

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет Информационные технологии

Кафедра Кибербезопасность информационных систем

**ОТЧЕТ ПО ЛАБОРАТОРНЫМ РАБОТАМ**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Автор |  | |  | Заболотный И.А. | | | |
|  | (подпись, дата) | |  |  | | | |
| Обозначение | ИиВТ.10.05.01 | | Группа | | ВКБ21 | | |
| Направление подготовки | | 10.05.01 Компьютерная безопасность | | | | | |
| Профиль | Математические методы защиты информации | | | | | | |
| Дисциплина | Основы информационной безопасности | | | | |  |
|  |  | |  |
| Проверил(а) |  | |  | доцент, Бурякова О.С. | | | |
|  | (подпись, дата) | |  |  | | | |

Ростов-на-Дону

2023

Содержание

Лабораторная работа №1 3

Лабораторная работа №2 11

Лабораторная работа №3 26

Лабораторная работа №4 33

Лабораторная работа №5 36

Лабораторная работа №6 42

Лабораторная работа №7 45

Лабораторная работа №8 50

Лабораторная работа №9 53

Лабораторные работы №10-11 61

Лабораторная работа №12 72

#### Лабораторная работа №1

«Защита паролем документов текстового редактора MS Word и табличного редактора MS Excel»

# Цель работы

Приобретение практических навыков по вычислению по формулам с использованием встроенных математических функций MS Excel

# Задание

Первое задание состоит в том, чтобы защитить документ паролем для открытия файла. Сохранить файл. Повторно открыть его и проверить функцию защиты. Для этого задания будем использовать Документ Word. Чтобы защитить документ Word необходимо перейти во вкладку зашифровать с использованием пароля по пути файл, сведения, защитить документ. (Рис. 1.1)

#### 

#### Рисунок 1.1

Выбираем из раскрывающегося списка «Зашифровать с использованием пароля» и назначаем пароль. В моём случае пароль – 123 (Рис. 1.2)

#### 

#### Рисунок 1.2

Обязательно сохраняем файл и далее закрываем. После вышеупомянутых действий повторно откроем файл для проверки функции

защиты (Рис. 1.3)

#### 

#### Рисунок 1.3

Убеждаемся, что функция защиты активна.

Второе задание состоит в том, чтобы защитить второй документ паролем для изменения файла. Сохранить файл. Повторно открыть его и проверить функцию защиты. Для этого мы должны пройти по такому же пути, как и в задании №1, но на этот раз нужно выбрать «Ограничить редактирование». (Рис. 1.4)

#### 

#### Рисунок 1.4

Выбираем из раскрывающегося списка «Ограничить редактирование» и нас переносит в вкладку «Рецензирование», а именно «Ограничить редактирование». (Рис. 1.5)

#### 

#### Рисунок 1.5

В «Ограничения на редактирование» выбираем из раскрывающегося списка «Только чтение» и нажимаем на «Да, включить защиту». Далее откроется окно для назначения пароля, в моём случае это будет пароль 123. (Рис. 1.6)

#### 

#### Рисунок 1.6

Далее необходимо подготовить документ для рецензирования в режиме примечаний. Установить на него защиту. Отрыть документ повторно и внести примечания в текст. По сути, мы делаем всё то же самое, что и в задании №2, однако из раскрывающегося списка нужно будет выбрать «Примечания». Сохраняем документ и вносим примечания (Рис. 1.7)

#### 

#### Рисунок 1.7

Далее необходимо подготовить документ для рецензирования в режиме исправлений. Установить на него защиту. Отрыть документ повторно и внести исправления в текст. По сути, мы делаем всё то же самое, что и в задании №2, однако из раскрывающегося списка нужно будет выбрать «Запись исправлений».

Сохраняем документ и вносим исправления (Рис. 1.8)

#### 

#### Рисунок 1.8

Далее необходимо сделать анкету вида (Рис. 1.9), то есть (Рис. 1.10)

#### 

#### Рисунок 1.9

#### 

#### Рисунок 1.10

Далее необходимо защитить от изменений лист электронной таблицы и закрыть ее паролем. Для этого мы должны сделать то же самое, что и в задании №1, но перед этим должны выделить все ячейки, потом нажать ПКМ, выбрать формат ячеек, защита и далее поставить галочку на «Скрыть формулы». (Рис. 1.11)

#### 

#### Рисунок 1.11

Далее необходимо защитить от изменений заданный диапазон ячеек. Для этого нужно выделить все ячейки потом нажат ПКМ, выбрать формат ячеек и убрать галочку на «Защищаемые ячейки». Потом же нужно выделить диапазон и перейти по такому же пути, но уже только поставить галочку на «Защищаемые ячейки». И потом защитить лист от изменений.

Далее необходимо разрешить доступ к моей книге определённым пользователям. Это можно сделать через «Рецензирование», а именно «Разрешить изменение диапазонов». Мы выделяем определённый диапазон, создаём его, чтобы он отобразился в списке, нажимаем на «Разрешения» и дальше через «Добавить» добавляем определённых пользователей. (Рис. 1.12)

#### 

#### Рисунок 1.12

Далее необходимо предоставить книгу в совместный доступ и защитить её. Прежде всего мы защищаем книгу точно также, как и лист. И потом сохраняем её в любое удобное облачное хранилище.

Далее необходимо защитить книгу от изменений. Для этого необходимо выбрать из раскрывающегося списка «Зашифровать с использованием пароля» (Рис. 1.13).

#### 

#### Рисунок 1.13

Далее, чтобы снять защиту на книгу, а также для просмотра и изменения её же, необходимо перейти во вкладку файл, потом сведения, и выбрать ту же строку, которую нажимали для защиты. Далее высветится окно для задания нового пароля. Именно там мы стираем символы, что были прежде, и оставляем поле пустым.

Вывод

Я приобрёл практические навыки защиты программ Microsoft.

#### Лабораторная работа №2

«Парольная защита баз данных в Microsoft Access». «Парольная защита и разграничение доступа в Windows XP»

# Цель работы

Приобретение практических навыков защиты программ Microsoft.

# Задание

1. Открываем монопольно базу данных в Microsoft Access (в моем случае она 2019 года);
2. Перейдем во вкладку "Файл" в верхнем меню;
3. Выбираем "Сведения" в левой панели навигации;
4. Нажимаем на "Зашифровать с использованием пароля" (Рисунок 2.1);
5. Вводим новый пароль: “12341234” – и подтверждаем его (Рисунок 2.2);
6. Нажимаем "OK" и сохраняем базу данных.

#### 

#### Рисунок 2.1

#### 

#### Рисунок 2.2

Второе задание состоит в том, чтобы отобразить и скрыть объекты базы данных в окне базы данных:

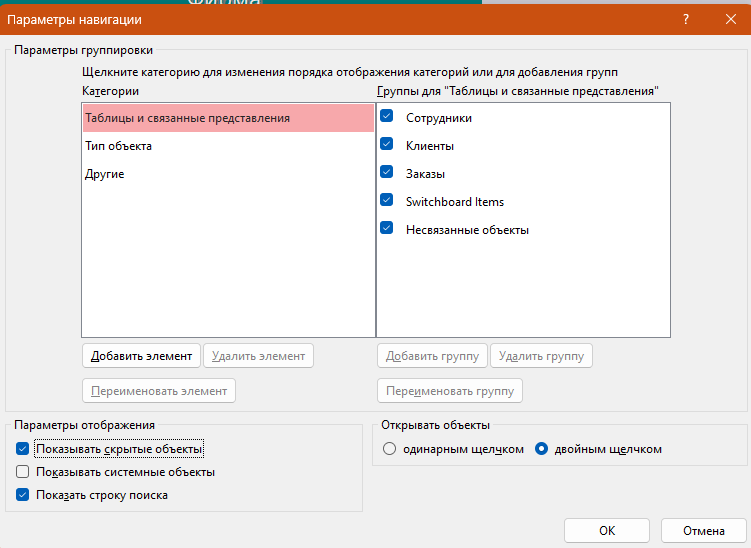
1. В окне “Объекты” скроем Таблицу “Switchboard Items”. Для этого кликнем по ней правой кнопкой мыши и выбираем “Скрыть в этой группе” (Рисунок 2.3);
2. Чтобы отобразить объект снова, перейдем в панель "Параметры навигации". Для этого по пустому месту в окне “Объекты” нажимаем правой кнопкой мыши и выбираем “Параметры навигации” (Рисунок 2.4), где нажимаем пункт “Показать скрытые объекты” (Рисунок 2.5);
3. Нажимаем правой кнопкой мыши на скрытом объекте, который вы хотим отобразить, и нажимаем “Показать в этой группе” (Рисунок 2.6);
4. Выберите "Отобразить объект" или "Скрыть объект" в выпадающем меню.

#### 

#### Рисунок 2.3

#### 

#### Рисунок 2.4



#### Рисунок 2.5

#### 

#### Рисунок 2.6

Далее необходимо отобразить или скрыть объекты, скрытые по умолчанию:

1. Перейдем во вкладку "Файл" в верхнем меню;
2. Выберем "Параметры" в левой панели навигации.
3. Выберем "Текущая база данных";
4. Найдем раздел "Параметры навигации", где снимаем флажок с пункта "Показать скрытые объекты" и наоборот (Рисунок 2.7);
5. Нажимаем "OK".

#### 

#### Рисунок 2.7

Далее необходимо создание макроса, который запускается при первом открытии файла Microsoft Access:

1. Перейдем во вкладку "Создание;
2. Выбираем "Макрос" в группе "Макросы и Код". (Рисунок 2.8);
3. Добавляем необходимые действия в макрос (Рисунок 2.9);
4. Сохраняем макрос под именем “AutoExec”;
5. Теперь он будет запускать при открытии файла Microsoft Access.

#### 

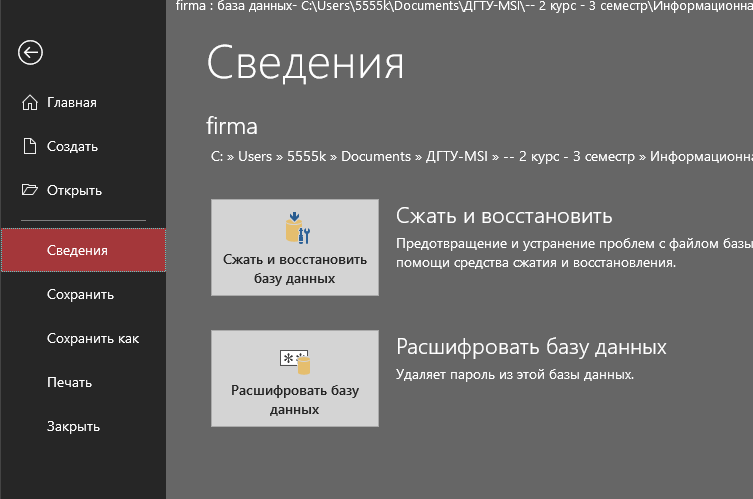
#### Рисунок 2.8

#### 

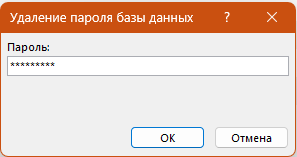
#### Рисунок 2.9

Далее необходимо удалить пароль в базе данных Microsoft Access:

1. Открываем монопольно базу данных в Microsoft Access 2019, для которой хотим удалить пароль;
2. Перейдем во вкладку "Файл" в верхнем меню;
3. Выбираем во вкладке “Сведения” и нажимаем "Расшифровать базу данных" (Рисунок 2.10);
4. Удаляем пароль (Рисунок 2.11);
5. Готово.



#### Рисунок 2.10



#### Рисунок 2.11

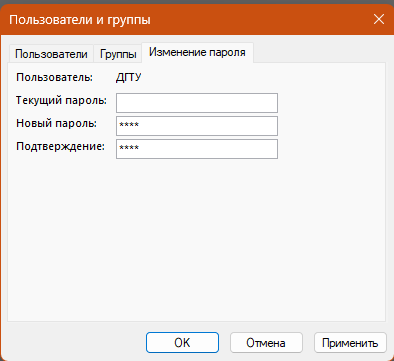
1. Далее необходимо создать или изменить пароля учетной записи пользователя в базе данных Microsoft Access: открываем монопольно базу данных в Microsoft Access 2019 только с расширением .mdb;
2. В поиске введем "Пользователи и разрешения";
3. Выбираем в нем "Пользователи и группы" (Рисунок 2.12);
4. Нажимаем на "Создать…" и создадим пользователя “ДГТУ” с кодом 2023 (Рисунок 2.13);
5. Во вкладке “Изменение пароля” и под пользователем admin устанавливаем пароль 1234;
6. Нажмите "ОК", чтобы сохранить изменения;
7. Затем заходим снова в файл базы данных .mdb под пользователем ДГТУ с пустым паролем. Выполняем пункты 2, 3 и 5 уже под пользователем ДГТУ (Рисунок 2.14) и устанавливаем пароль “2023”/

#### 

#### Рисунок 2.12

#### 

#### Рисунок 2.13



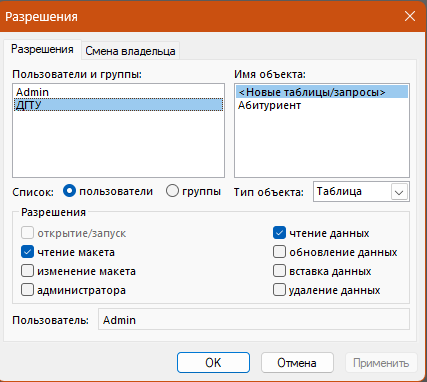
#### Рисунок 2.14

Далее нужно снять пароль с учётной записи пользователя:

1. Откроем снова базу данных в Microsoft Access 2019 с расширением .mdb;
2. В поиске введем "Пользователи и разрешения";
3. Выбираем в нем "Пользователи и группы"
4. Выбираем пользователя (ДГТУ), пароль которого необходимо снять.
5. Нажимаем “Снять пароль”
6. Нажмите "ОК", чтобы сохранить изменения.

