



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

---

**Институт  
информационных  
технологий**

**Кафедра  
Информационных систем**

**ОТЧЕТ О ВЫПОЛНЕНИИ ЛАБОРАТОРНОЙ РАБОТЫ № 4**  
**ПО ДИСЦИПЛИНЕ**  
**« Защита информации »**

**СТУДЕНТА 4 КУРСА бакалавриата ГРУППЫ ИДБ-20-02**

**Ердоган Дениз Ердалович**

---

**Тема: « Изучение программных средств шифрования, компьютерной  
стеганографии и защиты от вредоносных программ »**

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

Отчет сдан «\_\_\_\_\_» \_\_\_\_\_ 2023 г.

Оценка \_\_\_\_\_

Преподаватель \_\_\_\_\_ Симонов М.Ф. \_\_\_\_\_.

МОСКВА 2023

1. При работе в компьютерном классе университета пункты 1-8 выполняются в окне виртуальной ОС Windows XP. Скопировать в произвольную папку на локальном жестком диске файл mosafe21.exe из указанного преподавателем сетевого диска;
2. Запустить программу mosafe21.exe и разархивировать все файлы из этого самораспаковывающегося архива:

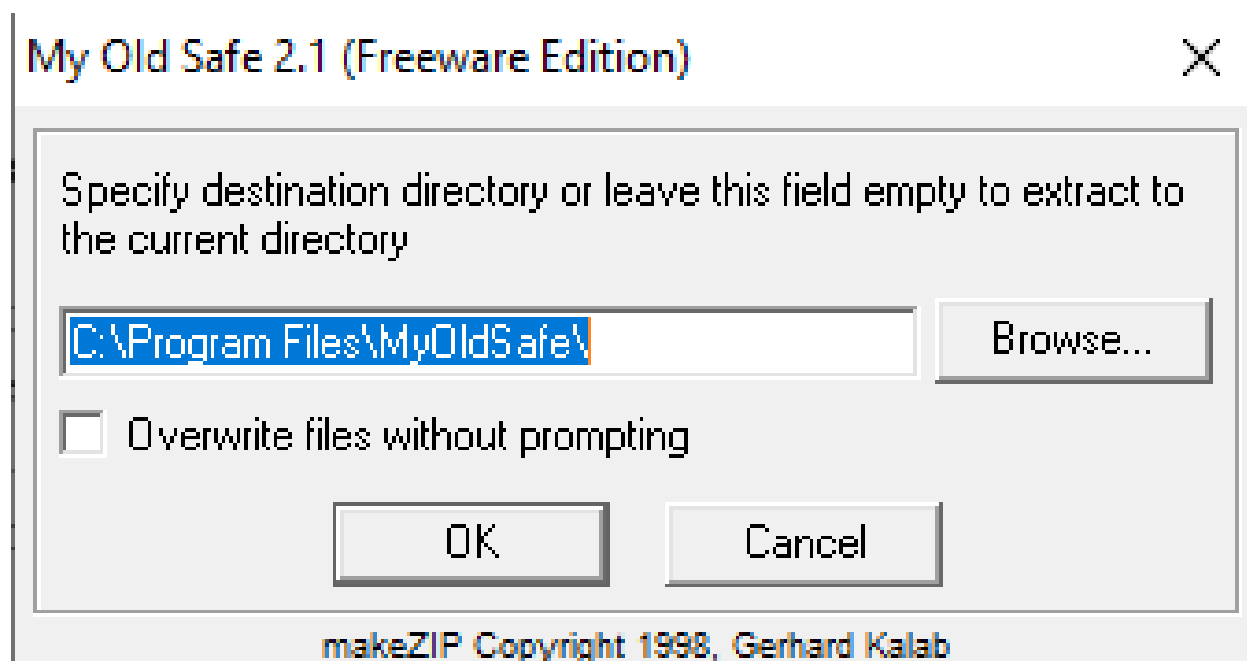
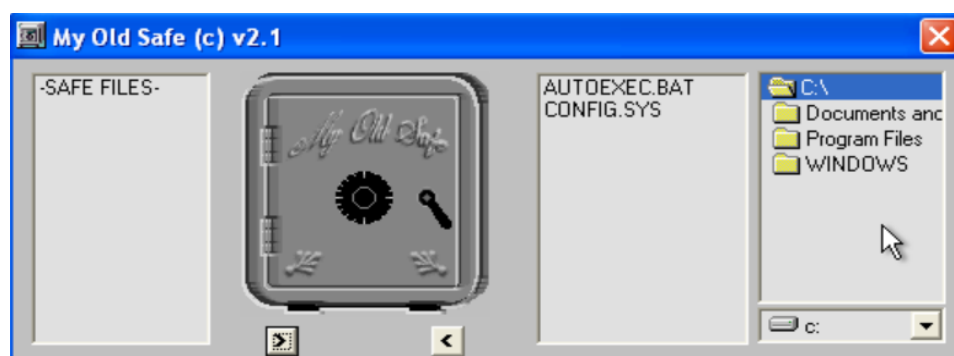


Рисунок № 1 – разархивирование файлов MyOldSafe (Windows XP).

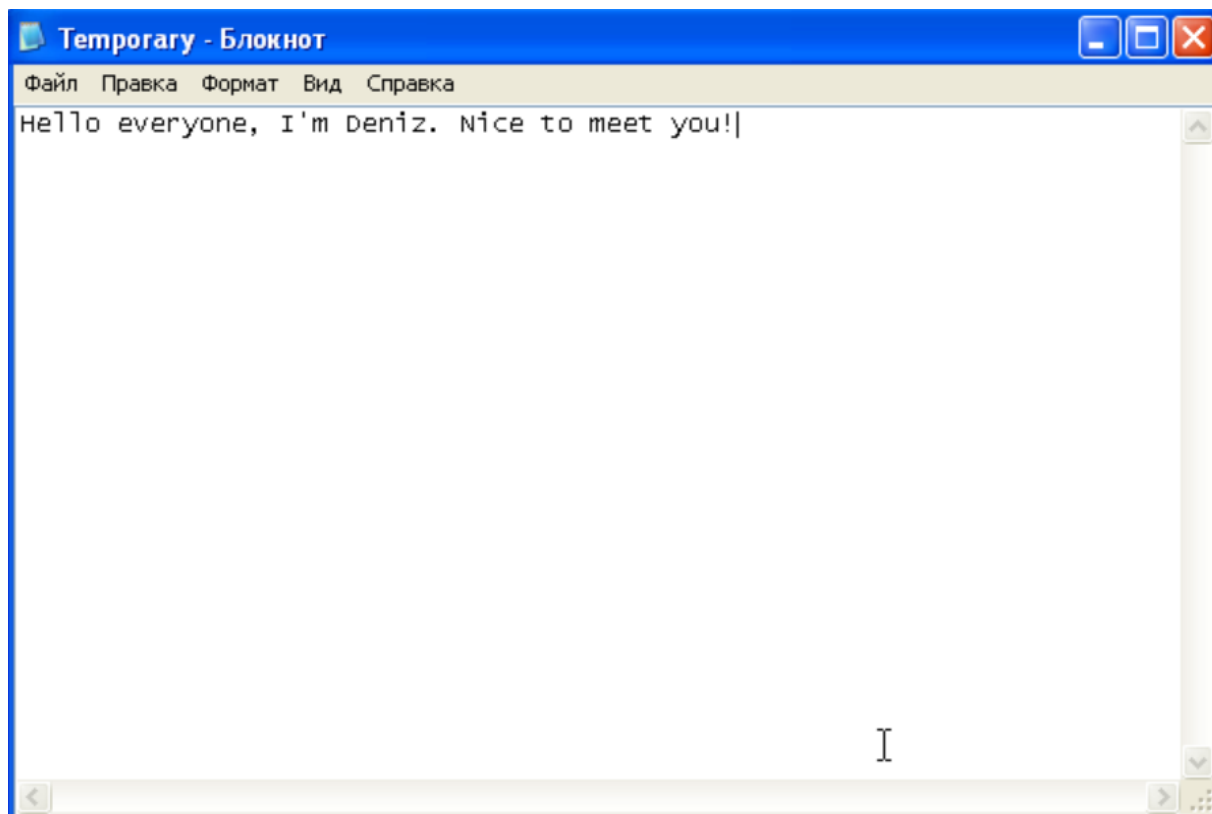
3. Запустить программу шифрования файлов MyOldSafe. На примере работы с произвольными (несистемными) файлами различного типа изучить функции программы и включить в электронную версию отчета о лабораторной работе копии экранных форм, полученных при использовании этой программы, после чего завершить работу с ней:

**MyOldSafe** – это ПО служащее для шифрования и дешифрования файлов.



**Рисунок № 2 – вид интерфейса программы MyOldSafe (Windows XP).**

Рассмотрим функционал программы на примере текстового файла. Для этого создадим текстовый файл с названием “*Temporary*”. Посмотрим на содержание файла:



**Рисунок № 3 – содержание текстового файла Temporary до шифрования (Windows XP).**

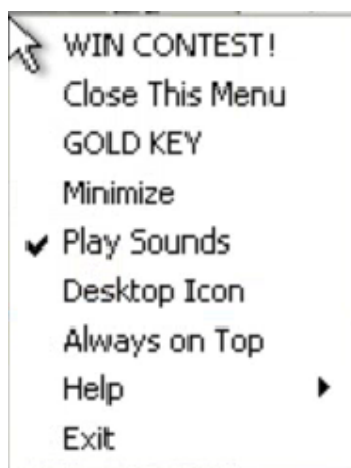
Теперь обратимся к программе, чтобы разобраться с её функционалом при помощи ранее созданного текстового файла:



#### Рисунок № 4 – окно программы MyOldSafe с созданным текстовым файлом Temporary (Windows XP).

Слева список зашифрованных файлов, справа - файлы которые можно зашифровать, правее находится текущая директория рассматриваемых файлов.

При нажатии левой кнопкой мышки на рисунок сейфа, появляется следующее контекстное меню:



#### Рисунок № 5 – контекстное меню приложения MyOldSafe (Windows XP).

Где:

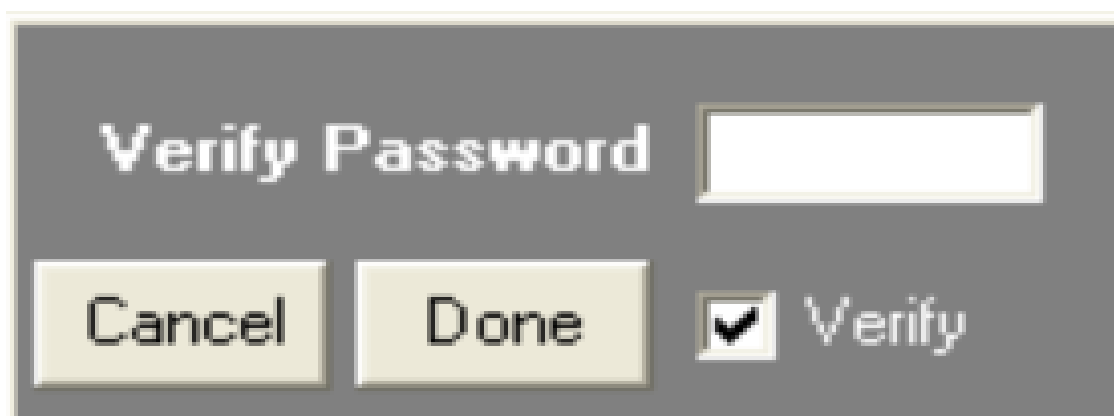
- *WIN CONTEST!* – документация приложения;
- *Close This Menu* – функция закрыть контекстное меню;
- *GOLD KEY* – информация о “Золотом ключе”;
- *Minimize* – минимизация окна приложения;
- *Play Sound* – включение/выключение звука приложения;
- *Desktop Icon* – отображение значка приложения;
- *Always on Top* – функция показа приложения поверх остальных;
- *Help* – подменю помощи;
- *Exit* – выход из приложения.

Разберёмся с шифрованием. При переносе файлов справа на рисунок сейфа, файл шифруется с указанным пользователем паролем. Пароль вводится в следующем окне:



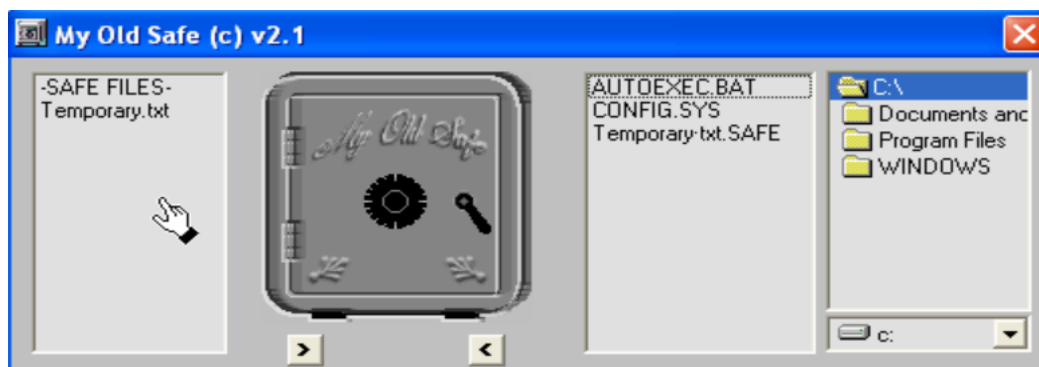
**Рисунок № 6 – окно ввода пользовательского пароля для шифрования (Windows XP).**

После ввода пароля и нажатия кнопки “*Done*” нужно подтвердить введённый пароль в следующем окне:



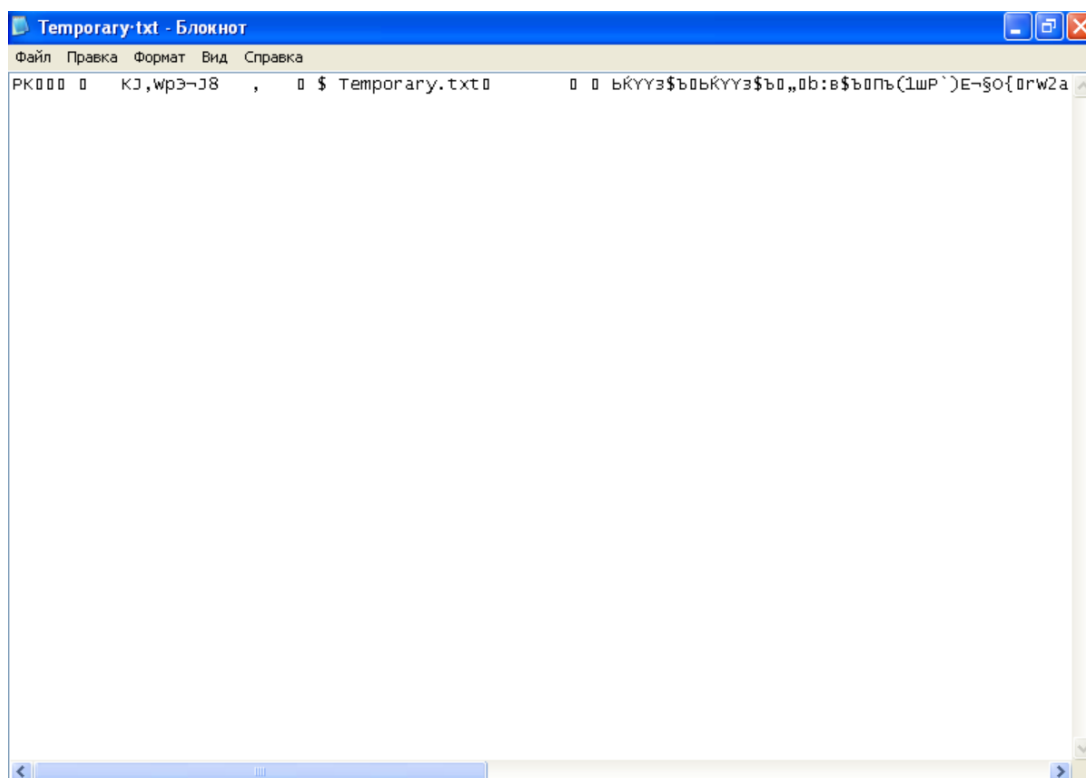
**Рисунок № 7 – окно подтверждения пользовательского пароля для шифрования (Windows XP).**

После чего файл получает расширение *\*.SAFE*, доступ к которому будут иметь только те, кто имеет доступ к паролю.



**Рисунок № 8 – файл Temporary в приложении MyOldSafe после шифрования (Windows XP).**

Рассмотрим содержание файла *Temporary.txt* после шифрования:



**Рисунок № 9 – содержание текстового файла после шифрования (Windows XP).**

Получить доступ к файлу можно только при переносе файла слева на рисунок сейфа, и ввода правильного пароля. Окна ввода и подтверждения пароля аналогичны с рисунками № 6 и 7. Если ничего не ввести в форме ввода пароля, то появится следующее информационное сообщение:



**Рисунок № 10 – информационное сообщений требований при вводе пароля (Windows XP).**

При неправильном вводе пароля всплывает предупреждение:



**Рисунок № 11 – предупреждение при неправильном вводе пароля (Windows XP).**

При повторном неправильном вводе программа выдаёт сообщение ошибки и закрывается:



**Рисунок № 12 – сообщение ошибки при повторном неправильном вводе пароля (Windows XP).**

При работе с несистемными файлами иных форматов действия аналогичные (\*.WAV - аудиофайл, \*.doc - файл *Microsoft Word*):



Рисунок № 13 – зашифрованные файлы разных форматов (Windows XP).

**Включить в отчет ответы на вопросы:**

- **3.1. Как выполняется шифрование и расшифрование файлов:**

С помощью программы *MyOldSafe*. Для шифрования и расшифрования необходимо перетаскивать файлы на изображение сейфа. После чего нужно ввести парольную фразу и подтвердить её в следующей форме. В результате чего создаётся файл с расширением \*.SAFE, и наоборот при дешифровании.

Данная программа использует архиватор. Она создает с помощью пользовательского пароля ключ и архивирует выбранные файлы, шифруя их по стандарту *AES-128* со сгенерированным ключом.

- **3.2. К какой криптосистеме относится эта программа и почему:**

Данная программа относится к симметричной криптосистеме с закрытым ключом, так как для шифрования и расшифрования применяется один и тот же ключ.

- **3.3. Как формируется ключ шифрования:**

Ключ шифрования создается на основе введенного пароля пользователем по определённому алгоритму.

- **3.4. Изменяется ли размер зашифрованного файла и, если изменяется, то почему:**



Размер зашифрованного файла изменяется. К нему добавляются стандартные заголовки *zip*-архива, а также производится сжатие шифруемых данных. Так до шифрования размер файла *Temporary* был 110 байт, после шифрования стал – 196 байт.

Так как большинство симметричных шифров являются блочными, то если размер файла не кратен блоку, то происходит дополнение сообщения до длины, кратной размеру блока.

- **3.5. Есть ли возможность выбора алгоритма шифрования:**

Возможности выбора алгоритма шифрования нет.

- **3.6. Возможен ли совместный доступ к зашифрованным файлам:**

Одновременно можно запустить лишь одну копию программы, так что совместный доступ к зашифрованным файлам невозможен.

**4. Скопировать в произвольную папку на локальном жестком диске файл *citadel.zip* из указанного преподавателем сетевого диска;**

**5. Извлечь файлы из архива, скопированного в пункте 4;**

**6. Запустить программу *setup.exe* для установки программы шифрования файлов Citadel Safstor:**



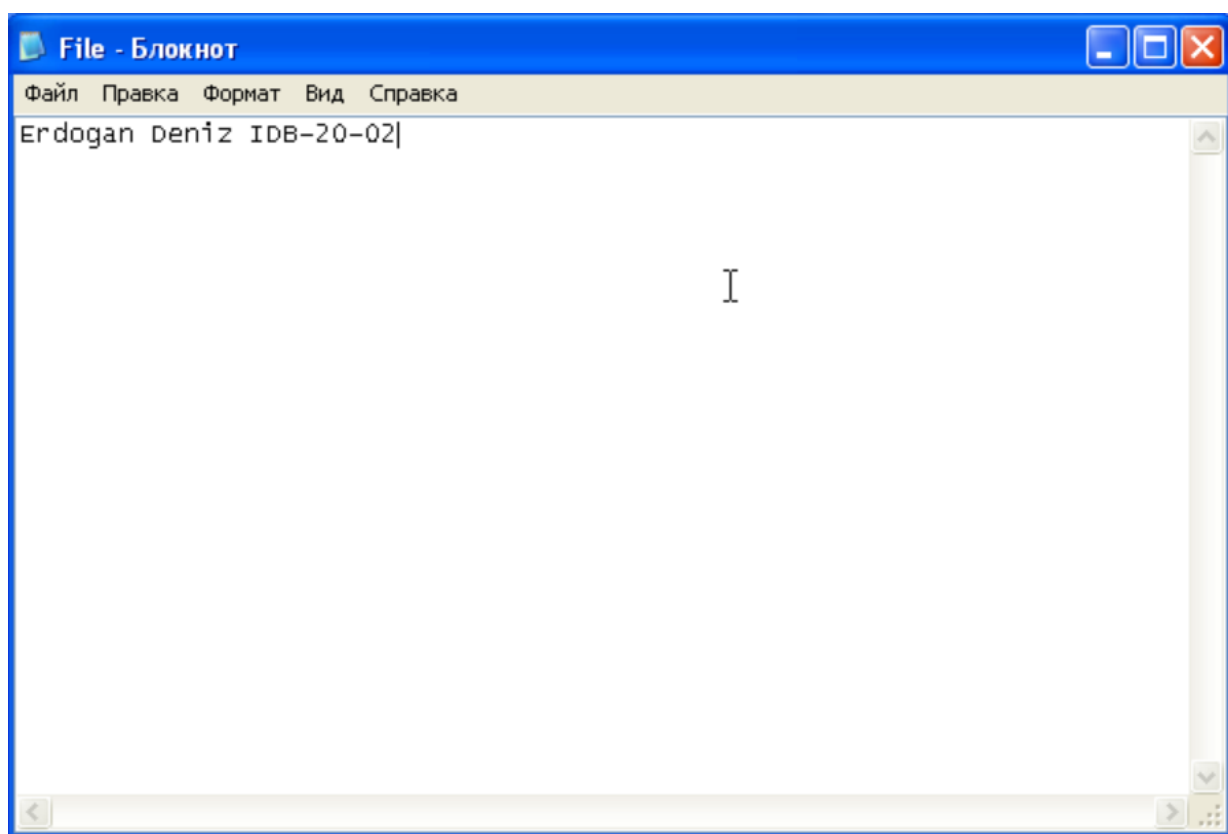
**Рисунок № 14 – установка приложения Citadel Safstor (Windows XP).**

**7. На примере работы с произвольными (несистемными) файлами различной природы изучить функции программы шифрования файлов Citadel Safstor, учитывая, что:**

- **доступ к шифрованию (расшифрованию) возможен через контекстное меню Проводника Windows. Если соответствующая команда не появилась в контекстном меню Проводника, то шифрование файла возможно с помощью команды главного меню Пуск | Выполнить | “C:\Program Files\Citadel Data Security\Citadel Safstor\csenc” полный путь к шифруемому файлу. Для расшифрования файла следует в этом случае использовать команду Пуск | Выполнить | “C:\Program Files\Citadel Data Security\Citadel Safstor\csdec” полный путь к зашифрованному файлу с расширением .css;**
- **другие пользователи программы Citadel Safstor могут быть созданы с помощью функции Citadel Safstor Панели управления (вкладка User Profiles, кнопка New User);**
- **«переключение» на другого пользователя программы Citadel Safstor производится также с помощью Панели управления (функция Citadel Safstor, вкладка Current User). Включить в электронную версию отчета о лабораторной работе копии экранных форм, полученных при использовании этой программы, после чего завершить работу с ней.**

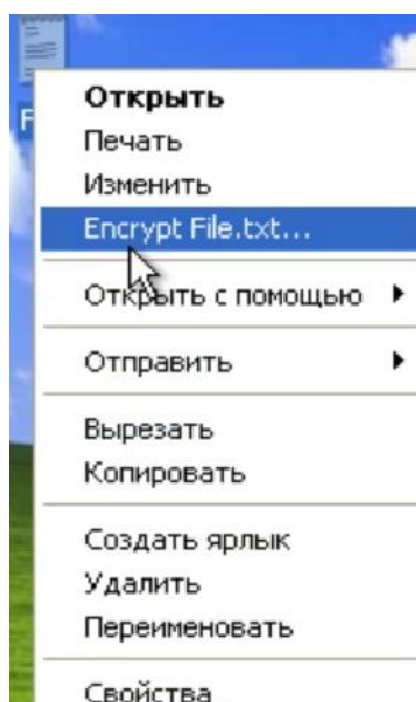
Ещё одной программой для шифрования файлов является - *Citadel Safstor*.

