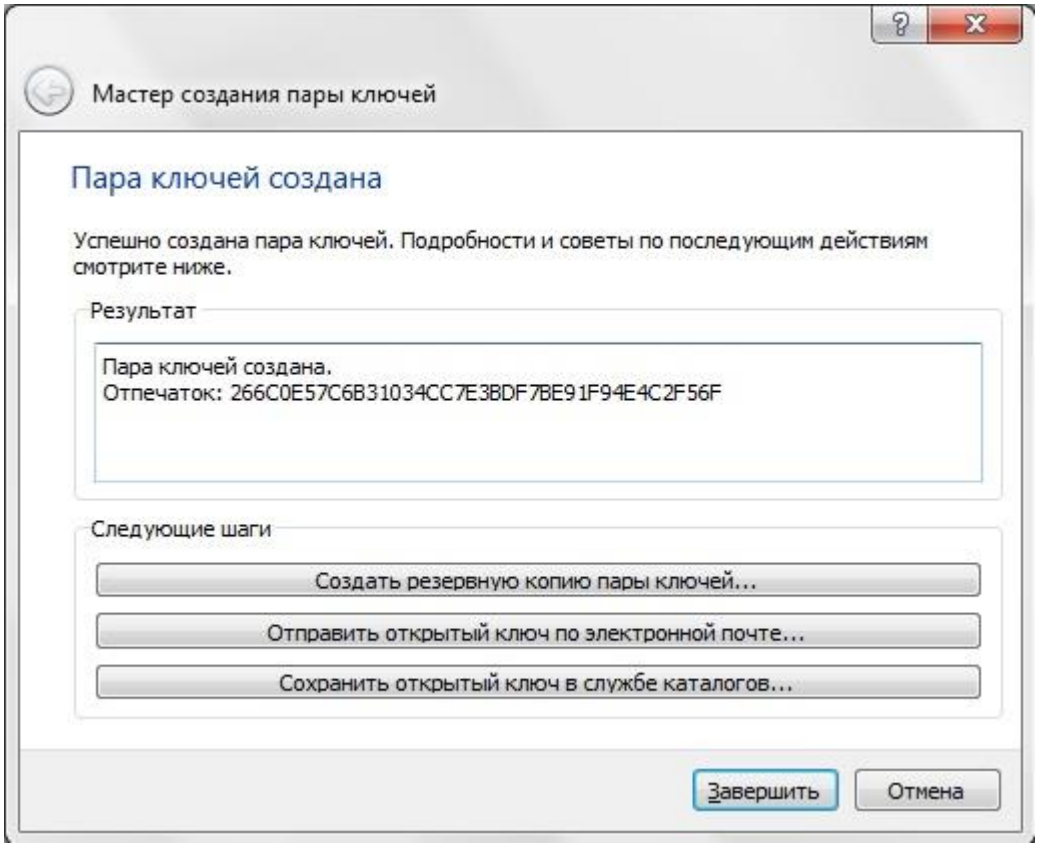


Рис. 11. Окно, оповещающее пользователя о создании новой пары ключей.

8. В списке сертификатов появится строчка, состоящая из имени пользователя, электронной почты, идентификатора пользователя, даты создания и окончания действия сертификата, а также идентификатора ключа (рис. 12). Полужирное начертание означает наличие пары ключей (открытого и закрытого).

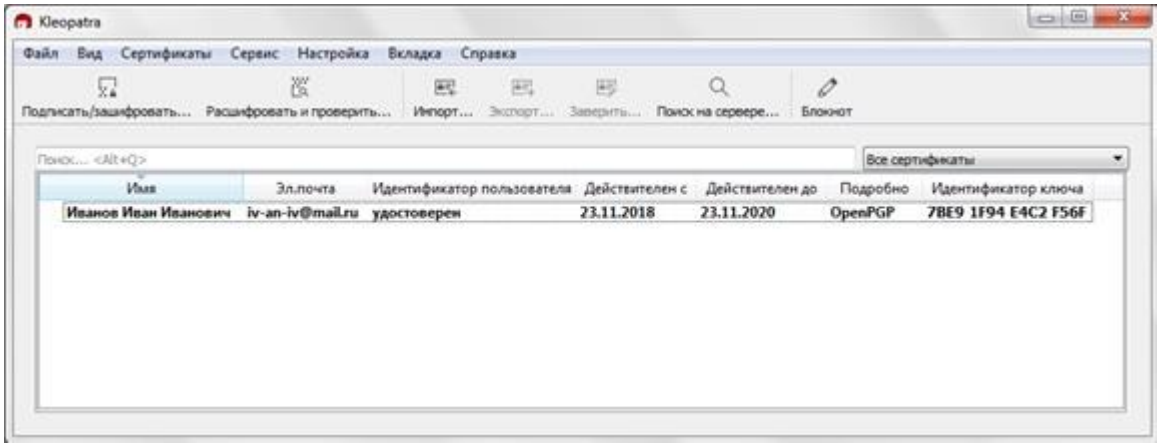


Рис. 12. Отображение сертификата в списке сертификатов после создания новой пары ключей

5. Экспорт открытого ключа в файл.

1. Для того, чтобы осуществлять шифрование и подпись файлов для передачи другим лицам, необходимо выполнить процедуру обмена открытыми ключами. Для этого сначала необходимо экспортировать открытый ключ в файл и передать его по какому-либо каналу связи.

2. Выберите сертификат, для которого необходимо выполнить экспорт открытого ключа в файл, нажав на него левой кнопкой мыши.

3. На панели инструментов нажмите кнопку **«Экспорт…»**

4. Выберите директорию, в которой будет располагаться экспортированный файл и нажмите «Сохранить». В данной директории появится файл с расширением .asc

5. Данный файл можно отправить другому лицу для того, чтобы:

- вам могли отправить файл, зашифрованный по вашему открытому ключу
- получатель имел возможность проверить вашу электронную подпись

6. Импорт стороннего открытого ключа (сертификата)

1. Допустим вы получили по электронной почте файл, содержащий открытый ключ другого лица. Для того, чтобы его можно было использовать данный открытый ключ для шифрования файлов или проверки электронной подписи, необходимо импортировать сертификат в приложение Kleopatra.

2. Нажмите кнопку **«Импорт…»**

3. Выберите файл, содержащий открытый ключ другого лица и нажмите «Открыть».

4. Появится окно, которое запросит от пользователя подтверждение операции, позволяющей заверить импортированный сертификат (открытый ключ), тем самым применяя дополнительную меру защиты, основанную на доверии к сертификатам, отпечаток которых был проверен с помощью информации, полученной по телефонному звонку, из визитки или после проверки на доверенном веб-сайте (рис.13). Нажмите кнопку «Да», чтобы заверить сертификат.

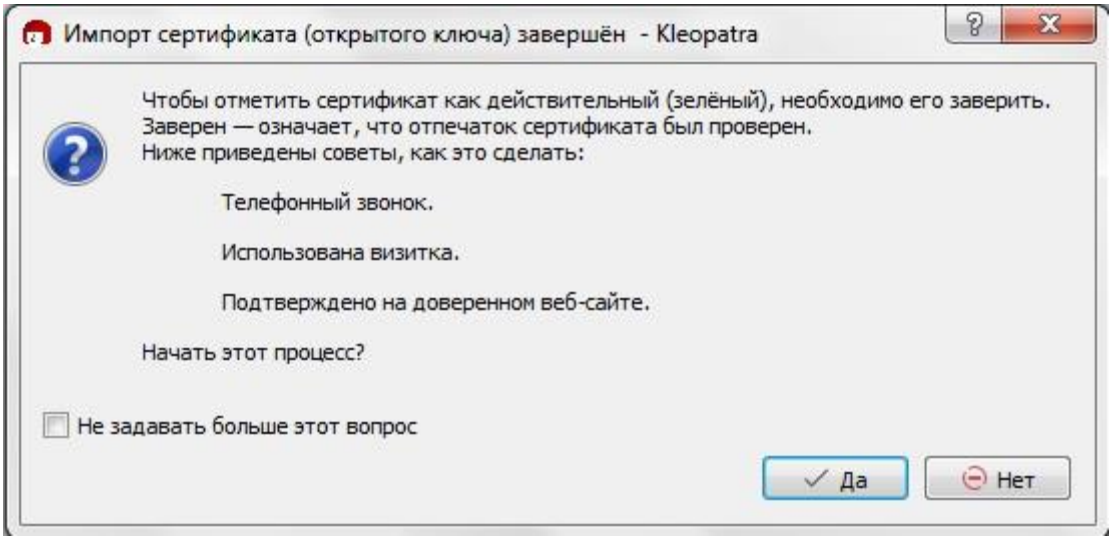


Рис. 13. Окно подтверждения операции, позволяющей заверить импортированный сертификат

5. Выберите сертификат, который будете заверять, поставив рядом с ним галочку. Проверьте контрольную сумму подписываемого сертификата с той, которую вам предоставил лично или другими безопасными способами партнер, сертификат которого вы заверяете (подписываете своим закрытым ключом). Если контрольные суммы совпадают, поставьте галочку рядом с надписью **«Я проверил контрольную сумму»** (рис. 14). Нажмите кнопку **«Далее»**.

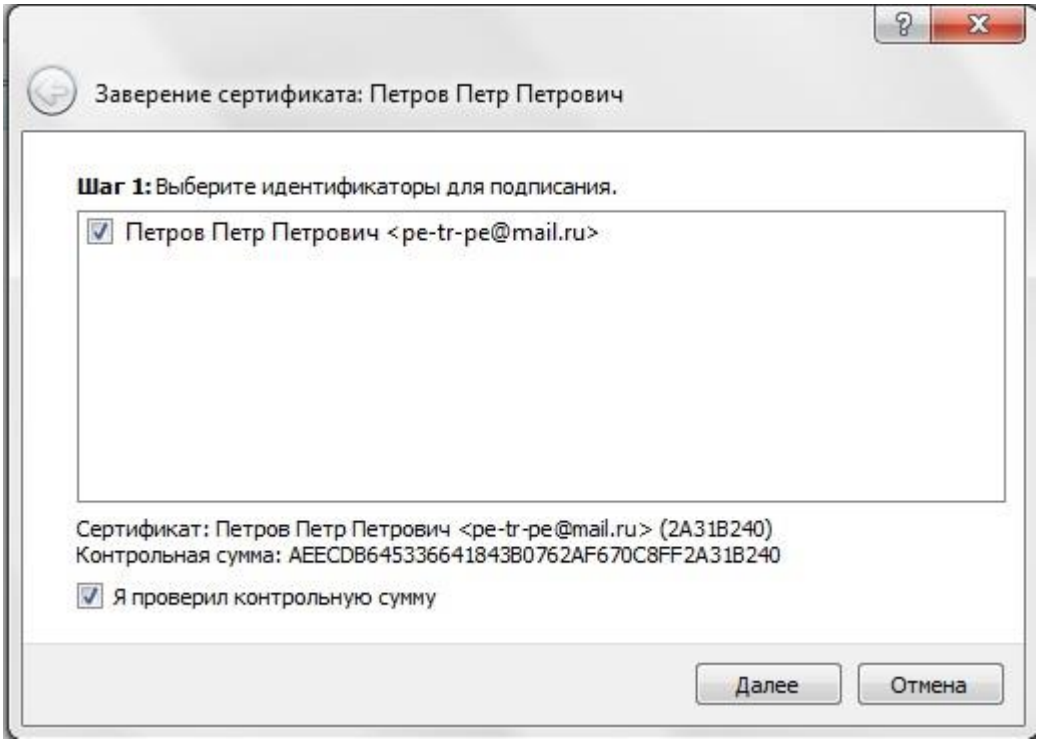


Рис. 14. Выбор подписываемого сертификата и проверка контрольных сумм.

6. В рамках выполнения данной практической работы необходимо выбрать способ удостоверения **«Удостоверить только для себя»** (рис. 15). Нажмите кнопку **«Заверить»**

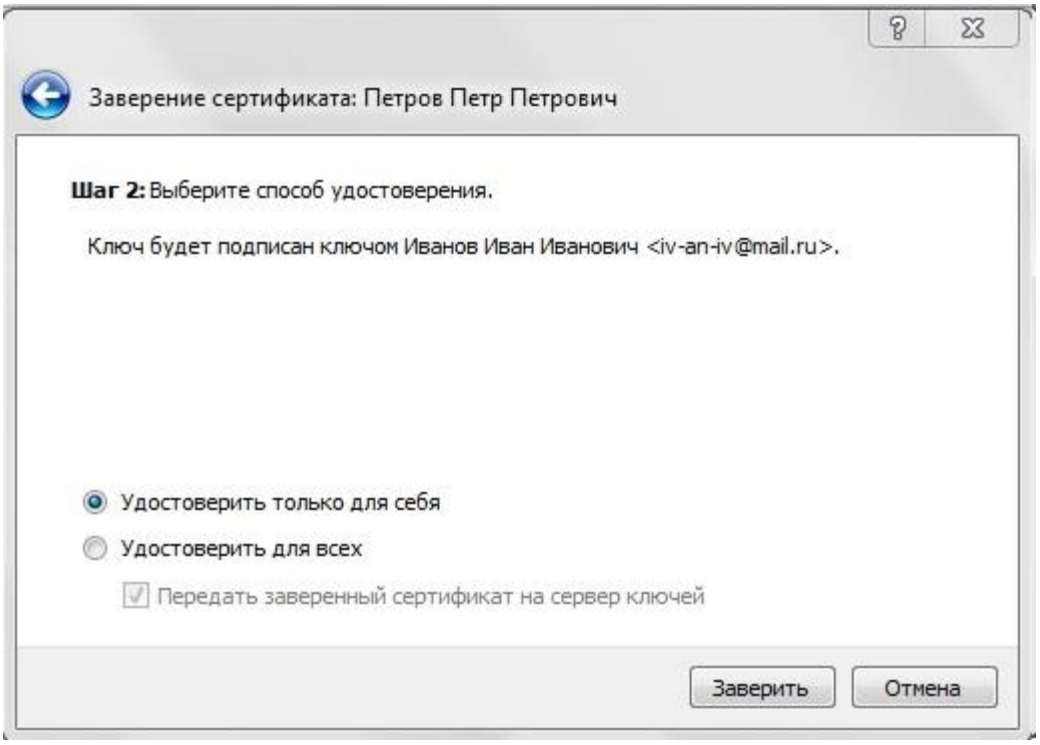


Рис. 15. Выбор способа удостоверения

7. Введи фразу-пароль для разблокировки вашего секретного ключа (которую вы вводили при создании пары ключей), чтобы с помощью него подписать импортированный сертификат (рис. 16). Нажмите **«ОК»**

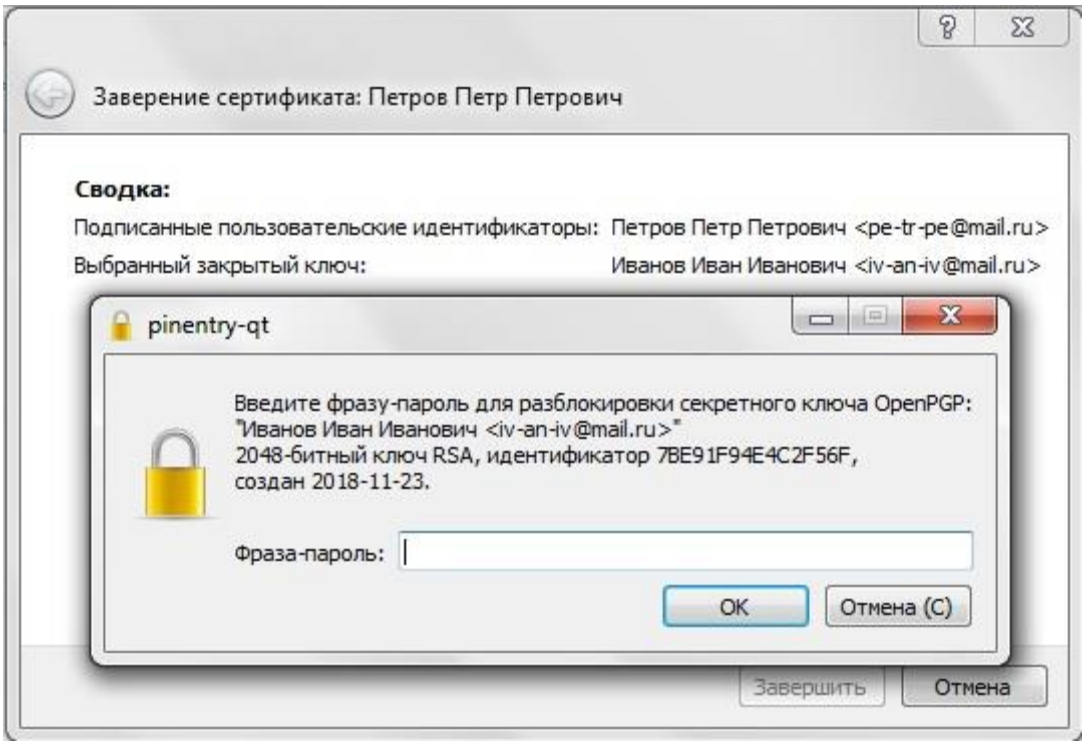


Рис. 16. Ввод фразы-пароля для разблокировки секретного ключа

8. Появится сообщение **«Успешно удостоверено»** (рис. 17).
Нажмите **«Завершить»**.

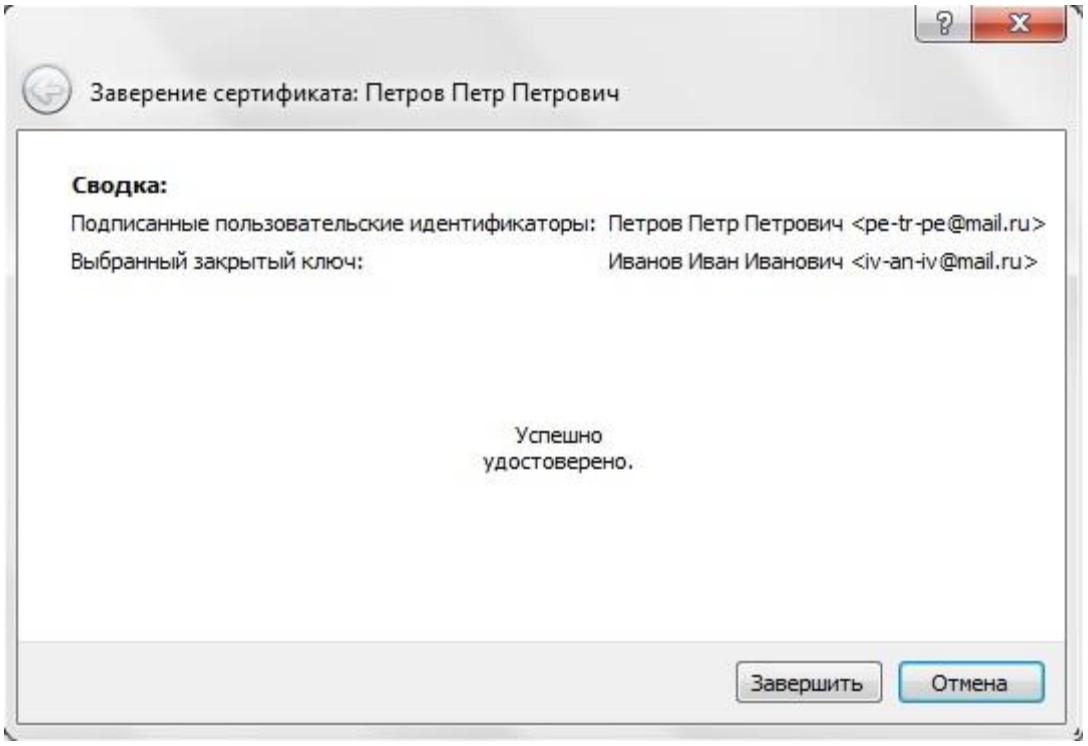


Рис. 17. Завершение процесса удостоверения сертификата.

