



МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Московский государственный технологический
университет «СТАНКИН»
(ФГБОУ ВО «МГТУ «СТАНКИН»)

Институт
информационных
технологий

Кафедра
информационных технологий
и вычислительных систем

ОТЧЕТ О ВЫПОЛНЕНИИ
ЛАБОРАТОРНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ
«ГИПЕРМЕДИЙНЫЕ СРЕДЫ И ТЕХНОЛОГИИ»

СТУДЕНТА 4-го КУРСА бакалавриата ГРУППЫ ИДБ-20-02
(уровень профессионального образования)

ЕРДОГАН ДЕНИЗ ЕРДАЛОВИЧ

НА ТЕМУ

**Организация совместной работы над гипермедийными
электронными документами: совместная работа, авторство,
электронная цифровая подпись**

Направление: 09.03.01 Информатика и вычислительная техника
Профиль подготовки: Программное обеспечение

Отчет сдан «_____» _____ 2024 г.

Оценка _____

Преподаватель _____ Рожкова О. А., ст. преподаватель _____
(Ф.И.О., должность, степень, звание.) (подпись)

МОСКВА 2024

Цель работы: приобретение теоретических и практических знаний, позволяющих осуществлять совместную работу над гипермедийными документами несколькими лицами, а также осуществлять создание и проверку электронных подписей документов.

Используемое ПО:

- рабочая станция с установленной ОС *Windows 11*;
- офисный пакет для создания и обработки файлов формата OOXML: *Microsoft Office 2023*;
- Приложение *GnuPG*;
- Программа Kleopatra;
- Приложение Telegram.

Основные термины:

- **Коллаборация** - совместная деятельность, например, в интеллектуальной сфере, двух и более человек или организаций для достижения общих целей, при которой происходит обмен знаниями, обучение и достижение согласия. Как правило, этот процесс требует наличия руководящего органа, при этом форма руководства может быть и общественной при сотрудничестве равноправных членов децентрализованного сообщества. Считается, что участники коллаборации могут получить больше возможностей достижения успеха в условиях конкуренции за ограниченные ресурсы. Коллаборация может существовать и при противоположности целей, но в этом контексте данное понятие используется редко;
- **Системы контроля версий** - программное обеспечение для облегчения работы с изменяющейся информацией. Система управления версиями позволяет хранить несколько версий одного и того же документа, при необходимости возвращаться к более ранним версиям, определять, кто и когда сделал то или иное изменение, и многое другое. Такие системы наиболее широко используются при разработке программного обеспечения для хранения исходных кодов разрабатываемой программы. Однако они могут с

успехом применяться и в других областях, в которых ведётся работа с большим количеством непрерывно изменяющихся электронных документов. В частности, системы управления версиями применяются в САПР, обычно в составе систем управления данными об изделии (PDM). Управление версиями используется в инструментах конфигурационного управления;

- **Авторское право** - в объективном смысле - право, позволяющее регулировать правоотношения, связанные с созданием и использованием (изданием, исполнением, показом и т. д.) произведений науки, литературы или искусства, то есть объективных результатов творческой деятельности людей в этих областях. Программы для ЭВМ и базы данных также охраняются авторским правом. Они приравнены к литературным произведениям и сборникам, соответственно;
- **Контрольная сумма (хэш-сумма)** – некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении. Также контрольные суммы могут использоваться для быстрого сравнения двух наборов данных на неэквивалентность: с большой вероятностью различные наборы данных будут иметь неравные контрольные суммы. Это может быть использовано, например, для обнаружения компьютерных вирусов. Несмотря на своё название, контрольная сумма не обязательно вычисляется путем суммирования;
- **Электронная цифровая подпись** (электронная подпись, ЭП, цифровая подпись, ЦП, ЭЦП) - реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость);
- **Сертификат открытого ключа** (сертификат ЭП, сертификат ключа подписи, сертификат ключа проверки электронной подписи (согласно ст. 2 Федерального Закона от 06.04.2011 «Об электронной подписи» № 63-ФЗ)) —

электронный или бумажный документ, содержащий открытый ключ, информацию о владельце ключа, области применения ключа, подписанный выдавшим его Удостоверяющим центром и подтверждающий принадлежность открытого ключа владельцу. Открытый ключ может быть использован для организации защищённого канала связи с владельцем двумя способами: - для проверки подписи владельца (аутентификация), - для шифрования посылаемых ему данных (конфиденциальность). Существует две модели организации инфраструктуры сертификатов: централизованная (PKI) и децентрализованная (реализуемая на основе т. н. сетей доверия), получившая наибольшее распространение в сетях *PGP*;

- **Digital rights management (DRM), Технические средства защиты авторских прав (ТСЗАП)** - программные или программно-аппаратные средства, которые намеренно ограничивают либо затрудняют различные действия с данными в электронной форме (копирование, модификацию, просмотр и т. п.), либо позволяют отследить такие действия. *DRM* представляет собой набор систем контроля и управления доступом, а также преднамеренного нарушения авторских прав.