Создадим текстовый файл “*File.txt*” для того, чтобы в дальнейшем продемонстрировать функционал работы программой. Содержание созданного файла будет следующим:



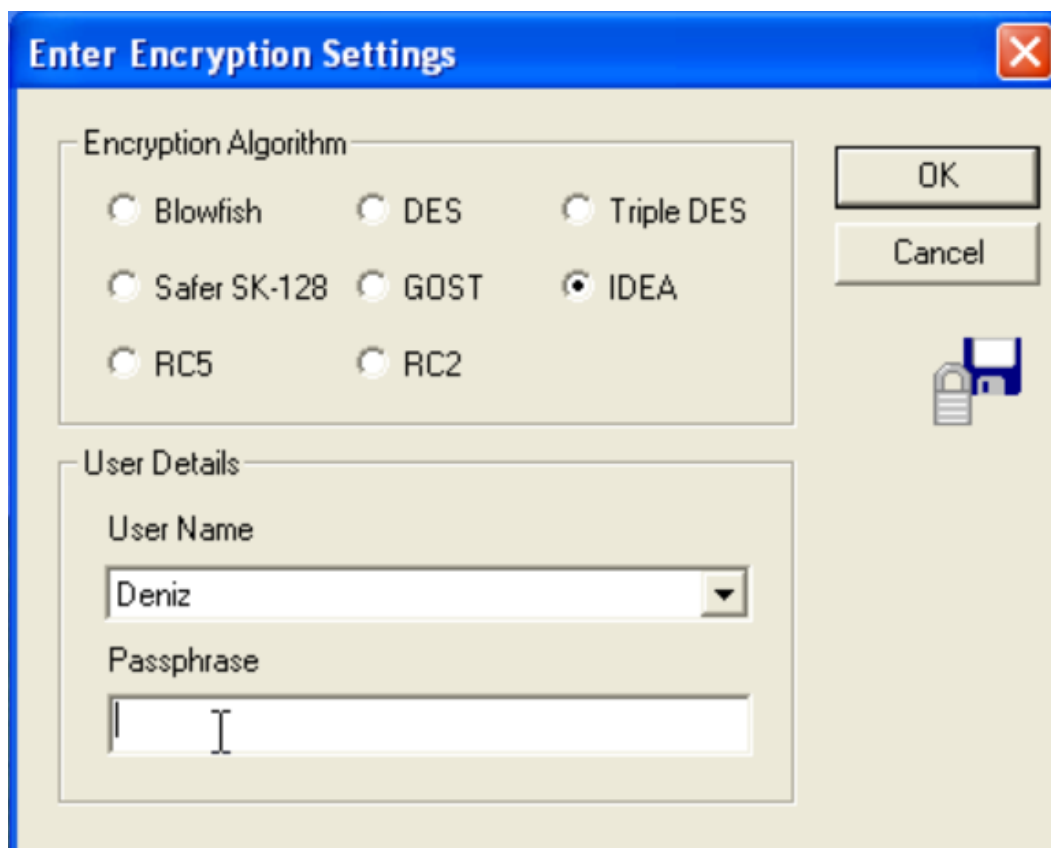
**Рисунок № 15 – содержание созданного файла до шифрования (Windows XP).**

Зашифровать файл можно при помощи данной программы выбрав соответствующий пункт “*Encrypt ...*” из контекстного меню. Прделаем данное действие:



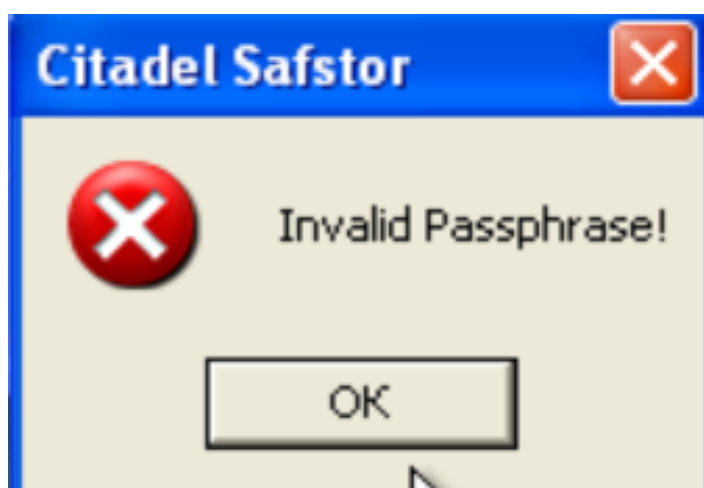
**Рисунок № 16 – контекстное меню файла с пунктом шифрования (Windows XP).**

Выберем пункт шифрования для созданного ранее файла:



**Рисунок № 17 – окно шифрования файла (Windows XP).**

Если неправильно ввести парольную фразу/не ввести парольную фразу, то появится следующее окно ошибки:



## Рисунок № 18 – сообщение ошибки ввода парольной фразы (Windows XP).

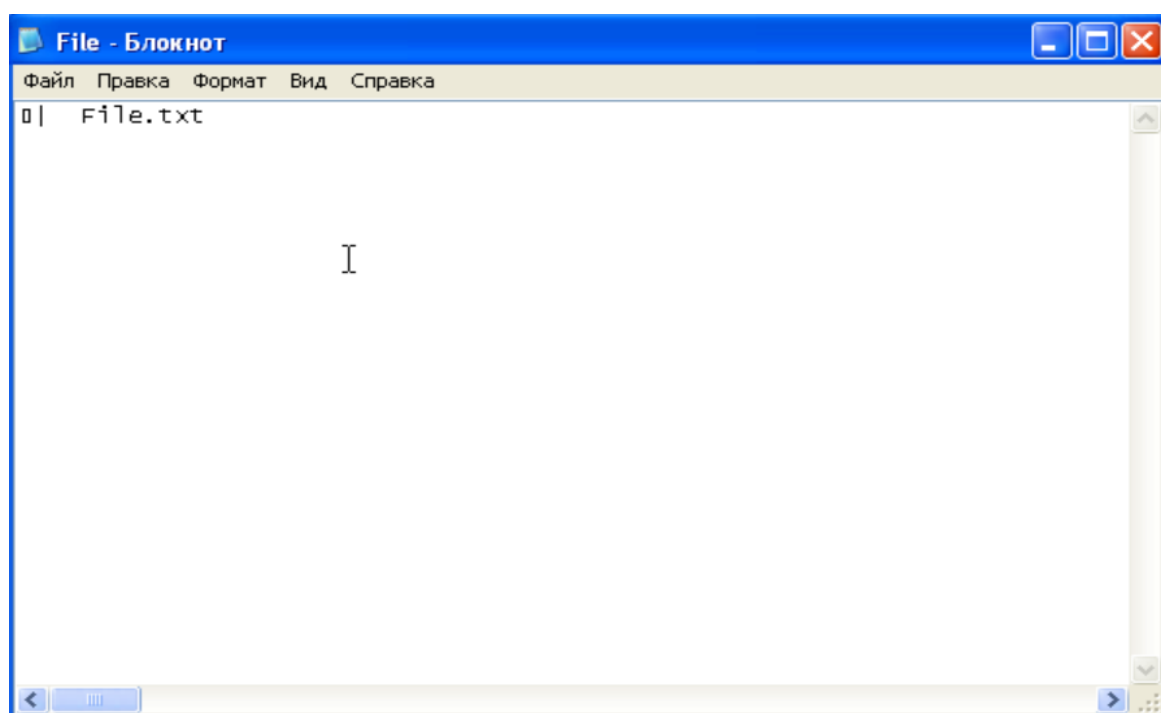
После выбора пункта “*Encrypt*” появилось окно с настройками шифрования. В этом окне можно выбрать: алгоритм шифрования, пользователя. А также доступен ввод секретной фразы для возможности шифрования через определённого пользователя.

После успешного ввода секретной фразы пользователя и также нажатия кнопки “*OK*”, файл зашифруется и получит расширение \*.*css*. Доступ к файлу будут иметь те, кто обладает парольной фразой. Внешний вид файла изменится на:



## Рисунок № 19 – файл File.txt после шифрования (Windows XP).

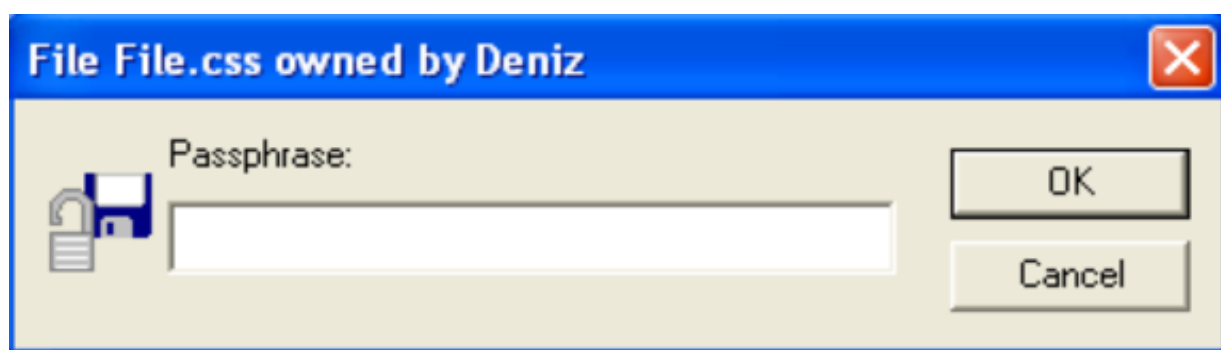
Посмотрим на содержание *File.txt* после шифрования:



**Рисунок № 20 – содержание файла File.txt после шифрования (Windows XP).**

Нужно отметить, что после шифрования размер файла изменился.

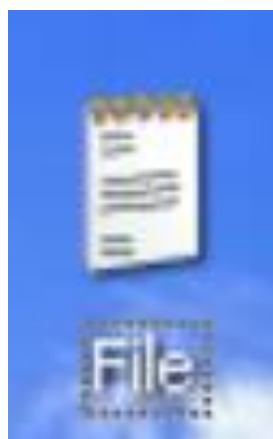
Если мы дважды нажмём левой кнопкой мышки на зашифрованный файл, то появится следующее окно, которое потребует ввод секретной фразы:



**Рисунок № 21 – окно ввода секретной фразы для дешифрования файла (Windows XP).**

При неправильном вводе парольной фразы появится окно аналогичное рисунку № 18 .

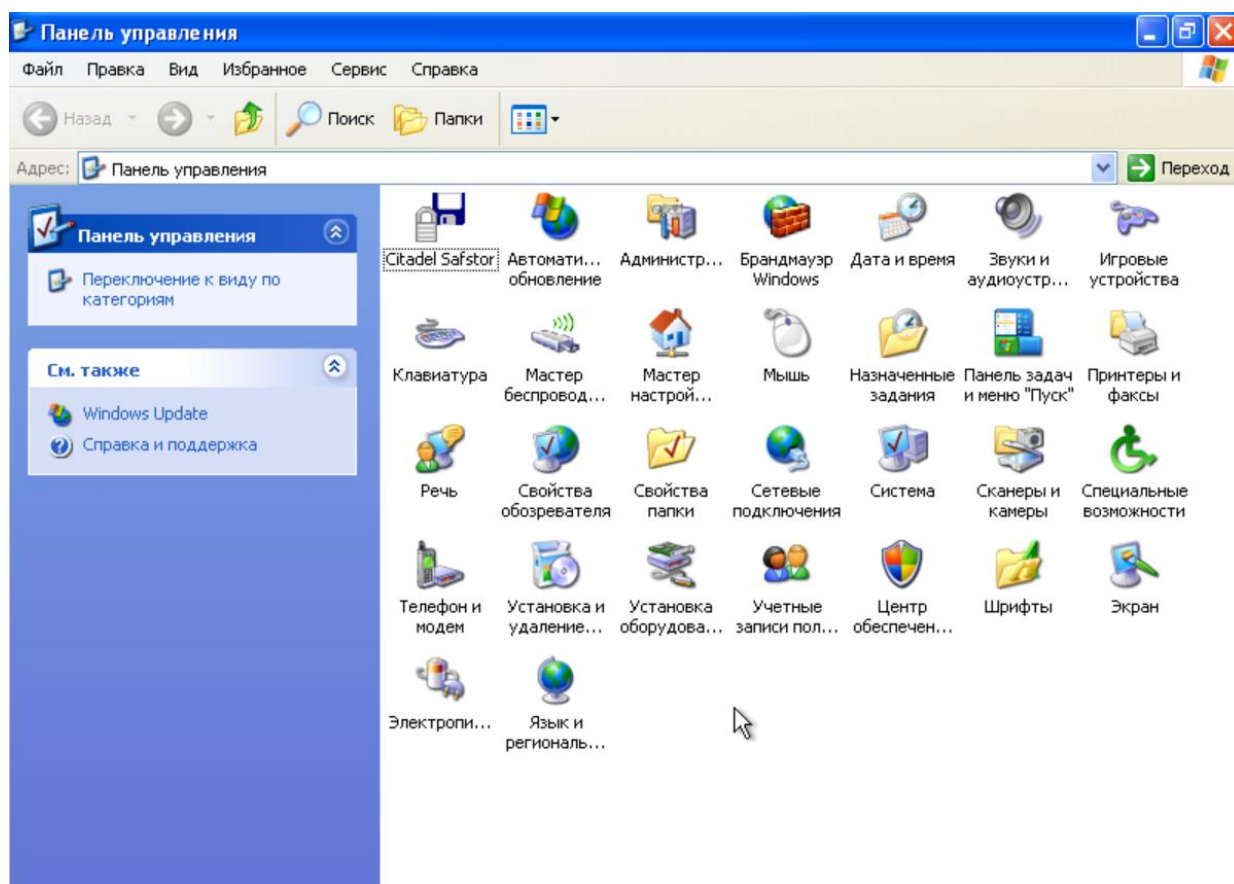
После успешного ввода файл дешифруется до начального состояния:



**Рисунок № 22 – дешифрованный файл File.txt (Windows XP).**

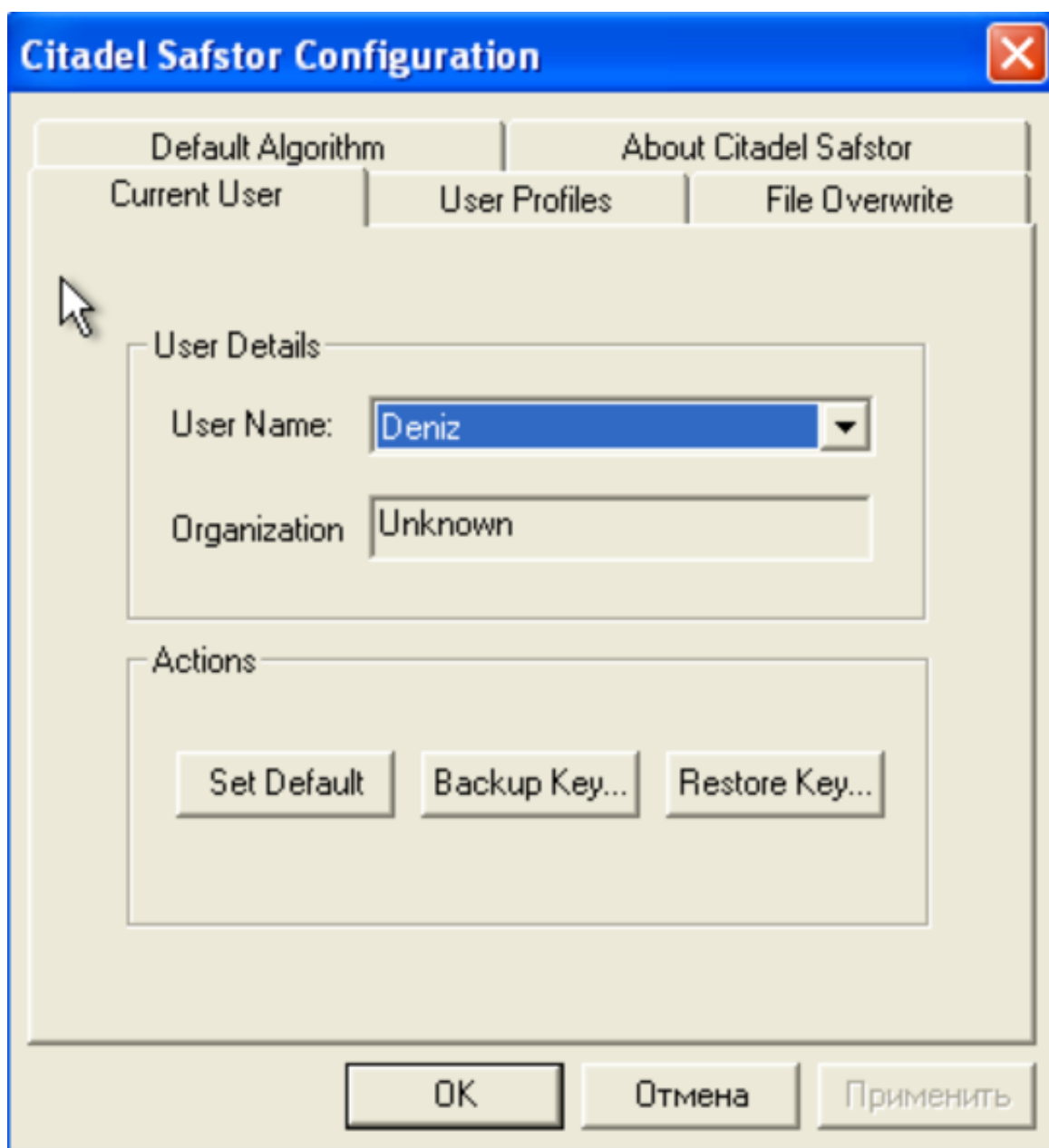
Работа с файлами расширения .WAV, .DOCX в программе аналогичная, так что отдельно её рассматривать не будем.