Далее нужно сделать защиту на уровне пользователей:

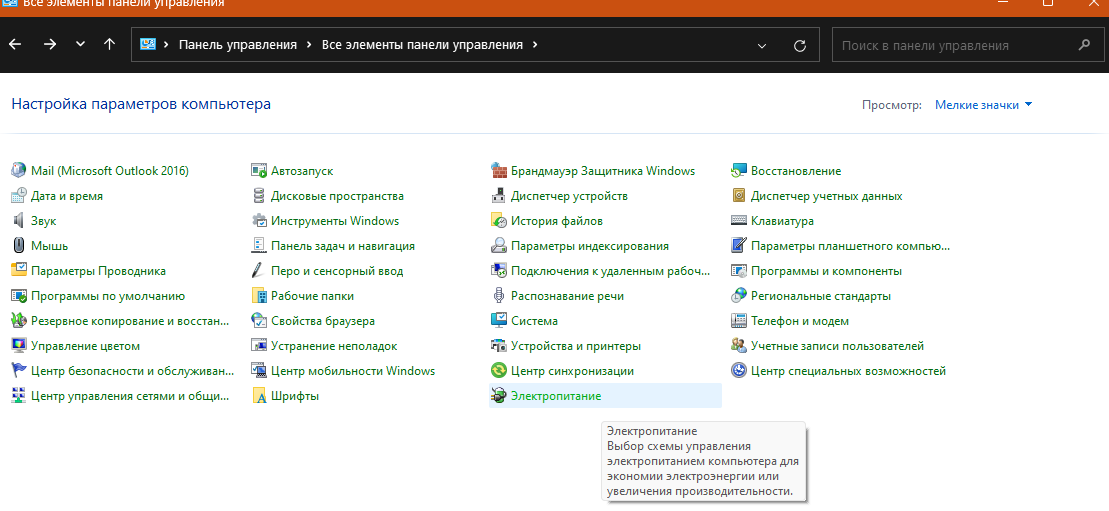
1. Выбираем "Пользователи и разрешения" и нажимает на пункт "Разрешения".
2. Устанавливаем соответствующие разрешения для пользователя ДГТУ (Рисунок 2.15)
3. Нажимаем Ок



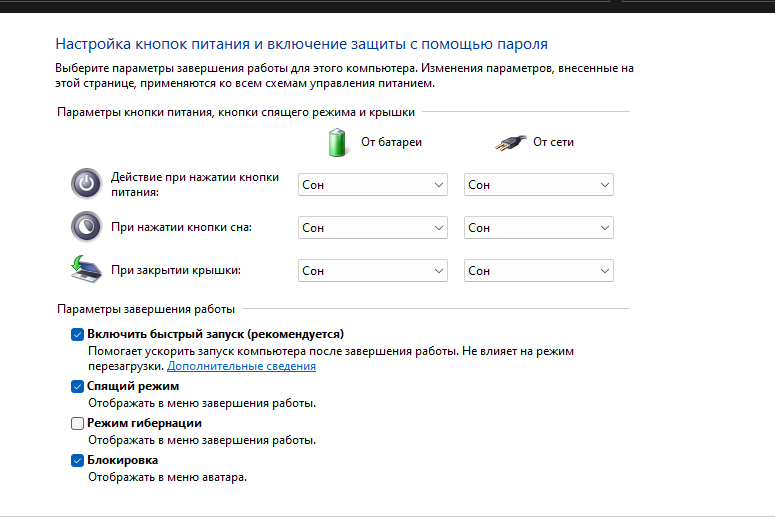
#### Рисунок 2.15

Далее нужно защитить паролем компьютер в ждущем и спящем режимах:

1. Открываем "Панель управления".
2. Выбираем "Электропитание (Рисунок 2.16)
3. На странице параметров плана выберите "Изменение параметров выключения".
4. На странице "Изменение параметров выключения" выберите "Изменение параметров, недоступных в данный момент".
5. Настраиваем его (Рисунок 2.17)
6. Готово



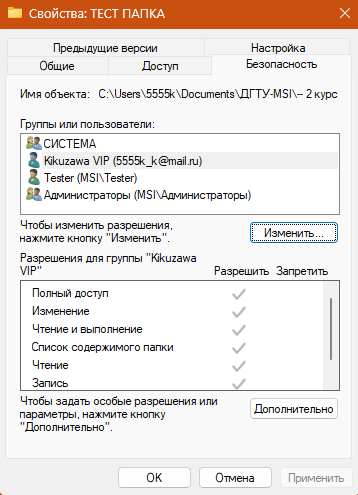
#### Рисунок 2.16



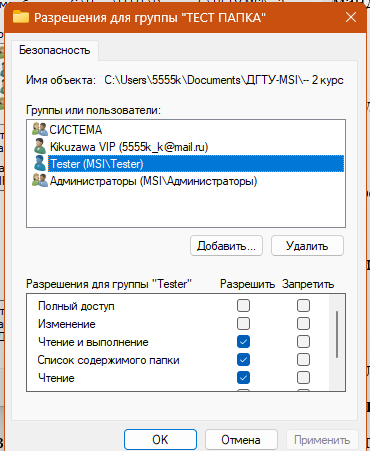
#### Рисунок 2.17

Далее необходимо установить, просмотреть, сменить или удалить разрешения для файлов и папок:

1. Откроем проводник Windows и найдите файл или папку, для которых нужно изменить разрешения;
2. Нажмем правой кнопкой мыши на файле или папке и выберем "Свойства";
3. В открывшемся окне "Свойства" выберем вкладку "Безопасность" (Рисунок 2.18);
4. Нажмем кнопку "Изменить", чтобы изменить существующие разрешения или добавить новых пользователей или группы;
5. Установим необходимые разрешения для выбранных пользователей или групп (Рисунок 2.19);
6. Нажмите "ОК", чтобы сохранить изменения.



#### Рисунок 2.18

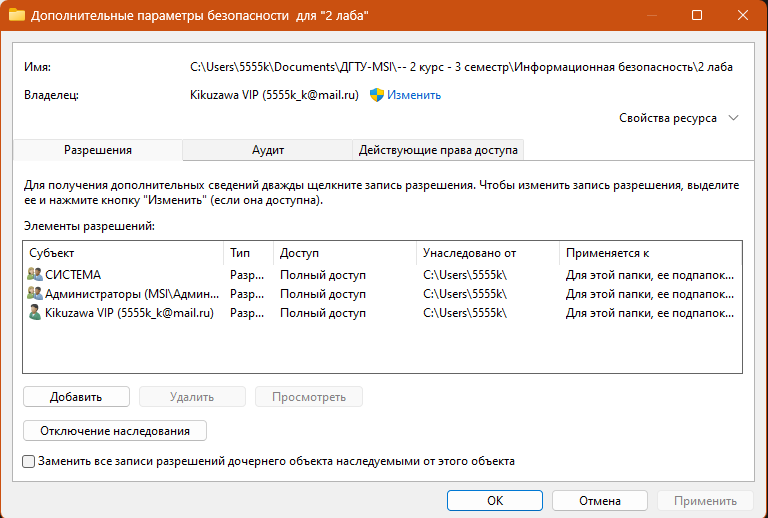


#### Рисунок 2.19

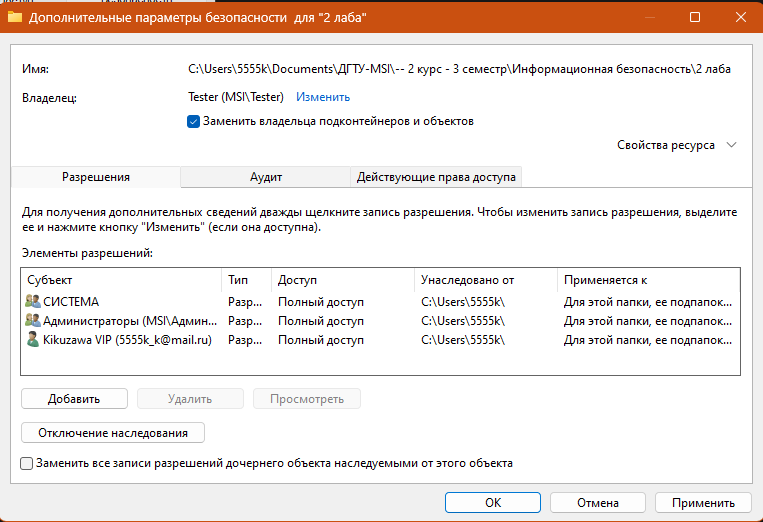
Далее необходимо стать владельцем файла или папки:

1. Откроем проводник Windows и найдем файл или папку, для которых нужно изменить владельца;
2. Нажмем правой кнопкой мыши на файле или папке и выберите "Свойства";
3. В открывшемся окне "Свойства" выбираем вкладку "Безопасность";
4. Нажмите кнопку "Дополнительно", чтобы открыть дополнительные параметры безопасности (Рисунок 2.20);
5. В разделе "Владелец" нажмите кнопку "Изменить";
6. Выбираем пользователя или группу, которой нужно сделать владельцем. В нашем случае – это будет пользователь Tester (Рисунок 2.21)

Нажмите "ОК" и подтвердите изменения.



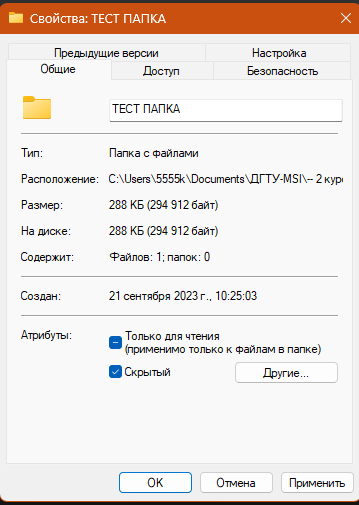
#### Рисунок 2.20



#### Рисунок 2.21

Далее необходимо скрыть файл или папку:

1. Откроем проводник Windows и найдем файл или папку, которые нужно скрыть.
2. Нажмем правой кнопкой мыши на файле или папке и выберем "Свойства".
3. В открывшемся окне "Свойства" установите флажок "Скрытый" в разделе "Атрибуты". (Рисунок 2.22)
4. Нажмите "ОК", чтобы сохранить изменения.



#### Рисунок 2.22

# Вывод

Я приобрёл практические навыки защиты программ Microsoft.

#### Лабораторная работа №3

«Работа с командной строкой. Сетевая активность.»

Цель работы

Получение практических навыков по работе с Командной строкой и по выявлению вредоносных программ на локальном компьютере под управлением Microsoft Windows XP с помощью командной строки.

# Задание

Первое задание состоит в том, чтобы посмотреть инструкцию пользованием такой команды как copy (Рис. 3.1)

#### 

#### Рисунок 3.1

Второе задание состоит в том, чтобы посмотреть инструкцию пользованием такой команды как shutdown (Рис. 3.2)

#### 

#### Рисунок 3.2

Продолжение инструкции (Рис. 3.3)

#### 

#### Рисунок 3.3

Третье задание состоит в том, чтобы посмотреть инструкцию пользованием такой команды как help (Рис. 3.4)

#### 

#### Рисунок 3.4

Четвёртое задание состоит в том, чтобы скопировать файл myfile.txt в папку Files (Рис. 3.5)

#### 

#### Рисунок 3.5

Пятое задание состоит в том, чтобы поменять дату на моём ПК, используя дату, которая записала в файл date.txt (Рис. 3.6)

#### 

#### Рисунок 3.6

Шестое задание состоит в том, чтобы поменять дату на моём ПК, используя дату, которая записала в файл date.txt (Рис. 3.7)

#### 

#### Рисунок 3.7

Седьмое и восьмое задание состоит в том, чтобы отсортировать по возрастанию (Рис. 3.8) и по убыванию (Рис. 3.9)

#### 

#### Рисунок 3.8

#### 

#### Рисунок 3.9

Далее необходимо отобразить инструкцию по использованию команды “netstat” (Рис. 3.10)

#### 

#### Рисунок 3.10

После чего нужно отобразить текущие сетевые подключения (Рис. 3.11)

#### 

#### Рисунок 3.11

# Вывод

Я приобрёл практические навыки по работе с Командной строкой и по выявлению вредоносных программ на локальном компьютере под управлением Microsoft Windows XP с помощью командной строки.

#### Лабораторная работа №4

«Защита от несанкционированного доступа и сетевых хакерских атак»

# **Цель работы**

Ознакомиться с процедурами создания учётных записей пользователей, а также с встроенными компонентами защиты ОС Microsoft Windows XP.

# Задание

Первое задание состоит в то, чтобы создать новую учетную запись пользователя: (Рис. 4.1)

#### 

#### Рисунок 4.1

Вводим имя пользователя и нажимаем кнопку создать. Как можно заметить, «Новый пользователь» появился. (Рис. 4.2)

#### 

#### Рисунок 4.2

Далее необходимо изменить пароль для пользователя Арес. Для этого нажмём по «Арес» и в меню Действие выберем команду «Установка Пароля». Зададим пароль «Греция» (Рис. 4.3)

#### 

#### Рисунок 4.3

Далее создадим локальную группу. Для этого нужно следовать алгоритму:

1. Открыть компонент «Управление компьютером».

2. В дереве консоли выбрать компонент «Локальные пользователи и труппы» и щелкнуть в нём узел Группы.

3. В меню Действие выбрать команду Новая группа.

4. Ввести имя новой группы в поле Имя группы

5. Ввести описание новой группы в поле Описание

6. Выполнить одно из следующих действий.

Чтобы создать другую группу, нажать кнопку Создать и повторите шаги 2 и 3. Чтобы завершить работу, нажмите кнопку Создать, а затем Закрыть. (Рис. 4.4)

#### 

#### Рисунок 4.4

Чтобы добавить пользователя в группу, необходим следовать следующему алгоритму:

1. Открыть компонент «Управление компьютером».

2. В дереве консоли выбрать компонент «Локальные пользователи и группы» и выбрать в нем узел Группы.

3. Выбрать нужную группу.

4. В меню Действие выбрать команду Свойства.

5. Нажать кнопку Добавить.

6. В нижнее поле ввести имена пользователей или групп, которые нужно добавить, или выбрать имена пользователей или групп из верхнего поля и нажать кнопку Добавить.

7. Если необходимо проверить имена добавляемых пользователей или групп необходимо нажать кнопку Проверить имена

А чтобы удалить локальную группу, необходимо следовать следующему алгоритму:

1. Открыть компонент «Управление компьютером».

2. В дереве консоли выбрать компонент «Локальные пользователи и группы» и щелкнуть в нём узел Группы.

3. Выбрать Группу, которую следует удалить.

4. В меню Действие выбрать команду Удалить.

5. В ответ на приглашение Подтвердить удаление нажав кнопку Да.

Следующее задание состоит в том, чтобы познакомиться с Брандмауэром Windows. (Рис. 4.5)

#### 

#### Рисунок 4.5

Вкладка Общие позволяет менять режим работы Брандмауэра Windows. Можно включить брандмауэр (после установки Операционной системы Microsoft Windows XP, система автоматически включает Брандмауэр Windows) или выключить его (при установке другого Брандмауэра на ваш компьютер, Брандмауэр Windows будет выключен автоматически).

Вкладка Исключения позволяет создавать исключения для нужных служб и приложений. Например, если вы точно уверены, что конкретное приложение не будет выполнять несанкционированных удаленных соединений или Брандмауэр Windows заблокировал сетевой доступ приложения, можно создать Исключение и блокировка будет снята.

Вкладка Дополнительно позволяет включить или отключить Брандмауэр Windows для конкретных сетевых подключений, заблокировать или разблокировать сетевые службы.

# Вывод

Я приобрёл практические навыки создания учётных записей пользователей, а также с настроил встроенные компоненты защиты ОС Microsoft Windows XP.

#### Лабораторные работы №5

«Резервное копирование программ, системных параметров и файлов»

Цель работы

Приобретение практических навыков резервного копирования.

# Задание

Первое задание состоит в том, чтобы выполнить архивацию файлов. (Рис. 5.1)

#### 

#### Рисунок 5.1

Далее выбираем нужные файлы и нажимаем на Далее. После чего запустится процесс резервного копирования (Рис. 5.2)

#### 

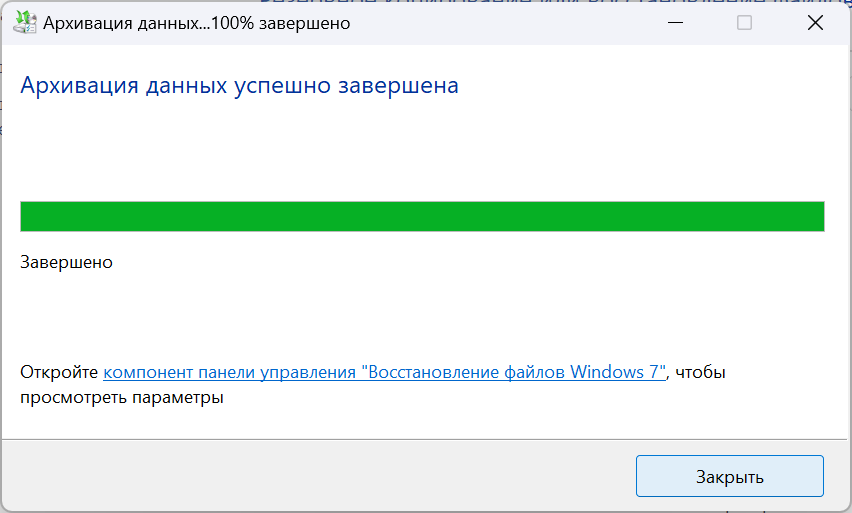
#### Рисунок 5.2

Есть возможность, если необходимо, прекратить резервное копирование (Рис. 5.3)

#### 

#### Рисунок 5.3

После весьма продолжительного ожидания процесс завершён. (Рис. 5.4)



#### Рисунок 5.4

Далее следующее задание состоит в том, чтобы создать образ системы (Рис. 5.5)

#### Создание образа системы Windows 11

#### Рисунок 5.5

Далее необходимо выбрать, где будет создаваться резервная копия. Также необходимо учитывать, что поскольку она содержит всю систему и все установленные программы, места потребуется много. При этом она не может создаваться на системных дисках. (Рис. 5.6)

#### Выбор диска для создания образа

#### Рисунок 5.6

На следующем этапе будут отображены и выбраны все необходимые для работы системы разделы, также, при наличии дополнительных разделов, которые не используются для сохранения резервной копии, их также можно будет включить в резервную копию. (Рис. 5.7)

#### Выбор разделов для записи в резервную копию

#### Рисунок 5.7

В завершение останется подтвердить сохранение резервной копии, в окне будет показано, какой объем места на диске она займёт. Если система зашифрована BitLocker, файлы в резервной копии всё равно будут без шифрования. Нажимаем «Архивировать» и дожидаемся завершения создания бэкапа, это может занять очень продолжительное время. (Рис. 5.8)

#### Запуск создания полной резервной копии Windows 11

#### Рисунок 5.8

На этом процесс создания бэкапа будет завершен и, если когда-либо возникнет такая необходимость, вы сможете восстановить систему полностью из него. Внимание: не переименовывайте папку с резервной копией на накопителе.

