Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Худин Александр Николаевич
Должность: Ректор
Дата подписания: 05.07.2023 11:01:14
Уникальный программный ключ:
08303ad8de1c60b987361de7085acb509ac3da143f415362ffaf0ee37e73fa19

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ

Федеральное государственное образовательное учреждение высшего образования
"Курский государственный университет"

УТВЕРЖДЕНО
Протокол заседания
ученого совета КГУ
от 19 октября 2020 г. № 2

Образовательная программа высшего образования – программа бакалавриата
направление подготовки 06.03.01 Биоэкология, направленность Биолэкология

Оценочные материалы для проведения текущего контроля
по дисциплинам
(*приложения к рабочим программам дисциплин)*

Курск 2020

Оценочные материалы для проведения
текущей аттестации по дисциплине
«Основы информационной безопасности»

Раздел 1
Лабораторная работа №1.

Подготовка домашнего компьютера к эксплуатации в условиях потенциальных угроз

В данной лабораторной работе рассматриваются основные способы настройки операционной системы (ОС) компьютера для противостояния интернет-атакам.

Цели:

• отразить потенциальные интернет-атаки на ОС Windows 7/Windows 8/ Windows 10;

• предоставить пользователю наибольшее количество информации о состоянии процессов, исполняемых в ОС;

Задание 1:
Создание учетной записи «user» в ОС Windows с ограниченными правами.

В текущем задании необходимо создать локальную учетную запись ОС Windows 10 для обеспечения безопасности учетной записи пользователя от внешних вторжений.

1. В меню **«Пуск»** необходимо кликнуть левой клавишей мыши на пункте **«Параметры»** и выбрать в появившемся контекстном меню пункт **«Свойства».** Откроется окно **«Параметры»**.

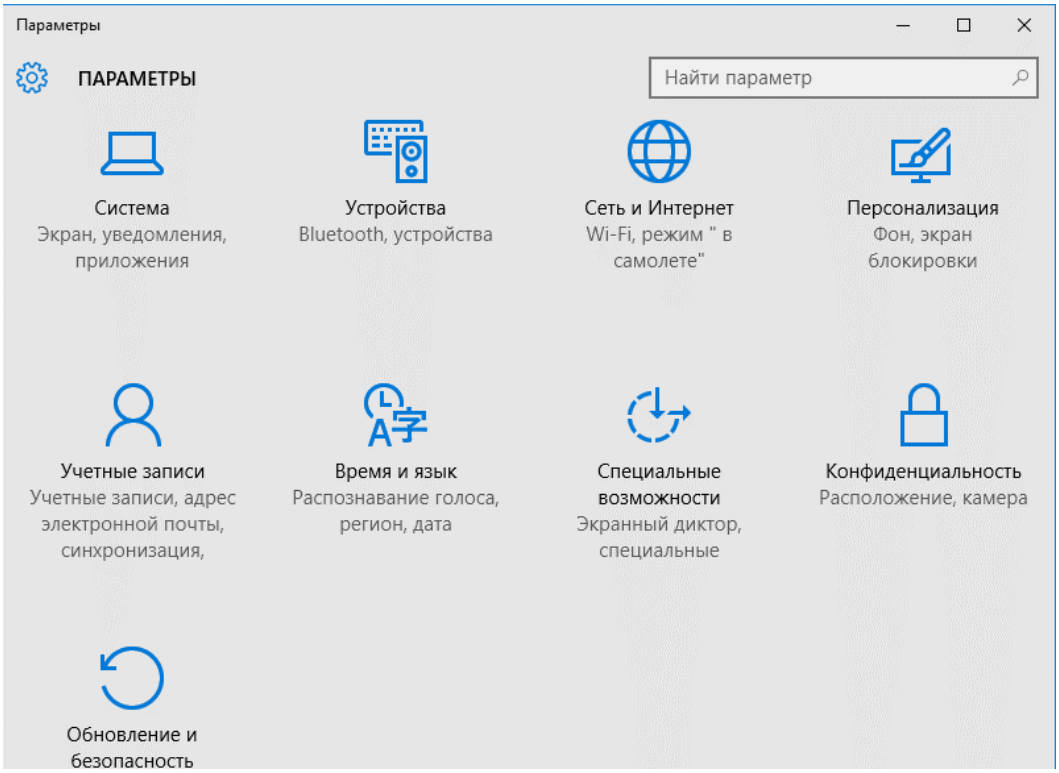


*Рисунок 1.1. Окно **«Параметры».***

2. В открывшемся окне **«Параметры»** (как изображено на рис. 1.1) необходимо щелкнуть левой кнопкой мыши на иконке **«Учетные записи».**

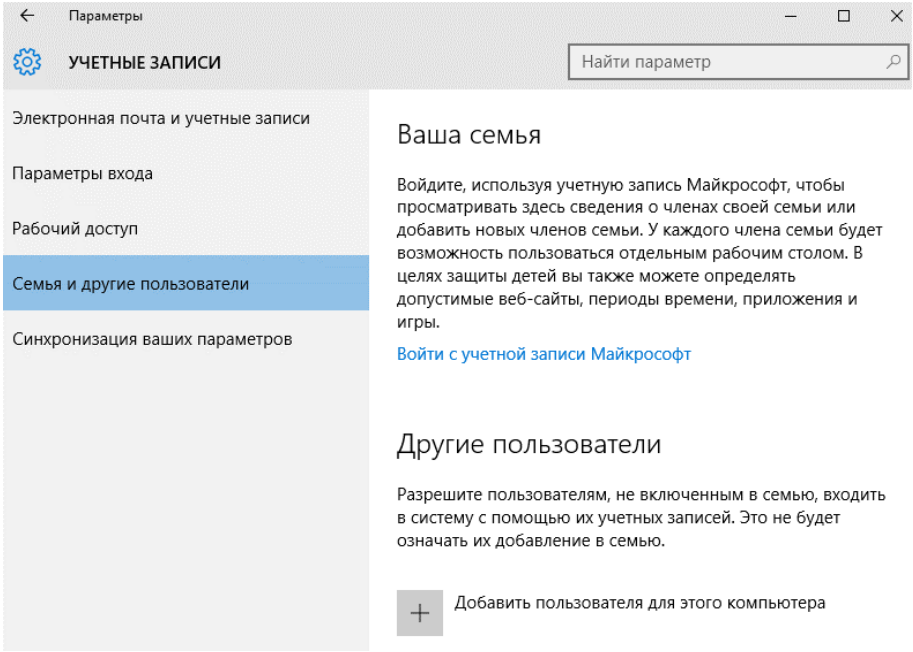


*Рисунок 1.2. Окно **«Учетные записи».***

3. В левой части окна **«Учетные записи»** (рис.1.2) необходимо выбрать пункт **«Семья и другие пользователи»**. В разделе **«Другие пользователи»** выберите пункт **«Добавить пользователя для этого компьютера»**.

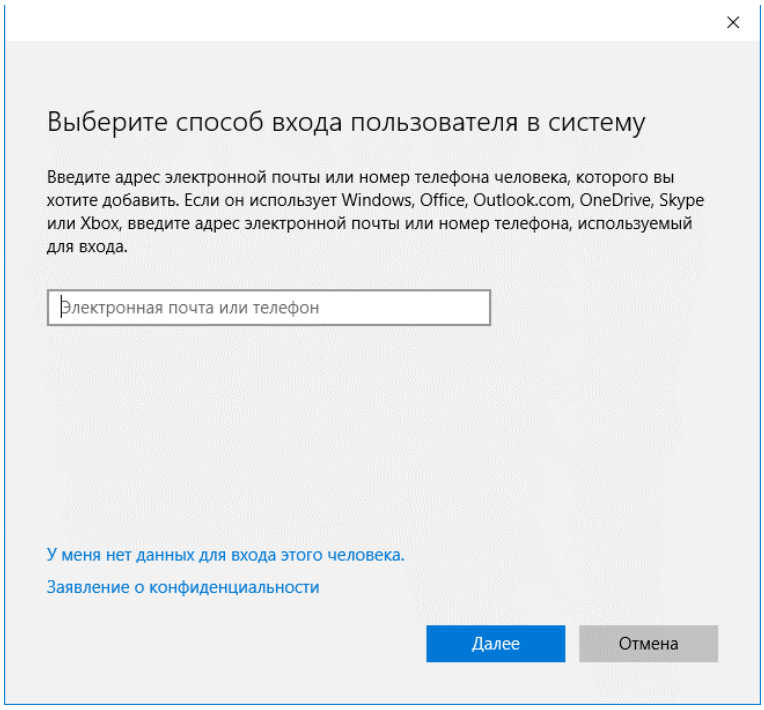


Рисунок 1.3. Окно ***«Добавление нового пользователя».***

4. В появившемся окне «Выберите способ входа пользователя в систему» (рис.1.3) сделайте щелчок левой кнопкой мыши по строке **«У меня нет данных для входа этого человека»**.

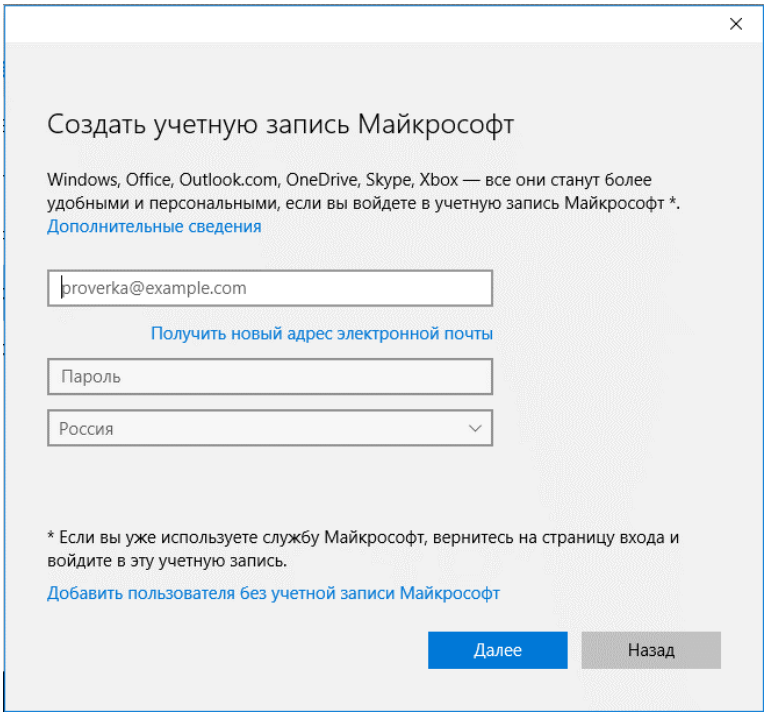


*Рисунок 1.4. Окно **«Создание учетной записи Майкрософт».***

5. В открывшемся окне **«Создать учетную запись Майкрософт»** (рис.1.4) сделайте клик мышкой по строке **«Добавить пользователя без учетной записи Майкрософт»**.

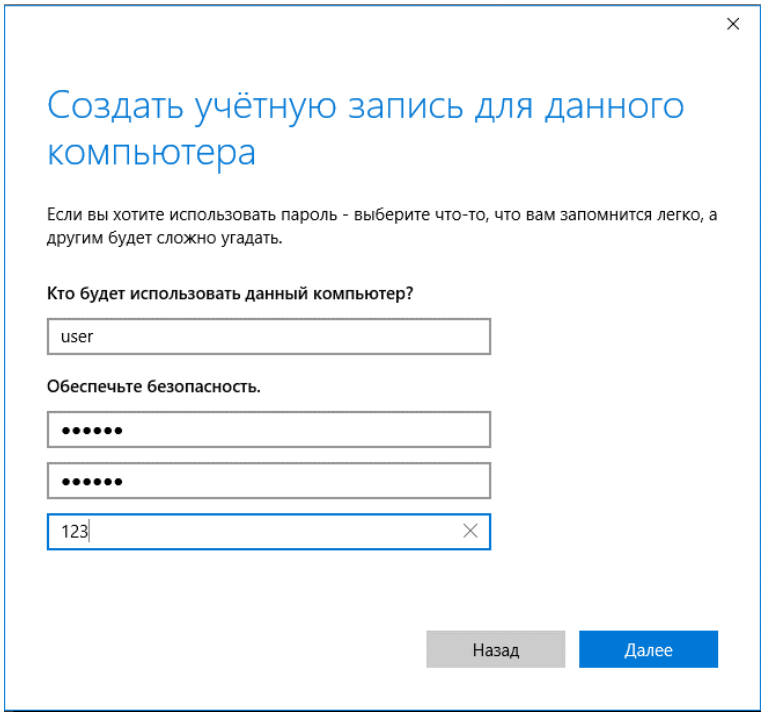


*Рисунок 1.5. Окно **«Создание учетной записи».***

6. В открывшемся окне **«Создать учетную запись для данного компьютера»** (рис.1.5) необходимо заполнить поля: "Имя пользователя",

"Введите пароль", "Введите пароль повторно и подсказать пароль", введя соответствующие значения, которые должны соответствовать варианту задания.

После нажатия на клавишу «Далее» Вы вернетесь в окно **«Учетные записи»** при этом будет создана новая учетная запись.

7. Перезагрузите компьютер нажав последовательно **«Пуск», «Выключение», «Перезагрузка».** После этого Вы увидите вновь созданную учетную запись (рис.1.6).

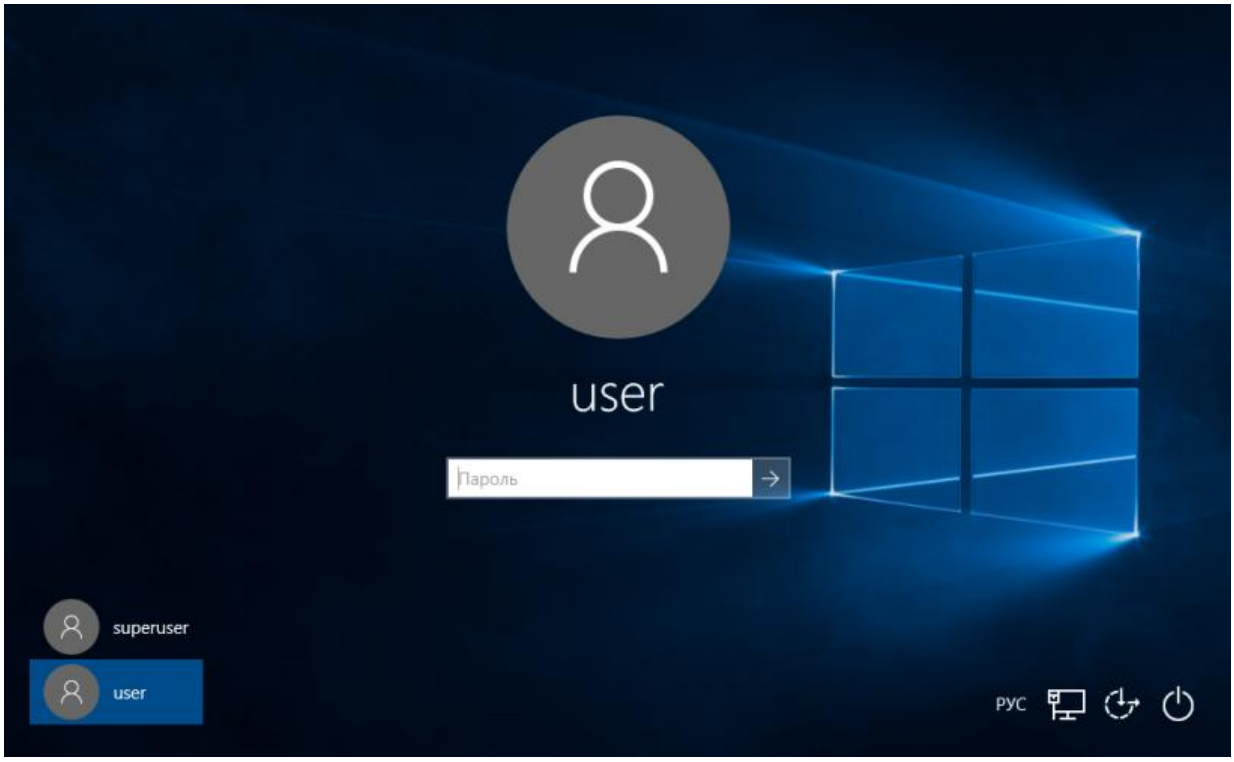


Рисунок 1.6. Окно входа в систему.

8. Сделайте скриншот этого окна для отчета, перейдя в основную ОС и нажав клавишу PrintScr.

Задание 2.

Настройка ОС Windows 10 для автоматического входа в учетную запись «user» по умолчанию.

В текущем задании необходимо настроить ОС Windows 10, чтобы при входе в ОС всегда стартовала учетная запись «user».

1. Кликните правой клавишей мышки по кнопке **«Пуск»** (рис. 2.1).

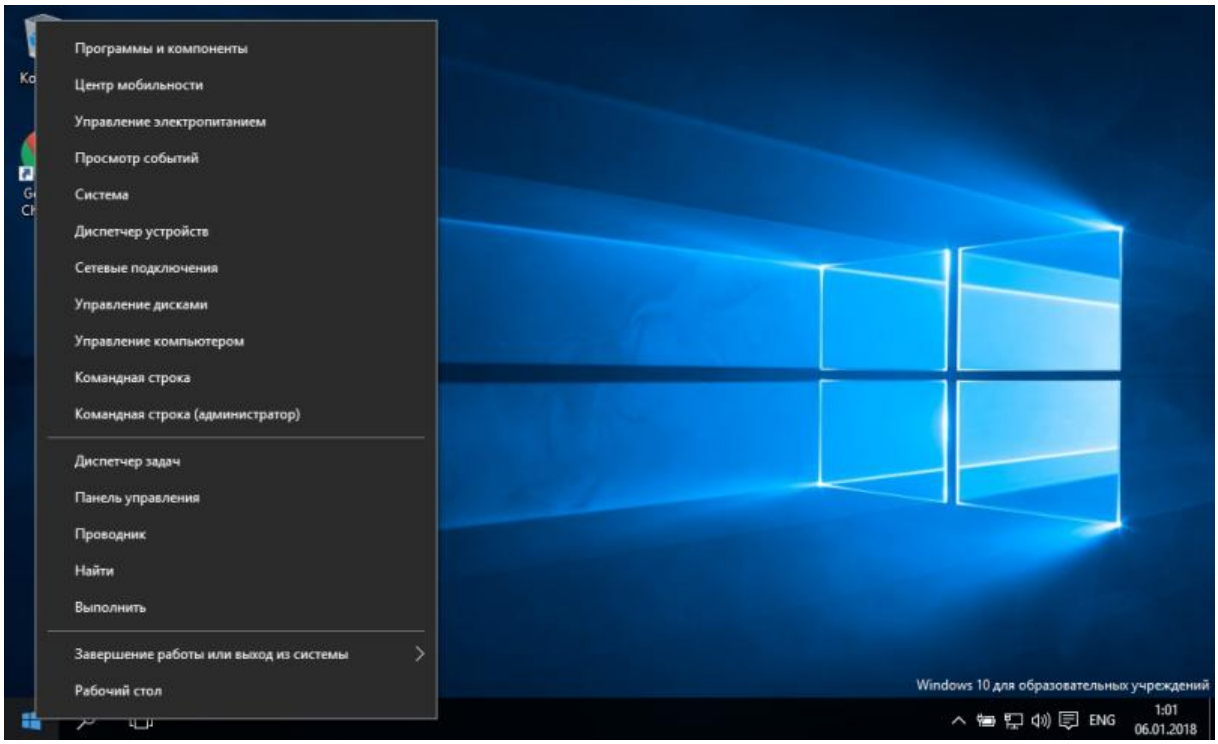


*Рисунок 2.1. Меню **«Пуск».***

2. В появившемся меню необходимо запустить командную строку, выбрав пункт **«Выполнить»** (рис.2.2)**.**

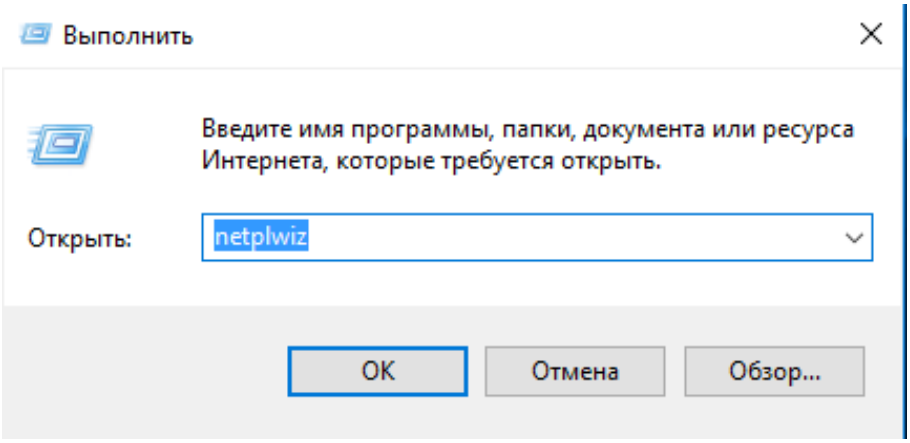


*Рисунок 2.2. Окно **«Выполнить».***

3. В окне **«Выполнить»** введите команду **netplwiz (рис.2.2)** и кликните левой клавишей мыши по кнопке **«OK».**

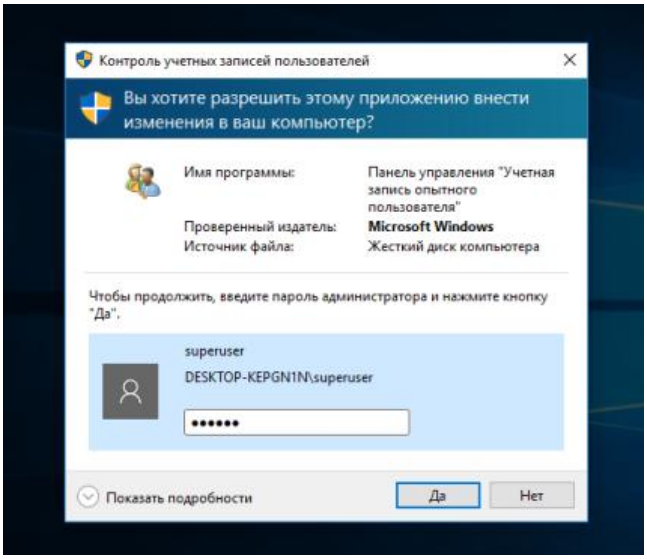


*Рисунок 2.3. Окно «**Контроль учетных записей пользователей**».*

4. В открывшемся окне «Контроль учетных записей пользователей» (рис.2.3) заполните пароль учетной записи администратора и щелкните левой клавишей мыши по кнопке **«OK».**

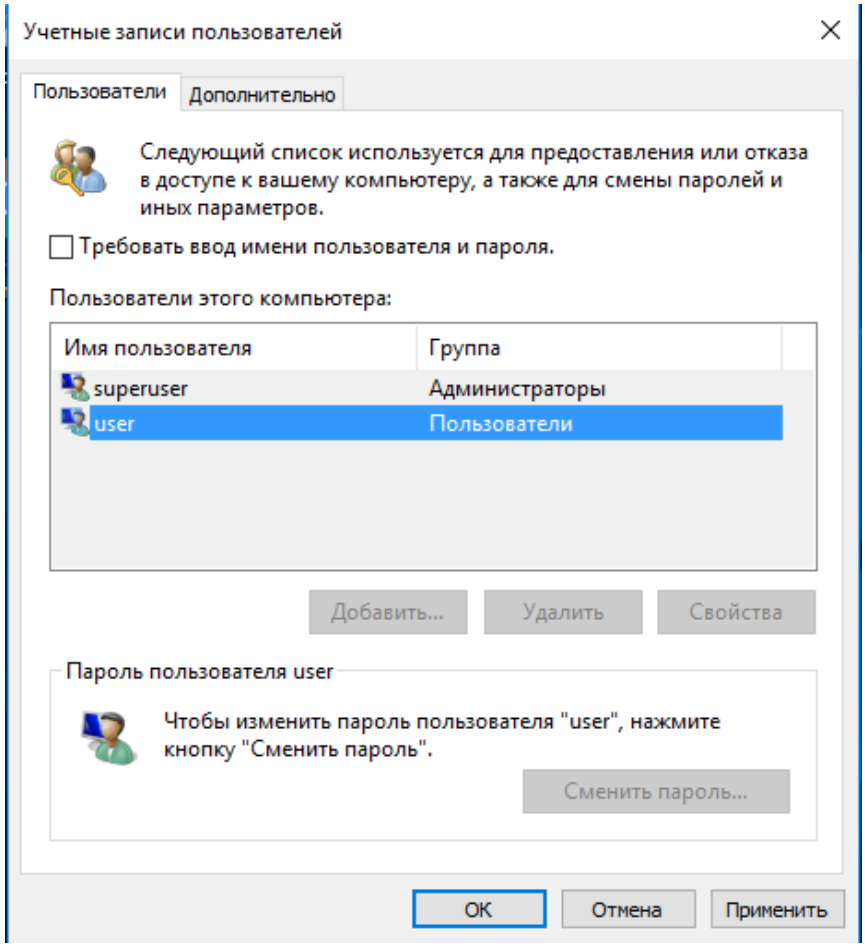


*Рисунок 2.4. Окно **«Учетные записи пользователей»**.*

5. В окне **«Учетные записи пользователей»** (рис. 2.4) выберите учетную запись пользователя, которому вы хотите предоставить возможность автоматического входа при загрузке ОС без ввода пароля. Снять галочку в пункте **«Требовать ввод имени пользователя и пароль»** и кликнуть левой клавишей мыши по кнопке **«Применить».** Сделать скриншот этого окна для отчета, перейдя в основную ОС и нажав клавишу PrintScr.

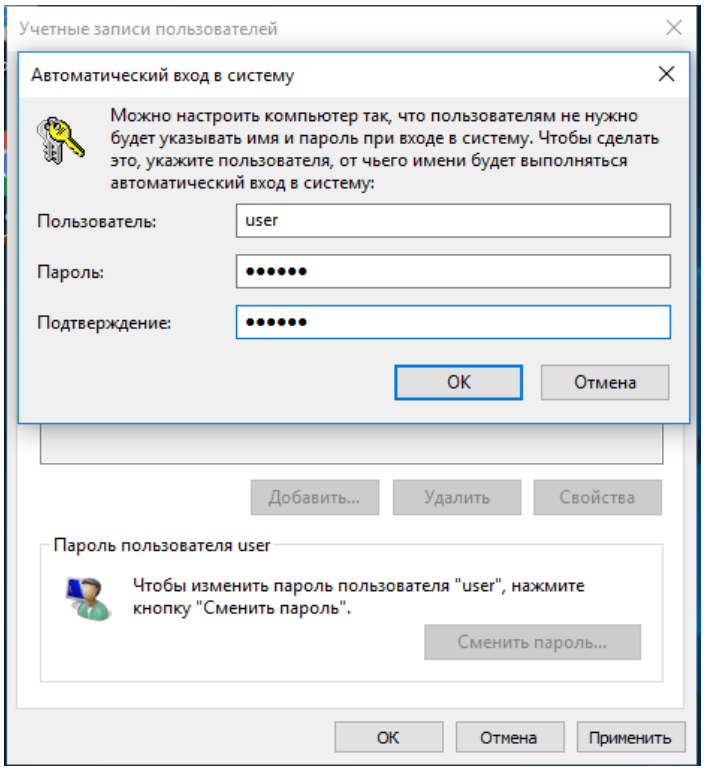


Рисунок 2.5. Окно «Автоматический вход в систему».

6. В окне «Автоматический вход в систему» (рис. 2.5) дважды введите пароль пользователя и кликните левой клавишей мыши по кнопке **«OK».**

7. Сделайте скриншот этого окна для отчета, перейдя в основную ОС и нажав клавишу PrintScr.

8. Перезагрузите компьютер нажав последовательно **«Пуск», «Выключение», «Перезагрузка».** После перезагрузки вы сможете убедиться, что вход в ОС Windows будет происходить автоматически.

Задание 3.

Разбиение жесткого диска на разделы.

В данном задании необходимо разбить жесткий диск ОС Windows10 на два раздела.

1. Кликните левой клавишей мыши по кнопке**«Пуск»** и в появившемся контекстном меню выберите вашу учетную запись (в данном случае user).В появившемся списке выберите учетную запись **superuser**. Введите пароль учетной записи **superuser**. Кликните правой клавишей мышки по кнопке **«Пуск»** и в появившемся меню выберите пункт **«Управление»**.

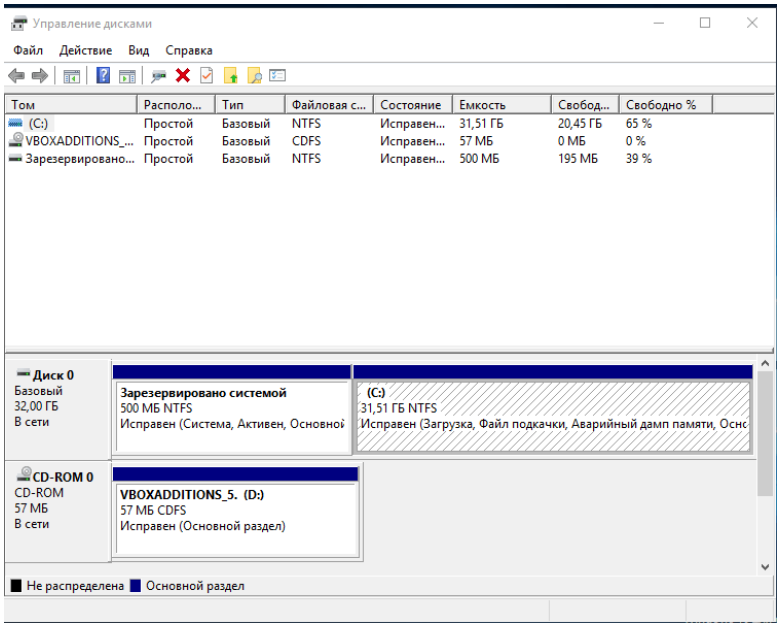


Рисунок 3.1. Окно «Управление дисками».

2. В открывшим окне необходимо выбрать пункт «**Управление дисками**» (см рис.3.1) .

3. Кликните правой кнопкой мыши по диску С и выберите пункт «Сжать том», как изображено на рис. 3.2.

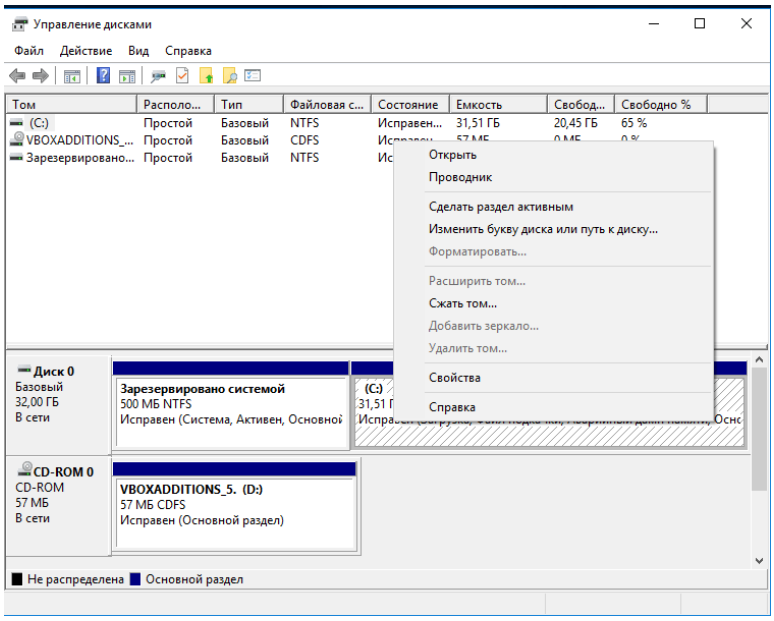


Рисунок 3.2 Контекстное меню диска.

4. Откроется окно «Сжать C:» (см. рис. 3.3):

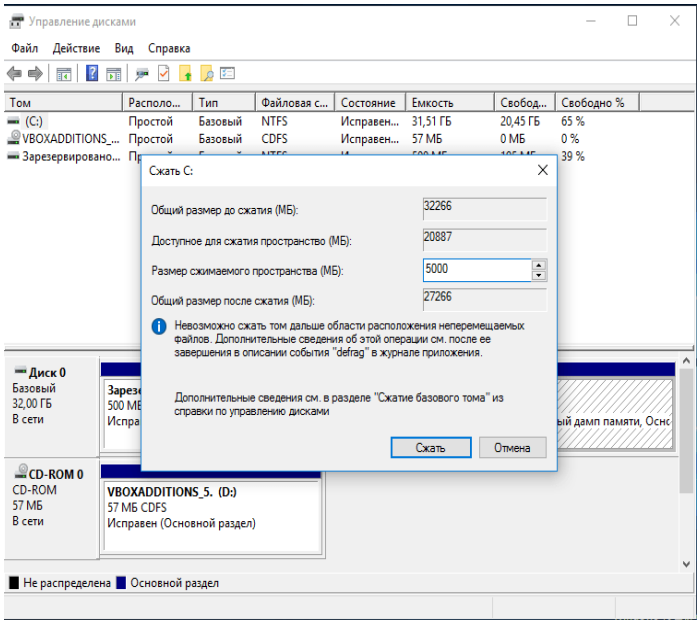


Рисунок 3.3 Окно «Сжать том».

4. По умолчанию, вам будет предложено сжать том (высвободить место для диска D, другими словами) на все доступное свободное пространство жесткого диска. Делать этого не рекомендуется - необходимо оставить по крайней мере 10-15 гигабайт свободного места на системном разделе. То есть, вместо предложенного значения введите то, которое сами считаете нужным для диска D. В моем примере на скриншоте - 5000 мегабайт или чуть менее 5 гигабайт. Нажмите «Сжать».

5. В управлении дисками появится новая нераспределенная область диска, а диск C уменьшится. Кликните по области «не распределена» правой кнопкой мыши и выберите пункт «Создать простой том», запустится мастер создания томов или разделов (см. рис. 3.4):

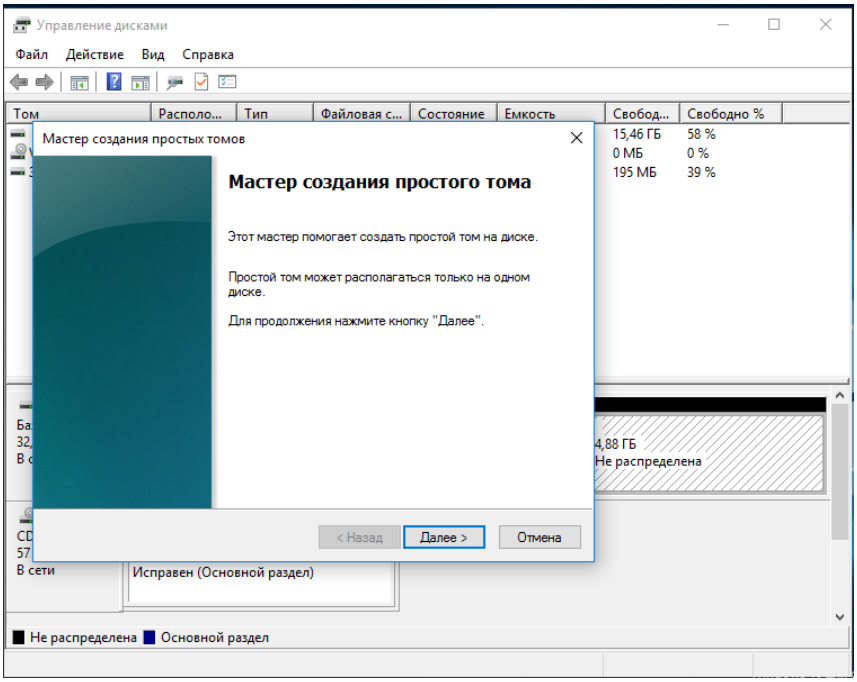


Рисунок 3.4. Мастер «Создать простой том».

6. Мастер запросит размер нового тома оставьте полный размер (см. рис. 3.5).

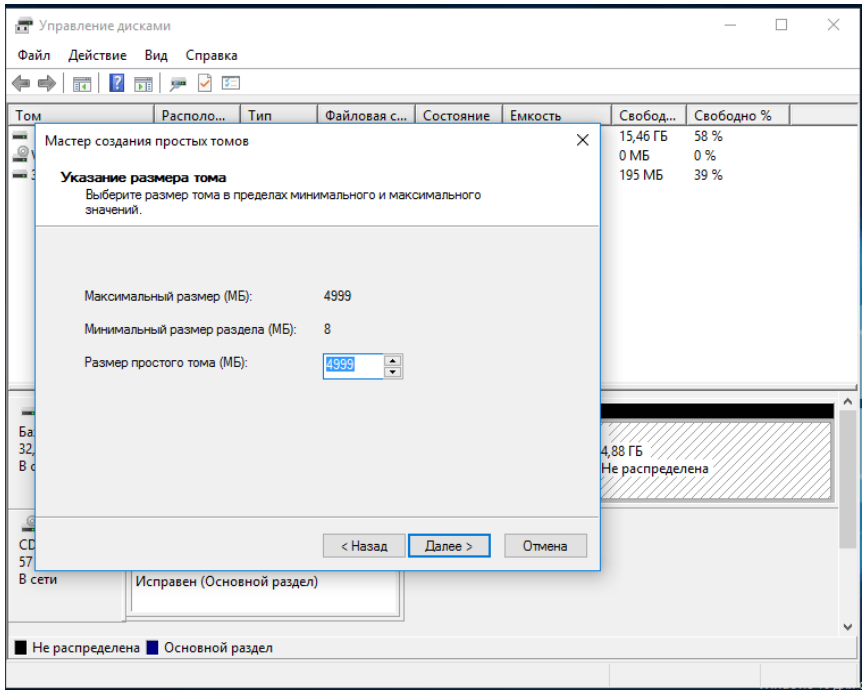


Рисунок 3.5. Окно «Указание размера тома».

7. Мастер предложит назначить букву диска. Поменяйте метку в соответствии с вариантом задания (аналогично рис. 3.6).

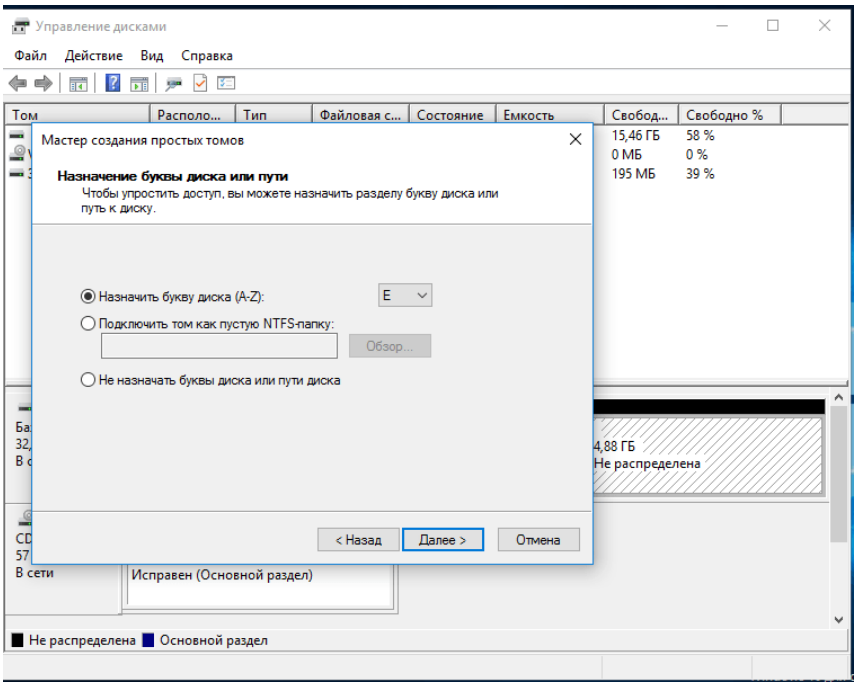


Рисунок 3.6. Окно «Назначение буквы диска или пути».