В *Панели управления* появился новый пункт связанный с выбором пользователя для шифрования/дешифрования:



**Рисунок № 23 – обновлённая панель управления (Windows XP).**

Если мы выберем новый пункт “*Citadel Safstor*”, то появятся следующие возможности программы:

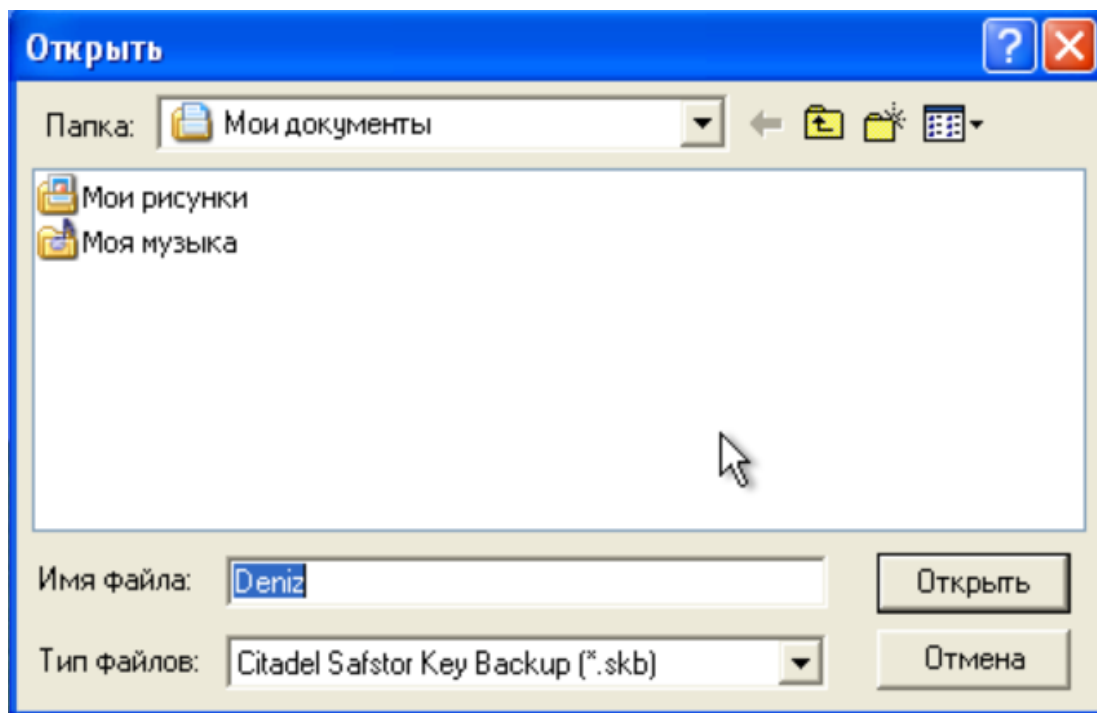


**Рисунок № 24 – окно настройки программы Citadel Safstor (Windows XP).**

В разделе “*Current User*” можно:

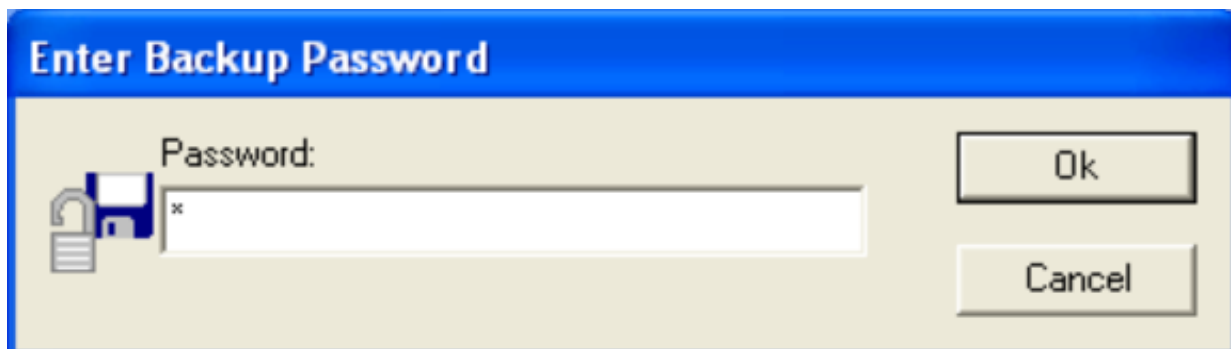
- Восстановить парольную фразу (при наличии ключа восстановления и необходимого файла с расширением \*.skb) по нажатию кнопки “*Restore Key ...*”:





**Рисунок № 25 – восстановление парольной фразы (Windows XP).**

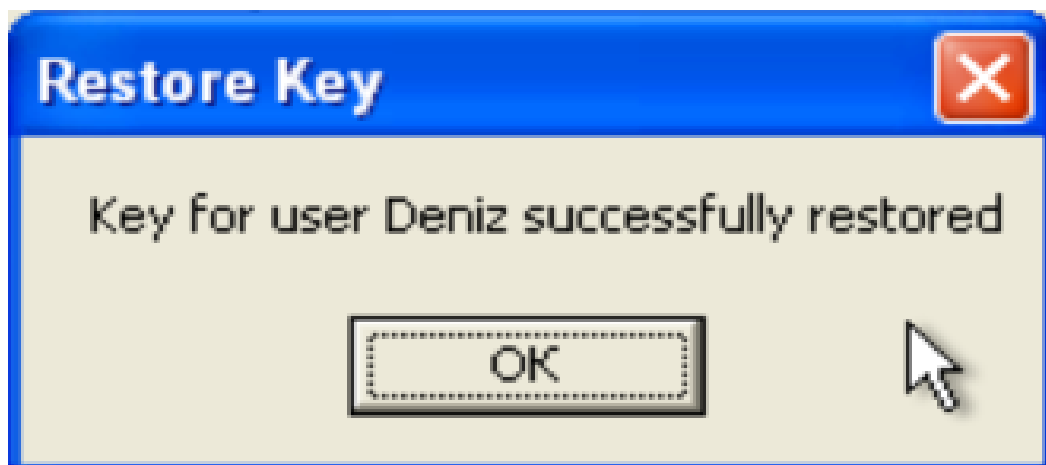
Если \*.skb файл был выбран, то появится следующее окно подтверждения парольной фразы:



**Рисунок № 26 – подтверждение текущей парольной фразы для восстановления старой парольной фразы (Windows XP).**

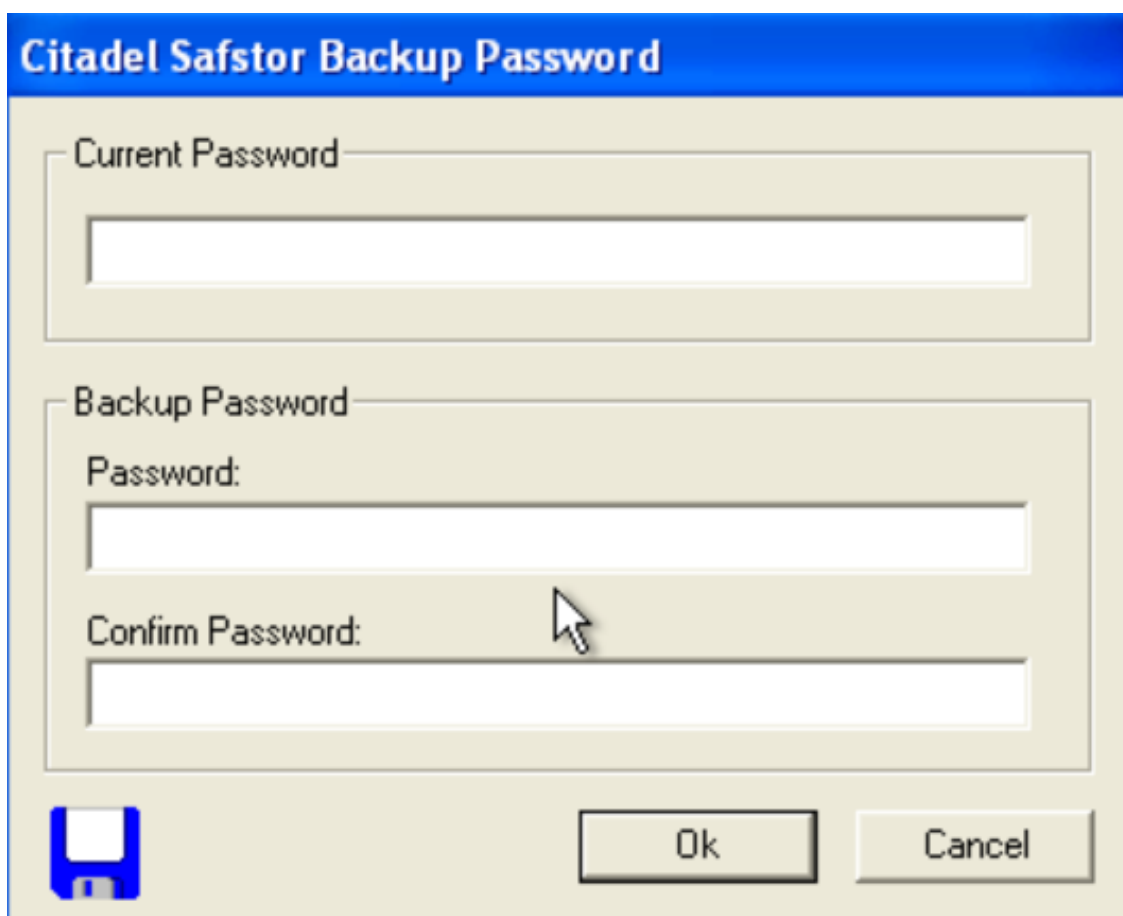
При неправильном вводе парольной фразы появится сообщение ошибки аналогичное рисунку № 18.

При успешном вводе текущей парольной фразы выведется информационное сообщение подтверждающие успешность восстановления:



**Рисунок № 27 – информационно окно сообщающие об успешности восстановления парольной фразы (Windows XP).**

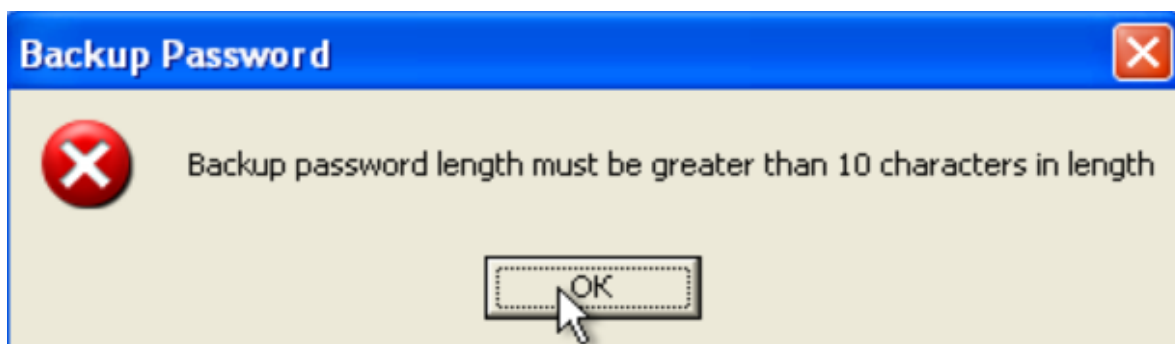
- Назначить пользователя по умолчанию по нажатию кнопки “*Set Default*”;
- Сменить парольную фразу по нажатию кнопки “*Backup Key...*”. Где нужно ввести старую секретную фразу, а также дважды новую. После чего необходимо нажать кнопку “*Ok*”:



**Рисунок № 28 – окно смены текущей парольной фразы (Windows XP).**

При неправильном вводе парольной фразы появится сообщение ошибки аналогичное рисунку № 18.

Если новая парольная фраза не подходит по критериям, то появится следующее сообщение:



**Рисунок № 29 – сообщение ошибки неудовлетворения новой парольной фразы (Windows XP).**

Если новая парольная фраза не была введена, то появится следующее сообщение об ошибке:



**Рисунок № 30 – сообщение отсутствия новой парольной фразы (Windows XP).**

При успешной смене парольной фразы появится следующее информационное сообщение:

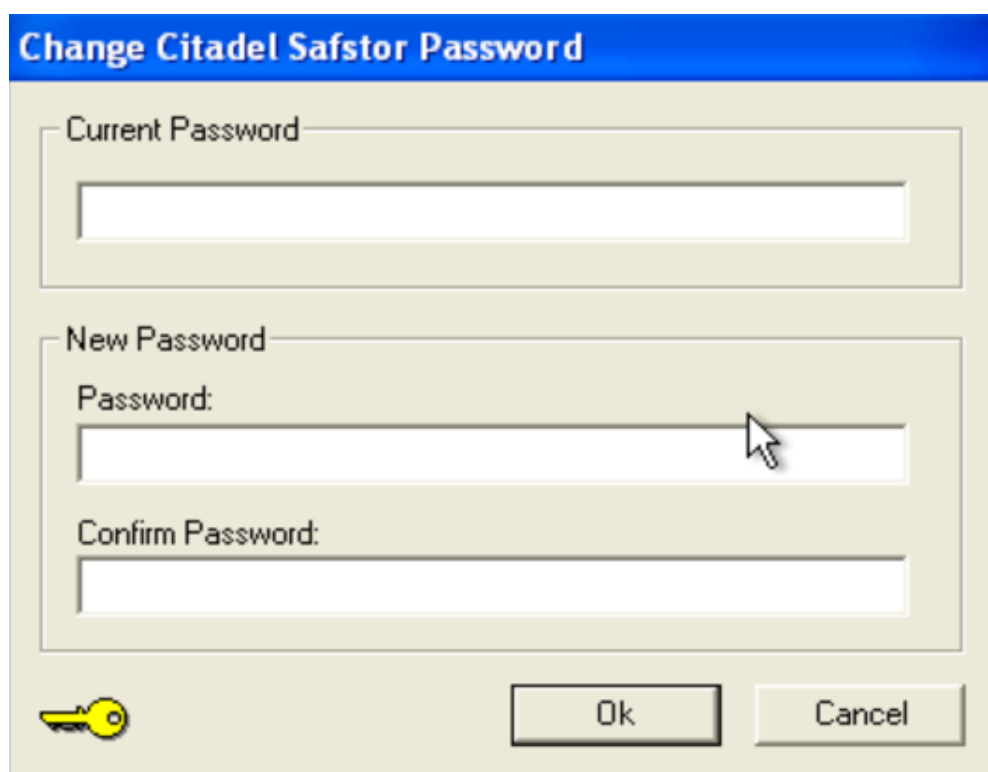


Рисунок № 31 – сообщение успешной смены парольной фразы (Windows XP).

- Выбрать пользователя нажав на подменю "*User name*".

В разделе "*User Profiles*" можно:

- Сменить пароль выбранного пользователя:



### Рисунок № 32 – смена пароля выбранного пользователя (Windows XP).

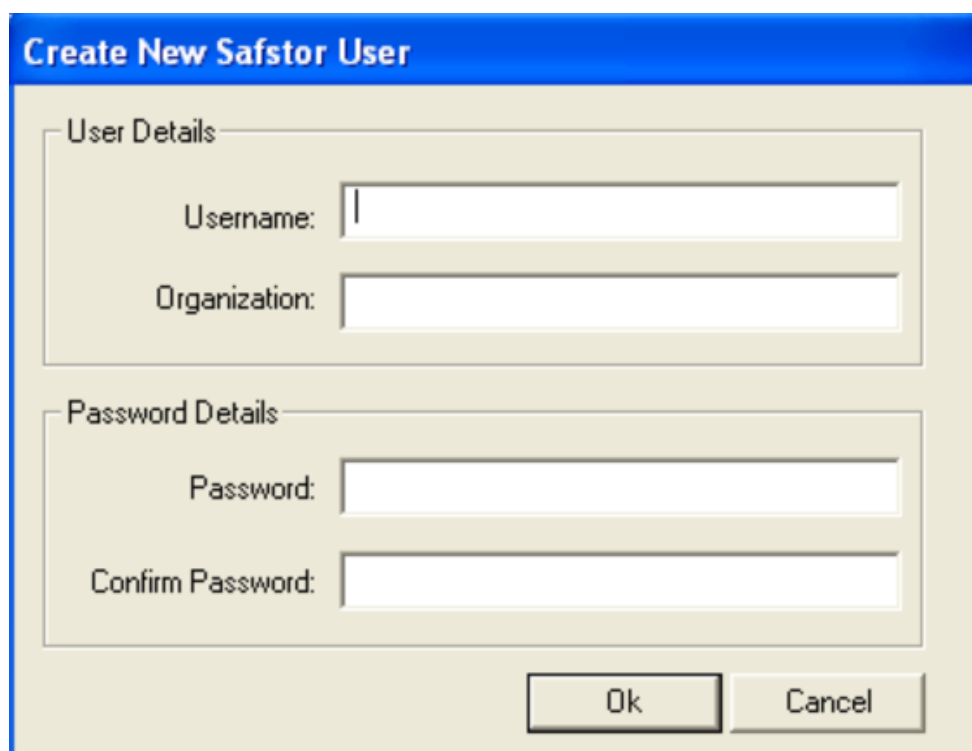
Что касается ошибок ввода пароля, то они аналогичные ошибкам ввода парольных фраз.

- Удаление пользователя по нажатию кнопки “*Remove...*”. После чего появится окно, в котором нужно подтвердить выбор нажатием на кнопку “Да”:



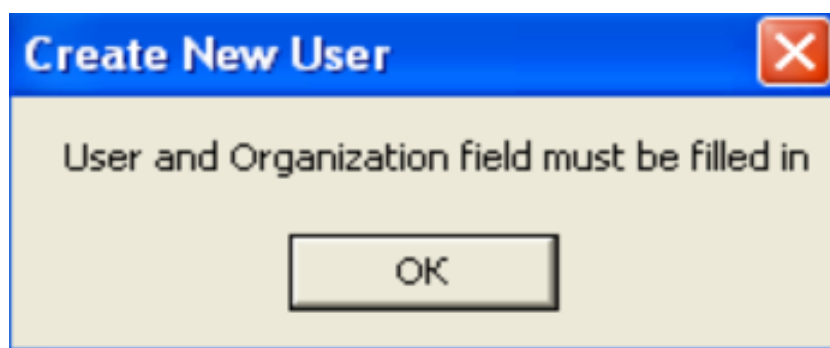
### Рисунок № 33 – удаление пользователя (Windows XP).

- Добавление нового пользователя по нажатию кнопки “*New User...*”, после чего появляется новое окно, в котором нужно ввести все необходимые параметры и нажать кнопку “*OK*” для подтверждения:



**Рисунок № 34 – создание нового пользователя (Windows XP).**

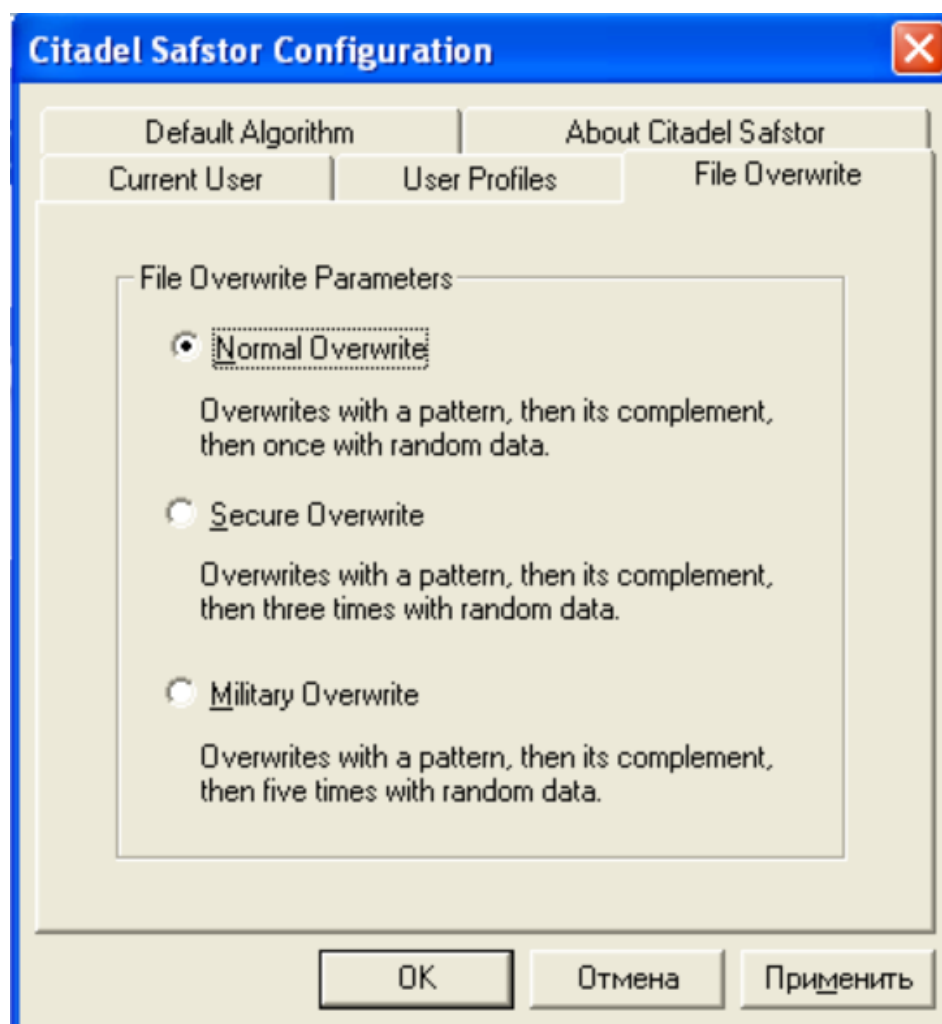
Если ничего не ввести, то появится следующее окно ошибки:



**Рисунок № 35 – окно ошибки отсутствия имени пользователя/названия организации (Windows XP).**

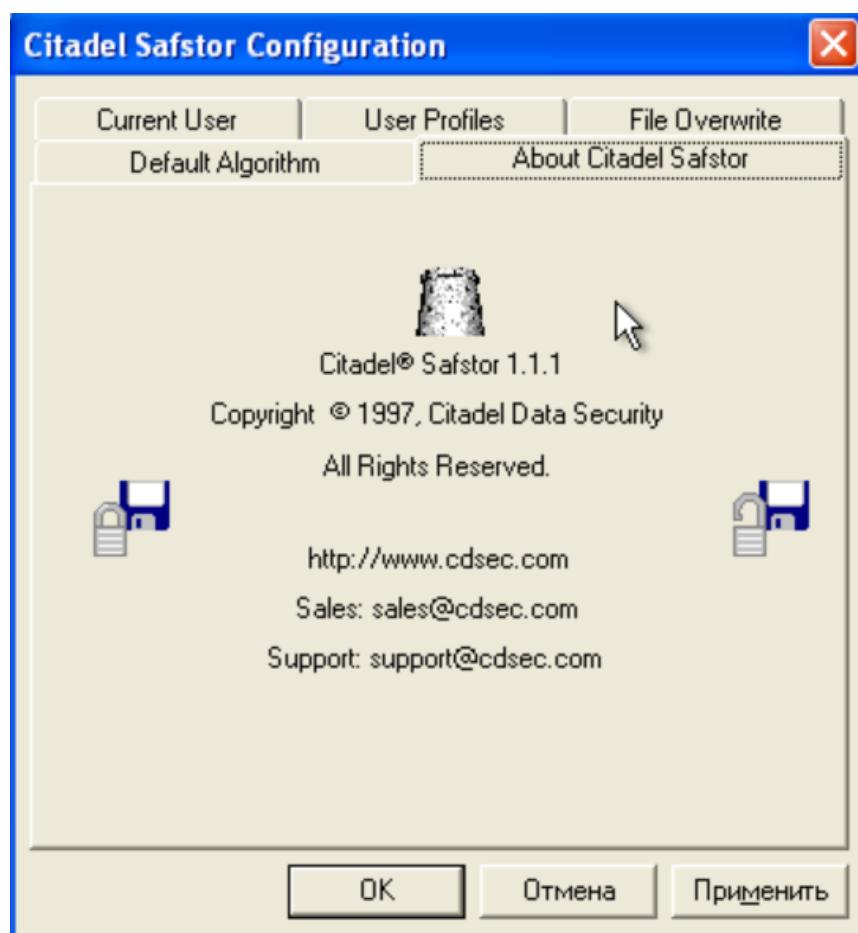
Что касается ошибок ввода пароля, то они аналогичные ошибкам ввода парольных фраз.