# Вывод

Я приобрёл практические навыки резервного копирования

#### Лабораторная работа №6

«Реестр операционной системы Windows»

Цель работы

Приобретение практических навыков в использовании функций реестра операционных систем семейства Windows.

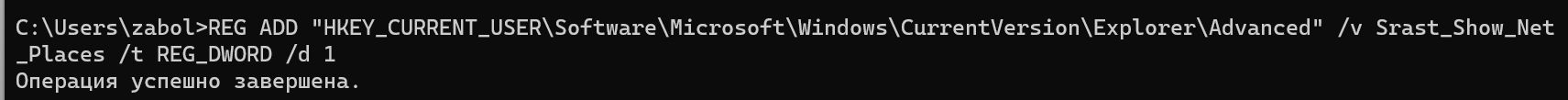
# Задание

Сделать резервную копию ветвей реестра, изменяемых в следующих пунктах задания. (Рис. 6.1)

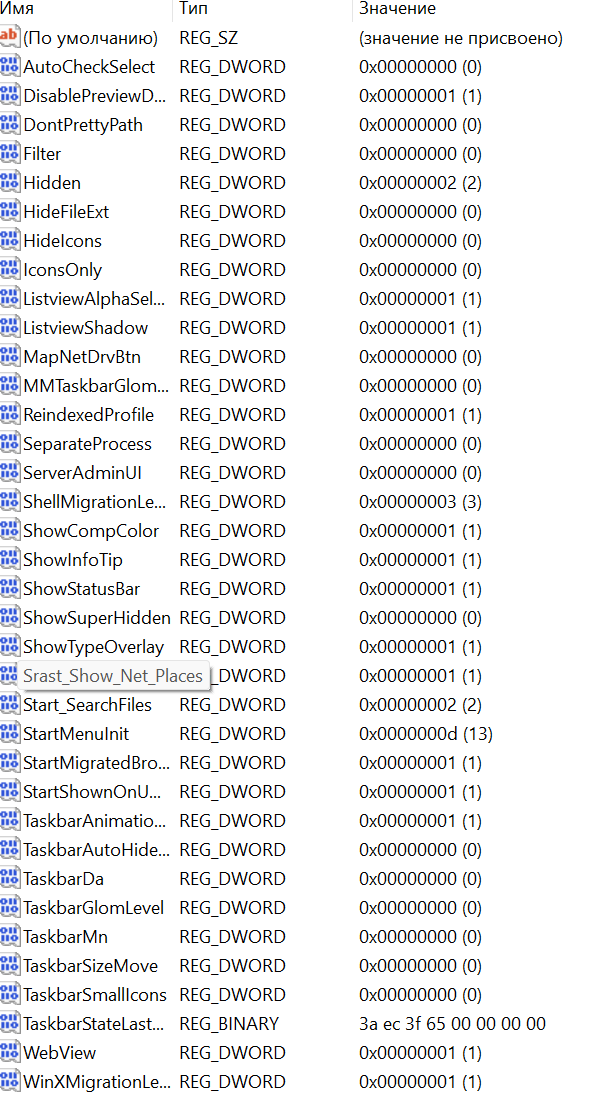
#### 

#### Рисунок 6.1

C помощью утилиты regedit внести информацию в ветвь реестра Windows HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced. (Рис. 6.2, 6.3)



#### Рисунок 6.2



#### Рисунок 6.3

Далее необходимо внести информацию в реестр с помощью reg-файла в соответствии с вариантом задания (Рис. 6.4)

#### 

#### Рисунок 6.4

Далее необходимо восстановить исходные значения ключей реестра, используя при необходимости резервные копии, созданные в п. 1) и убедиться, что все параметры имеют прежние значения.

# Вывод:

Я приобрёл практические навыки в использовании функций реестра операционных систем семейства Windows.

#### Лабораторная работа №7

«Средства защиты компьютера от вирусов. Работа с антивирусными пакетами»

Цель работы

Ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидностями вирусов, способами заражения и методы борьбы. Ознакомиться с различными видами программных средств защиты от вирусов. Проверка настроек антивирусов, сканирование файлов, папок и дисков, обновления антивирусной базы. Получить навыки работы с антивирусным пакетом Антивирус Касперского.

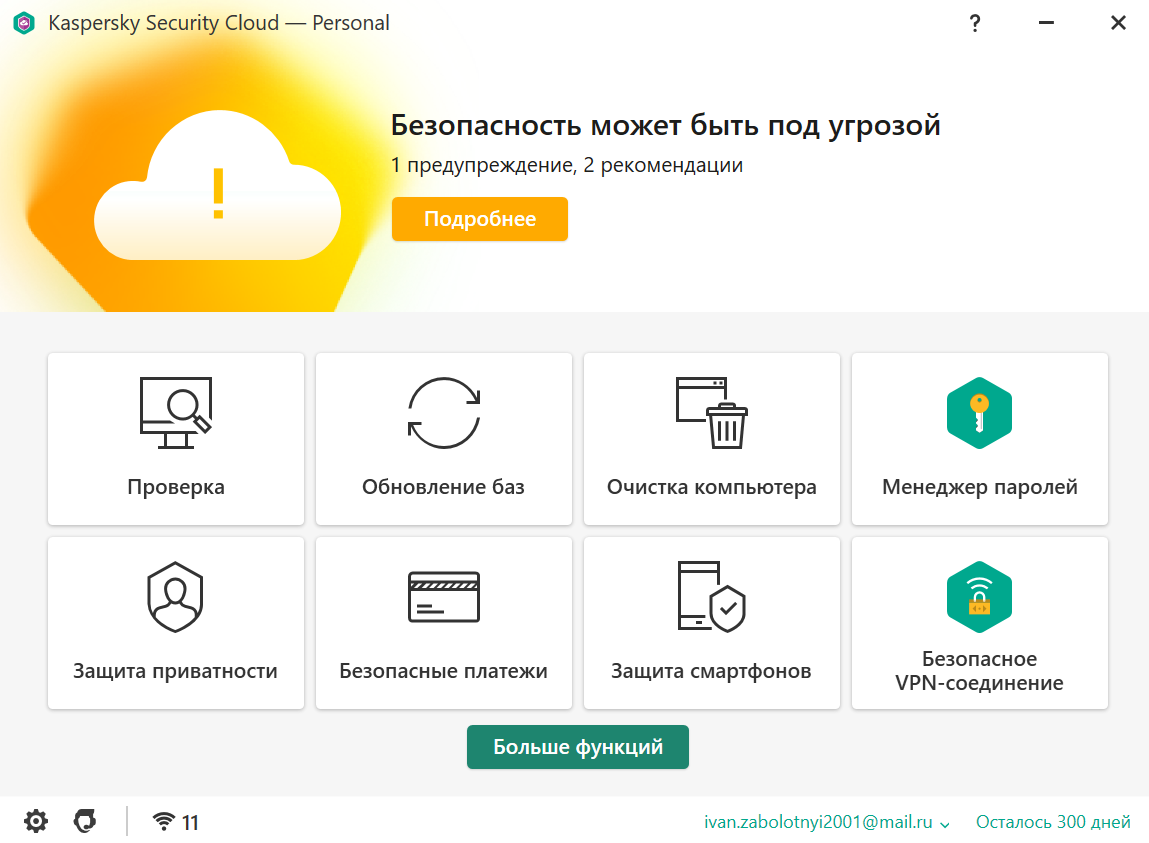
# Задание

Первое задание заключается в том, чтобы сделать инфографику на сайте Visme.co на тему: «Antivirus AVG» (Рис. 7.1)

#### 

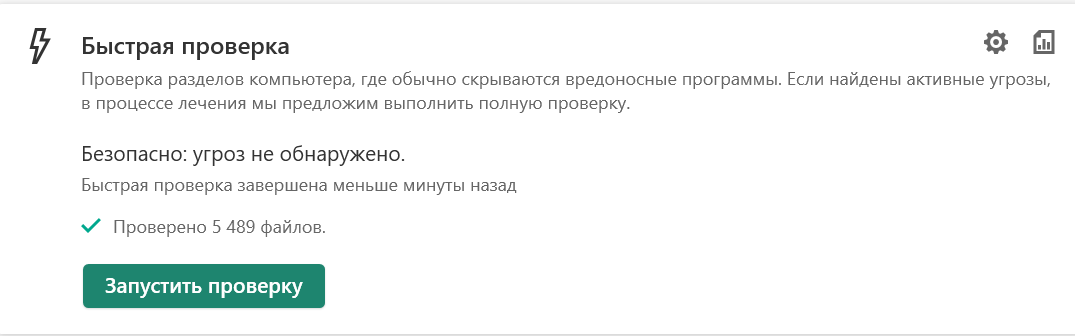
#### Рисунок 7.1

Второе задание заключается в том, чтобы изучить пакет Антивирус Касперского. (Рис. 7.2)



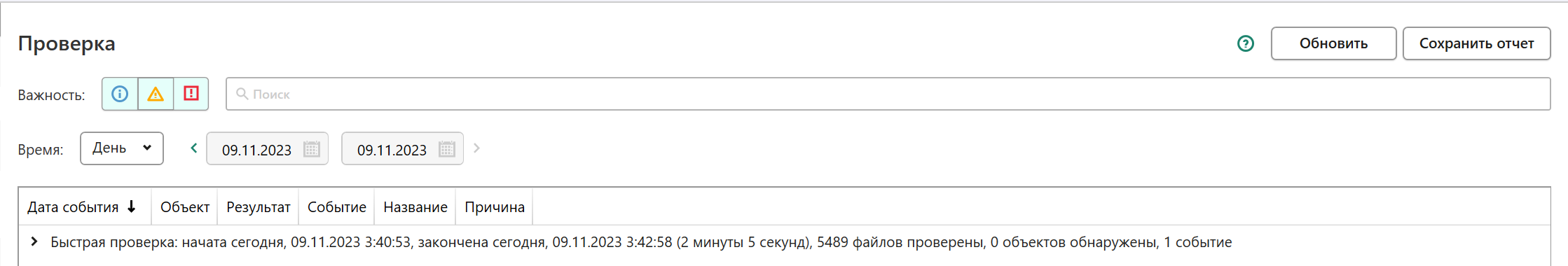
#### Рисунок 7.2

1. Сканирование папок на наличие вирусов. Для этого зайдем в программу и нажмем пункт Проверка. После нажимаем запустить проверку. Отчёт по быстрой проверке предоставлен на рисунке 7.3.



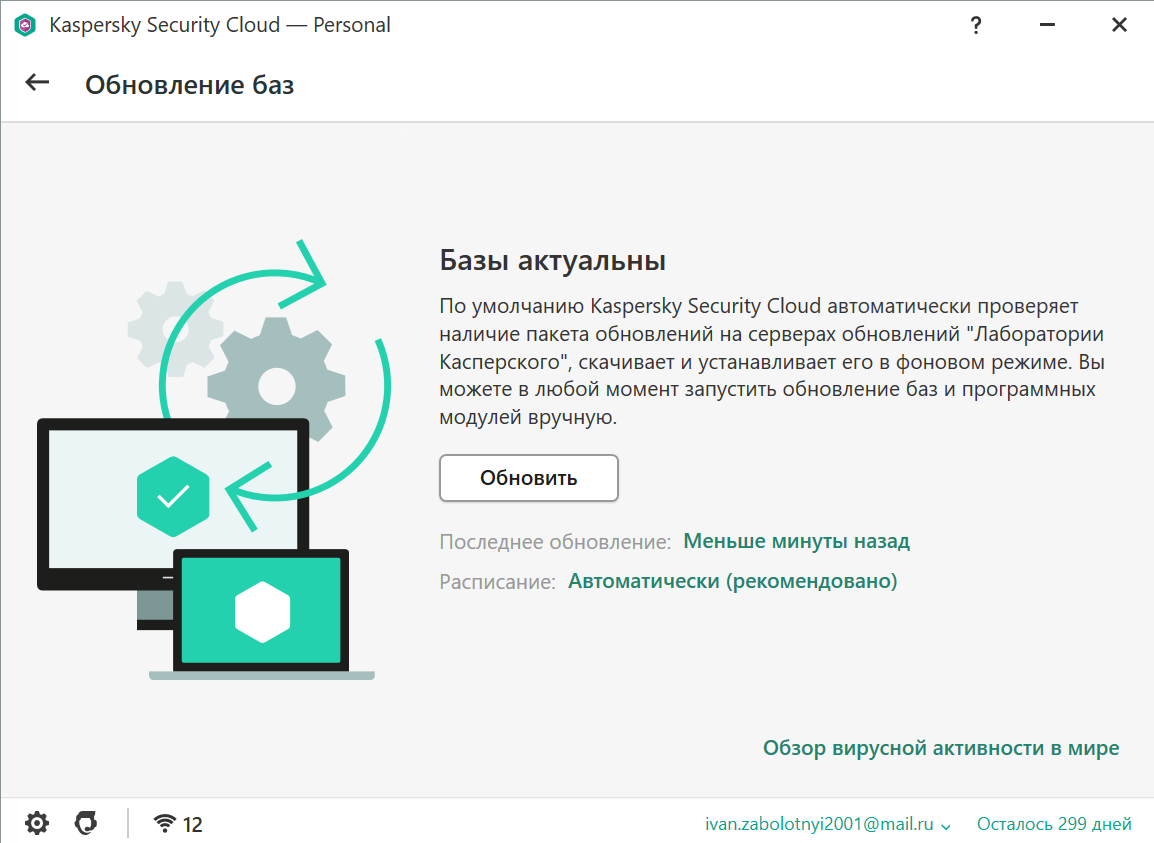
#### Рисунок 7.3

По необходимости отчёт можно сохранить. (Рис. 7.4)



#### Рисунок 7.4

1. Обновление антивирусной базы. Выбираем пункт обновление баз (Рис. 7.5)



#### Рисунок 7.5

Далее в третьем задании необходимо изучить пакет Антивирус Avast.

Avast — это один из крупнейших и наиболее известных производителей антивирусного программного обеспечения. Компания Avast Software разрабатывает широкий спектр продуктов для защиты устройств от вредоносных программ, включая антивирусы для компьютеров, мобильных устройств и других устройств IoT.

Основные характеристики и возможности продуктов Avast могут включать:

Защита от вирусов и вредоносных программ: Avast предлагает сканирование в реальном времени и регулярные обновления своих баз данных для обнаружения и удаления вирусов, троянов, шпионского ПО и других угроз.

Защита в режиме реального времени: Программы Avast работают в фоновом режиме, предотвращая заражение устройства до того, как вредоносное программное обеспечение сможет причинить вред.

Защита от фишинговых атак: Некоторые версии Avast обладают функциями защиты от фишинга, блокируя доступ к веб-сайтам, известным как источники мошенничества.

Брандмауэр и дополнительные функции защиты: Некоторые версии Avast также включают функции, такие как брандмауэр, защита от спама, защита в реальном времени от уязвимостей ПО и другие.

Удобство использования: Продукты Avast обычно имеют интуитивно понятный пользовательский интерфейс и обширные настройки, что делает их доступными для широкого круга пользователей.

Надо отметить, что выбор антивирусного программного обеспечения зависит от индивидуальных потребностей, типа операционной системы, личных предпочтений и других факторов. Avast - один из многих продуктов на рынке антивирусного ПО, и его эффективность может изменяться со временем в зависимости от обновлений и развития угроз

И в последнем четвёртом задании необходимо изучить пакет Антивирус Dr. Web. Доктор Веб (Dr.Web) — это известное российское антивирусное программное обеспечение, разработанное компанией Doctor Web. Dr.Web предназначен для обнаружения и удаления вредоносных программ, таких как вирусы, трояны, черви, шпионские программы и другие угрозы для компьютерной безопасности.