8. Мастер предложит отформатировать новый раздел (см. рис 3.7)

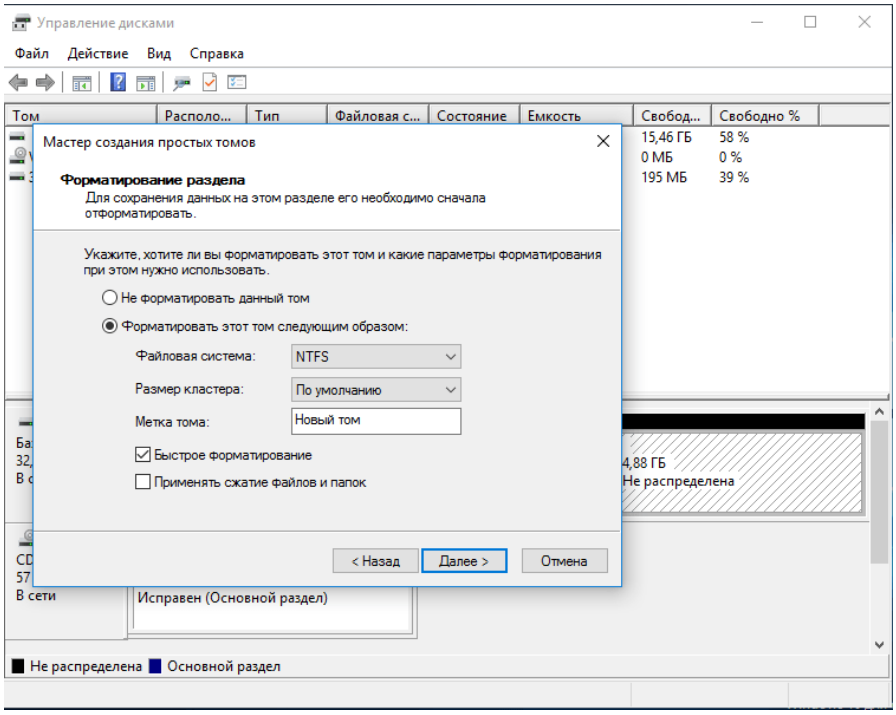


Рисунок 3.7. Окно «Форматирование раздела».

9. После этого, новый раздел будет автоматически отформатирован и смонтирован в системе под заданной вами буквой (т.е. появится в проводнике и в окне «Мой компьютер», см. рис. 3.8).

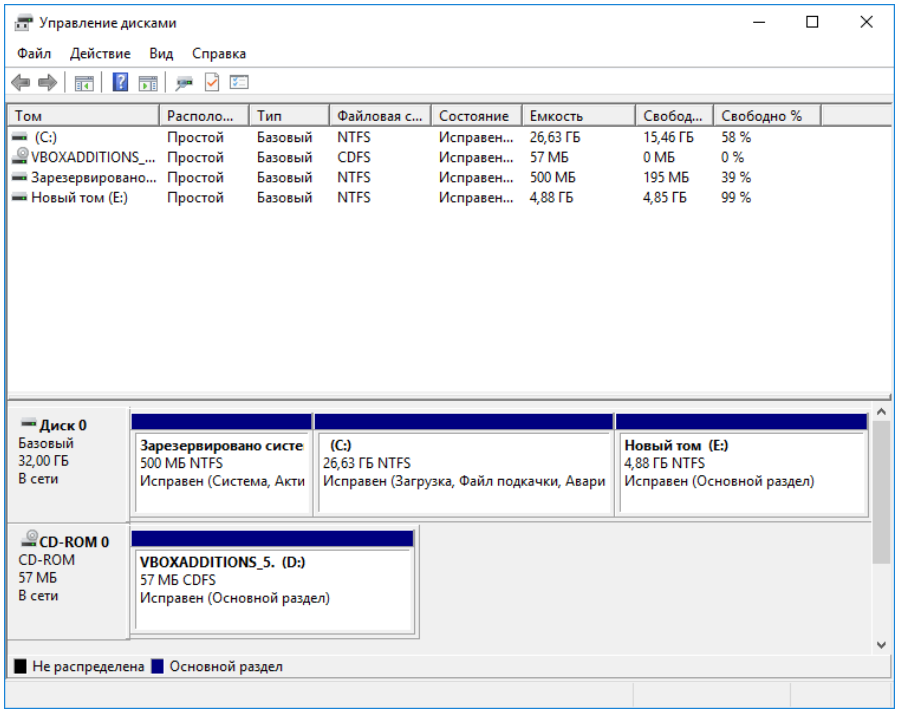


Рисунок 3.8. Новый том.

10. Сделайте скриншот этого окна для отчета, перейдя в основную ОС и нажав клавиши Alt+PrintScr. Перезагрузите компьютер.

Задание 4.

Создание ярлыков на рабочем столе.

Как правило, сохраненные на рабочем столе файлы, находятся в первом разделе диска С, который, в случае выхода ОС из строя, теряется. Вместе с ним теряется и информация пользователя, находящаяся в этих файлах. Чтобы обезопасить пользователя от таких потерь, рекомендуется на рабочем столе хранить ярлыки, а полезную информацию хранить в другом месте. Как это сделать разберем в данном задании.

1. Открыть «Мой компьютер» и выбрать диск, соответствующий созданному разделу.

2. Создать на диске Е новую папку с именем, соответствующим варианту задания (см. рис. 4.1).

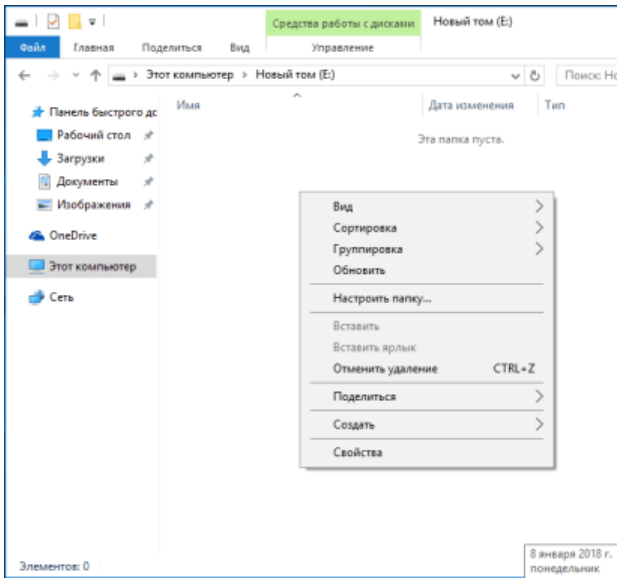


Рисунок 4.1. Окно нового тома .

2. На рабочем столе создать ярлык. Для этого необходимо кликнуть правой кнопкой мыши в свободную область рабочего стола. В появившемся контекстном меню найти строку "Создать", и выбрать пункт "Ярлык", как изображено на рис. 4.2.

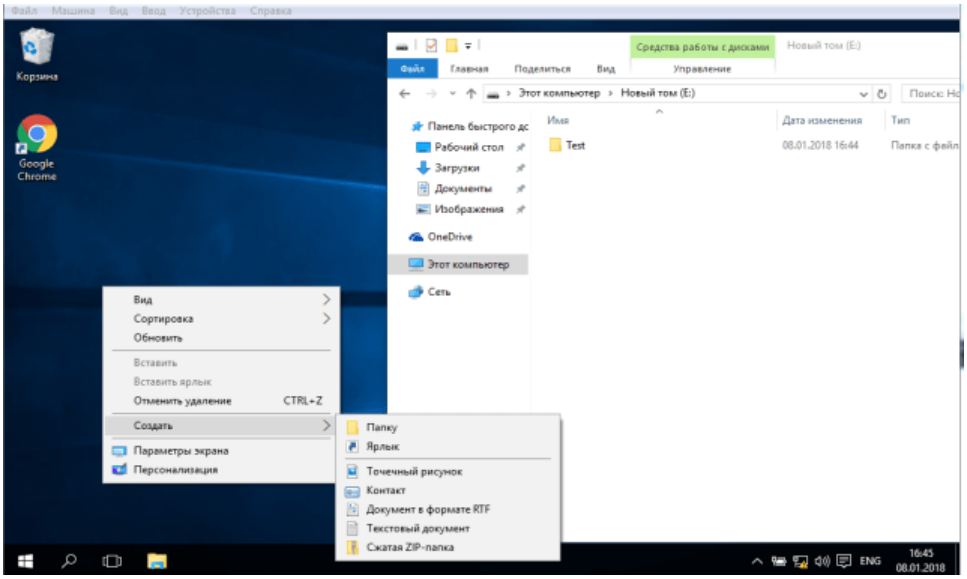


Рисунок 4.2. Создание ярлыка .

3. В окне «Создать ярлык» выбираем с помощью кнопки «Обзор» вновь созданную папку «Тест» в разделе E (см. рис. 4.3).

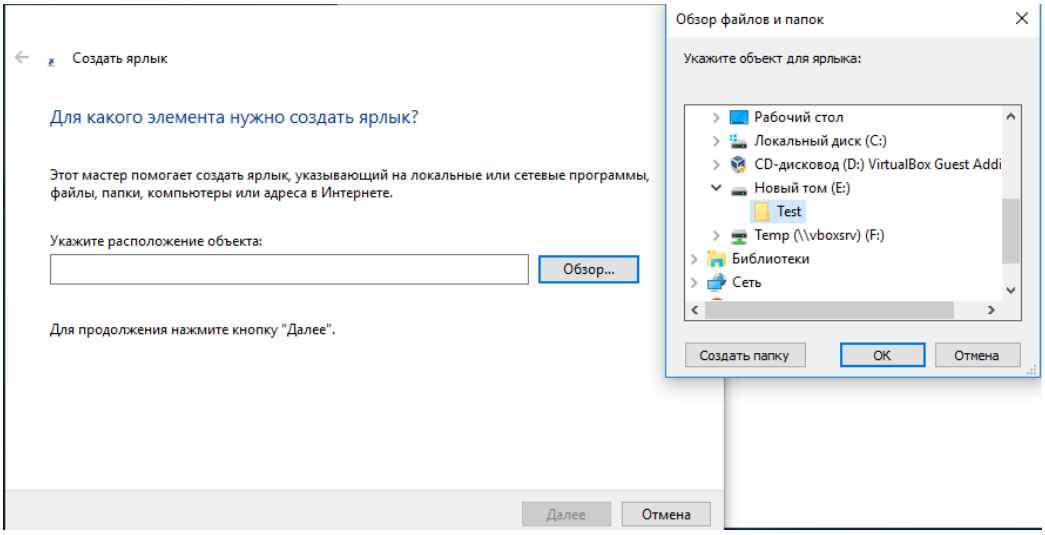


Рисунок 4.3. Выбор адреса назначения ярлыка .

4. Нажать левой клавишей мышки по кнопке «Далее» (см. рис 4.4).

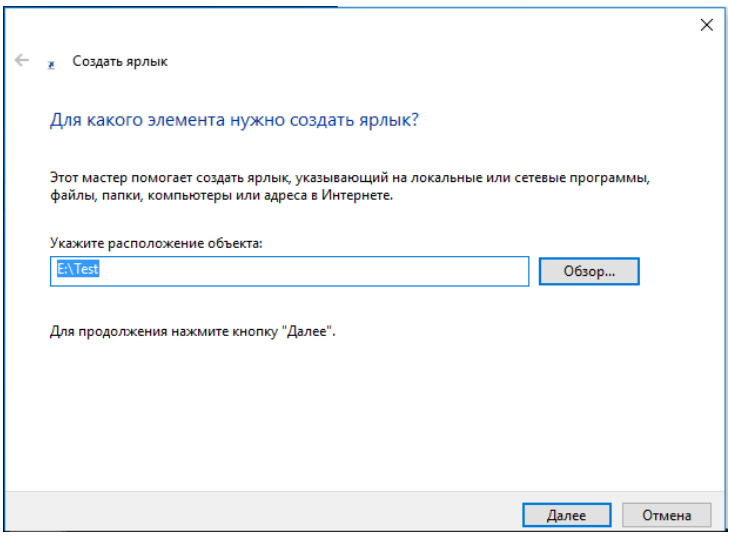


Рисунок 4.4. Адрес назначения объекта ярлыка .

5. Нажать левой клавишей мышки по кнопке «Далее» (см. рис 4.5).

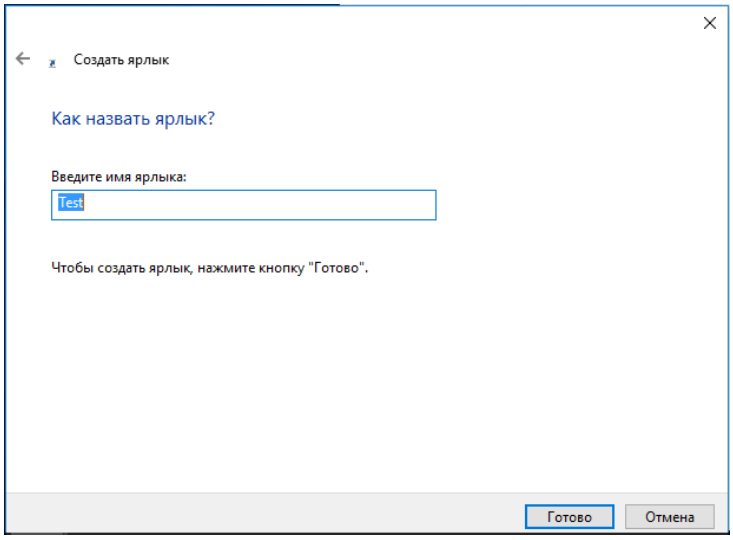


Рисунок 4.5. Название ярлыка.

6. Оставляем имя ярлыка без изменения и кликаем левой клавишей мышки по кнопке «Готово».

7. А теперь как пользоваться созданным ярлыком:

8. На рабочем столе, аналогично ярлыку, создадим текстовый файл с именем «Мой текст» (см. рис. 4.6).

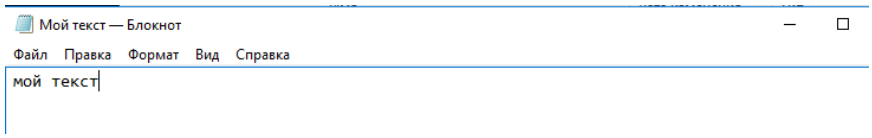


Рисунок 4.6. Содержание тестового файла.

9. Наведем указатель мышки на пиктограмму, изображающую созданный текст, и, удерживая правую клавишу мышки, перетянем ее на пиктограмму ярлыка. В появившемся контекстном меню выберем пункт «Переместить». Ваш файл будет перенесен в созданную папку (см. рис. 4.7).

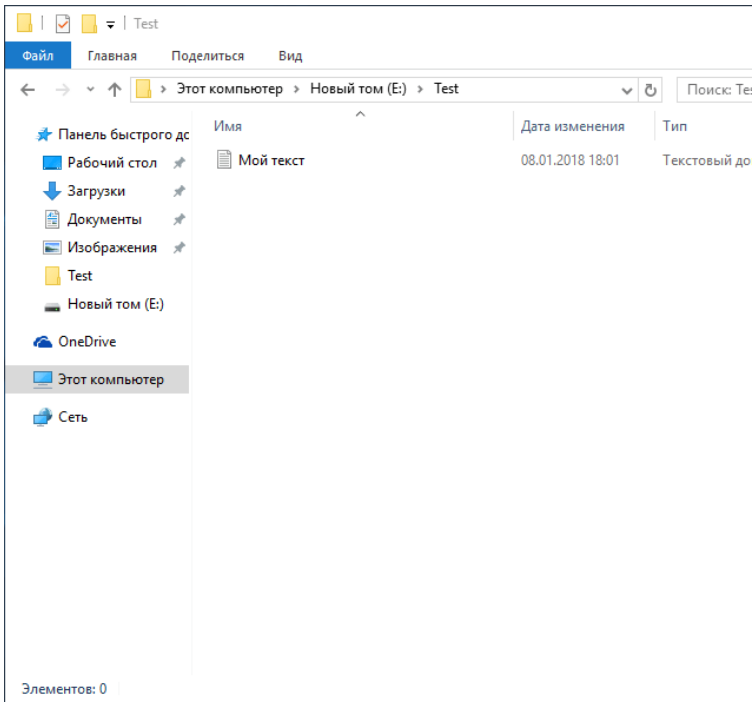


Рисунок 4.7. Результат переноса файлов по ярлыку.

Теперь начальная настройка ОС завершена и рабочая станция защищена от несанкционированных вторжений начального уровня.

Варианты индивидуальных заданий.

Таблица 1 – Варианты заданий

№	Имя пользователя	Метка диска	Имя папки
1	bookbinder	E	canenclem
2	apron	F	heaconric
3	gendarme	G	drulatcra
4	anarchist		booglapra
5	quidnunc	H	kilrimhus
6	locksmith	I	pacunbinf
7	adventurer	J	ditarract
8	beaver	K	droworran
9	athlete	L	proailpra
10	midwife	M	dovstrdef
11	holidayer	N	booselgru
12	aquacckit	O	pasanngab
13	kitten	P	midexphol
14	critic	Q	abbskumin
15	albatross	R	abdquiaer
16	renter	S	idesmowal
17	costumier	T	parcozaca
18	grazier	U	orideptes
19	miller	V	farpulpil
20	pilgrim	W	motdisdem
21	duck	X	scabeddet
22	meteor	Y	coslikint
23	mendicant	Z	baredugoo

Лабораторная работа № 2.
Восстановление и удаление данных

В данной лабораторной работе рассматриваются основные вопросы работы с жестким диском и оптимизации операционной системы компьютера.

Цели:

- Использование программ дефрагментации дисков.
- Восстанавливать случайно удаленные файлы.
- Восстанавливать данные после форматирования раздела.
- Уничтожать данные без возможности восстановления.

Задание 1.

Установка программы дефрагментации Disk Defrag.

В этом задании Вам необходимо установить программу дефрагментации Disk Defrag, проанализировать состояние жесткого диска, определить объем удаленных данных и возможность их восстановления.

1. Открыть Интернет-браузер и найти в сети интернет программу установки Auslogics Disk Defrag Free (см рис. 1.1):

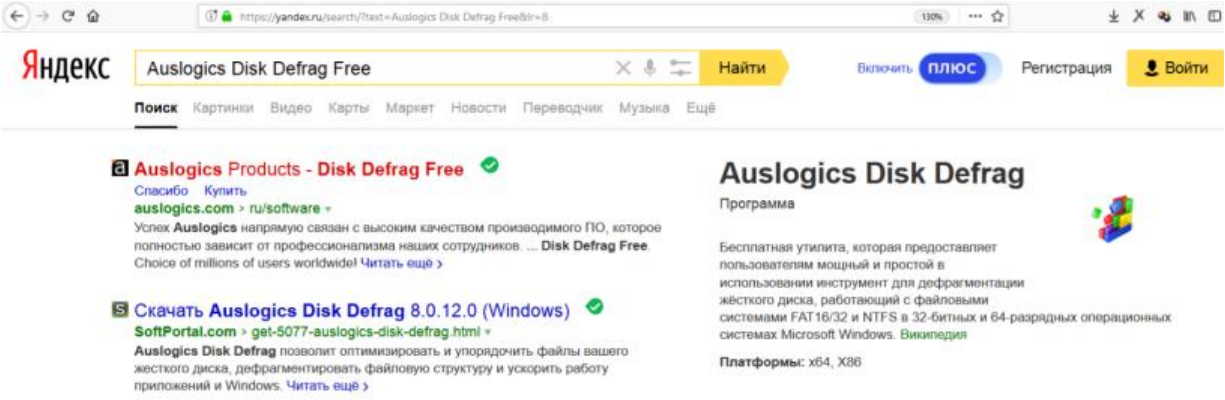


*Рисунок 1.1. Поиск программы"**Auslogics Disk Defrag Free"** в сети Интернет*

2. Из выпавшего списка ресурсов выбрать первую ссылку на сайт производителя www.auslogics.com (как изображено на рис. 1.1).

3. Если ресурсы вашего компьютера удовлетворяют системным требованиям программы - необходимо скачать установочный пакет с сайта производителя на свой рабочий компьютер (см. рис. 1.2).

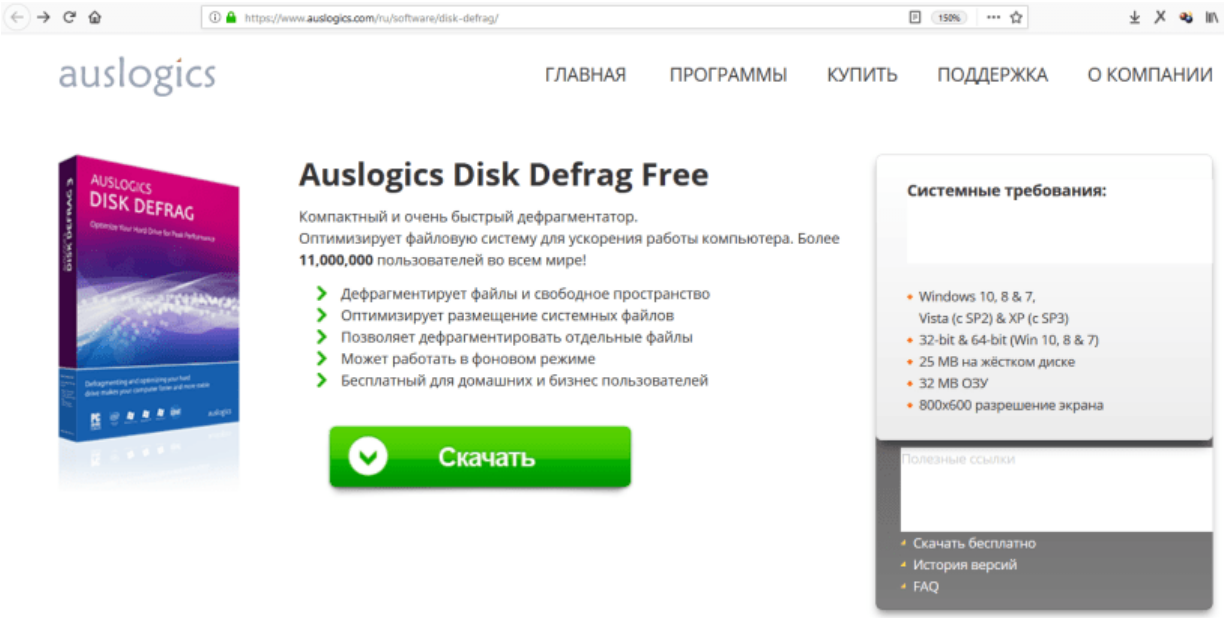


*Рисунок 1.2. Окно для скачивания дистрибутива "**Auslogics Disk Defrag Free"**.*

4. Находясь в учетной записи администратора запустить установку программы Disk Defrag.

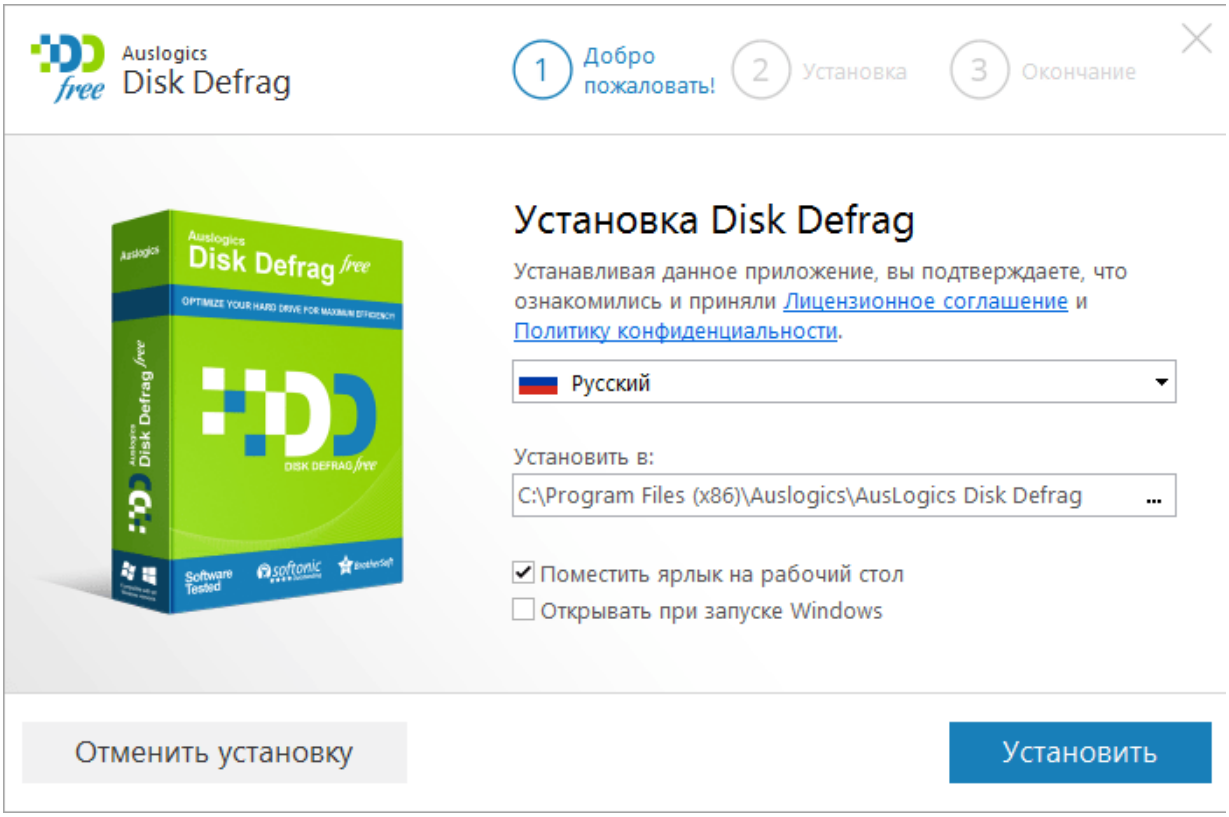


Рисунок 1.3. Окно установки программы ***Auslogics Disk Defrag Free***.

5. Оставить флажки, как изображено на рис. 1.3 и нажать кнопку **«Установить»**.

Рисунок 1.4. Окно установки программы ***Auslogics BoostSpeed****.*

6. Оставить выбор без изменений (см. рис. 1.4) и нажать кнопку **«Далее».**

7. Снять выбранные галочки и нажать кнопку **«Отказаться»**. По окончании установки программы нажать кнопку **«Завершение»** и закрыть появившееся окно.

8. Выбирать действие **«Закрыть окно программы»**.

9. Запустить только что установленную программу ***Disk Defrag***, выбрав пиктограмму.

10. Поставить галочку в окне программы **Disk Defrag** напротив диска (см. рис. 1.5). Кликните по выбранной строке правой клавишей мыши и в появившемся меню выберите **«Анализ»**.

11. Вы увидите фрагментированные участки диска, отмеченные красным цветом. Если таких участков мало или они отсутствуют, то попробуйте удалить некоторые файлы с диска и записать их вновь, но только в другой последовательности и снова выберать **«Анализ»**. Чем больше будете удалять, затем записывать файлов, тем больше будет фрагментация. Белые участки указывают на освободившееся место от удаленных файлов. Если этот участок диска не был занят данными от новых файлов, то информацию с них можно восстановить.

12. Сделать скриншот окна для отчета, перейдя в основную ОС и нажав клавишу Alt+PrintScr.

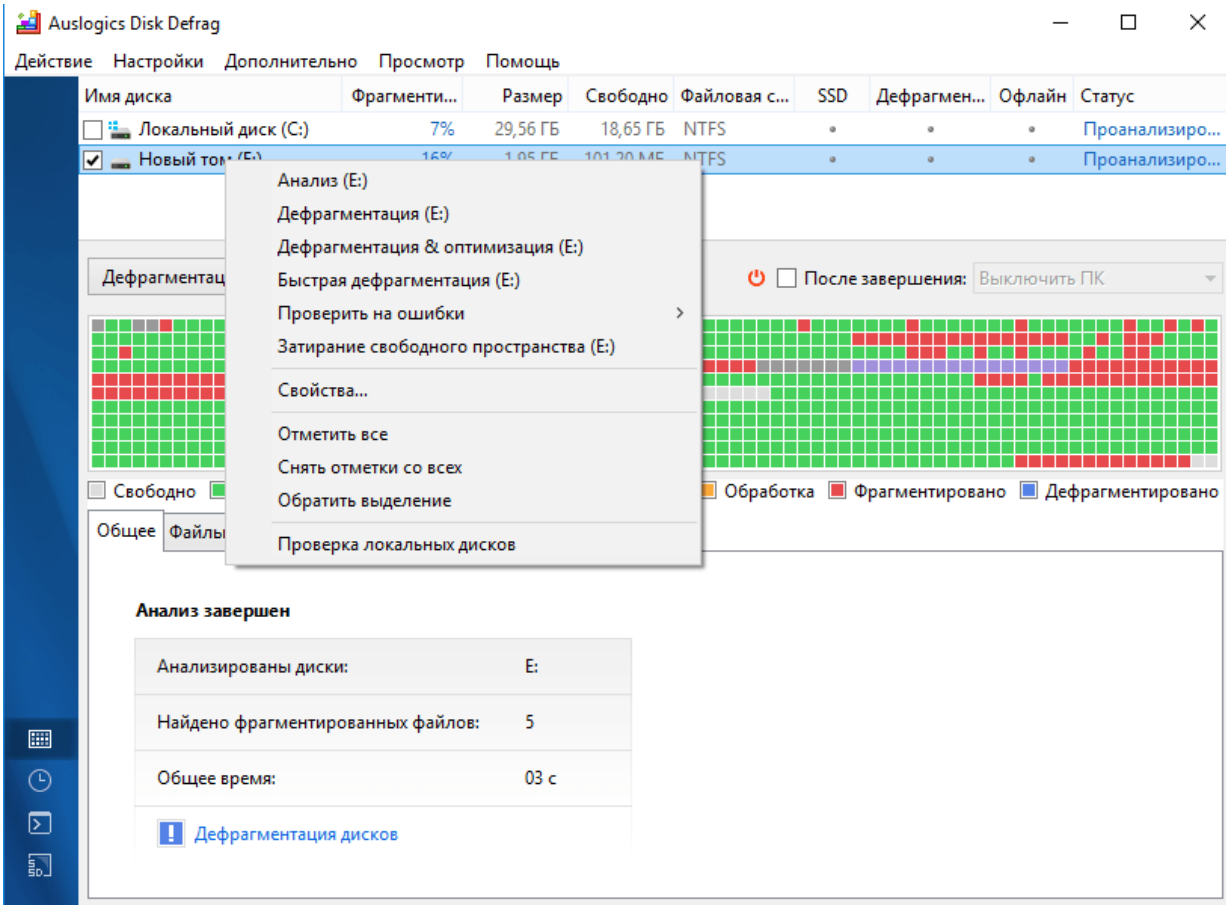


Рисунок 1.5. Анализ дисков перед дефрагментацией.

Задание 2.

Восстановление случайно удаленных файлов.

1. Используя навыки из лабораторной работы №1 выделить на диске новый раздел (или воспользуйтесь разделом, созданным на прошлом занятии). В примере используется имя файла test.txt. При выполнении работы использовать имя файла, заданное в соответствии с вариантом задания (согласно приложению). Записать на него несколько файлов среди них файл test.txt, содержащий некоторую текстовую информацию, например, "В чащах юга жил бы цитрус? Да, но фальшивый экземпляр!".

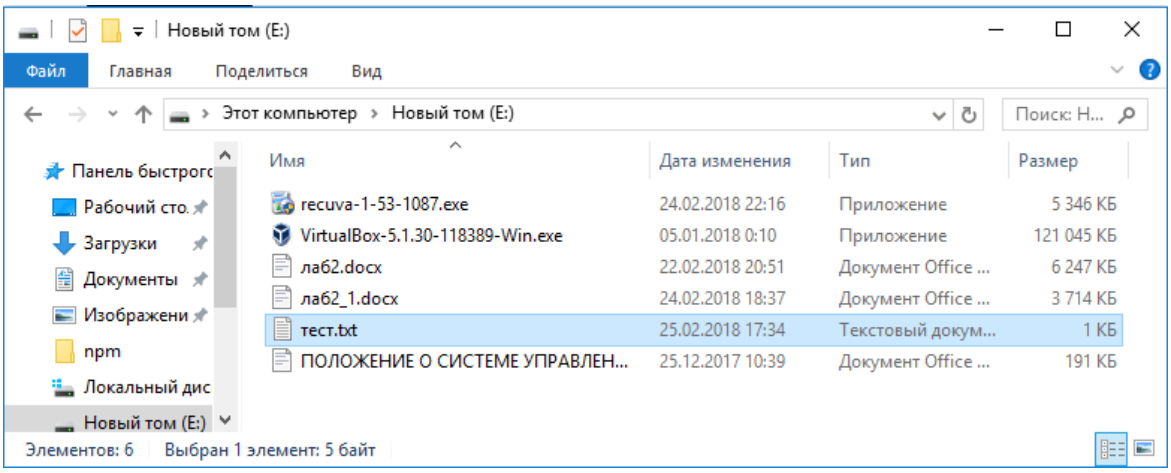


Рисунок 2.1. Обзор раздела диска.

2. Удалить файл ***test.txt***. Открыть корзину, используя показанную ниже пиктограмму на рабочем столе.

3. В открывшемся окне кликнуть правой кнопкой мыши по файлу ***test.txt*** и выберите «Восстановить». На месте удаленного файла появится файл ***test.txt***. Таким образом, Вам удалось восстановить удаленный файл.

4. Удалить файл ***test.txt*** с диска. Открыть корзину и удалить этот же файл оттуда.

5. Осуществить поиск бесплатного программного обеспечения для восстановления данных ***Recuva Free***.

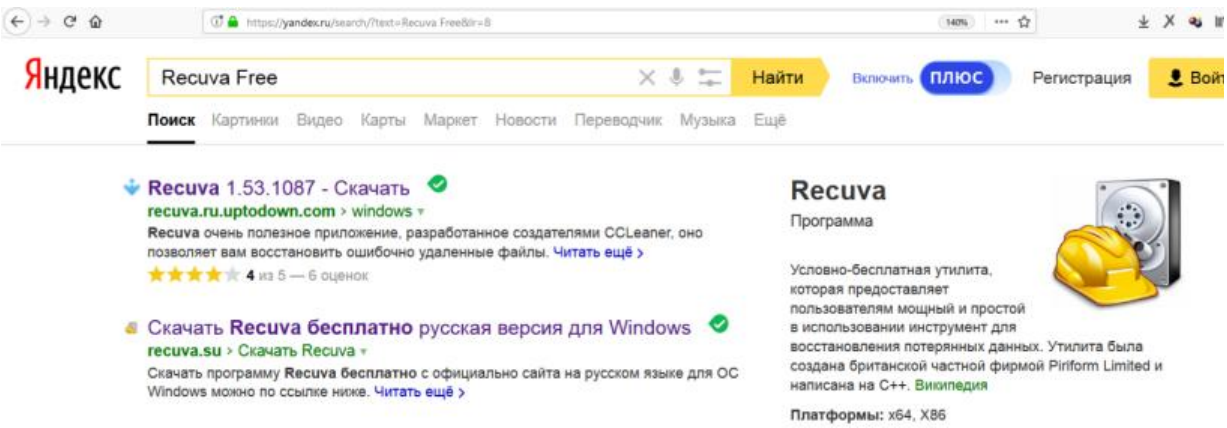


Рисунок 2.2. Поиск программы ***Recuva Free****.*

6. Установить программу ***Recuva Free***, скачав дистрибутив из сети Интернет (см. рис. 2.3)

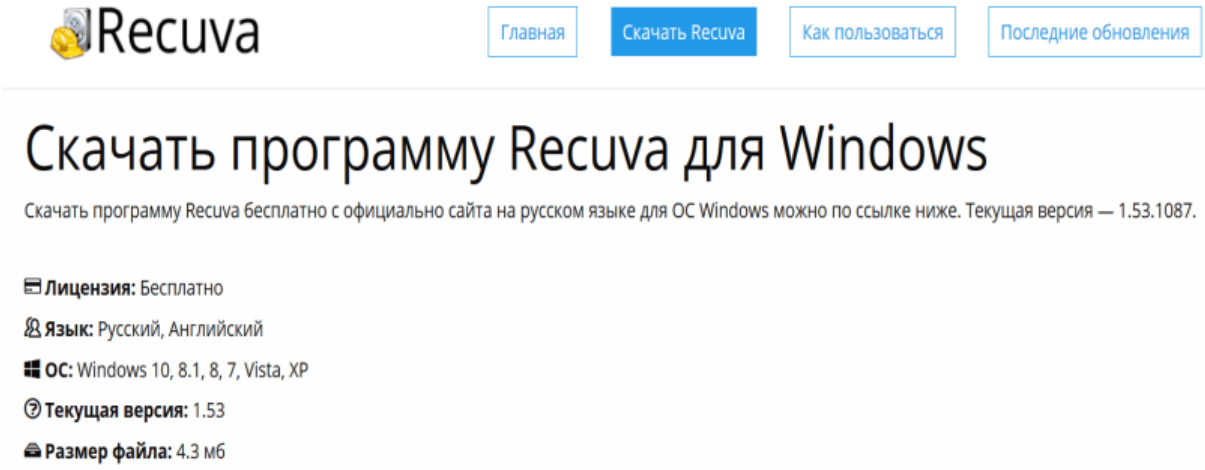


Рисунок 2.3. Скачивание дистрибутива ***Recuva Free****.*

7. Запустить вновь установленную программу.

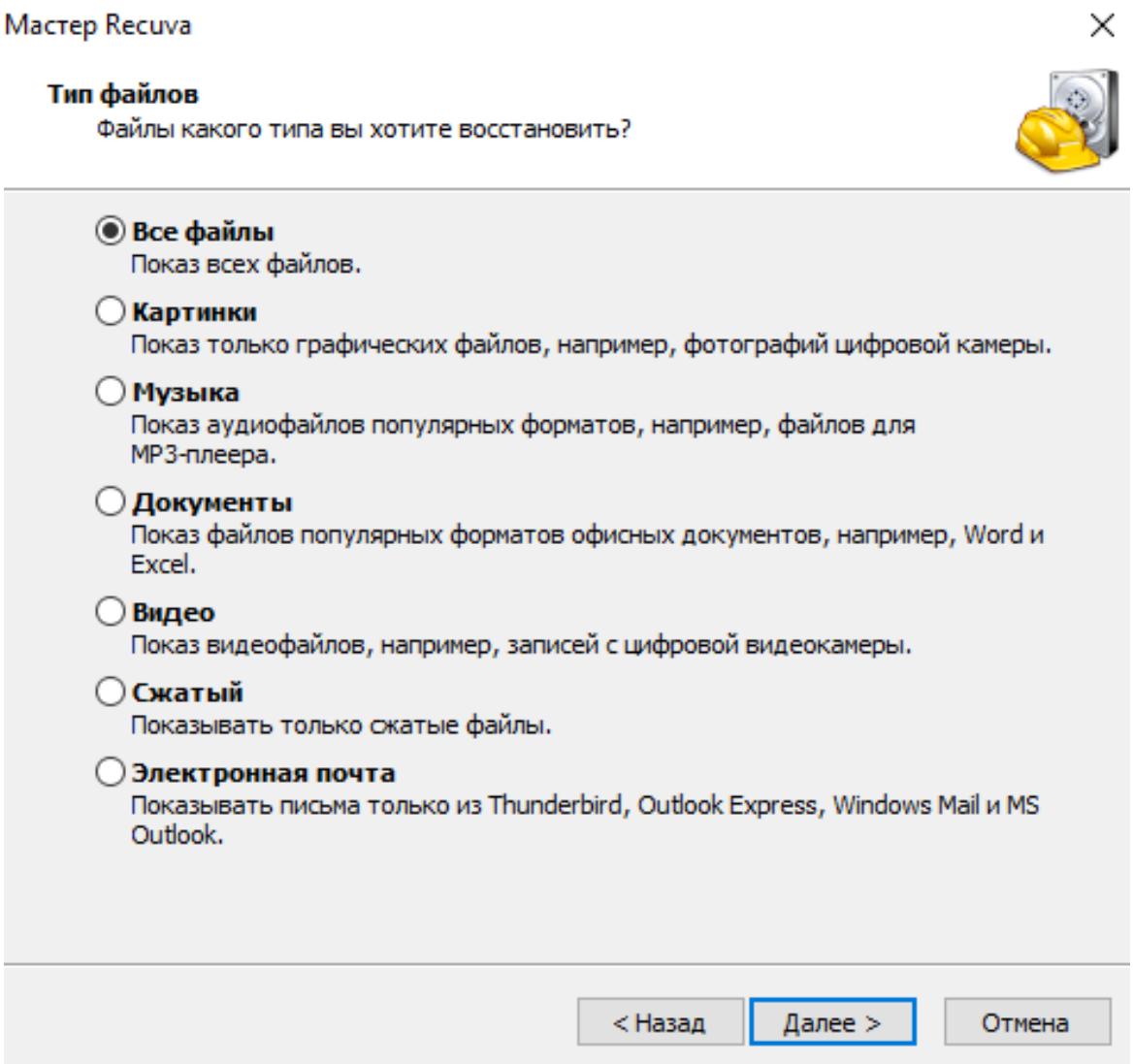


*Рисунок 2.4. Выбор типов файлов в мастере **Recuva**.*

8. Оставить выбор по умолчанию (как изображено на рис. 2.4).