Практическая часть:

Задание № 1:

Требуется: Открыть файл документации, ограничить доступ к файлу в виде записи исправлений, сохранить файл.

Результат:

Был выбран *.docx* файл для выполнения задания представленный на рисунке

№ 1:

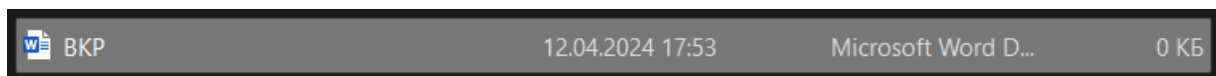


Рисунок № 1 – файл выбранный для выполнения поставленного задания.

Для того, чтобы ограничить доступ к файлу, нужно его (файл) открыть в режиме “Редактирование”, зайти во вкладку “Review”, там выбрать пункт “Restrict Editing” как показано на рисунке № 2:

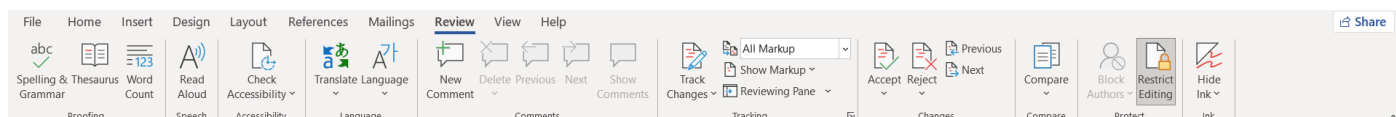


Рисунок № 2 – раздел ограничения доступа к файлу.

После чего появится меню для определения пунктов ограничений. В нём (меню) необходимо в разделе “Editing restrictions” поставить галочку напротив “Allow only this type of editing in the document”, а также в выскакивающем меню выбрать подпункт “Tracked changes”. После подтвердить изменения как показано на рисунке № 3 путём нажатия кнопки “Yes, Start Enforcing Protection”:

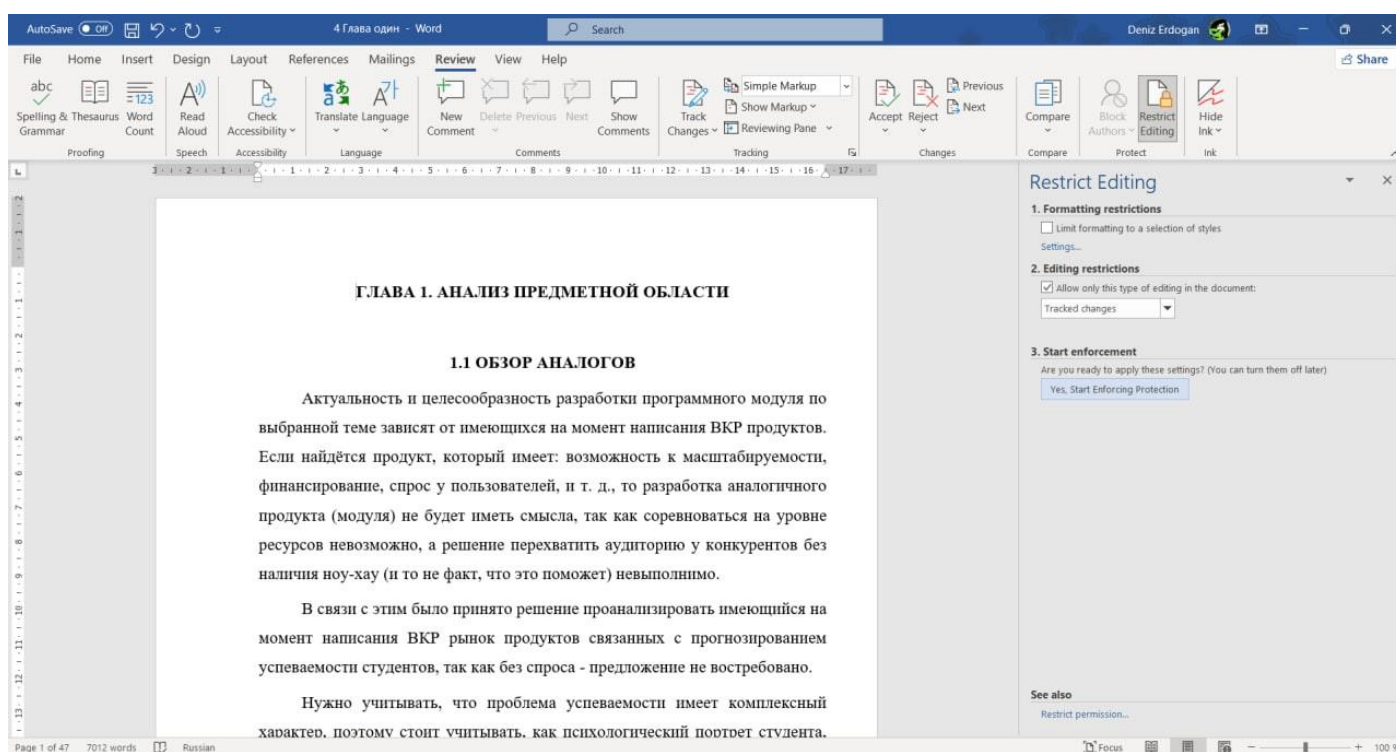


Рисунок № 3 – меню ограничения доступа к файлу.

После чего *Microsoft Word* предложит установить пароль для снятия ограничений как показано на рисунке № 4:



Рисунок № 4 – окно установки пароля для снятия ограничений файла.

Установка пароля необязательна, но ради обеспечения безопасности стоит его (пароль) ввести.

После следует закрыть файл и сохранить изменения как показано на рисунке № 5:

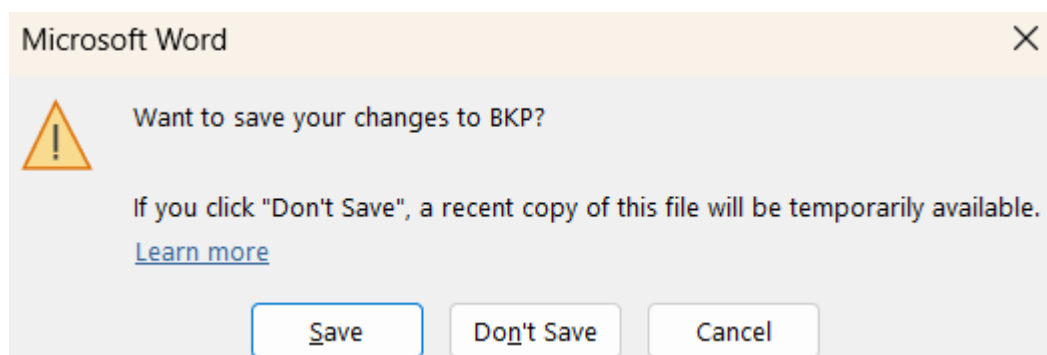


Рисунок № 5 – сохранение изменений.

Задание № 2:

Требуется: Сформировать пару ключей GPG, экспортировать открытый ключ в файл.

Результат:

Была создана пара ключей путём ввода команды `gpg --gen-key` в терминал ОС Windows 11 после установки программного обеспечения GnuPG. Однако генерация происходит не моментально, для начала от пользователя требуется ввести личные данные (полное имя, почта) как показано на рисунке № 6:

```

PS C:\Users\Deniz> gpg --gen-key
gpg (GnuPG) 2.4.5; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Замечание: "gpg --full-generate-key" вызывает полнофункциональный диалог создания ключа.

GnuPG должен составить идентификатор пользователя для идентификации ключа.

Ваше полное имя: Deniz Erdogan
Адрес электронной почты: erdogan33@mail.ru
Вы выбрали следующий идентификатор пользователя:
  "Deniz Erdogan <erdogan33@mail.ru>"

Сменить (N)Имя, (E)Адрес; (O)Принять/(Q)Выход? |

```

Рисунок № 6 – ввод личных данных для генерации пары ключей.

После появляется меню для дальнейших действий. Если выбрать пункт “Принять”, то появится окно требующие установку пароля как показано на рисунке № 7:

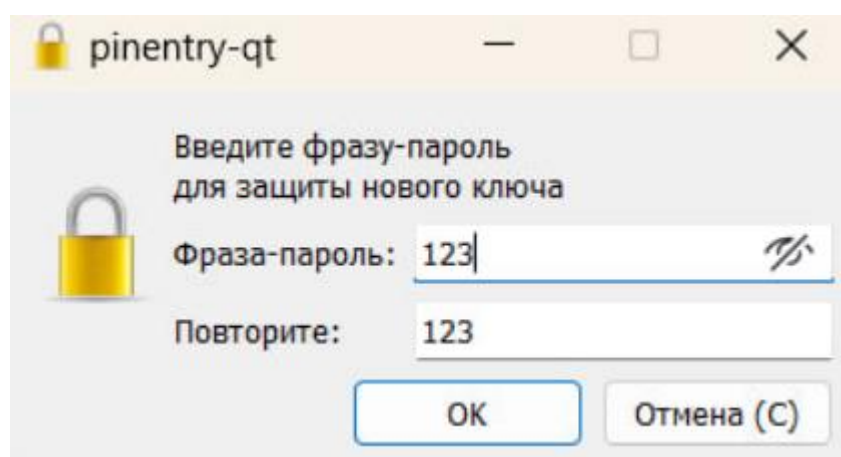


Рисунок № 7 – окно создания пароля при генерации ключей.