Некоторые ключевые особенности и характеристики Dr.Web включают:

Многоплатформенность: Dr.Web доступен для различных операционных систем, включая Windows, macOS, Linux, а также для мобильных устройств под управлением Android и iOS.

Высокая скорость сканирования: Dr.Web обещает быстрое и эффективное сканирование файлов и системы на наличие вредоносных программ.

Поддежка облачных технологий: Dr.Web обновляется регулярно с использованием облачных баз данных, что позволяет быстро реагировать на новые угрозы.

Функции родительского контроля: Dr.Web предоставляет средства для контроля и фильтрации контента.

Поиск и лечение инфицированных файлов: Программа позволяет обнаруживать и лечить файлы, зараженные вредоносными программами, в некоторых случаях даже восстанавливая поврежденные файлы.

Фаервол и другие дополнительные функции: В Dr.Web также включены дополнительные инструменты, такие как фаервол и защита от спама.

Важно отметить, что эффективность и популярность антивирусных программ может меняться со временем, рекомендуется провести исследование и ознакомиться с отзывами, чтобы определить, насколько это соответствует вашим потребностям в области компьютерной безопасности.

# Вывод

Я ознакомился с различными видами программных средств защиты от вирусов, а также приобрел практические навыки работы с антивирусным пакетом Антивирус Касперского.

#### Лабораторная работа №8

«Защита от разрушающих программных воздействий. Использование антивирусных средств»

Цель работы

Изучение принципов работы антивирусных средств и их использования для зашиты от вредоносных программных воздействий. Работа выполняется с помощью программы «Антивирус Касперского.

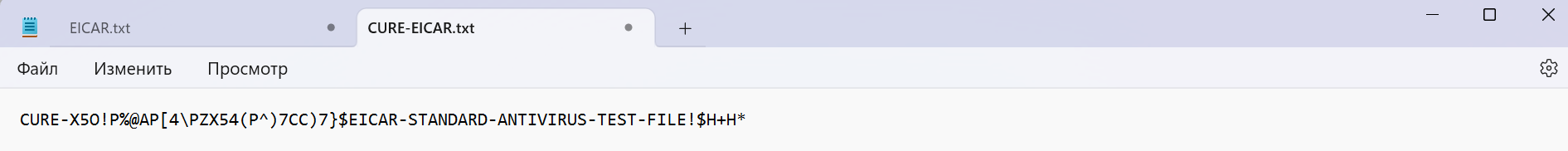
# Задание

Первое задание заключается в том, чтобы создать вирус EICAR и сохранить его в расширении .txt (Рис. 8.1)

#### 

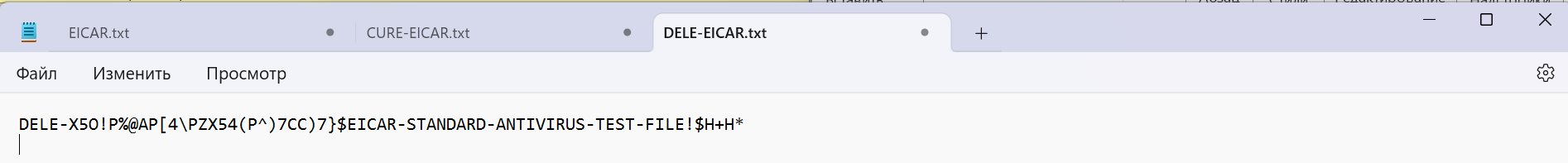
#### Рисунок 8.1

Второе – создать вирус CURE-EICAR и сохранить его в расширении .txt (Рис. 8.2)



#### Рисунок 8.2

Третье – создать вирус DELE-EICAR и сохранить его в расширении .txt (Рис. 8.3)



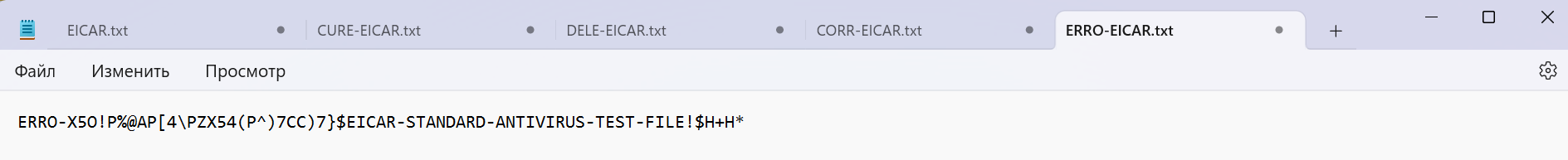
#### Рисунок 8.3

Четвёртое задание заключается в том, чтобы создать вирус CORR-EICAR и сохранить его в расширении .txt (Рис. 8.4)



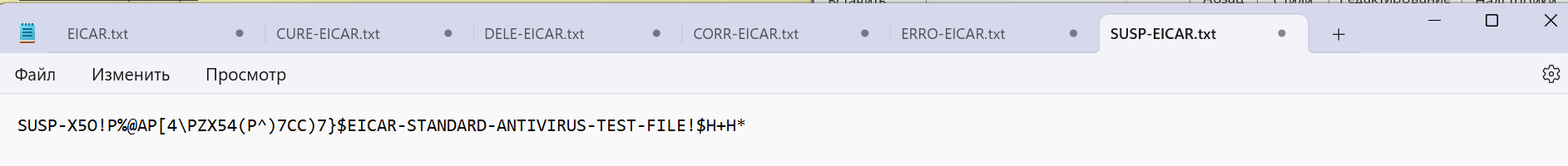
#### Рисунок 8.4

Пятое задание заключается в том, чтобы создать вирус ERRO-EICAR и сохранить его в расширении .txt (Рис. 8.5)



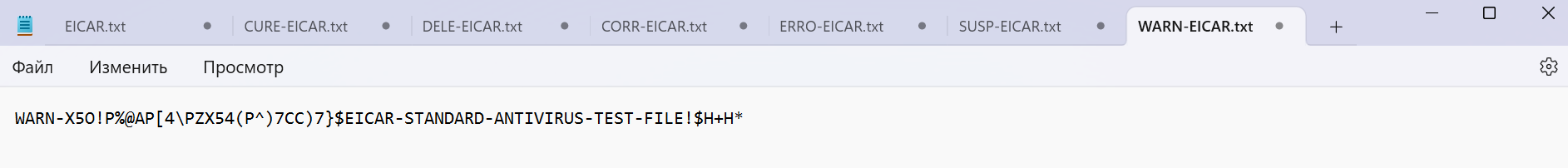
#### Рисунок 8.5

Шестое задание заключается в том, чтобы создать вирус SUSP-EICAR и сохранить его в расширении .txt (Рис. 8.6)



#### Рисунок 8.6

Седьмое задание заключается в том, чтобы создать вирус WARN-EICAR и сохранить его в расширении .txt (Рис. 8.7)

Рисунок 8.7

Далее посмотрим на то, как антивирус Касперского отреагирует на эти файлы. (Рис. 8.8, Рис. 8.9)

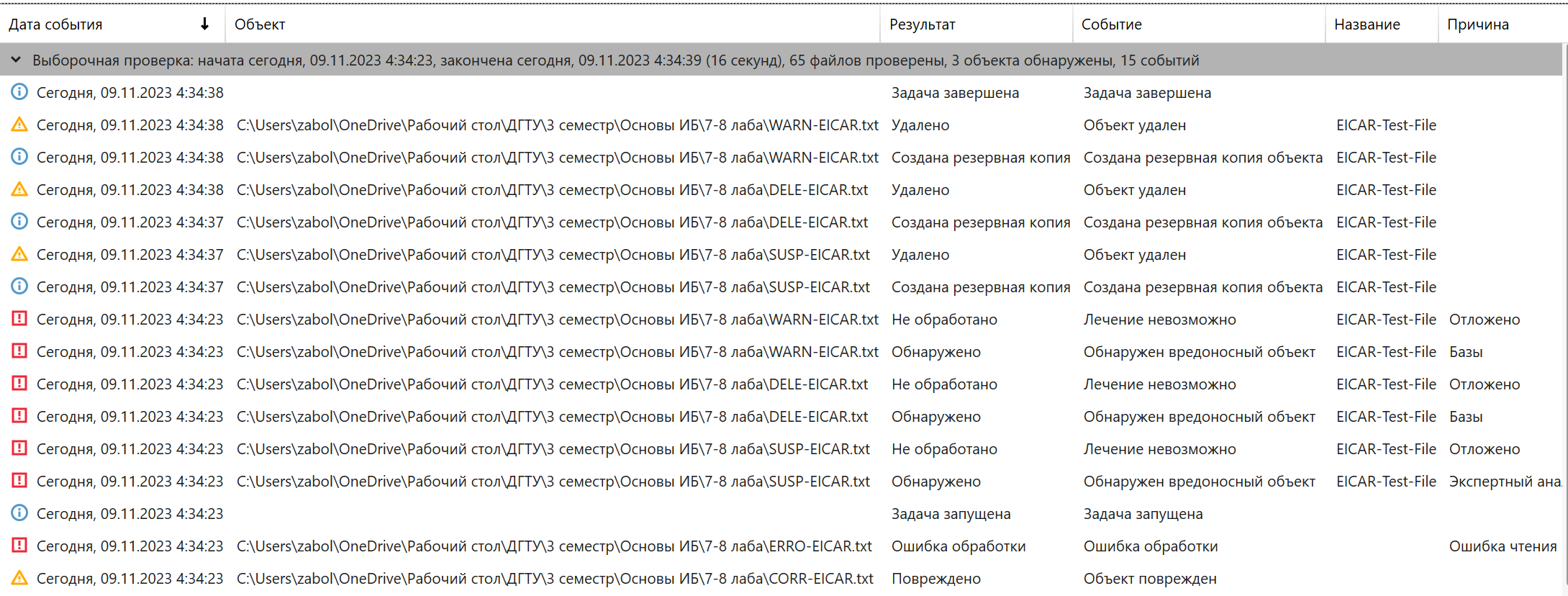
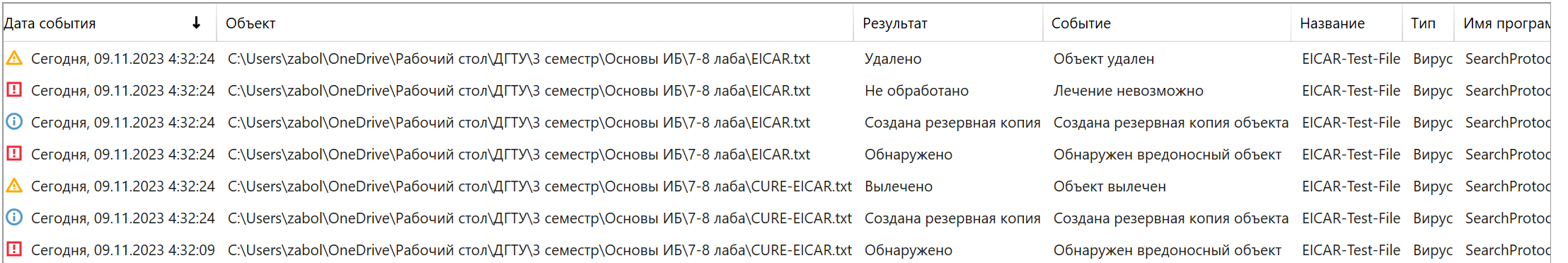


Рисунок 8.8

Рисунок 8.9

# Вывод

Я изучил принципы работы антивирусных средств и их использования для зашиты от вредоносных программных воздействий, а также приобрёл практические навыки в программе «Антивирус Касперского.

#### Лабораторная работа №9

«Стандарты информационной безопасности»

Цель работы

Изучить стандарты информационной безопасности

# Задание

Первое задание: «Используя ГОСТ Р ИСО/МЭК 27002-2012, решить ситуационную задачу. Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек). Вам необходимо разработать комплекс мероприятий (от 10 до 20) по следующему направлению: привлечение сторонних организаций к обработке информации. Цель: обеспечение информационной безопасности при передаче ответственности за обработку информации другой организации. Изучить разделы ГОСТ Р ИСО/МЭК 27002-2012.».

1. Идентификация информации:
2. Определите какие конкретные данные и информацию необходимо передавать сторонним организациям;
3. Оцените степень конфиденциальности и важности этих данных;
4. Определите, какие сторонние организации будут вовлечены в обработку информации.
5. Риски и оценка рисков:
6. Проведите анализ рисков, связанных с передачей информации сторонним организациям;
7. Оцените уровень угроз и уязвимостей при обработке данных сторонними организациями;
8. Оцените потенциальные последствия инцидентов в области информационной безопасности.
9. Разработка политики и процедур:
   1. Разработайте политику и процедуры, которые определяют условия передачи данных сторонним организациям;
   2. Включите в политику меры по обеспечению конфиденциальности, целостности и доступности данных.
10. Соглашения и контракты:
    1. Разработайте соглашения и контракты, которые определяют права и обязанности в области информационной безопасности для сторонних организаций;
    2. Включите в контракты меры по мониторингу и аудиту информационной безопасности сторонних организаций.
11. Обучение и осведомление:
    1. Обучите сотрудников вашей организации о правилах и процедурах взаимодействия с сторонними организациями в рамках информационной безопасности;
    2. Обеспечьте осведомленность сотрудников о рисках и мероприятиях в области информационной безопасности.
12. Инциденты информационной безопасности:
    1. Разработайте процедуры управления инцидентами в области информационной безопасности для реагирования на возможные инциденты с данными, передаваемыми сторонними организациями.
13. Оценка эффективности:
    1. Периодически оценивайте эффективность мероприятий и корректируйте их в соответствии с изменениями рисков и требований.
14. Документация и обучение:
    1. Внимательно документируйте все мероприятия и соглашения в области информационной безопасности.

Второе здание: «Используя основные положения части 4, главы 70 Гражданского кодекса РФ, решить ситуационную задачу. Гражданин Смирнов А.В. создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием «Albert 3D» и зарегистрировал на него свои права. 15.09.2019 этот гражданин заключил договор с компанией «MosTechnology» и передал свои имущественные права на распространение своего программного продукта сроком на один год. После заключения договора компания «MosTechnology» распространила версию программы «Albert 3D» с предварительной модификацией данного программного продукта без ведома автора. Вопрос: имеет ли место в данной ситуации нарушение авторского права гражданина Смирнова? Ответ: согласно статьи №….».

В данной ситуации имеет место нарушение авторского права гражданина Смирнова согласно статье 1229 части 4 Гражданского кодекса Российской Федерации.

Статья 1229 ГК РФ устанавливает, что автор имеет право на охрану своего произведения. Авторские права включают в себя право на создание производных произведений. В данной ситуации гражданин Смирнов передал компании "MosTechnology" имущественные права на распространение программного продукта "Albert 3D", но это не означает, что компания имеет право модифицировать программу без согласия автора.

Поэтому, если "MosTechnology" внесла предварительные модификации в программу "Albert 3D" без согласия автора, то это нарушение авторских прав гражданина Смирнова.

Третье задание: «Используя статьи УК РФ, ответьте на вопросы после ознакомления с ситуацией. Ситуация: А.Н. Иванов, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (расширение .exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 780000 рублей. Вопросы: − Какая статья УК РФ была нарушена? − Что послужило предметом преступления? − Какие неправомерные информационные действия были совершены А.Н. Ивановым?».

1. А.Н. Иванов нарушил статью 273 Уголовного кодекса РФ, которая относится к компьютерной мошенничеству. Конкретно, это может быть часть 3 данной статьи.
2. Предметом преступления была компьютерная банковская система и внедренный вирус, который уничтожил исполняемые файлы (.exe), принадлежащие банку.
3. А.Н. Иванов совершил следующие неправомерные (информационные) действия:
4. Внедрение вредоносного вируса в компьютерную систему банка.
5. Уничтожение исполняемых файлов банковских программных приложений, что привело к материальному ущербу для банка.
6. Совершение данных действий без согласия и разрешения компетентных органов и вопреки интересам банка, что является неправомерным доступом к информационным ресурсам.

Четвёртое задание: «Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек). Вам необходимо разработать требования к хранению, использованию и утилизации информации для вашей организации. Цель: обеспечение информационной безопасности при хранении, обработке, передаче и уничтожении информации.»