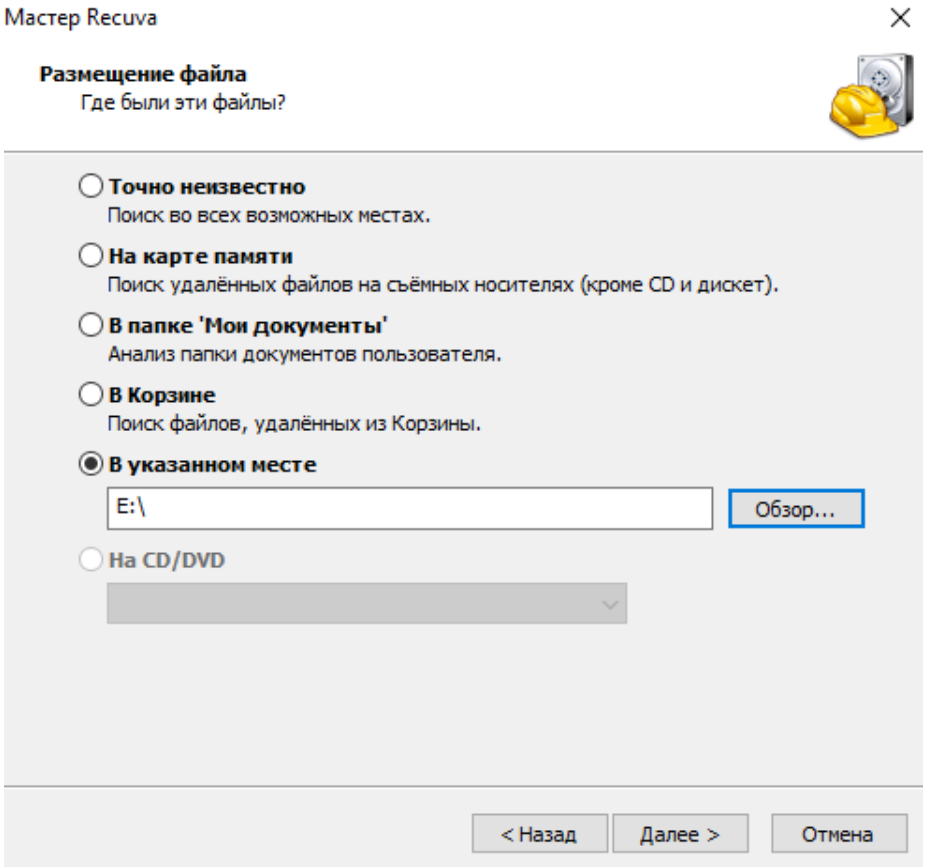


Рисунок 2.5. Выбор носитель удаленной информации.

9. Выбрать флаг **«В указанном месте»** и укажите диск, на котором нужно восстановить файлы (см. рис.2.5).

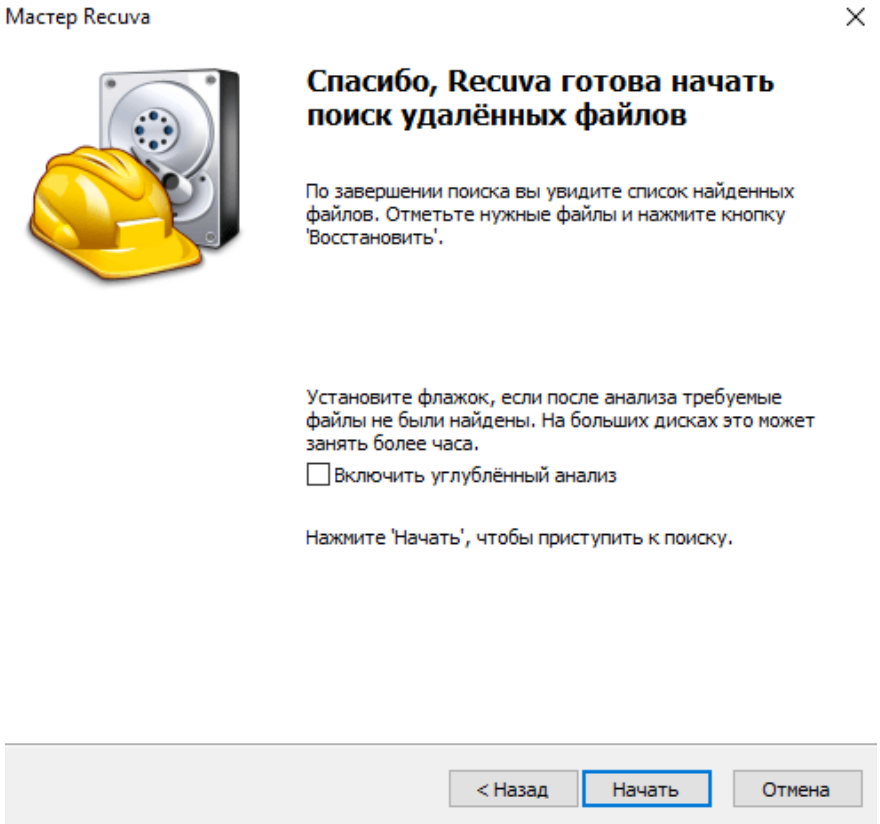


Рисунок 2.6. Окончание мастера установки.

10. Нажать кнопку**«Начать»** (см. рис. 2.6)**.**

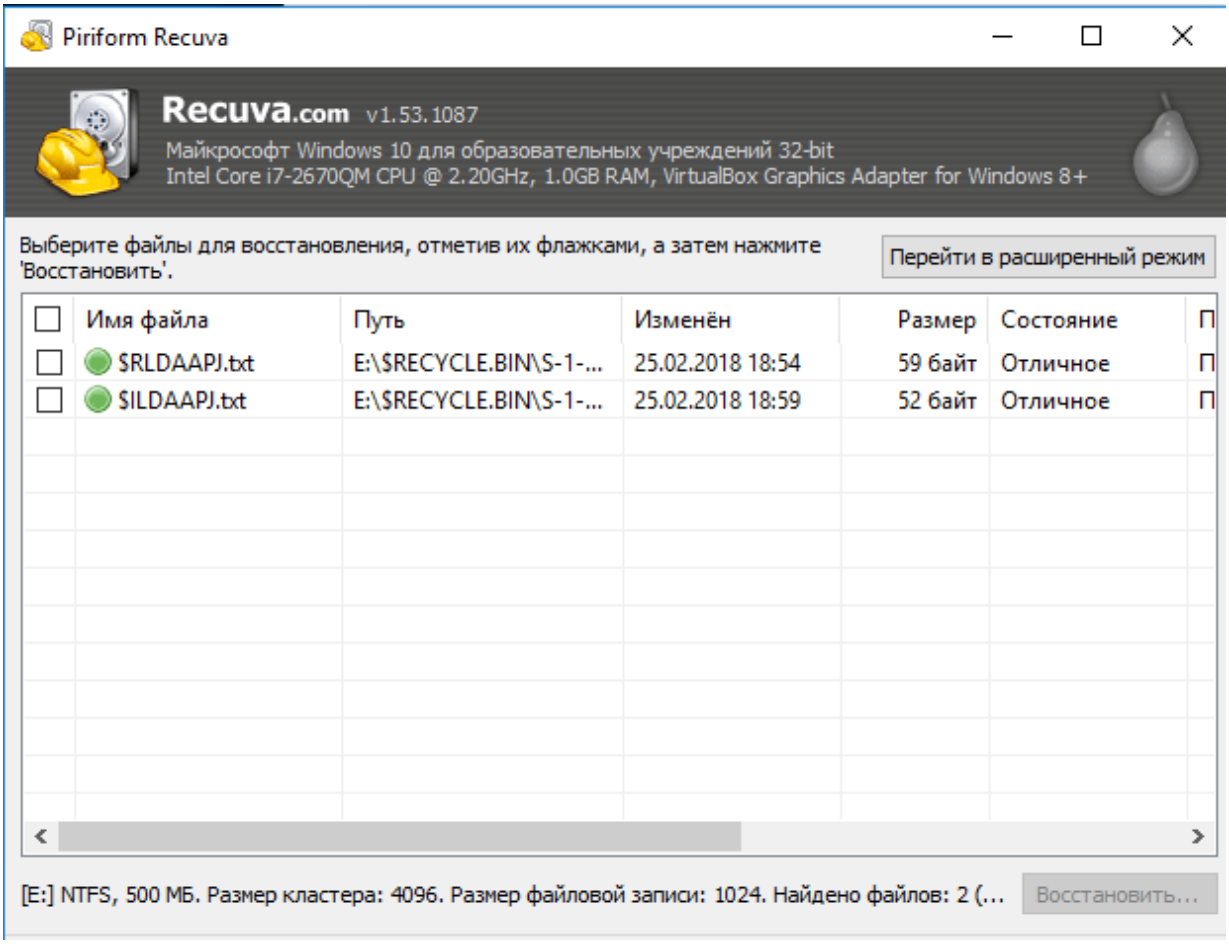


Рисунок 2.7. Выбор файлов для восстановления

11. Получить один или несколько файлов с расширением .txt с неизвестными именами (согласно рис. 2.7). Выделить их все и нажмите кнопку **«Восстановить».**

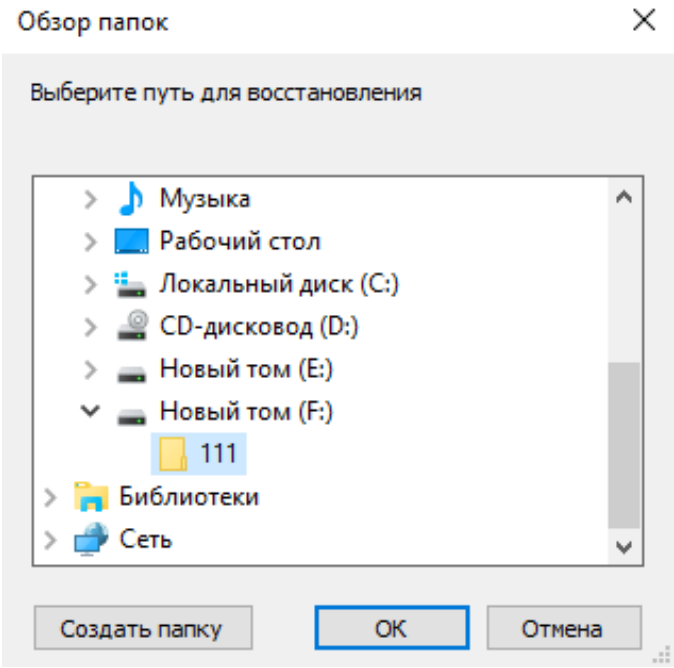


Рисунок 2.8. Выбор носителя для восстановления.

12. В окне **«Обзор папок»** указать папку, в

которую нужно восстановить файлы (см. рис. 2.8). Папка должна находиться на диске, отличном от восстанавливаемого диска. Имя папки задается в соответствии с вариантом задания. Нажмите кнопку **«ОК».**

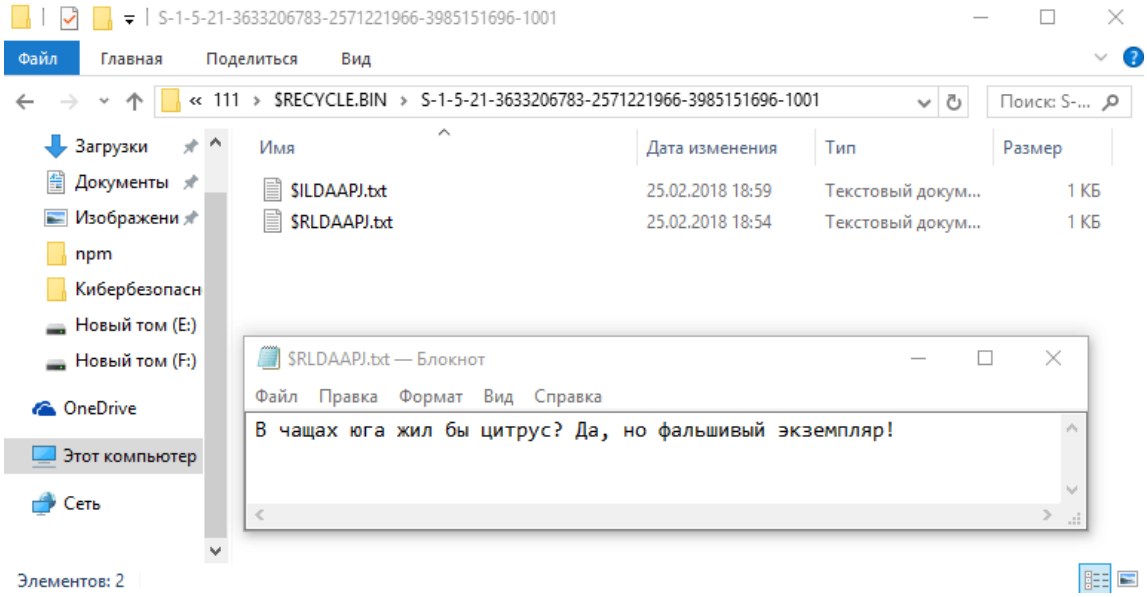


Рисунок 2.9. Просмотр восстановленного файла

13. В папке назначения появились один или несколько файлов. Открыть последовательно их и вы обнаружите удаленный файл (см. рис 2.9). Сделать скриншот окна для отчета, перейдя в основную ОС и нажав клавишу PrintScr.

Задание 3.

Восстановление данных после форматирования раздела.

1. Переименовать восстановленный файл, присвоив ему имя «цитрус.txt». Скопировать его на диск с которого восстанавливали файлы

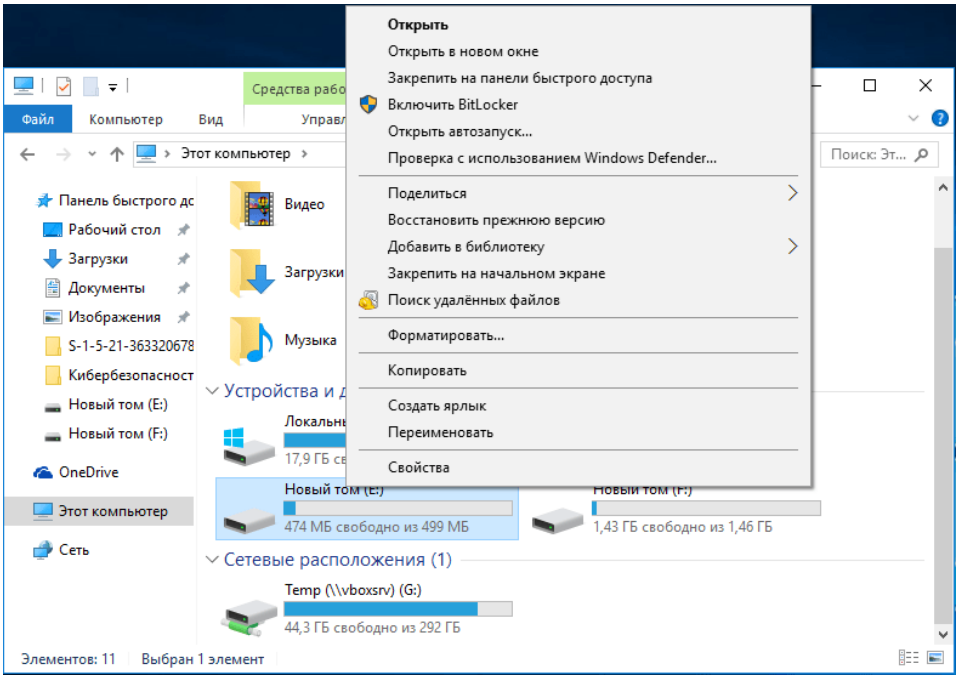


Рисунок 3.1. Выбор диска для форматирования

2. Отформатировать диск (как изображено на рис 3.1).

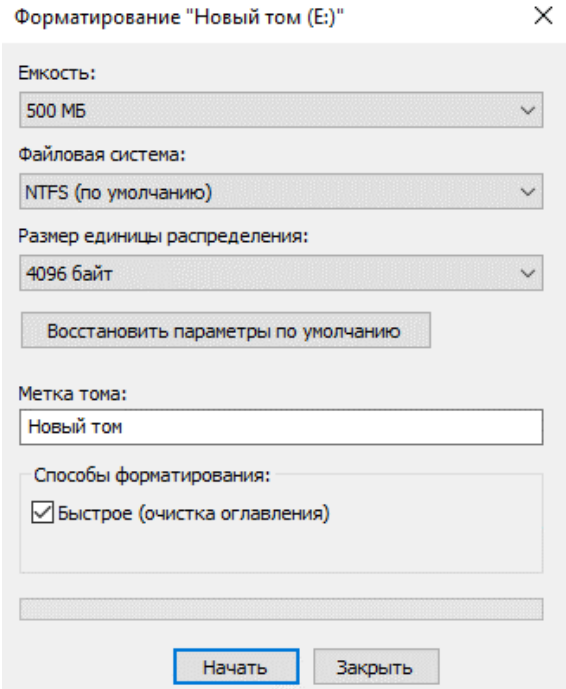


Рисунок 3.2 Окно форматирование диска

3. При форматировании не снимать галочку «Быстрое (очистка оглавления) (см. рис. 3.2). После форматирования диска запустить программу Recuva.exe. Указать размещение на форматированный диск.

4. Установить галочку на **«Включить углубленный анализ»** и нажмите кнопку **«Начать».**

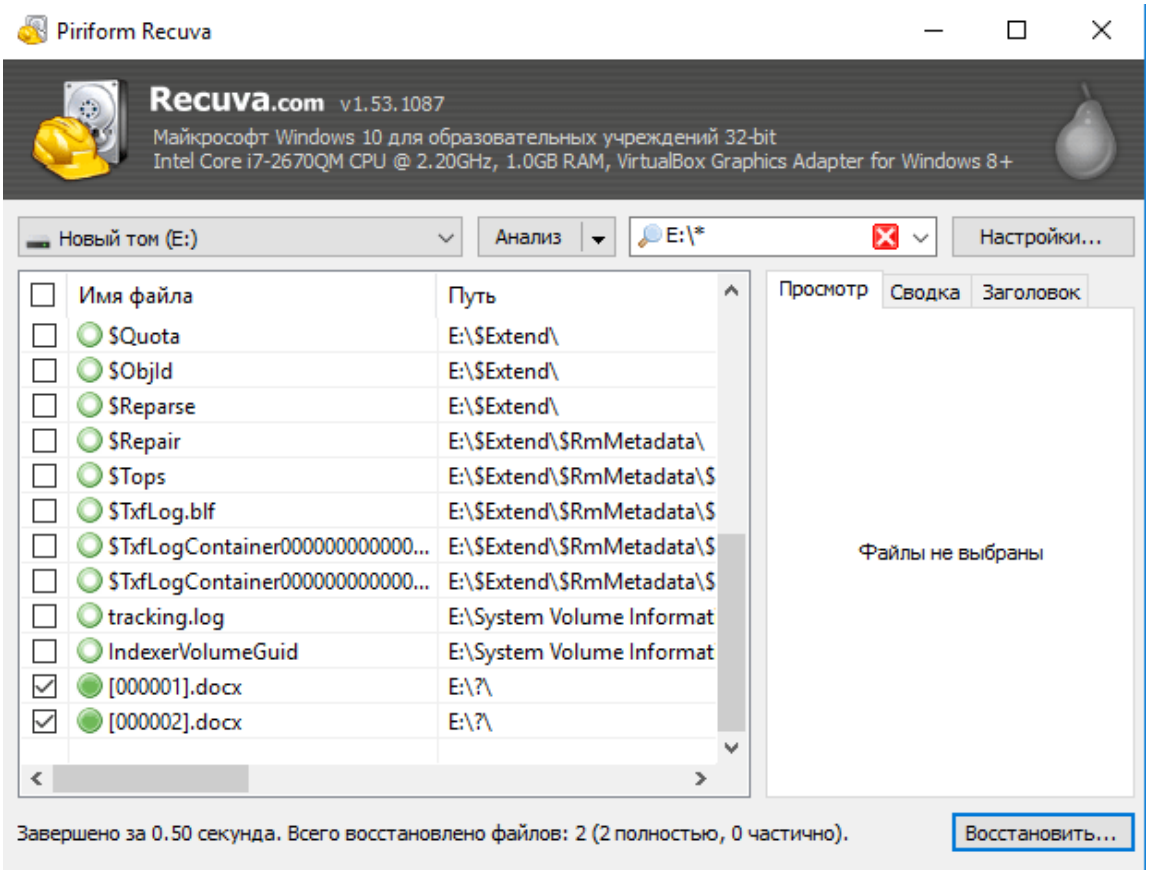


Рисунок 3.3. Восстановления данных после форматирования

5. Можно заметить, что восстановлено достаточно большое количество файлов с уже отформатированного диска (см. рис. 3.3). Среди них два файла с расширением .docx, которые содержат текстовые документы. После восстановления их можно читать.

6. Сделать скриншот окна для отчета, перейдя в основную ОС и нажав клавишу PrintScr.

7. Нажать правой клавишей мышки по кнопке **«Пуск»** и в появившемся меню выберать пункт **«Управление дисками»** (см рис. 3.4).

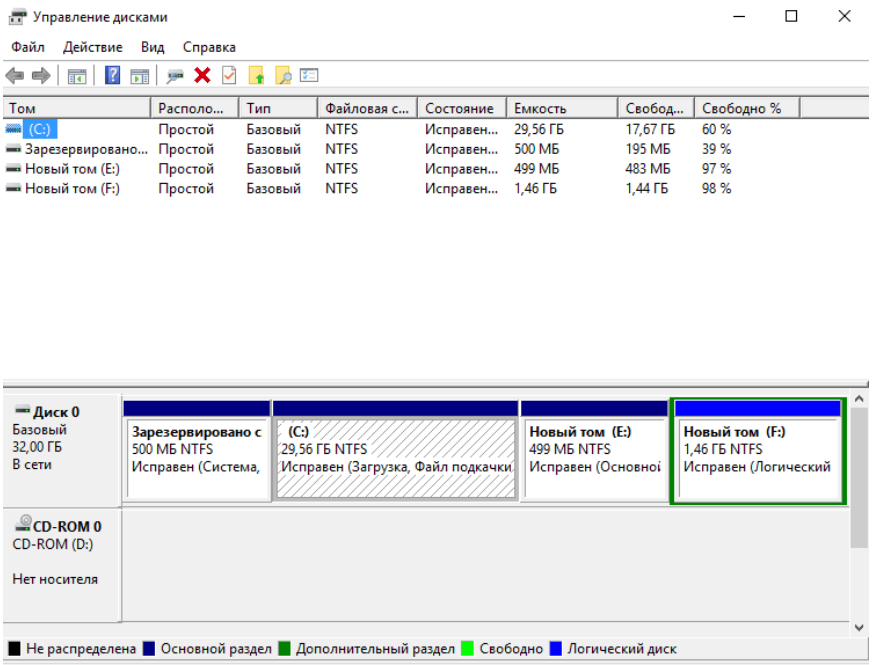


Рисунок 3.4. Управление жесткими дисками

8. Удалить исследуемый раздел с жесткого диска (рис.3.5). Сделать скриншот окна для отчета, перейдя в основную ОС и нажав клавишу PrintScr.

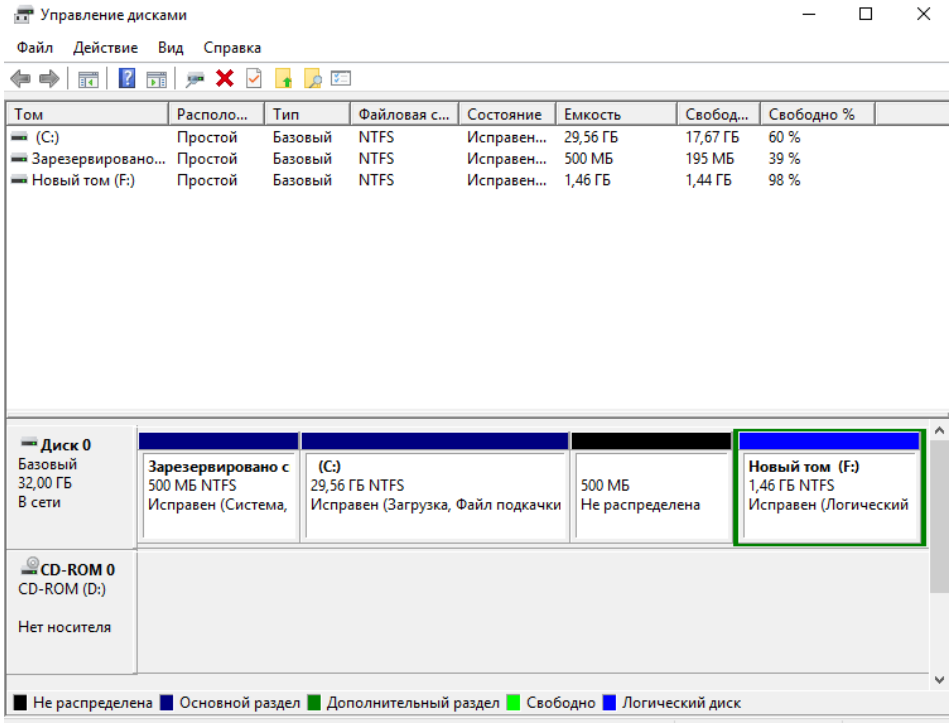


Рисунок 3.5. Удаление раздела диска

9. Создать раздел заново. При создании используйте настройки по умолчанию. С помощью программы Recuva.exe восстановить данные на вновь созданном диске.

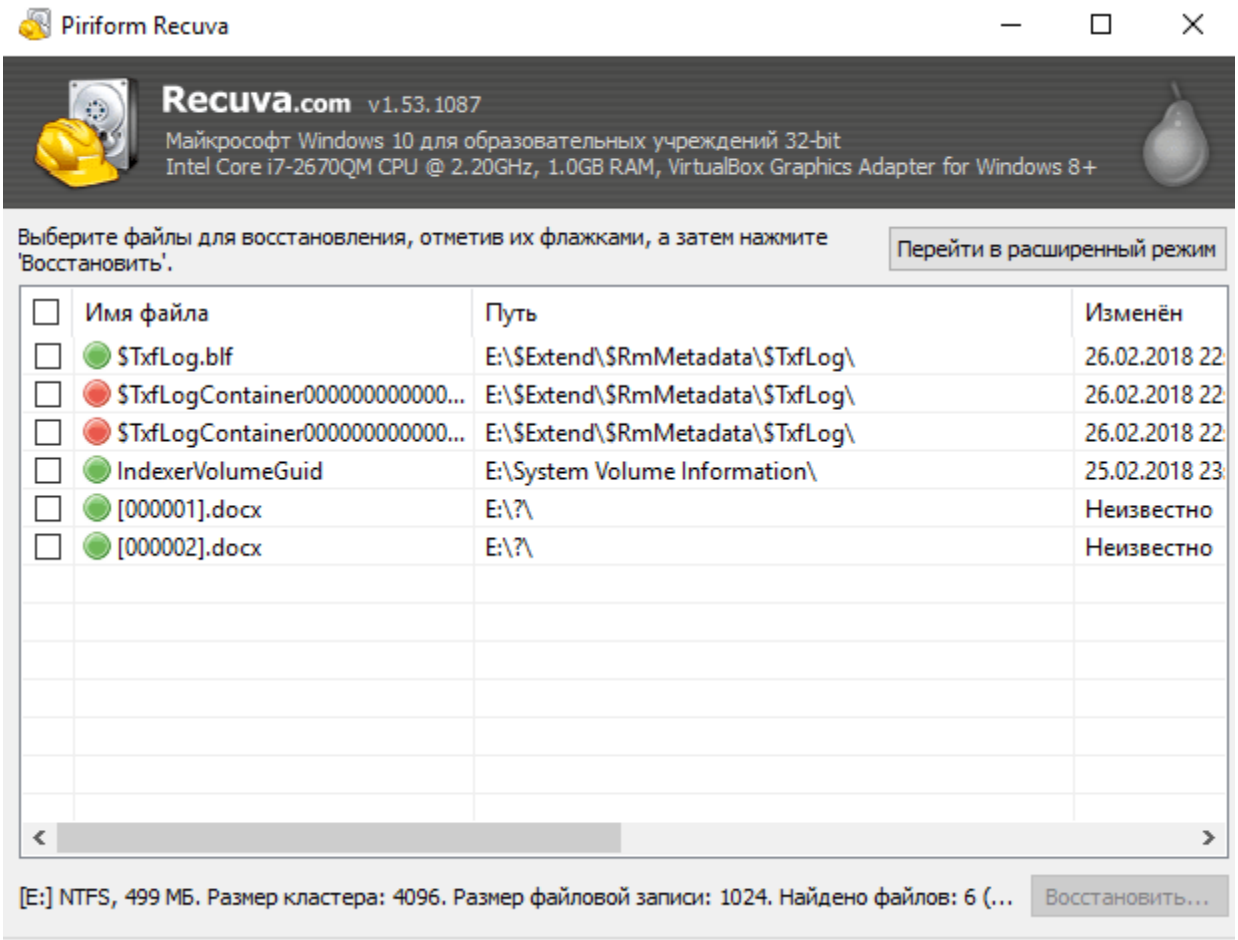


Рисунок 3.6. Данные на диске после удаления раздела

10. Как видно на рис. 3.6, при удалении раздела диска и нового его создания данные смогли уцелеть. Сделайте скриншот окна для отчета, перейдя в основную ОС и нажав клавишу PrintScr.

Задание 4.
Уничтожение данных без возможности восстановления.

1. Отформатировать диск со снятой галочкой «Быстрое (очистка оглавления). После форматирования диска запустить программу Recuva.exe. Указать размещение на форматированный диск.

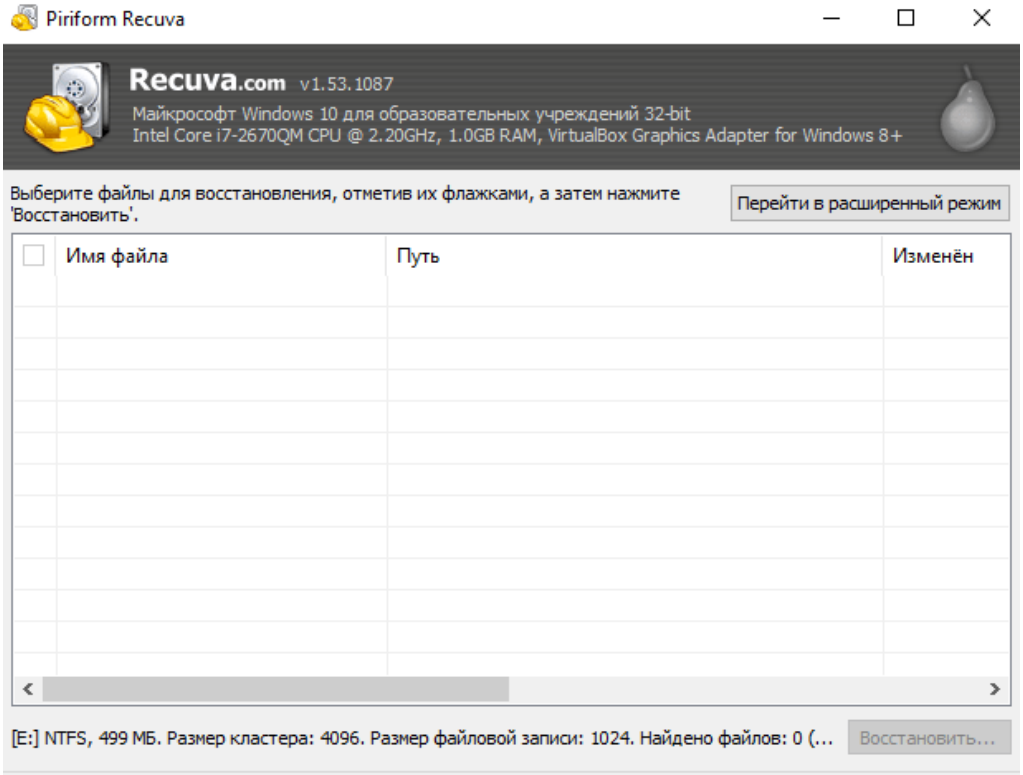


Рисунок 4.1. Данные на диске после полного форматирования

2. Наконец-то данные были уничтожены и ничего не восстановилось (см. рис. 4.1). Однако и в этом случае о надежном уничтожении данных говорить рано. С помощью более продвинутых программ часть информации можно восстановить. Чтобы надежно уничтожить данные необходима программа ***Disk Wipe***.

3. Найти и скачать в сети Интернет программу для удаления данных ***Disk Wipe*** (как изображено на рис. 4.2).

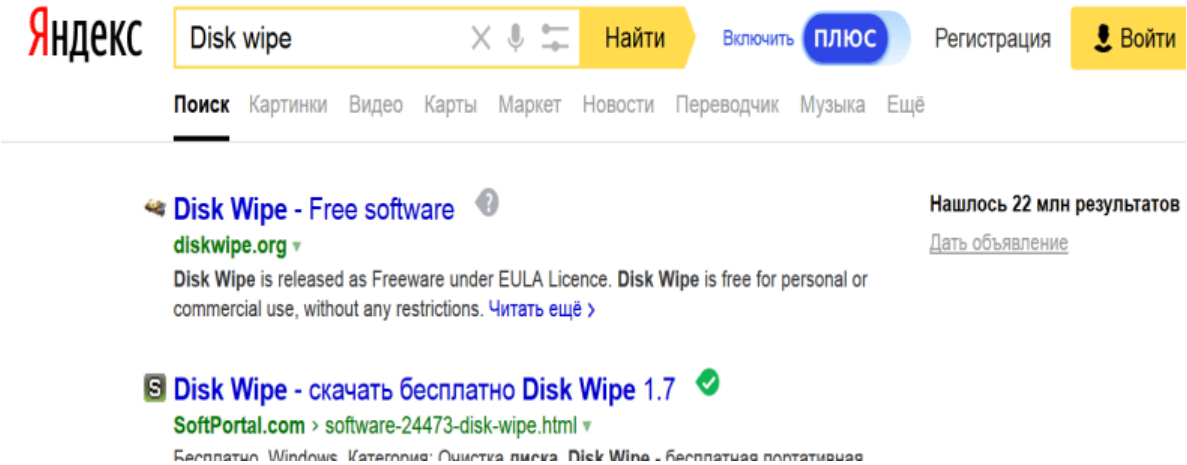


*Рисунок 4.2. Поиск программы **Disk Wipe**.*

4. Запустить скачанную программу ***Disk Wipe,*** нажав на иконку.

5. В рабочем окне программе (см рис. 4.3) выбирать диск, данные на котором хотите безвозвратно уничтожить и нажмите на кнопку **Wipe Disk.**

DiskWipe

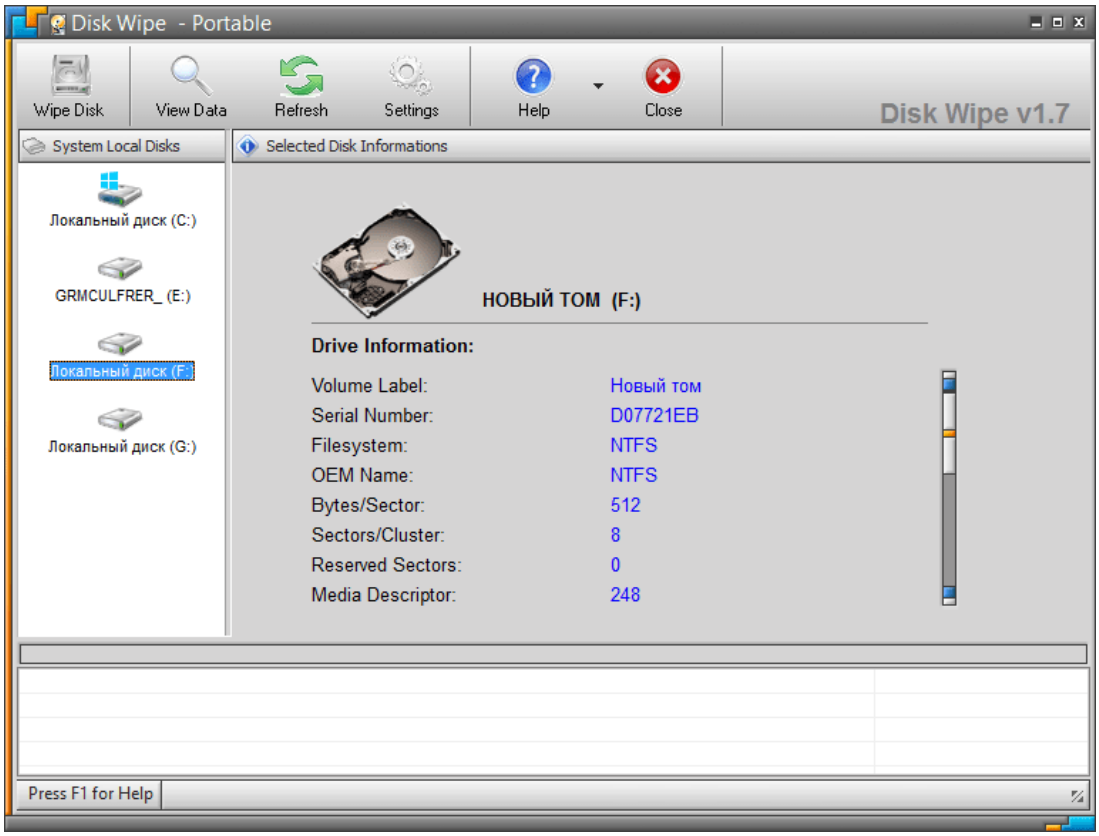


*Рисунок 4.3. Рабочее окно программы **Disk Wipe**.*

6. В открывшимся окне выбирать тип файловой системы жесткого диска (рекомендуется NTFS) (см. 4.4). Не забудьте снять флажок с быстрого форматирования (**Perform Quick Format**).

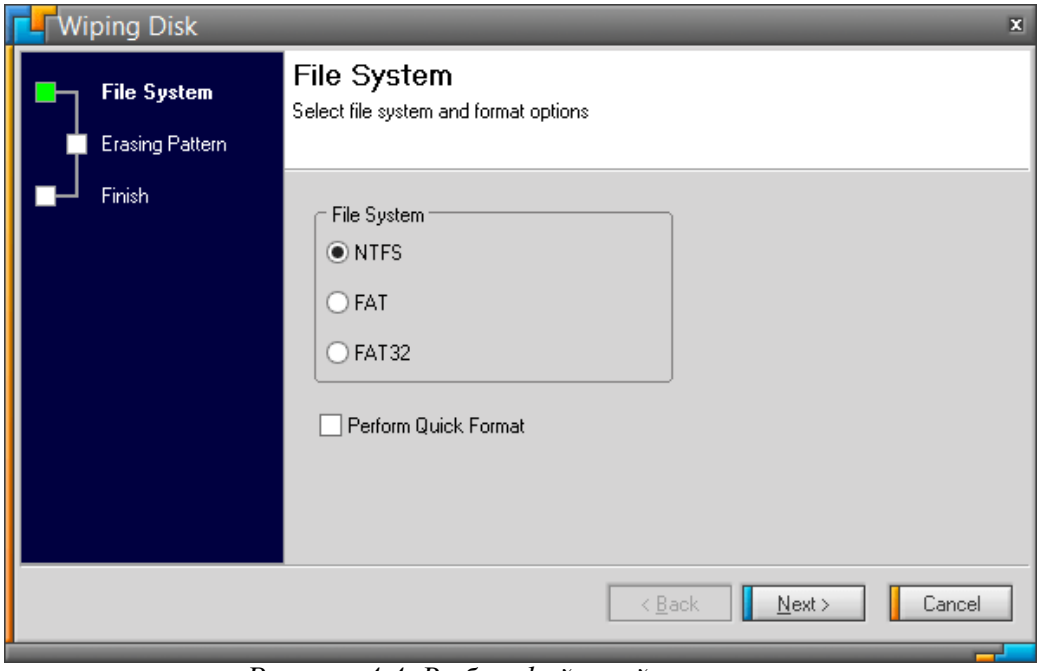


Рисунок 4.4. Выбор файловой системы.

7. Обычное форматирования заполняет нулевыми битами кластеры жесткого диска. Disk Wipe позволяет создать имитацию заполненных данных заполняя случайным набором бит. Для этого необходимо выбрать флажок **One Pass Random (quick)** (см. рис. 4.5).