В разделе “*File Owerwrite*” можно переписать файл с одним из трёх доступных вариантов:



**Рисунок № 36 – окно переписывания файла (Windows XP).**

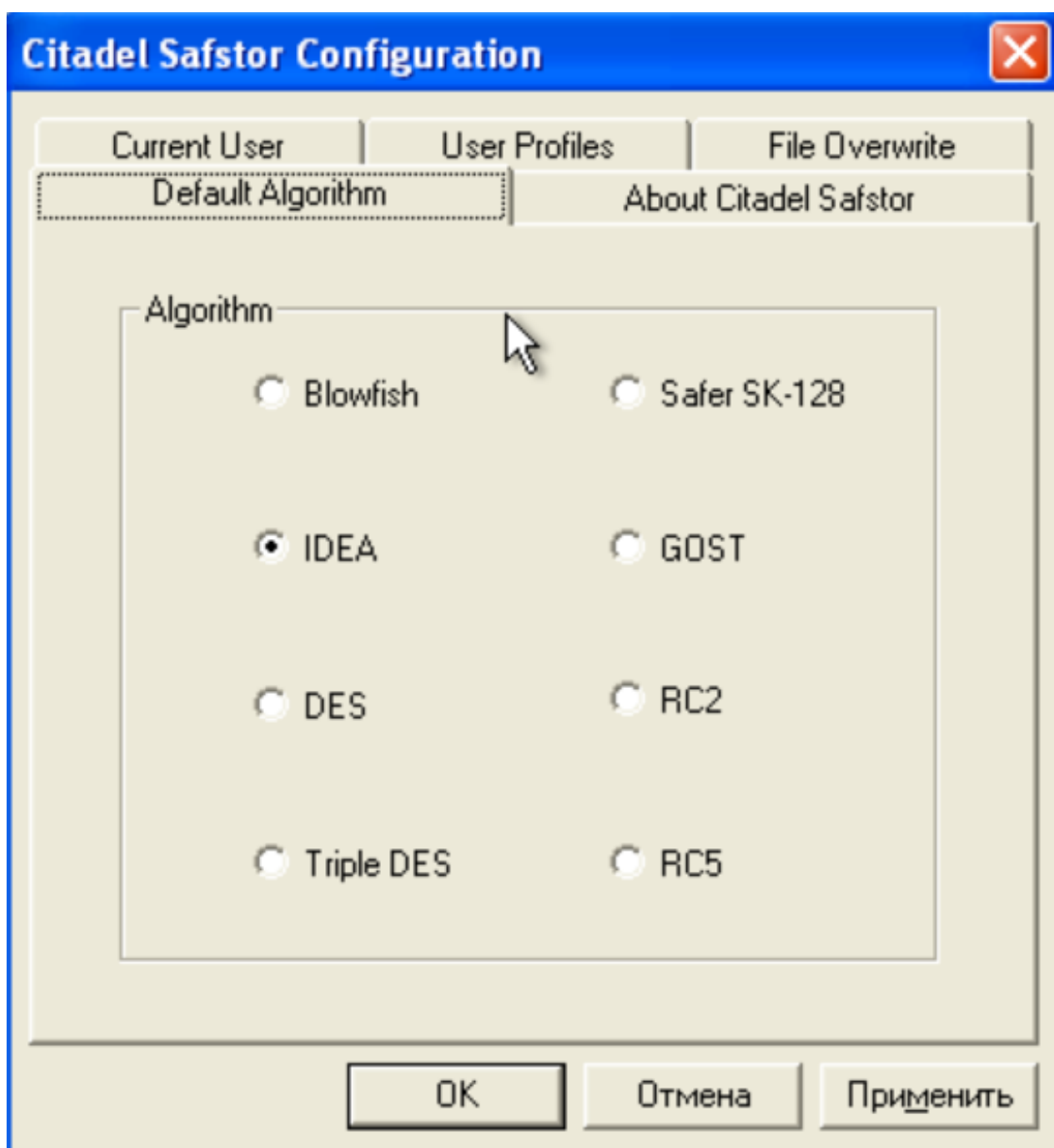
В разделе “*About Citadel Safstor*” можно прочитать информацию о приложении:



**Рисунок № 37 – удаление пользователя (Windows XP).**

В разделе “*Default Algorithm*” можно выбрать алгоритм по умолчанию для шифрования/дешифрования:





**Рисунок № 38 – окно выбора алгоритма шифрования/дешифрования по умолчанию (Windows XP).**

Для того, чтобы изменения вошли в силу, нужно в правом нижнем углу приложения нажать кнопку “Применить”.

**7.1. Включить в отчет ответы на те же вопросы, что и в пунктах 3.1-3.6, а также ответы на вопросы;**

**1. Как выполняется шифрование и расшифрование файлов:**

Через контекстное меню и выбором раздела “*Encrypt*” или “*Decrypt*”, после выбирается: алгоритм шифрования, пользователь. В обоих вариантах необходим ввод парольной фразы пользователем. После шифрования

исходный файл заменяется файлом с расширением \*.css, после расшифрования – наоборот.

**2. К какой криптосистеме относится эта программа и почему:**

К симметричной системе с закрытым ключом. Так как для шифрования и расшифрования применяется один и тот же ключ.

**3. Как формируется ключ шифрования:**

Генерируется на основе парольной фразы пользователя.

**4. Изменяется ли размер зашифрованного файла и, если изменяется, то почему:**

Да, до шифрования размер файла был 110 байт, после – 193 байт. Так как большинство симметричных шифров являются блочными, то если размер файл не кратен блоку, то происходит дополнение сообщения до длины, кратной размеру блока.

**5. Есть ли возможность выбора алгоритма шифрования:**

Есть возможность выбора из нескольких алгоритмов. На выбор имеется 8 блочных алгоритмов симметричного шифрования.

**6. Возможен ли совместный доступ к зашифрованным файлам:**

Совместный доступ к зашифрованным файлам невозможен.

**7.2. Какие действия выполняет пользователь при установке программы:**

При установке программа генерирует семя для генератора псевдослучайных чисел. После этого, пользователь задает имя и пароль.

**7.3. Для чего предназначена парольная фраза:**

Парольная фраза — это ключ, по которую зашифровывается и расшифровывается информация.

**7.4. Дополнительно включить в отчет краткое сравнение двух изученных программ шифрования файлов:**

Общая задача обеих программ одинаковая – защита файлов от *НСД*.

*MyOldSafe:*

- Для шифрования файлов необходимо непосредственно работать с программой, а именно перетаскивать файлы на изображение сейфа;
- Пользователь лишь один, для каждого файла можно задать свою парольную фразу. Однако для расшифровки файла необходимо, чтобы зашифрованный файл находился в той же директории, где и был зашифрован;

- Программа не позволяет выбирать алгоритм шифрования, выглядит проще и сжимает шифруемые данные.

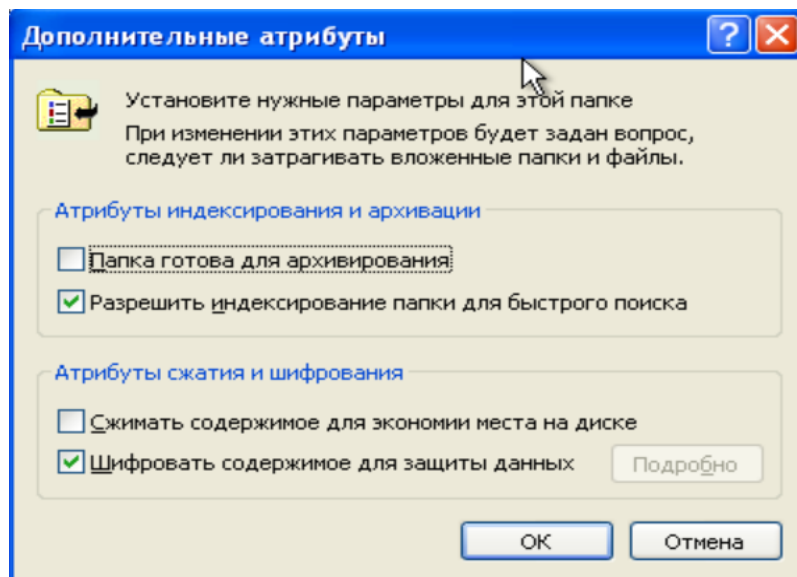
Citadel Safstor:

- Для работы с программой нужно контекстное меню;
- В Citadel Safstor можно добавлять разных пользователей, однако у каждого пользователя лишь одна парольная фраза для всех файлов;
- У пользователя на выбор 8 блочных алгоритмов симметричного шифрования;
- Citadel встраивается в проводник и позволяет использовать контекстное меню файлов для использования функционала программы, что является более удобным способом взаимодействия.

**8. Данный пункт выполняется в операционных системах Windows 2000 / Windows XP Professional на дисках, использующих файловую систему NTFS. На примере папок и файлов из папки Мои документы освоить средства обеспечения конфиденциальности информационных ресурсов с помощью шифрующей файловой системы (команда Свойств контекстного меню объекта, вкладка Общие, кнопка Другие, выключатель Шифровать содержимое для защиты данных). Включить в отчет ответы на вопросы:**

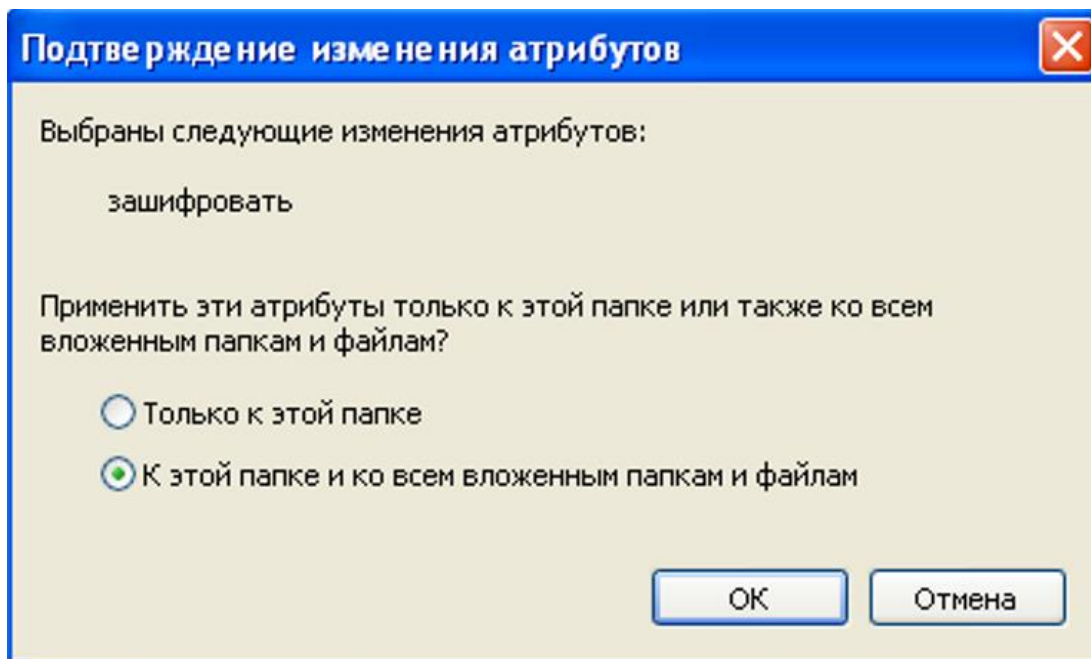
Разберём средства обеспечения конфиденциальности информационных ресурсов с помощью шифрующей файловой системы на примере папки в разделе “Мои документы” – “Мои рисунки”. Как найти необходимое меню описано в задании.

Включим шифрование, выбрав пункт “Шифровать содержимое для защиты данных”:



**Рисунок № 39 – шифрование папки (Windows XP).**

Что касается шифрования файлов, то ход работы похожий, но имеются некоторые отличия. Так при шифровании файла появляется следующее дополнительное окно:



**Рисунок № 40 – окно подтверждения шифрования файла (Windows XP).**

### **8.1. Скрывается ли наличие в системе зашифрованных файлов и папок:**

Не скрывается, зашифрованные папки и файлы по умолчанию выделяются зелёным цветом, данную функцию можно отключить с помощью раздела “Свойства папки” в “Панели управления”.

### **8.2. Где хранится ключ шифрования файла:**

Ключи шифрования *EFS* хранятся в резидентном пуле памяти, что исключает несанкционированный доступ к ним через файл подкачки.

### **8.3. Как обеспечивается в системе возможность восстановления зашифрованных файлов при невозможности входа пользователя в систему или при его отсутствии:**

Через агента восстановления (по умолчанию – администратор). Если сертификат агента восстановления удален, восстановление невозможно.

#### **8.4. На дисках с какой файловой системой возможно использование функции шифрования файлов:**

На дисках с файловой системой *NTFS*.

#### **8.5. При выполнении работы в операционной системе Windows XP Professional дополнительно освоить средства обеспечения совместного доступа к зашифрованным файлам и включить в отчет сведения о порядке использования этих средств и ответ на вопрос, среди каких пользователей возможен выбор тех, кому будет разрешен доступ к зашифрованному файлу:**

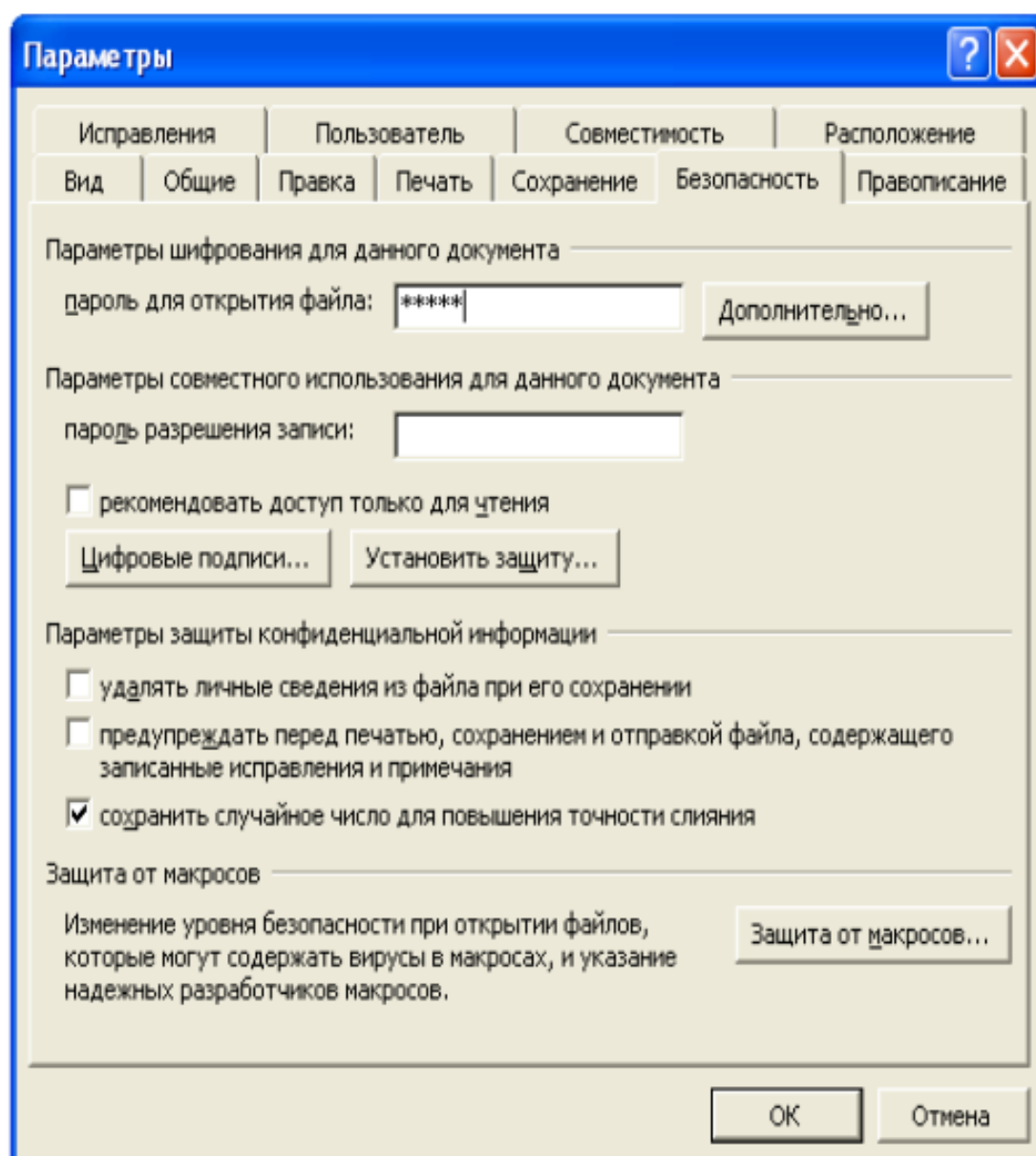
При совместной работе первый пользователь, который защитил файл или папку, управляет доступом остальных. Выполнив первоначальную процедуру защиты файла или папки, пользователь может указать дополнительных пользователей, щелкнув на кнопке «*Подробнее*».

Число добавляемых пользователей не ограничено. Каждый пользователь имеет собственный экземпляр *FEK*, зашифрованного с помощью его *EFS*-ключа. Пользователь обязан получить сертификат *EFS* перед тем, как его можно будет назначить дополнительным пользователем.

#### **8.6. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта;**

### **9. Начать работу с Microsoft Word из пакета Microsoft Office (версии XP или старше) или текстовым процессором из пакета Open Office. Освоить средства управления параметрами шифрования конфиденциальных документов (команда Сервис | Параметры, вкладка Безопасность, кнопка Дополнительно):**

Перейдём в вышеописанные настройки документа *Word*.



**Рисунок № 41 – параметры безопасности Word документа (Windows XP).**

Тут можно установить: пароль для доступа к файлу, пароль для разрешения изменения файла. Также для этих паролей можно выбрать тип шифрования при нажатии на кнопку “Дополнительно”:

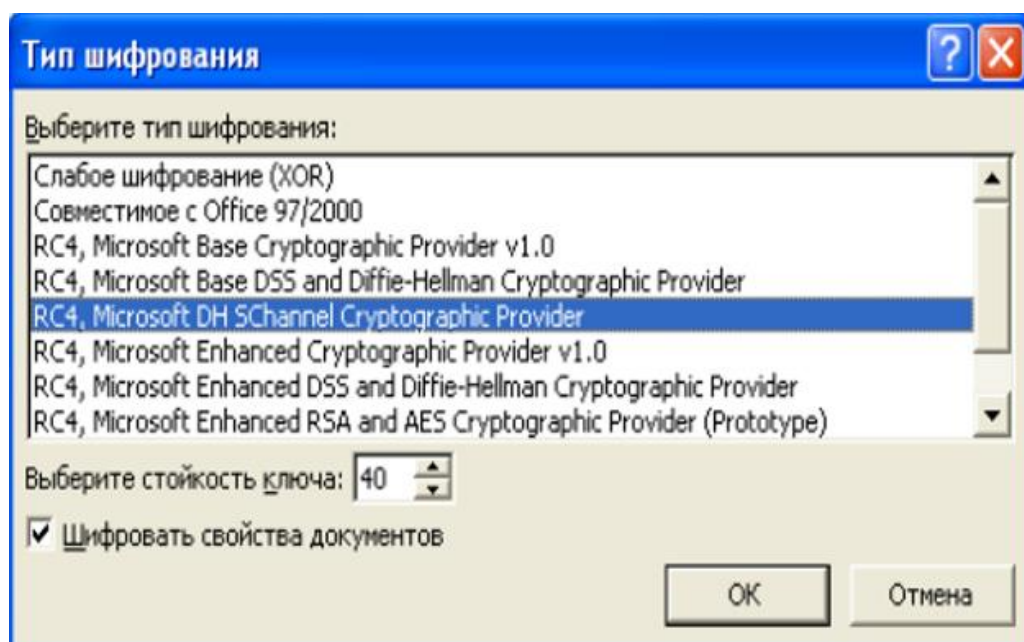
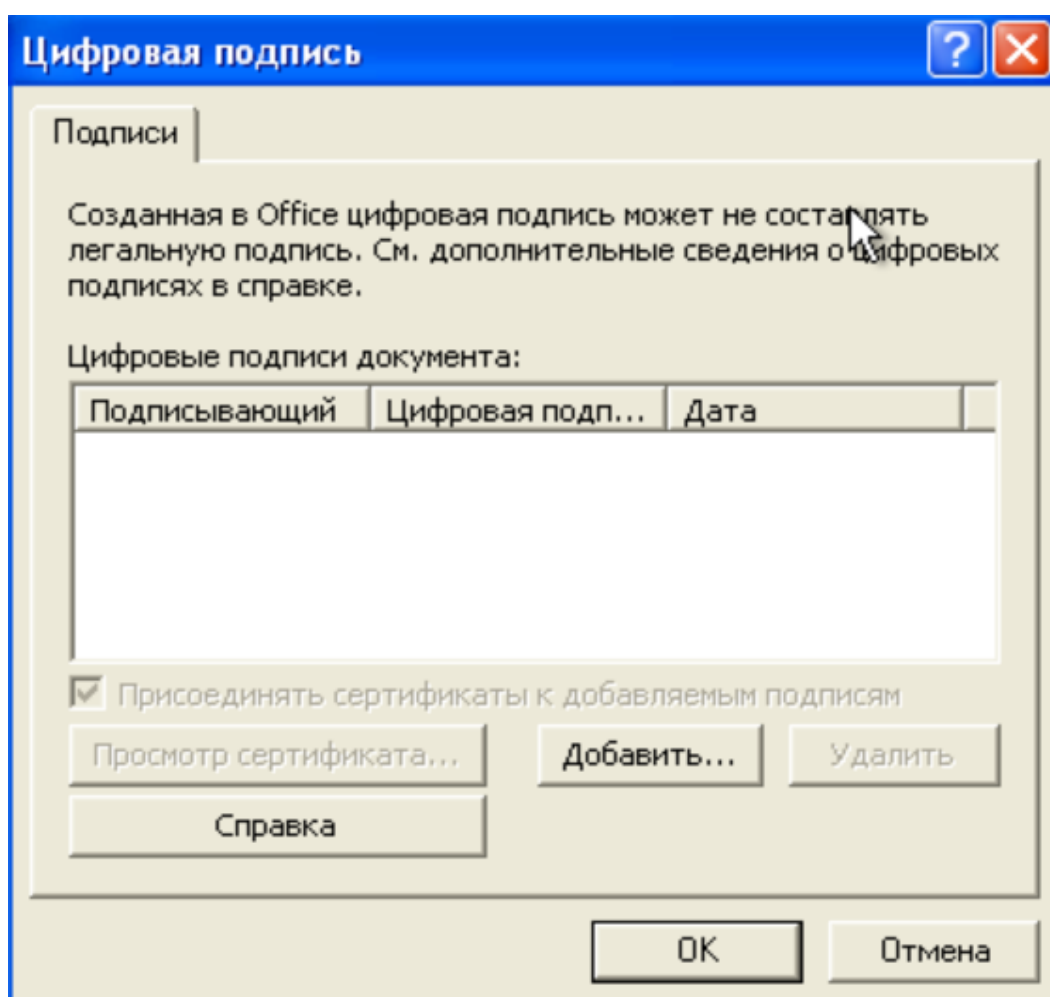


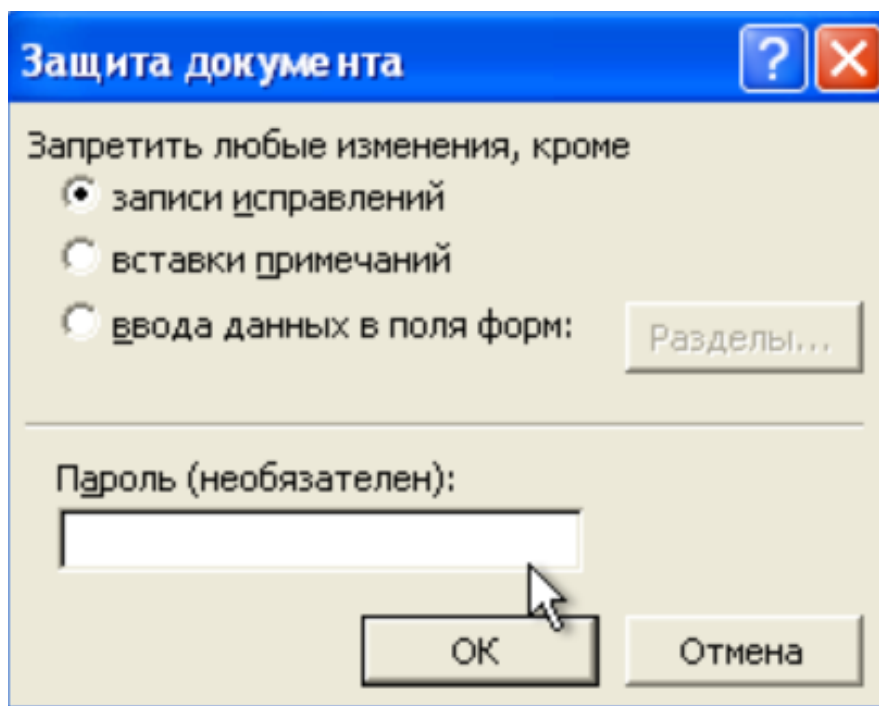
Рисунок № 42 – окно типов шифрования файлов (Windows XP).