9. В списке сертификатов появится импортированный сертификат. Его начертание будет обычное, так как он содержит только открытый ключ (рис. 18).

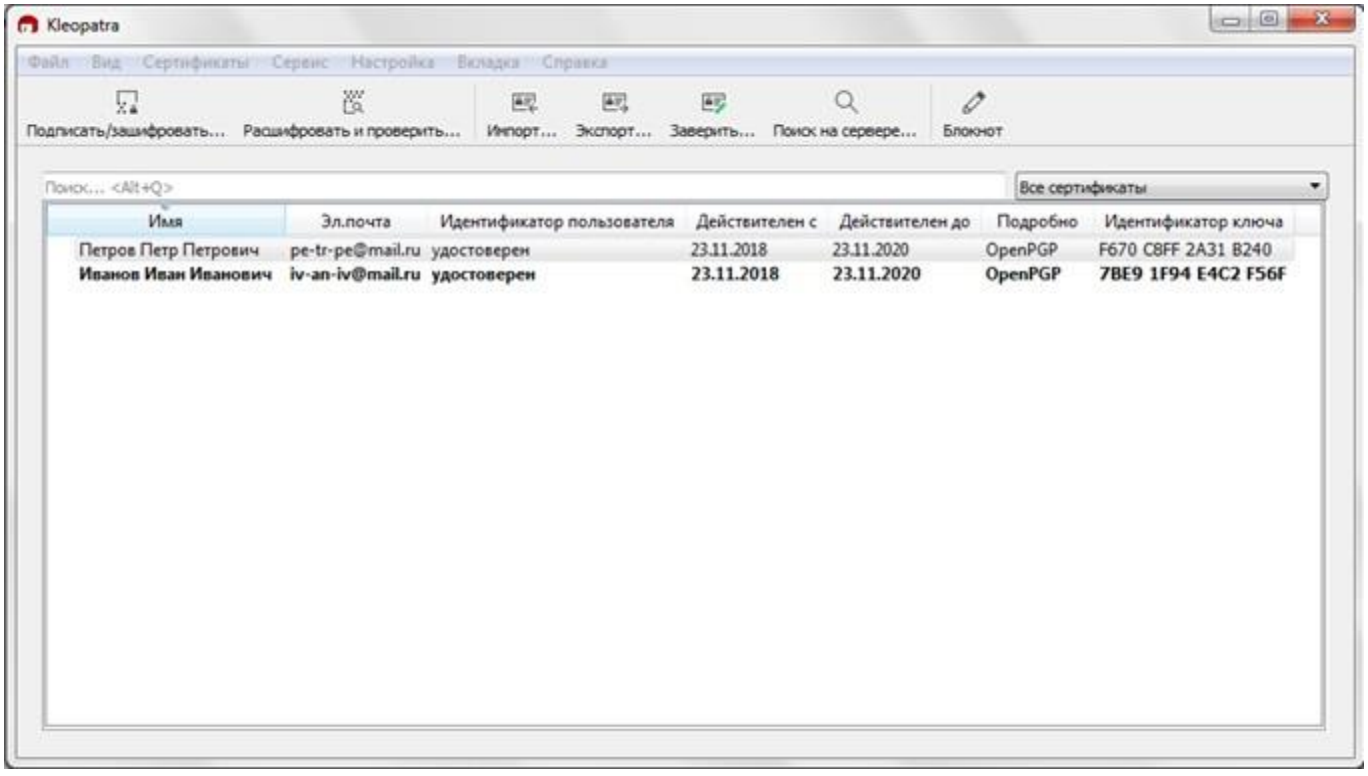


Рис. 18. Список сертификатов

Лабораторная работа № 2. Защищенные системы электронного документооборота

В данной главе рассматривается шифрование и расширование файлов с помощью приложения Kleopatra с электронной подписью и без электронной подписи.

7. Шифрование и расшифрование файлов

7.1. Шифрование и расшифрование файлов без подписи

1. В рамках данной практической работы будет рассмотрено шифрование файлов для передачи электронных документов с конфиденциальной информацией определенному лицу (данная программа также позволяет осуществлять шифрование файлов только для личного пользования). Так как в программе GnuPG используется ассиметричное шифрование, исходный файл будет зашифрован с помощью открытого ключа (сертификата) получателя. В предыдущих разделах был рассмотрен обмен сертификатами с помощью операций экпорта в файл и импорта из файла. У пользователя имеется пара своих ключей, и открытый ключ его партнера, который затем расшифрует зашифрованный файл своим секретным ключом.

2. Для дальнейшего шифрования необходимо подготовить электронный документ формата .doc/.docx с названием «Секретный документ.docx», содержащий текст «Конфиденциальная информация» (рис. 19).

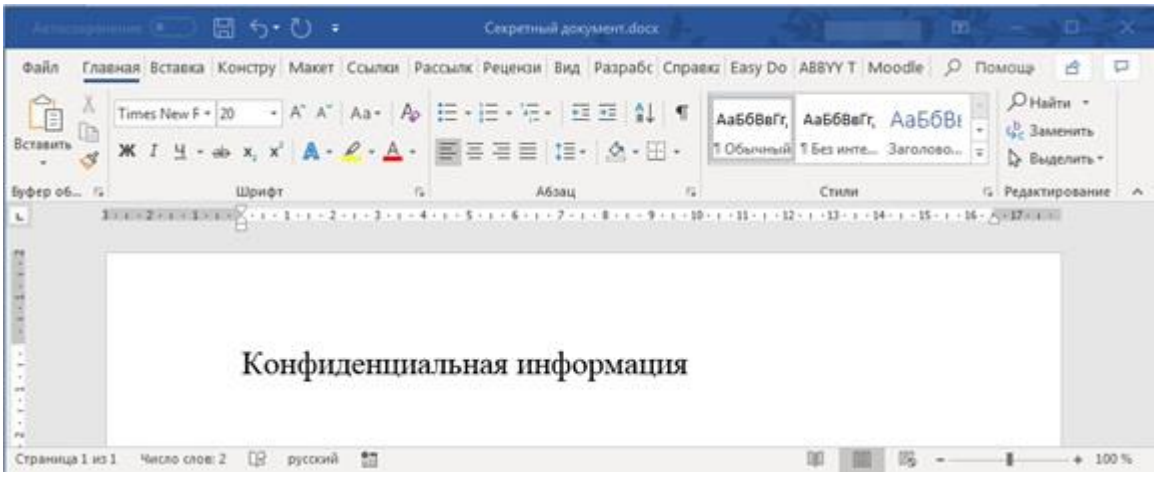


Рис. 19. Подготовленный документ для шифрования

3. В приложении Kleopatra нужно нажать кнопку **«Подписать/Зашифровать…»**

4. Далее необходимо выбрать файл для шифрования и нажать кнопку **«Открыть»**

5. В появившемся окне (рис. 20) выбираем (ставим галочки) в разделе Шифрование напротив пунктов **«Зашифровать для других»** и **«Зашифровать для себя»** (на тот случай, если возникнет необходимость расшифровать зашифрованные файлы для собственного пользования)

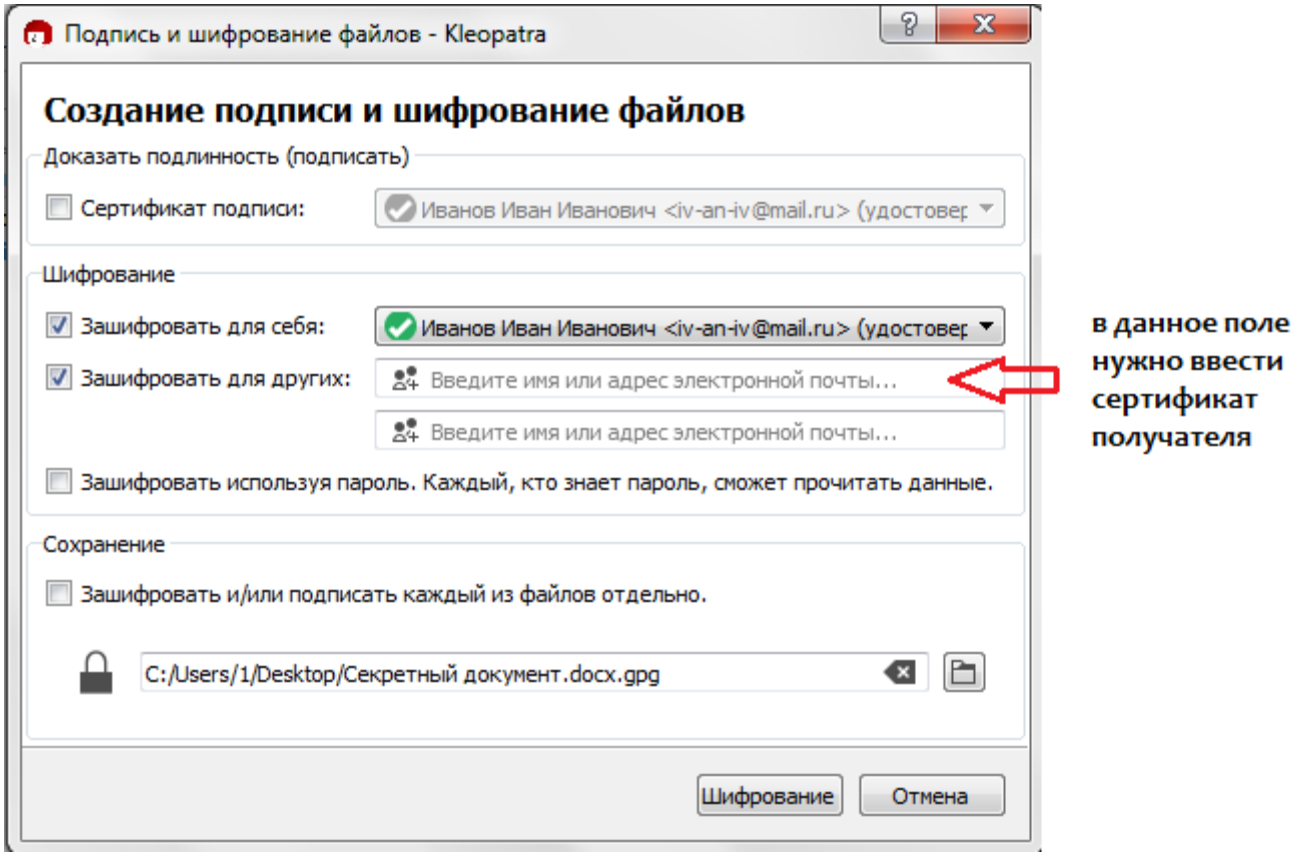


Рис. 20. Шифрование данных

6. Рядом с пунктом **«Зашифровать для других»** имеется поле ввода, где нужно выбрать сертификат партнера, которому будет направлено зашифрованное сообщение.

7. В дополнение к шифрованию с использованием открытых ключей получателя, возможно зашифровать данные, используя пароль. Любой, кто знает пароль, сможет прочесть данные без закрытого ключа. Использование пароля, даже очень сложного менее безопасно, чем использование шифрования на основе двухключевой криптосистемы. В данной работе использование пароля для шифрования файлов не используется, поэтому галочку рядом с пунктом «Зашифровать используя пароль…» ставить не надо.

8. Далее необходимо нажать на кнопку **«Шифрование»**. Если шифрование произошло успешно, будет отображено следующее окно (рис. 21)

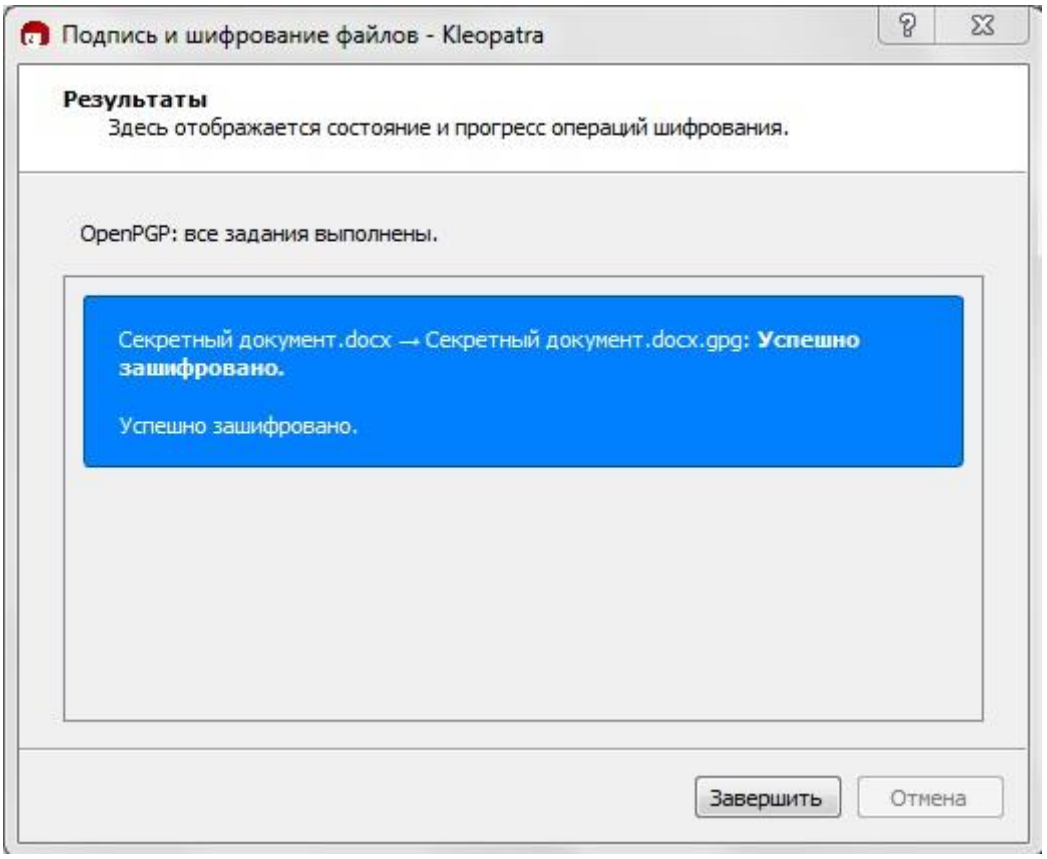
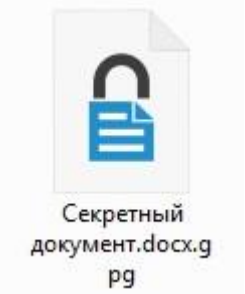


Рис. 21. Завершение шифрования файлов

9. После шифрования в назначенной директории появится зашифрованный файл **«Секретный документ.docx.gpg»**



10. Для расшифровки полученного файла необходимо в приложении **Kleopatra** нажать на кнопку **«Расшифровать и проверить…»**

11. Выберите зашифрованный файл, который заканчивается на .gpg и нажмите «Открыть». Появится окно «Расшифровка и проверка файлов», где необходимо ввести фразу-пароль для разблокировки секретного ключа (рис. 22)

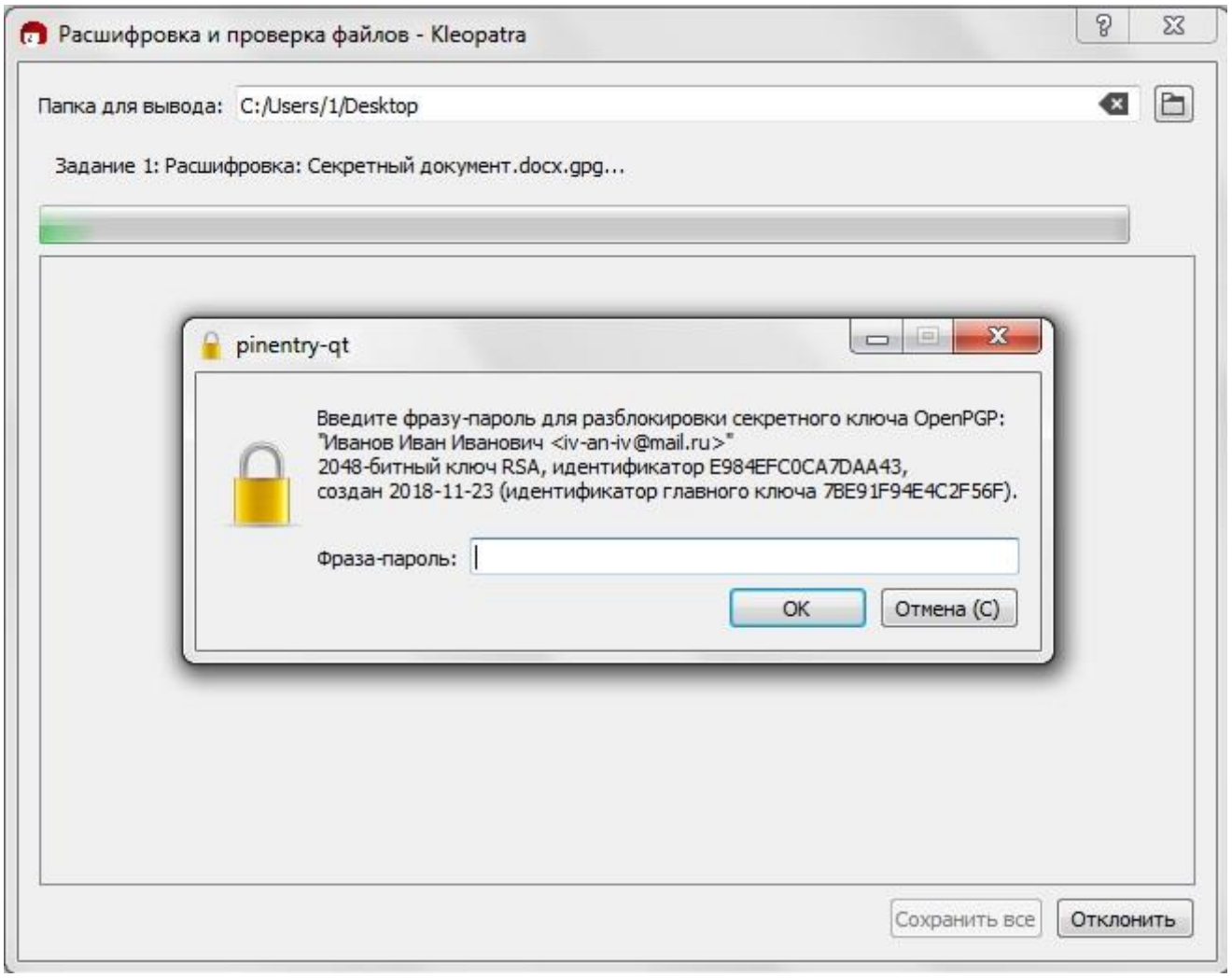


Рис. 22. Расшифровка и проверка файлов

12. После ввода фразы-пароля нажмите **«ОК»**. Приложение расшифрует файл в указанную директорию и сообщит пользователю о завершении процесса расшифровки (рис. 23). Чтобы закрыть окно и сохранить расшифрованный файл нажмите **«Сохранить все»**