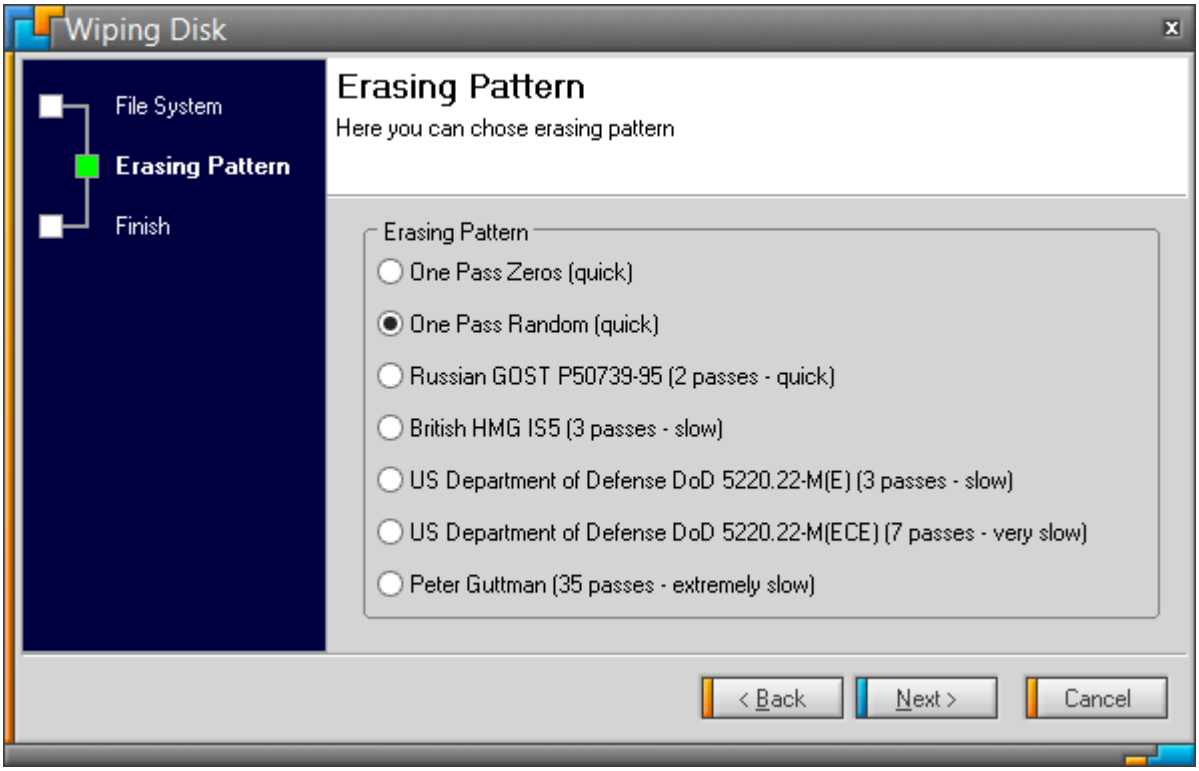


Рисунок 4.5. Выбор типа форматирования.

8. В последнем окне (рис. 4.6) для уничтожения данных необходимо вписать **"ERASE ALL".**

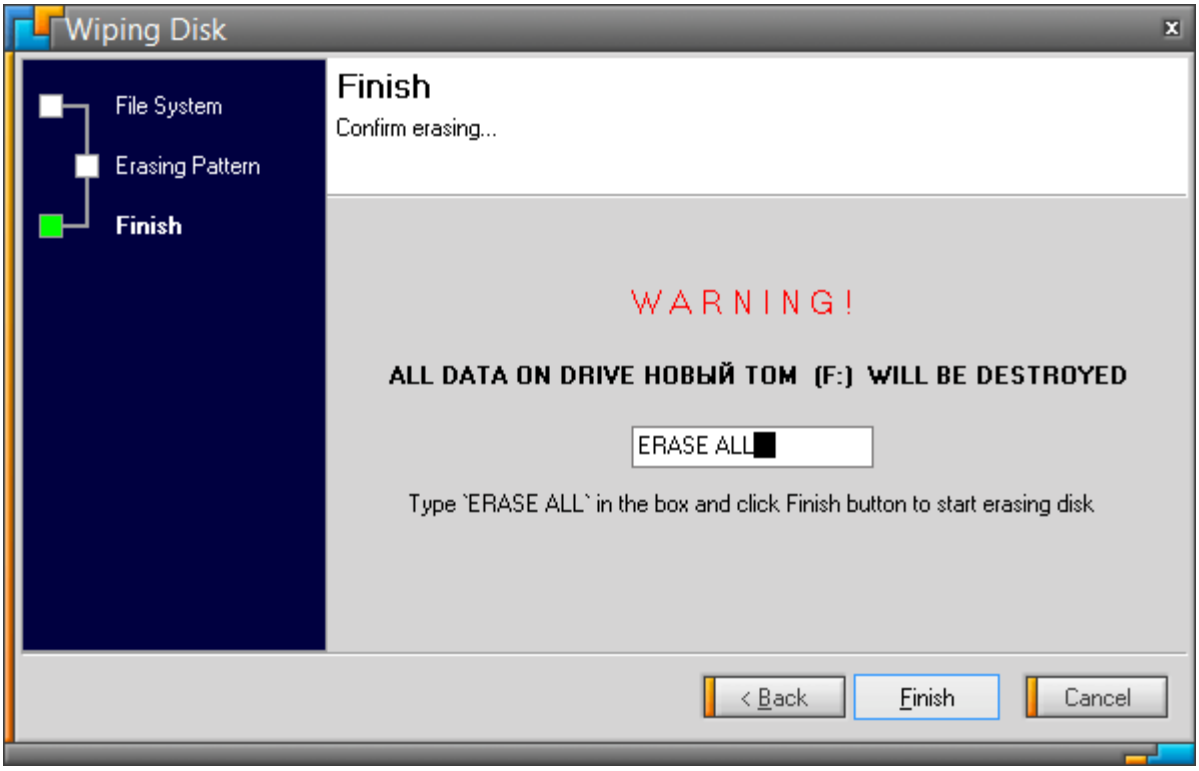


Рисунок 4.6. Команда для подтверждения операции

9. После окончания операции уничтожения данных вся информация на данном разделе жесткого диска будет удалена безвозвратно. Открыть программу Recuva и посмотрите на содержимое жесткого диска после затирания данных случайной информацией.

10. Для уничтожения информации в отдельных файлах существуют специальные программы. Если это необходимо сделать незаметно, то сделайте дефрагментацию данных на жестком диске. Программе переставит байты информации, оптимизируя работу диска и перезапишет удаленные данные новыми. Для этого необходимо кликнуть по выбранному диску правой клавишей мыши и в появившемся меню выберите **«Дефрагментация»**. Понаблюдат за процессом дефрагментации.

11. По окончании сделать скриншот окна для отчета, перейдя в основную ОС и нажав клавишу Alt+PrintScr.

Индивидуальные варианты

Таблица 1 – варианты заданий

№ п/п	Имя папки	Имя файла
1	canenclem	bookbinder
2	heaconric	apron
3	drulatcra	gendarme
4	booglapra	anarchist
5	kilrimhus	quidnunc
6	pacunbinf	locksmith
7	ditarract	adventurer
8	droworran	beaver
9	proailpra	athlete
10	dovstrdef	midwife
11	booselgru	holidayer
12	pasanngab	aquacckit
13	midexphol	kitten
14	abbskumin	critic
15	abdquiaer	albatross
16	idesmowal	renter
17	parcozaca	costumier
18	orideptes	grazier
19	farpulpil	miller
20	motdisdem	pilgrim
21	scabeddet	duck
22	coslikint	meteor
23	baredugoo	mendicant

Раздел 2

Лабораторная работа № 3.
Защита текстовых документов

В данной лабораторной работе рассматриваются основные вопросы защиты документов различных форматов.

Цели:

•Защитить текстовый документ от изменения, форматирования и редактирования.

•Зашифровать документ и заверить его подлинность электронной цифровой подписью.

•Электронную таблицу пометить как окончательный документ .

•Защитить PDF-документ от несанкционированного открытия и копирования данных.

Задание 1.
Ограничение редактирования тестового документа в редакторе Microsoft Word.

1. Открыть документ Microsoft Word (например, реферат по прикладным аспектам кибербезопасности), затем на панели инструментов зайти в закладку «Рецензирование» и выбрать пункт «Ограничить редактирование» (см. рис.1.1):

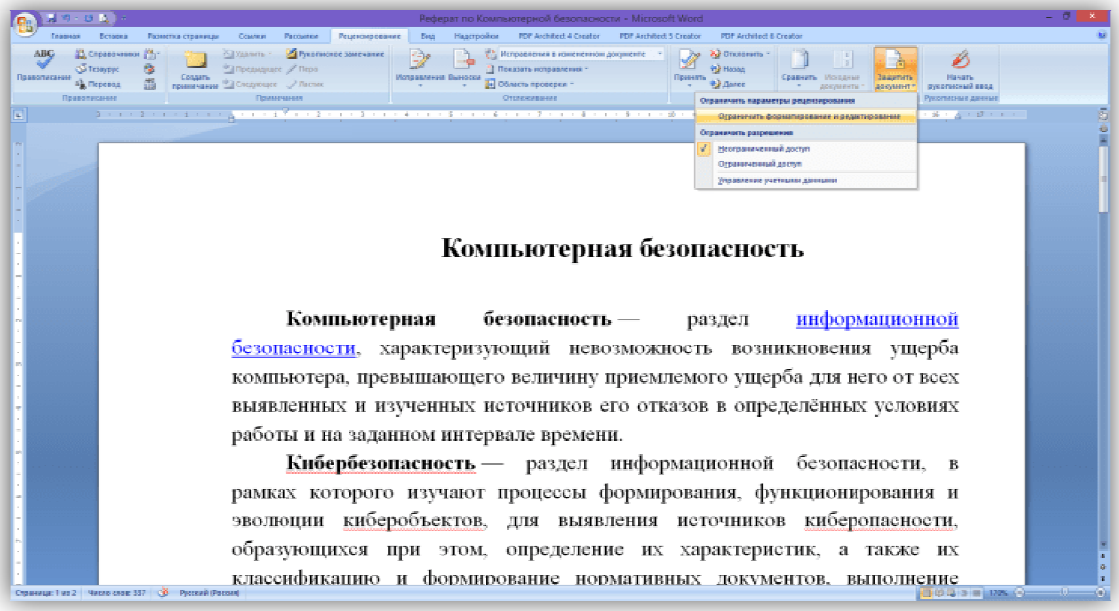


Рисунок 1.1. Ограничение редактирования

2. В появившемся окне справа поставить флаг в окне «Разрешить только чтение».

3. Затем нажать на кнопку «Да, включить защиту» (см. рис. 1.2).

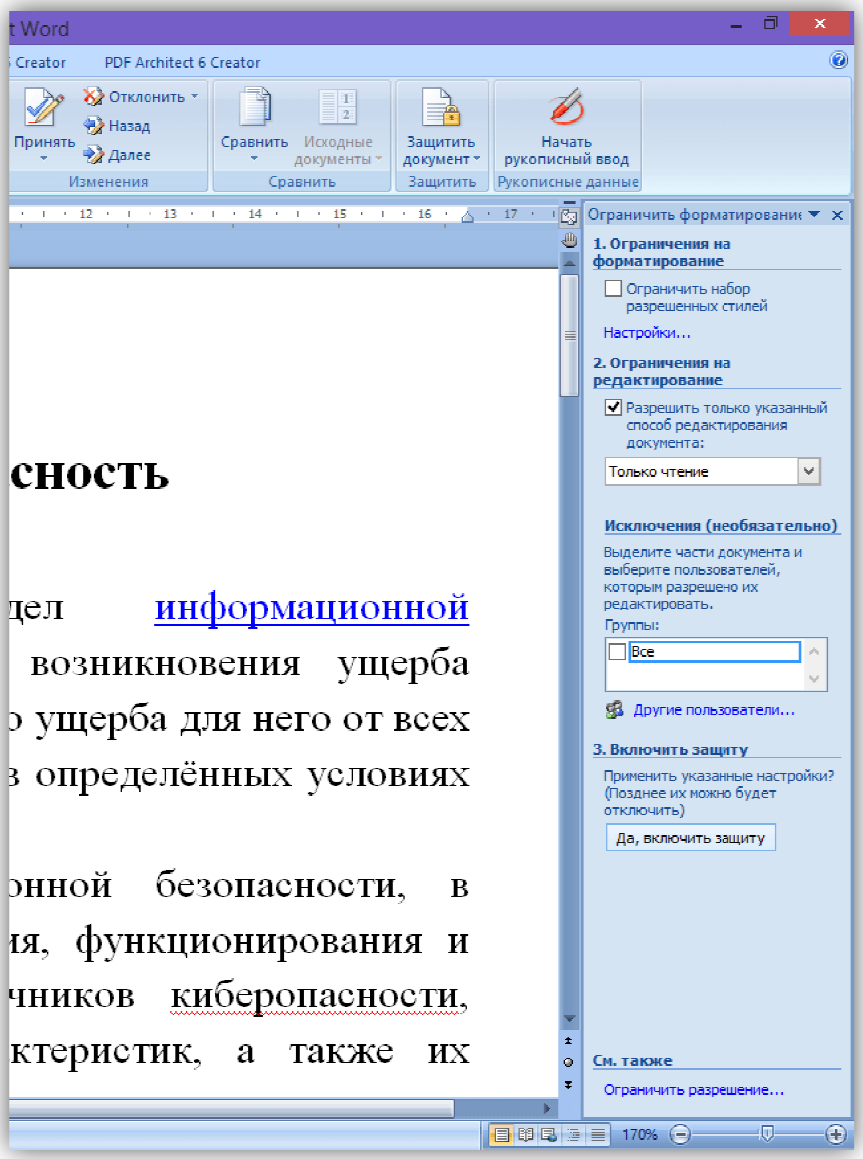


*Рисунок 1.2. Включение режима **"Только чтение"***

4. В появившемся окне (см. рис. 1.3) ввести пароль, подтвердить его. Нажать кнопку ***"ОК"***.

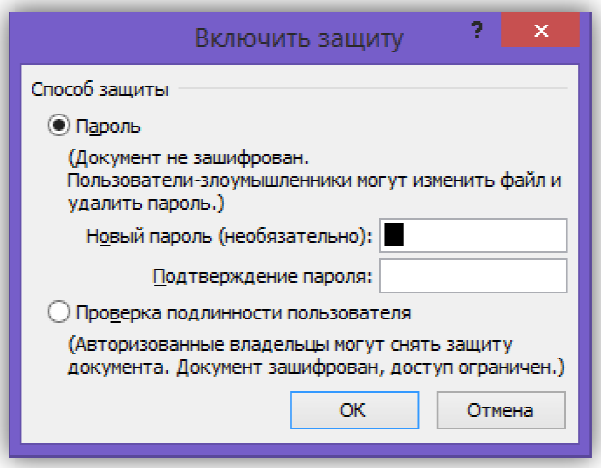


Рисунок 1.3. Включение парольной защиты

5. Документ теперь нельзя будет редактировать, а панель инструментов заблокирована, что можно увидеть на рис. 1.4.

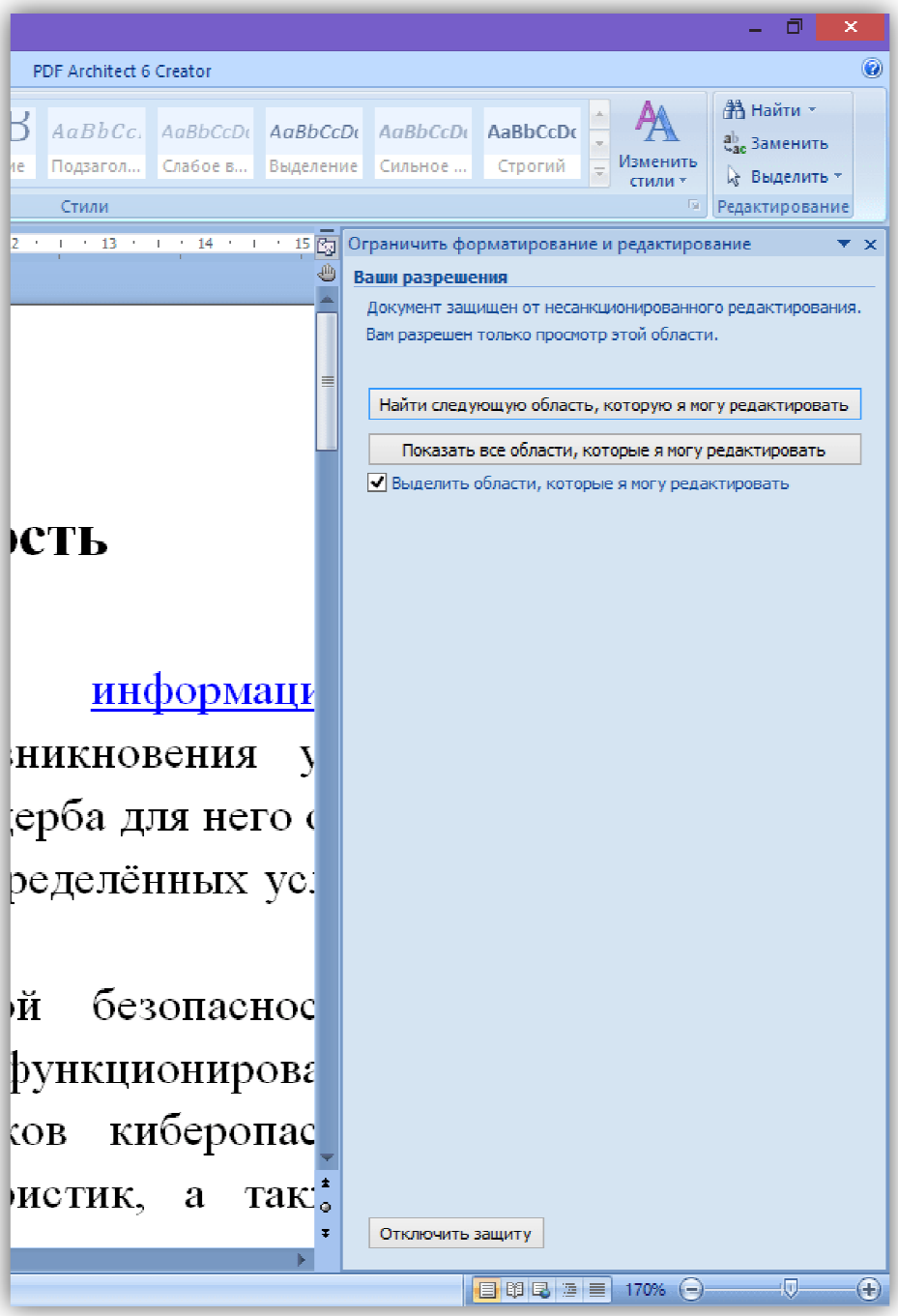


Рисунок 1.4. Отключение парольной защиты

6. Сделать снимок экрана полученного документа и добавить в отчет.

Задание 2.

Пометить документ Microsoft Word как окончательный.

1. Открыть документ Microsoft Word, в разделе «Файл» выбрать закладку «Подготовить» и функцию «Пометить как окончательный»
(см. рис. 2.1).

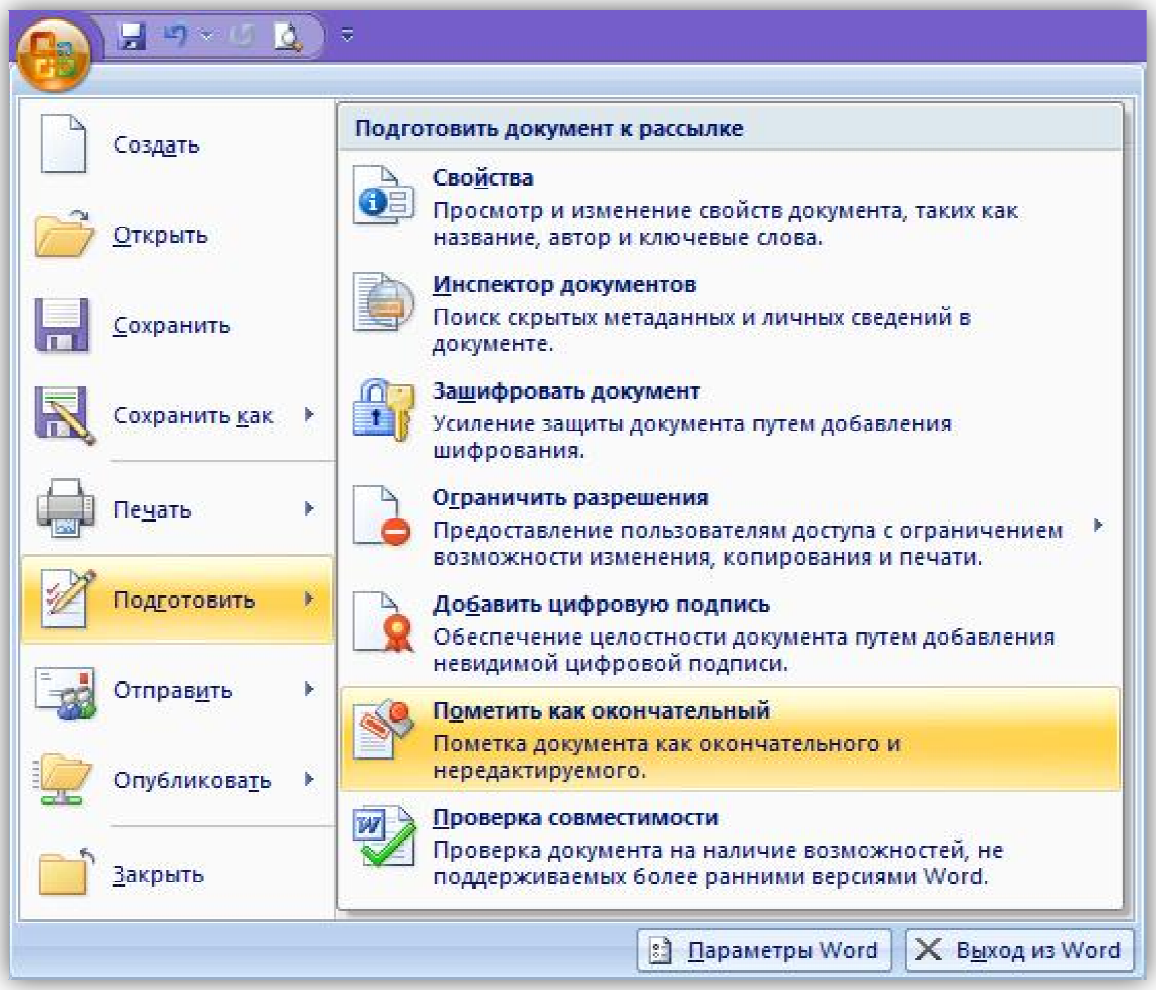


*Рисунок 2.1. Раздел **"Подготовить"***

2. Документ стал окончательным и доступен только для чтения.

Как можно заметить заблокировались кнопки на верхней панели.

3. С этого момента в документе нельзя ничего изменить добавить и даже поменять оформление.

4. Сделать снимок окна полученного документа и добавить его в отчет по лабораторной работе.

Задание 3.
Шифрование документа редактором Microsoft Word с использованием пароля.

1. Открыть документ Microsoft Word, созданный в предыдущем задании и пересохранить его под именем "Зашифрованный".
2. Затем в разделе «Файл» открыть закладку «Подготовить» и функцию «Защитить документ».

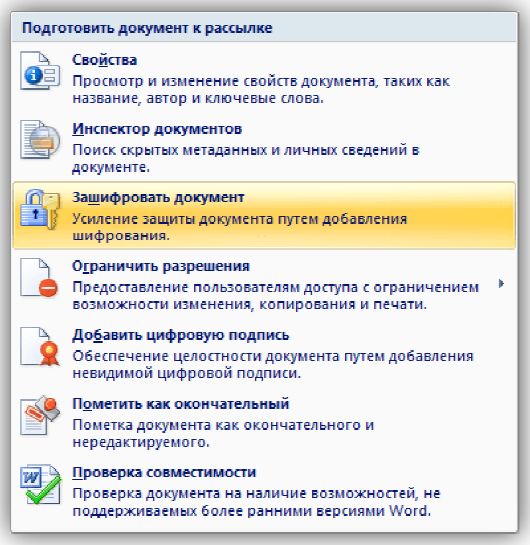


*Рисунок 3.1. Функция **"Зашифровать паролем"***

3. В открывшемся окне выбрать функцию «Зашифровать паролем».

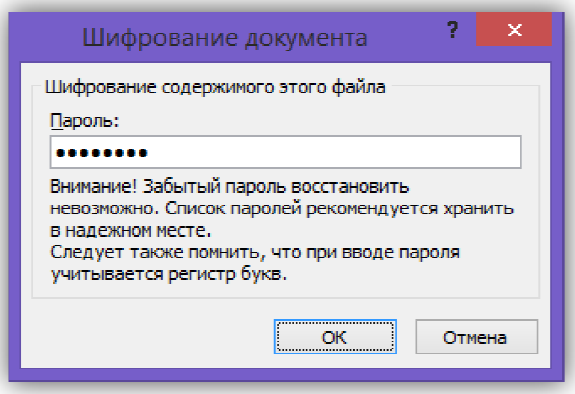


*Рисунок 3.2. Окно **"Ключ шифрования"***

4. В появившемся окне (см. рис. 3.2) ввести пароль, подтвердить его. Теперь при открытии документа Word будет необходимо вводить пароль в качестве ключа шифрования (см. рис. 3.3).

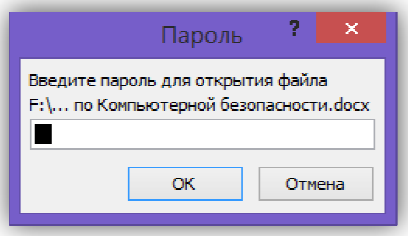
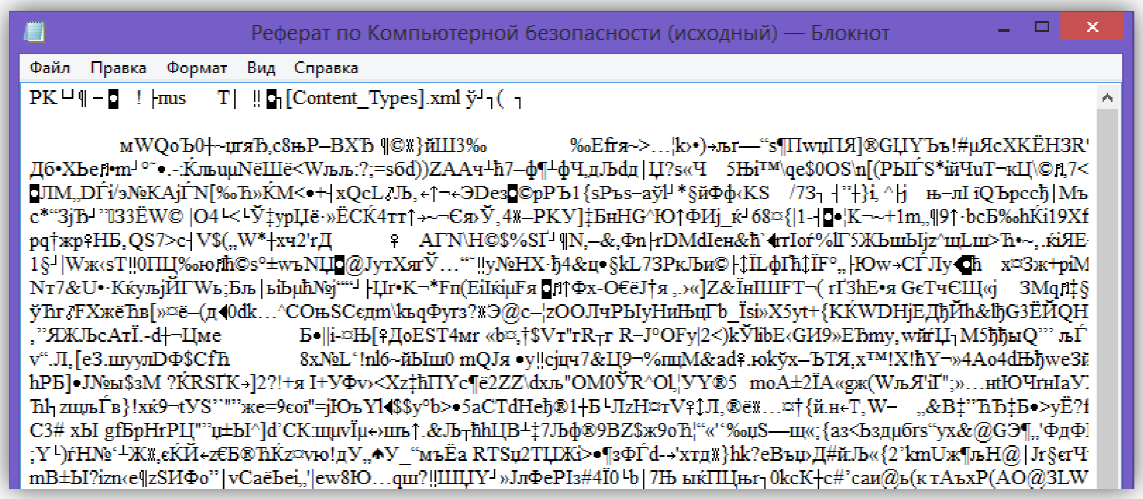
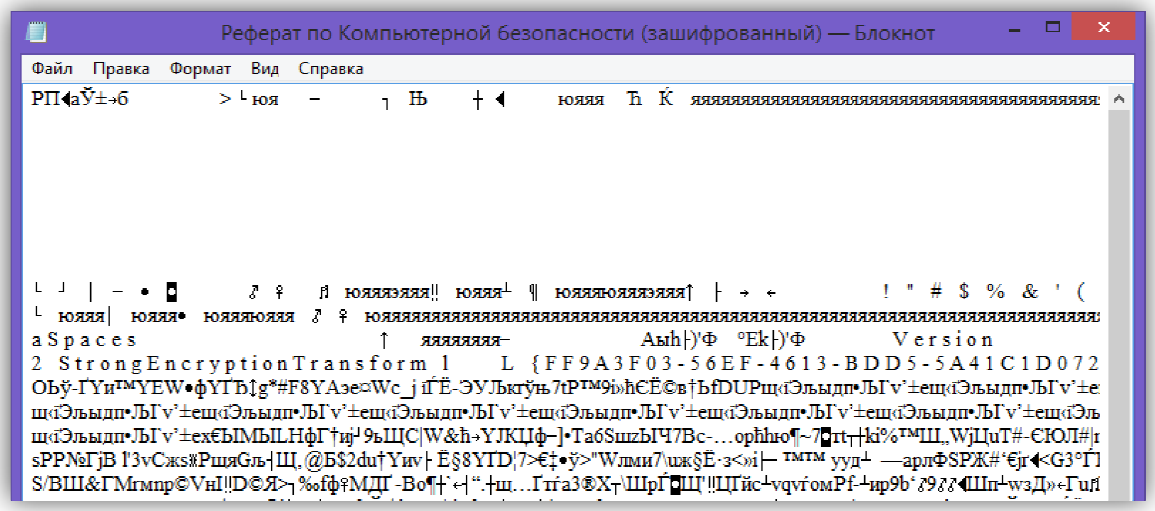


*Рисунок 3.3. Окно **"Введите ключ шифрования"***

5. Процесс шифрования документа отличается от пароля на открытие файла или разрешений форматирование тем, что поддается криптографическим преобразованиям внутренняя часть документа и изменяется его структура. Тем самым, при открытии кода файла нельзя будет добыть его содержимое. Чтобы продемонстрировать этот эффект, откройте этот файл с помощью текстового редактора "Блокнот" и точно также откройте исходный документ. Сравните его код, как показано на рисунке 3.4.



а)



б)

Рисунок 3.4. Структура исходного а)(сверху) и зашифрованного б)(снизу) документа

6. Как видно из рисунка 3.4, структура файла полностью изменилась. Об использовании встроенной в ***MS Word*** процедуры шифрования говорят,

например, надписи "Microsoft Enhanced RSA and AES Cryptographic Provider" и "Strong Encryption Transform".

7. Примечание: в тот момент когда зашифрованный документ открыт, на него не распространяется защита MS Word и из него возможно скопировать информацию другим пользователям, например, с помощью команды ***"Вставка"→"Объект"→"Текст из файла"***.

8. На всех стадиях шифрования документа необходимо сделать скриншоты рабочего экрана для последующего добавления в отчет студента.

Задание 4.
Добавление цифровой подписи в Microsoft Word.

1. Открыть документ Microsoft Word, в разделе «Файл» выбрать раздел «Подготовить». В появившемся окне выбрать функцию «Поставить цифровую подпись» (см. 4.1).

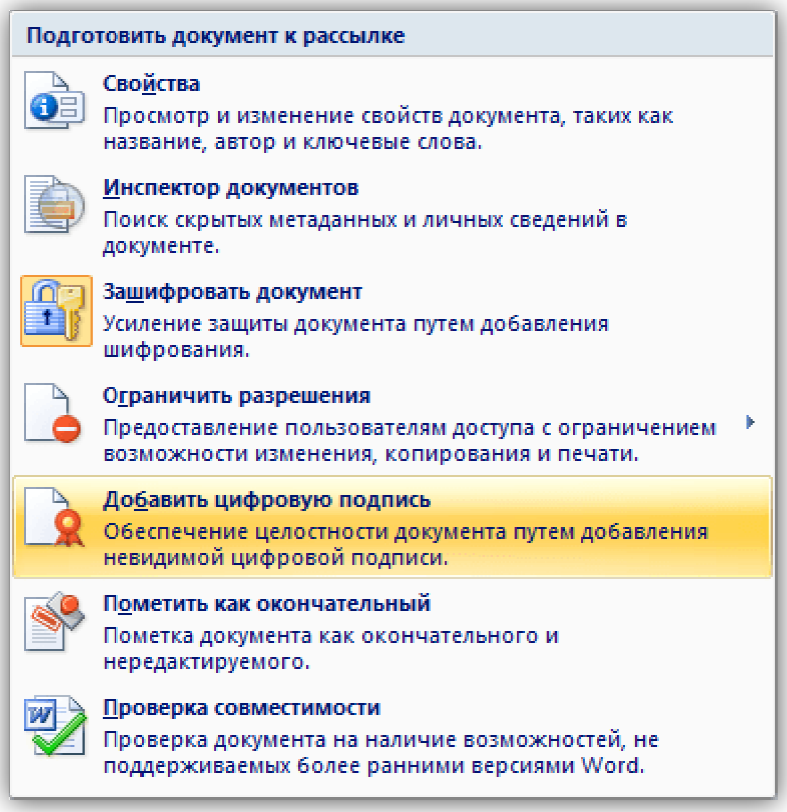


*Рисунок 4.1. Функция **"Добавить цифровую подпись"***

2. Чтобы в дальнейшем подлинность созданной электронной цифровой подписи (ЭЦП) мог проверить любой пользователь из любой точки мира, необходимо, чтобы она хранилась на некотором облачном сервисе. Поэтому при создании ЭЦП сервис Microsoft предложить воспользоваться таким сервисом. (см. рис. 4.2).

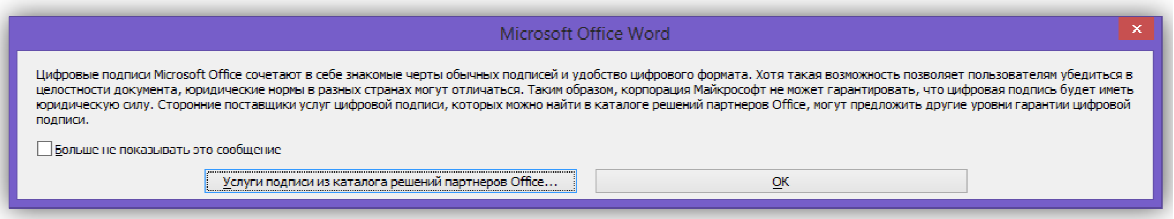


Рисунок 4.2. Услуга "Каталог решений"

3. В рамках лабораторной работы создать локальную ЭЦП. Для этого в открывшемся окне выбрать «Создать свое цифровое удостоверение». (см. рис. 4.3).

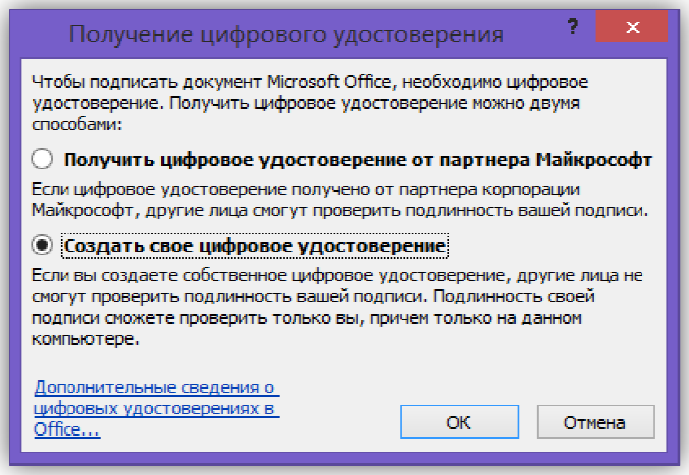


Рисунок 4.3. Окно "Получение цифрового удостоверения"

4. Ввести "Имя", "Адрес электронной почты", "Организация" и "Расположение", согласно данных на рисунке 4.4.

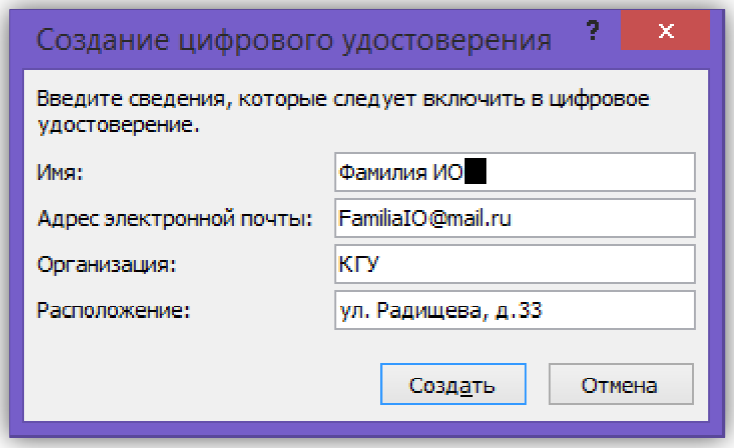


Рисунок 4.4. Окно "Создание цифрового удостоверения"

5. В следующем окне введите в поле "Цель подписания документа" текст "Лабораторная работа №3". (см. рис. 4.5).

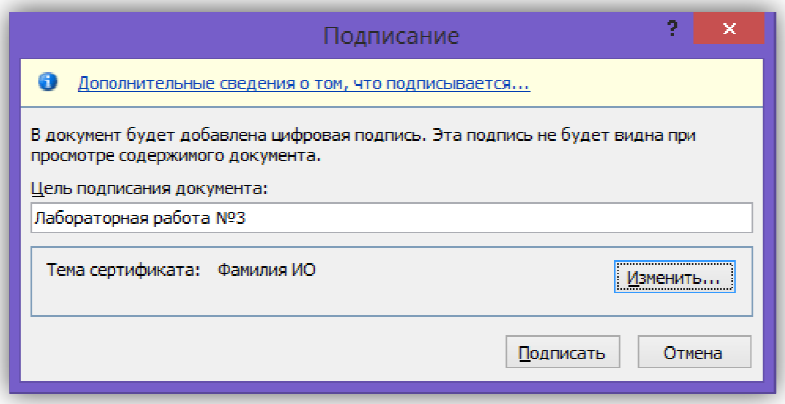


Рисунок 4.5. Окно "Подписание"

6. Перед созданием Вы можете просмотреть будущий сертификат и при необходимости скорректировать на нем данные. Для этого необходимо нажать на кнопку ***"Изменить"***. (см. рис. 4.5).

7. Вначале нужно подтвердить сертификат конпкой ***"ОК".***

(см. рис. 4.6)

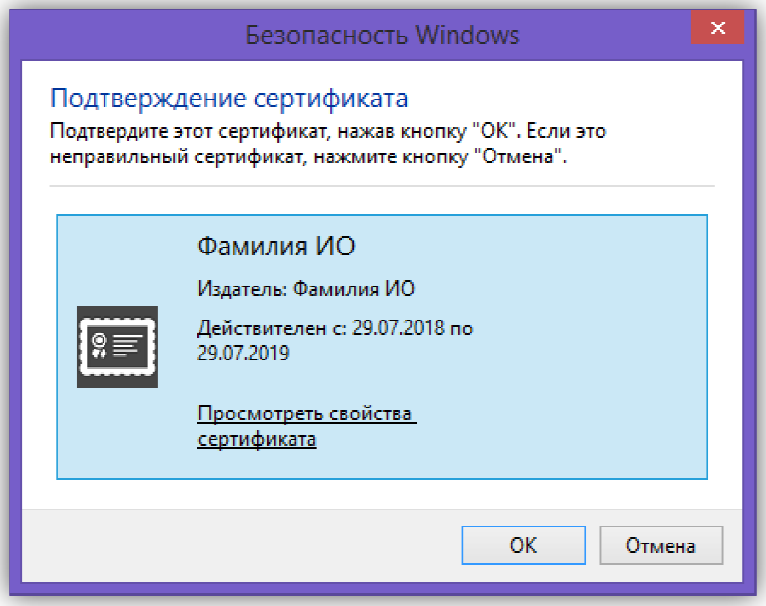
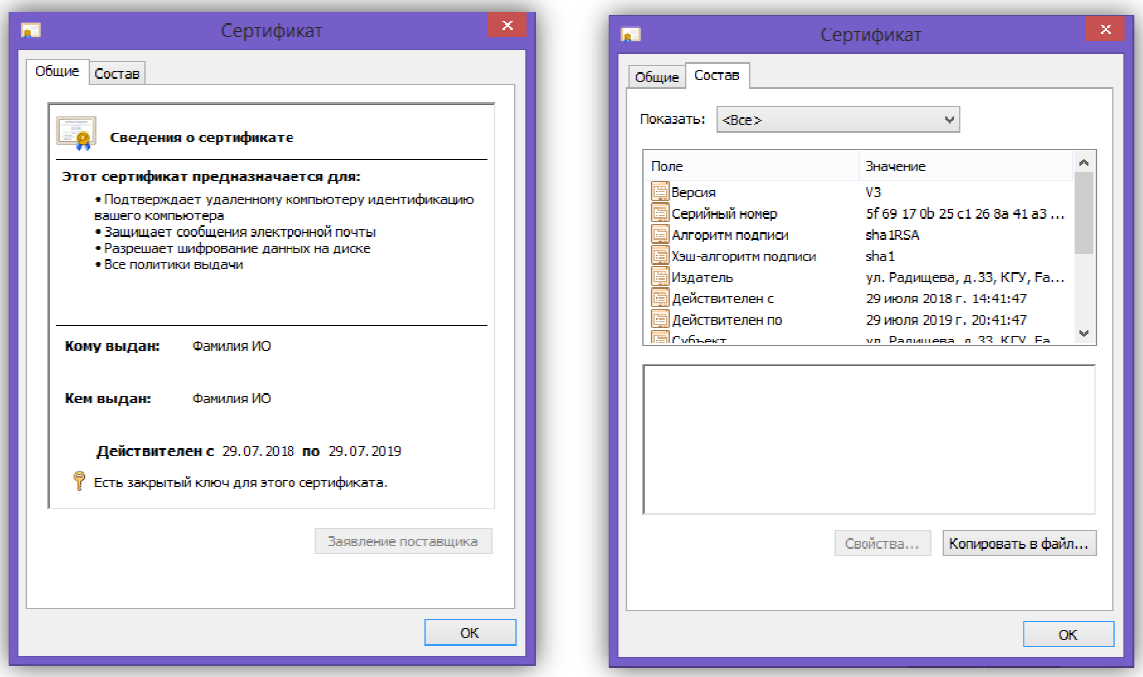


Рисунок 4.6. Окно "Подписание"

8. В открывшимся шаблоне сертификата Вы можете увидеть основную информацию об автора сертификата и сроках действия политики безопасности. На второй странице ***"Состав"*** (см. рис. 4.7) содержится информация о методе и ключах шифрования, а также дополнительная информация, запонелненная в пердыдущих полях выше.