Можно посмотреть список цифровых подписей при нажатии кнопки “Цифровые подписи...”, а также добавить/удалить цифровую подпись:



**Рисунок № 43 – окно работы с цифровыми подписями (Windows XP).**

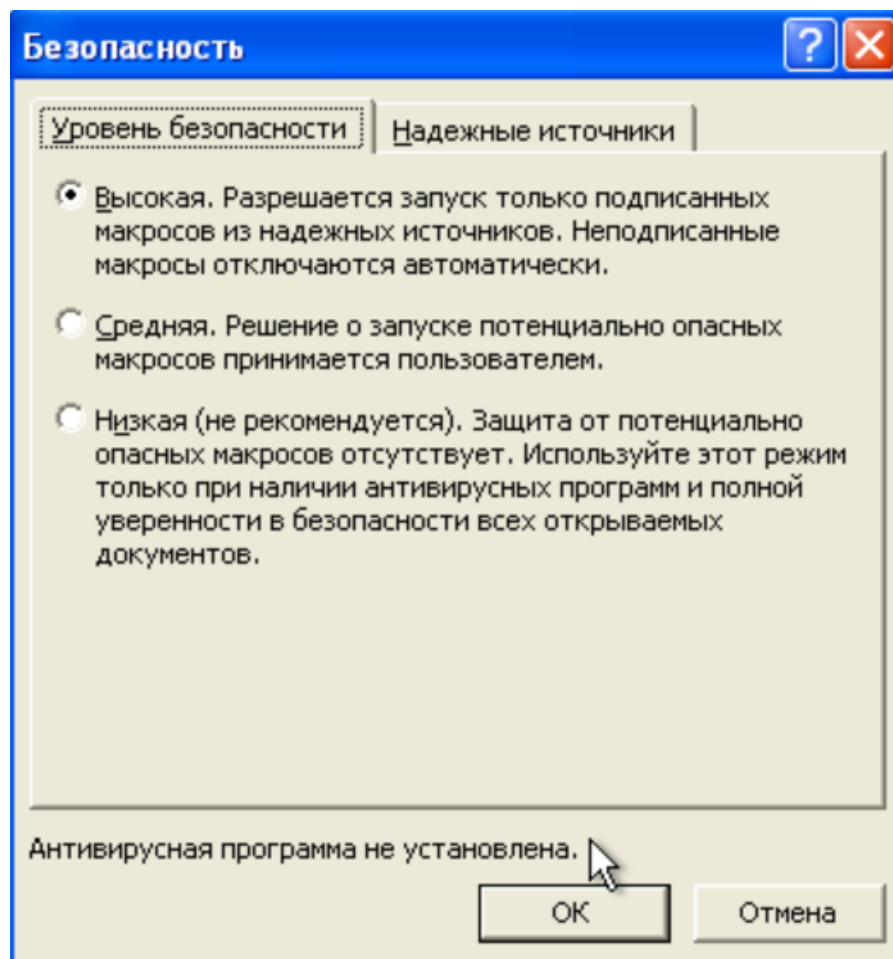
Также при нажатии на кнопку “Установить защиту” появится следующее окно, которое позволяет ставить пароль на определённый тип действий:



**Рисунок № 44 – окно защиты документа (Windows XP).**

Если нажать на клавишу “Защита от макросов...”, то можно задать степень безопасности файла, а также список надёжных источников для ресурсов:





**Рисунок № 45 – окно безопасности файла (Windows XP).**

**Включить в отчет ответы на вопросы:**

**9.1. Какие дополнительные параметры шифрования могут быть установлены:**

Защита: *раздела, страницы, документа*. Можно выбрать тип шифрования, задать стойкость ключа и указать шифровать ли свойства документа.

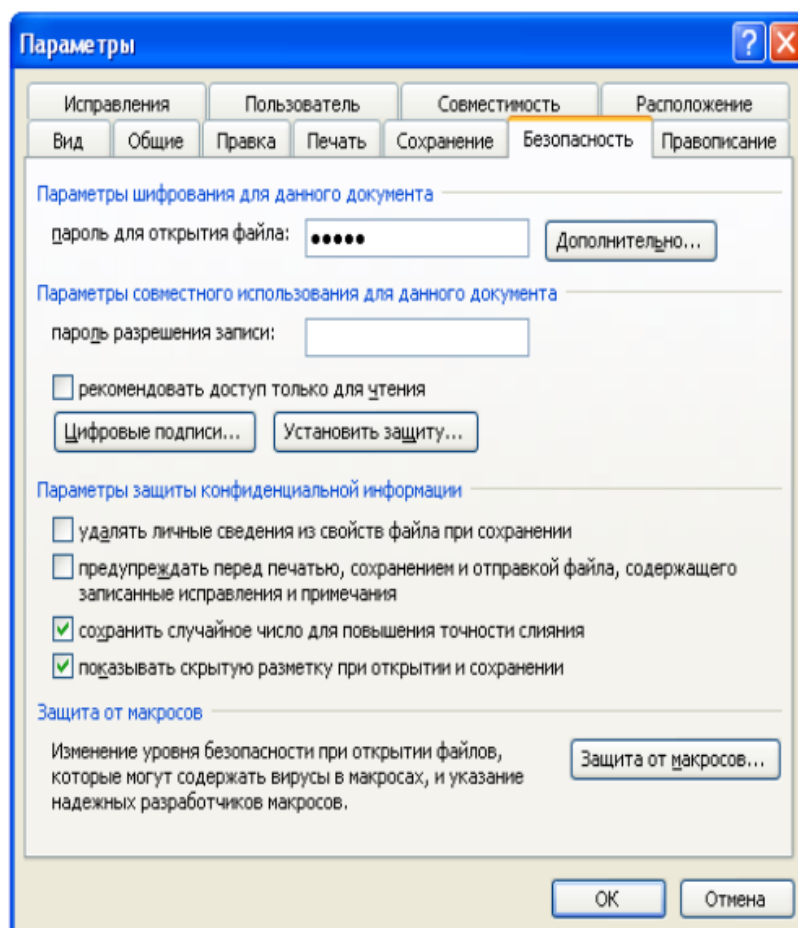
**9.2. От чего зависит список доступных типов шифрования и можно ли им управлять:**

По умолчанию есть встроенное шифрование, дополнительные надстройки можно скачать и установить. Список доступных типов шифрования зависит от версии MS Office.

**9.3. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта;**

**10. Повторить п. 9 для программы Microsoft Excel или табличного процессора из пакета Open Office. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта:**

Продедаем аналогичную работу для *Excel* файла:



**Рисунок № 46 – окно безопасности Excel файла (Windows XP).**

Можно заметить что функционал при работе с *Excel* файлами аналогичен с функционалом работы с *Word* файлами.

**Какие дополнительные параметры шифрования могут быть установлены:**

Защитить: ячейки, лист, структуру, книгу. Можно выбрать тип шифрования, задать стойкость ключа и указать шифровать ли свойства документа.

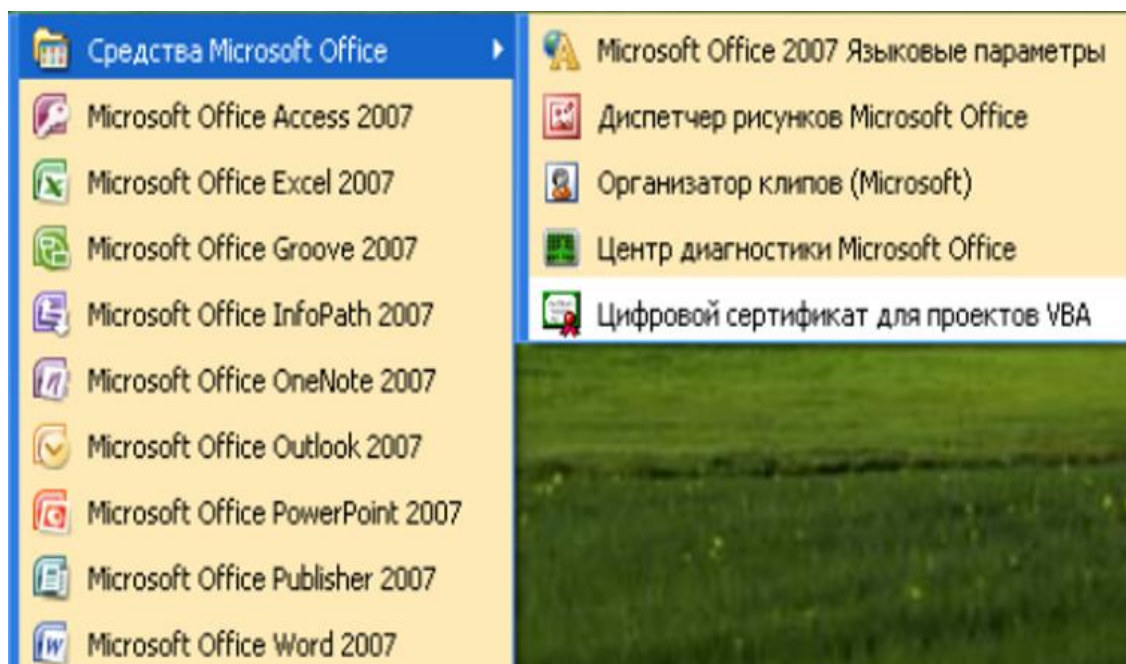
**От чего зависит список доступных типов шифрования и можно ли им управлять:**

По умолчанию есть встроенное шифрование, дополнительные надстройки можно скачать и установить, например, для шифрования.

Список доступных типов шифрования зависит от версии MS Office.

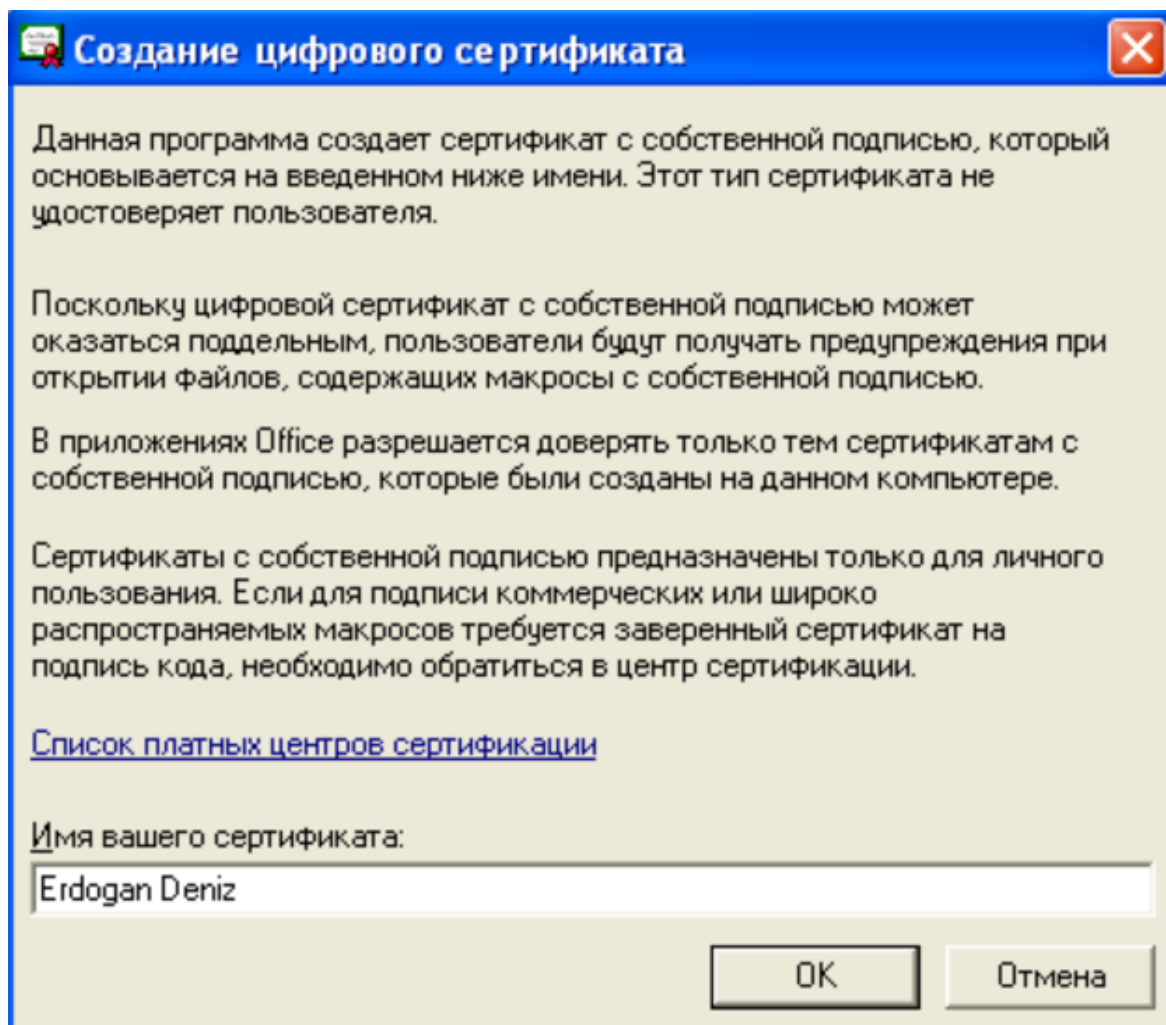
**11. С помощью программы selfcert.exe из пакета Microsoft Office (в версиях Office 2003 и старше вызов этой программы возможен через меню Пуск | Программы | Средства Microsoft Office | Цифровой сертификат) создать собственную пару ключей асимметричного шифрования и «самоподписанный» сертификат своего открытого ключа. Если эта программа не установлена, то создать самоподписанный сертификат с помощью утилиты makecert (makecert /r /n "cn=Фамилия И.О." /ss my), для вызова которой использовать командную строку Пуск | Программы | Microsoft Visual Studio | Visual Studio Tools | Visual Studio Command Prompt):**

Создадим цифровой сертификат с помощью программы *selfcert.exe* из пакета *Microsoft Office*. Для этого перейдём по следующему пути: *Пуск -> Все программы -> Microsoft Office -> Средства Microsoft Office -> Цифровой сертификат для проектов VBA*:



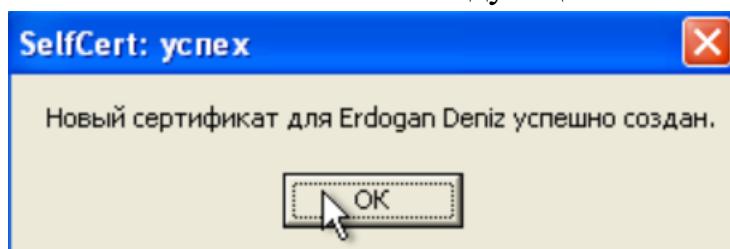
**Рисунок № 47 – подпункт создания цифрового сертификата для проектов VBA (Windows XP).**

Введём название нашего сертификата:



**Рисунок № 48 – окно ввода создаваемого сертификата (Windows XP).**

После нажатия кнопки “OK” появится следующее окно:



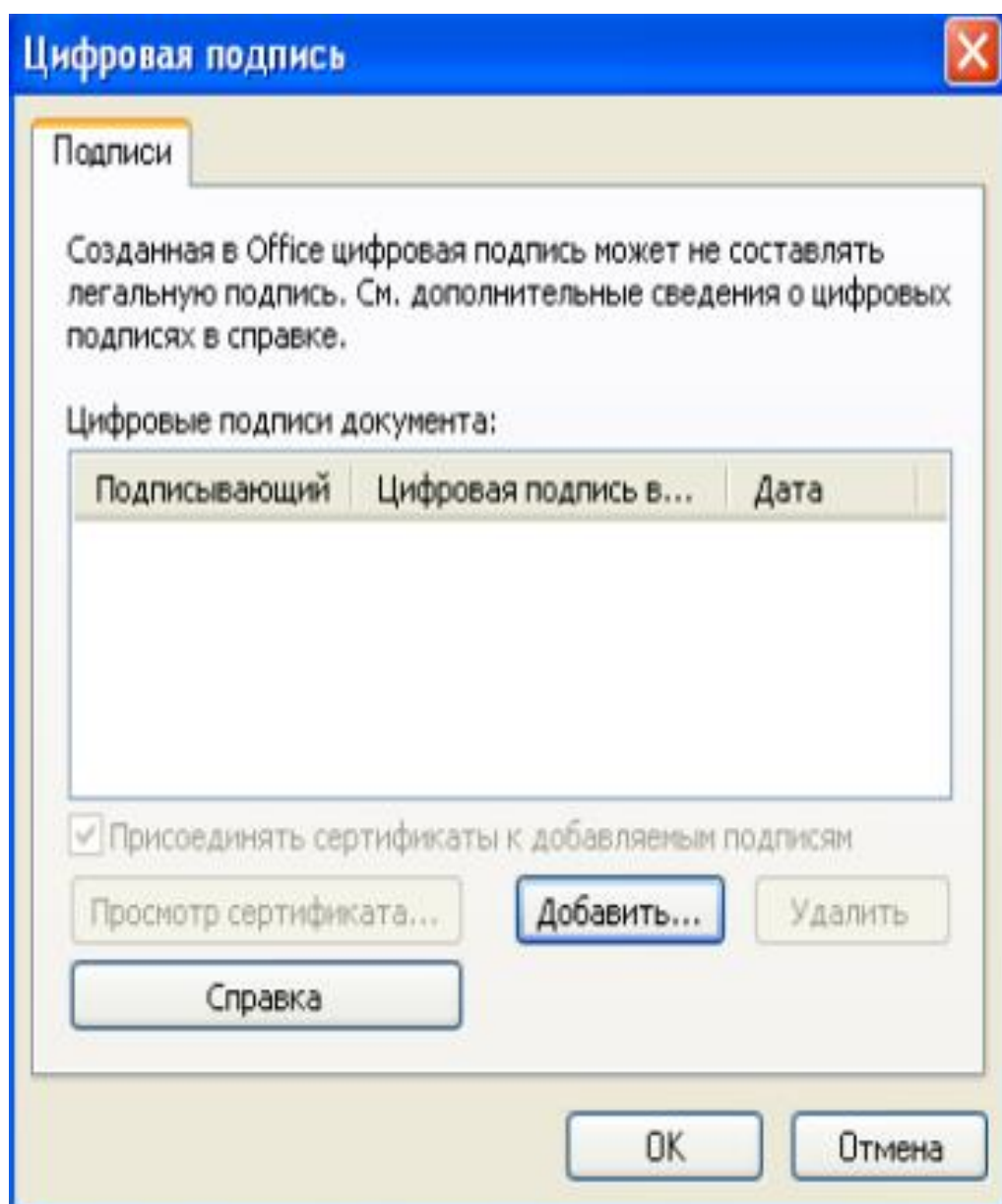
**Рисунок № 49 – сообщение об создании цифрового сертификата (Windows XP).**

**11.1. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта;**

**12. Освоить средства добавления электронной цифровой подписи к документам Microsoft Office (версии XP или старше) или Open Office на примере программы Microsoft Word (команда Сервис | Параметры, вкладка Безопасность, кнопки Цифровые подписи и Добавить) или текстового процессора Open Office. С помощью кнопки Просмотр сертификата ознакомиться с содержанием сертификата открытого ключа. Включить в отчет ответы на вопросы:**

В том же разделе, что и в предыдущем пункте рассмотрим цифровые подписи рисунок № 43.

Добавим цифровую подпись по созданному ранее сертификату:



**Рисунок № 50 – окно для создания цифрового сертификата (Windows XP).**

### 12.1. Какая информация содержится в сертификате открытого ключа:

Версия, серийный номер, алгоритм подписи, имя поставщика, сроки действия, имя пользователя, открытый ключ пользователя, улучшенный ключ, идентификатор ключа центра сертификатов, алгоритм отпечатка, отпечаток.