Основные требования, которые могут быть полезны:

1. Классификацияинформации:
   1. Определение категорий информации по степени конфиденциальности (например, общедоступная, внутренняя, конфиденциальная, секретная);
   2. Установление правил для маркировки и классификации информации.
2. Доступ к информации:
   1. Управление доступом к информации на принципе "необходимости знания";
   2. Установление процедур аутентификации и авторизации для доступа к информации;
   3. Ограничение физического доступа к информационным ресурсам.
3. Хранение информации:
   1. Определение мест хранения информации, включая серверы, файловые хранилища, бумажные документы и т.д.;
   2. Установление мер безопасности для защиты хранимой информации, включая шифрование данных, резервное копирование и физическую защиту серверов.
4. Обработка информации:
   1. Установление правил и процедур обработки информации, включая соблюдение принципов целостности и конфиденциальности;
   2. Обучение сотрудников по правилам обработки информации.
5. Передача информации:
   1. Определение процедур для безопасной передачи информации, включая защищенную передачу по сети и использование шифрования;
   2. Установление правил для обмена информацией с внешними сторонами (партнерами, клиентами) и контроль передачи конфиденциальных данных.
6. Уничтожение информации:
   1. Определение процедур и сроков уничтожения информации, включая физическое уничтожение бумажных документов и безвозвратное удаление электронных данных;
   2. Поддержание журналов уничтожения для отслеживания процесса.
7. Мониторинг и аудит:
   1. Установление системы мониторинга и аудита для отслеживания действий пользователей и обнаружения инцидентов в области информационной безопасности;
   2. Регулярная проверка соответствия политик и требований.
8. Обучение и осведомленность:
   1. Обучение сотрудников в области информационной безопасности и их осведомленность о правилах и процедурах;
   2. Регулярное информирование сотрудников о новых угрозах и мероприятиях по обеспечению информационной безопасности.
9. Инциденты информационной безопасности:
   1. Разработка процедур управления инцидентами и реагирования на нарушения информационной безопасности.
10. Соблюдение законодательства:
    1. Обязательное соблюдение всех применимых законов и нормативных актов, связанных с информационной безопасностью.

Пятое задание: «Проработайте требования для специалистов по подбору кадров вашей организации с целью внесения пунктов об информационной безопасности в трудовой договор новых сотрудников. Цель: уведомление новых сотрудников о строгом выполнении требований по обеспечению информационной безопасности и ответственности за их нарушение.»

Несколько ключевых требований для специалистов по подбору кадров:

1. Понимание информационной безопасности: специалисты по подбору кадров должны иметь глубокое понимание информационной безопасности и знать ее важность для организации.
2. Знание политики информационной безопасности: они должны быть хорошо знакомы с существующей политикой информационной безопасности в организации, включая стандарты и процедуры.
3. Согласование требований: специалисты по подбору кадров должны работать в тесном сотрудничестве с отделом информационной безопасности, чтобы гарантировать, что требования по информационной безопасности согласованы с политикой организации.
4. Интеграция в процесс подбора: они должны внедрить требования по информационной безопасности в процесс подбора кадров, включая вопросы об информационной безопасности в собеседованиях и анкетах для кандидатов.
5. Информирование и обучение кандидатов: специалисты по подбору кадров должны уведомлять кандидатов о важности информационной безопасности и обязанностях в этой области. Это может включать в себя проведение информационных сессий или предоставление руководств по информационной безопасности.
6. Внесение в трудовой договор: они должны внести соответствующие пункты о информационной безопасности в трудовой договор новых сотрудников, включая ответственность за соблюдение политики информационной безопасности.
7. Мониторинг и соблюдение: специалисты по подбору кадров должны следить за соблюдением требований информационной безопасности и обязательств новых сотрудников в этой области.
8. Обратная связь и улучшение: они должны поддерживать обратную связь с отделом информационной безопасности и участвовать в улучшении процессов подбора кадров с учетом информационной безопасности.

# Вывод

Я изучил стандарты информационной безопасности, а также требования при хранении, обработке, передаче и уничтожении информации.

#### Лабораторные работы №10,11

«Асимметричная криптография и электронная цифровая подпись на

примере системы GnuPG»

Цель работы

Ознакомиться с принципами криптографической защиты информации с использованием алгоритмов асимметричного шифрования и электронной цифровой подписи, приобрести навыки практического применения указанных методов защиты информации на основе системы GnuPG.

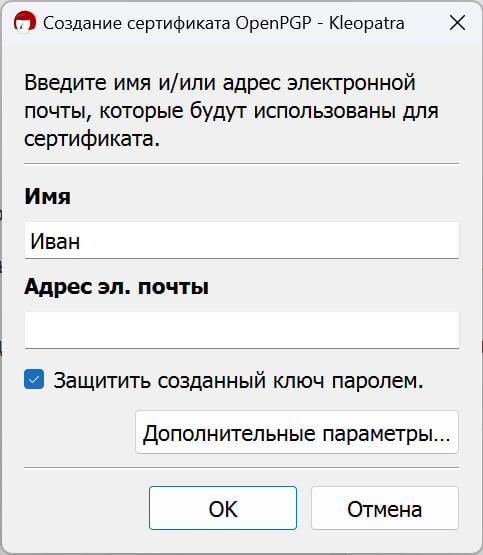
# Задание

Первое задание заключается в том, чтобы создать пару ключей в менеджере ключей Cleopatra. (Рис. 10-11.1)

#### 

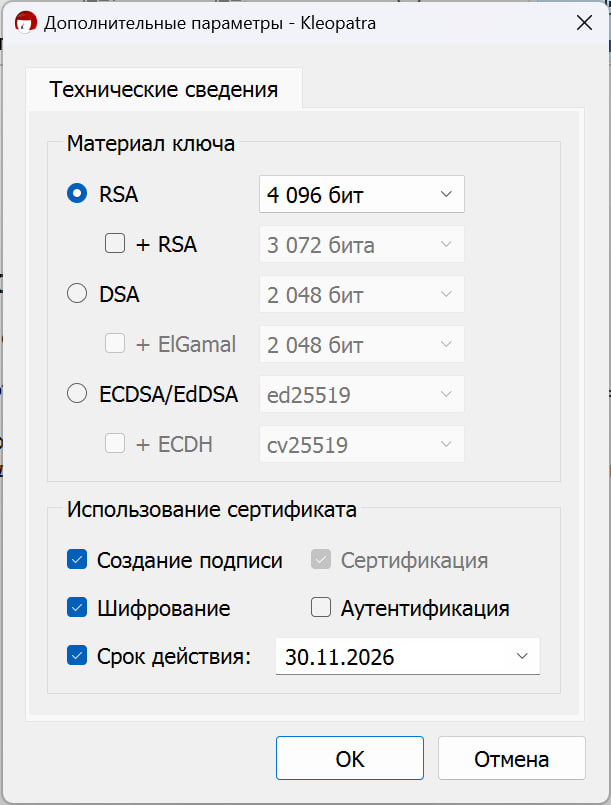
#### Рисунок 10-11.1

Вводим имя, которое будет использовано для сертификата. (Рис. 10-11.2).



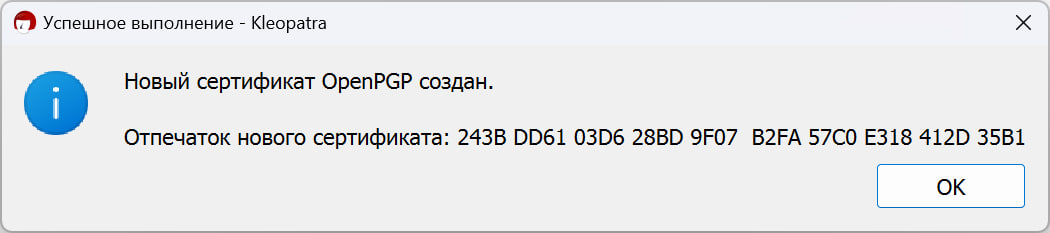
#### Рисунок 10-11.2

Далее выбираем каким криптографическим алгоритмом будет зашифрован текст. (Рис. 10-11.3)



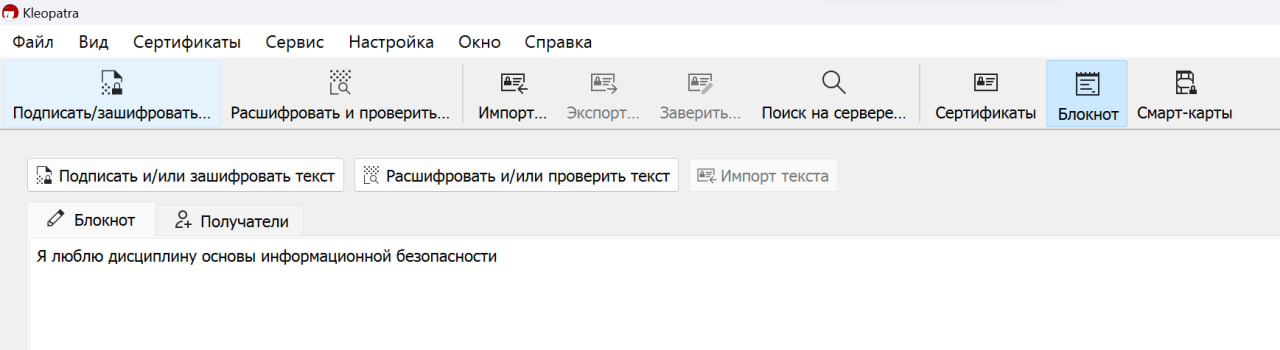
#### Рисунок 10-11.3

Нажимаем кнопку “OK”. Убеждаемся в том, что новый сертификат был создан. (Рис. 10-11.4)



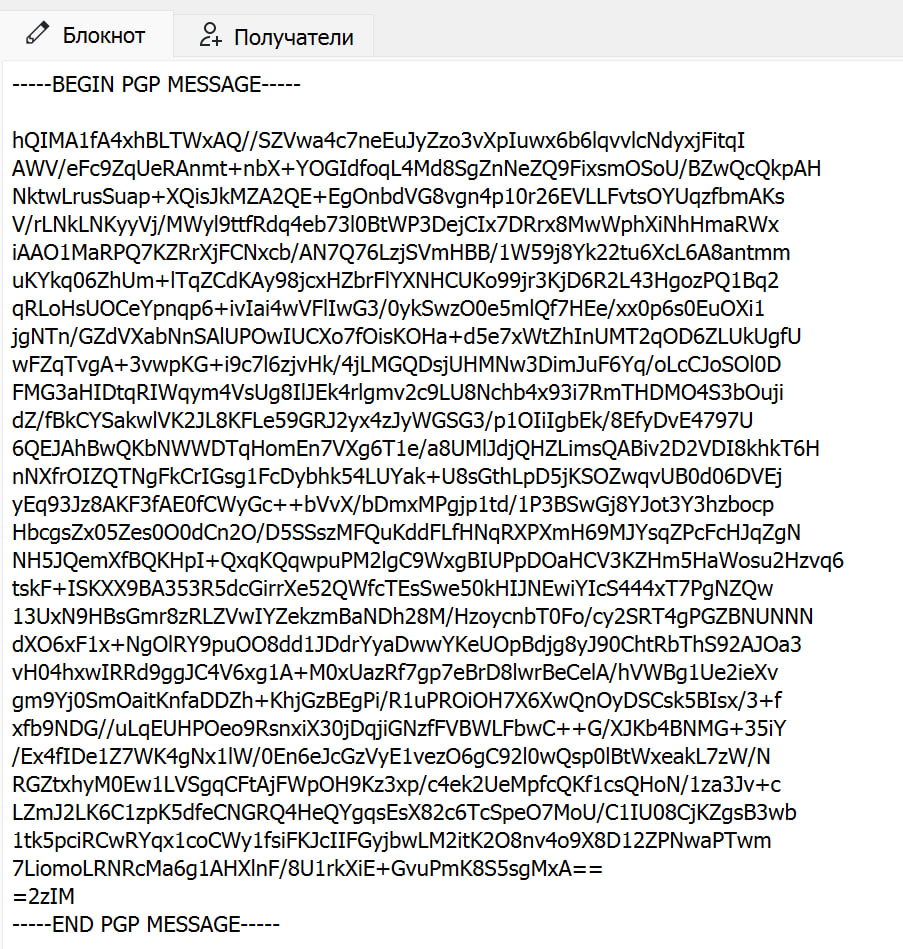
#### Рисунок 10-11.4

Следующее задание заключается в том, чтобы скопировать произвольный текст в буфер обмена. Зашифровать содержимое буфера обмена с помощью своего открытого ключа. Вставить содержимое буфера обмена в текстовый редактор, и убедится, что оно зашифровано. Для начала необходимо ввести в блокнот шифруемый текст и зашифровать (Рис. 10-11.5)



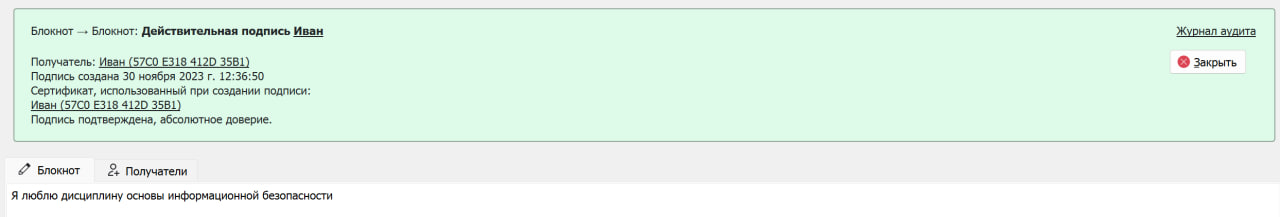
#### Рисунок 10-11.5

Далее необходимо убедиться, что оно зашифровано. (Рис. 10-11.6)



#### Рисунок 10-11.6

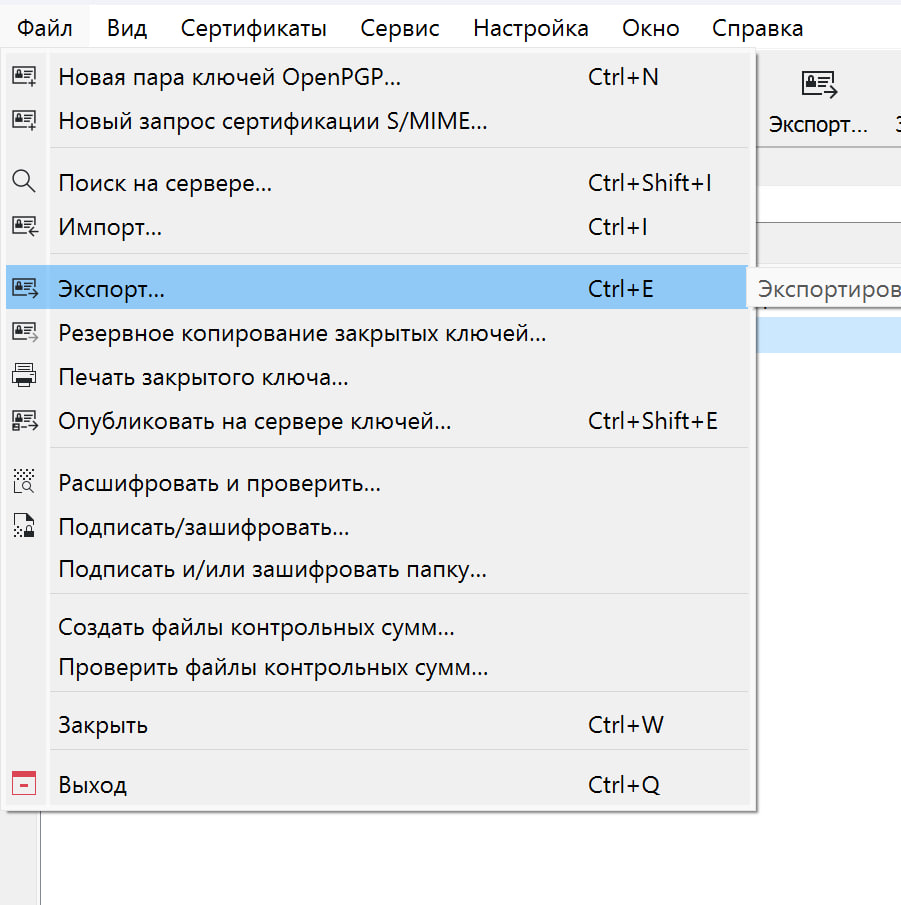
Теперь же нужно скопировать в буфер шифротекст, дешифровать его своим закрытым ключом, вновь вставить содержимое буфера обмена в текстовый редактор, и убедится, что текст был успешно расшифрован. Результат виден на Рис. 10-11.7