а) *б)*

Рисунок 4.7. Окно "Сертификат"

9. После ознакомления с данными сертификата, вернуться к окну "Подписание" на рис. 4.5 и нажать кнопку «Подписать». Документ будет автоматически сохранен вместе с заверенной цифровой подписью. (см. рис.4.8)

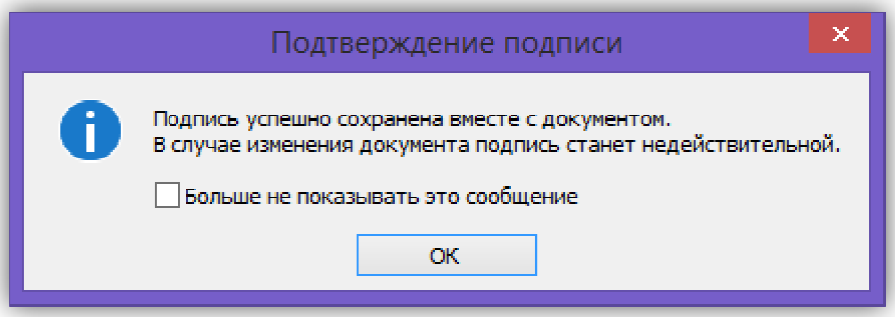


Рисунок 4.8. Окно "Подтверждение подписи"

10. При открытии документа Вы можете также обнаружить, что после установки цифровой подписи все панели заблокированы от форматирования и редактирования (см. рис.4.9), аналогично результату в задании 2.

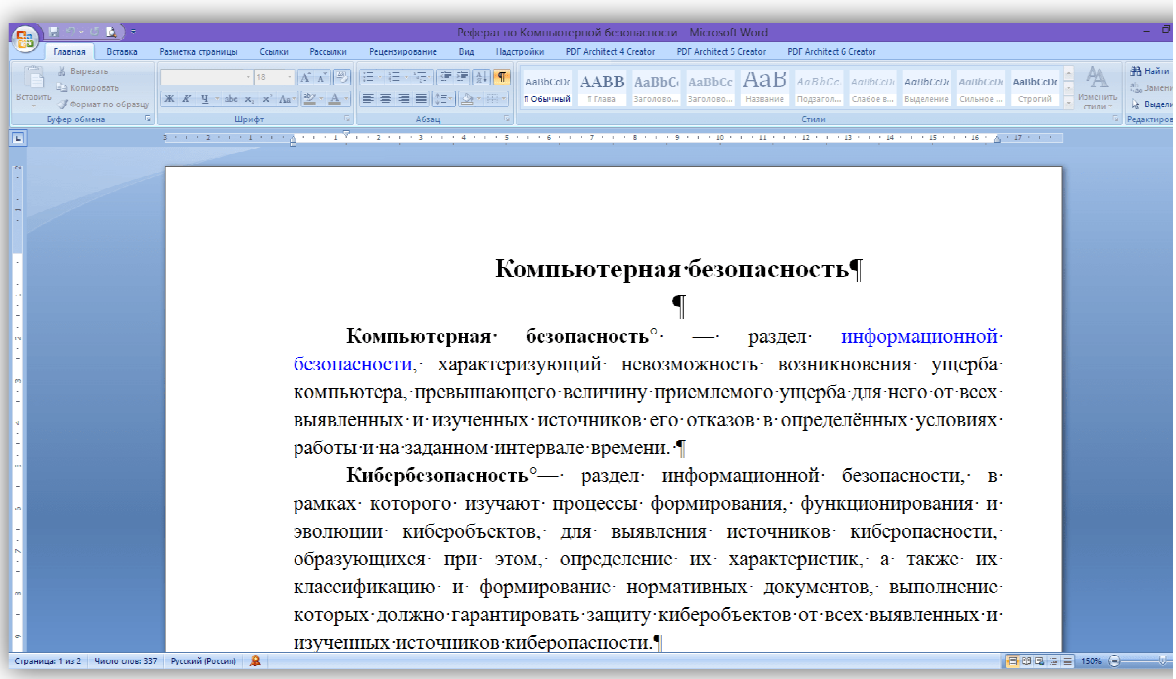


Рисунок 4.9. Пример документа, подписанного электронной цифровой подписью.

11. Свидетельство наложения на документ ЭЦП можно обнаружить внизу документа при помощи специальной иконки. После нажатия на эту пиктограмму сбоку появиться панель с электронными подписями, наложенными на данный документ.

12. Сделать скриншот данного документа и вставить в отчет по лабораторной работе.

Задание 5.
Проверка подлинности электронной подписи и подписание документа двумя сторонами.

1. Документ с электронной подписью необходимо сохранить.
2. Разбиться в группе по парам и обменяться с одногруппником документами, заверенными ЭЦП.
3. Открыть полученный документ.
4. Обратите внимание, что в верхней части документа появилась панель ***"Подписи"*** (см. рис. 5.1).

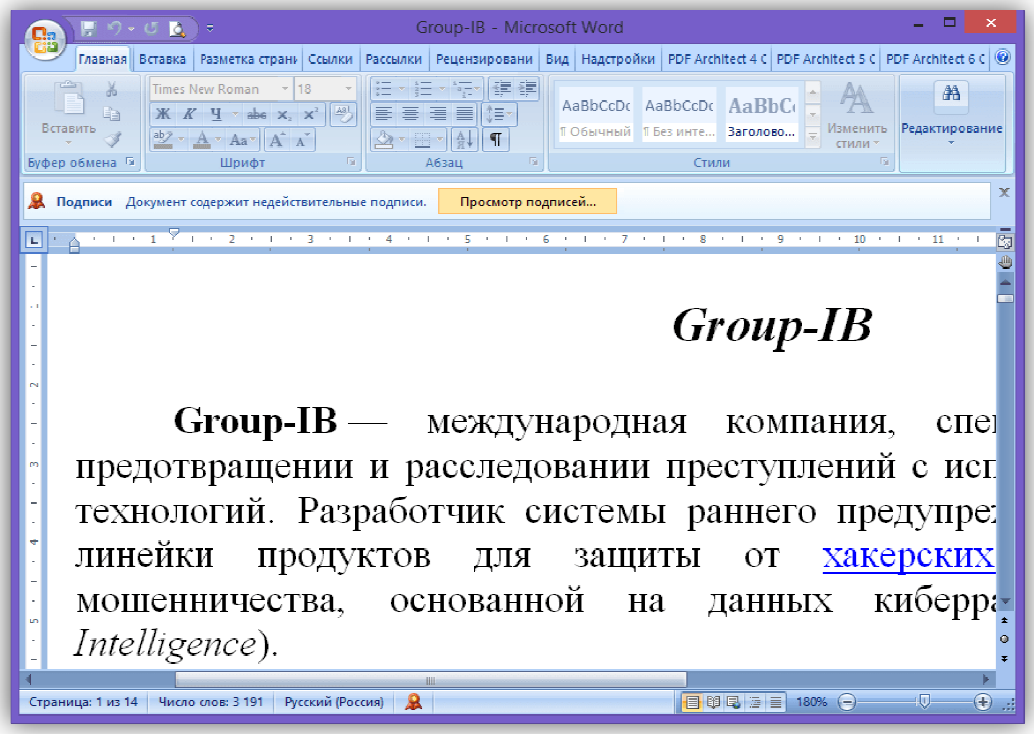


Рисунок 5.1. Документ, заверенный ЭЦП

5. Проверить подлинность ЭЦП можно нажав на значок  или на кнопку Просмотр подписей... .
6. Нажмите на подпись вашего напарника и в выпадающем меню подписи выберите пункт "Состав подписи".(см. рис. 5.2).

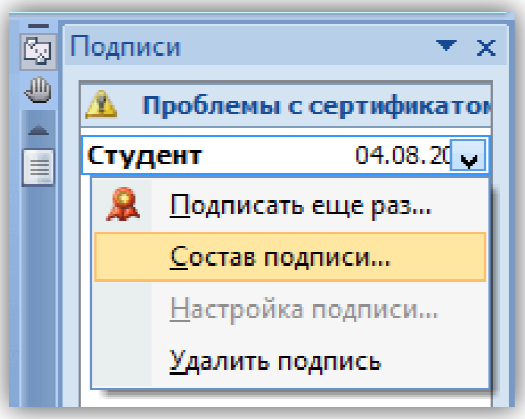


Рисунок 5.2. Проверка электронной цифровой подписи.

7. Вы увидите окно "Состав подписи" вашего напарника см.5.3), аналогичное тому, который вы создавали сами (см. 4.5). Для дальнейшего просмотра сертификата подписи необходимо нажать кнопку "Просмотр".

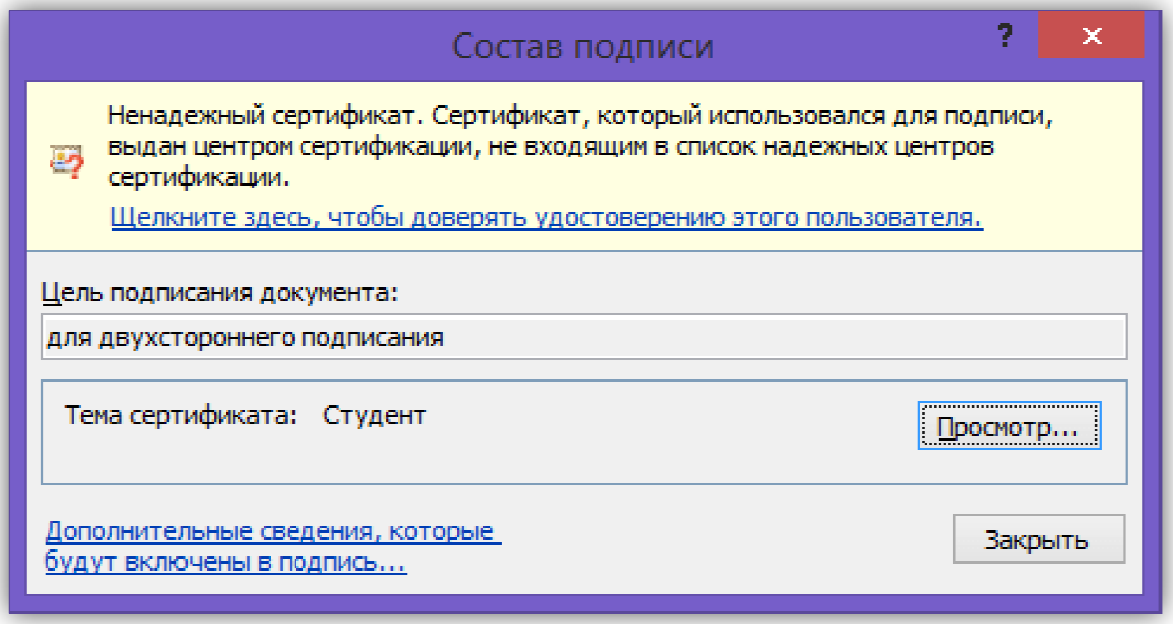
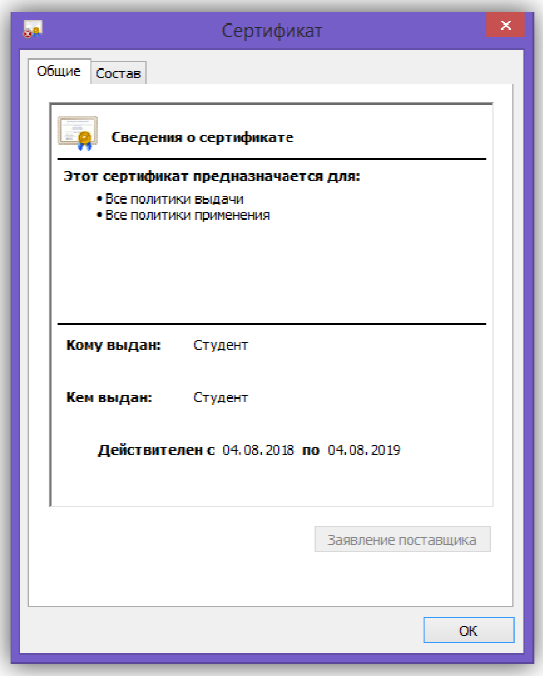
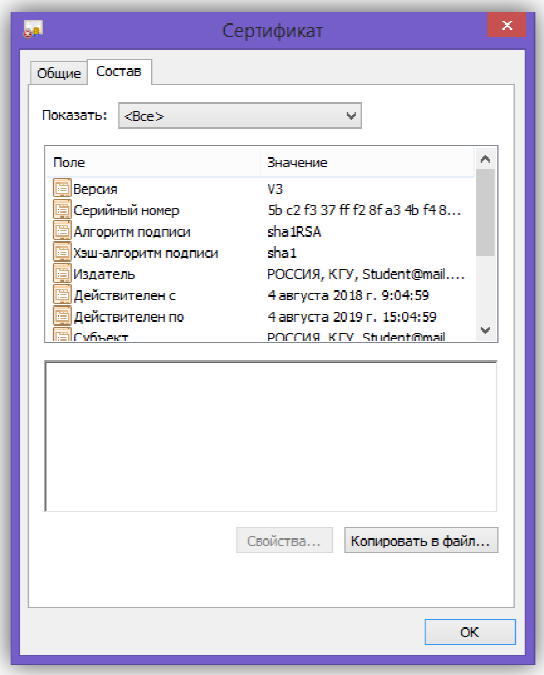


Рисунок 5.3. Окно "Состав подписи".

8. Вы увидите всю необходимую информацию (см. рис. 5.4) о сертификате: где, кем и когда он создан, срок службы и т.д. Также все данные сертификата можно сохранить (см .рис. 5.4 б) в необходимом для проверки формате нажав на кнопку "***Копировать в файл"*** в случае необходимости обращения в юридические службы.





а) *б)*

Рисунок 5.4. Окно "Состав подписи"

9. Сделайте скриншот сертификата напарника (см. рис. 5.4. а) и добавьте его в отчет.

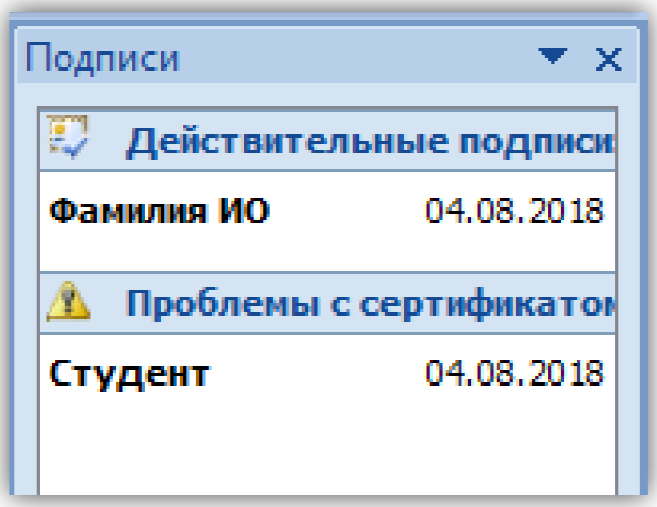


Рисунок 5.5. Добавление второй ЭЦП

10. Далее необходимо заверить документ свой электронной подписью, чтобы он был заверен с двух сторон. При это необходимо свою подпись добавить рядом не уничтожив подпись партнера. Если выбрать пункт "Подписать еще раз"(см. рис. 5.5), то это будет означать, что Вы исправили в документе некую информацию и хотите заменить своей подписью старую ЭЦП, которая сразу же станет недействительной. Чтобы этого не произошло необходимо сделать это точно также как в задании 4. Только в

этом случае подписей на документе будет стоять 2 без нарушения целостности каждой из них.

11. Сделать скриншот окна с документом, заверенного двумя электронными цифровыми подписями.

Индивидуальные варианты

Таблица 1 − варианты заданий

№ п/п	Имя файлов MS Word	Имя файлов MS Excel
1	canenclem	bookbinder
2	heaconric	apron
3	drulatcra	gendarme
4	booglapra	anarchist
5	kilrimhus	quidnunc
6	pacunbinf	locksmith
7	ditarract	adventurer
8	droworran	beaver
9	proailpra	athlete
10	dovstrdef	midwife
11	booselgru	holidayer
12	pasanngab	aquacckit
13	midexphol	kitten
14	abbskumin	critic
15	abdquiaer	albatross
16	idesmowal	renter
17	parcozaca	costumier
18	orideptes	grazier
19	farpulpil	miller
20	motdisdem	pilgrim
21	scabeddet	duck
22	coslikint	meteor
23	baredugoo	mendicant

Лабораторная работа № 4.
Защищенный документооборот

В данной лабораторной работе рассматриваются основные вопросы защиты документов различных форматов.

Цели:

•Научиться защищать данные в табличном редакторе MS Excel.

•Обеспечить защиту структуры и окон электронной таблицы

Организовать скрытие и отображение дополнительных листов в MS Excel.

Научиться создавать защищенные PDF-документы.

•Защитить PDF-документ от несанкционированного открытия и копирования данных.

Задание 1.

Защита данных в табличном редакторе MS Excel.

1. Создать электронную таблицу. Наполнить данными, формулами и диаграммами, например, на тему "Семейный бюджет " (см. рис.1.1).

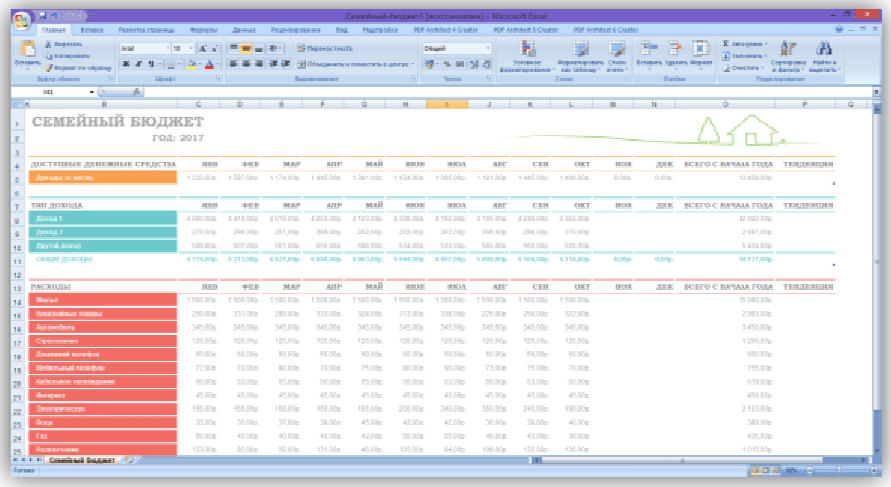


Рисунок 1.1.Исходный документ в табличном редакторе MS Excel.

2. Необходимо защитить документ от введения новых данных в таблицу и удаления старых, а также редактирования формул в ячейках. Для этого необходимо открыть закладку ***"Редактирование"*** и выбрать функцию ***"Защитить лист"*** как изображено на рисунке 1.2.

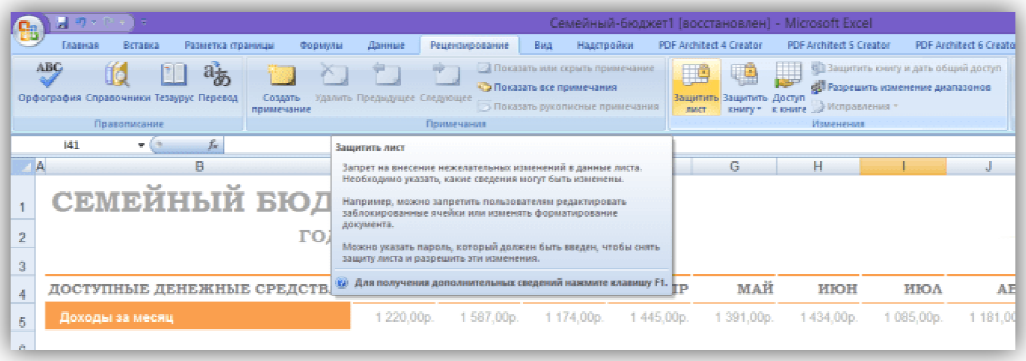


Рисунок 1.2.Защита данных листа MS Excel.

3. В открывшемся окне установить галочки аналогично рисунку 1.3, ввести дважды пароль и нажать кнопку **"ОК"**.

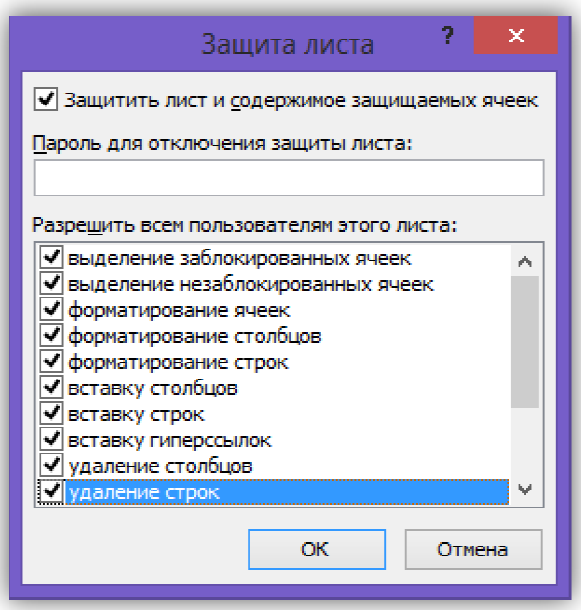


Рисунок 1.3.Пункты защиты

4. Далее необходимо сохранить документ и открыть его заново.

5. Теперь после обращения к какой-либо ячейке будет возникать ошибка, аналогичная рис. 1.4.

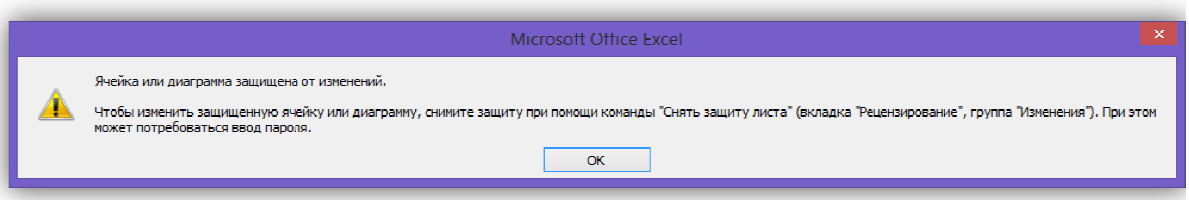


Рисунок 1.4. Защита от изменений

6. Чтобы добавить в таблицу новые данные или каким-то изменить информацию на листе, необходимо также открыть закладку "Рецензирование" и выбрать функцию "Снять защиту листа" (см. 1.5).

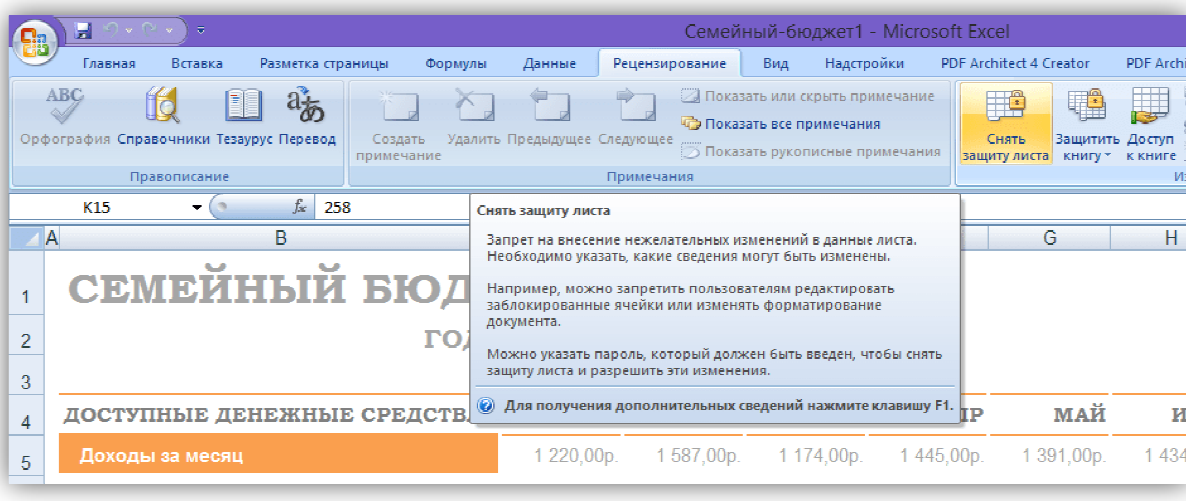


Рисунок 1.5. Снять защиту листа

Задание 2.

Защита структуры и окон электронной таблицы.

1. Создать новую электронную таблицу, содержащую данные на нескольких листах. В закладке ***"Рецензирование"*** выбрать функцию ***"Защитить книгу"***, а в открывшемся контекстном меню защита структуры и окон, как изображено на рис. 2.1.

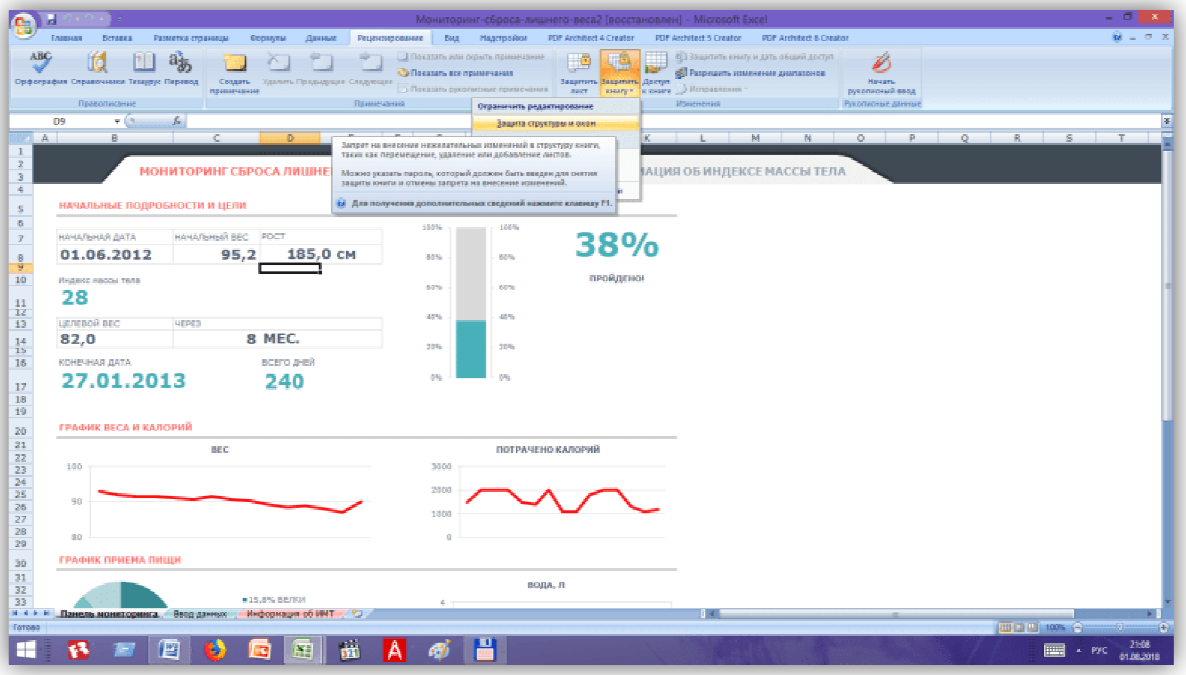


Рисунок 2.1. Защита книги

2. Далее у нас есть возможность ограничить права доступа по двум пунктам ***"структуру"*** и ***"окна".*** Начнем изучение с первого пункта ***"структуру"*** и введем секретный пароль, аналогично рис. 2.2. Так как пароль закрыт "звездочками" от посторонних глаз, его необходимо ввести дважды.

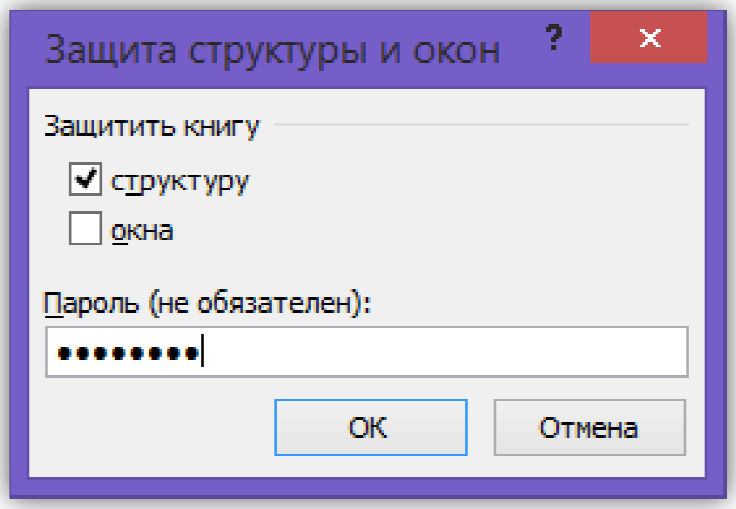


Рисунок 2.2. Защита структуры

3. Теперь стали запрещены большинство операций с листами и структурой документа. Так например, теперь стало невозможным перемещать листы, менять их местами, а также .удалить какой-либо лист без вашего ведома. В этом можно убедиться нажав на закладку любого листа правой кнопкой мыши (см .рис. 2.3.).

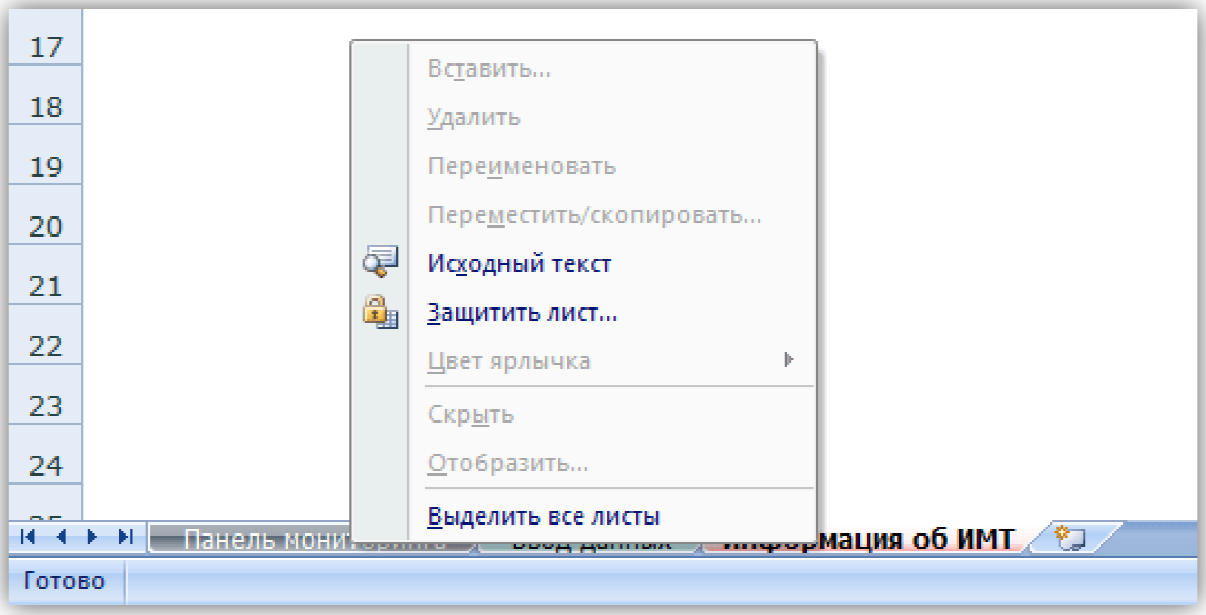


Рисунок 2.3. Блокировка команд, изменяющих структуру документа

4. Сделать снимок с экрана список заблокированных команд и добавить в отчет по лабораторной работе.

5. Если же в пункте ***"Защитить книгу"*** выбрать флажок ***"Окна",*** аналогично рис. 2.4, то это защитит открытый документ от случайного сбоя, закрытия и потери табличных данных.

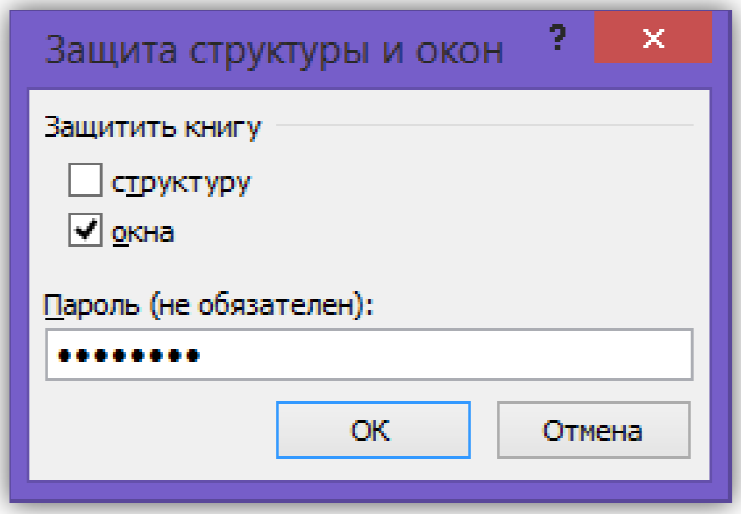


Рисунок 2.4. Защиты системы окон

6. Теперь даже нажатие на иконку  в верхней части окна программы, то Вы не сможете закрыть эту таблицу. Если же вы решили завершить работу с этими данными окончательно, необходимо нажать ***"Файл"***, а потом функция ***"Закрыть"*** (см. рис. 2.5)

.

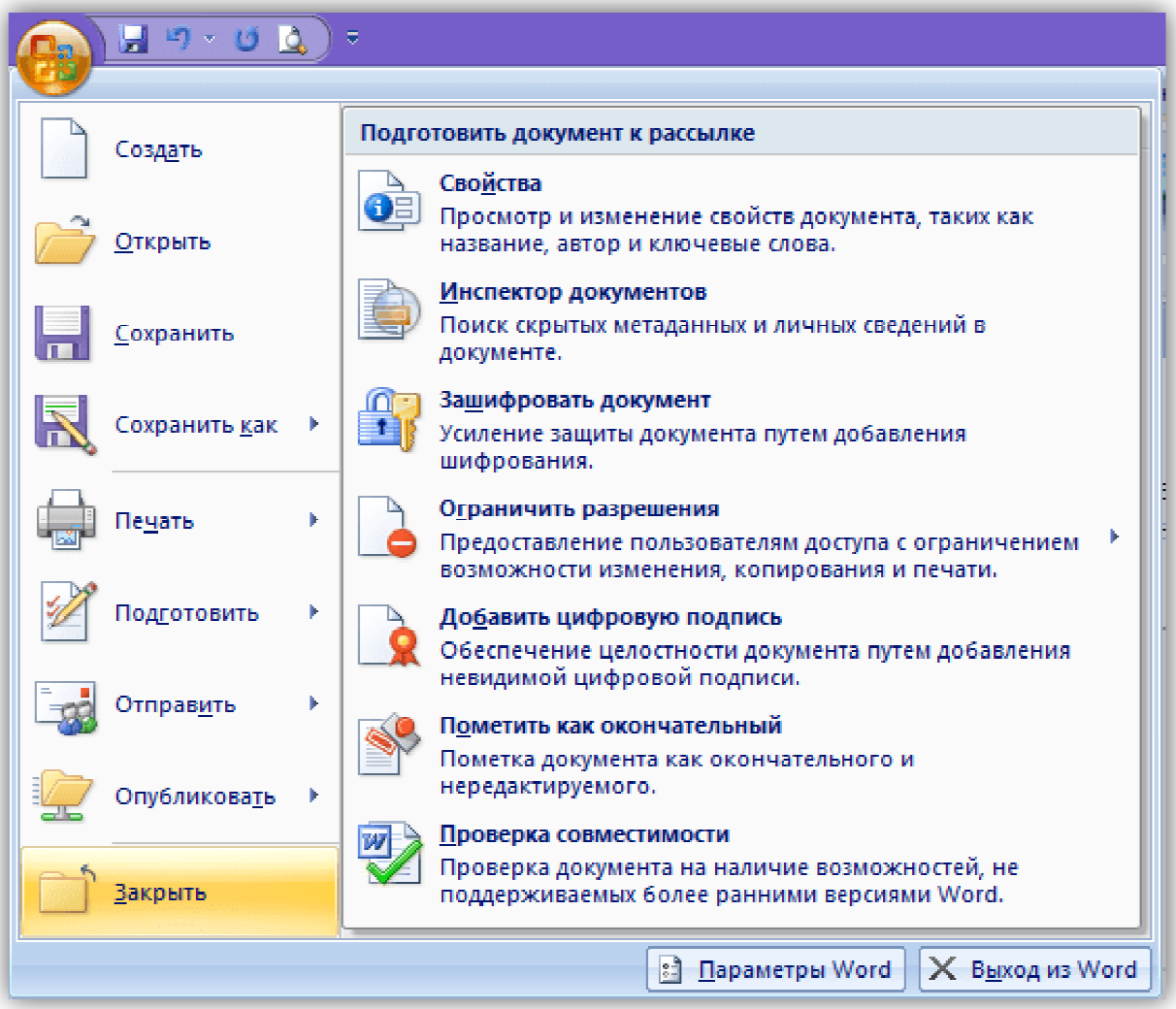


Рисунок 2.5. Функция "Закрыть"

7. Также к таблицами в редакторе MS Excel применимы те же дополнительные методы защиты документа, которые были изучены при защите документов в MS Word *(сделайте их самостоятельно)*.

8. Сделать скриншоты результатов, полученных в результате выполнения задания и добавить их в отчет.

Задание 3.
Скрытие и отображение дополнительных листов MS Excel.

1. Для скрытия служебной информации от посторонних глаз в MS Excel существует служебная команда ***"Скрыть лист"***. Для этого необходимо нажать правой кнопкой мыши на закладке с наименованием необходимого листа в нижней части таблицы. На выпадающем контекстном меню выбрать функцию ***"Скрыть"***. (см. рис. 3.1).