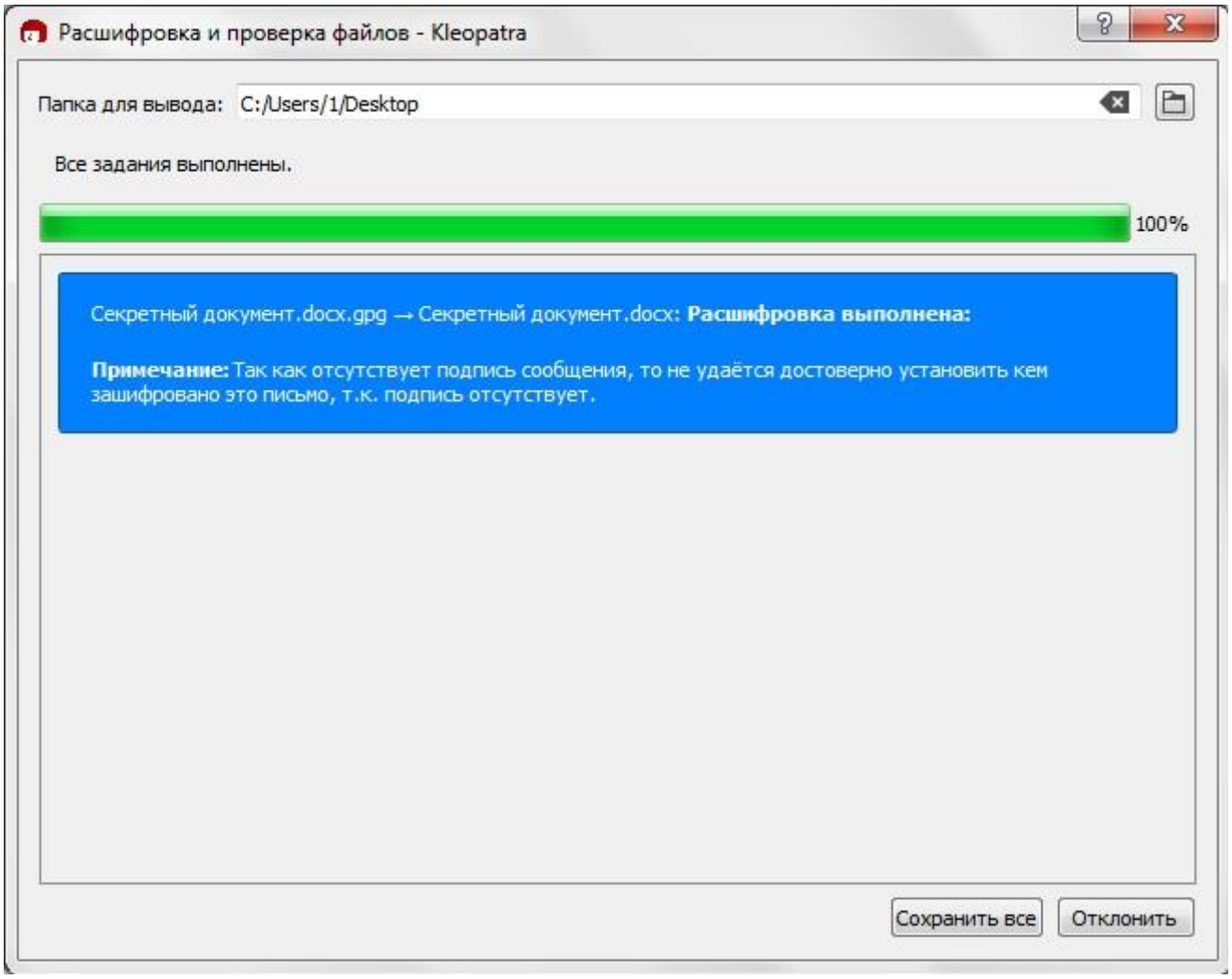


Рис. 23. Расшифровка файла выполнена.

13. Так как шифрование происходило без подписи, то будет отображено примечание, которое имеет следующее содержание: *«Так как отсутствует подпись сообщения, то не удается достоверно установить кем зашифровано это письмо, т.к. подпись отсутствует».*

7.2. Шифрование и расширование файлов с подписью

14. Если помимо шифрования необходимо, чтобы получатель мог установить кем был зашифрован файл, то можно дополнительно подписать зашифрованный файл сертификатом отправителя, поставив галочку напротив пункта **«Сертификат подписи»** и выбрать нужный сертификат (см. п. 5 данного раздела, рис. 20). После шифрования приложение оповестит пользователя, что шифрование и подпись прошли успешно (рис. 24). После этого нужно нажать кнопку **«Завершить».**

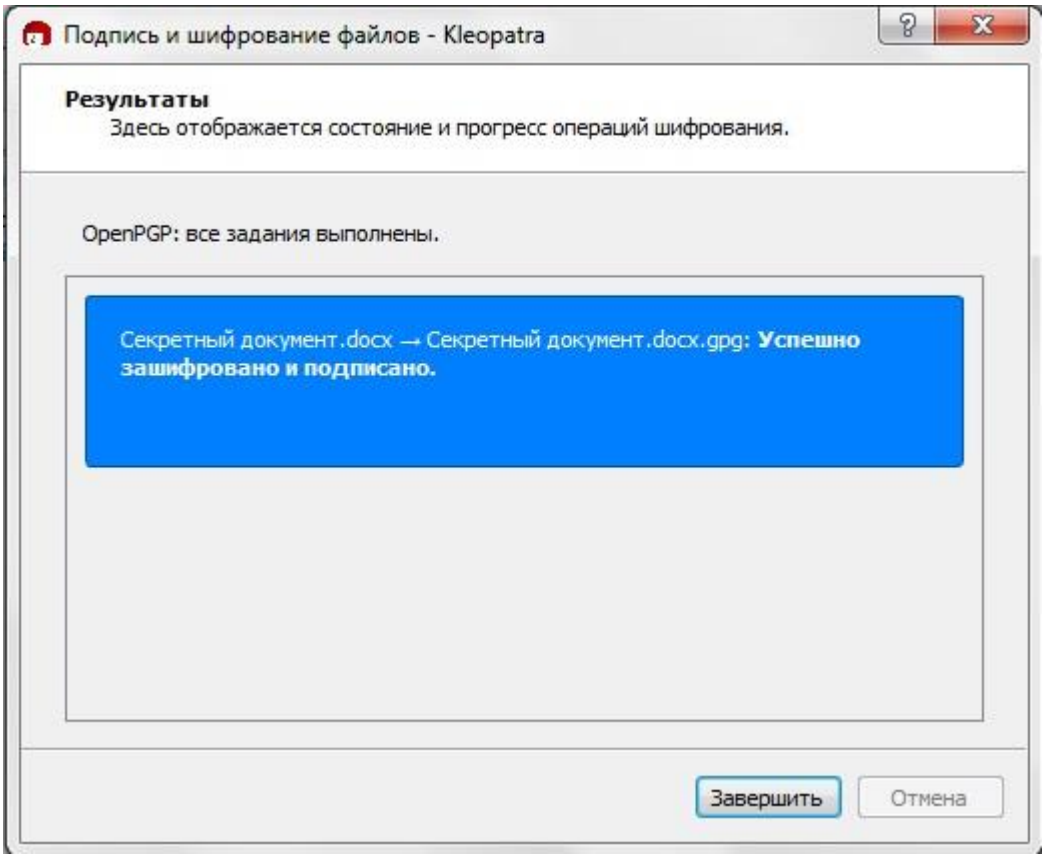


Рис. 24. Шифрование файла с подписью.

15. Тогда после расшифровки получатель увидит информацию о том, кем был подписан зашифрованный файл (рис. 25). Для закрытия окна и сохранения расшифрованного файла нажмите **«Сохранить все».**

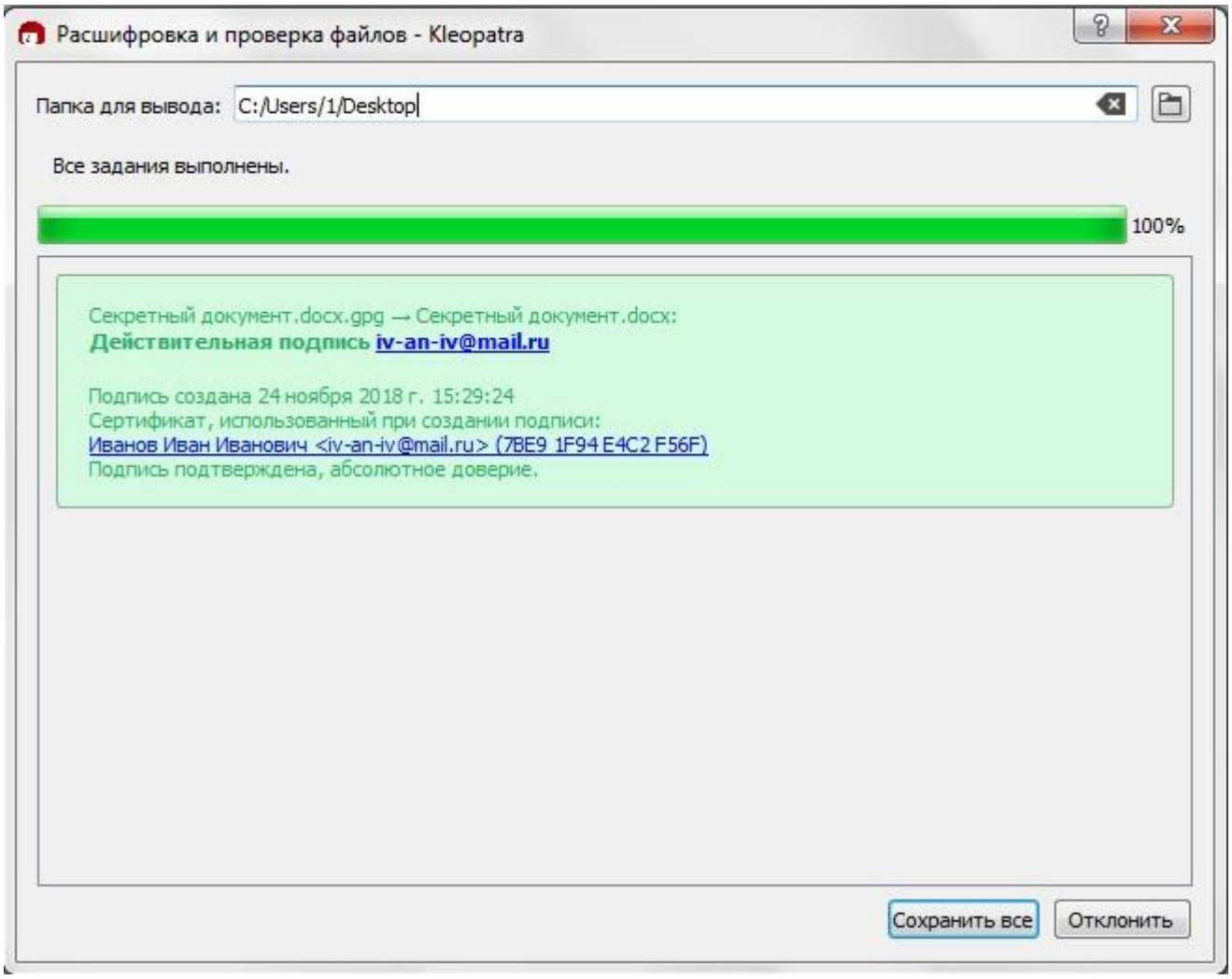


Рис. 25. Расшифровка файла и проверка подписи выполнены.

Лабораторная работа № 3. Применение электронной подписи в системах электронного документооборота

8. Электронная подпись для файлов и ее проверка

1. Приложение Kleopatra позволяет формировать электронную подпись для проверки целостности подписываемых электронных документов и установления их авторства на основе сертификатов подписывающих лиц.

2. Для подписывания будет использован подготовленный ранее файл **«Секретный документ.docx»** (п.2 предыдущего раздела).

3. В приложении Kleopatra нужно нажать кнопку **«Подписать/Зашифровать…»**

4. Далее необходимо выбрать подписываемый файл и нажать кнопку **«Открыть»**

5. В появившемся окне поставьте галочку рядом с пунктом **«Сертификат подписи»**. Выберите необходимый сертификат и нажмите кнопку **«Подписать»** (рис. 26).

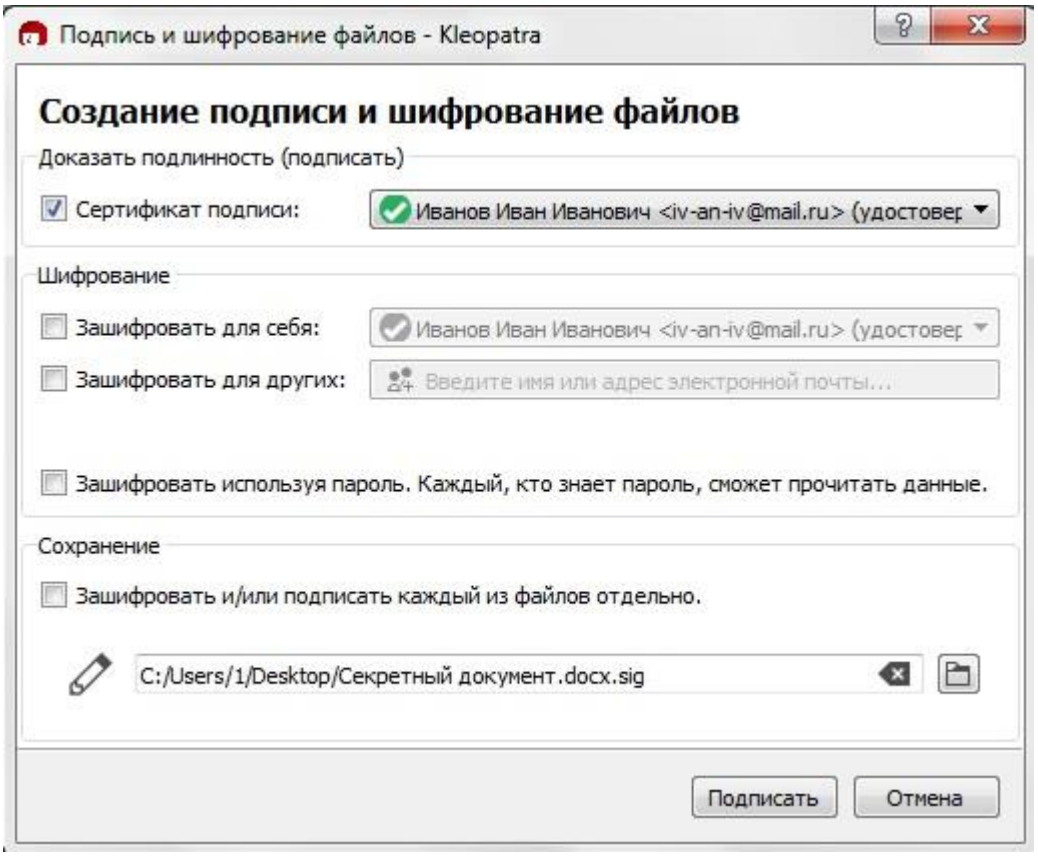


Рис. 26 Создание подписи

6. Введите фразу-пароль для разблокировки секретного ключа (рис. 27)

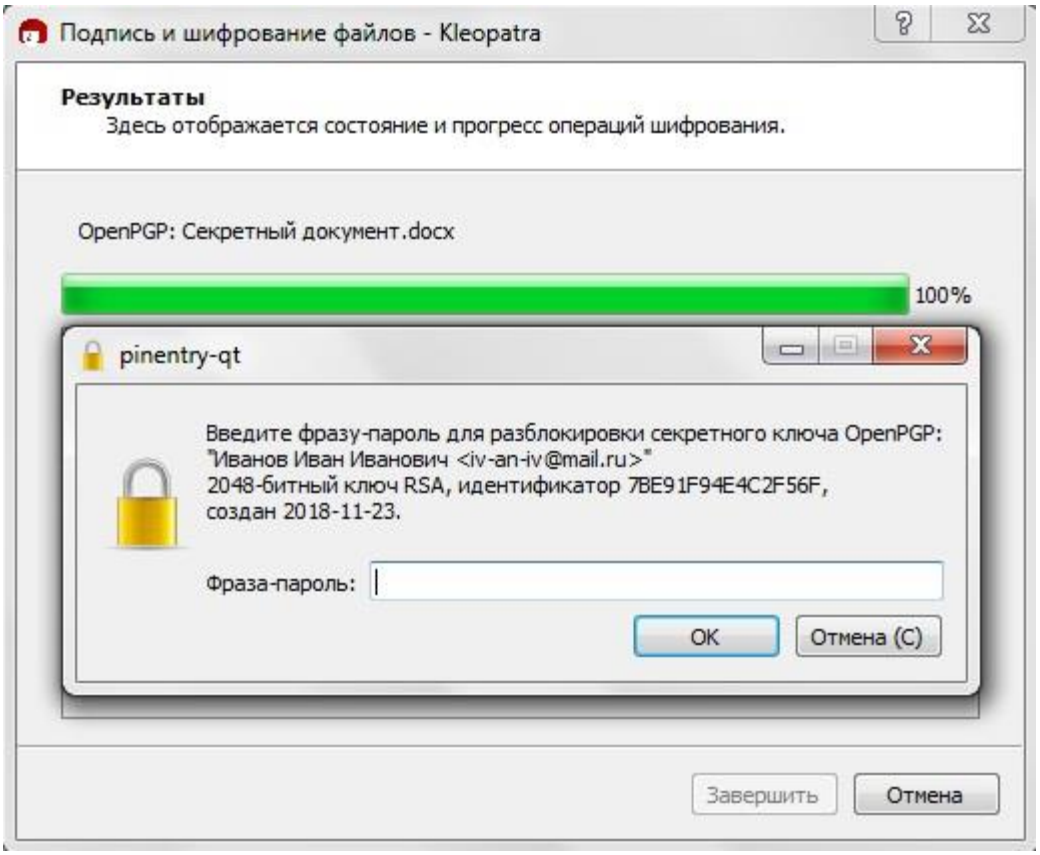


Рис. 27. Ввод фразы-пароля для подписи файла

7. Приложение оповестит пользователя о том, что файл успешно подписан (рис. 28). Необходимо нажать кнопку **«Завершить».**