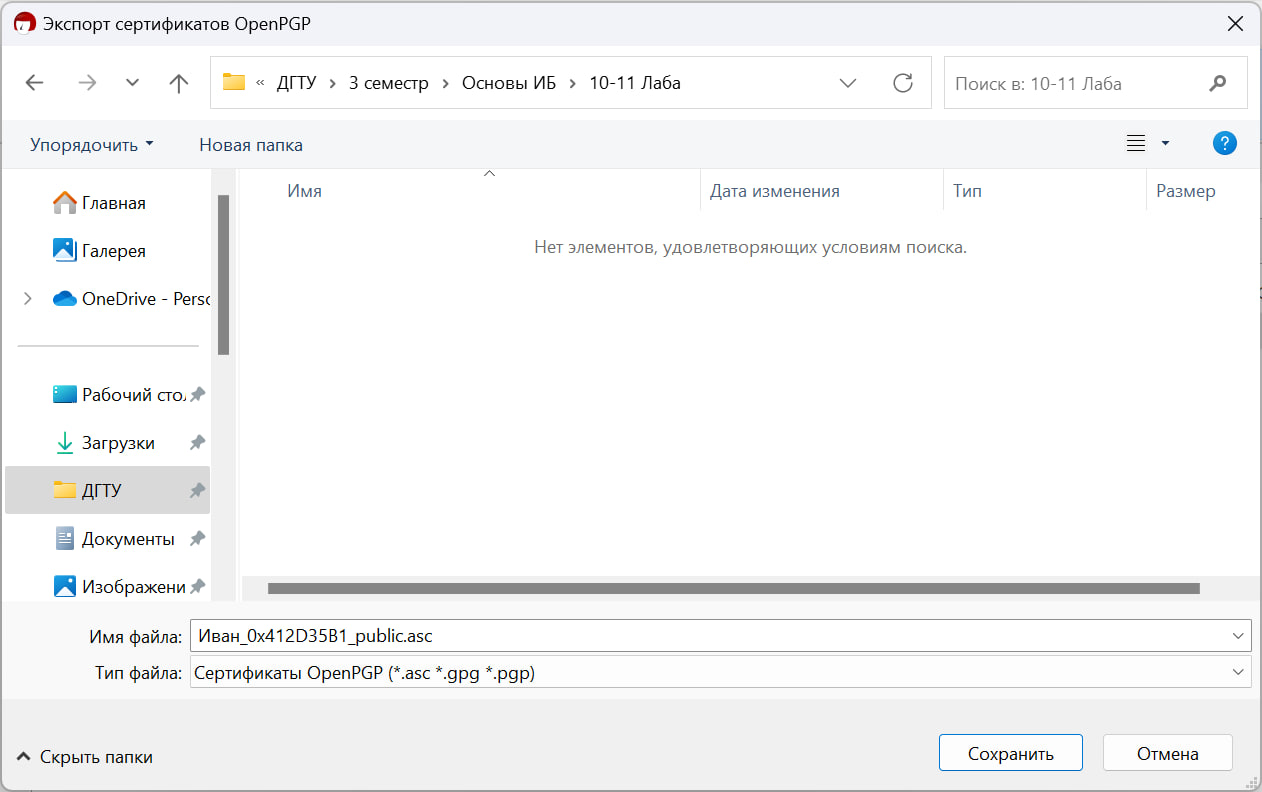
#### Рисунок 10-11.7

Следующее задание состоит в том, чтобы экспортировать сертификат открытого ключа из своей пары ключей в файл и передать его напарнику.

Первым делом надо экспортировать сертификат открытого ключа (Рис. 10-11.8), предварительно сохранив его (Рис. 10-11.9).

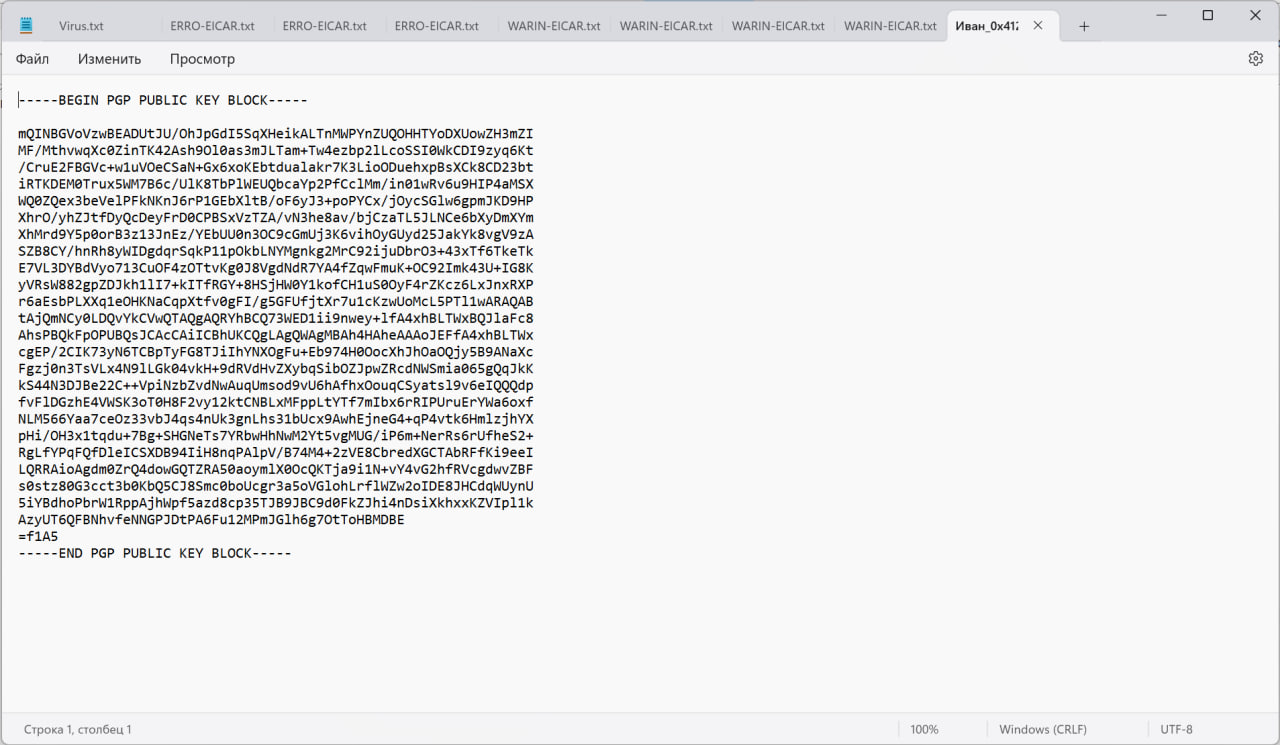


#### Рисунок 10-11.8



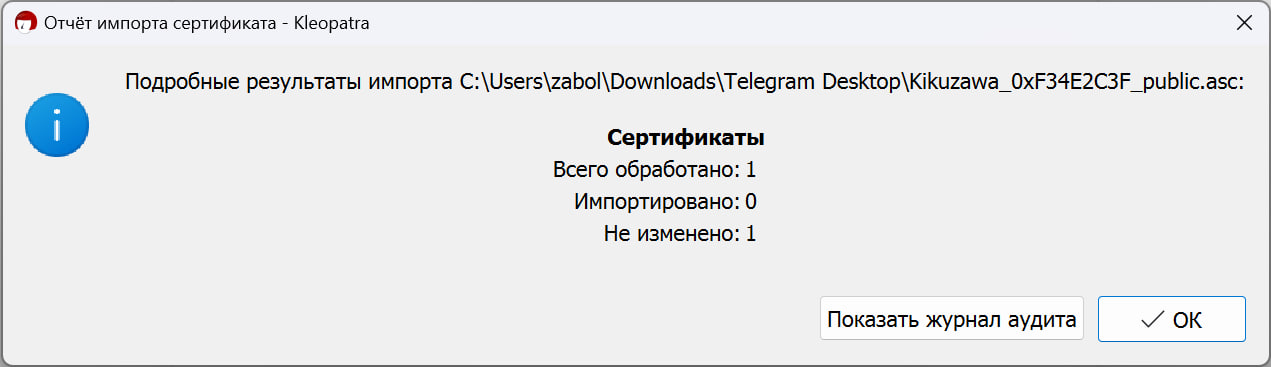
#### Рисунок 10-11.9

Проверяем, что текст зашифрован (Рис. 10-11.10).



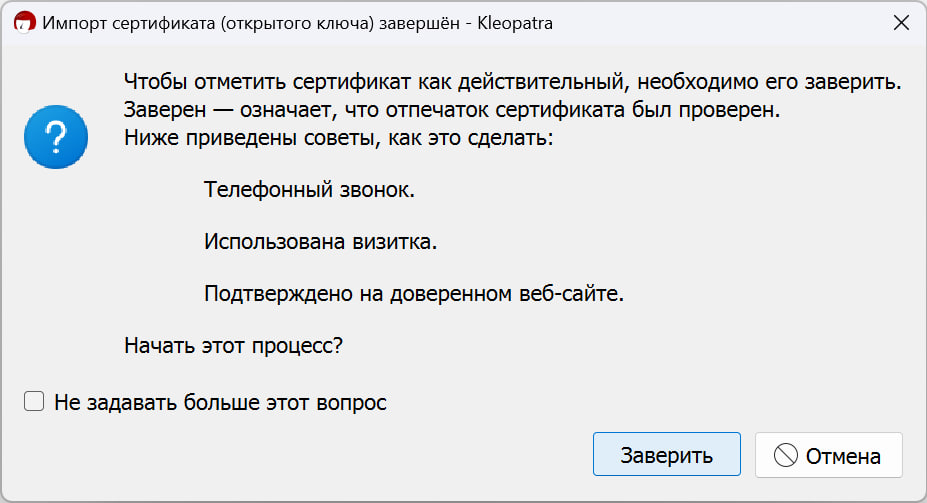
#### Рисунок 10-11.10

Далее, получив файл с экспортированным ключом от напарника, нужно импортировать его в менеджер ключей. Установить для импортированного ключа полное доверие. Поэтому импортируем файл напарника (Рис. 10-11.11)

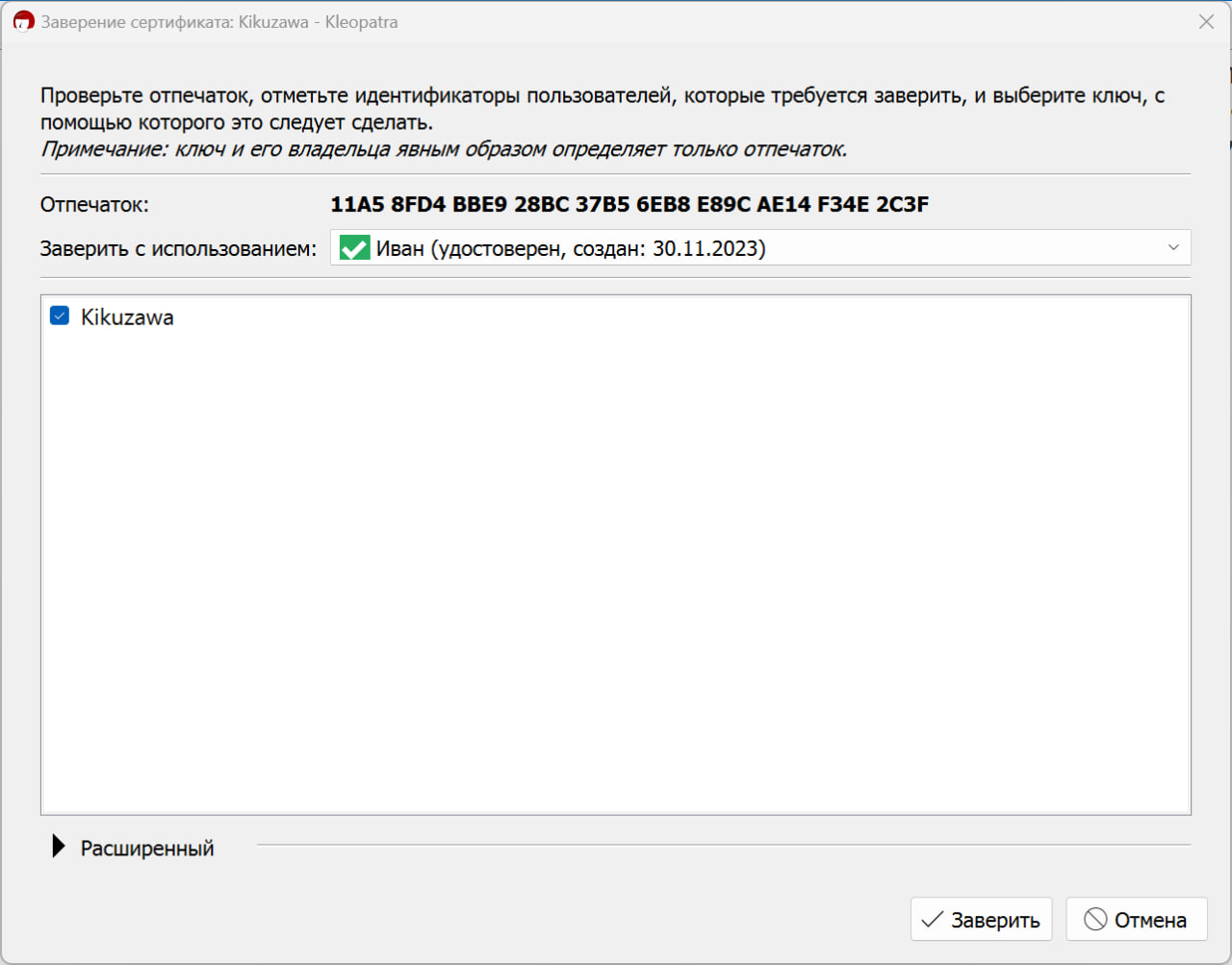


#### Рисунок 10-11.11

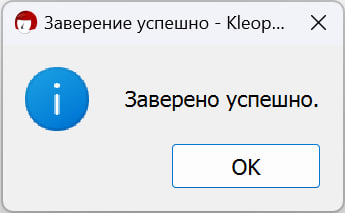
И заверяем полученный сертификат напарника (Рис. 10-11.12-14)