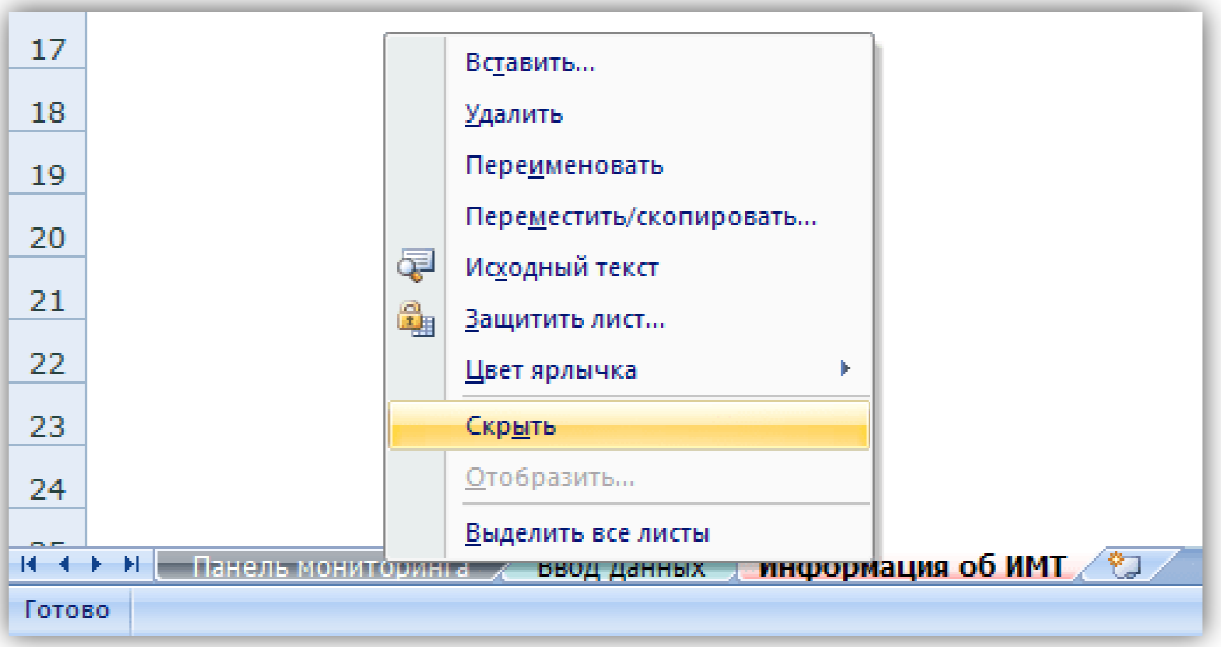


Рисунок 3.1. Функция "Скрыть"

2. После чего это лист исчезнет из списка отображаемых листов таблицы (см. рис. 3.2).

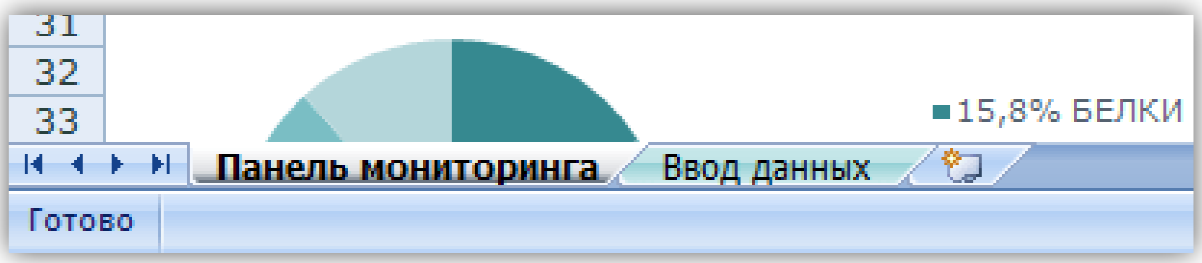


Рисунок 3.2. Список листов в таблице.

3. Чтобы вернуть себе доступ к скрытым листам необходимо нажать правой кнопкой мыши на закладке с наименованием любого из листов в нижней части экрана и выбрать функцию ***"Отобразить"***

(см. рис.3.3.), которая раньше была заблокирована.

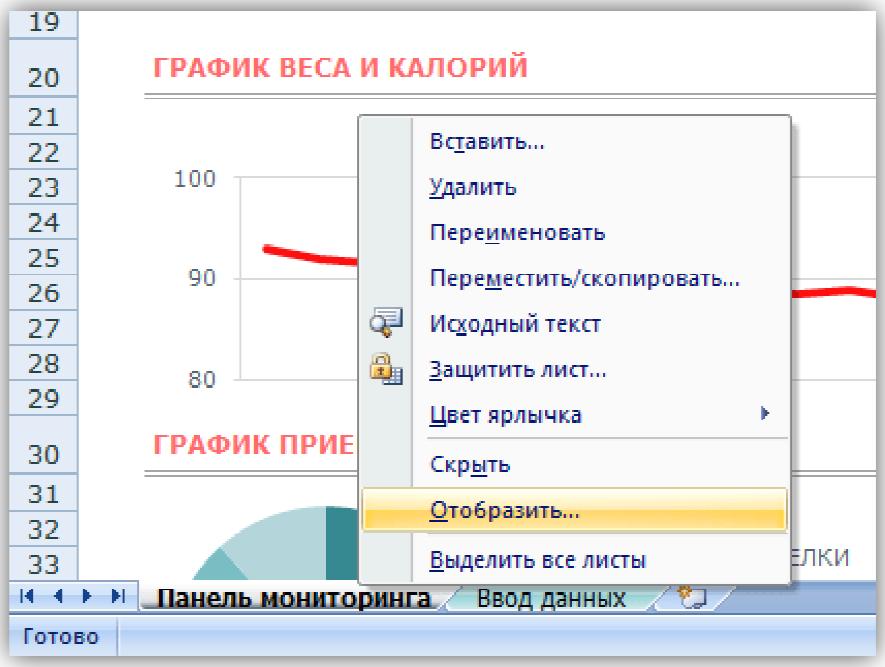


Рисунок 3.3. Функция "Отобразить"

4. Появится список ранее скрытых листов в MS Excel (см.рис. 3.4).

5. Сделать снимок окна со списком скрытых листов и добавить его в отчет.

6. Необходимо выбрать ранее скрытый лист и нажать кнопку ***"ОК"***.

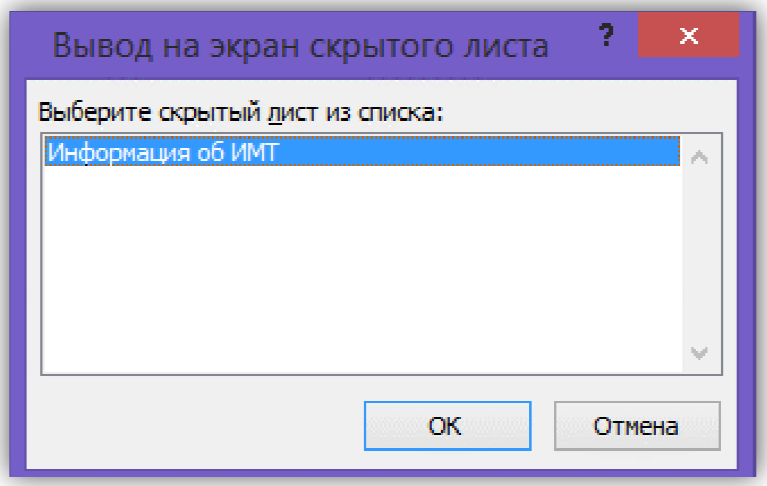


Рисунок 3.4. Функция "Отобразить"

7. Данный лист снова отобразиться в списке используемых листов в нижней части таблицы (аналогично как

это было в начале работы (рис. 3.1.).

8. Сделать снимки экрана на всех стадиях прохождения работы с изображением скрытых и отображенных листов.

Задание 4.
Установка и настройка PDFCreator Free .

1. С целью создания pdf-документов из любых программ редактирования документов необходимо скачать бесплатную программу "PDFCreator" (см. рис. 4.1).

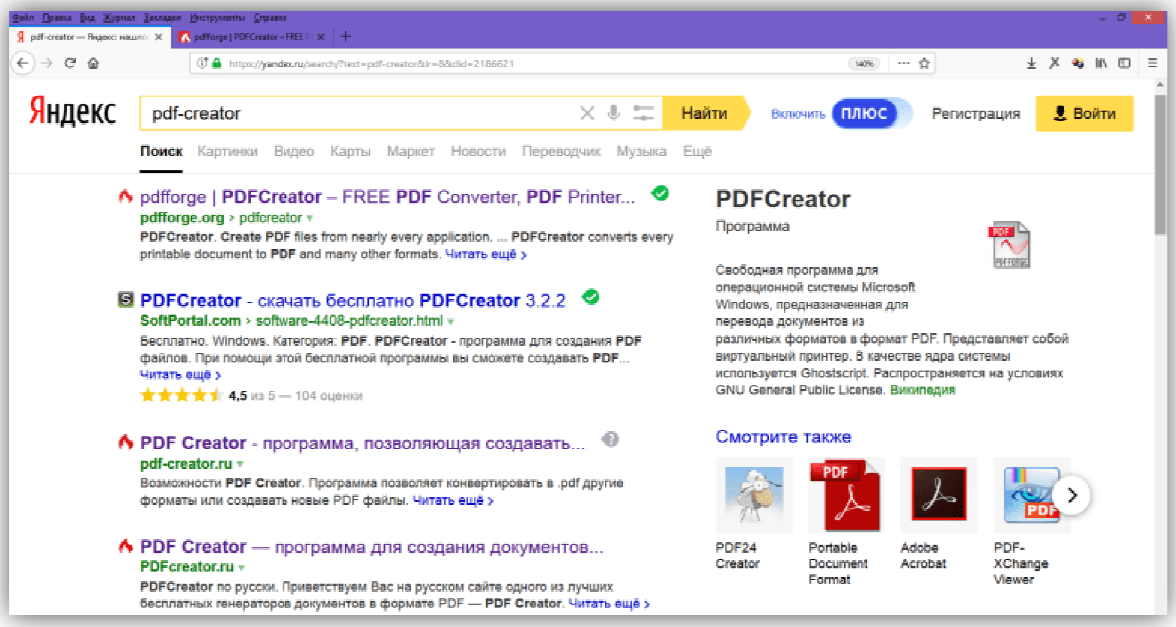


*Рисунок 4.1. Поиск программы **"PDFCreator".***

2. Выбрать первую ссылку с сайтом производителя https://www.pdfforge.org/pdfcreator (см. рис. 4.1).

3. Нажать левой кнопкой мыши на кнопку 

(см. рис. 4.2)

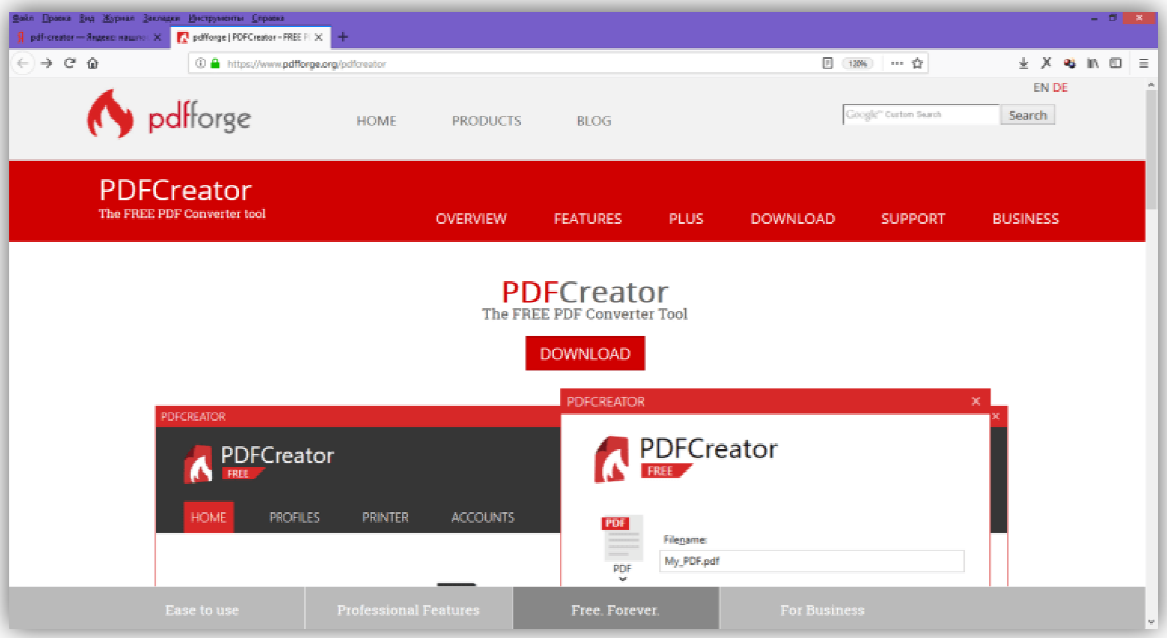


Рисунок 4.2. Скачивание с сайта производителя

4. Среди предложенных трех версий выбираем версию для бесплатного распространения ***"PDFCreator Free"*** (см. рис. 4.3).

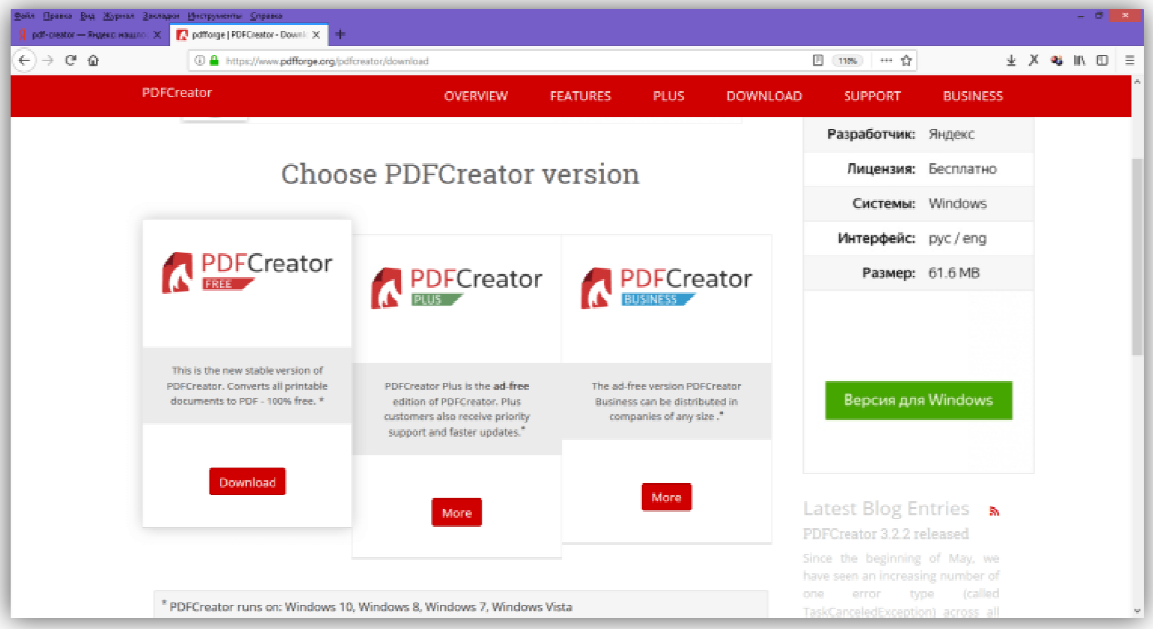


Рисунок 4.3. Выбор версии для скачивания

5. Ждем 5 секунд и скачиваем дистрибутив программного обеспечения на компьютер.

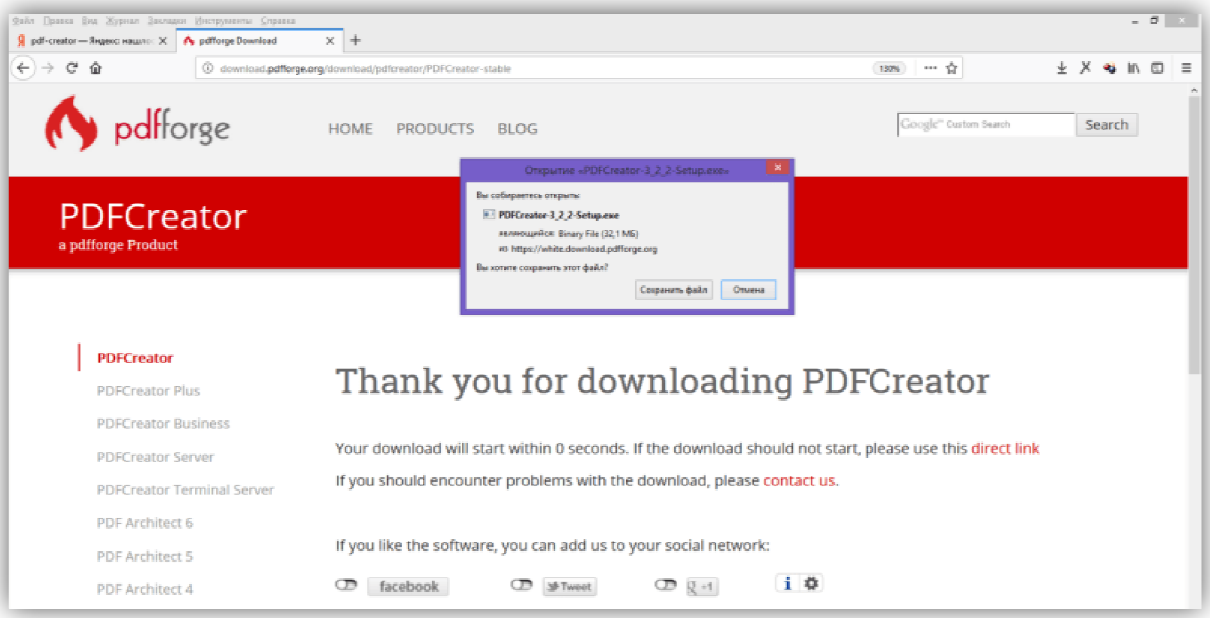


Рисунок 4.4. Скачивание установочного пакета PDFCreator Free

6. Запустить установщик программного обеспечения ***"PDFCreator Free".*** В окне с выбором языка установки выбрать ***"Русский"*** (см. рис. 4.5).

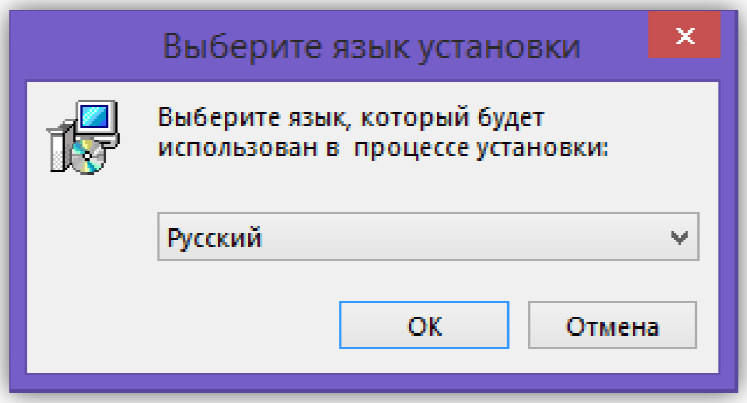


Рисунок 4.5. Выбор языка для установки пакет программного обеспечения

7. Откроется окно мастера установки программы ***"PDFCreator"***. Все установки можно оставить по умолчанию. Нажать кнопку ***"Далее"***.

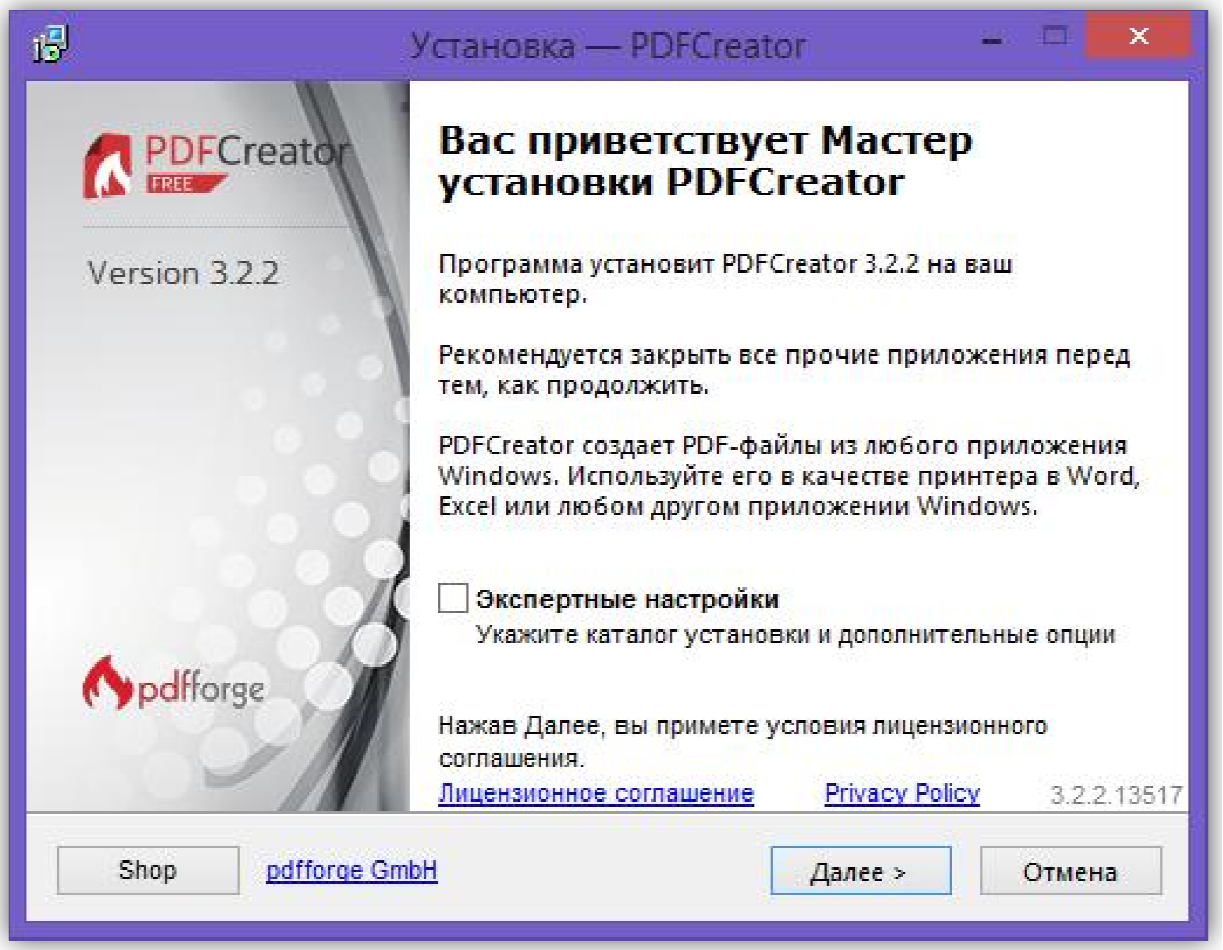


*Рисунок 4.6. Первое окно мастера установки программы **"PDFCreator"***

8. Во втором окне мастера установки перечислены основные параметры инсталляции программы (см. рис. 4.7). Если бы флажок "Экспертные настройки" был выбран, то их можно было бы изменить. Теперь, когда все готово к распаковке необходимо нажать кнопку "Установить".

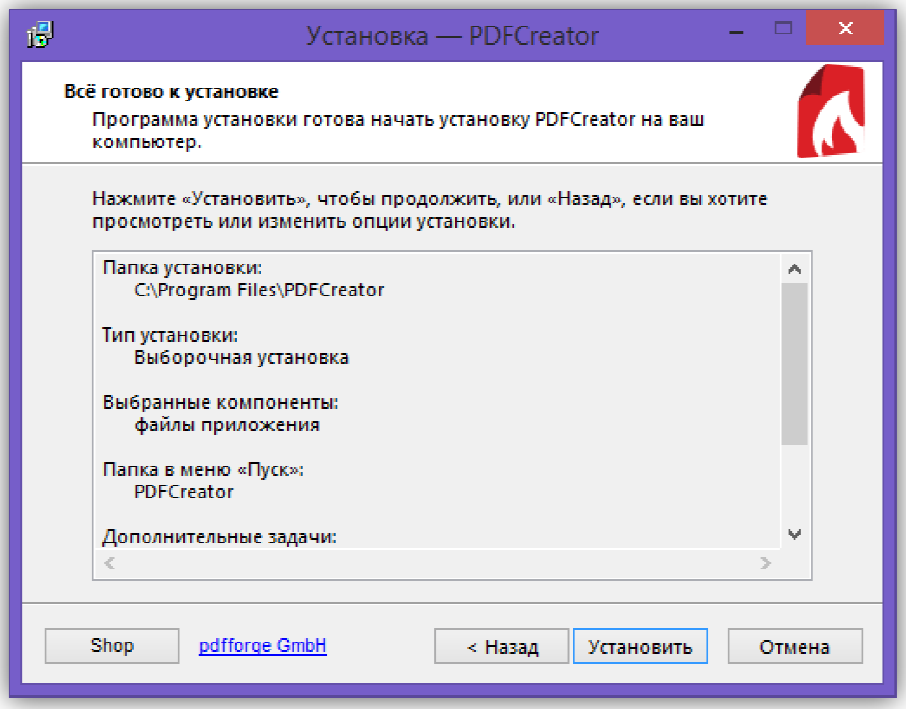


Рисунок 4.7. Второе окно мастера установки программы ***"PDFCreator"***

9. После установки основного пакета мастер предложит дополнительно установить "Яндекс-браузер". Необходимо снять предложенные флажки и нажать кнопку "Пропустить"/"Skip", аналогично рис. 4.8.

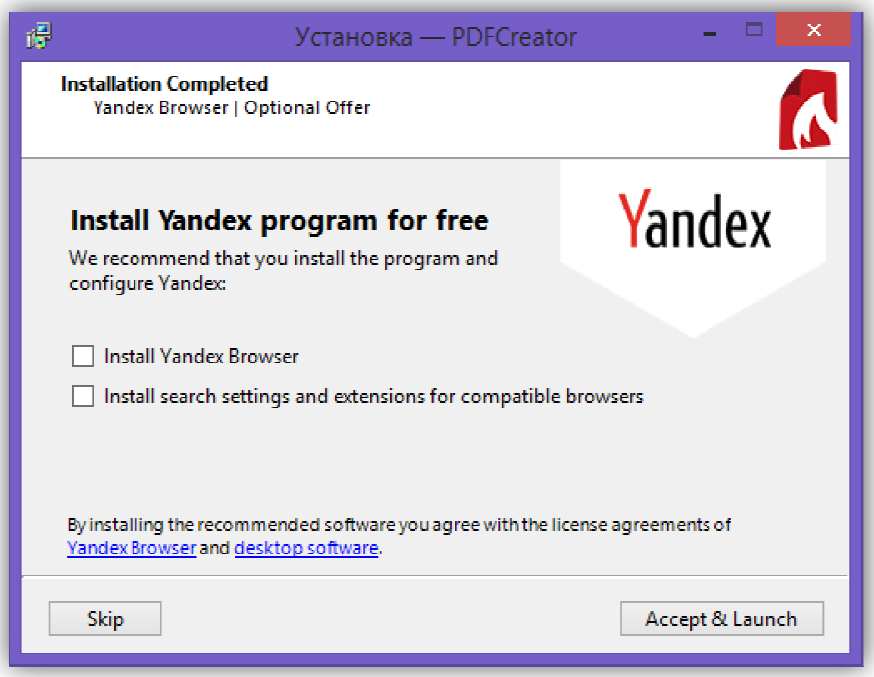


Рисунок 4.8. Установка дополнительного пакета программного обеспечения

10. После этого шага установка подойдет к концу (см. рис. 4.9). Для ускорения процесса необходимо снять флажок ***"Показать справку после установки"*** и нажать кнопку ***"Завершить"***.

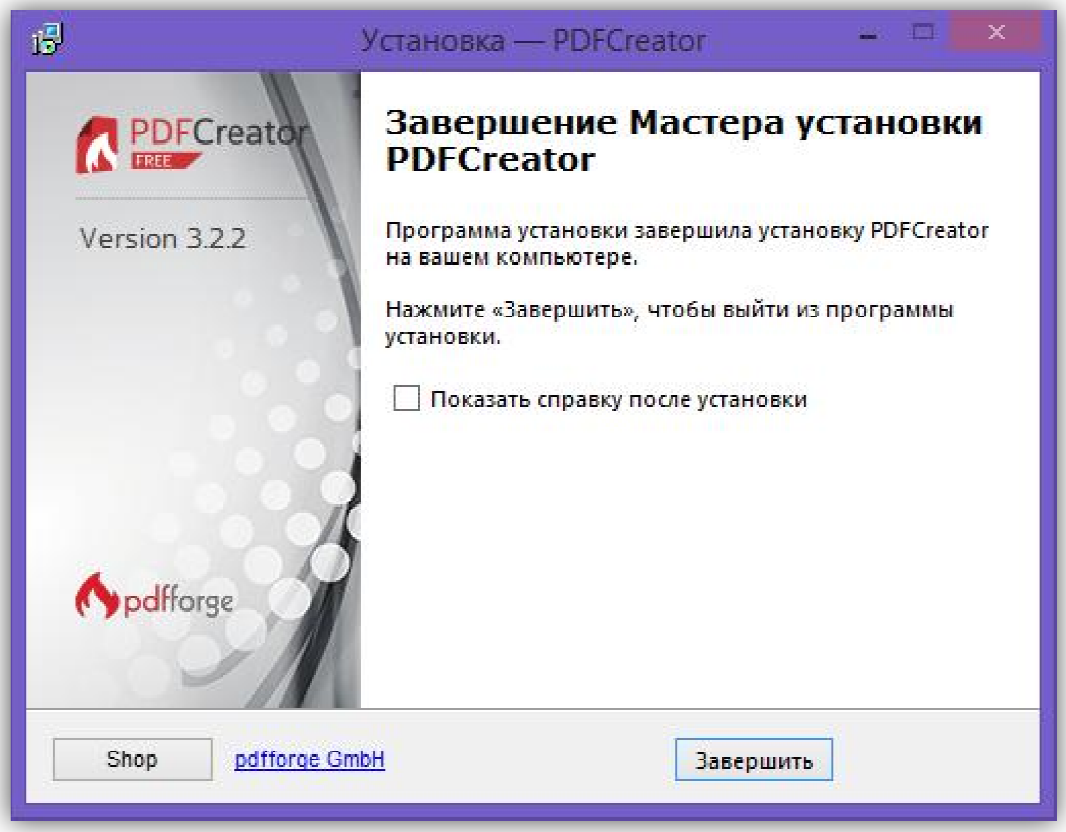


Рисунок 4.9. Завершение установки

11. Теперь есть возможность открыв любой документ,

преобразовать его в PDF-формат.

Задание 5.
Создание PDF-документов и защита паролем.

1. Открыть любой документ (например, созданный в предыдущих заданиях) и создать на его основе PDF-файл. Для этого необходимо его распечатать, но в качестве принтера выбрать ***"PDFCreator"*** (см. рис. 5.1).

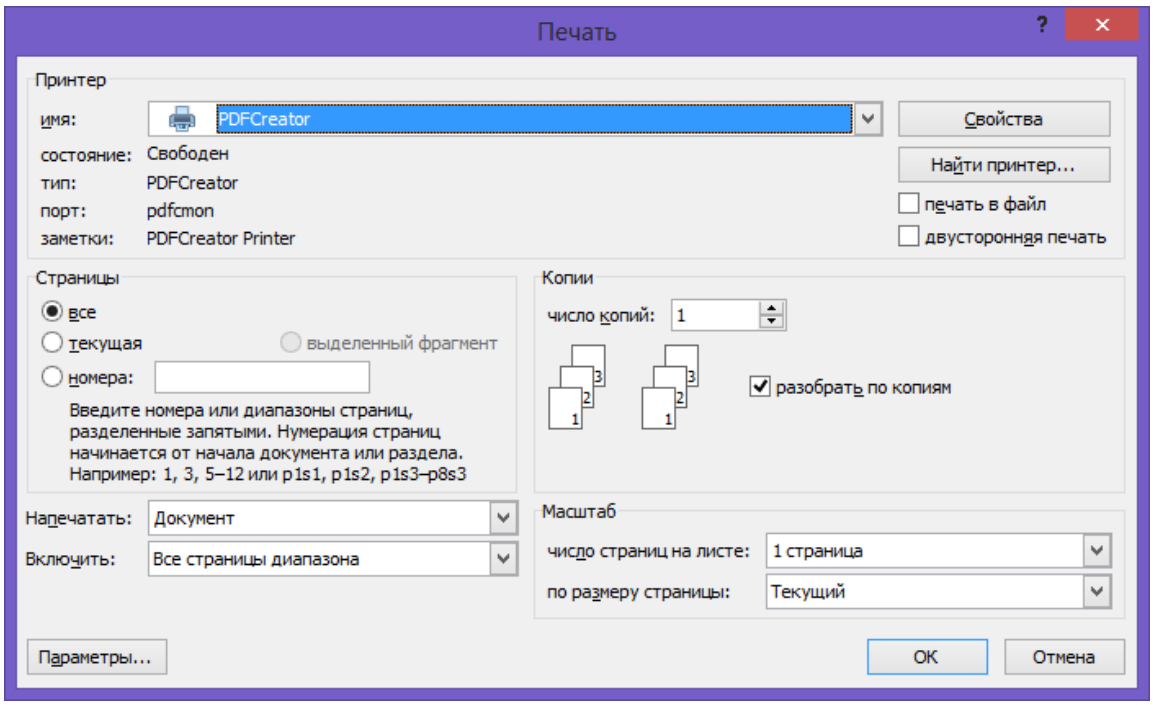


Рисунок 5.1. Выбор "PDFCreator" в качестве принтера для печати

1. Откроется специальное окно программы PDFCreator (см. рис. 5.3). В верхнем поле можно указать заголовок и имя будущего файла, а во втором папку расположения.

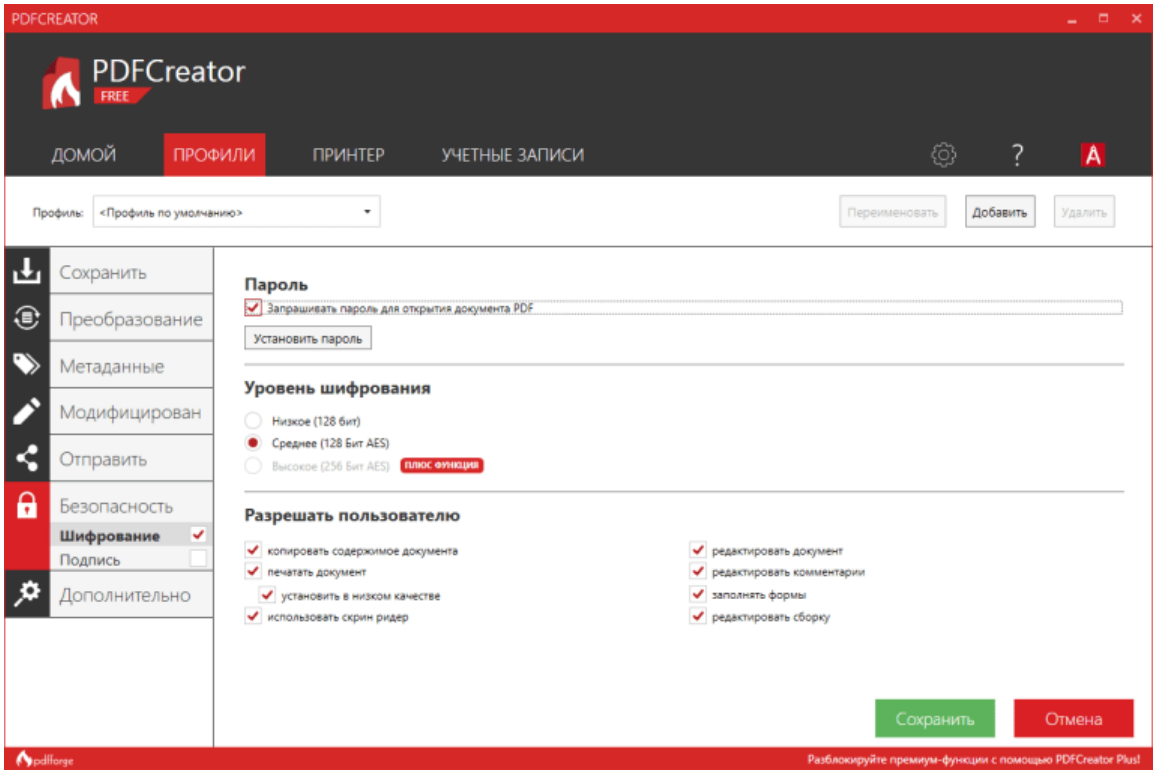


Рисунок 5.2. Установки для защита документа от несанкционированного доступа

2. Сохраните полученный документ под именем "Реферат 1".

3. Теперь необходимо создать документ с шифрованием данных. Повторить операцию п.1 над исходным документом. В окне, по аналогии с рис. 5.3, поставить в поле имени файла "Реферат 2". Чтобы настроить защиту в поле профиля нажмите на кнопку ***"Изменить"***.

4. Зайти в раздел "Безопасность" (слева) и выбрать функцию "Шифрование". Установите флажок "Запрашивать пароль на открытие". Остальные настройки поставить аналогично рис. 5.2. Нажать кнопку "Сохранить".

5. Система вернется к окну, изображенному на рис. 5.3, и т.к. все предварительные настройки завершены, необходимо нажать кнопку "Сохранить".

6. В следующем окне программа запросит пароль на открытие файла (см. рис. 5.4). Так как пароль скрыт "*" от посторонних глаз программа потребует повторного подтверждения пароля. Потом нажать кнопку "ОК".

7. Теперь при открытии документа он будет требовать пароль, аналогично MS Word в задании 3.

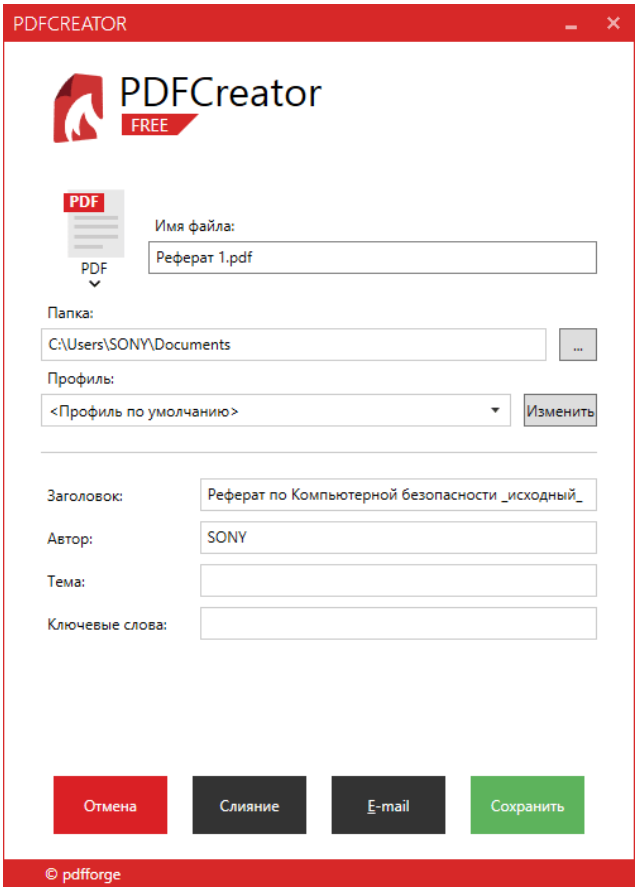


Рисунок 5.3. Рабочее окно "PDFCreator"

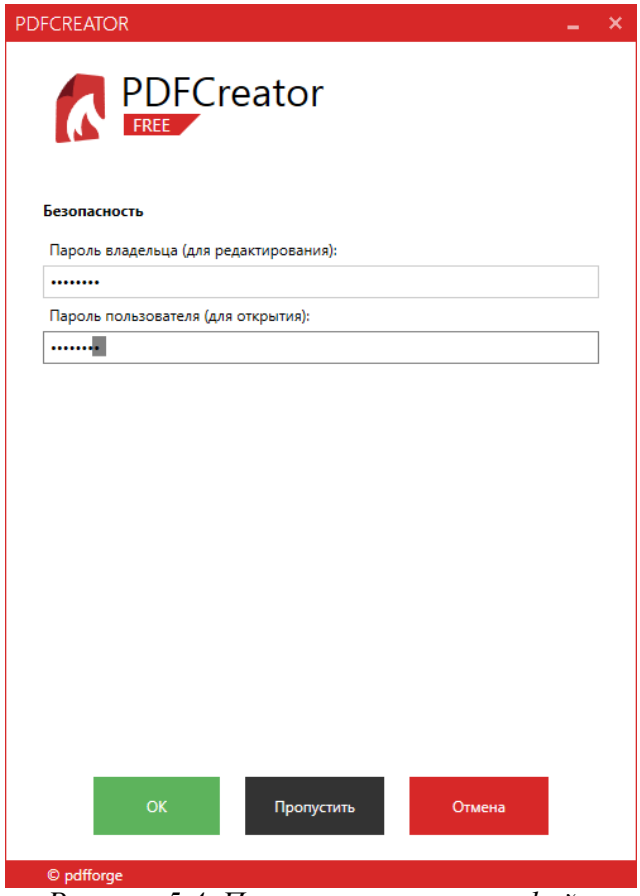


Рисунок 5.4. Пароль на открытие файла

Задание 6.
Создание PDF-документов с защитой от плагиата и других видов утечки информации.