Если ввести небезопасный пароль, то появится следующее предупреждение как на рисунке № 8:

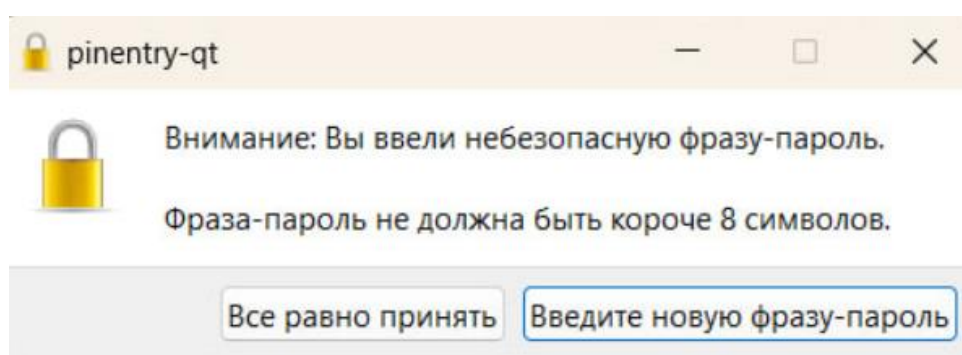


Рисунок № 8 – предупреждение о небезопасности пароля.

После чего создастся пара ключей как показано на рисунке № 9:

```
открытый и секретный ключи созданы и подписаны.  
  
pub    ed25519 2024-04-09 [SC] [    годен до: 2027-04-09]  
       48065AD6095176813F59A26D0A77E32653D9DAA0  
uid    Deniz Erdogan <erdogan33@mail.ru>  
sub    cv25519 2024-04-09 [E] [    годен до: 2027-04-09]  
  
PS C:\Users\Deniz> |
```

Рисунок № 9 – сгенерированные ключи.

Для экспортирования открытого ключа в файл воспользуемся удобной программой с интерфейсом *Kleopatra*.

Так при открытии программы появится список имеющихся на момент открытия программы ключей. В этом меню следует выбрать недавно созданный ключ, в меню инструментов сверху от списка ключей выбрать пункт “Экспортировать в файл...” как показано на рисунке № 10:

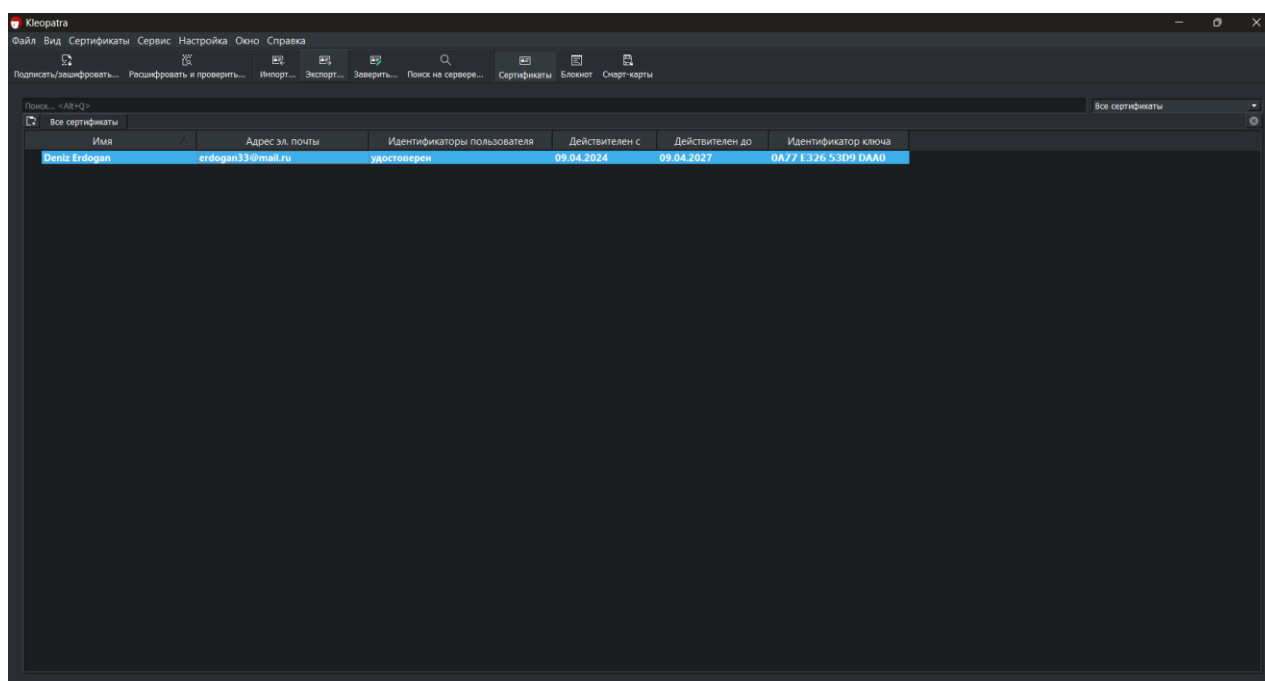


Рисунок № 10 – экспорт ключа в файл.

После появится меню для выбора файла, в который будет экспортироваться ключ, как показано на рисунке № 11:

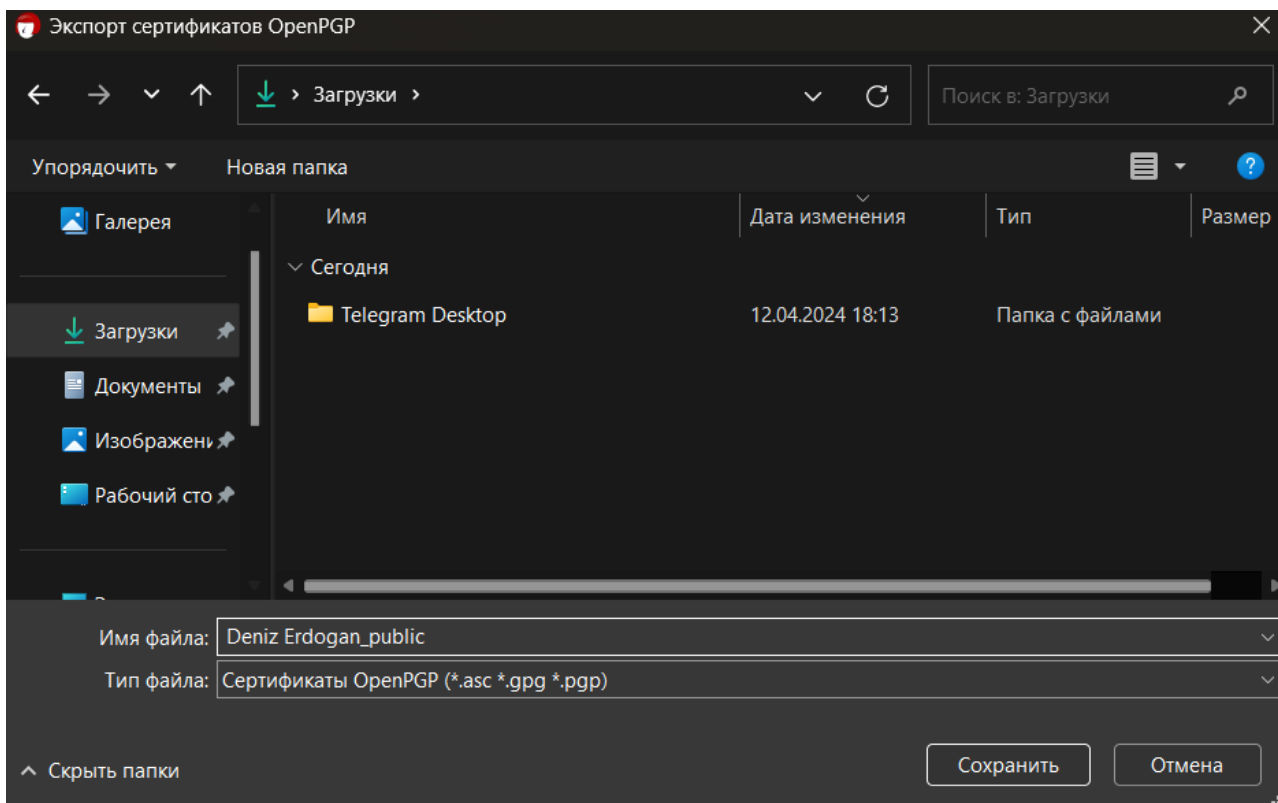


Рисунок № 11 – выбор файла для экспорта ключа.

В этом меню нужно выбрать файл рассмотренный в первом задании.