### 12.2. Что такое путь сертификации:

Путь сертификации – упорядоченная последовательность сертификатов в иерархическом каталоге, которая вместе с открытым ключом начального объекта пути позволяет получить сертификат окончательного объекта пути.

### 12.3. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта;

13. При работе в компьютерном классе университета пункты 13-15 выполняются в окне виртуальной ОС Windows XP. Скопировать в произвольную папку на локальном жестком диске файлы contrabd.zip и test.bmp из указанного преподавателем сетевого диска и извлечь файлы из архива contrabd.zip;

14. Запустить программу setup.exe для установки стеганографической программы Contraband:

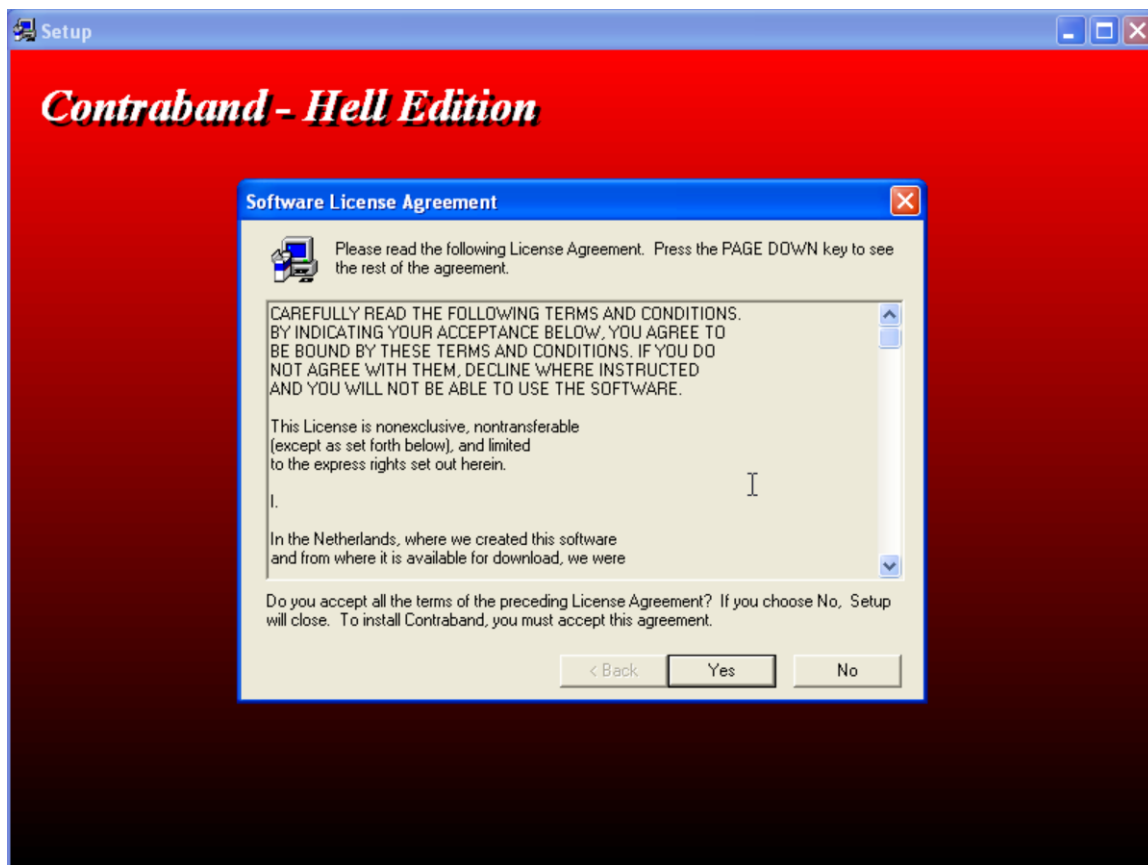




Рисунок № 51 – установка программы contrabd (Windows XP).

15. Запустить стеганографическую программу contrab.exe. На примере работы с произвольными файлами изучить функции программы и включить в электронную версию отчета копии экранных форм, полученных при использовании этой программы, после чего завершить работу с ней. В качестве файла-контейнера можно использовать файл test.bmp или произвольный графический файл в формате BMP:

Запустим программу.

Нас приветствует вкладка “About” дающая информацию о программе:

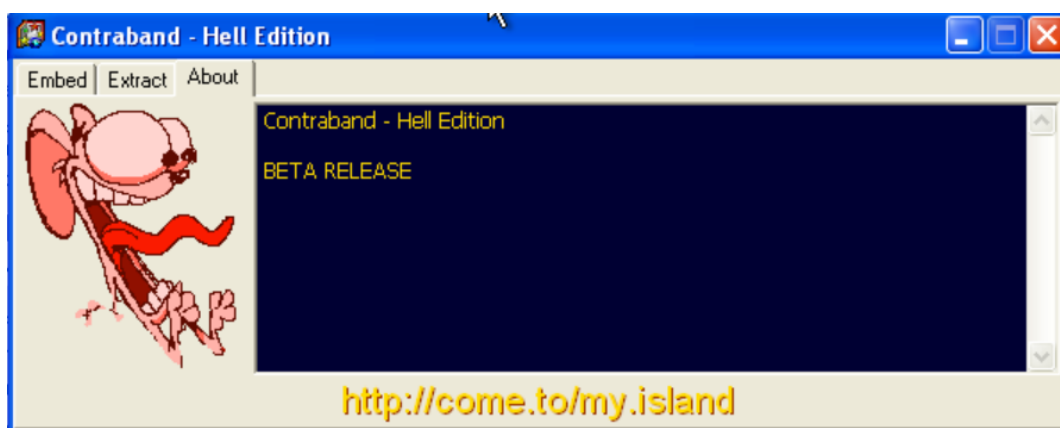
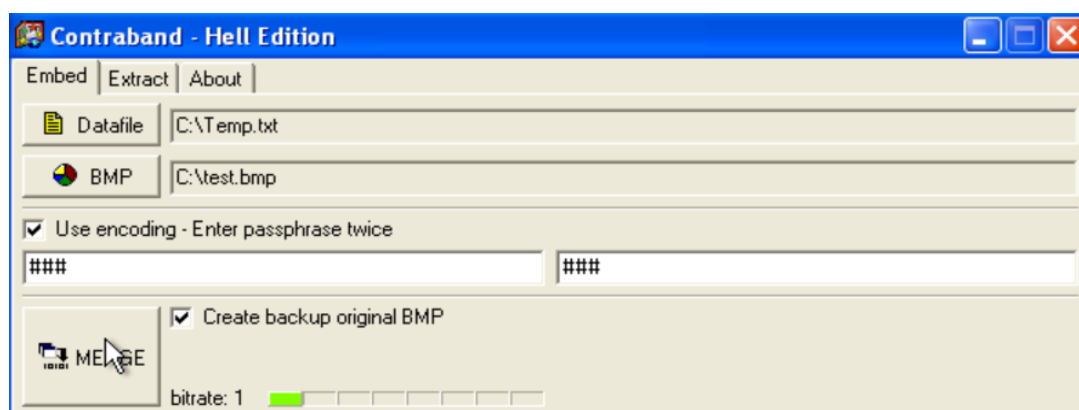


Рисунок № 52 – вкладка About программы contrabd (Windows XP).

Рассмотрим вкладку “Embed”.

Выберим файл, откуда будем брать информацию и файл формата \*.bmp, куда будем записывать информацию из выбранного файла. Также введём пароли для шифрования/дешифрования и создадим резервную копию исходного изображения нажав кнопку “MERGE”:



**Рисунок № 53 – записывание информации об файле в .bmp файл (Windows XP).**

После нажатия клавиши “*MERGE*” появляется следующие сообщение об успешном вложении информации в изображение:



**Рисунок № 54 – сообщение успешности вложения информации в изображение (Windows XP).**

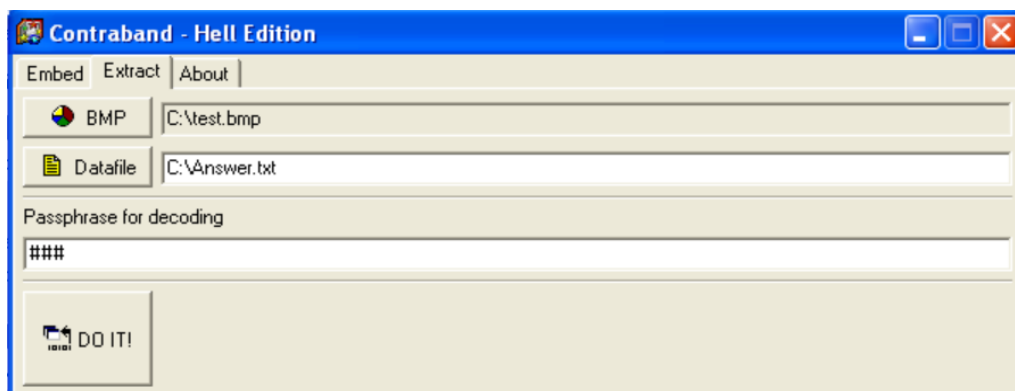
В итоге, получаем изображение с вложенной в него текстовой информацией и резервную копию исходного изображения:



**Рисунок № 55 – результат вышеописанной работы (Windows XP).**

Откроем вкладку “*Extract*”, выберем изображение с вложенной в него информацией, и выберем/создадим файл, куда запишется вложенная информация. После введём пароль и нажмём “*DO IT!*”:





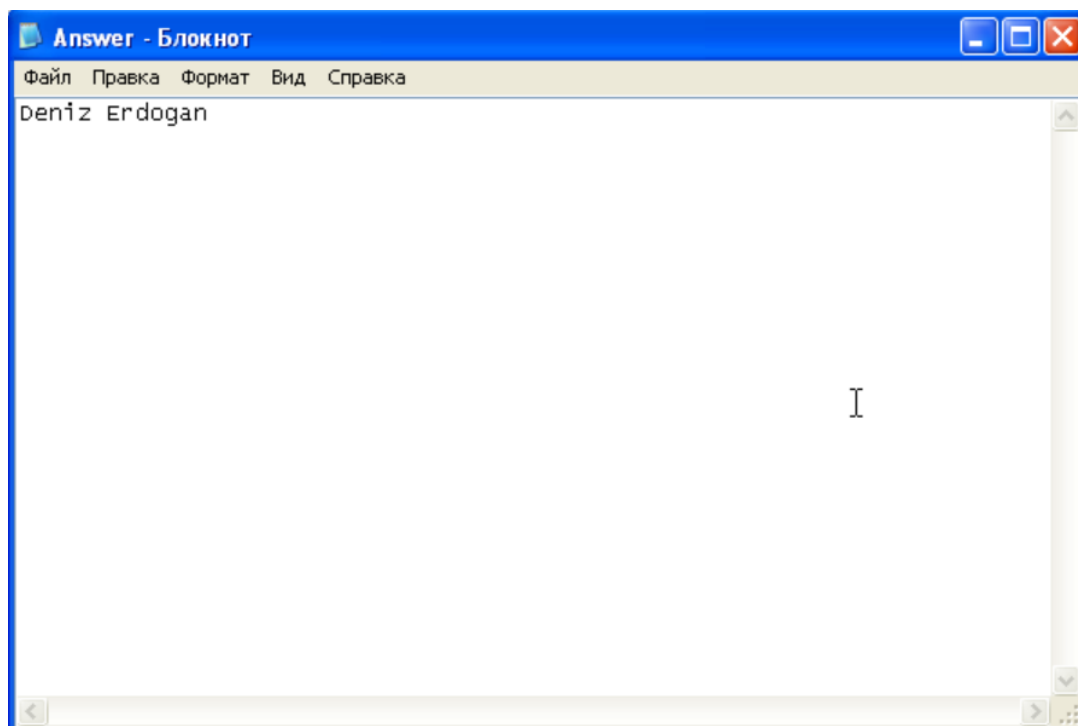
**Рисунок № 56 – окно получение вложенной ранее информации (Windows XP).**

При успешном получении информации из изображения, появится следующие сообщение:



**Рисунок № 57 – сообщение об успешности получения информации из картинки (Windows XP).**

В итоге получаем новый файл с текстовой информацией, которую мы получили из изображения:



**Рисунок № 58 – результат получения информации из изображения (Windows XP).**

**Включить в отчет ответы на вопросы:**

**15.1. Как происходит скрытие и извлечение сообщений из контейнеров:**

**Стегосистема** – это совокупность средств и методов, осуществляющих внедрение сообщения внутрь контейнера, а также извлечение этого сообщения из контейнера. Данный алгоритм заменяет наименее значимый бит в нескольких байтах файла-носителя, чтобы скрыть последовательность байтов, содержащих скрытые данные. Для человека подобные изменения визуально неотличимы, что позволяет передавать скрытые сообщения в безобидном, на первый взгляд, изображении.

**15.2. В чем разница между методами криптографии и стеганографии:**

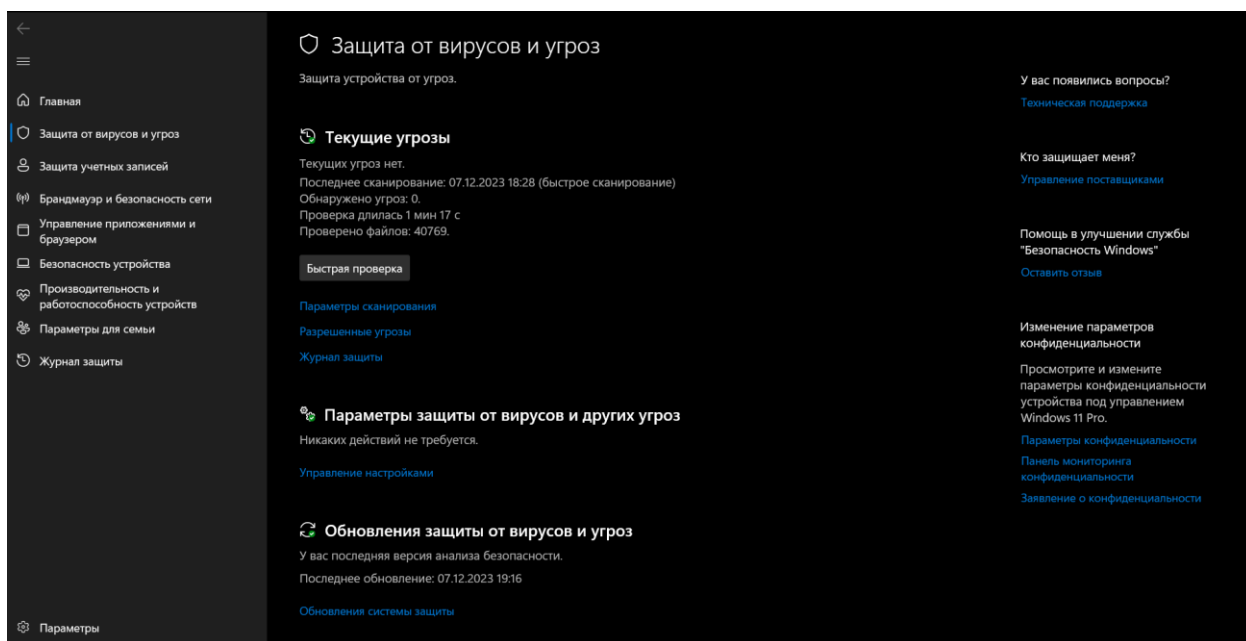
**Криптография** – это совокупность методов для шифрования передаваемого сообщения. **Стеганография** – это метод скрытия самого факта наличия, скрытого в отправляемом сообщении.

**15.3. Каким должно быть соотношение между размерами файла-контейнера и файласообщения при использовании программы contrab.exe и почему:**

Размер файла-сообщения должен быть в несколько раз меньше, чем размер файла-контейнера. Для увеличения скрытости указанное соотношение должно быть как можно большим.

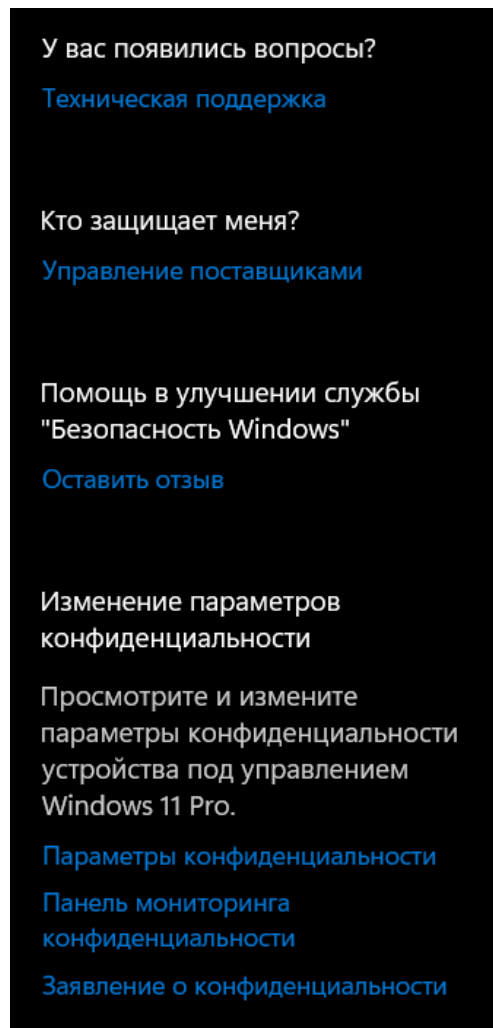
**16. Запустить установленную в системе программу антивирусного сканирования и освоить работу с ней. Включить в электронную версию отчета о выполнении лабораторной работы копии экранных форм, полученных при использовании этой программы. Включить в отчет о лабораторной работе:**

Нажмём “Win + I”, выберим “Обновление и безопасность” -> “Безопасность Windows” -> “Открыть службу Безопасность Windows” -> “Защита от вирусов и угроз”:



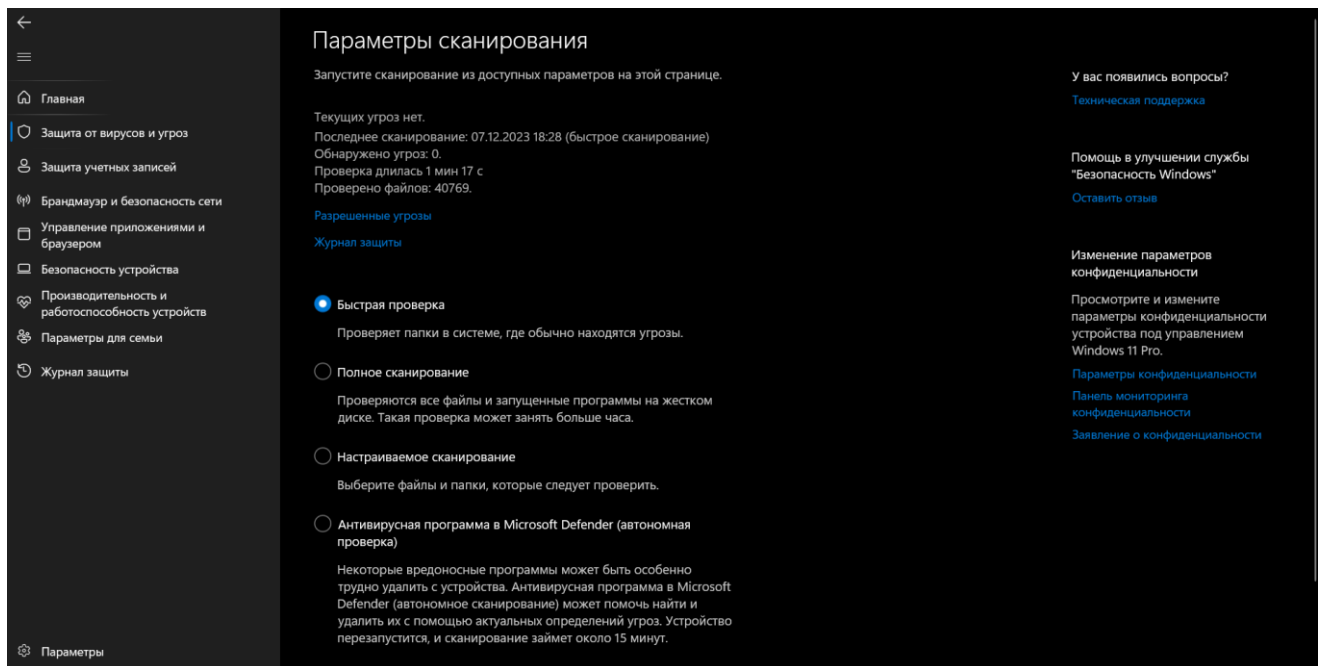
**Рисунок № 59 – разделы системы Защита от вирусов и угроз (Windows 11).**

Справо представлена вспомогательная информация о программе:



**Рисунок № 60 – вспомогательная информация о системном антивирусе (Windows 11).**

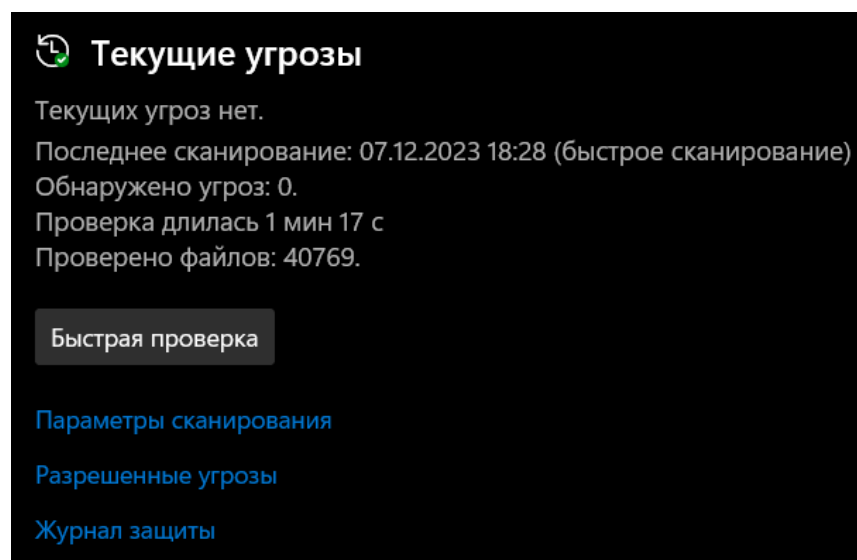
Выбрав “*Параметры сканирования*”, можно настроить область сканирования и задать объекты проверки на наличие вирусов:



**Рисунок № 61 – параметры сканирования вирусов (Windows 11).**

Основные разделы:

- “*Текущие угрозы*”, в котором можно проверить файлы на наличие вирусов:



**Рисунок № 62 – раздел Текущие угрозы (Windows 11).**

Дополнительные пункты:

- “*Параметры сканирования*” – раздел, где можно настроить быструю проверку вирусов:

## Параметры сканирования

Запустите сканирование из доступных параметров на этой странице.