1. Создать PDF-документ, с защитой от утечки информации. Повторить над исходным документом операцию аналогичную п.1 задания 10. В окне, по аналогии с рис. 5.3, поставить в поле имени файла "Реферат 3". Чтобы настроить защиту в поле профиля нажмите на кнопку ***"Изменить"***.
2. В разделе "Безопасность" также выбираем функцию "Шифрование". Установить флажки в соответствии с рис 6.1 и нажать кнопку "Сохранить".

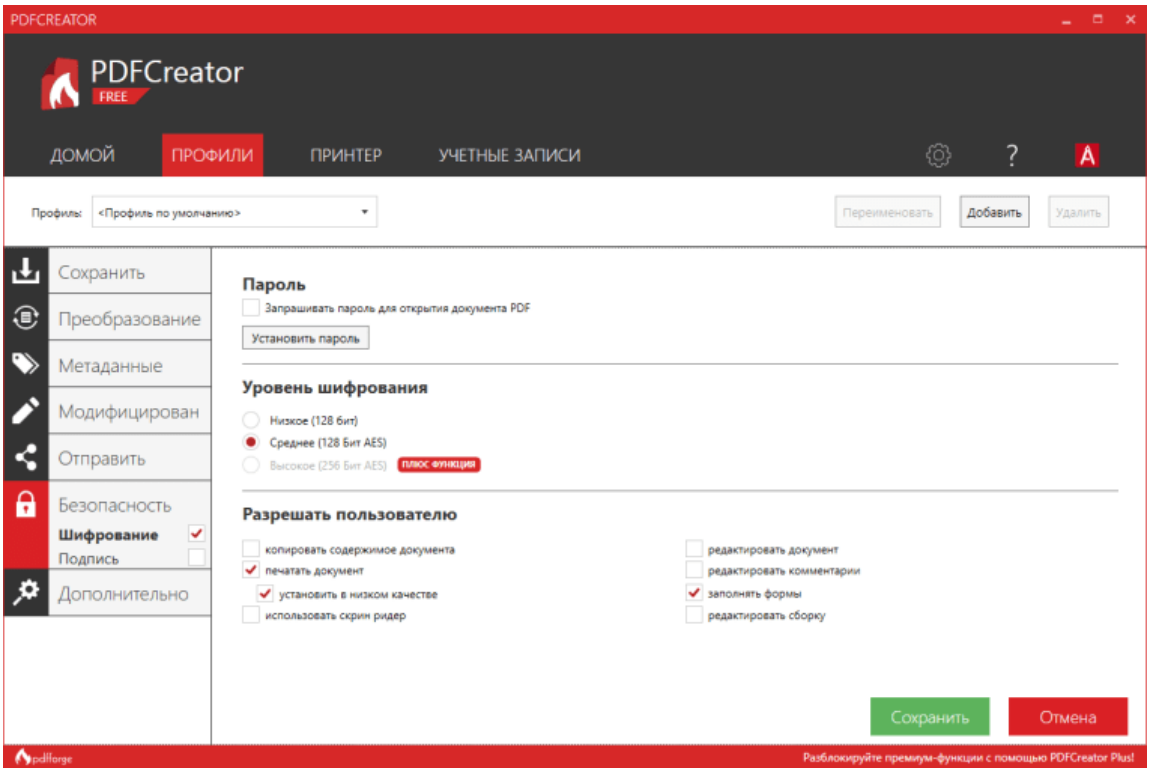


Рисунок 6.1. Установки для защиты документа от утечки информации

3. Теперь документ защищен от утечки информации. Для проверки необходимо его открыть, выделить фрагмент текста и попытаться скопировать. Далее необходимо открыть текстовый редактор и вставить скопированные данные.
4. Попытка будет неудачной, т.к. информация либо не вставиться в текстовый документ, либо система выдаст ошибку (как на рис. 6.2).

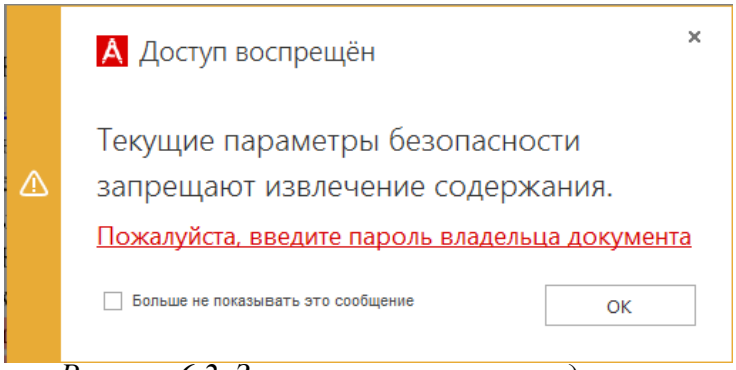
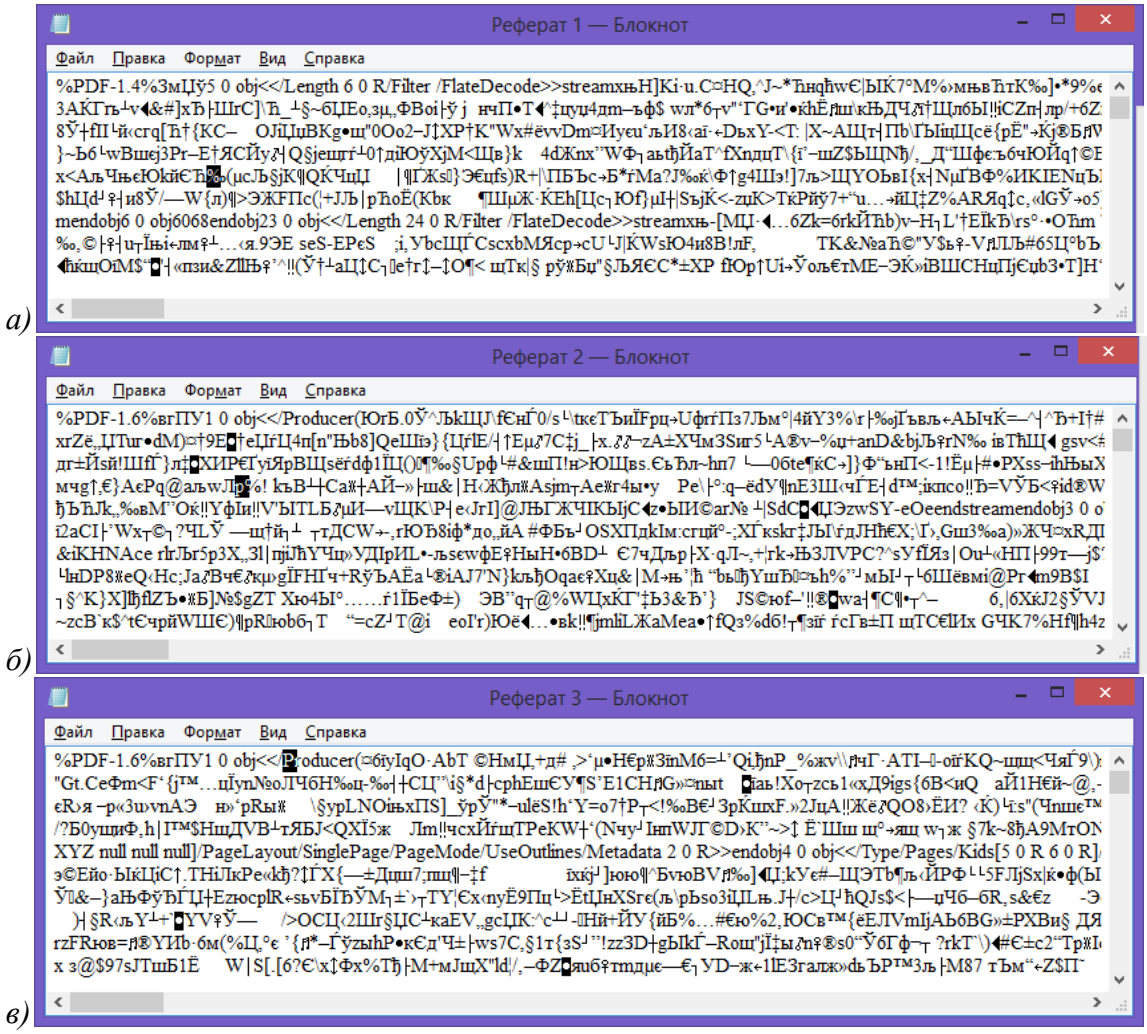


Рисунок 6.2. Запрет на копирование данных

Задание 7.
Сравнение структур оригинальных и зашифрованных PDF-файлов.

1. Необходимо сравнить архитектуру трех файлов, созданных в заданиях 10 и 11. В отличие от пароля, шифрование не только накладывается запрет доступа на открытие, но и меняет само содержимое файла, записывая его в недоступном для чтения виде.
2. Открыть кодировку файлов "Реферат 1", "Реферат 2" и
Реферат 3" при помощи программы "Блокнот" и сделать скриншоты окон.
3. В файле "Реферат 1" (см. рис. 7.1 а), который не подвергался шифрованию можно увидеть исходную структуру PDF-файла: версию, с помощью которой он был создан, длину файла, кодеки которые использовались по время преобразования.
4. В файлах "Реферат 2" (рис. 7.1 б) и "Реферат 3" (рис. 7.1 в) видно, что данные подвергались шифрованию, и кроме версии PDF никаких других данных выяснить не удастся.
5. Таким образом, анализ показывает, что при шифровании данных файлы изменяют свою структуру, при чем независимо от того файл шифровался на открытие или от копирования данных с одним и тем же ключом - содержимое абсолютно разное.



а)

б)

в)

Рисунок 7. Структура исходного и зашифрованных PDF-файлов

Задание 8.
Использование online-сервисов.

1. Наберите в поиске сети Интернет сайт https://pdfio.co/ru.
2. Данный online-сервис кроме преобразований имеет еще две функции связанных с защитой данных: "Защитить PDF" и "Разблокировать PDF".
3. На сайте выбрать функцию "Защитить PDF" (см. рис. 8.1).

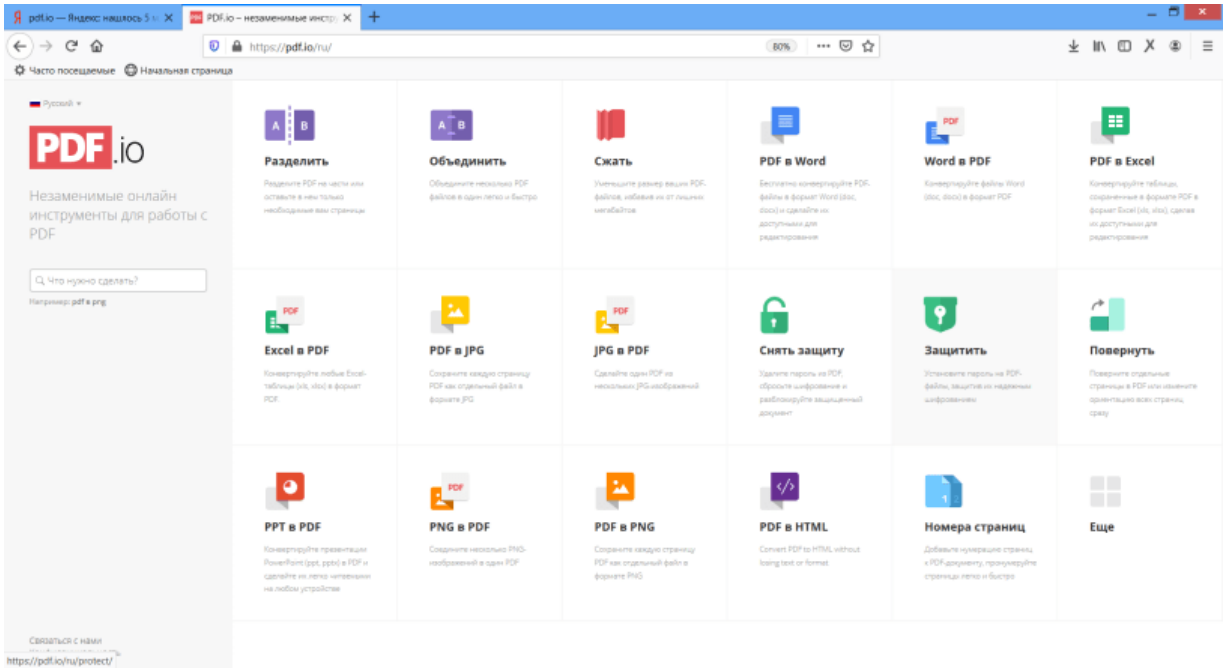


Рисунок 8.1. Главная страница сайта pdf.io.

4. Появиться новая страница для загрузки файла (см. рис. 8.2). Стоит отметить, что загрузить можно только документы в формате pdf. Для примера можно взять "Реферат 1", который не подвергался преобразованиям.

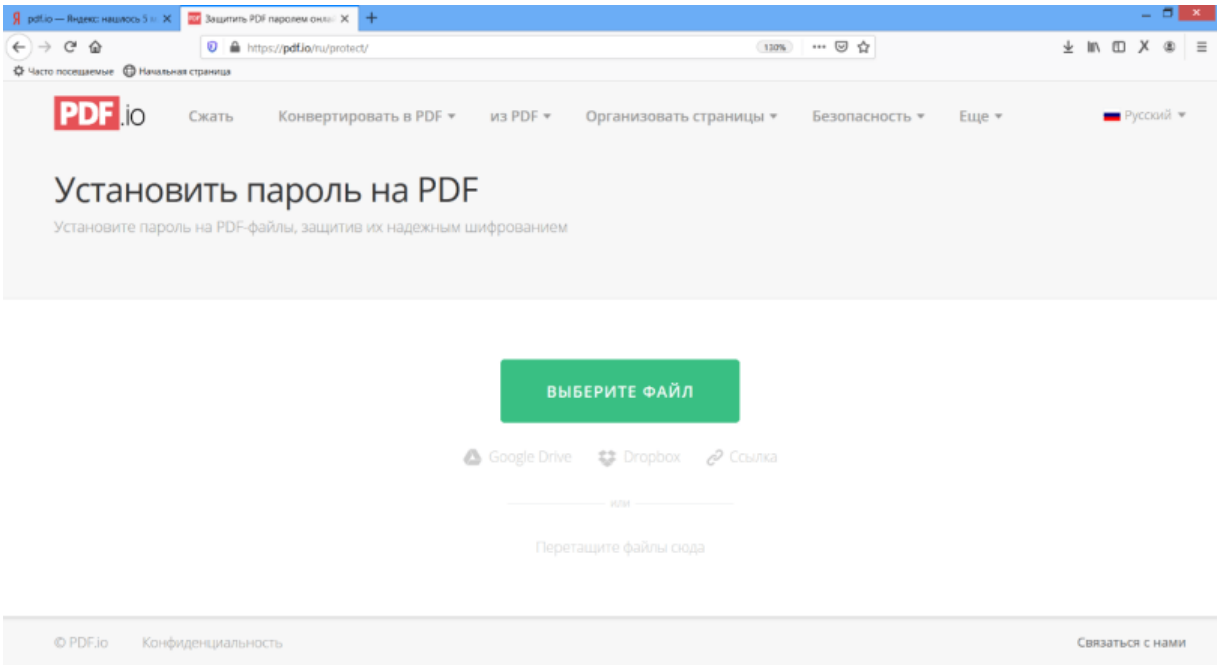


Рисунок 8.2. Страница "Установить пароль на PDF"

5. После загрузки pdf-файла появиться окно для ввода секретного пароля (см. рис. 8.3). Как говорилось ранее, во время ввода пароль скрыт значками "*" и есть вероятность ошибки при вводе, в связи с чем предусмотрена функция "показать пароль", которая, тем самым, снижает вероятность ввода неправильного пароля. Далее необходимо нажать кнопку "Защитить".

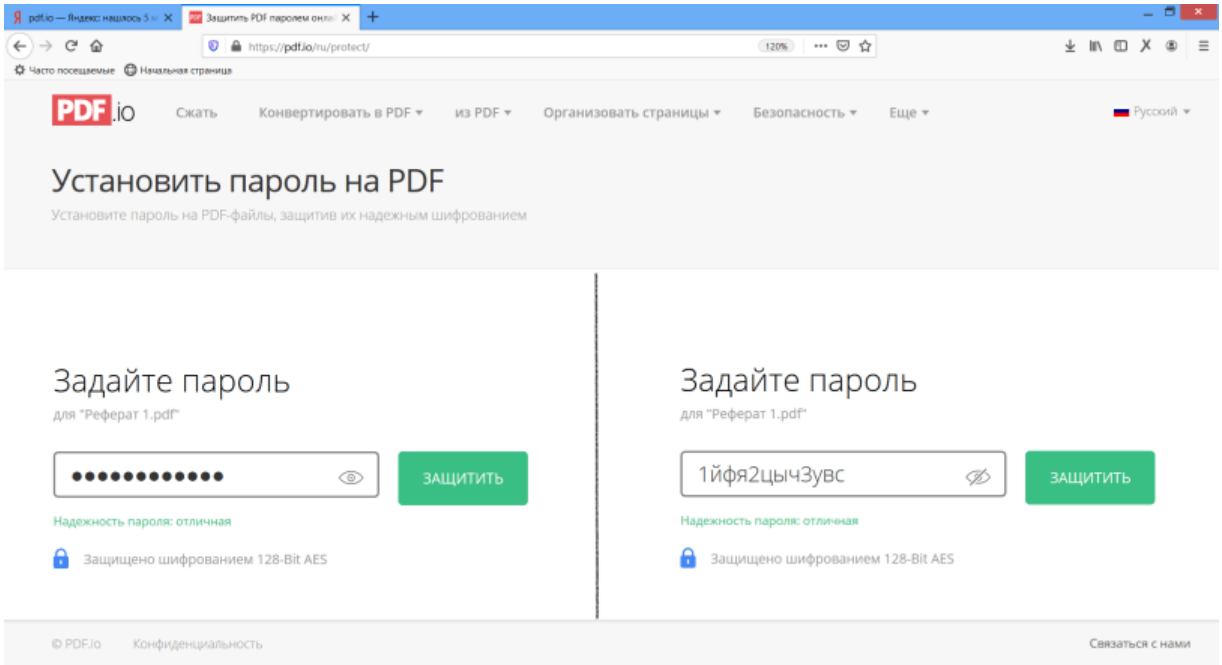


Рисунок 8.3. Страница "Защитить PDF"

6. Перекодирование файла может занимать несколько секунд. После окончания процедуры шифрования (см. рис. 8.4) его необходимо скачать и присвоить ему имя "Реферат 4".

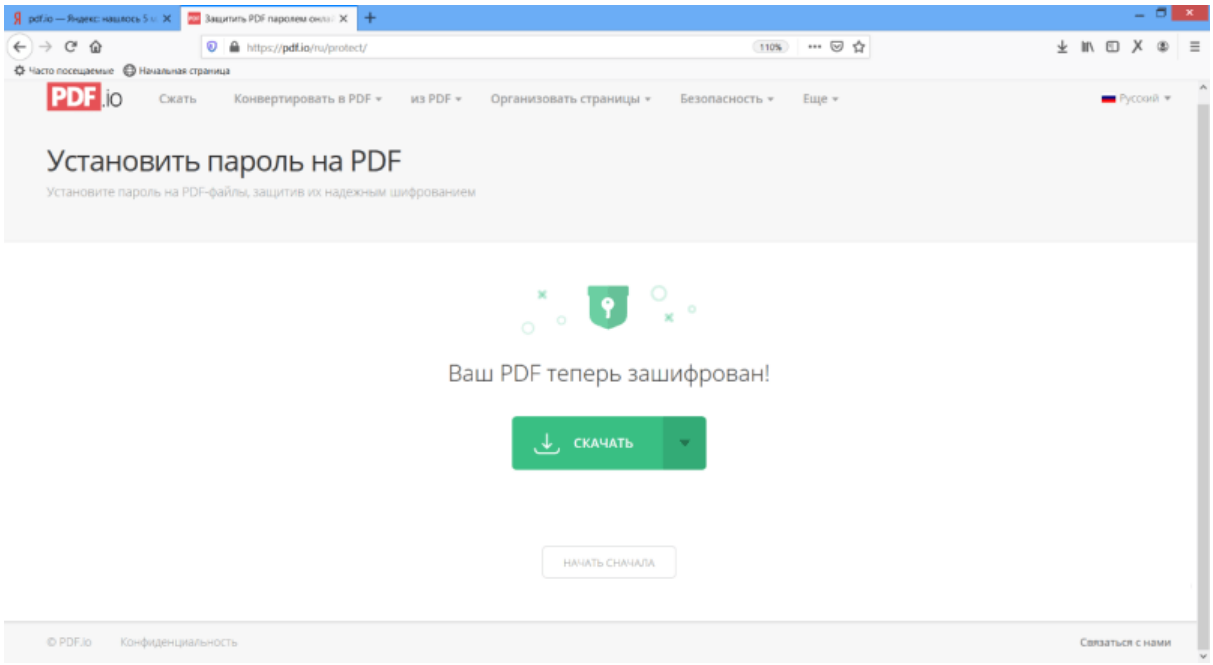


Рисунок 8.4. Страница "Скачать зашифрованный файл"

7. Открыть зашифрованный файл. Программа для открытия pdf-файлов потребует введение пароля (см. рис. 8.5.), аналогично тому, как такое же действие требовалось для файла, созданного в задании 10 с помощью программы PDFCreator.

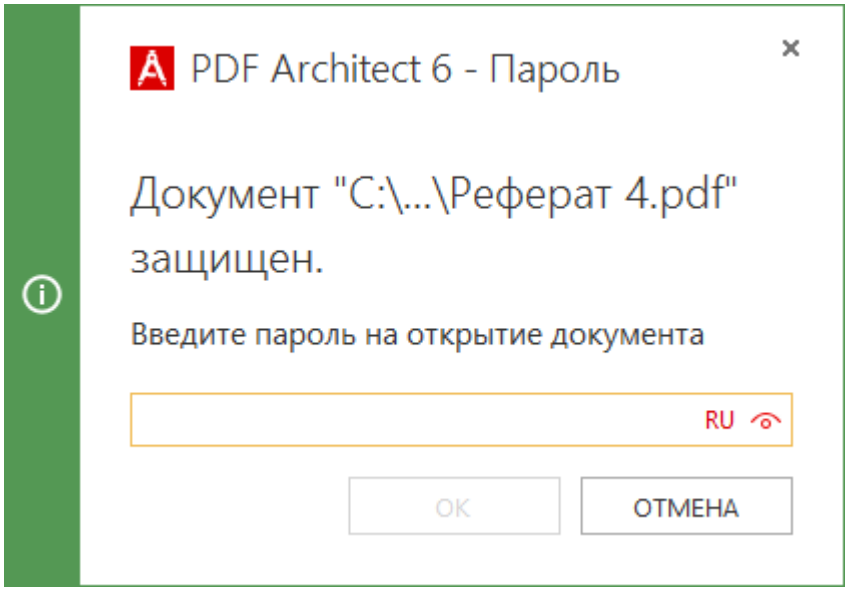


Рисунок 8.5. Окно для ввода пароля на открытие документа

8. При этом данные система не защищает данные от копирования их традиционными методами в текстовый файл.

9. Открыть данный файл для просмотре в редакторе "Блокнот" (см. рис. 8.6). Можно сразу заметить, что кодировка, используемая сайтом кардинально отличается от кодировки другим программ для создания pdf.

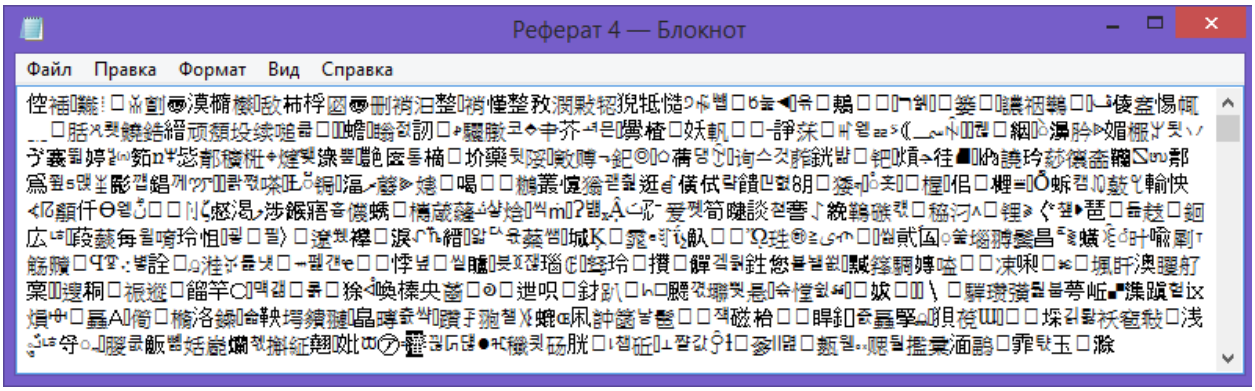


Рисунок 8.6. Структура файла, зашифрованного сайтом pdfio

11. Сделать снимки экрана по мере выполнения задания и добавить их в отчет.

Задание 9.
Разблокировка PDF.

1. На сайте pdfio выбрать функцию "Разблокировать PDF", аналогично рис. 9.1.

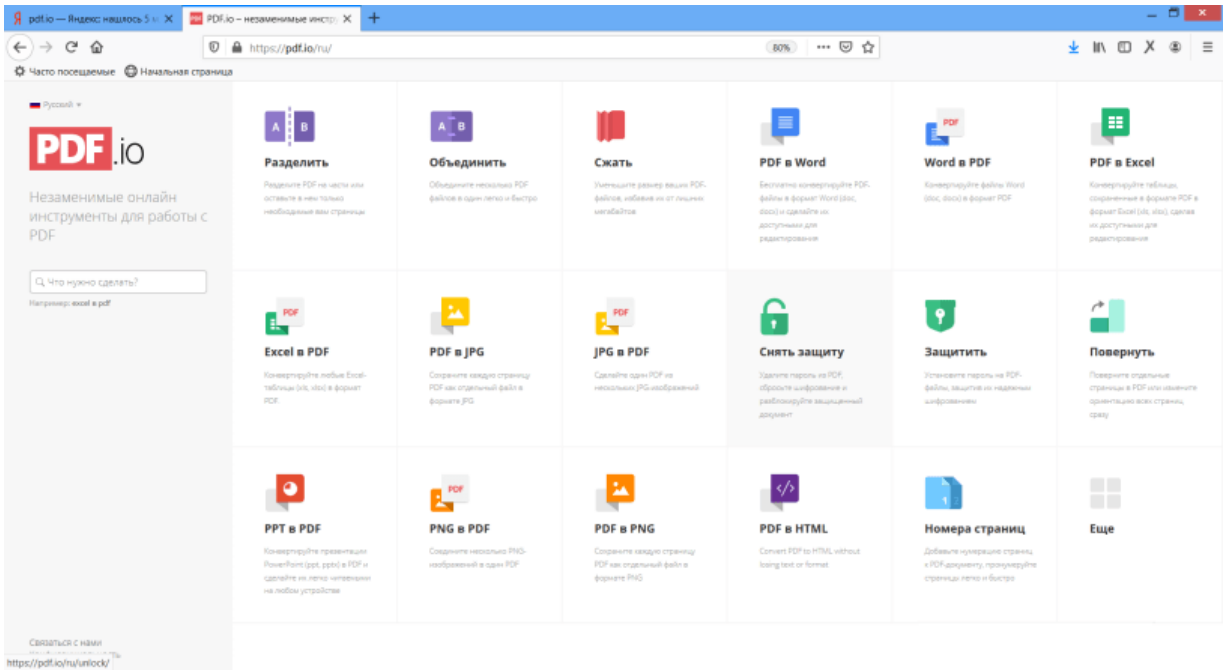


Рисунок 9.1. Выбор функции "Разблокировать PDF" на главной странице сайта

2. Появиться новая страница для загрузки файла (см. рис. 9.2). Стоит отметить, что загрузить можно только документы в формате pdf, созданные ранее. Проведем исследования над документами "Реферат 2", "Реферат 3" и "Реферат 4".

3. Загрузить файл "Реферат 3", нажав кнопку "Выберете файл"
(см. рис. 9.2).

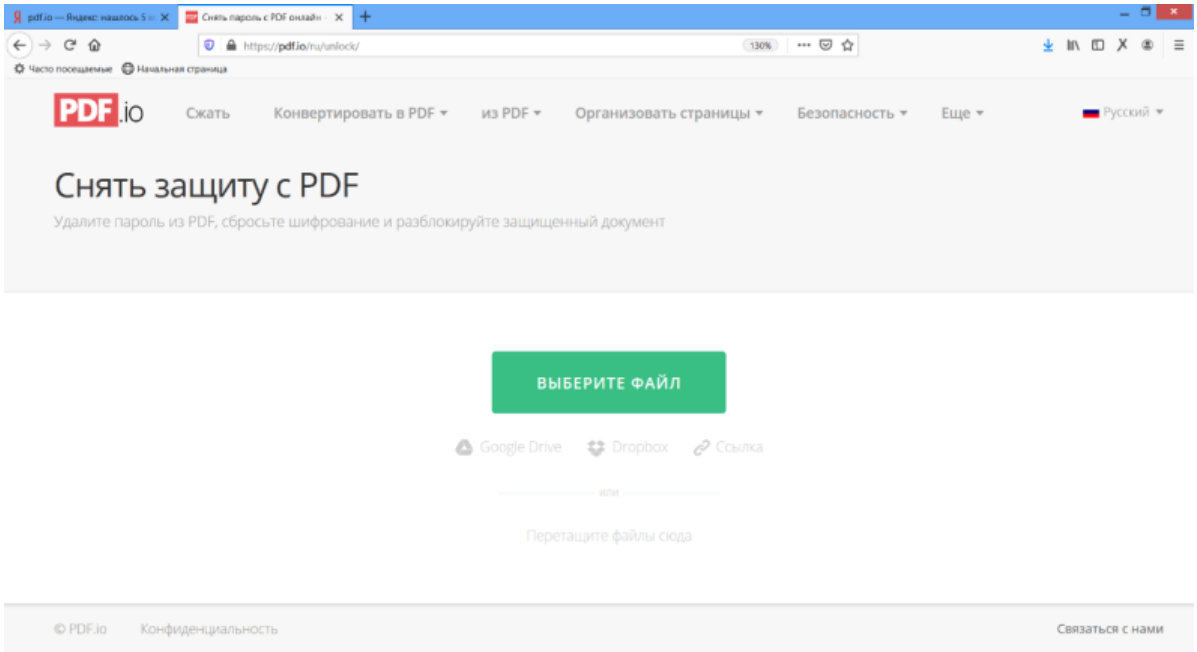


Рисунок 9.2. Выбор функции "Разблокировать PDF" на главной странице сайта

4. Стоит заметить, что сайт не спросил секретный пароль и спустя несколько секунд преобразования было предложено скачать разблокированный файл (см. рис. 9.3). Скачайте его под именем "Реферат 3 - разблокированный".

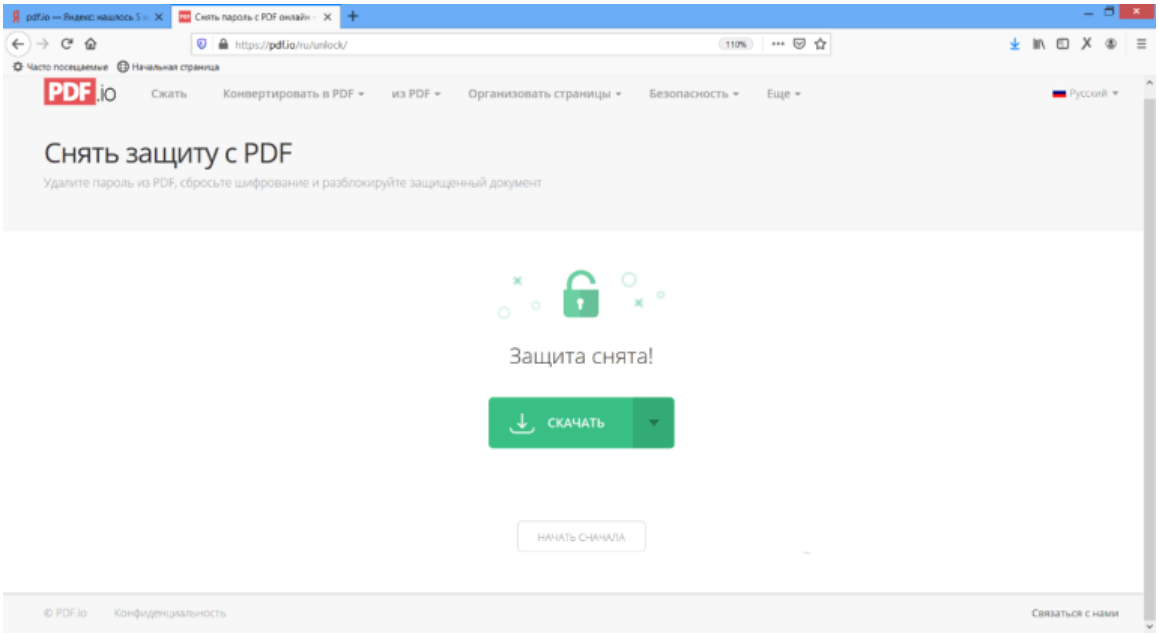


Рисунок 9.3. Страница для скачивания разблокированного файла

5. Открыть этот файл. Замечание: раньше на этом файле была наложена защита от копирования данных. Проверить снята ли защита с копирования данных. Для этого необходимо выделить часть текста и попытаться скопировать.

6. Открыть текстовый редактор и вставить скопированный текст. Убедиться, что текст копируется, а защита снята. Сделать скриншот.

7. Повторить процесс разблокировки для файлов "Реферат 2" и "Реферат 4", начиная с пункта 2.

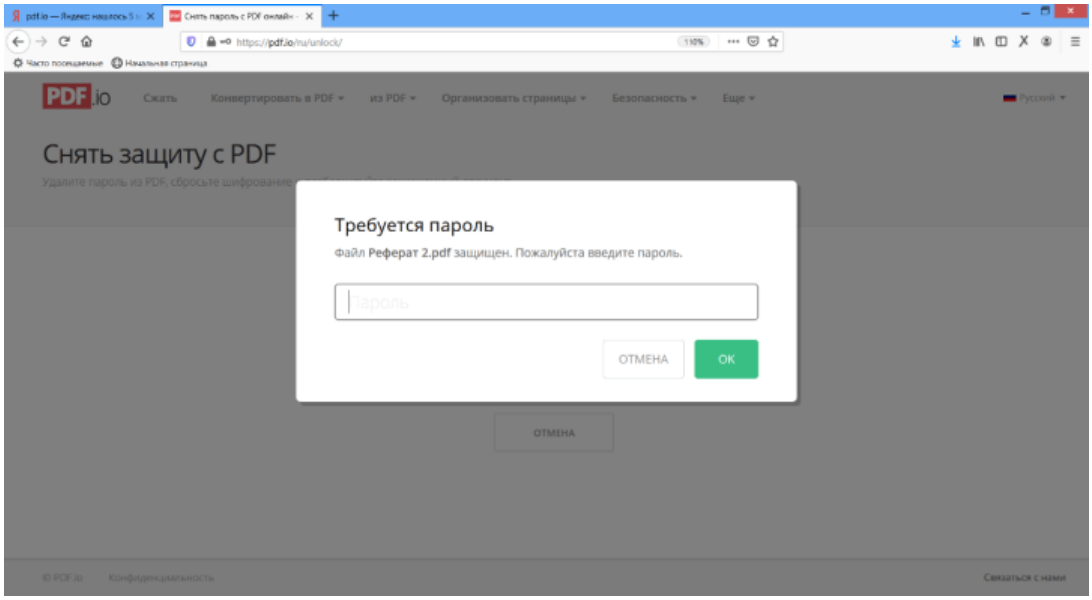


Рисунок 9.4. Страница ввода пароля для разблокировки файла pdf

8. В отличие от файла "Реферат 3" для данных файлов на шаге 5 появится табличка с вводом пароля (см. рис. 9.4). Это объясняется тем, что для этих фалов был установлен пароль на открытие файла, поэтому система сайта не может его открыть для разблокировки. С PDF-документа будет снята защита только в случае ввода настоящего пароля.

9. Сохраните его себе в память компьютера под именем "Реферат 2 - разблокированный", по кнопке "Скачать" (рис. 9.5).

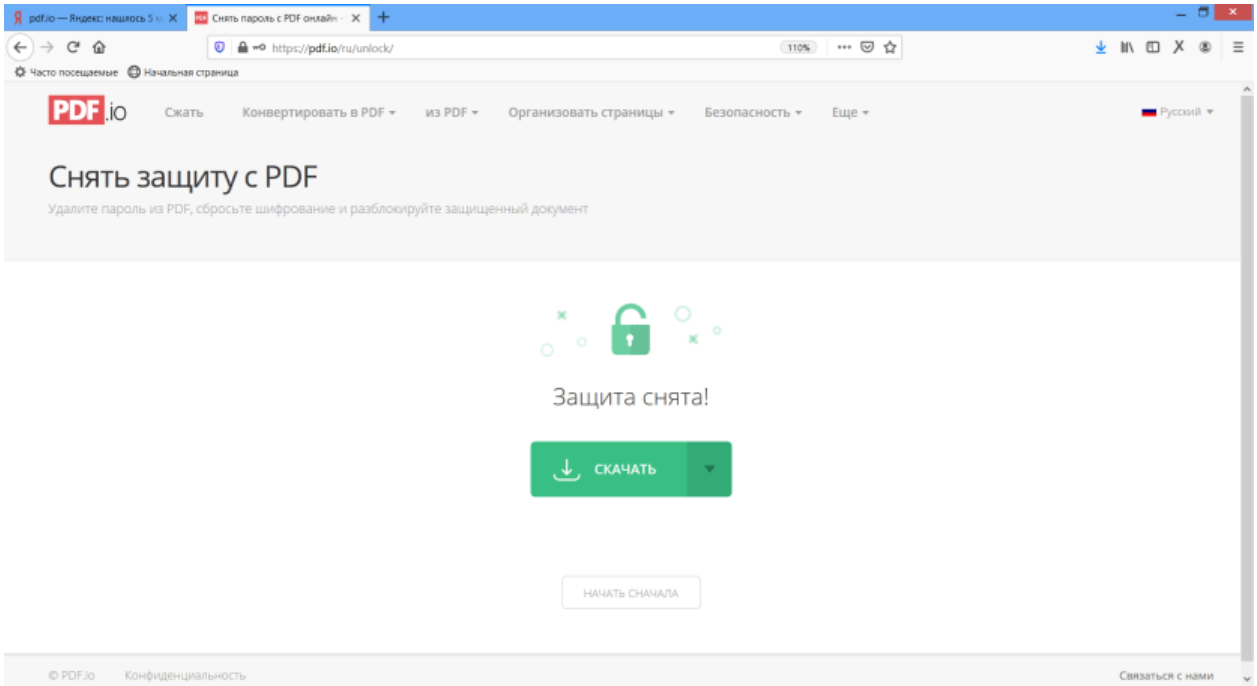


Рисунок 9.5. Страница ввода пароля для разблокировки файла pdf

10. Открыть полученные файлы "Реферат 2 - разблокированный" и "Реферат 3 - разблокированный" для просмотра кода в программе "Блокнот". Сравнить полученные коды.

11. Сделать скриншоты походу выполнения лабораторной работы и вставить в содержание студенческого отчета.

Индивидуальные варианты

Таблица 1 – варианты заданий

№ п/п	Имя файлов MS Excel	Имя файлов PDF
1.	bookbinder	canenclem
2.	apron	heaconric
3.	gendarme	drulatcra
4.	quidnunc	kilrimhus
5.	locksmith	pacunbinf
6.	adventurer	ditarract
7.	beaver	droworran
8.	athlete	proailpra
9.	midwife	dovstrdef
10.	holidayer	booselgru
11.	aquacckit	pasanngab
12.	kitten	midexphol
13.	critic	abbskumin
14.	albatross	abdquiaer
15.	renter	idesmowal
16.	costumier	parcozaca
17.	grazier	orideptes
18.	miller	farpulpil
19.	pilgrim	motdisdem
20.	duck	scabeddet
21.	meteor	coslikint
22.	mendicant	baredugoo

Раздел 3

Лабораторная работа № 5.
Криптография и стеганография

В данной лабораторной работе рассматриваются основные вопросы защищенного обмена данными.