Задание № 3:

Требуется: Сформировать отторгаемую подпись к файлу документации.

Результат:

Для формирования отторгаемой подписи к файлу введём команду `gpg -b` “путь к документу” как показано на рисунке № 12:

```
PS C:\Users\Deniz> gpg -b "C:\Users\Deniz\Downloads\Deniz Erdogan_0x53D9DAA0_public.asc"
```

Рисунок № 12 – создание отторгаемого ключа.

После чего терминал попросит ввести пароль для разблокировки секретного ключа как показано на рисунке № 13:

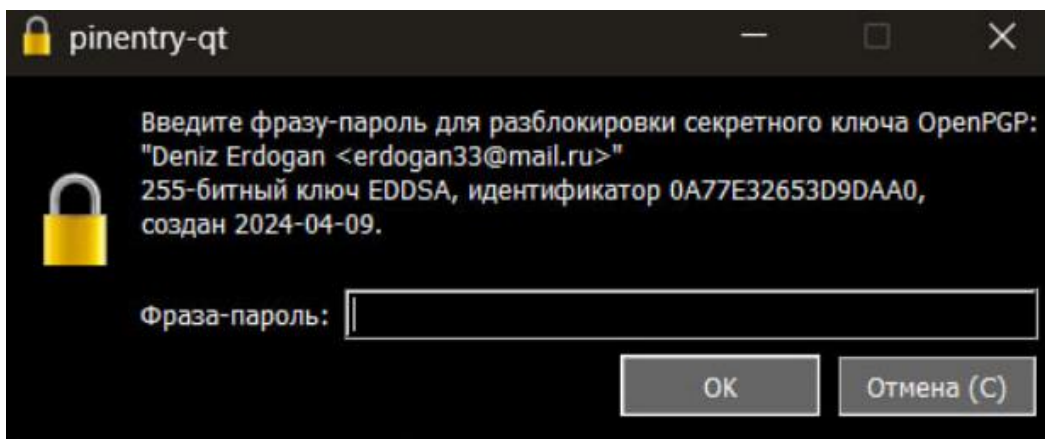


Рисунок № 13 – окно для ввода пароля от секретного ключа.

Для проверки подписи можно ввести команду в терминале `gpg --verify "путь до файла"`.

Задание № 4:

Требуется: Передать файл документации, подпись и открытый ключ другому студенту, аналогичным образом получить пакет его файлов, НЕ ПЕРЕДАВАТЬ И НЕ СООБЩАТЬ СТУДЕНТУ КЛЮЧ ДЛЯ РАЗБЛОКИРОВКИ ДОКУМЕНТА.

Результат:

Передать файлы можно при помощи любого файло-обменника. В данной работе выполнение данного задания было осуществлено при помощи клиента *Telegram*. Таким образом файл документации, подпись и открытый ключ были переданы другому студенту (Вадим Сардаров). Аналогичным образом получен пакет его файлов.

Задание № 5:

Требуется: Импортировать открытый ключ, проверить подпись файла.

Результат:

Для импортирования открытого ключа студента воспользуемся программой *Kleopatra* аналогично заданию № 2, однако в меню инструментов стоит выбрать “Импорт сертификата из файла”. В результате появится следующее окно рисунок № 14:

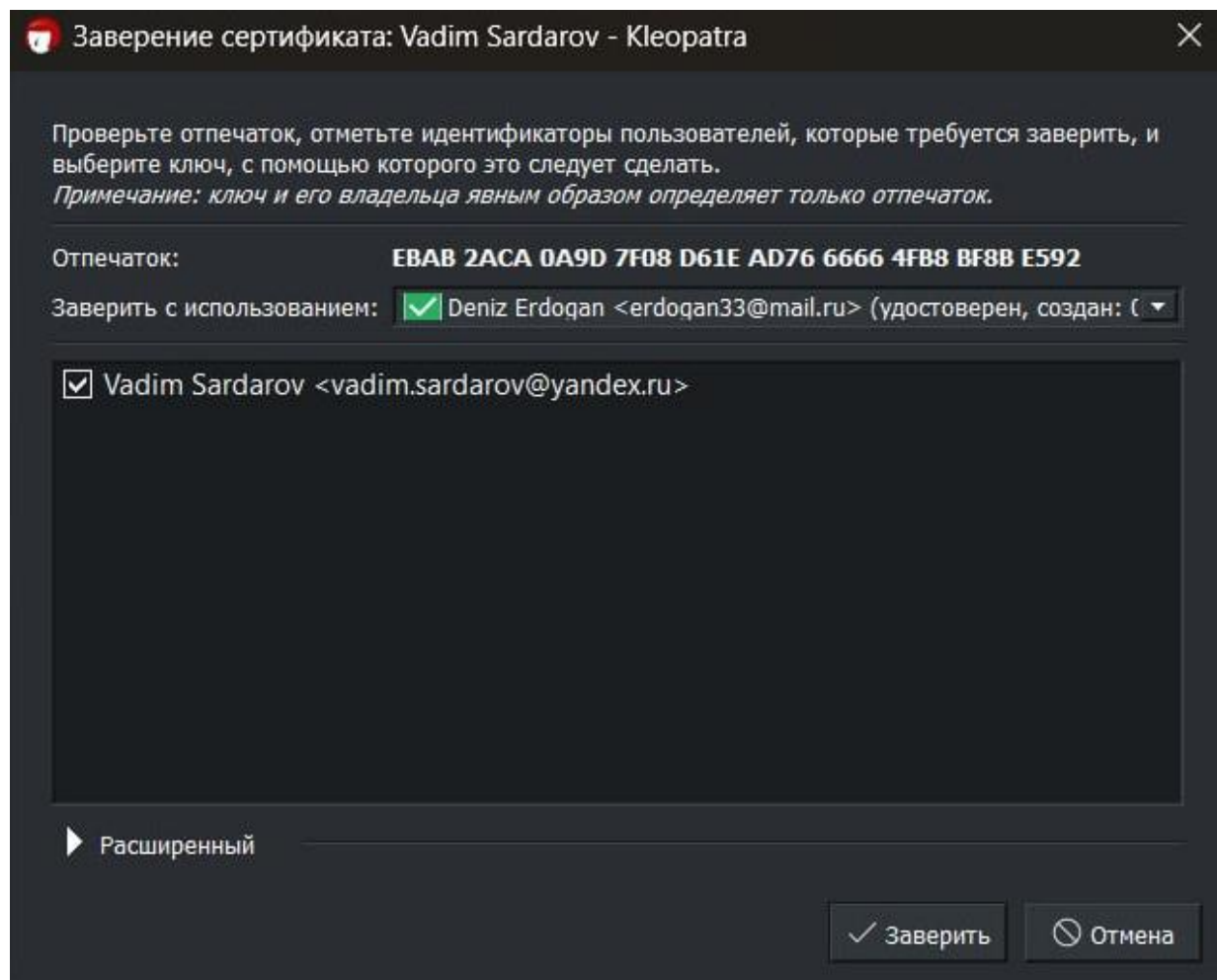


Рисунок № 14 – импорт открытого ключа.

По завершению импорта появится следующее окно уведомлений как показано на рисунке № 15:

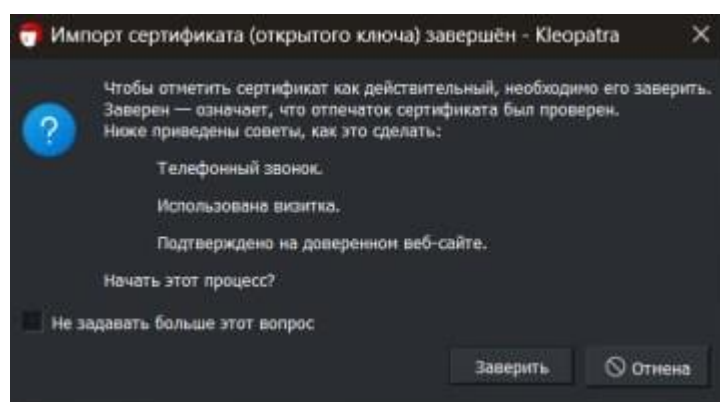


Рисунок № 15 – завершение импорта сертификата.

В результате успешно проделанной работы появится следующее окно:

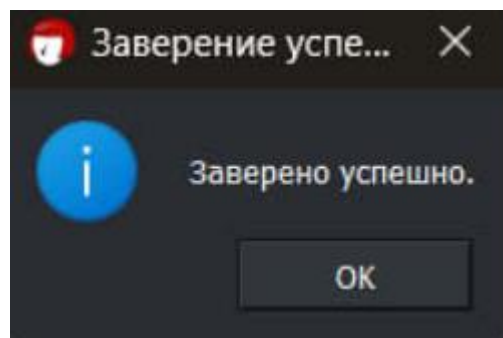


Рисунок № 16 – успешный импорт сертификата.

Задание № 6:

Требуется: Открыть файл документации, произвести не менее 10 полезных исправлений и добавить не менее 5 комментариев, сохранить файл.