Текущих угроз нет.

Последнее сканирование: 07.12.2023 23:38 (быстрое сканирование)

Обнаружено угроз: 0.

Проверка длилась 1 мин 3 с

Проверено файлов: 19634.

[Разрешенные угрозы](#)

[Журнал защиты](#)

☒ Быстрая проверка

Проверяет папки в системе, где обычно находятся угрозы.

☐ Полное сканирование

Проверяются все файлы и запущенные программы на жестком диске. Такая проверка может занять больше часа.

☐ Настраиваемое сканирование

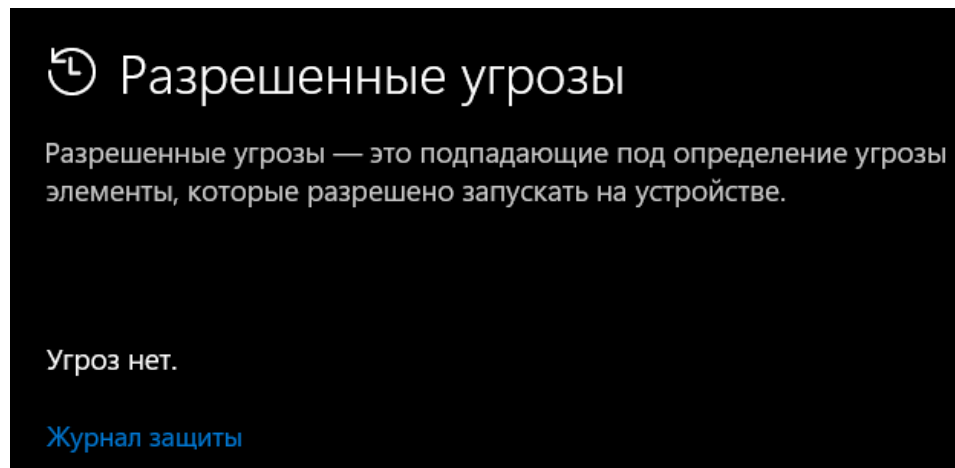
Выберите файлы и папки, которые следует проверить.

☐ Антивирусная программа в Microsoft Defender (автономная проверка)

Некоторые вредоносные программы может быть особенно трудно удалить с устройства. Антивирусная программа в Microsoft Defender (автономное сканирование) может помочь найти и удалить их с помощью актуальных определений угроз. Устройство перезапустится, и сканирование займет около 15 минут.

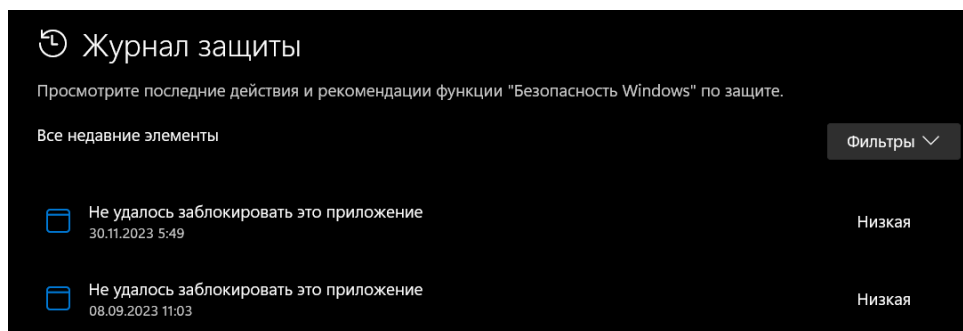
Рисунок № 63 – подраздел Параметры сканирования (Windows 11).

- “Разрешённые угрозы” – список игнорируемых угроз:



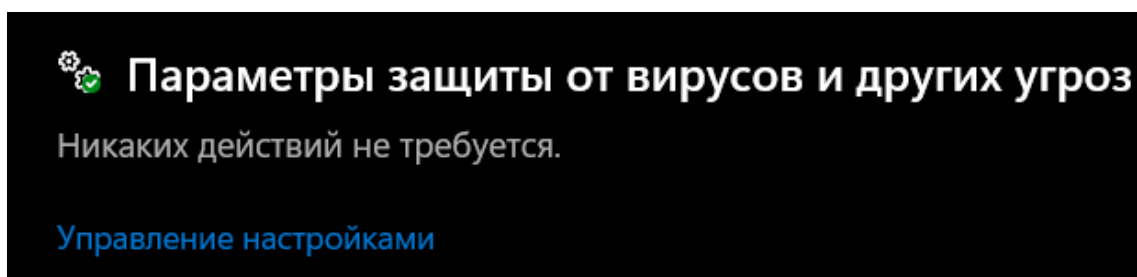
**Рисунок № 64 – подраздел Разрешённые угрозы (Windows 11).**

- “Журнал защиты” – журнал проверок на вирусы:



**Рисунок № 65 – подраздел Журнал защиты (Windows 11).**

- “Параметры защиты от вирусов и других угроз” – раздел для настройки защиты от вирусов ОС Windows 11:



**Рисунок № 66 – раздел Параметры защиты от вирусов и других угроз (Windows 11).**

Подразделы:

- “Управление настройками”:

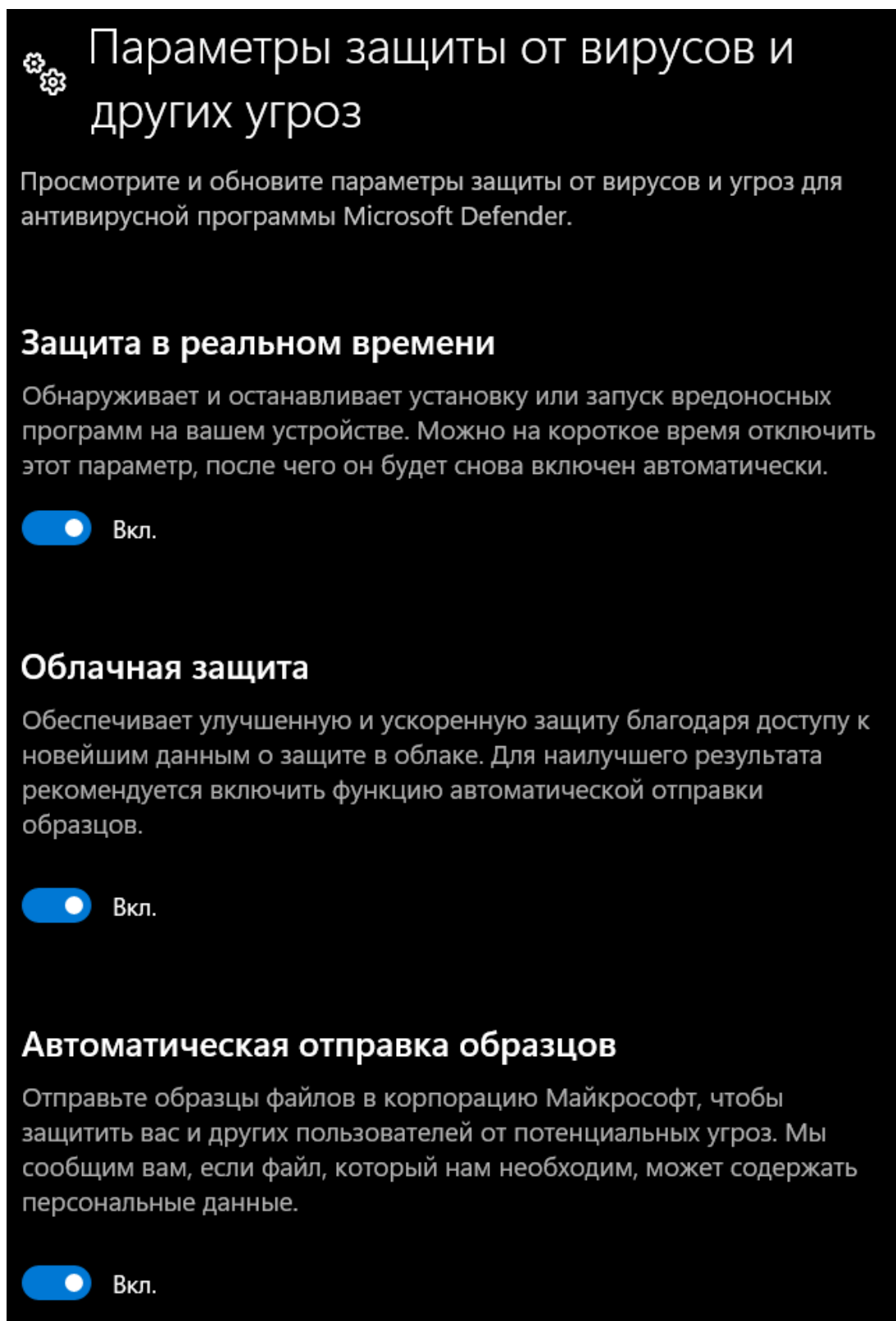


Рисунок № 67 – подраздел Параметры защиты от вирусов и других угроз (Windows 11).



- “Обновления защиты от вирусов и угроз”:

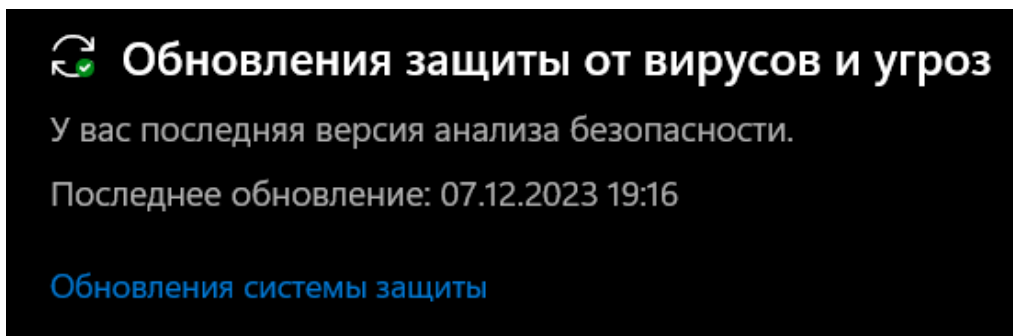


Рисунок № 68 – раздел Обновления защиты от вирусов и угроз (Windows 11).

Подпункты:

- “Обновления системы защиты”:

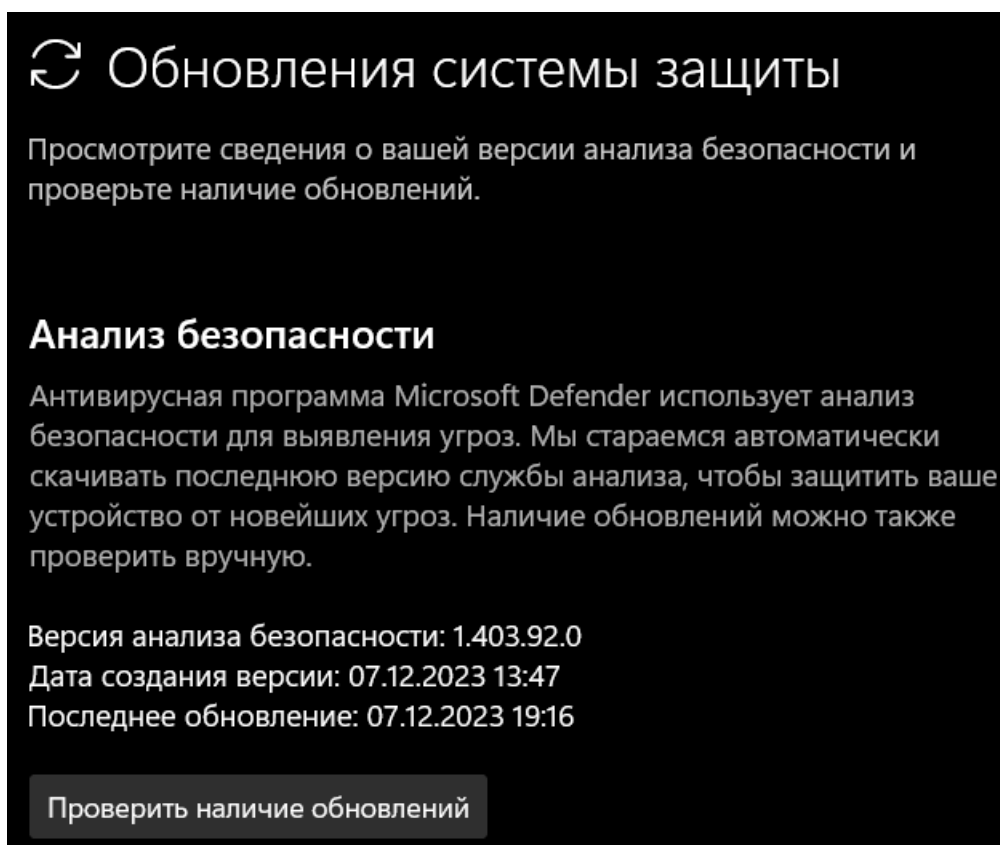
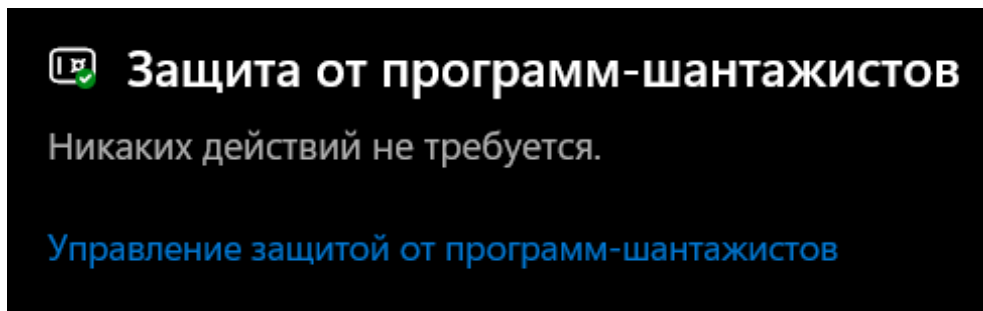


Рисунок № 69 – подраздел Обновления системы защиты (Windows 11).

- “Защита от программ-шантажистов”:



**Рисунок № 70 – подпункт Защита от программ-шантажистов (Windows 11).**

Подпункты:

- “Управление защитой от программ-шантажистов”:



**Рисунок № 71 – подраздел Защита от программ-шантажистов (Windows 11).**

**16.1. Сведения о назначении и основных функциях программы, а также ответы на вопросы:**

**16.2. Как задаются области сканирования:**

“Параметры сканирования” -> “Настраиваемое сканирование”.

**16.3. Как задаются объекты проверки на наличие вирусов:**

*“Параметры сканирования” -> “Настраиваемое сканирование”, а также с помощью настройки “Исключений” можно выбрать те объекты, которые не будут учувствовать в проверки на наличие вирусов.*

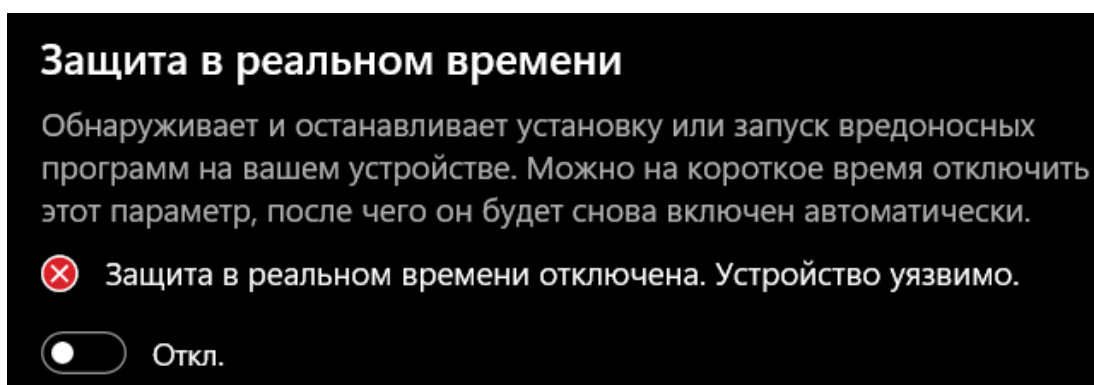
#### **16.4. Как определяется реакция сканера в случае обнаружения зараженного файла:**

При обнаружении заражённого появляется соответствующее предупреждение с выбором вариантов действий с данным файлом.

**Завершить работу с программой;**

#### **17. Проверить, обеспечена ли в системе возможность автоматического запуска (после загрузки Windows) антивирусной программы-монитора:**

Для включения антивирусной программы-мониторинга нужно в разделе *“Параметры защиты от вирусов и угроз”* включить *“Защиту в режиме реального времени”*:



**Рисунок № 72 – функция Защита в реальном времени (Windows 11).**

**Включить в отчет ответы на вопросы:**

#### **17.1. В чем разница в назначении антивирусных программ-сканеров и программмониторов:**

Антивирусный сканер проверяет по требованию, т.е. когда пожелает пользователь, тогда он и запустит проверку. Также сканер может проверять все файлы на всех дисках или на выбранных, любые файлы, осуществлять углублённую проверку, которая сильно нагружает центральный процессор и память.

Монитор всё время в оперативной памяти компьютера проверяет все обращения к файлам и веб-адресам и следит за иной активностью системы и

программ. Часть сложных проверок он не осуществляет, чтобы не тормозить компьютер, а выполняет лишь базовые необходимые и достаточные проверки, которые обеспечивают достаточный уровень безопасности. Кроме того, монитор запускается при старте системы.

## **17.2. Как может быть обеспечена возможность автоматического запуска программ антивирусного мониторинга:**

Достаточно поместить ссылку на программу в каталог автозагрузки и эта программа будет запускаться при каждом входе пользователя в систему.

Чтобы открыть папку “*АВТОЗАГРУЗКА*”, достаточно открыть каталог: “%userprofile%\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup” (ссылки на программы, запускаемые только при входе текущего пользователя);

открыть каталог: “%programdata%\Microsoft\Windows\Start Menu\Programs\Startup” (ссылки на программы, запускаемые при входе любого пользователя).

**18. Начать работу с Microsoft Word или текстовым процессором пакета Open Office. Включить средства защиты от вирусов в макросах в документах Word или Open Office. Освоить использование других рассмотренных на лекциях средств защиты от вирусов в макросах (для проверки их эффективности создать новый документ с собственными автоматически выполняемыми и (или) стандартными макросами, используя в них строку с вызовом макрокоманды вывода сообщения MsgBox “Текст сообщения”). Завершить работу с Word.**

В *MS Word* есть четыре уровня безопасности защиты от макровирусов, чтобы выбрать нужный уровень надо зайти в раздел: “Сервис” -> “Макрос” -> “Безопасность”.

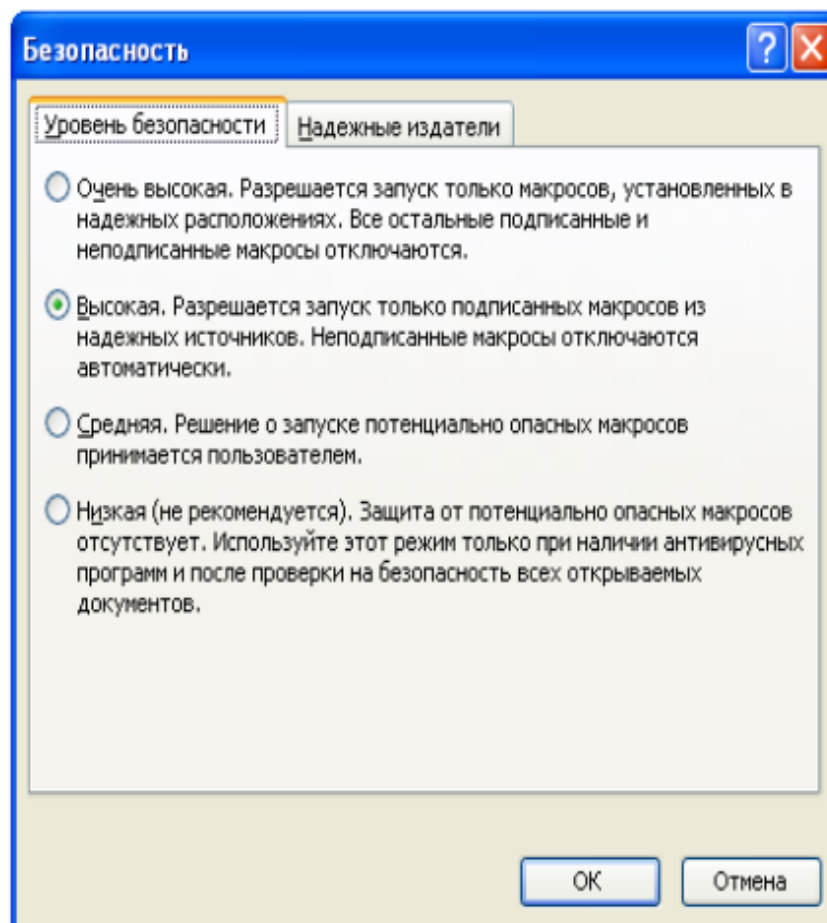


Рисунок № 73 – раздел Безопасность (Windows XP).

В *MS Excel* также есть четыре уровня безопасности защиты от макровирусов аналогичные рисунку № 73.