#### Рисунок 10-11.12



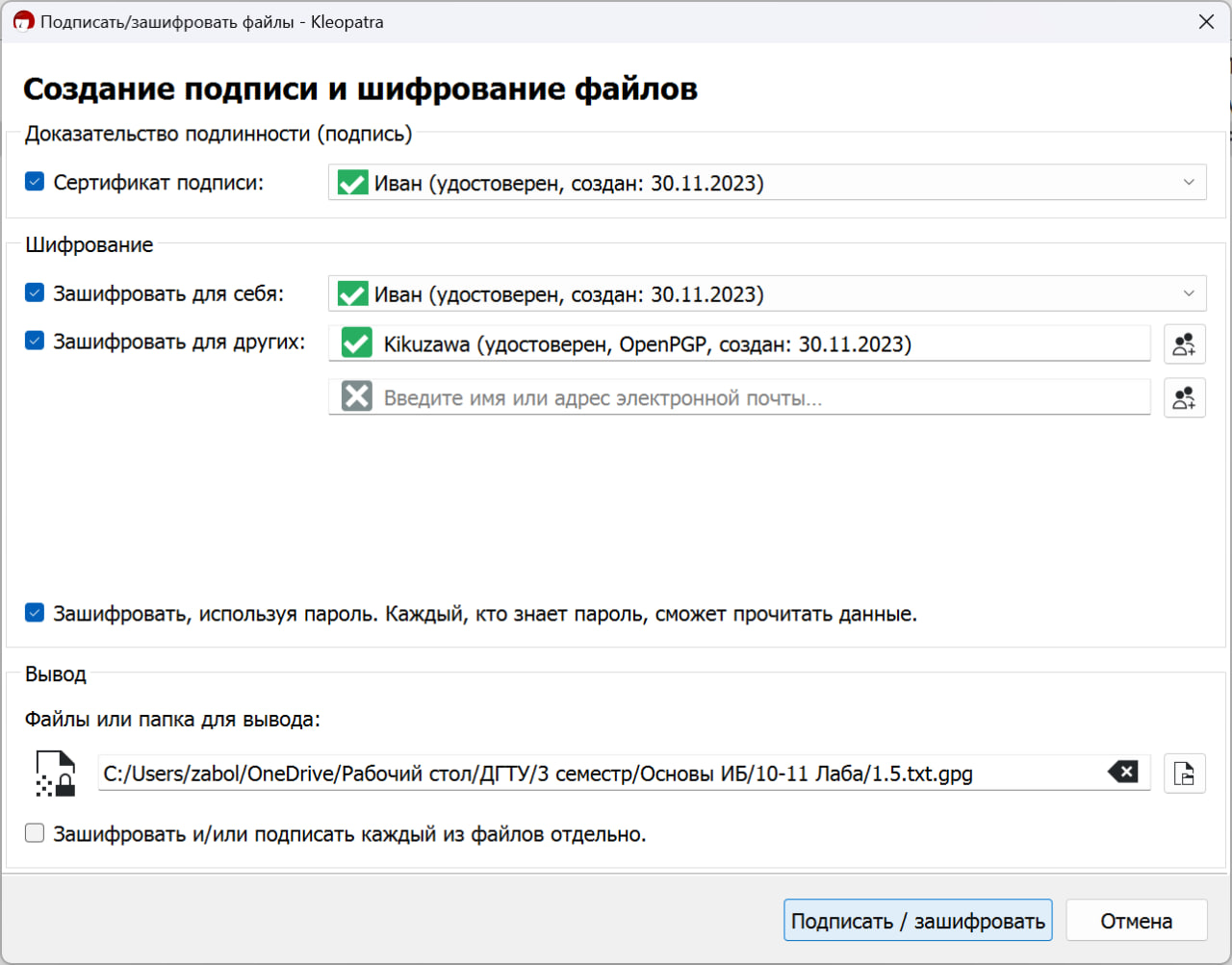
#### Рисунок 10-11.13



#### Рисунок 10-11.14

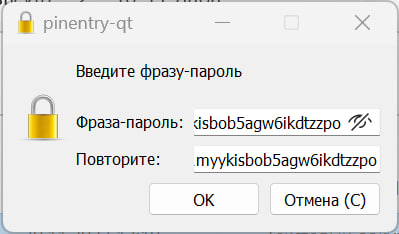
По требованию следующего задания необходимо зашифровать с использованием импортированного ключа напарника произвольный текст на диске. Передать зашифрованный текст напарнику.

Шифруем текст используя импортированный ключ напарника (Рис. 10-11.15).

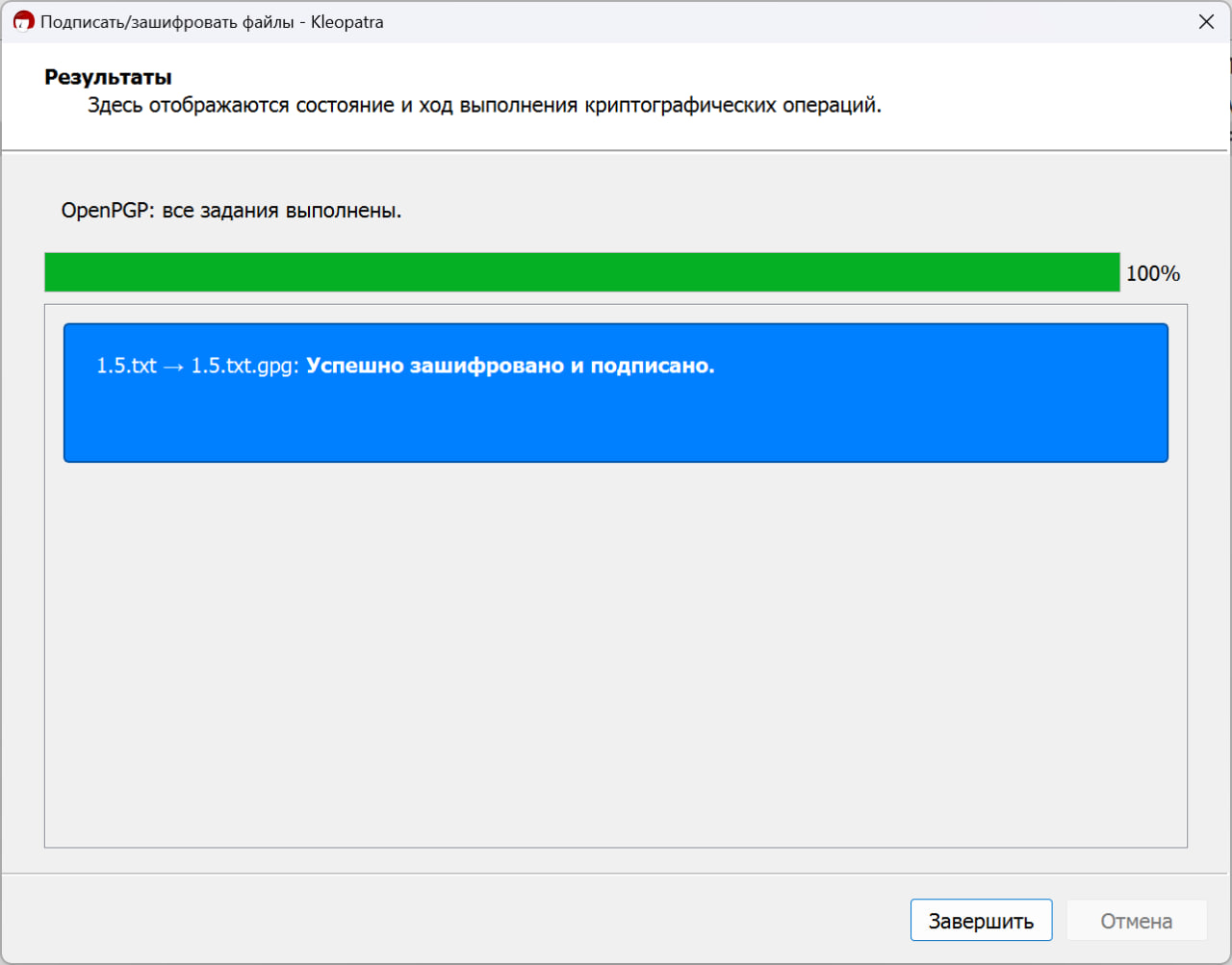


#### Рисунок 10-11.15

Вводим фразу-пароль и ожидаем (Рис. 10-11.16, Рис. 10-11.17)



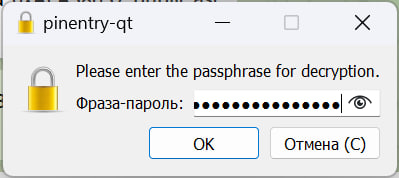
#### Рисунок 10-11.16



#### Рисунок 10-11.17

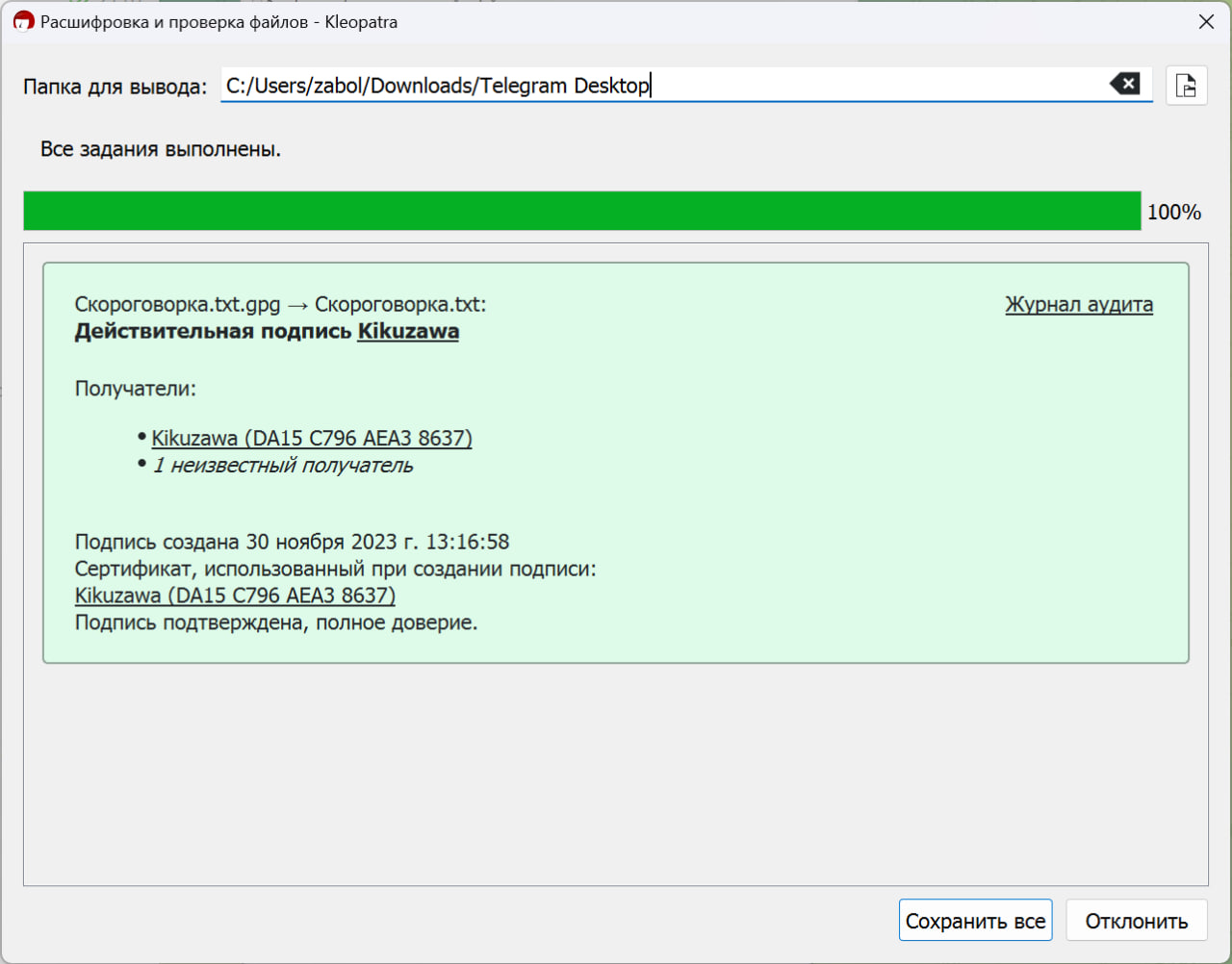
Далее по заданию получив зашифрованный файл от напарника, дешифровать его своим закрытым ключом. Убедится, что файл был успешно дешифрован.

Для этого нужно ввести закрытый ключ для дешифровки (Рис. 10-11.18).



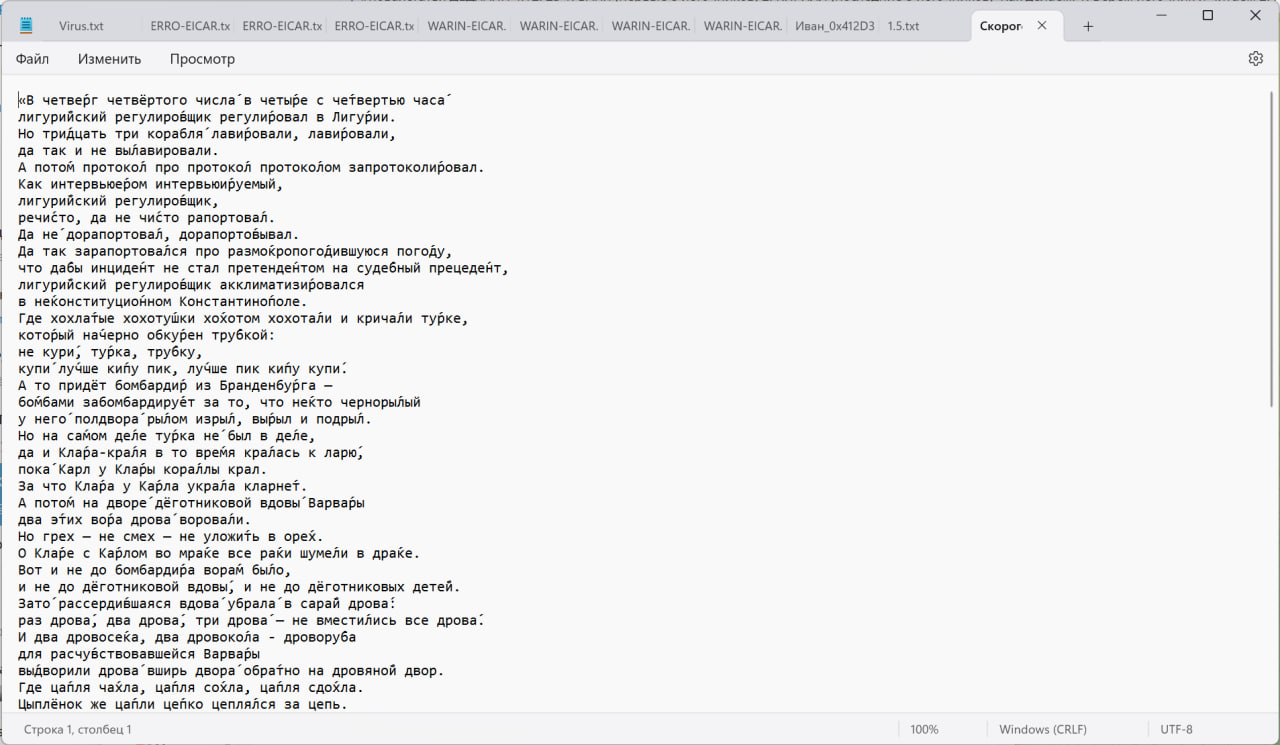
#### Рисунок 10-11.18

Далее необходимо ожидать процесс дешифровки. (Рис. 10-11.19).



