НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«МОСКОВСКИЙ ЭНЕРГЕТИЧЕСКИЙ ИНСТИТУТ»

Отчет по лабораторной работе № 5.

По дисциплине “Защита данных”

Выполнил: Гайчуков Дмитрий
группа А-13-21
Вариант 29

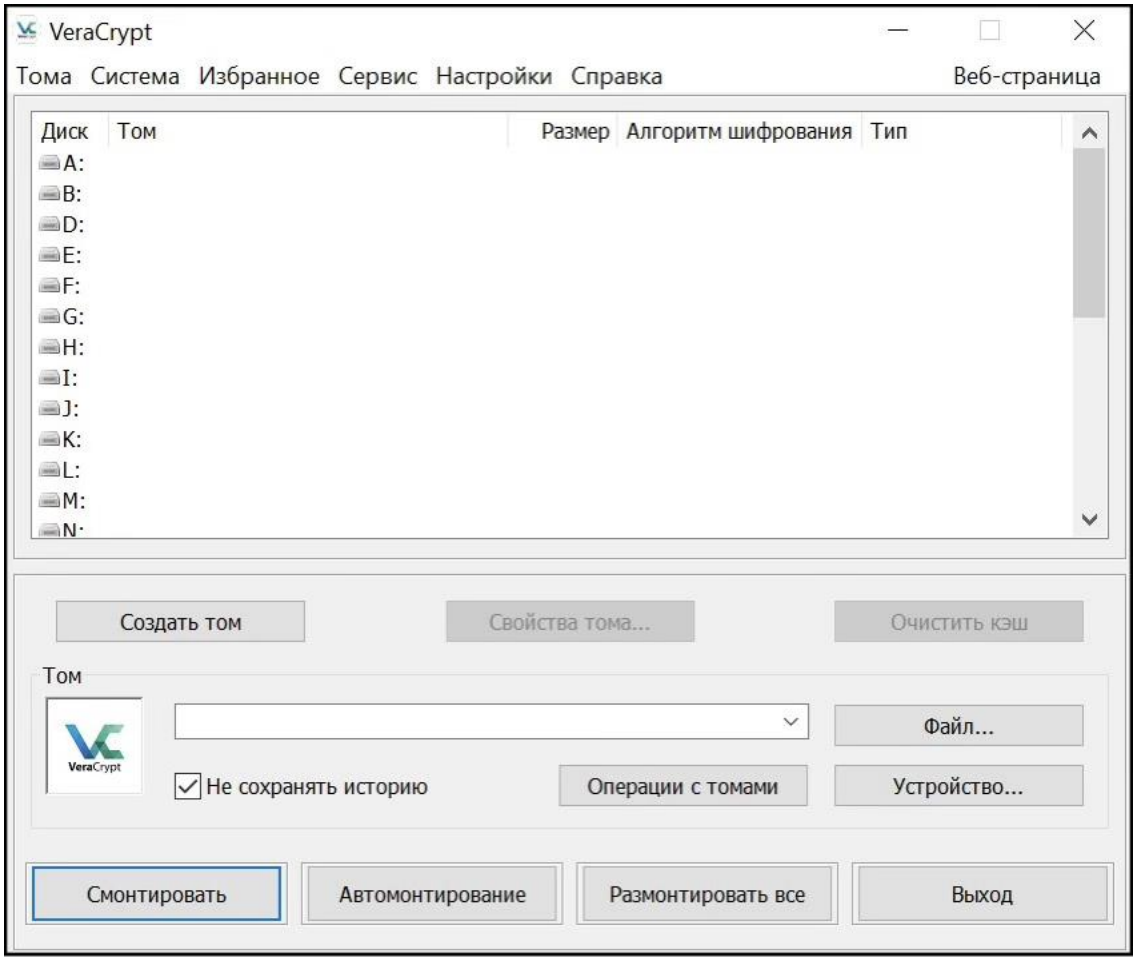
2024

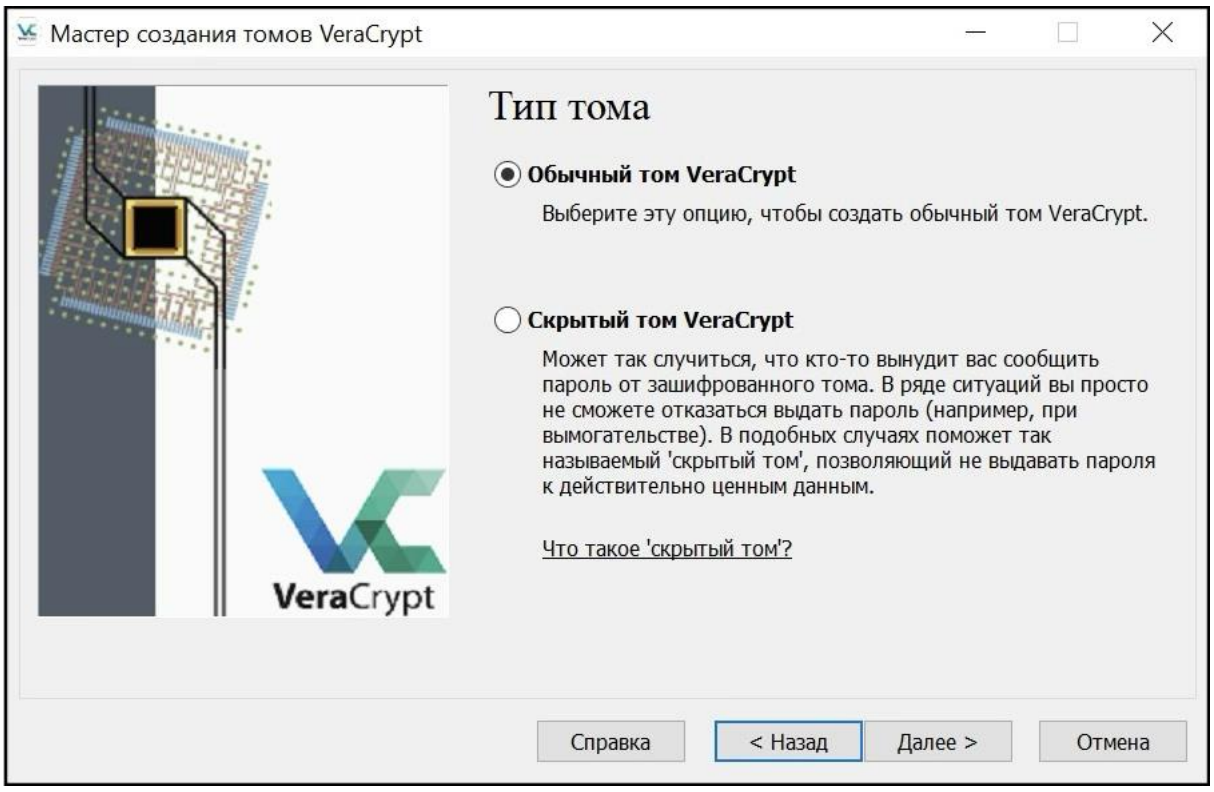
Лабораторная работа №5