Цели:

- Шифровать свою переписку при передачи по открытым канал данных.
- Организовать получение писем по принципа ассиметричного шифрования.
- Внедрять информацию в графические контейнеры.
- Находить хеш-значения контрольных данных.

Задание 1.

Без ключевое кодирование информации. Создание QR-кодов.

7. Открыть в сети Интернет сайт Crypt-online, набрав в адресной строек браузера ссылку http://crypt-online.ru/.
8. На панели "Преобразования" выбрать раздел "Утилиты" и категорию "QR-код".
9. В поле текст необходимо вписать свою Фамилию, Имя, Отчество и нажать кнопку "Кодировать".
10. В результате получим изображение QR-кода с закодированными ваши данными, как изображено на рис. 1.1.
11. Сделать скриншот данного изображения и вставить в отчет.
12. С помощью мобильного приложения на смартфоне постараться считать с данного QR-кода закодированную информацию.

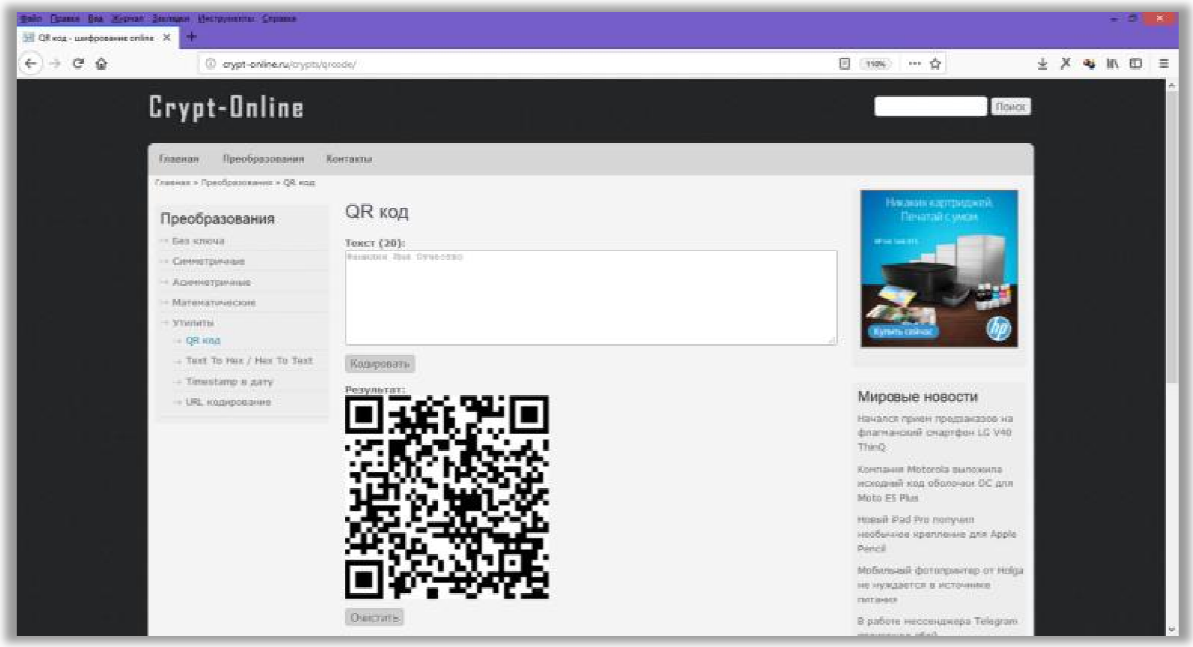


Рисунок 1.1.Создание QR-кодов.

Задание 2.
Симметричное шифрование с помощью ресурса Crypt-online.

1. На панели "Преобразования" выбрать раздел "Симметричные " и категорию "RC4".

2. В поле текст необходимо вписать секретную фразу, например "Съешь еще этих мягких французских булочек", а в поле "Ключ" - секретный пароль, например "Кибербезопасность" и нажать кнопку "Кодировать".

3. В результате преобразования получим зашифрованное сообщение, аналогичное изображению на рис. 2.1.

4. Сделать скриншот полученного шифра.

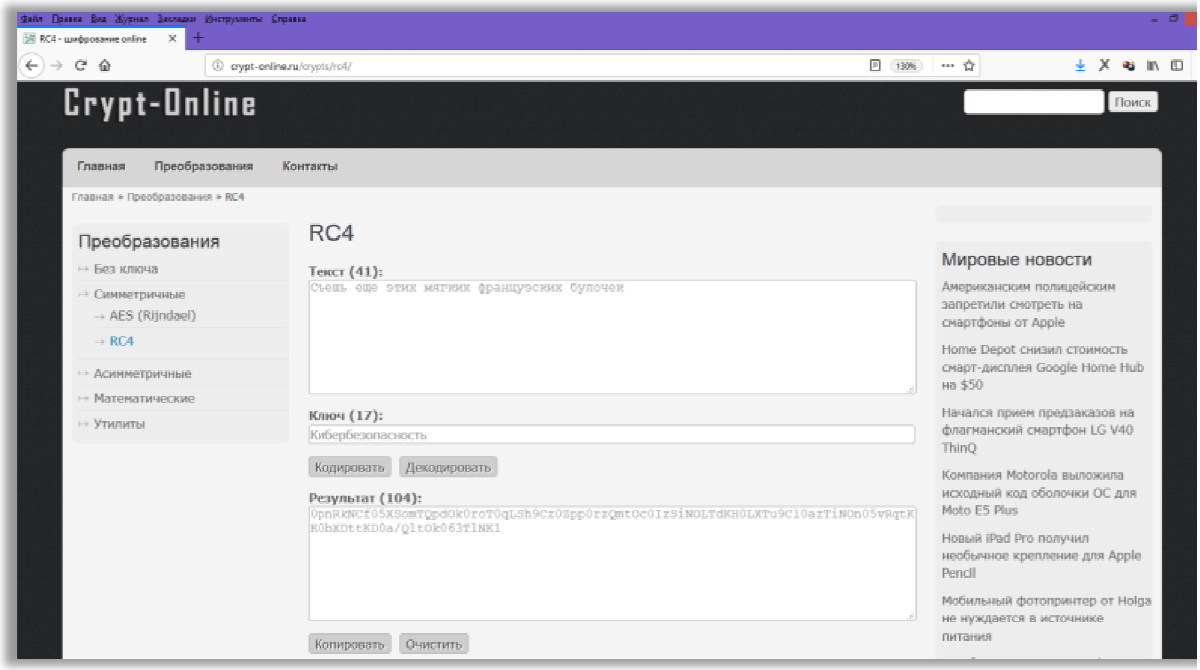


Рисунок 2.1.Шифрование текста методом RC4.

5. Далее, для проверки обратимости процесса шифрования, необходимо скопировать в буфер обмена зашифрованное сообщение, нажать на кнопку «Очистить» или обновить страницу.

6. В поле текста ввести шифр, полученный на шаге 1, а в строку ключа - тоже самое парольное слово.

7. Нажать на кнопку «Декодировать». Проверить, чтобы в поле результат сгенерировалось исходное секретное сообщение (см. рис. 2.2.).

8. Сделать снимок экрана с результатами дешифрования.

Задание 3. (самостоятельно)
Передача зашифрованных сообщений.

Необходимо договориться с однокурсниками о единой ключевой фразе, которая будет использоваться для шифрования сообщений. Организовать обмен зашифрованными сообщениями в группе, используя методы симметричного шифрования и дешифрования данных.

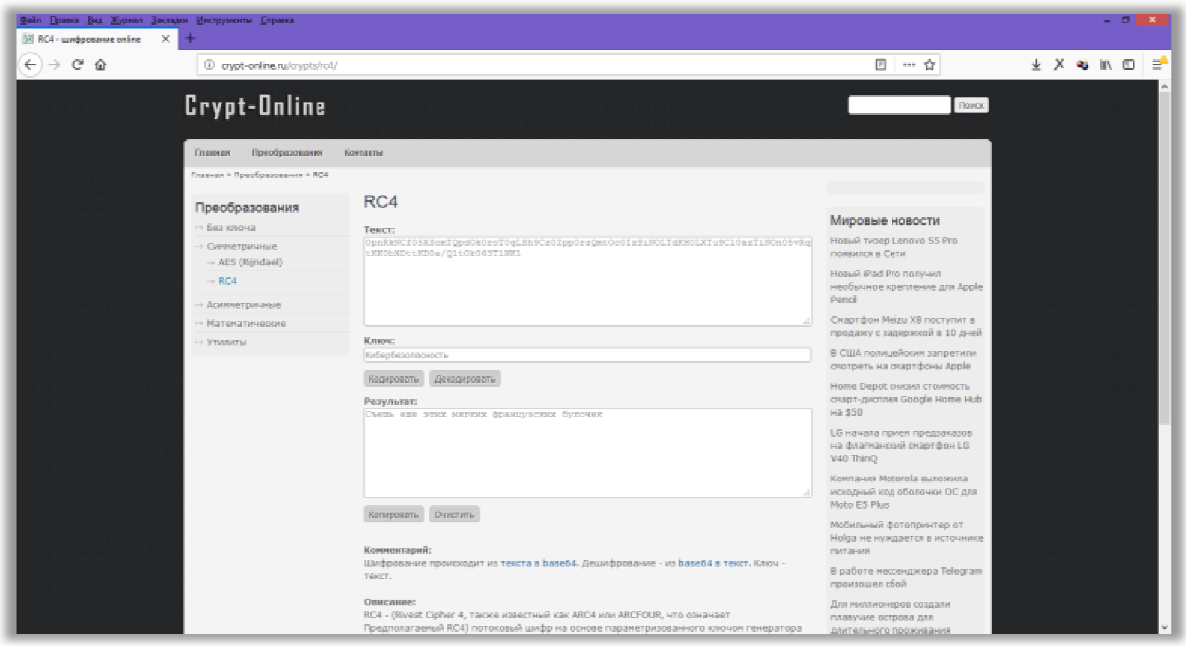


Рисунок 2.2. Дешифрование текста методом RC4.

Задание 4.

Ассиметричное шифрование с помощью ресурса Crypt-online.

1. На панели "Преобразования" выбрать раздел "Ассимметричные " и категорию "RSA".

2. Теперь необходимо сгенерировать пару ключей: открытый и закрытый. Для этого в нижней части панели необходимо найти кнопку "Генерировать". В полях "Открытый ключ" и "Закрытый ключ" появятся ключи шифрования.

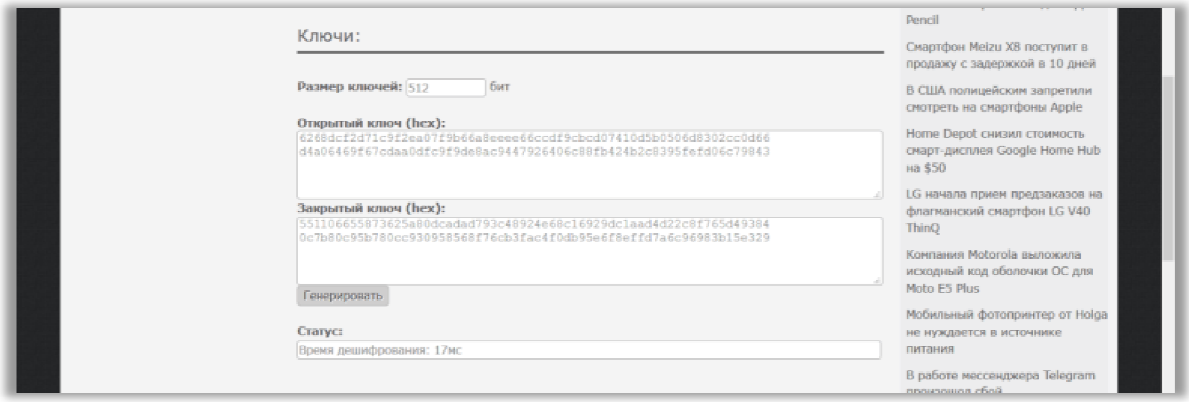


Рисунок 4.1. Генерация пары ключей в алгоритме RSA.

3. Необходимо написать свое секретное сообщение в поле "Текст".

4. С помощью открытого ключа можно зашифровать сообщение и послать его по каналу связи послать его по каналу связи.

5. С помощью закрытого ключа можно дешифровать полученное сообщение и прочитать содержимое.(см. рис. 4.2).

6. Сделайте снимок с экрана с зашифрованным/дешифрованным сообщением.

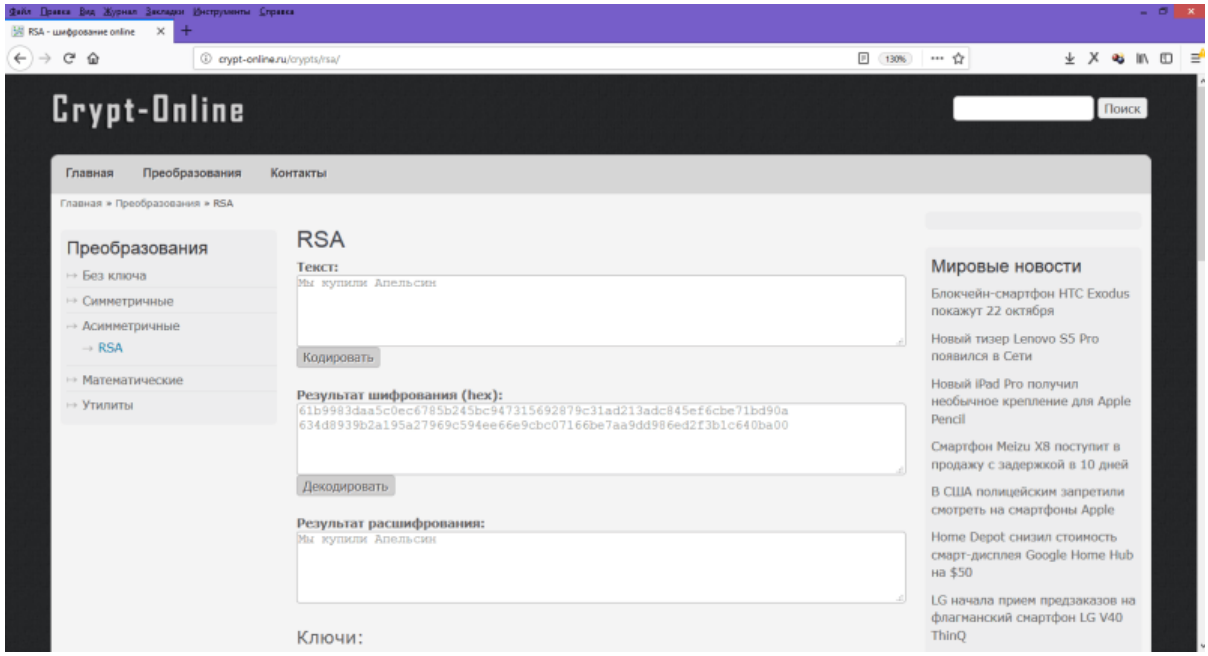


Рисунок 4.2. Процесс шифрования/дешифрования в алгоритме RSA.

Задание 5. (самостоятельно)
Передача зашифрованных сообщений.

В этой лабораторной работе понадобятся 2 окна браузера для одновременной переписки. В одном окне необходимо сгенерировать пару "открытый-закрытый" ключ, и "открытый"переслать всем собеседникам по сети, для того, чтобы они могли Вам написать сообщение, а "закрытый" хранить в тайне для дешифрования входящих писем.

В другом окне браузера необходимо вставить чужой "открытый" ключ, присланный по сети, чтобы была возможность посылать в сеть ответные сообщения. Организовать обмен зашифрованными сообщениями в группе, используя методы ассиметричного шифрования и дешифрования данных.

Задание 6.
Скрытие текстовой информации в растровых изображениях.

В сети интернет открыть сайт *«Steganography Online» («Онлайн стеганография»)* перейдя по ссылке http://stylesuxx.github.io/steganography/ (рис. 4.3). В разделе «Encode» («Зашифровать») загрузить любое изображение, нажав кнопку «Обзор» («Выбрать файл»). В поле ниже ввести сообщение, которое необходимо внедрить в изображение (желательно на английском языке). Нажать на кнопку «Encode» («Зашифровать») (рис. 4.4).

Появятся бинарное разложение текстового сообщения, которое будет внедрено в изображение. Загруженное изображение вначале будет нормализовано, а по следующему изображению будет распределены биты текста. Поэтому на компьютер необходимо скачать последнее из них.

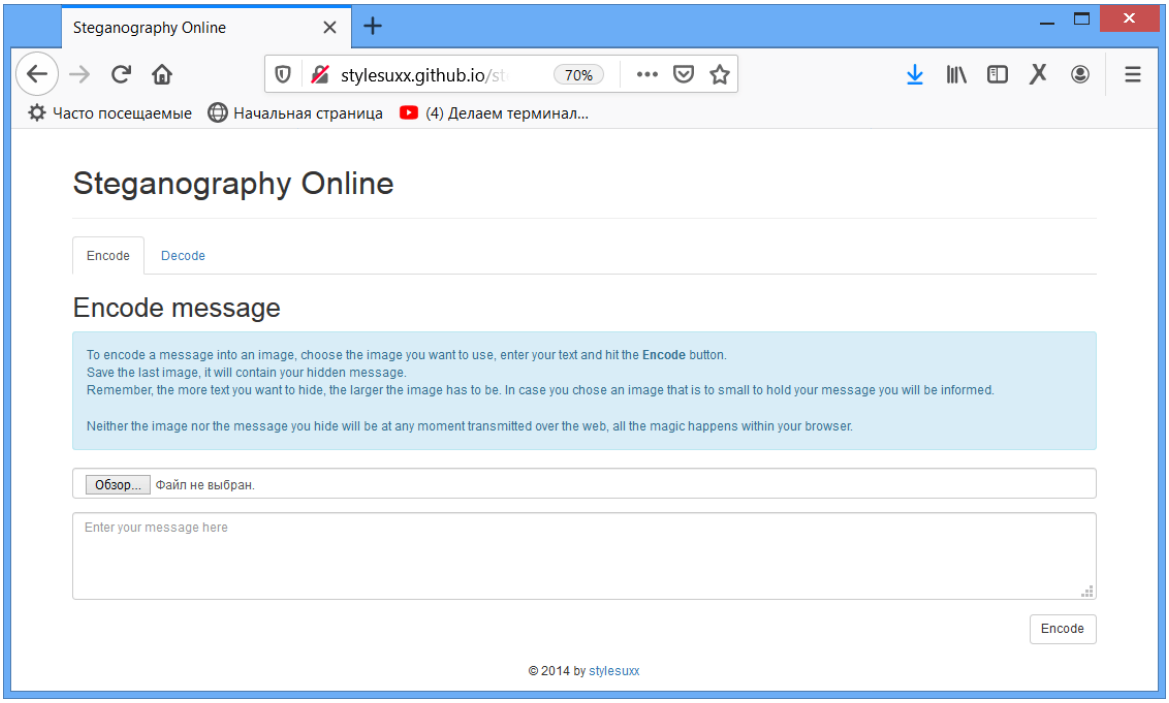


Рисунок 4.3. Страница сайта "Steganography Online".

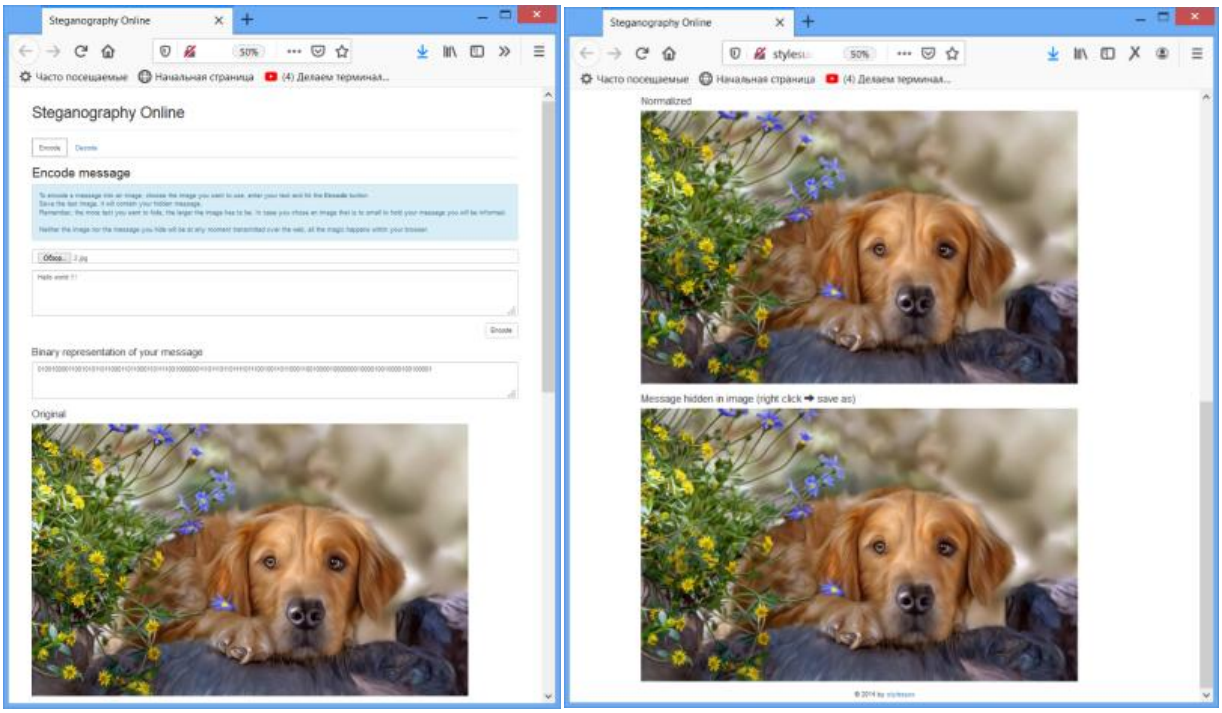


Рисунок 4.4. Процесс скрытия сообщения в цифровой сигнал.

Необходимо перейти в раздел «Decode» («Расшифровать») и загрузить последнее скаченное изображение, нажав «Обзор» («Выбрать файл»). Нажать на кнопку «Decode» («Расшифровать»). В окне "Hidden message" («Скрытое сообщение») появится скрытое сообщение (рис. 4.5).

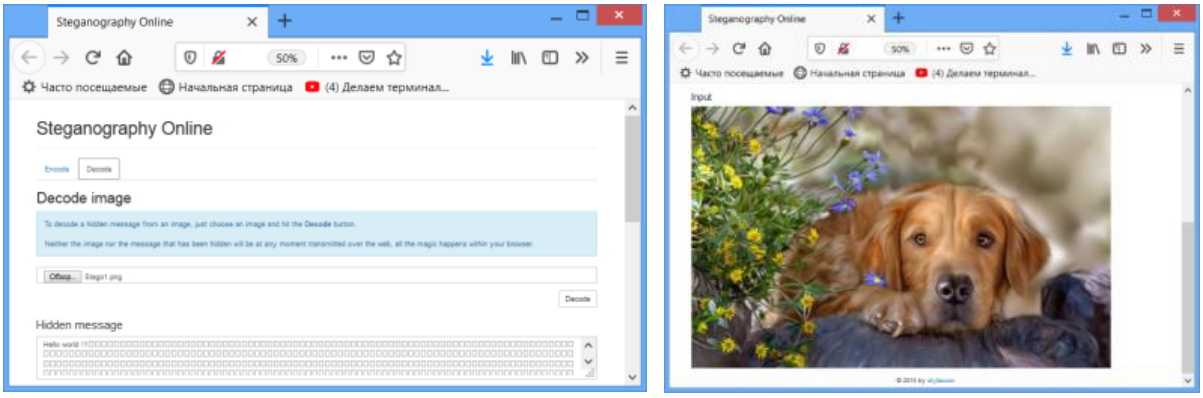


Рисунок 4.5. Процесс изъятия сообщения из цифрового сигнала.

Задание 7. (самостоятельно)
Передача скрытых сообщений.

Необходимо договориться с однокурсником о методе стеганографии и организовать переписку в закрытом диалоге студенческой группы, публикуя посты с изображениями, в которых внедрен скрытый текст.

Задание 8.
Скрытие графической информации в растровых изображениях.

Открыть сайт в интернете сайт «Image Steganography» «Графическая стеганография» (рис. 4.6). После загрузки вы увидите следующую страницу.

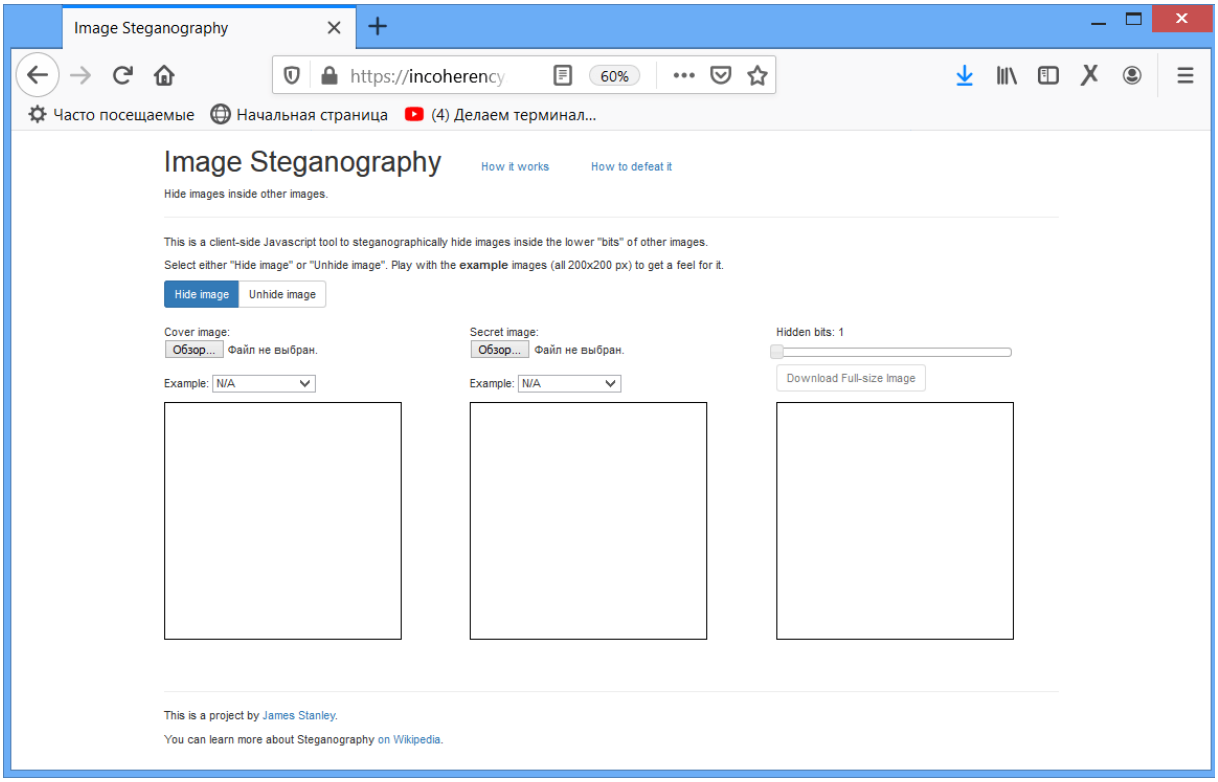


Рисунок 4.6. Страница сайта " Image Steganography".

В разделе «Hide image» («Скрыть изображение») присутствуют 3 окна: «Cover image» («Изображение-носитель»), «Secret image» («Скрываемое изображение») и «Finish image» («Окончательное изображение»). В первое окно необходимо загрузить изображение, которое станет носителем информации. Во второе окно - загрузить изображение, которое необходимо спрятать. После загрузки изображения результат внедрения появится в 3 окне автоматически(рис. 4.7).

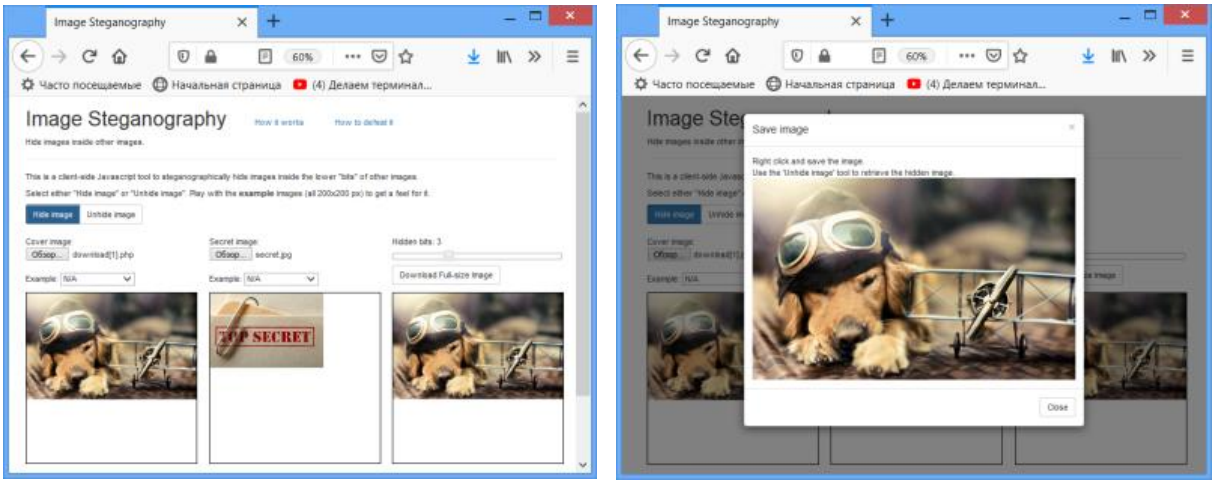


Рисунок 4.7. Внедрение секретного изображения в носителе информации.

Бегунок «Hidden bits» («Внедряемые биты») необходимо открутить до крайнего правого положения и перемещать до тех пор, по внедрение изображения не перестанет быть заметным.

После чего необходимо нажать кнопку «Download Full-size image» («Загрузить полноразмерное изображение»). Скачайте увеличенную картинку на компьютер.

Перейдите в раздел «Unhide image» («Показать изображение»). Нажать кнопку «Обзор» («Выберите файл») и загрузите графический файл, полученный на предыдущем этапе.

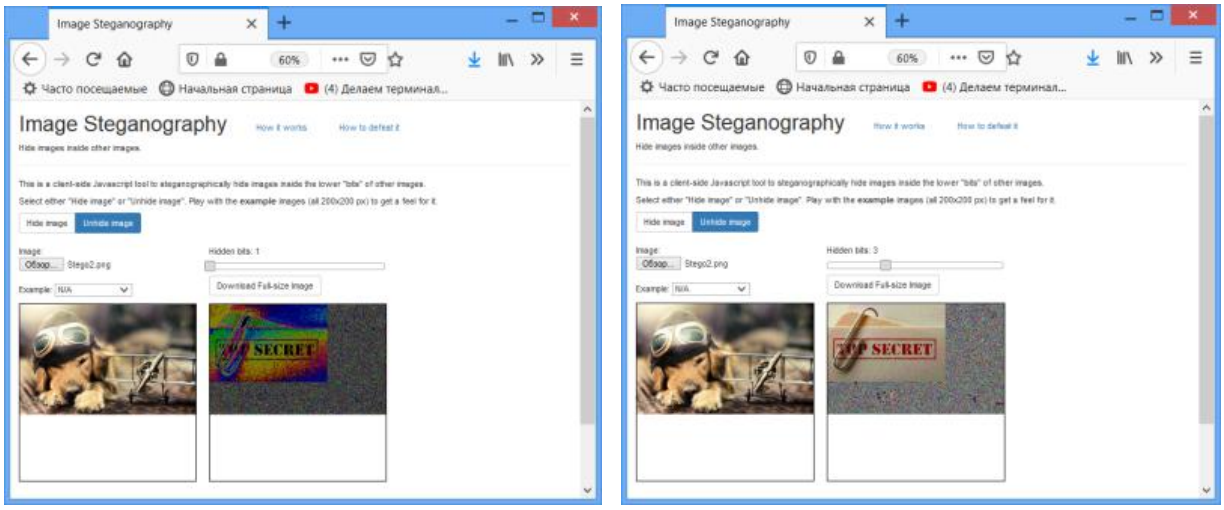


Рисунок 4.8. Извлечение секретного изображения из носителя информации.

На последнем шаге необходимо установить бегунок «Hidden bits» («Внедряемые биты») на уровень, заданный при внедрении, тогда внедряемое изображение примет естественный вид.

Задание 9. (самостоятельно)
Передача скрытых изображений.

Договоритесь с однокурсником о методе стеганографии и организовать переписку в закрытом диалоге, обмениваясь растровыми изображениями.

Задание 10.
Хэширование сообщений.

Для верификации различных данных необходимо использование хэш-кодов. Откройте сайт в сети интернет «https://www.tools4noobs.com». В открывшемся сайте выберите категорию «Online hash calculator».

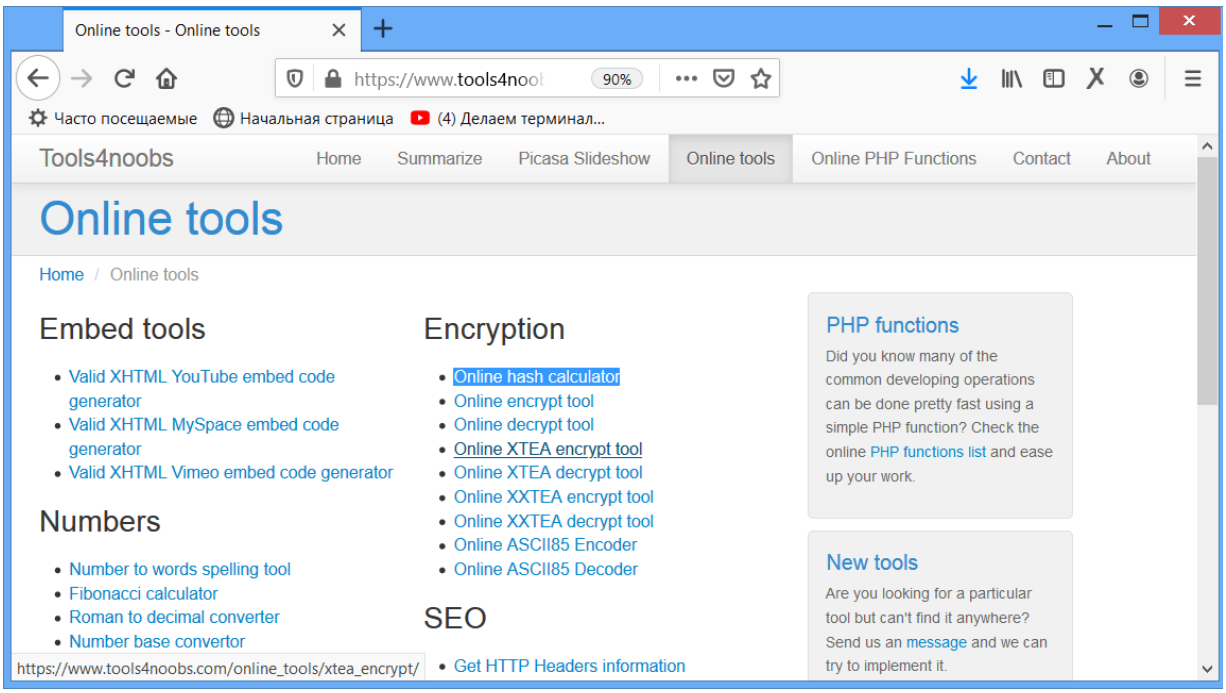


Рисунок 4.9. Страница сайта "Tools4noobs".

В появившемся окне необходимо ввести текст для создания хеш-кода. В качестве алгоритма выбрать sha1. Получим результат, изображенный на рисунке 4.10. Полученное сообщение является хэш-кодом для проверки оригинальности введенного текста. Скопируйте его в отдельный файл.

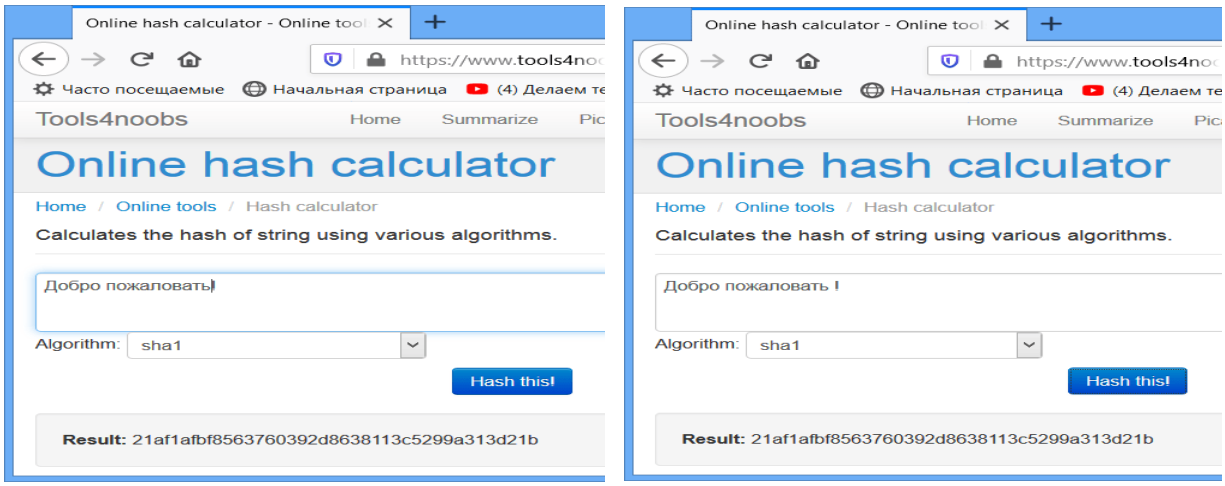


Рисунок 4.10. Пример хэширования текстовой информации.

Теперь если добавить в текст некоторую информацию или изменить исходное сообщение, то должен измениться и хэш-код. При этом стоит отметить, что даже при изменении одного символа измениться не один символ хэш-кода, а весь хэш-код целиком (т.е. каждый символ хэш-кода не совпадет с первичным). Скопируйте полученный хэш-код после внесений изменений в текст, в тот же файл, что и первый и сравните их.

Задание 11. (самостоятельно)
Шифрование данных стандартными методами.

С помощью ресурса *"Tools4noobs"* организуйте с одногруппником переписку с помощью двух инструментов Online encrypt tool и Online decrypt tool, выбрав один. из алгоритмов шифрования, например "Enigma". Пример изображен на рис 4.11.

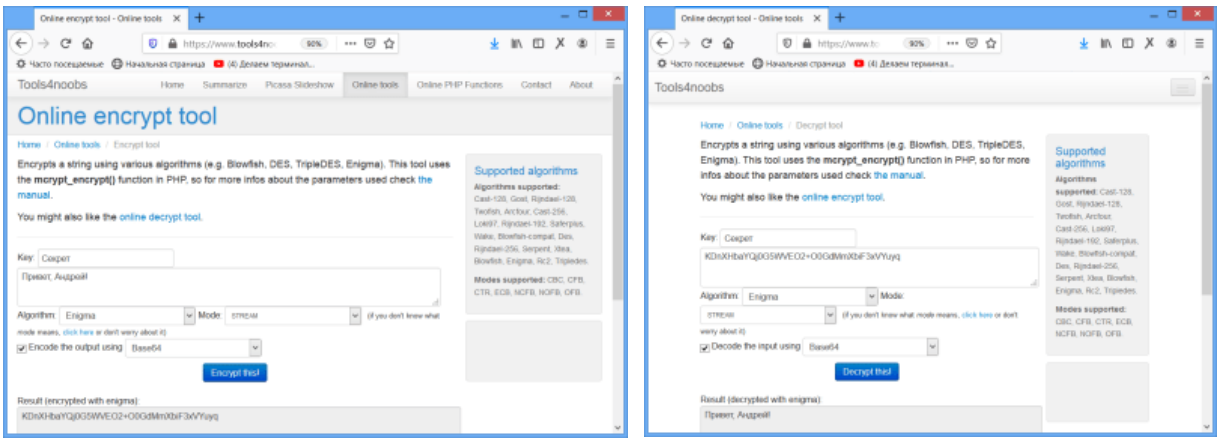


Рисунок 4.11. Пример шифрования текста методом Enmiga.