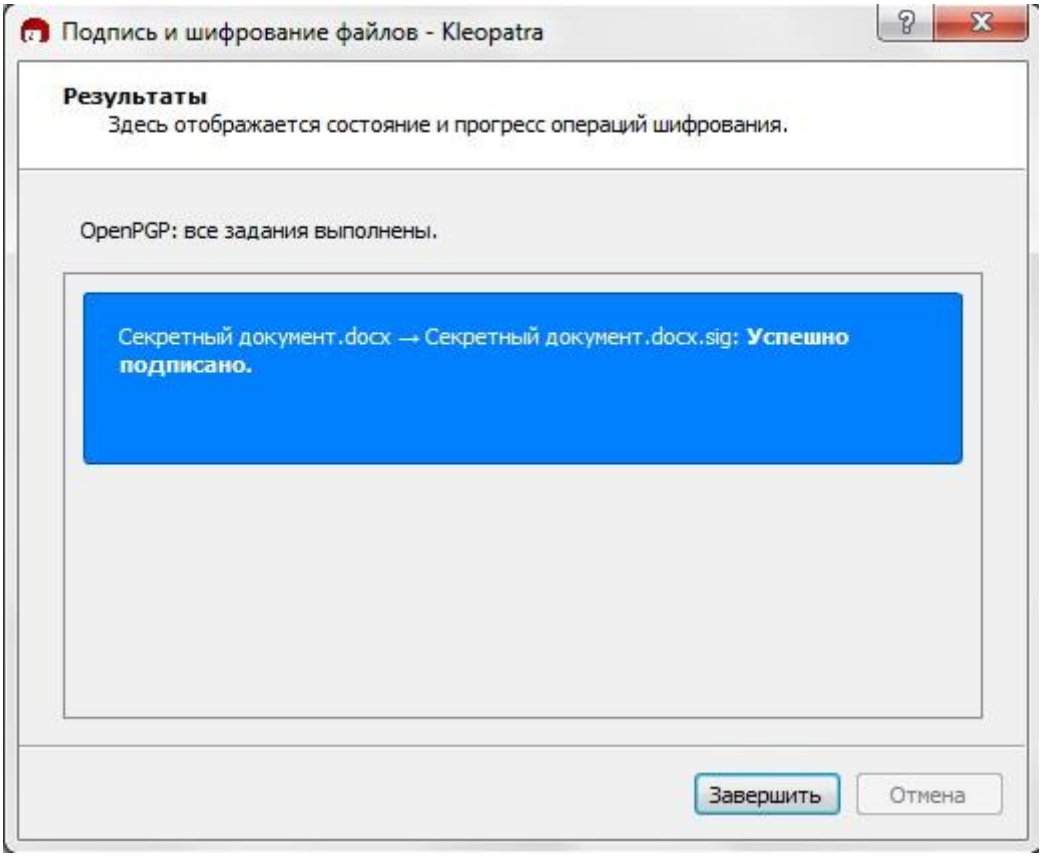
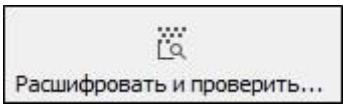


Рис. 28. Файл успешно подписан

8. В директории, где расположен подписываемый файл, появится отдельный файл подписи **«Секретный документ.docx.sig»**. Данный файл отправляется вместе с подписываемым файлом.

9. Для проверки подписи необходимо в приложении Kleopatra нажать на кнопку **«Расшифровать и проверить…»**



10. Далее выберите файл подписи, который должен заканчиваться на .sig и нажмите **«Открыть».**

Примечание. Файл подписанного документа и файл подписи должны находиться в одной папке, иначе проверка подписи пройдет некорректно.

11. Если проверка подписи прошла успешно, приложение оповестит пользователя, что подпись действительна и покажет информацию о том, кем она была произведена (рис. 29).

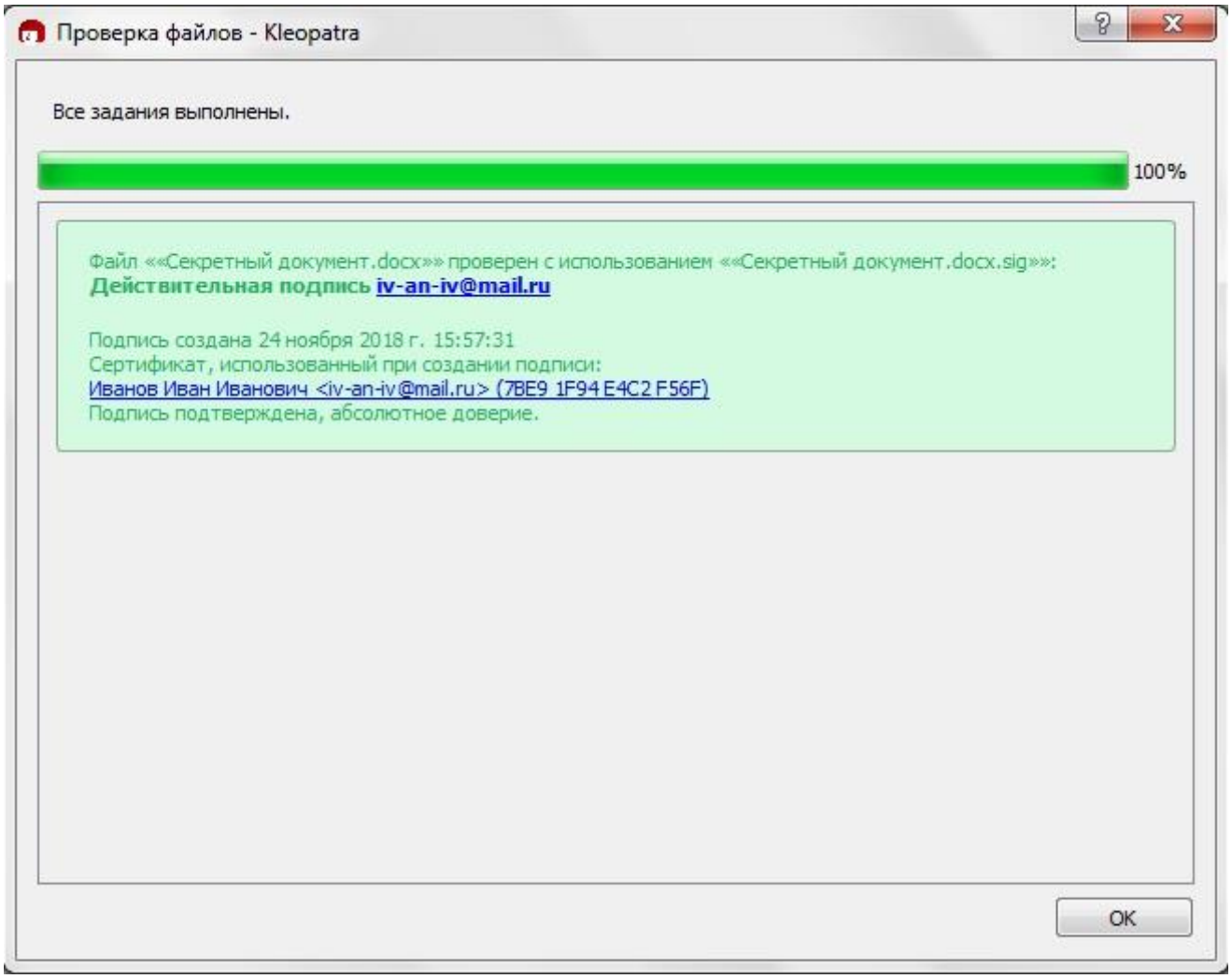


Рис. 29. Подтверждение подписи

12. Как известно, электронная подпись позволяет не только определить лицо, подписавшее электронный документ, но и обнаружить факт внесения изменений в электронный документ после момента его подписания. Для проверки данной полезной функции внесите изменения в уже подписанный документ **«Секретный документ.docx»** (например, поставьте в конце одну запятую) и сохраните его (рис. 30)

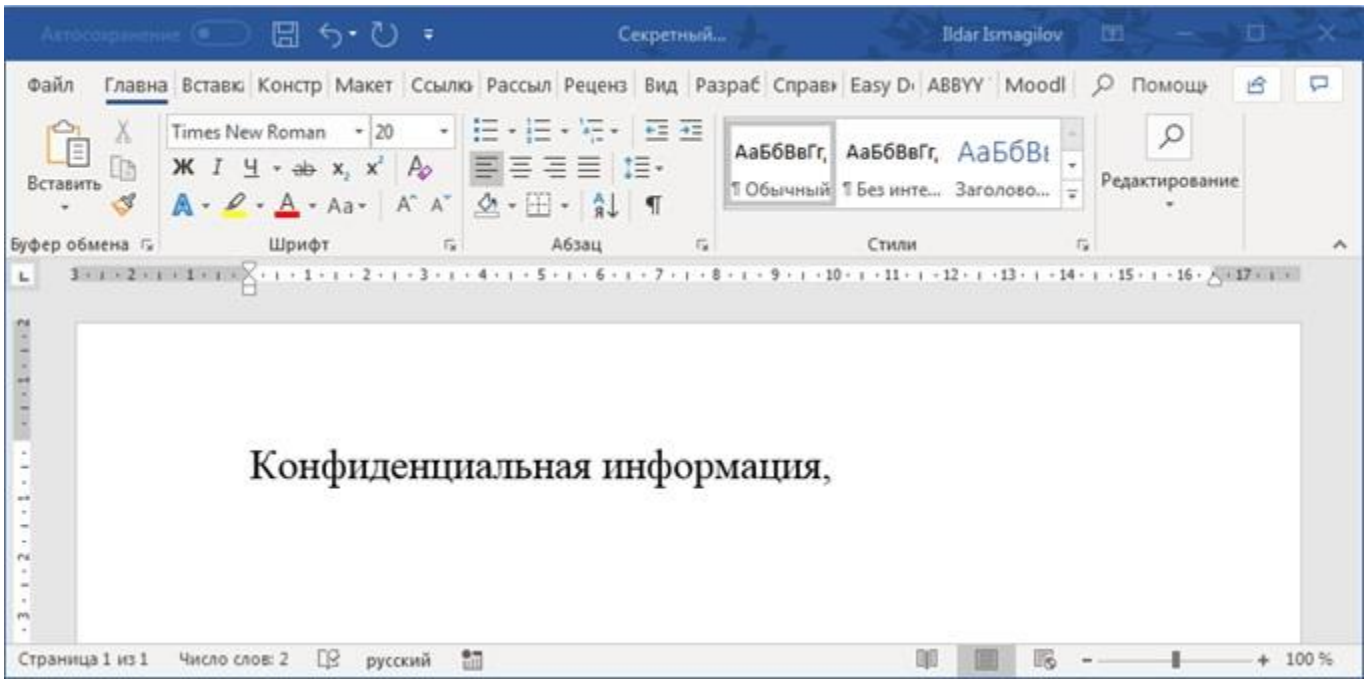


Рис. 30. Внесение изменений в подписанный документ.

13. Повторите действия, описанные в п.п. 9-11 данного раздела. Приложение оповестит пользователя о том, что подпись неверна (рис. 31).

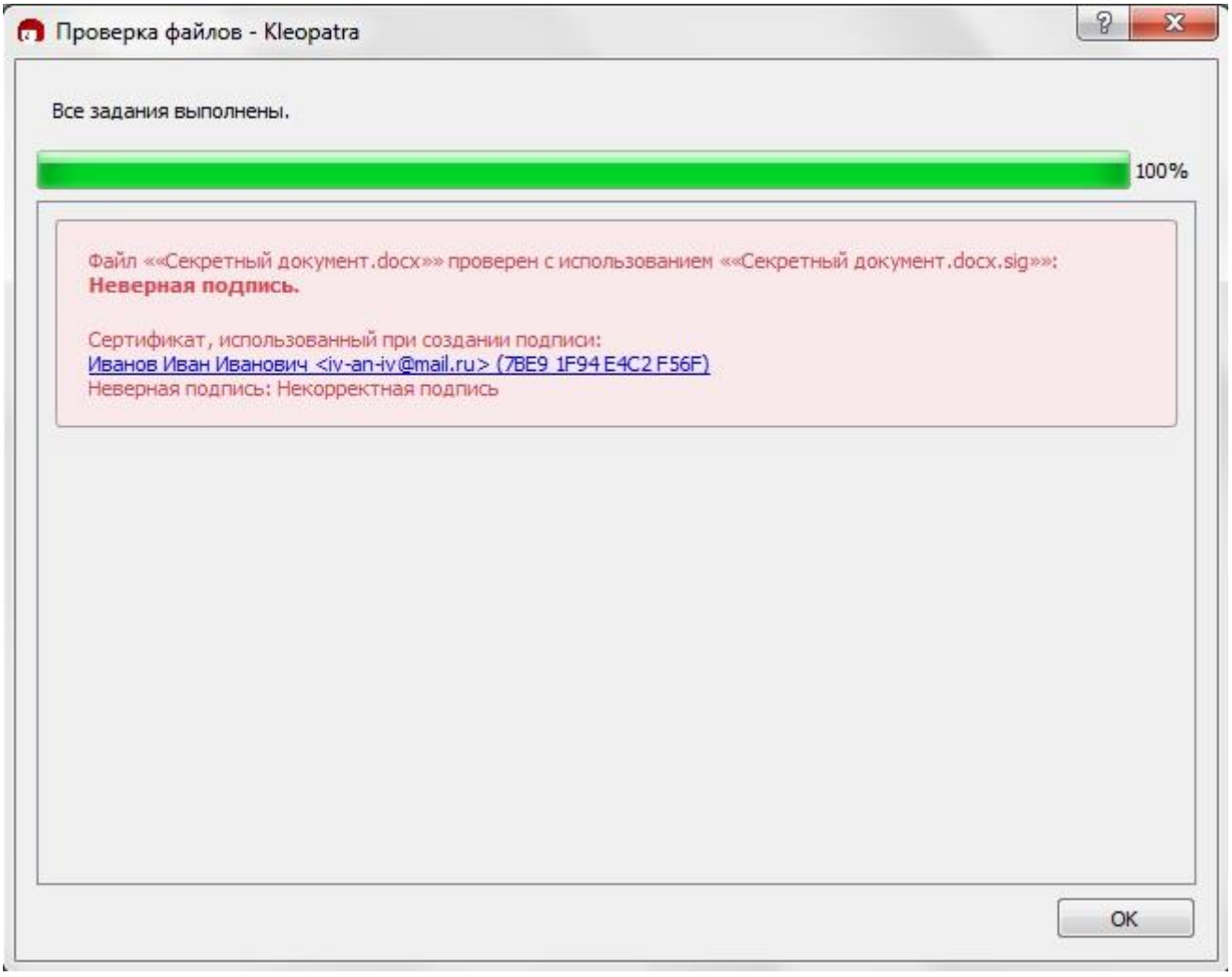


Рис. 31. Оповещение пользователя о неверной подписи.

Лабораторная работа № 4. Настройка межсетевого взаимодействия

ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – научиться налаживать сетевое взаимодействие между сетями.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание
2. Изучить теоретическую часть
3. Описать со скриншотами предметную область
4. Написать вывод

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист
2. Задание в соответствии с вариантом
3. Описание предметной области со скриншотами
4. Вывод

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Межсетевое взаимодействие позволяет устанавливать защищенное соединение между узлами разных сетей ViPNet. Организация межсетевого взаимодействия между двумя сетями состоит из следующих этапов:

1. Администратор первой сети ViPNet, инициирующий межсетевое взаимодействие, создает файл с межсетевой информацией и межсетевой мастер-ключ.
2. Администратор второй сети ViPNet принимает межсетевую информацию, импортирует межсетевой мастер-ключ, затем создает файл с ответной межсетевой информацией и передает его администратору первой сети.
3. Администратор первой сети завершает организацию взаимодействия приемом ответной межсетевой информации.
4. Администраторы отправляют на узлы своих сетей обновления справочников и новые ключи узлов.

После этого узлы доверенных сетей, участвующие во взаимодействии, могут устанавливать защищенные соединения друг с другом.

Рис. 1 – Схема настройки межсетевого взаимодействия

При организации межсетевого взаимодействия, как и при любой модификации сети, тем более, реальной, стоит полностью продумывать все этапы запланированного мероприятия от начала до конца. Поэтому из уже имеющейся сети и сети Федеральной службы выделим тольео те сетевые узлы, которые нам понадобится связать и представим их в виде схемы (рис. 2).

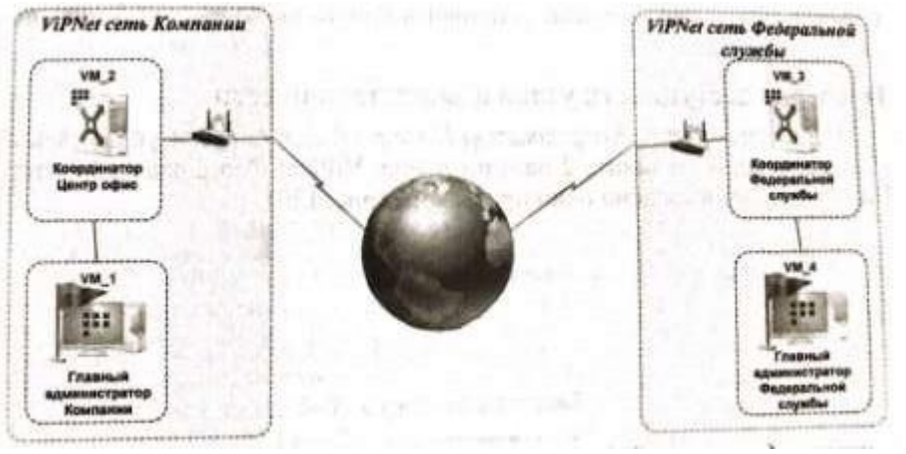


Рис. 2 – Схема установления межсетевого взаимодействия между сетями

В реальной ситуации количество узлов, которые потребуется связать может оказаться гораздо больше и все их необязательно отражать на схеме, но общую модель и план действия лучше составить, а остальные связи узлов проработать в виде таблицы.

На VM1 должен быть развернут узел Главного администратора (ViPNet Administrator и ViPNet Client), на VM2 – Координатор Центр офис (ViPNet Coordinator), на VM3 – Координатор Федеральной службы (ViPNet Coordinator), на VM4 – узел Главного администратора Федеральной службы (ViPNet Administrator и ViPNet Client).

Защищенная сеть Федеральной службы представлена на таблице 1.

Таблица 1 – Состав защищенной сети Федеральной службы

№	Тип СУ	Название СУ	Расположение СУ	Комментарии
1	Координатор	Координатор Федеральной службы	Федеральная служба	Для развертывания ViPNet

№	Тип СУ	Название СУ	Расположение СУ	Комментарии
				Coordinator
2	Клиент	Администратор Федеральной службы		Для развертывания ViPNet Administrator

Матрица связей узлов защищенной сети Федеральной службы представляет собой два узла – Координатор Федеральной службы и Администратор Федеральной службы, между которыми установлена связь. На каждом узле присутствует по одному пользователю – Координатор Федеральной службы и Админ ФедСлужбы Новиков.