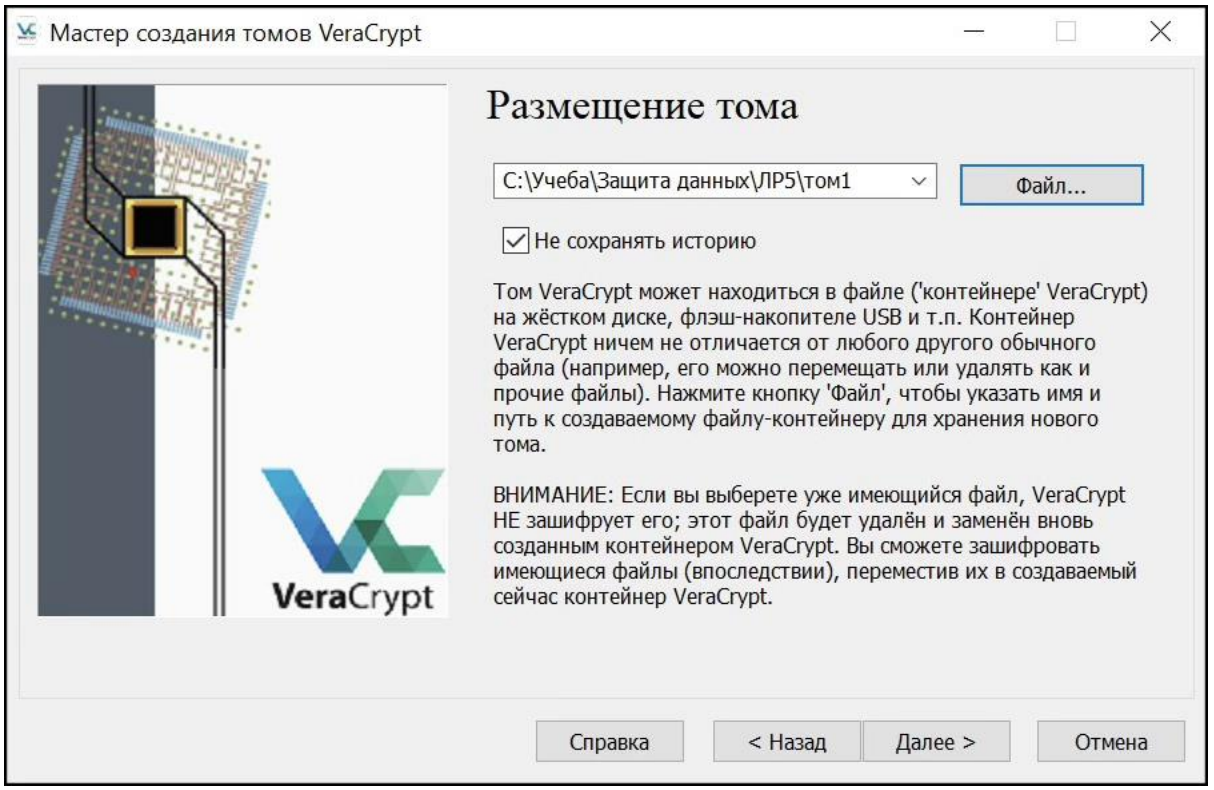
Изучение программных средств шифрования и электронной подписи, компьютерной стеганографии и защиты от вредоносных программ