Результат:

Файл документации был открыт, были написаны комментарии по работе студента как показано на рисунке № 17:

Оглавление	
ВВЕДЕНИЕ	7
ГЛАВА 1. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ	8
1.1. ПОНЯТИЕ ВЕБ-РЕСУРСА, ПОСВЯЩЕННОГО ОБУЧЕНИЮ ПРОГРАММИРОВАНИЮ	8
1.2. АНАЛИЗ ВЕБ-РЕСУРСОВ, ПОСВЯЩЕННЫХ ОБУЧЕНИЮ ПРОГРАММИРОВАНИЮ	10
1.3. ПУТИ УСТРАНЕНИЯ ТИПОВЫХ НЕДОСТАТКОВ ВЕБ-РЕСУРСОВ, ПОСВЯЩЕННЫХ ОБУЧЕНИЮ ПРОГРАММИРОВАНИЮ	17
1.4. ВЫВОДЫ ПО ГЛАВЕ 1	18
ГЛАВА 2. РАЗРАБОТКА СТРУКТУРЫ И ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ВЕБ-ПРИЛОЖЕНИЯ	19
2.1. ФОРМИРОВАНИЕ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ ВЕБ-ПРИЛОЖЕНИЯ	19
2.2. ФОРМИРОВАНИЕ СТРУКТУРЫ ВЕБ-ПРИЛОЖЕНИЯ	22
2.3. ФОРМИРОВАНИЕ БАЗЫ ДАННЫХ ДЛЯ ВЕБ-ПРИЛОЖЕНИЯ	24
2.3.1. Определение составляющих базы данных	24
2.3.2. Формирование структуры пользователя	25
2.3.3. Формирование структуры статьи	26
2.3.4. Формирование структуры категории	26
2.3.5. Формирование структуры таблицы с проблемами пользователей	27
2.3.6. Формирование структуры таблиц с оценками и комментариями к статьям ..	27
2.4. ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ	28
СПИСОК ЛИТЕРАТУРЫ	30

Рисунок № 17 – комментарии к работе.

А также были проделаны исправления работы студента как показано на

рисунке № 18:

- проверять новые статьи перед их публикацией;
- удалять некачественный контент;
- Переносить контент в другие темы
- решать проблемы пользователей.

Рисунок № 18 – исправления в работе студента.

После чего файл был сохранён.

Задание № 7:

Требуется: Произвести действие аналогично п. 3 для полученного и отредактированного файла.

Результат:

Создана отторгаемая подпись к отредактированному файлу Вадима как показано на рисунке № 19:

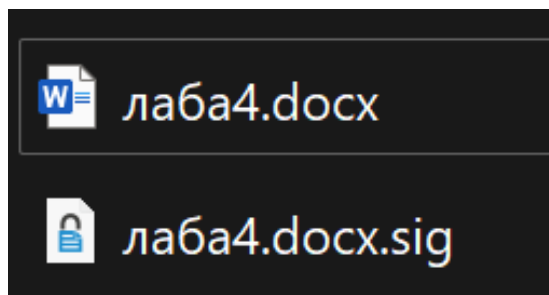


Рисунок № 19 – создание отторгаемой подписи.

Задание № 8:

Требуется: Передать отредактированный файл и получить отредактированную версию собственного файла.

Результат:

Был произведен обратный обмен отредактированными файлами.

Задание № 9:

Требуется: Произвести отмену или принятие исправлений по усмотрению, принять или создать комментарии к комментариям рецензента.

Результат:

Были рассмотрены и приняты по усмотрению исправления Вадима как показано на

рисунках № 20-21:

IX. Исправление 1

Рисунок № 20 – принятие исправлений.

математику, физику, химию, биологию и другие.

Важно отметить, что WDP обладает уникальной способностью визуализации термодинамических процессов, делая их более доступными и понятными для студентов, исследователей и преподавателей. Интерактивные

Рисунок № 21 – прочтение комментариев.

Задание № 10:

Требуется: Произвести действия 3 – 8 еще раз исключая требование к количеству исправлений и комментариев.

Результат:

В результате были (там, где это было необходимо) прокомментированы недочёты работы студента Вадими, а также были исправлены все ошибки в работе однокурсника.

Вывод:

В ходе этой работы мы изучили теорию и практику совместной работы над гипермедийными документами. Мы освоили инструменты, которые предлагает пакет Microsoft Office для совместной работы, и теперь уверенно работаем с данными в коллективе. Также мы изучили криптографические средства на примере *GnuPG*. Теперь мы понимаем, как работают цифровые подписи, и можем обеспечивать подлинность и безопасность документов. Кроме того, мы изучили **DRM** и теперь знаем, как защищать авторские права на гипермедийные и другие документы. Таким образом, эта работа дала нам теоретические знания и практические навыки, которые необходимы для эффективной работы с гипермедийными данными и обеспечения их безопасности.