Не забудьте отключить у пользователей создание электронной подписи.

ВЫПОЛНЕНИЕ РАБОТЫ

1. Инициация межсетевого взаимодействия

Вначале необходимо задать IP-адреса сетевым узлам *(Глав admин, Координатор Центр офис, Координатор Федеральной службы* и *Глав admин Федеральной службы*), чтобы они находились в одной подсети.

Чтобы инициировать межсетевое взаимодействие с сетью ViPNet *Федеральной службы*, выполните следующие действия на рабочем месте *Главный администратор* сети *Компании*:

1. В окне программы ViPNet Центр управления сетью в меню *Доверенные сети* выберите пункт *Установить взаимодействие*. Будет запущен мастер *Установка межсетевого взаимодействия*.

2. На первой странице мастера выберите вариант *Я инициатор межсетевого взаимодействия* и нажмите кнопку *Далее.*

3. На странице *Задайте информацию о другой сети ViPNet и координатор для связи с ней* (необходимо правильно указать номер доверенной сети, с которой вы устанавливаете межсетевое взаимодействие, в противном случае могут возникнуть проблемы), имя сети - *Федеральная служба*, которое будет отображаться в программе ViPNet Центр управления сетью, и выберите шлюзовой координатор своей сети – *Координатор Центр офис*. Затем нажмите кнопку *Далее* (рис. 3).

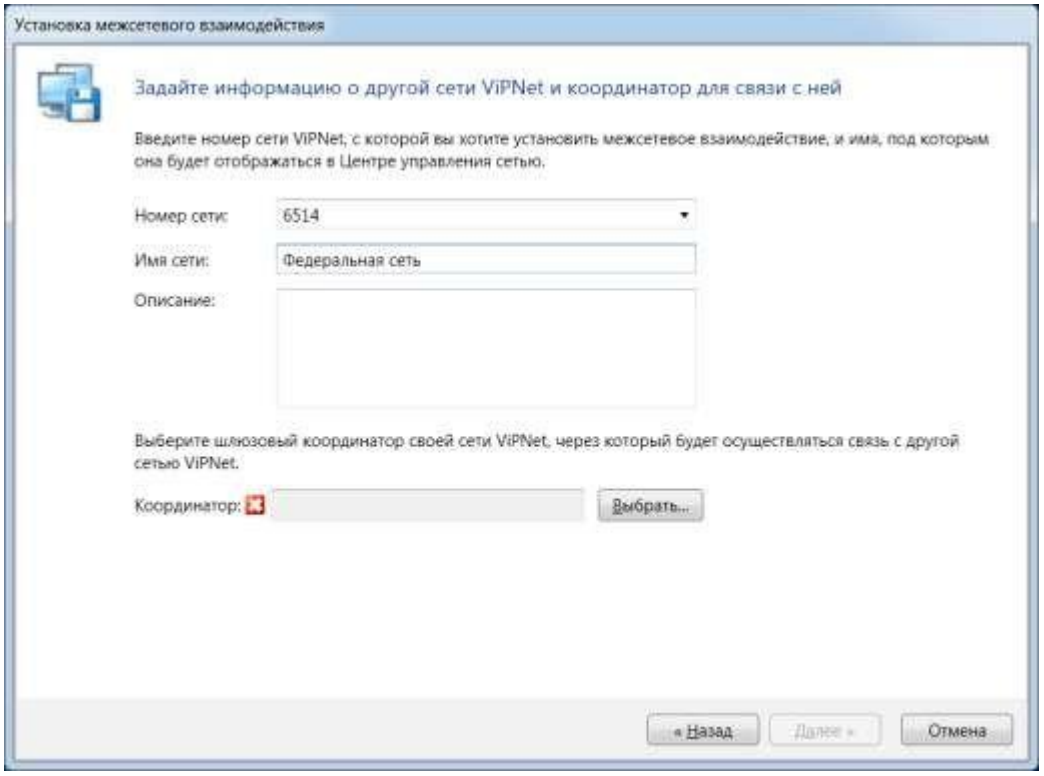


Рис. 3 – Фрагмент окна Установка межсетевого взаимодействия

4. На странице *Укажите сетевые узлы своей сети ViPNet для связывания* выберите узлы сети, которые будут участвовать во взаимодействии с узлами сети *Федеральной службы - Главный администратор* и *Координатор Центр офис*.

5. Центр управления сетью и шлюзовой координатор своей сети должны обязательно присутствовать в списке узлов для взаимодействия, их невозможно удалить. Выбрав узлы, нажмите кнопку *Далее*.

6. На странице *Укажите пользователей своей сети ViPNet для связывания* выберите пользователя *Координатор Центр офис*.

7. Если для межсетевого взаимодействия выбран сетевой узел, но не выбран ни один пользователь этого узла, сведения об этом узле не будут включены в межсетевую информацию. Исключениями являются *Центр управления сетью и шлюзовой координатор*. Выбрав пользователей, нажмите кнопку *Далее*.

8. На открывшейся странице *Подготовка к сохранению межсетевой информации завершена* при необходимости укажите комментарий для администратора сети *Федеральной службы* и нажмите кнопку *Далее*.

9. На странице *Укажите файл для сохранения межсетевой информации* нажмите кнопку *Обзор* и укажите каталог для сохранения файла межсетевой информации - *Рабочий стол*. Затем нажмите кнопку *Далее*.

10. На странице *Сохранение межсетевой информации* после завершения записи файла нажмите кнопку *Далее*, на следующей странице нажмите кнопку *Готово*.

Чтобы создать индивидуальный симметричный межсетевой мастер-ключ, выполните следующие действия:

1. В окне программы ViPNet Удостоверяющий ключевой центр на панели навигации выберите представления *Ключевой центр*.

2. Перейдите и раздел с номером доверенной сети, для связи с которой будет использоваться межсетевой мастер-ключ, и на панели инструментов нажмите кнопку *Создать*.

3. Появится окно с сообщением о необходимости согласования мастер-ключа с администратором доверенной сети. Нажмите в данном окне кнопку *Да*. В результате межсетевой мастер-ключ будет создан и отобразится в соответствующем разделе (рис. 4).

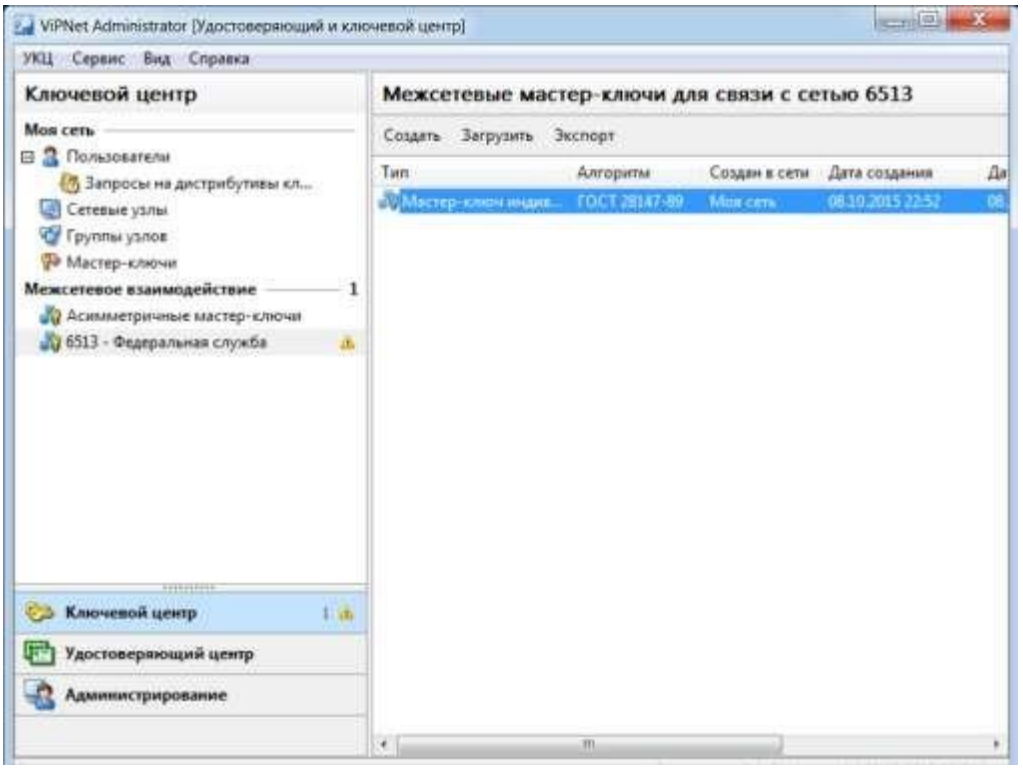


Рис. 4 – Создание ИСММК

4. Щелкните по созданному межсетевому мастер-ключу правой кнопкой мыши и в контекстном меню выберите пункт *Экспорт.*

5. Появится окно ввода пароля. Укажите в нем пароль - 11111111 и нажмите кнопку *ОК*. На указанном пароле будет зашифрован экспортируемый ключ.

6. В появившемся окне укажите каталог, в который будет сохранен межсетевой мастер-ключ, - *Рабочий стол*, затем нажмите кнопку *ОК*.

7. Передайте доверенным способом файл межсетевой информации с расширением **.lzh*, межсетевой мастер-ключ *«net ****.key»* и пароль, на котором зашифрован межсетевой мастер-ключ - 11111111, администратору сети *Федеральной службы*.

2. Прием первичной межсетевой информации

Чтобы принять межсетевую информацию перейдите на рабочее место администратора сети *Федеральной службы* и выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню *Доверенные сети* выберите пункт *Установить взаимодействие*. Будет запущен мастер *Установка межсетевого взаимодействия*.

2. На первой странице мастера выберите вариант *Я принимаю файл с межсетевой информацией* и нажмите кнопку *Далее*.

3. На странице *Загрузка межсетевой информации* из файла укажите

файл с межсетевой информацией, полученный от *Главного администратора* сети ViPNet *Компании*, который инициировал межсетевое взаимодействие. После указания файла в окне мастера появится предупреждение, что взаимодействие с сетью не установлено (рис. 5).

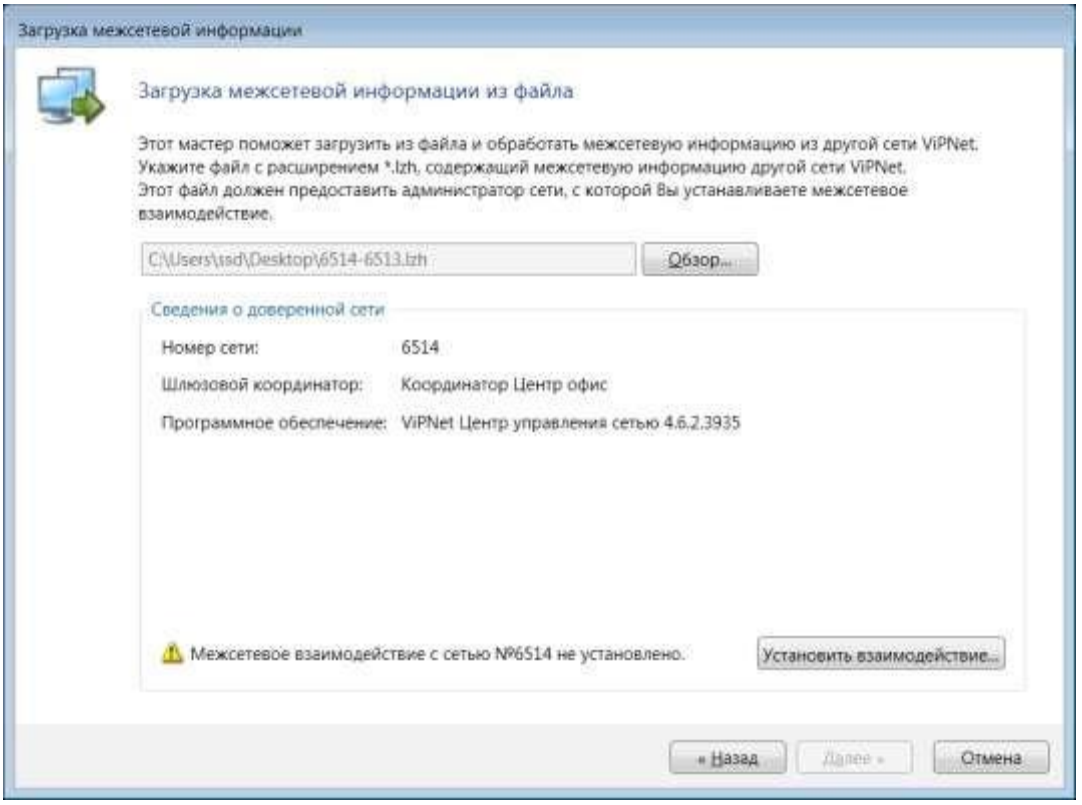


Рис. 5 – Прием первичной межсетевой информации

3. Чтобы продолжить загрузку межсетевой информации, нажмите кнопку *Установить взаимодействие*.

4. На странице *Задайте информацию о другой сети ViPNet* и *координатор для связи с ней* выберите шлюзовой координатор – *Координатор Федеральной службы*, затем нажмите кнопку *Далее*.

5. На странице *Изменения в межсетевой информации* ознакомьтесь со списком узлов и пользователей, которые были выбраны для межсетевого взаимодействия *Главным администратором сети ViPNet Компании*, который инициировал межсетевое взаимодействие. Затем нажмите кнопку *Далее*.

6. Если файл межсетевой информации содержит ошибки, откроется страница *Проверка межсетевой информации* со списком обнаруженных конфликтных или неполных данных. При обнаружении конфликтных данных загрузка межсетевой информации будет невозможна. В этом случае обратитесь к администратору доверенной сети для устранения конфликтов.

7. Чтобы продолжить обработку межсетевой информации, нажмите кнопку *Далее*.

8. На странице *Загрузка межсетевой информации* после завершения обработки информации нажмите кнопку *Готово*.

9. В представлении *Доверенные сети* выберите *Сеть №***** (вместо звездочек будет номер сети, инициировавшей межсетевое взаимодействие) перейдите на вкладку *Пользователи*. В свойствах пользователя *Координатор Центр офис* на вкладке *Связи с пользователями* установите связь с *Координатор Федеральной службы* (рис. 6).

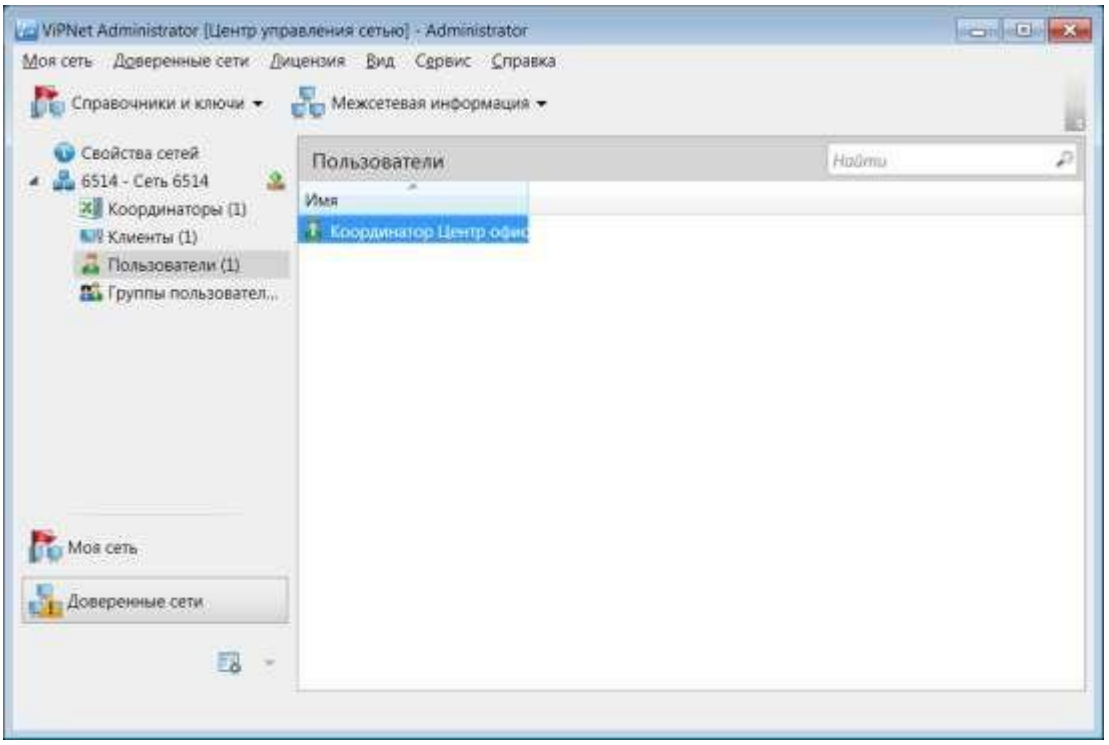


Рис. 6 – Вкладка Пользователи доверенной сети

После приема первичной межсетевой информации в программе ViPNet Удостоверяющий и ключевой центр импортируйте переданный *Главным администратором Компании* межсетевой мастер-ключ. Для этого:

1. В окне программы на панели навигации выберите представление *Ключевой центр* и перейдите в раздел с номером доверенной сети, из которой поступил данный мастер-ключ.

2. На панели инструментов нажмите кнопку *Загрузить*.

3. При импорте индивидуального симметричного межсетевого мастер-ключа *«net ****.key»* появится окно ввода пароля. Введите пароль, на котором был зашифрован данный ключ - 111111111. При правильном вводе пароля мастер-ключ будет импортирован. Импортированный мастер-ключ будет сразу добавлен в список межсетевых мастер-ключей выбранного раздела. После того, как ключ будет импортирован, в УКЦ необходимо зайти в раздел

Межсетевое взаимодействие, выбрать строку с ИСММК, щелкнуть по строке правой кнопкой мыши и выбрать пункт *Использовать*.

4. Подготовьте сертификаты администраторов и списки аннулированных сертификатов вашей сети для передачи в доверенную сеть (сеть *Компании*) в составе ответной межсетевой информации. Для этого в программе ViPNet Удостоверяющий и ключевой центр в меню *Сервис* выберите пункт *Экспорт межсетевой информации*.

5. В программе ViPNet Центр управления сетью в представлении *Доверенные сети* выберите раздел *Свойства сетей*.

6. На панели просмотра щелкните правой кнопкой мыши добавленную доверенную сеть и в контекстном меню выберите пункт *Создать межсетевую информацию* (рис. 7).