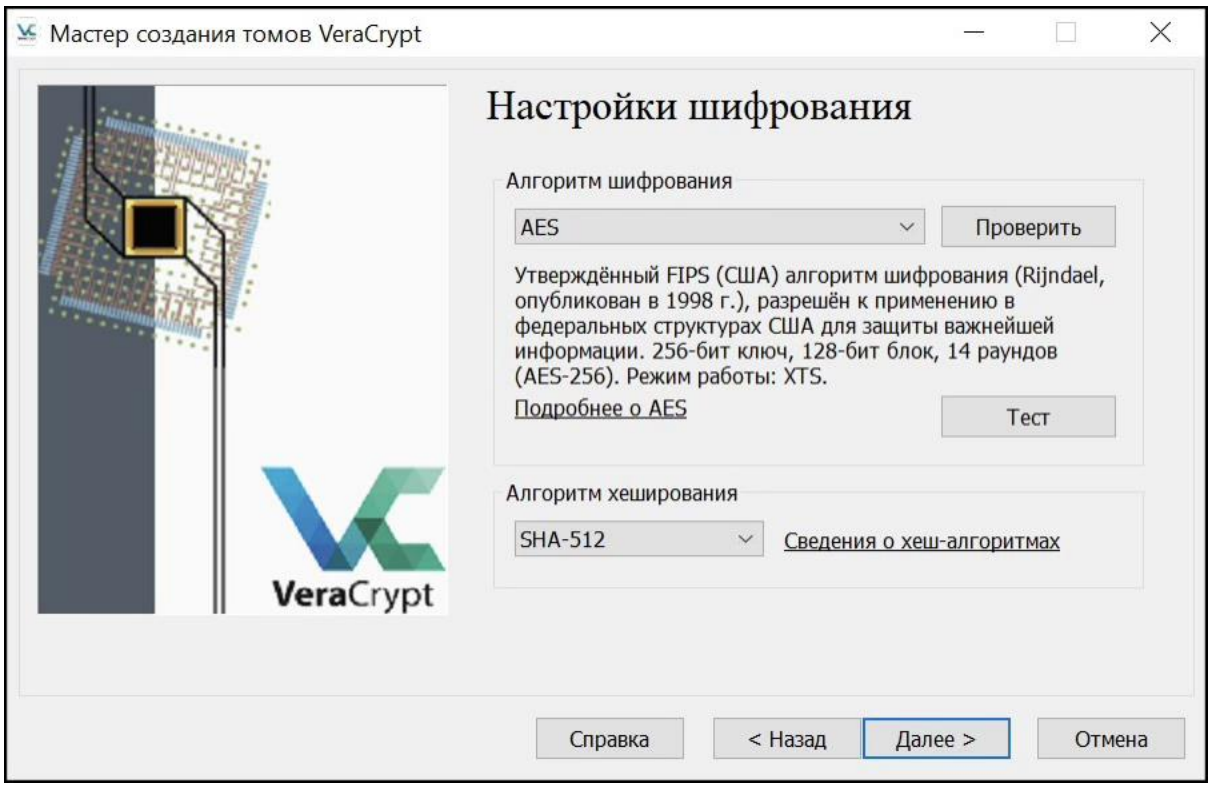
Содержание задания

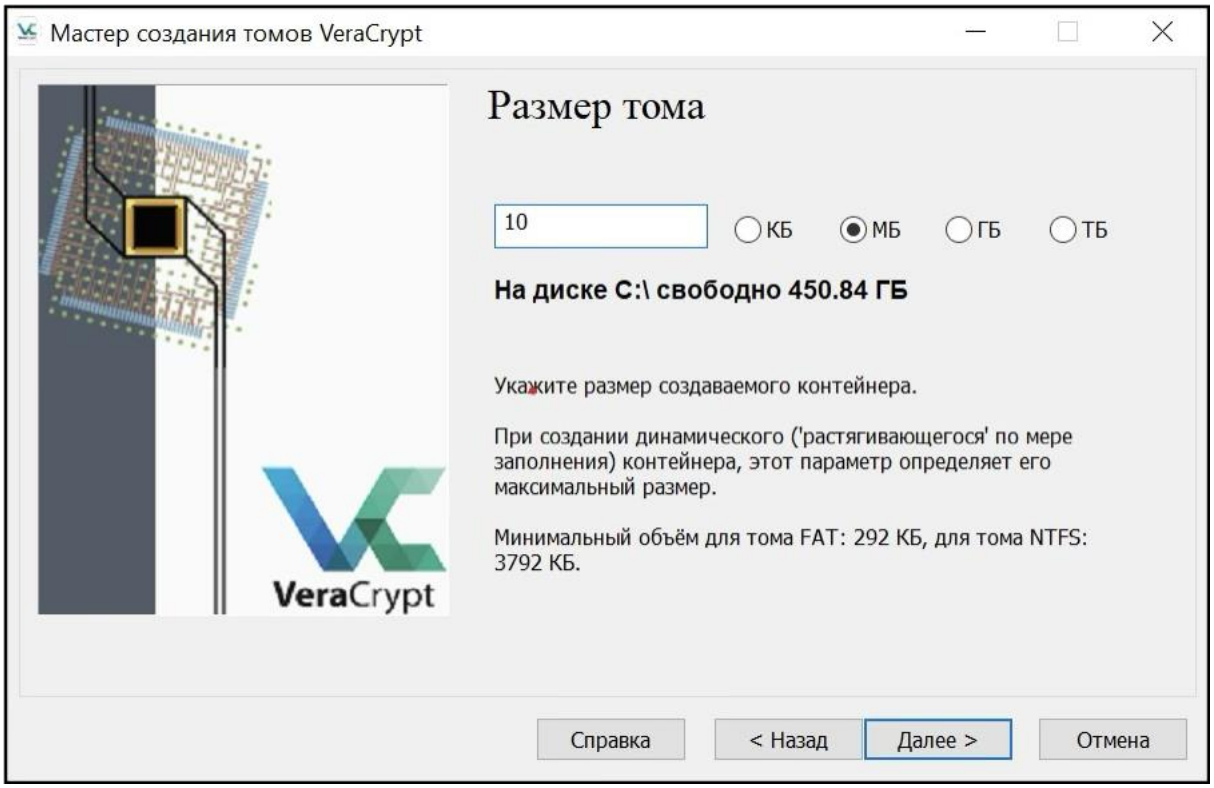
1. Скопировать в произвольную папку на локальном жестком диске файл VeraCrypt Setup 1.17.exe.
   1.1. Если программа VeraCrypt не установлена (отсутствует соответствующий пункт в главном меню), выполнить установку программы VeraCrypt, согласившись со всеми параметрами установки по умолчанию.
   1.2. Для русификации интерфейса программы выполнить после ее первого запуска команду меню Settings | Language | Русский.
   1.3. На примере работы с произвольными (несистемными) файлами различного типа изучить функции программы шифрования VeraCrypt, учитывая, что:
   - перед шифрованием файлов необходимо создать том (зашифрованный файловый контейнер) с помощью кнопки «Создать том» и мастера создания томов VeraCrypt: выбрать тип тома – обычный том VeraCrypt, выбрать размещение тома (файл с произвольным именем в любой доступной папке на любом диске), выбрать алгоритмы шифрования и хеширования (любые из доступных в программе), выбрать размер тома (рекомендуется 10 МБ), ввести и подтвердить пароль тома (для генерации ключа его шифрования), выполнить форматирование тома (потребуется хаотичное перемещение курсора мыши внутри окна мастера);