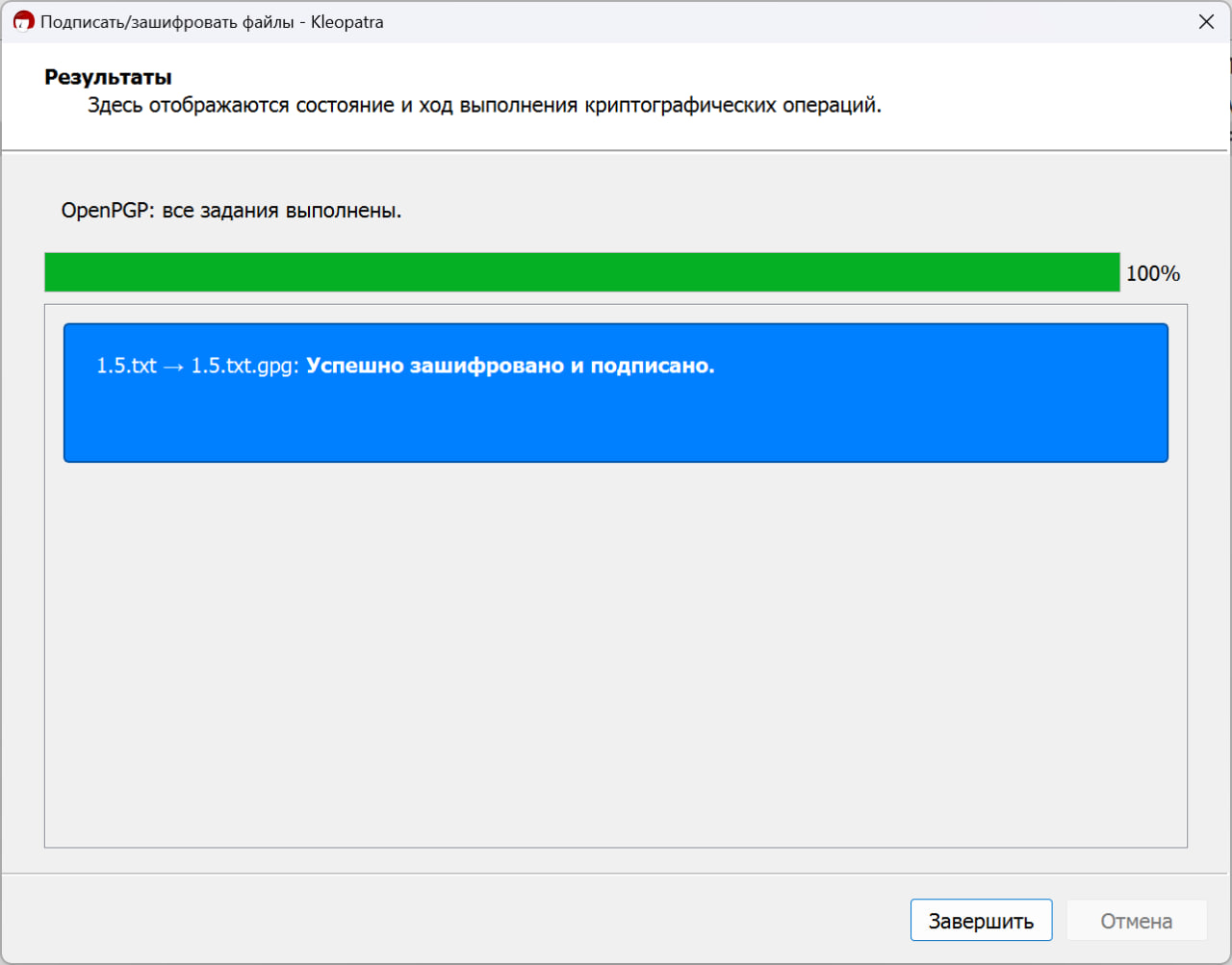
#### Рисунок 10-11.19

Проверим, что текст действительно был дешифрован (Рис. 10-11.20)



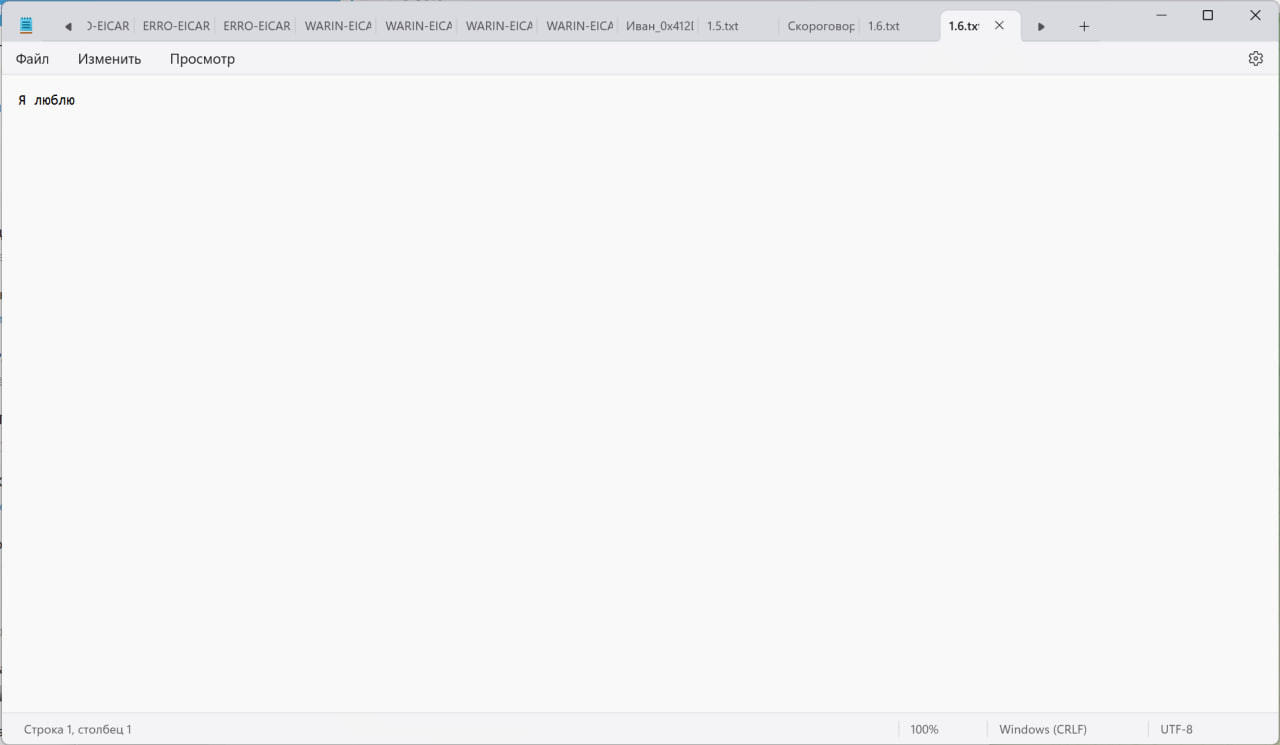
#### Рисунок 10-11.20

В следующем задании нужно, используя свой закрытый ключ, подписать произвольный файл на диске электронной подписью. И передать подписанный документ вместе с подписью напарнику. (Рис. 10-11.21)

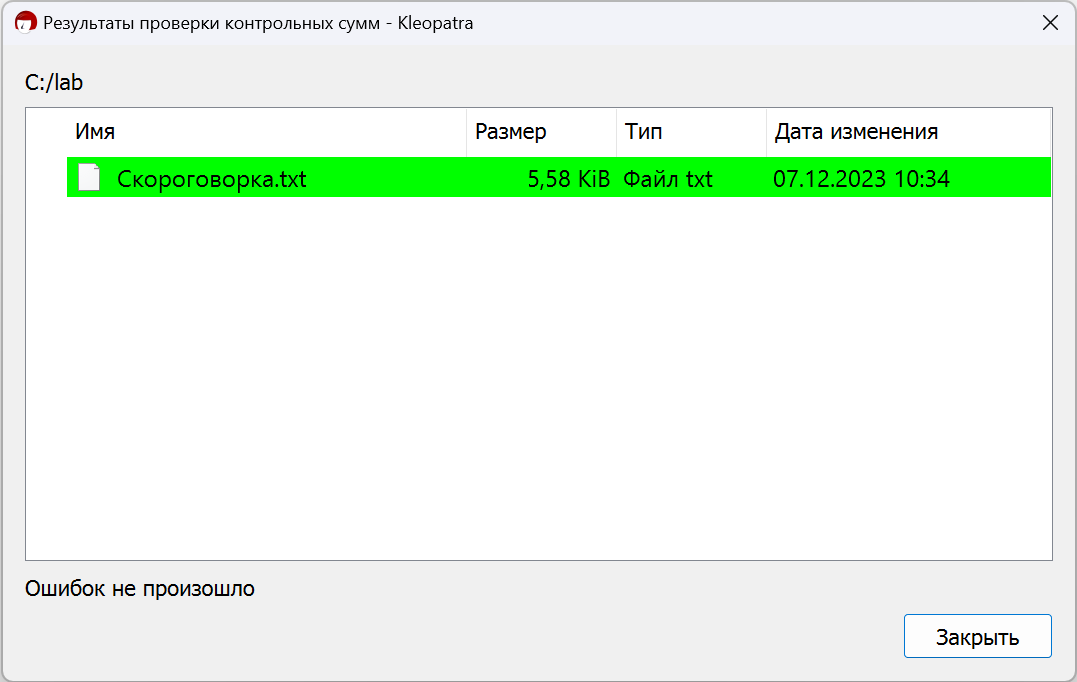


#### Рисунок 10-11.21

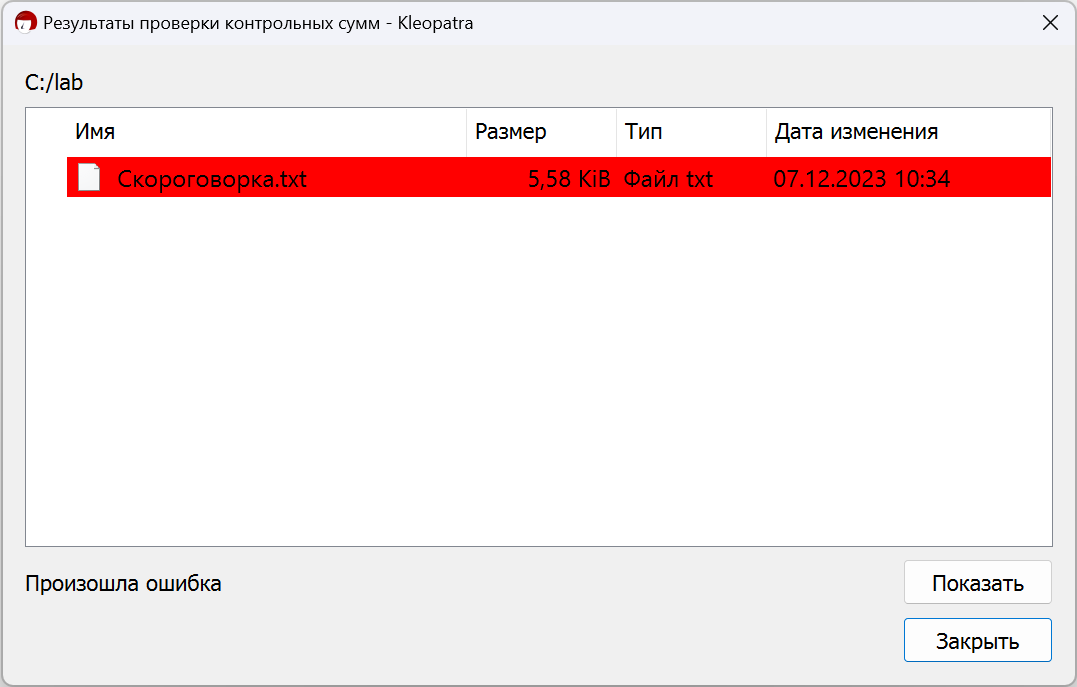
Получив от напарника документ с подписью, убедитесь, что подпись верна. Измените подписанный документ и убедитесь, что подпись стала неверна. Верните документ к первоначальному состоянию и вновь убедитесь, что подпись верна. (Рис. 10-11.22-25)



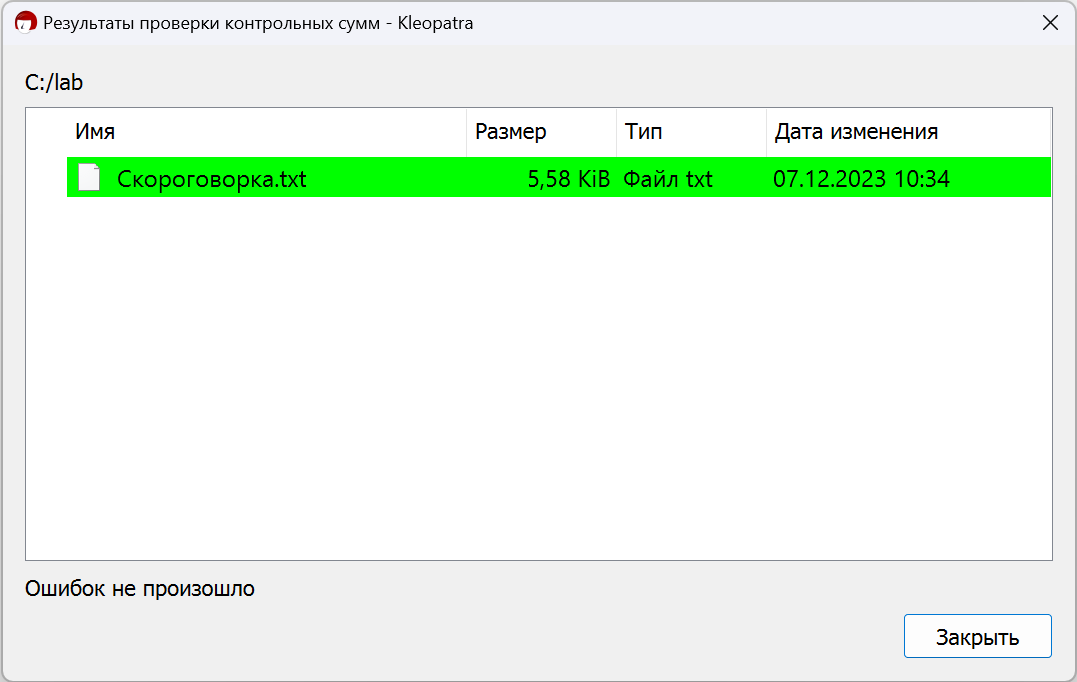
#### Рисунок 10-11.22



#### Рисунок 10-11.23



#### Рисунок 10-11.24



#### Рисунок 10-11.25

# Вывод

Я ознакомился с принципами криптографической защиты информации с использованием алгоритмов асимметричного шифрования и электронной цифровой подписи, а также приобрел практические навыки практического применения указанных методов защиты информации на основе системы GnuPG.

#### Лабораторная работа №12

«Реестр операционной системы Windows»

Цель работы

Сформировать умения шифрования с использованием систем Цезаря и системы Трисемуса.

# Задание

Первое задание заключается в том, чтобы зашифровать сообщение «МЫ ДОЛЖНЫ ПРИЗНАТЬ ОЧЕВИДНОЕ: ПОНИМАЮТ ЛИШЬ ТЕ, КТО ХОЧЕТ ПОНЯТЬ», используя систему Цезаря со значением ключа, соответствующим номеру по журналу, k = 7. (Рис. 12.1)

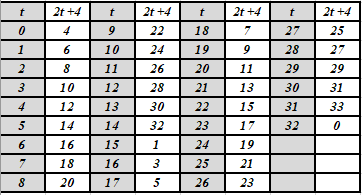
#### 

#### Рисунок 12.1

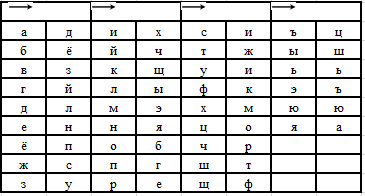
Ответ: АО ЧВЯЪБО ГДЬЫБУЁП ВКШХЬЧБВШ: ГВБЬАУСЁ ЯЬЛП ЁШ, ЮЁВ ИВКШЁ ГВБТЁП

Понедельник - цхфлклтгфпс

Второе задание заключается в том, чтобы зашифровать сообщение «СМЫСЛ ЖИЗНИ НАШЕЙ - НЕПРЕРЫВНОЕ ДВИЖЕНИЕ», используя аффинную систему подстановок Цезаря с ключами, согласно своему варианту, a = 2, b = 4. (Рис. 12.2-3)



#### Рисунок 12.2

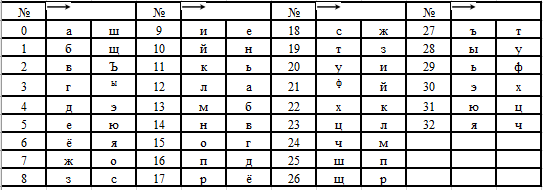


#### Рисунок 12.3

СРЕДА - ИЕНЛД

Ответ: ЕТМЕО ЫВЯЦВ ЦГАЧЖ - ЦЧЮБЧБМЛЦЪЧ УЛВЫЧЦВЧ

Третье задание заключается в том, чтобы выполнить шифрование сообщения «РАЗУМА ЛИШАЕТ НЕ СОМНЕНИЕ, А УВЕРЕННОСТЬ», используя систему шифрования Цезаря с ключами, соответствующими варианту, k = 7, ключевое слово «ОСЕНЬ» (Рис. 12.4)

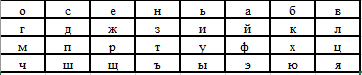


#### Рисунок 12.4

СРЕДА - ЖЁЮЭШ

Ответ: ХСЪБЯС ЮЫЖСЧА ОЧ ИРЯОЧОЫЧ, С БУЧХЧООРИАЛ

Четвёртое задание заключается в том, чтобы выполнить шифрование сообщения «УСПЕХ — ЭТО КОГДА ТЫ ДЕВЯТЬ РАЗ УПАЛ, НО ДЕСЯТЬ РАЗ ПОДНЯЛСЯ», используя систему Трисемуса с ключевым словом из задания 3. Размер таблицы подстановок 4 х 8. (Рис. 12.5)



#### Рисунок 12.5

УДАР – ЫПЙЩ

Ответ: ыдшжю – агъ хгмпй ъь пжлвъи щйт ышйц, зг пждвъи щйт шгпзвцдв

# Вывод:

Я приобрёл практические навыки шифрования с использованием систем Цезаря и системы Трисемуса