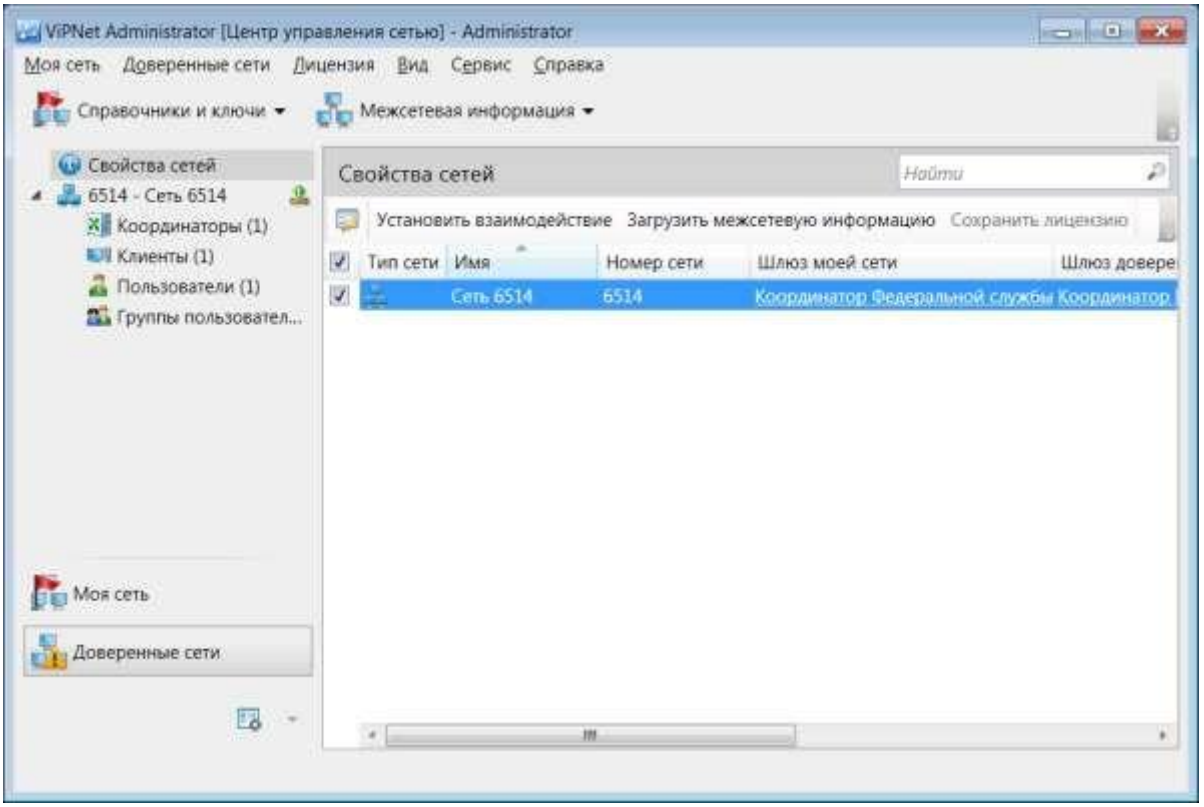


Рис. 7 – Создание ответной межсетевой информации для доверенной сети

7. В появившемся окне нажмите кнопку *Создать*.

8. После создания ответной межсетевой информации сохраните ее на жесткий диск. Для этого снова щелкните доверенную сеть правой кнопкой мыши и в контекстном меню выберите пункт *Сохранить межсетевую информацию в файл*,

затем в окне *Сохранить как* укажите папку для сохранения файла межсетевой информации ****-****.*lzh* – *Рабочий стол*.

9. Создайте новые справочники и ключи для узлов сети *Федеральной службы*, участвующих в межсетевом взаимодействии – *Администратор ViPNet Федеральной службы* и *Координатор Федеральной службы*, и отправьте их на узлы.

10. Передайте созданный файл межсетевой информации ****-****.*lzh* администратору сети *Компании*.

3. Завершение организации межсетевого взаимодействия

Чтобы принять ответную межсетевую информацию и завершить организацию взаимодействия, выполните следующие действия на рабочем месте *Главный администратор* (сеть Компании):

1. Получите у администратора доверенной сети ViPNet *Федеральной службы* файл, содержащий ответную межсетевую информацию ****-****.*lzh*

2. В окне программы ViPNet Центр управления сетью в меню *Доверенные сети* выберите пункт *Загрузить межсетевую информацию из файла.*

3. В окне *Загрузка межсетевой информации* укажите файл межсетевой информации, полученной от администратора другой сети ViPNet, и следуйте мастеру, нажимая кнопку *Далее*, на заключительном шаге *Готово*.

4. Примите ответную межсетевую информацию с помощью мастера *Обработка межсетевой информации* (рис. 8).

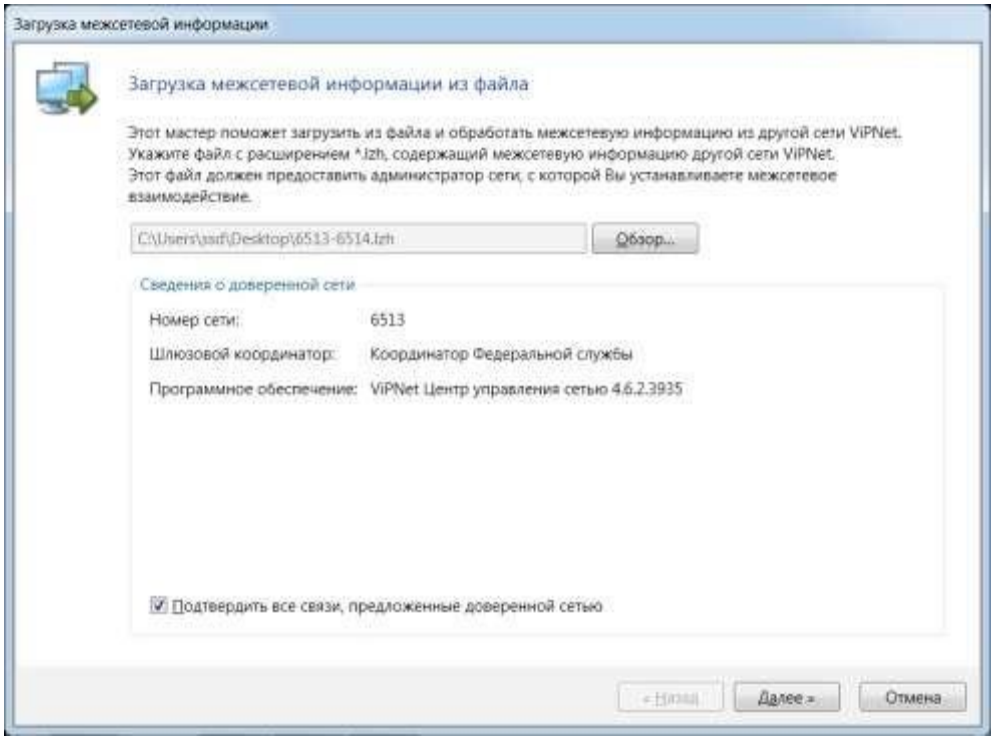


Рис. 8 – Прием ответной межсетевой информации из сети Федеральной службы

5. В окне программы ViPNet Удостоверяющий и ключевой центр перейдите в представление *Администрирование* и на панели навигации выберите раздел *Необработанные данные> Контейнеры сертификатов администратора сетей ViPNet*.

6. На панели просмотра выберите контейнер *Федеральная служба* и на панели инструментов нажмите кнопку *Обработать* (рис. 9).

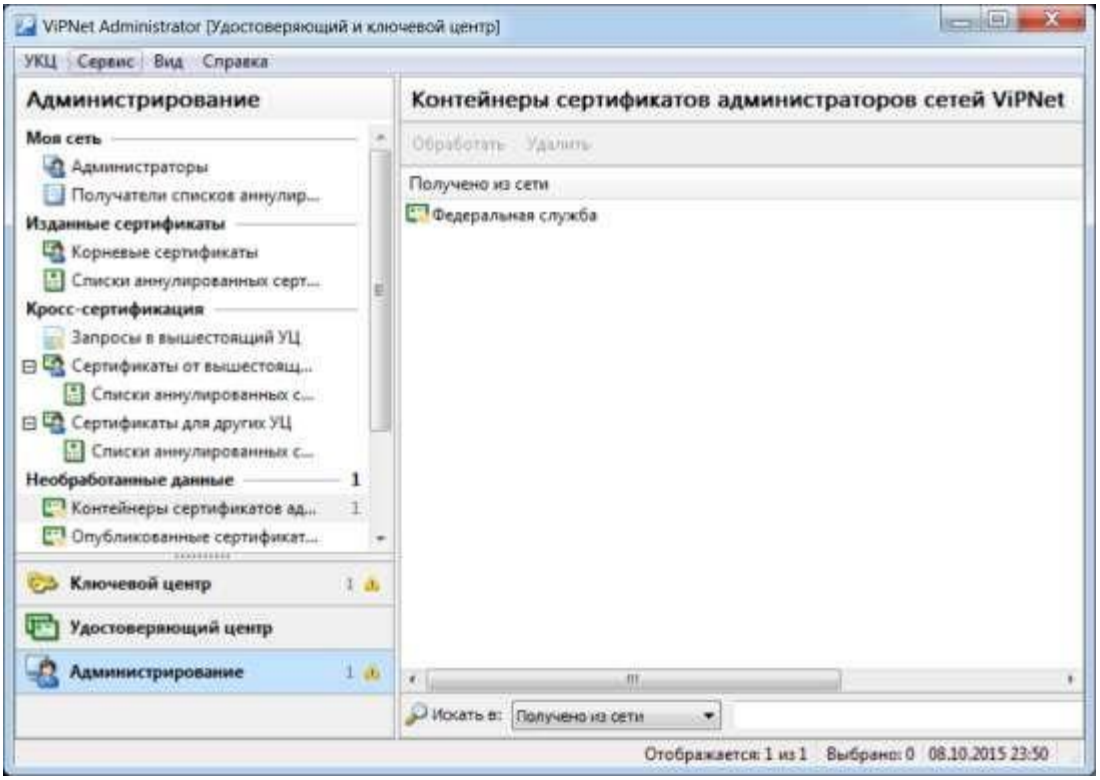


Рис. 9 – Обработка контейнеров сертификатов и CRL Федеральной службы

7. В появившемся окне будет представлен список администраторов, сертификаты и CRL которых содержатся в выбранных контейнерах. Выберите администратора сети и нажмите кнопку *Импортировать* (рис. 10).

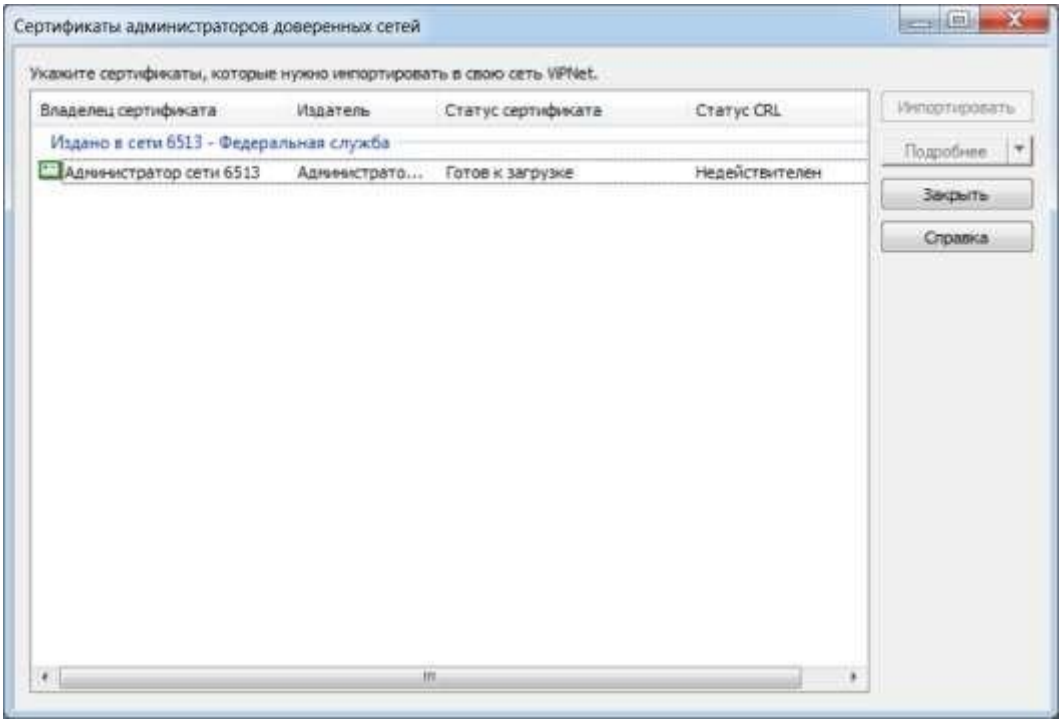


Рис. 10 – Сертификаты администраторов доверенных сетей

8. В окне программы ViPNet Удостоверяющий и ключевой центр в представлении *Ключевой центр* выберите раздел *Межсетевое взаимодействие> Федеральная служба*.

9. Выберите межсетевой мастер-ключ и щелкните по нему правой кнопкой мыши. В контекстном меню выберите команду *Текущий* для ввода межсетевого мастер-ключа в действие.

10. Для узлов сети *Компании*, участвующих в межсетевом взаимодействии, *Главный администратор* и *Координатор Центр офис*. создайте и отправьте новые справочники и ключи.

11. Проверьте взаимодействие узлов *Координатор Федеральной службы* (сеть Федеральной службы) и *Координатор Центр офис* (сеть Компании).

12. На рабочем месте *Главного администратора* (сеть Компании), отправьте межсетевую информацию по защищенному каналу.

13. Убедитесь, что межсетевая информация поступила в ЦУС *Федеральной службы* и обработайте ее.

Проверка взаимодействия осуществляется в окне программы ViPNet

Coordinator *Монитор> Защищенная сеть* в контекстном меню узла выбрать *Проверить соединение*.

4. Модификация межсетевого взаимодействия

4.1 Установление связей между пользователями доверенных сетей

Чтобы добавить связи пользователей сети ViPNet *Компании* и *Федеральной службы*, выполните следующие действия на рабочем месте *Главный администратор* (сеть Компании):

1. В окне программы ViPNet Центр управления сетью в представлении *Доверенные сети* выберите сеть Федеральная служба и перейдите на вкладку *Пользователи*.

2. Зайдите в свойства пользователя *Координатор Федеральной службы*.

3. В открывшемся окне перейдите на вкладку *Связи с пользователями* и добавьте в список пользователей *Сотрудник_1 Центр Кузнецов, Зам бухгалтера Захарова, Директор Абросимов*.

4. В представлении *Доверенные сети* выберите раздел *Свойства сетей*.

5. На панели просмотра щелкните правой кнопкой мыши на доверенную сеть *Федеральная служба* и в контекстном меню выберите пункт *Создать межсетевую информацию*. В открывшемся окне установите флажок *Отправить межсетевую информацию* после создания и нажмите кнопку *Создать*.

Чтобы принять межсетевую информацию из сети *Компании*, перейдите на рабочее место администратора сети *Федеральной службы* и выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню *Доверенные сети* выберите пункт *Обработать межсетевую информацию*.

2. В открывшемся окне выберите сеть *Компании* и нажмите кнопку *Обработать выбранные*.

3. В представлении *Доверенные сети* выберите раздел *Свойства сетей*.

4. На панели просмотра щелкните правой кнопкой мыши доверенную сеть *Компании* и в контекстном меню выберите пункт *Создать межсетевую информацию*.

5. В открывшемся окне установите флажок *Отправить межсетевую информацию* после создания и нажмите кнопку *Создать*.

6. Создайте и отправьте новые справочники и ключи для узла *Координатор Федеральной службы*.

Чтобы принять ответную межсетевую информацию от сети *Федеральной службы*, перейдите на рабочее место *Главный администратор* сети *Компании* и выполните следующие действия:

l. В окне программы ViPNet Центр управления сетью в меню *Доверенные сети* выберите пункт *Обработать межсетевую информацию*.

2. В открывшемся окне выберите сеть *Федеральная служба* и нажмите кнопку *Обработать выбранные*.

3. Создайте и отправьте новые справочники и ключи для узлов *Сотрудник_1 Центр офис, Зам бухгалтера, Директор*.

Для проверки правильности выполнения задания перейдите на узел *Координатор Федеральной службы* и убедитесь, что в списке узлов защищенной сети в программе ViPNet Coordinator Монитор

появились клиенты *Сотрудник Центр офис, Зам бухгалтер, Директор*.

4.2. Удаление связей между пользователями доверенных сетей

Чтобы удалить связи пользователей сети ViPNet Компании и Федеральной службы, выполните следующие действия на рабочем месте *Главный администратор* (сеть Компании):

1. В окне программы ViPNet Центр управления сетью в представлении *Доверенные сети* выберите сеть *Федеральная служба* и перейдите на вкладку *Пользователи*.
2. Зайдите в свойства пользователя *Координатор Федеральной службы*.
3. В открывшемся окне перейдите на вкладку *Связи с пользователями* и удалите из списка пользователей *Директор Абросимов*.
4. В представлении *Доверенные сети* выберите раздел *Свойства сетей*.
5. На панели просмотра щелкните правой кнопкой мыши доверенную сеть *Федеральная служба* и в контекстном меню выберите пункт *Создать межсетевую информацию*.
6. В открывшемся окне установите флажок *Отправить межсетевую информацию* после создания и нажмите кнопку *Создать*.

Чтобы принять межсетевую информацию от сети *Компании*, перейдите на рабочее место администратора сети *Федеральной службы* и выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню *Доверенные сети* выберите пункт *Обработать межсетевую информацию*.
2. В открывшемся окне выберите сеть и нажмите кнопку *Обработать выбранные*.
3. В представлении *Доверенные сети* выберите раздел *Свойства сетей*.
4. На панели просмотра щелкните правой кнопкой мыши доверенную сеть *Компании* и в контекстном меню выберите пункт *Создать межсетевую информацию*.

5. В открывшемся окне установите флажок *Отправить межсетинформацию после создания* и нажмите кнопку *Создать*.

6. Создайте и отправьте новые справочники и ключи для узла *Координатор Федеральной службы.*

Чтобы принять ответную межсетевую информацию от сети *Федеральной службы*, перейдите на рабочее место *Главный администратор* (сеть Компании) и выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню *Доверенные сети* выберите пункт *Обработать межсетевую информацию*.

2. В открывшемся окне выберите сеть *Федеральной службы* и нажмите кнопку *Обработать выбранные*.

3. Создайте н отправьте новые справочники и ключи для узла *Директор*.

Для проверки правильности выполнения задания перейдите узел *Координатор Федеральной службы* и убедитесь, что в списке узлов защищенной сети в программе ViPNet Coordinator Монитор отсутствует клиент *Директор*.

4.3 Прекращение межсетевого взаимодействия

Чтобы прекратить межсетевое взаимодействие *Компании* и *Федеральной службы*, выполните следующие действия на рабочем месте *Главный администратор* (сеть Компании):

1. В окне программы ViPNet Центр управления сетью выберите представление *Доверенные сети*.

2. На панели навигации выберите раздел *Свойства сетей*.

3. На панели просмотра щелкните правой кнопкой мыши доверенную сеть *Федеральная служба,* межсетевое взаимодействие с которой требуется прекратить, и в контекстном меню выберите пункт *Прекратить взаимодействие*.

4. В окне подтверждения установите флажок *Прекратить взаимодействие*, затем нажмите кнопку *Прекратить взаимодействие*. В открывшемся окне *Прекращение взаимодействия* с выбранными сетям будет отображен процесс удаления данных об объектах доверенной сет и их связях с объектами вашей сети. Также информация о доверенной сети будет удалена в программе ViPNet Удостоверяющий и ключевой центр.