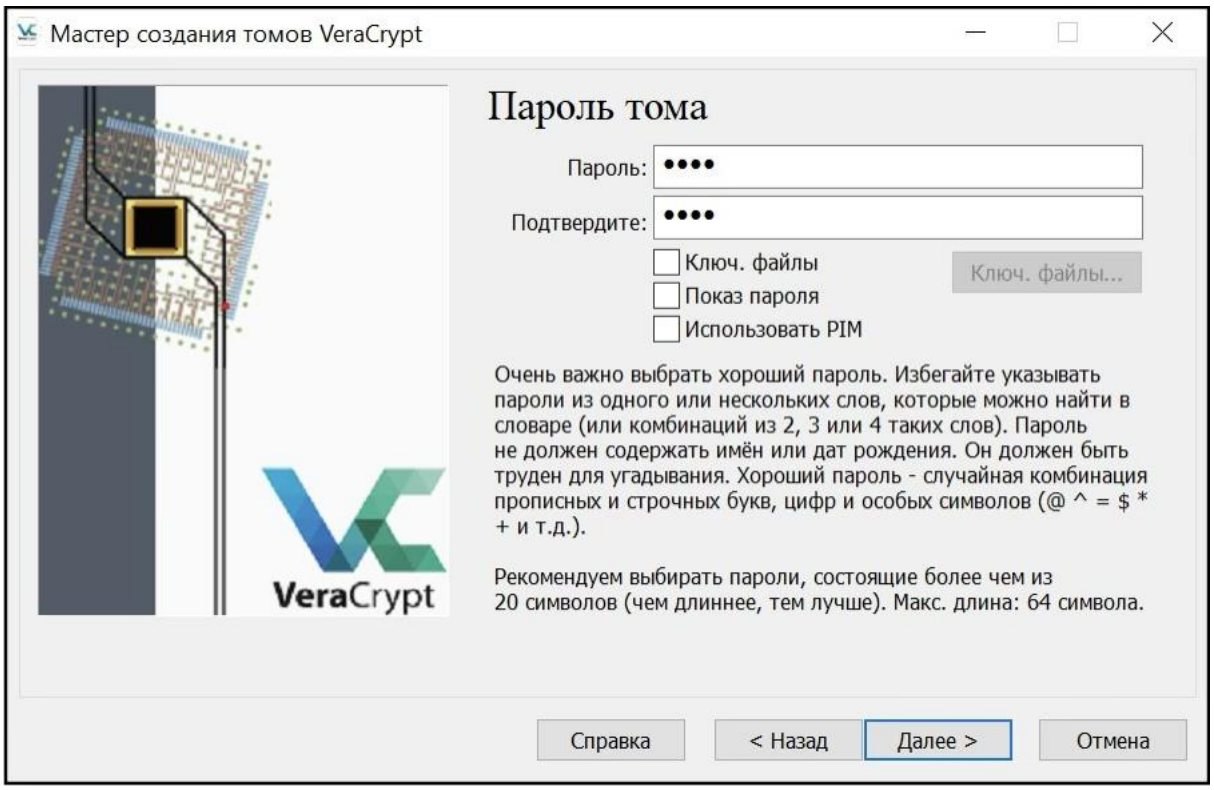


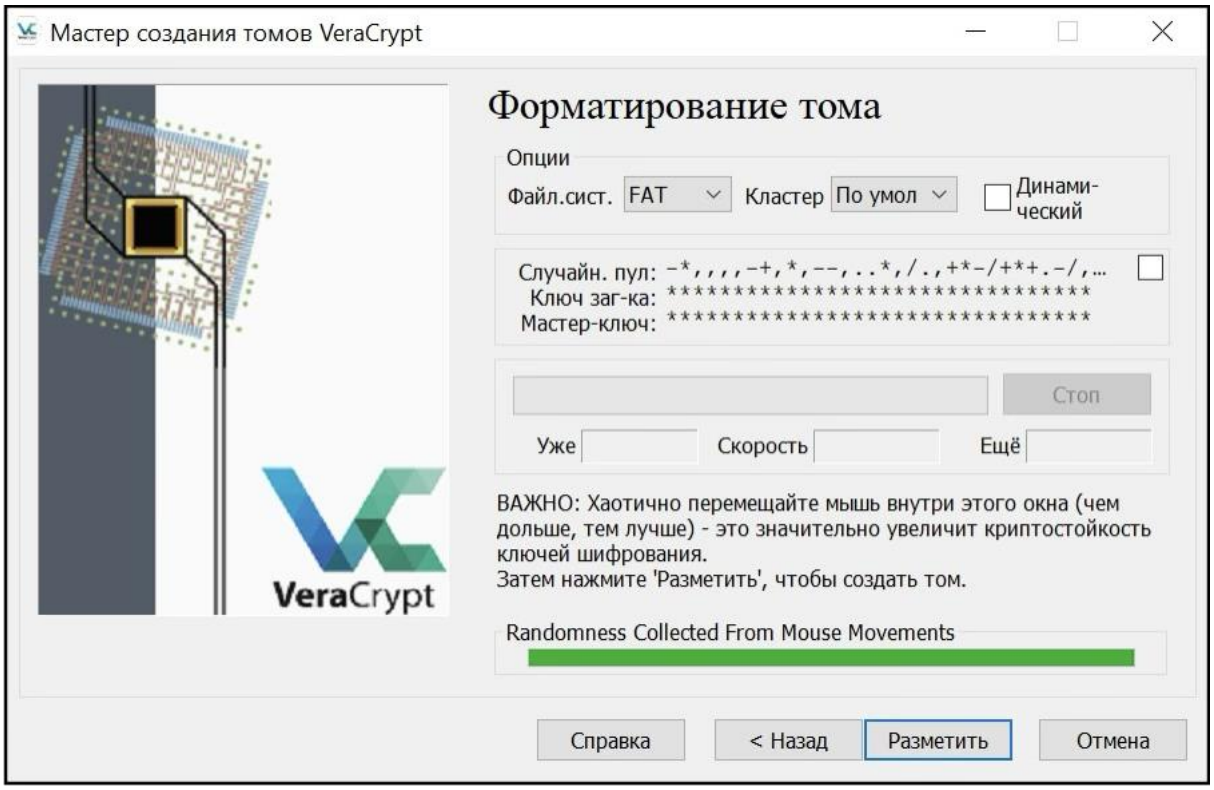

Мастер создания томов VeraCrypt
Тип тома
Обычный том VeraCrypt
Выберите эту опцию, чтобы создать обычный том VeraCrypt.
Скрытый том VeraCrypt
Может так случиться, что кто-то вынудит вас сообщить пароль от зашифрованного тома. В ряде ситуаций вы просто не сможете отказаться выдать пароль (например, при вымогательстве). В подобных случаях поможет так называемый 'скрытый том', позволяющий не выдавать пароля к действительно ценным данным.
Что такое 'скрытый том'?
VeraCrypt
Справка
< Назад
Далее >
Отмена


Мастер создания томов VeraCrypt
Размещение тома
C:\Учеба\Защита данных\ЛР5\том1
Файл...
Не сохранять историю
Том VeraCrypt может находиться в файле ('контейнере' VeraCrypt) на жёстком диске, флэш-накопителе USB и т.п. Контейнер VeraCrypt ничем не отличается от любого другого обычного файла (например, его можно перемещать или удалять как и прочие файлы). Нажмите кнопку 'Файл', чтобы указать имя и путь к создаваемому файлу-контейнеру для хранения нового тома.
ВНИМАНИЕ: Если вы выберете уже имеющийся файл, VeraCrypt НЕ зашифрует его; этот файл будет удалён и заменён вновь созданным контейнером VeraCrypt. Вы сможете зашифровать имеющиеся файлы (впоследствии), переместив их в создаваемый сейчас контейнер VeraCrypt.
VeraCrypt
Справка
< Назад
Далее >
Отмена