**18.1. Включить в отчет сведения о способах защиты от вирусов в документах Word;**

**18.2. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта;**

**19. Повторить п. 18 для программы Microsoft Excel или табличного процессора из пакета Open Office. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта;**

**20. Освоить средства добавления электронной цифровой подписи к макросам, включаемым в состав документов Microsoft Office версии XP или старше (на примере программы Microsoft Word) или пакета Open Office: добавить в документ автоматически выполняющийся макрос**

(команда Сервис | Макрос | Макросы) и воспользоваться командой Редактора Visual Basic Tools | Digital Signature:

Добавим в документ автоматически выполняющийся макрос. Для это перейдём по следующему пути: “Сервис” -> “Макрос” -> “Макросы” или нажмём сочетание клавиш “Alt + F8”. В появившемся окне введём имя “Autoopen” и нажмём “Создать”:

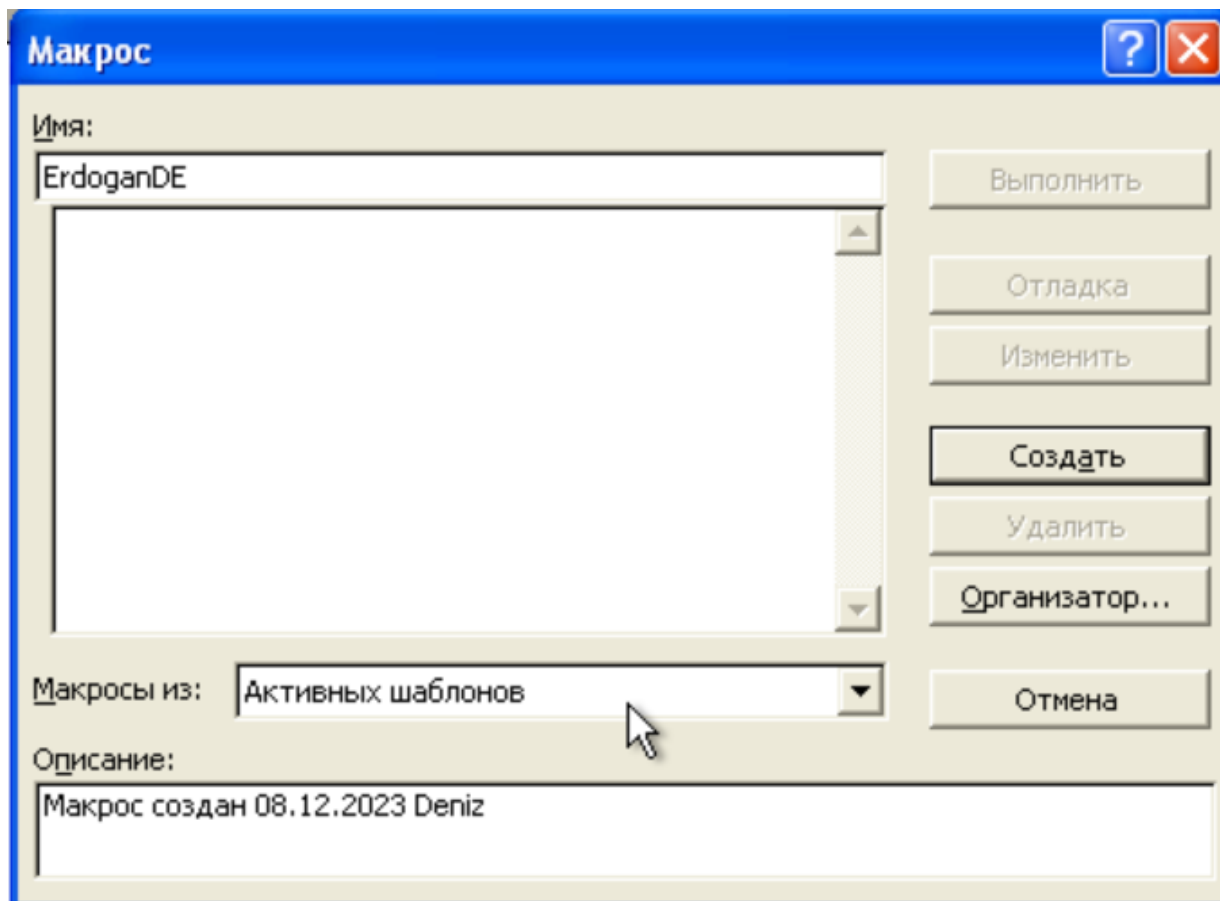
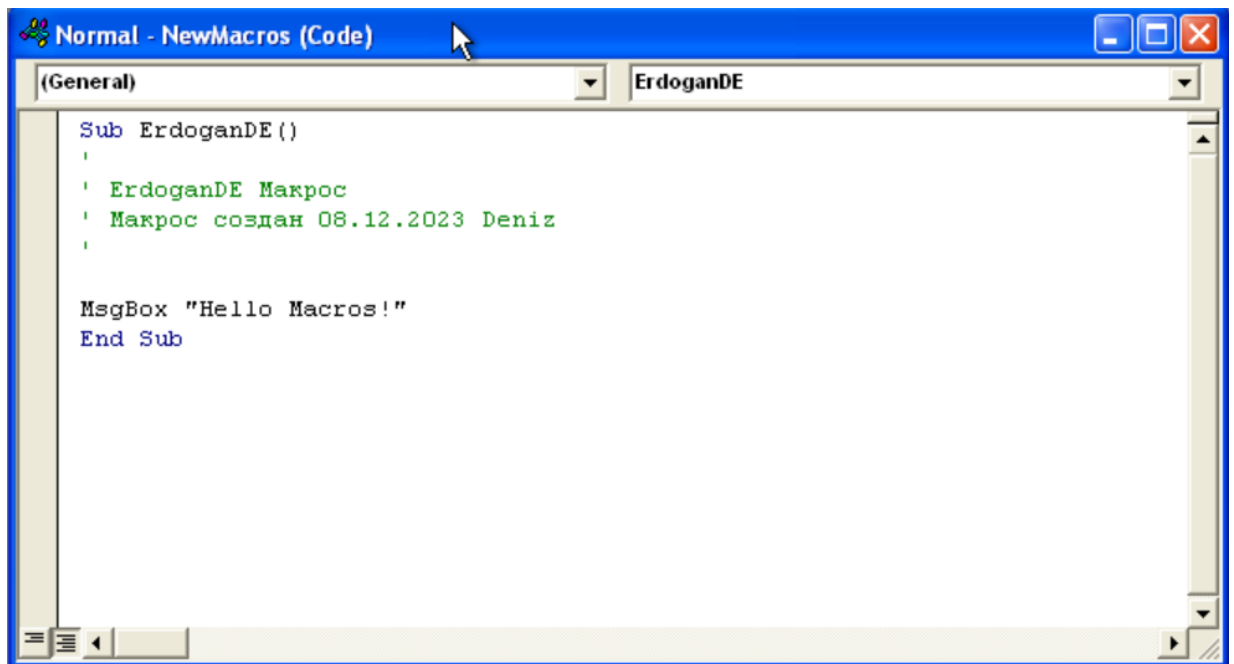


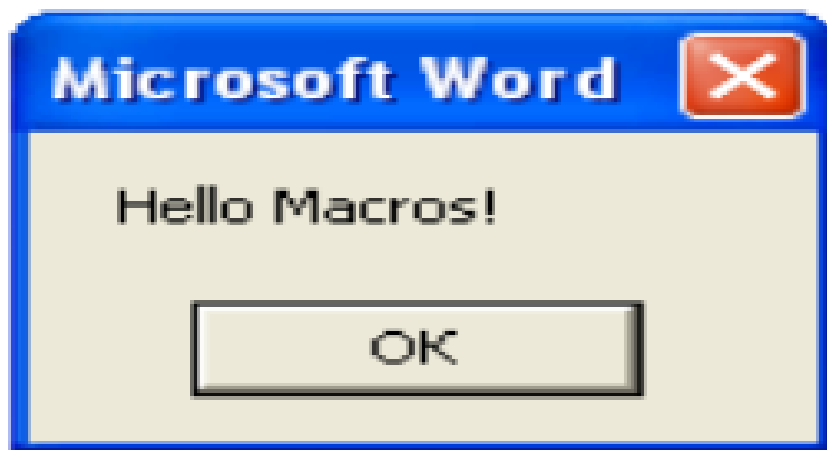
Рисунок № 74 – окно Макрос (Windows XP).

В окне редактора VB допишем строку Msg “Hello Macros!” (вывод текстового сообщения на экран):



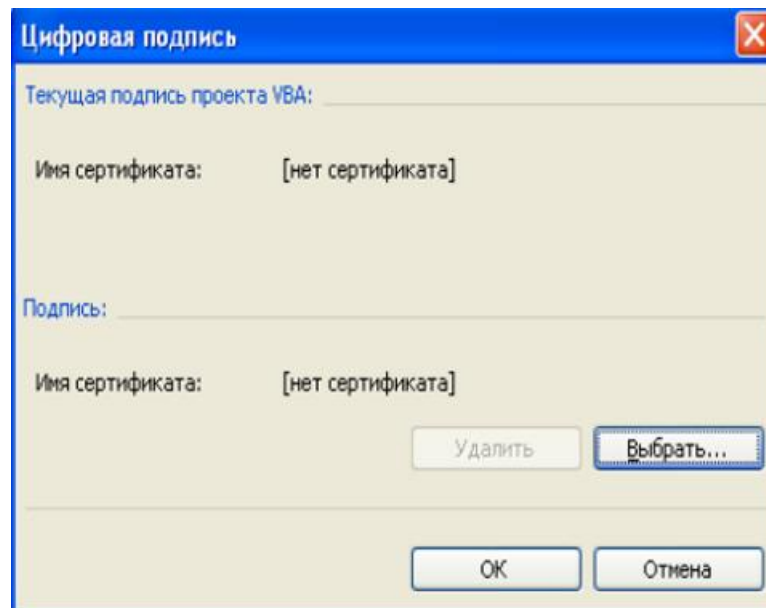
**Рисунок № 75 – код макроса (Windows XP).**

Закроем редактор *VB* и закроем документ с сохранением. При повторном запуске появится следующее сообщение:



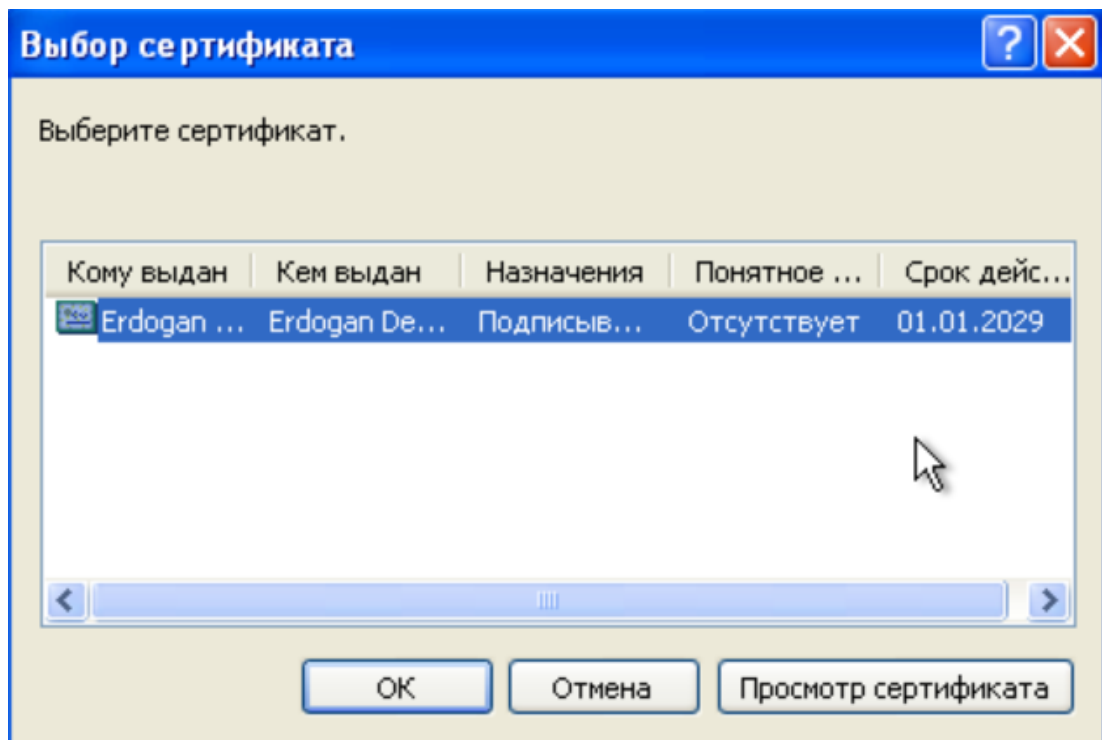
**Рисунок № 76 – сообщение от макроса (Windows XP).**

Снова зайдём в редактор *VB* и перейдём по следующему пути “*Tools*” -> “*Digital Signature*” в разделе добавления цифровой подписи:



**Рисунок № 77 – окно Цифровая подпись (Windows XP).**

Нажмём «*Выбрать*» и в появившемся окне выберем созданный ранее цифровой сертификат:



**Рисунок № 78 – выбор ранее созданного сертификата (Windows XP).**



В результате мы увидим:

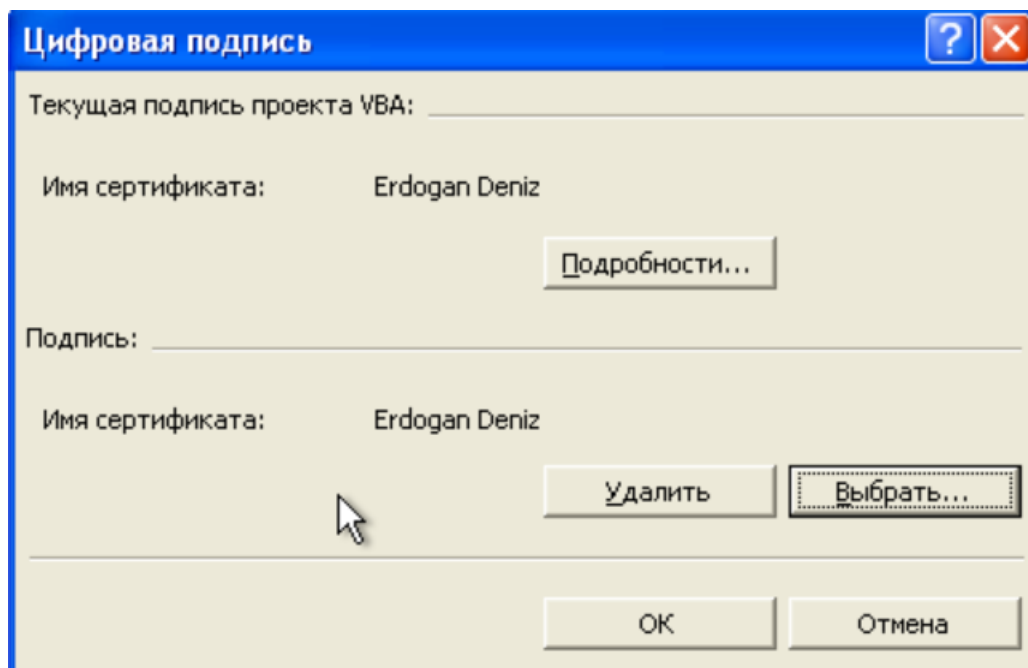


Рисунок № 79 – результат выбора (Windows XP).

**20.1. Включить в отчет ответ на вопрос, что произойдет после внесения изменений в документ, снабженный электронной цифровой подписью:**

После внесения изменений в документ, снабженный электронной цифровой подписью, все цифровые подписи удаляются.

**20.2. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта;**

**21. Включить в отчет титульный лист и сохранить файл с электронной версией отчета в произвольной папке на локальном жестком диске;**

**22. Предъявить преподавателю электронную версию отчета о лабораторной работе с копиями использовавшихся экранных форм и соответствующими им номерами пунктов задания (3, 7, 8.6, 9.3, 10, 11.1, 12.3, 15, 16, 18.2, 19, 20.2);**

**23. После проверки электронной версии отчета о выполнении лабораторной работы преподавателем удалить файл с отчетом о лабораторной работе и файлы программы MyOldSafe. Удалить программы Citadel Safstor и Contraband с помощью Панели управления Windows. Удалить файлы архивов mosafe21.exe, citadel.zip и contrabd.zip, а также файл test.bmp;**

**24. Включить в отчет ответы на контрольные вопросы, номера которых выбираются в соответствии с номером варианта:**

**Какие симметричные криптосистемы наиболее распространены в настоящее время:**

Наиболее распространены в настоящее время следующие симметричные криптосистемы:

- AES (Advanced Encryption Standard) – самый популярный симметричный алгоритм, использующийся для шифрования данных. Он используется во множестве приложений, включая защиту информации в банковских системах, коммуникации, облачных сервисах и других;
- DES (Data Encryption Standard) – один из первых симметричных алгоритмов шифрования. В настоящее время он менее распространен из-за ограниченной длины ключа (56 бит), что делает его уязвимым к атакам перебора;
- 3DES (Triple Data Encryption Standard) – улучшенная версия DES, которая использует три этапа шифрования для повышения уровня безопасности. Однако его использование также уменьшается в связи с наличием более современных алгоритмов;
- Blowfish – алгоритм, разработанный для замены DES. Он позволяет использовать ключи длиной от 32 до 448 бит, что делает его более безопасным по сравнению с DES. Однако Blowfish также становится менее популярным из-за развития более мощных алгоритмов;
- Twofish – алгоритм, основанный на Blowfish, который разработан как конкурент AES. Он также позволяет использовать длинные ключи и обеспечивает высокий уровень безопасности;
- IDEA (International Data Encryption Algorithm) – алгоритм, который широко используется в коммерческих продуктах и протоколах связи. IDEA обладает высоким уровнем безопасности благодаря использованию 128-битных ключей.

**Что такое сертификат открытого ключа и для чего он применяется:**

**Сертификат открытого ключа** - это цифровой документ, используемый в системе шифрования информации для идентификации открытого ключа. **Открытый ключ** - это часть ключевой пары (открытый и закрытый ключи), которая используется для шифрования данных, отправляемых пользователем.

Сертификат открытого ключа применяется для следующих целей:

- Идентификация: Сертификат содержит информацию об открытом ключе, такую как его владелец, срок действия и другие атрибуты. Это позволяет получателю определить, соответствует ли открытый ключ

отправителя заявленной личности;

- Проверка подлинности: Сертификат может быть подписан доверенным центром сертификации (СА), что подтверждает его подлинность и гарантирует, что открытый ключ действительно принадлежит указанному владельцу;
- Хэш-функция: Сертификат также содержит хэш-значение открытого ключа, что позволяет проверить его целостность при получении;
- Цифровая подпись: Сертификат открытого ключа может использоваться для создания цифровой подписи, которая позволяет подтвердить авторство и целостность сообщения;
- Шифрование: Сертификат открытого ключа используется для обмена данными с использованием асимметричного шифрования. Данные шифруются с помощью открытого ключа получателя, а затем расшифровываются с использованием его закрытого ключа.

### **В чем сущность методов компьютерной стеганографии:**

Сущность методов компьютерной стеганографии заключается в сокрытии конфиденциальной информации (скрытых данных) внутри обычных цифровых объектов, таких как изображения, аудиофайлы, видеофайлы и документы. Скрытые данные могут включать в себя секретные сообщения, ключи шифрования, цифровые подписи и другие конфиденциальные данные.

Методы компьютерной стеганографии используют различные алгоритмы и техники для встраивания скрытых данных в цифровые объекты таким образом, чтобы эти данные оставались невидимыми и недоступными для посторонних. Они также могут использовать методы криптографии для защиты скрытых данных от несанкционированного доступа.

Одним из основных преимуществ компьютерной стеганографии является то, что она позволяет скрывать конфиденциальную информацию внутри обычных цифровых объектов, которые не вызывают подозрений у посторонних. Это делает ее идеальным инструментом для передачи секретных сообщений и другой конфиденциальной информации в условиях, когда традиционные методы шифрования могут быть обнаружены или заблокированы.

### **Для чего могут применяться методы компьютерной стеганографии:**

Методы компьютерной стеганографии могут применяться в различных областях, где требуется скрытая передача или хранение конфиденциальной информации.

Некоторые из этих областей включают:

- Секретные сообщения: Скрытая передача секретных сообщений между агентами или организациями;
- Защита авторских прав: Встраивание цифровых водяных знаков в

аудио- и видеофайлы для защиты авторских прав и предотвращения пиратства;

- Цифровые подписи: Встраивание цифровой подписи в изображение или документ для подтверждения авторства и целостности данных;

- Криптография: Использование стеганографии для скрытой передачи ключей шифрования между участниками сети;

- Шпионаж и разведка: Скрытая передача конфиденциальной информации между агентами разведки или шпионами;

- Противодействие шпионажу и кибербезопасности: Встраивание скрытых маркеров или цифровых водяных знаков в данные для обнаружения неавторизованного доступа или изменения данных.

### **В чем опасность вирусов в макросах электронных документов:**

Опасность вирусов в макросах электронных документов заключается в их способности выполнять вредоносные действия на компьютере пользователя.

Вот некоторые примеры опасных действий, которые могут быть выполнены вирусами в макросах:

**Распространение:** Вирус может использовать адресную книгу или список контактов пользователя, чтобы автоматически отправлять его копии другим пользователям. Это может привести к широкому распространению вируса и заражению большого количества компьютеров;

**Удаление или повреждение данных:** Вирус может быть запрограммирован на удаление или изменение файлов на компьютере пользователя. Это может привести к потере или повреждению важной информации;

**Шпионаж:** Вирус может собирать конфиденциальную информацию с компьютера пользователя, включая логины, пароли, банковские данные и другие личные данные. Эта информация может быть передана злоумышленникам и использоваться в криминальных целях;

**Захват компьютера:** Вирус может захватить контроль над компьютером пользователя и использовать его для выполнения различных вредоносных действий, таких как атаки на другие компьютеры, отправка спама или даже участие в ботнете;

**Уязвимость системы:** Вирус в макросах может использовать выявленные уязвимости в операционной системе или других программах для запуска и распространения других вредоносных программ на компьютере пользователя;

**Фишинг и социальная инженерия:** Вирус в макросах может создавать фальшивые всплывающие окна или запросы, выдающиеся за официальные

сообщения или запросы на обновление программного обеспечения. Это может побудить пользователя выполнить действия, такие как ввод логина и пароля, что может привести к раскрытию личной информации или установке других вредоносных программ.

Поэтому важно быть осторожным при открытии документов с макросами, особенно если они получены от ненадежного источника или выглядят подозрительно. Рекомендуется использовать антивирусные программы и регулярно обновлять их для защиты от вирусов в макросах электронных документов.

**В чем заключается профилактика заражения компьютерными вирусами:**

- постоянно обновлять установленное на ПК программное обеспечение;
- все файлы и программы, получаемые из сети интернет, перед открытием нужно обязательно проверять антивирусной программой;
- на архивные диски следует поставить защиту от записи;
- не рекомендуется копировать информацию с компьютеров, на которых не установлено антивирусное ПО;
- во время работы в интернете, а также при копировании/переносе данных, находящихся на внешних носителях, программы-фильтры должны быть активированы;
- с помощью программ детекторов следует регулярно проверять винчестер на наличие вирусов.