5. Создайте и отправьте новые справочники и ключи для узлов, которые были задействованы в межсетевом взаимодействии.

Аналогичные действия проделайте на рабочем месте *Администратор сети ViPNet Федеральной службы*. Убедитесь, что связи между узлами *Координатор Центр офис* и *Координатор Федеральной службы* больше нет.

ВАРИАНТЫ ЗАДАНИЙ

Создать новый сетевой узел в сети Федеральной службы в соответствии с вариантом задания, на этом узле создать пользователя со своим ФИО (в виде: *ФамилияИмяОтчество*). Установить связь между созданным пользователем и Координатором Центрального офиса. Проделать необходимые действия при изменении структуры сети, принимая во внимание межсетевое взаимодействие. Проверить правильность выполнения задания.

Таблица 2 – Варианты заданий

№	Название СУ
1	Специалист по продажам
2	Начальник отдела кадров
3	Менеджер по управлению персоналом
4	Ведущий юрист-консультант
5	Менеджер по финансовому планированию
6	Инженер по безопасности
7	Системный администратор
8	Специалист по связам с общественностью
9	Специалист по внедрению ПО
10	Программист-разработчик

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Для чего предназначено межсетевое взаимодействие?

2. Межсетевые мастер ключи. Дать определения межсетевым мастер ключам.

3. Виды межсетевых мастер ключей.

4. Какими принципами следует руководствоваться при выборе межсетевого мастер ключа?

5. Для чего необходимо прекращение взаимодействия между сетями?

6. Для чего при организации межсетевого взаимодействия назначается шлюзовой координатор?

7. Возможно ли экспортировать межсетевой мастер ключ без пароля?

Лабораторная работа № 5. ViPNet Деловая почта

ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – освоить на наглядном примере методы и способы по работе с ПО ViPNet Деловая почта. Так же изучить возможности настройки данного ПО для своих нужд.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание
2. Изучить теоретическую часть
3. Описать со скриншотами предметную область
4. Написать вывод

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист
2. Задание в соответствии с вариантом
3. Описание предметной области со скриншотами
4. Вывод

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Назначение и функциональные возможности программы Деловая почта

Программа **Деловая почта** (или просто **Деловая Почта**) предназначена для организации **защищенной передачи** электронных документов по открытым каналам связи по всему маршруту следования документа от отправителя к получателю в сети ViPNet. В почтовый защищенный сервис входят следующие услуги, предоставляемые программой:

• отправка и получение писем с прикрепленными к ним вложениями;

• отправка файлов (в виде вложений) из Windows Explorer адресатам ViPNet;

• получение подтверждений (квитанций) о доставке и использовании документов;

• шифрование писем и вложений к ним;

• электронная подпись (внутренними и внешними сертификатами) писем и вложений к ним;

• электронная подпись (и проверка подписи) отдельных файлов (не вложений);

• предоставление информации о документе: дате и времени создания и получения документа, размере документа (в килобайтах), информации о получателях и отправителях;

• ведение регистрационной нумерации документов;

• экспорт и импорт писем.

Кроме того, программа предоставляет гибкие возможности по работе с документами: сортировка документов, архивация документов, поиск нужного документа, автоматическая обработка файлов и входящих писем в соответствии с различными правилами, задаваемыми пользователем (автопроцессинг) и др.

Внимание! В версии программы (3.1.x) вводится отмена обработки квитанций для писем, отсутствующих в рабочем хранилище. Это приведет к утрате интерактивности статуса для отправленных писем в архивах. Квитанции о доставке, прочтении писем, помещенных в архив, не будут обработаны при открытии архива.

Основные определения деловой почты

Рассмотрим основные определения письма и его компоненты, а так же другие возможности по работе с ПО ViPNet Деловая почта.

Письмо

Программа **Деловая почта** предназначена для автоматизации работы с документами. В **Деловой почте** документ представлен как „**электронное' письмо**, которое состоит из следующих составляющих:

1. Текст письма – отправитель письма может написать текст в поле письма.
2. Вложения – это файлы, прикрепленные к письму. Эти файлы будут отправлены вместе с письмом.
3. Список получателей – адресаты, которым предназначено письмо.
4. Различные поля (тема, аннотация, дата отправки и т.п.).

При этом некоторые составляющие являются необязательными, а некоторые необходимы для отправки (список получателей).

Все документы в **Деловой почте** хранятся в иерархической **системе папок**, которая организуется пользователем в зависимости от его потребностей.

Письмо можно **зашифровать**. Зашифрованное письмо не может быть прочитано из хранилища сообщений на диске посторонними лицами.

Письмо можно **подписать электронно-цифровой подписью**. Поскольку можно проверить сертификат ключа подписи, то наличие подписи позволяет:

- определить точно, кем было отправлено письмо;
- выявить, нет ли искажений письма;
- исключить возможность отказа от присланного письма со стороны отправителя.

Таким образом электронное письмо в качестве документа может заменить соответствующий бумажный документ.

Квитанция

Квитанция – это подтверждение выполнения какого-то действия (например, отправка письма, доставка, прочтение и др.). В Деловой Почте существует несколько видов квитанций: квитанция об отправке, квитанция о доставке, квитанция о прочтении. Информация о приходе какой-то квитанции выражается появлением буквы (**О** - отправка, **Д, д** - доставка, **Ч, ч** - прочтение) в графе **Атрибуты** главного окна Деловой Почты (подробно см. раздел 7.1, Таблица 2). Кроме того, квитанция может быть представлена в виде

письма, если отправителем письма был сформирован запрос об отправке квитанций о доставке/прочтении в виде отдельного письма (извещения).

Письмо упаковано - При отправке письма это письмо сначала попадает в каталог **.**каталога транспорта, а потом отправляется по назначению, но если транспортный модуль не работает (выключен канал или файла запуска транспорта нет), то состояние письма называется **упаковкой**. В графе **Атрибуты** главного окна появится признак **У, у**.

Письмо отправлено – письмо считается отправленным, когда приходит квитанция об отправке.

Письмо доставлено - письмо считается доставленным, когда приходит квитанция о доставке.

Письмо прочитано - письмо считается прочитанным, когда приходит квитанция о прочтении. Под **прочтением** понимается различное использование письма, как-то:

• Текст письма считается прочитанным, если была выполнена одна из следующих операций: письмо было открыто для просмотра, сохранено на диске, выполнена пересылка письма или выполнена пересылка письма как вложения, письмо помечено как прочтенное.

• Вложение считается прочитанным, если была выполнена одна из следующих операций: открытие вложения для просмотра, сохранение его на диске, печать, копирование вложения в другое приложение (с помощью механизма drag-and-drop или с помощью команды **Копировать файл**), пересылка письма или пересылка письма с вложениями как вложение (с помощью команды **Переслать как вложения**), письмо помечено как прочтенное.

При этом для письма из папки **исходящих**: письмо считается полностью прочитанным, если оно было прочитано всеми получателями письма (заглавная **Ч** в **Атрибутах**) и прочитано частично, если не все получатели прочли его (строчная **ч**). А для **входящего** письма считается, что письмо прочитано полностью (заглавная **Ч)**, если прочитаны текст письма и все вложения, письмо прочитано частично (строчная **ч)**, если остались непрочитанными некоторые вложения.

Автопроцессинг

Автопроцессингом называется автоматическая обработка файлов и писем. В Деловой Почте предусмотрена автоматическая обработка файлов (для отправки по почте) и входящих писем в соответствии с различными **правилами**, задаваемыми пользователем.

Адресная книга – список всех адресатов, которым Вы можете отправлять письма, и от которых Вы можете получать письма.

Понятие об административных программах сети . Ключевая информация для пользователя и АП

Программа **Деловая почта** предназначена для работы в VPN (Virtual Private Network) сети, конфигурация которой создается специальной административной программой, которая называется **Центр Управления Сетью** (ЦУС). Кроме того, в сети VPN используется система защиты информации, которой управляет тоже специальная административная программа **Удостоверяющий и Ключевой центр** (УКЦ). УКЦ выполняет две основные функции:

- заверение сертификатов;
- создание и обновление **ключевой информации**.

Обе эти программы (ЦУС и УКЦ) используются для создания некоторых ключевых наборов файлов для каждого пользователя и для каждого абонентского пункта (АП), без которых **Деловая почта** не может начать свою работу.

Для абонентского пункта программа **ЦУС** создает набор справочников (адресная информация), который должен быть помещен в каталог установки **Деловой почты.**

Для абонентского пункта программа **УКЦ** создает набор файлов, содержащих ключевую информацию (т.н. ключевой набор), общую для всего абонентского пункта. Этот ключевой набор располагается в специальном подкаталоге каталога транспорта. **Деловая почта** пользуется защищенным транспортом сети ViPNet, который может обслуживать несколько прикладных задач. Данная версия **Деловой почты** подразумевает, что каталог транспорта задается в настройках. Обычному пользователю не нужно ничего настраивать, так как это задается по умолчанию.

Для каждого пользователя АП программа **УКЦ** создает один набор файлов с ключевой информацией (т.н. ключевую дискету) и **парольную информацию**. Без ключевой дискеты невозможно запустить программу Деловая Почта. Термин 'ключевая дискета' сложился исторически с тех времен, когда ключевая информация для пользователей действительно размещалась на дискетах. Теперь эта информация может быть расположена на любом диске в любом каталоге. На одном абонентском пункте может быть сколько угодно пользователей.

Адресная книга

Этот раздел посвящен описанию **Адресной книги** и работе с ней.

Определение Адресной книги

При создании письма, если выбрать пункты меню **Редактирование> Добавить получателя** или просто нажать кнопку **Добавить получателя,** Вы оказываетесь в адресном справочнике, в котором перечислены все получатели, которым Вы можете отправлять письма, и от которых Вы можете получать письма. Этот адресный справочник называется **Адресная книга** (Рисунок).

Уровни адресации

Адресация имеет **три уровня**

Первый уровень сетевой и соответствует различным абонентским пунктам. Этот уровень называется **Абонентский пункт.** Зашифрованная информация при выборе адресата на этом уровне может быть прочитана всеми пользователями АП - получателя.

На абонентском пункте может быть несколько коллективов. **Второй уровень** соответствует **коллективам** абонентского пункта, выбранного на первом уровне, и имеющим различные ключи для шифрования информации. Этот уровень называется **Коллектив**. Зашифрованная информация при выборе адресата на этом уровне может быть прочитана всеми пользователями выбранного коллектива АП-получателя.

В коллективе может быть несколько пользователей. **Третий уровень** соответствует **конкретным лицам** коллектива, выбранного на втором уровне. Этот уровень называется **Пользователь**. Зашифрованная информация при выборе адресата на этом уровне также может быть прочитана всеми пользователями выбранного коллектива. Этот адрес служит для информации и нигде не используется с точки зрения разграничения доступа.

Один пользователь может входить в несколько коллективов. Причем он может входить в коллективы разных абонентских пунктов.

Замечание: Если в коллективе есть только один пользователь и его имя совпадает с именем коллектива, то **третий уровень** не отображается в адресной книге Деловой почты.

Конкретная система абонентских пунктов, коллективов и пользователей определяется администратором в ЦУС. У пользователя **Деловой Почты** нет возможности создавать или удалять абонентские пункты, коллективы, пользователей.

В адресном справочнике абонентские пункты обозначены пиктограммой в виде компьютера. Если раскрыть эту пиктограмму, то она раскрывается и показывает все коллективы данного пункта. Если аналогичным образом раскрыть коллектив, то становятся видны все пользователи данного коллектива.

При выборе получателя можно воспользоваться любым уровнем адресации.

Автопроцессинг

Автопроцессингом называется автоматическая обработка файлов и писем. В Деловой Почте предусмотрена автоматическая обработка файлов (для отправки по почте) и входящих писем в соответствии с различными правилами, задаваемыми пользователем. В программе имеется возможность вручную запускать выбранные правила автопроцессинга.

Правило для обработки файлов означает, что файлы с заданной маской, предварительно положенные пользователем в заданную папку, будут автоматически отправлены Деловой почтой в заданные адреса.

Правило для обработки входящих писем означает, что файлы вложений и текст письма, поступившие от заданного отправителя, будут автоматически положены в заданную папку. Файлы вложений в этой папке будут иметь имена, под которыми они были отправлены. Имя файла текста письма всегда blank.txt. По умолчанию присутствие этого файла не зависит от того, есть ли вообще текст письма.

После создания правил автопроцессинга, обрабатывающих файлы, сканирование каталогов на наличие в них файлов, происходит каждые 5 секунд.

Для того чтобы задать правила автопроцессинга, нужно выбрать в главном меню пункт **Инструменты**, а в нем подпункт **Настройка.** При этом откроется окно **Настройка**. Нужно выбрать вкладку **Автопроцессинг**.

Созданные правила можно удалить, отключить, редактировать.

Программа применяет только так называемые “включенные” правила (помеченные специальным флажком). Включение (установка флажка) и отключение (снятие флажка) правила производится на вкладке **Автопроцессинг**. Запуск обработки писем (файлов) производится либо автоматически (без участия пользователя, не считая настроек правил), либо вручную с использованием команды **Выполнить…** на вкладке **Автопроцессинг**.

Применение нескольких правил автопроцессинга к одному и тому же письму (файлу) регулируется программой. Для управления этим пользователь задает:

• порядок выполнения правил автопроцессинга с помощью кнопок **Вверх** и **Вниз** в окне настроек Деловой Почты на вкладке **Автопроцессинг**. Эти кнопки позволяют задавать порядок обработки правил по списку сверху вниз;

• включение/выключение опции **Остановить дальнейшую обработку правил** в окне редактирования правила. Включение этой опции означает, что следующие по заданному списку правила не будут далее применяться к данному файлу (письму).

Программа применяет правила автопроцессинга (автоматический и ручной запуск) к письму (файлу) согласно списку и опции остановки применения правил.

В случае возникновения **ошибки** при применении какого-то правила для письма (файла), программа применяет следующее правило по списку и так до конца списка, а затем производит вторичное применение правил по списку, исключая те правила, при которых ошибок не возникло.

Внимание! При попытке автопроцессинга файлов с атрибутами „read-only“, „system“ или „hidden“ программа **не отправляет** письмо, а выдает сообщение об ошибке файлового автопроцессинга, что письмо не может быть преобразовано в конверт, и предлагает пользователю отключить данное правило автопроцессинга в текущей сессии Деловой почты (ответы: **Да, Нет**). При ответе **Да** данное правило отключается. При ответе **Нет** программа не будет пытаться больше отправлять данный файл в этой сессии. Но при повторной загрузке программы, сообщение об ошибке появится вновь.

ПРАКТИЧЕСКАЯ ЧАСТЬ

Описание возможностей по работе с письмом

Для создания и отправки письма используется программа ПО ViPNet Деловая почта. Она устанавливается вместе с ПО ViPNet Client. Запустить ее можно непосредственно с рабочего стола или через ПО ViPNet Монитор. После ее запуска мы окажемся в главном меню Деловой почты (рис.1).

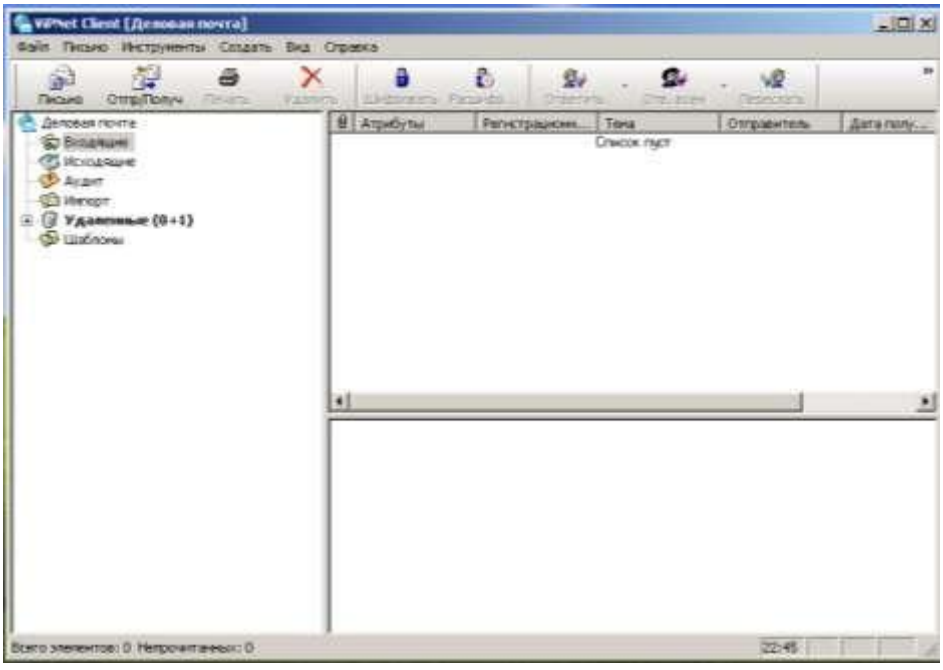


Рис.1 – Главное меню ПО ViPNet Деловая почта

Для того, чтобы создать письмо необходимо выбрать вкладку письмо (рис.1). Появится окно создания письма и назначения получателей (рис.2)

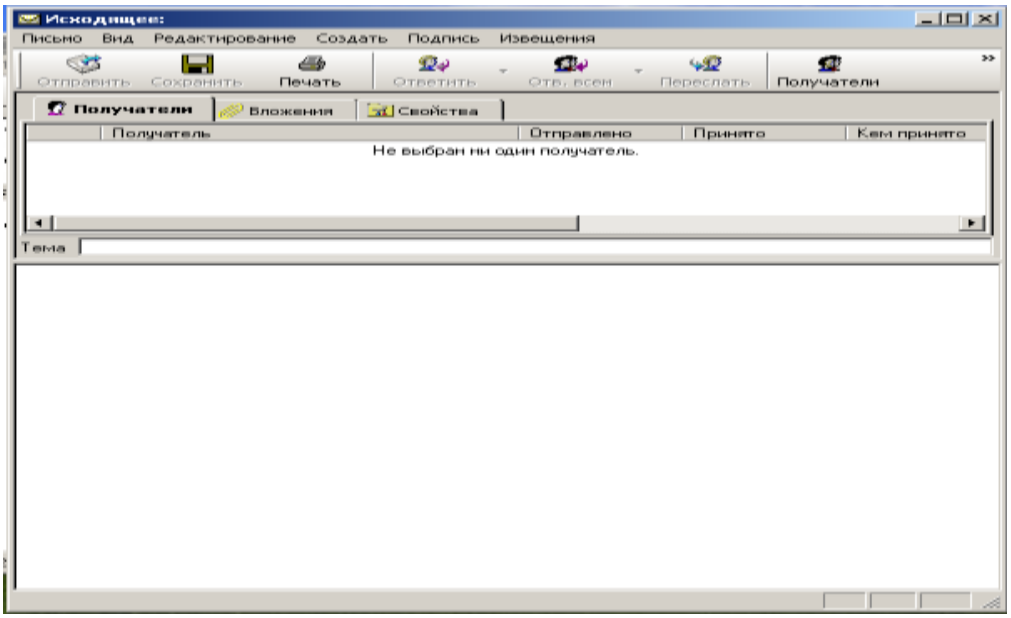


Рис.2 – Окно создания писем

Чтобы выбрать получателей данного письма необходимо выбрать вкладку Получатели (рис.2). Откроется адресная книга, в которой будут содержаться все пользователи вашей и доверенной сетей (рис.3).

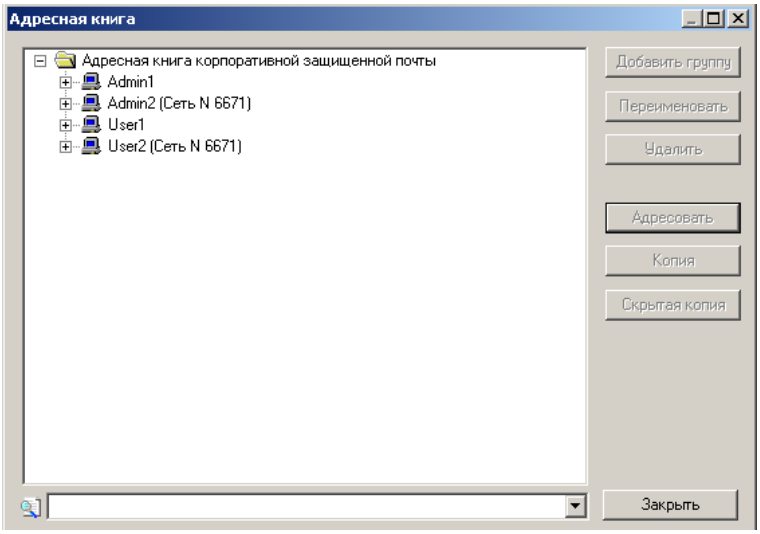


Рис.3 – Адресная книга

После выбора получателя нужно выбрать вкладку Адресовать и затем активировать вкладку Отправить(рис.2).

При получении письма другим пользователем появится уведомление о входящем письме и будет предложено его открыть (рис.4).

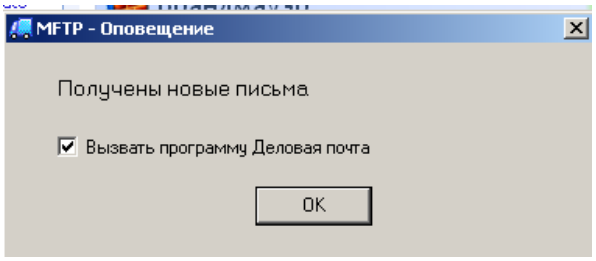


Рис.4 –Уведомление о получении письма.

Стоит заметить, что при отправке письмо шифруется и при получении его необходимо расшифровать. Для этого используется вкладки Шифровать и расшифровать (рис.1).

Так же, полученное письмо можно разослать остальным пользователям при необходимости. Для этого используется вкладка Переслать (рис.1).

Для повышения сохранности письма можно его подписать с помощью текущего сертификата. Для этого используется вкладка Подпись (рис.2)

Для проверки подписи необходимо при получении письма щелкнуть по нему правой кнопкой мыши и выбрать пункт Проверить подпись. Откроется окно в котором будет описан сертификат (рис.5).

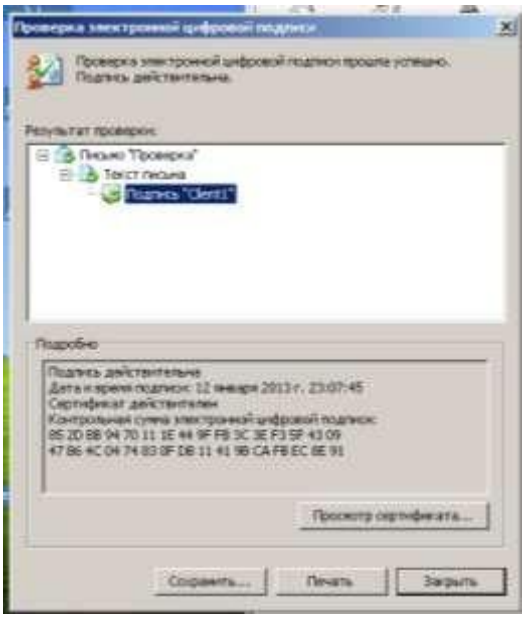


Рис.5 – Проверка подписи письма

АВТОПРОЦЕССИНГ И ЕГО НАСТРОЙКА

При выборе вкладки **Автопроцессинг** можно настроить автоматическую обработку файлов (для отправки по почте) и входящих писем в соответствии с различными правилами, задаваемыми пользователем.

Для этого необходимо выбрать Инструменты – Настройки - Автопроцессинг (рис.6).

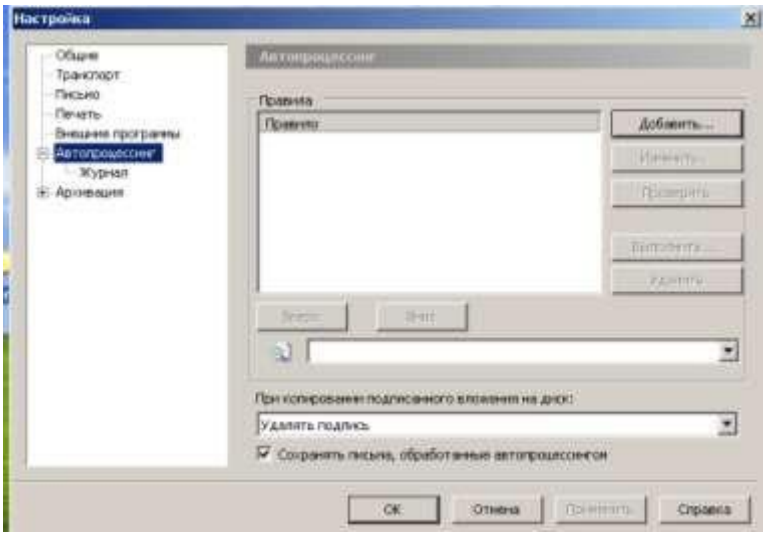


Рис.6 – Вкладка Автопроцессинг

Данный пункт помогает упростить отправку писем, путем добавлений правил оформления писем. Для того, чтобы добавить новое правило необходимо выбрать Добавить (рис.6). Далее появится сообщение, в котором будет предложено выбрать для чего будет настроено правило (рис.7).

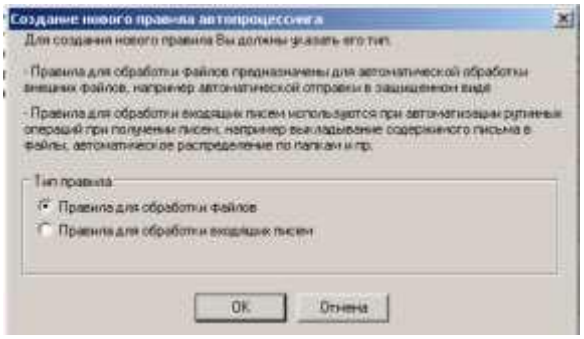


Рис.7 – Меню выбора

Далее появится меню настройки правила (рис.8 и рис.9)

Рис.8 –Задание условий

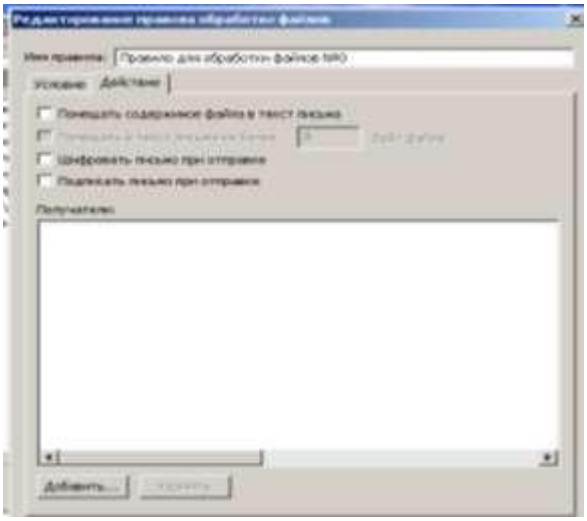


Рис.9 – Задание действий

Рассмотрим настройку условий. В поле каталог можно указать любую папку, при добавлении в которую текстового файла-он будет автоматически отправлено. В поле маска можно указать тип файла(например .docx,.txt и т.д.).

Рассмотрим настройку действий. Обязательным условием отправки файла в виде письма является пункт Помещать содержимое файла в текст письма. Если будет стоять флажок напротив этого пункта, то при помещении текстового файла в папку, указанную в действиях, оно будет отправлено в виде письма. Если не будет указано-то в виде вложения. Так же, можно зашифровать и подписать письмо при отправке при выборе соответствующих пунктов. Так же можно выбрать получателей данного письма. Для этого необходимо воспользоваться вкладкой Добавить (рис.9).

Теперь рассмотрим настройку автопроцессинга при получения писем. Для этого при добавлении правила необходимо выбрать Правила для обработки входящих писем (рис.7). После этого появится меню настройки правила (рис.9 и рис.10).

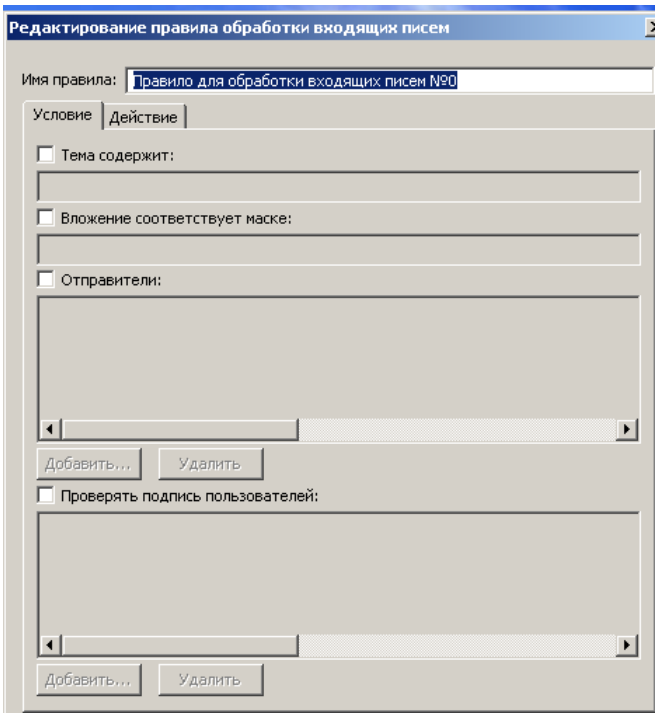


Рис.9 – Настройка условий

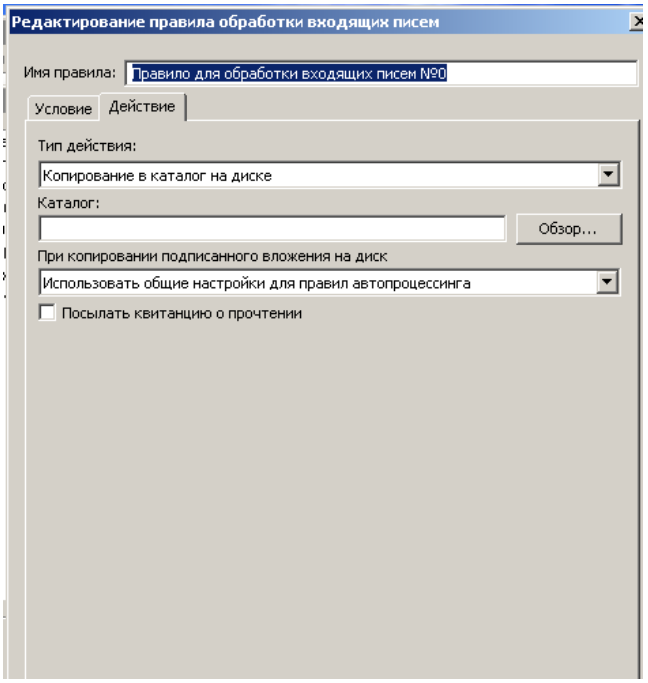


Рис.10 – Настройка действий.

Рассмотрим настройку условий. Как видно из рисунка, можно указать тему письма, для этого необходимо поставить флажок на данном пункте и ввести название темы. Можно указать отправителей, при получении писем от которых они будут автоматически обрабатываться. Так же, можно проверять подписи этих пользователей при получении письма.

Рассмотрим настройку действий. Можно указать тип действия, который будет применяться к полученному файлу. Как видно из рисунка 10 выбран тип Копирование в каталог на диске. То есть, при получении письма будет создана его копия и помещена в каталог, который можно задать в поле Каталог. Немаловажным пунктом служит пункт Показывать квитанцию о прочтении. Ведь можно настроить автопроцессинг и не узнать, пришло письмо или нет, так как оно будет автоматически обработано. А с помощью данной вкладки будет выведено сообщение об успешной обработке письма.

ВАРИАНТЫ ЗАДАНИЙ

1. Создать правило автопроцессинга для обработки файлов. Указать произвольный каталог и выставить маску файлов для docx файлов. Поместить в файл не более 5 байт файла и отправить всем пользователям сети.

2. Создать правило автопроцессинга для входящих писем. Название темы "Проверка". В качестве отправителя установить одного пользователя и не проверять подпись. Выбрать произвольный каталог. Действия с файлами реализовать по указанию преподавателя.

3. Создать письмо с подписью пользователя и отправить всем пользователям сети.

4. Отправить вложение с подписью пользователю в сети.

КОНТРОЛЬНЫЕ ВОПРОСЫ

Лабораторная работа№1 «Механизмы обеспечения информационной безопасности электронных документов»

1. Что такое ECM?
2. Что такое система электронного документооборота?
3. Назовите недостатки бумажного документооборота?
4. Что такое документооборот?
5. Назовите преимущества электронного документооборота?
6. Какие основные механизмы обеспечения конфиденциальности электронных документов можно применить?
7. Какие средства защиты доступа используются для обеспечения целостности электронных документов?
8. Какие методы аутентификации могут быть использованы для обеспечения безопасности электронных документов?
9. Какие технические меры могут быть применены для обеспечения защиты от несанкционированного доступа к электронным документам?
10. Какие процедуры контроля и мониторинга могут быть использованы для обнаружения нарушений информационной безопасности электронных документов?

Лабораторная работа№2 «Защищенные системы электронного документооборота»

1. Что такое СЭД?
2. Главные особенности российского делопроизводства влияющих на специфику отечественных СЭД?
3. Основные черты переносимости СЭД?
4. Какие существуют целы физической реализации СЭД?
5. Кто несет ответственность за содержание и оформление документа?
6. Какие основные принципы обеспечения безопасности могут быть применены в системе электронного документооборота?
7. Каким образом могут быть защищены электронные документы от утраты или повреждения?
8. Какие меры могут быть предприняты для защиты от вредоносного программного обеспечения в системе электронного документооборота?
9. Какие процедуры резервного копирования и восстановления могут быть применены для обеспечения надежности системы электронного документооборота?
10. Каким образом может осуществляться контроль доступа к системе электронного документооборота и ее компонентам?

Лабораторная работа№3 «Применение электронной подписи в системах электронного документооборота»

1. Что такое электронная подпись?
2. Основные свойства ЭЦП?
3. Для чего нужна ЭЦП?
4. Дайте определение электронного документооборота.
5. Какие существуют проблемы при использовании электронного документооборота?
6. Как работает электронная подпись и какие преимущества она может предоставить в системе электронного документооборота?
7. Какие требования и правила существуют для использования электронной подписи в системах электронного документооборота?
8. Каким образом можно проверить подлинность электронной подписи в системе электронного документооборота?
9. Какие технические и организационные меры могут быть применены для защиты от подделки или несанкционированного использования электронной подписи?
10. Какие существуют стандарты и законодательные нормы относительно использования электронной подписи в системах электронного документооборота?

Лабораторная работа№4 «Настройка межсетевого взаимодействия»

1. Для чего предназначено межсетевое взаимодействие?
2. Виды межсетевых мастер ключей.
3. Какими принципами следует руководствоваться при выборе межсетевого мастер ключа?
4. Для чего необходимо прекращение взаимодействия между сетями?
5. Перечислите по порядку основные действия при настройке взаимодействия между сетями?
6. Какие протоколы и стандарты обеспечивают безопасное межсетевое взаимодействие?
7. Каким образом может быть обеспечена конфиденциальность данных при передаче между сетями?
8. Какие меры могут быть применены для обеспечения целостности данных при межсетевом взаимодействии?
9. Каким образом может быть организован контроль доступа и аутентификация при настройке межсетевого взаимодействия?
10. Какие существуют методы обнаружения и предотвращения атак при межсетевом взаимодействии?

Лабораторная работа№5 «ViPNet Деловая почта»

1. Перечислите функциональные возможности деловой почты?
2. Что такое автопрессинг?
3. Что создает УКЦ и ЦУС для абонентского пункта?
4. Перечислите уровни адресации и поясните каждый из них.
5. Для чего необходимо подписывать письмо с помощью сертификата пользователя?
6. ак работает ViPNet Деловая почта и какие функции она предоставляет?
7. Какие меры безопасности и шифрования применяются в ViPNet Деловой почте?
8. Каким образом обеспечивается конфиденциальность и целостность сообщений при использовании ViPNet Деловой почты?
9. Какие механизмы аутентификации могут быть использованы для обеспечения безопасности при работе с ViPNet Деловой почтой?
10. Какие преимущества и ограничения имеет использование ViPNet Деловой почты в системах электронного документооборота?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. 1. Безопасность электронного документооборота : учебное пособие / П. А. Тищенко, Ю. М. Казаков, Р. А. Филиппов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 54 с. – URL: https://biblioclub.ru/index.php?page=book&id=602225 (дата обращения: 16.02.2023). – Режим доступа: по подписке. – Текст : электронный.
2. Ипатова, Э. Р. Методологии и технологии системного проектирования информационных систем : учебник / Э. Р. Ипатова, Ю. В. Ипатов. – 3-е изд., стер. – Москва : ФЛИНТА, 2021. – 256 с. – URL: https://biblioclub.ru/index.php?page=book&id=79551 (дата обращения: 28.02.2023). – Режим доступа: по подписке. – Текст : электронный.
3. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю. Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 255 с. – URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 28.02.2023). – Режим доступа: по подписке. – Текст : электронный.
4. Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие / В. Г. Спицын ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Эль Контент, 2011. – 148 с. – URL: https://biblioclub.ru/index.php?page=book&id=208694 (дата обращения: 28.02.2023). – Режим доступа: по подписке. – Текст : электронный.
5. Системы защиты информации в ведущих зарубежных странах : учебное пособие / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский ; науч. ред. В. И. Аверченков. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 224 с. - URL: https://biblioclub.ru/index.php?page=book&id=93351 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.
6. ViPNet Client [Деловая почта] версия 3.1 – Руководство пользователя. [Электронный ресурс]/ - http://www.infotecs.ru.