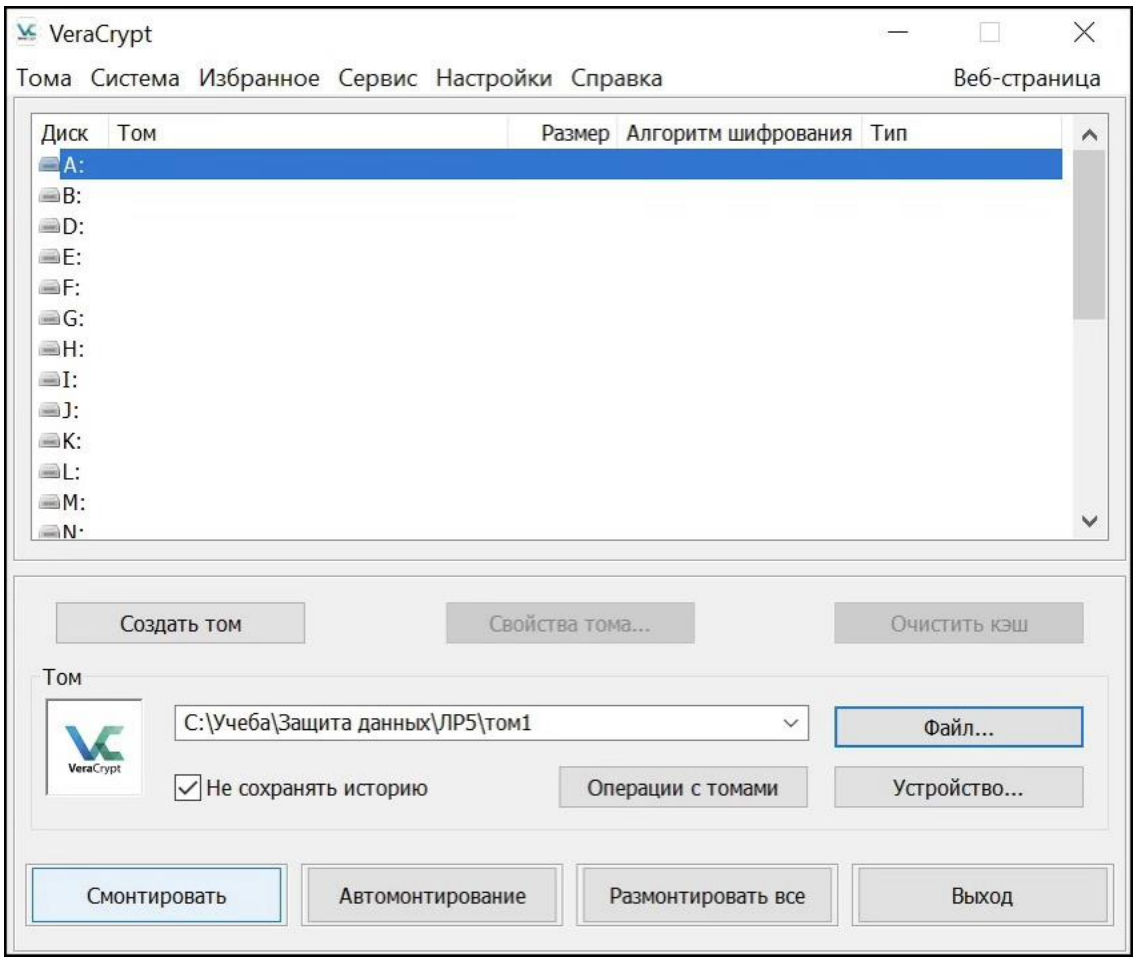

Мастер создания томов VeraCrypt
Настройки шифрования
Алгоритм шифрования
AES
Проверить
Утверждённый FIPS (США) алгоритм шифрования (Rijndael, опубликован в 1998 г.), разрешён к применению в федеральных структурах США для защиты важнейшей информации. 256-бит ключ, 128-бит блок, 14 раундов (AES-256). Режим работы: XTS.
Подробнее о AES
Тест
Алгоритм хеширования
SHA-512
Сведения о хеш-алгоритмах
VeraCrypt
Справка
< Назад
Далее >
Отмена

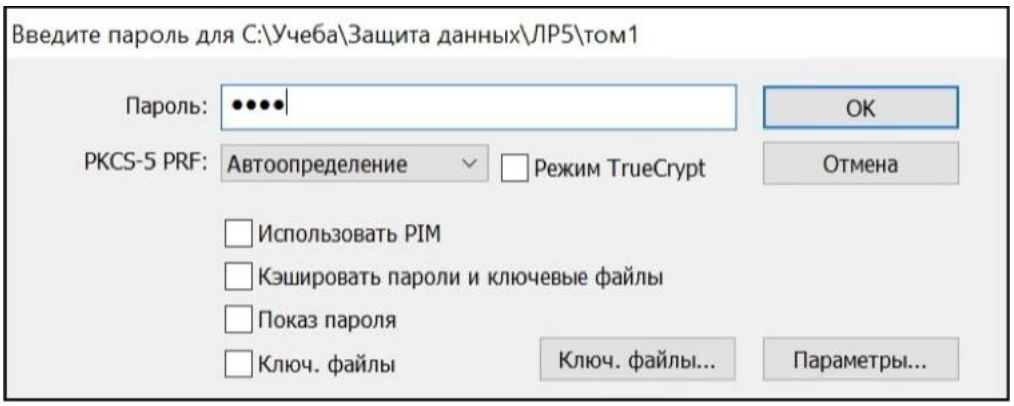

Мастер создания томов VeraCrypt
Размер тома
10
КБ
МБ
ГБ
ТБ
На диске C:\ свободно 450.84 ГБ
Укажите размер создаваемого контейнера.
При создании динамического ('растягивающегося' по мере заполнения) контейнера, этот параметр определяет его максимальный размер.
Минимальный объём для тома FAT: 292 КБ, для тома NTFS: 3792 КБ.
VeraCrypt
Справка
< Назад
Далее >
Отмена



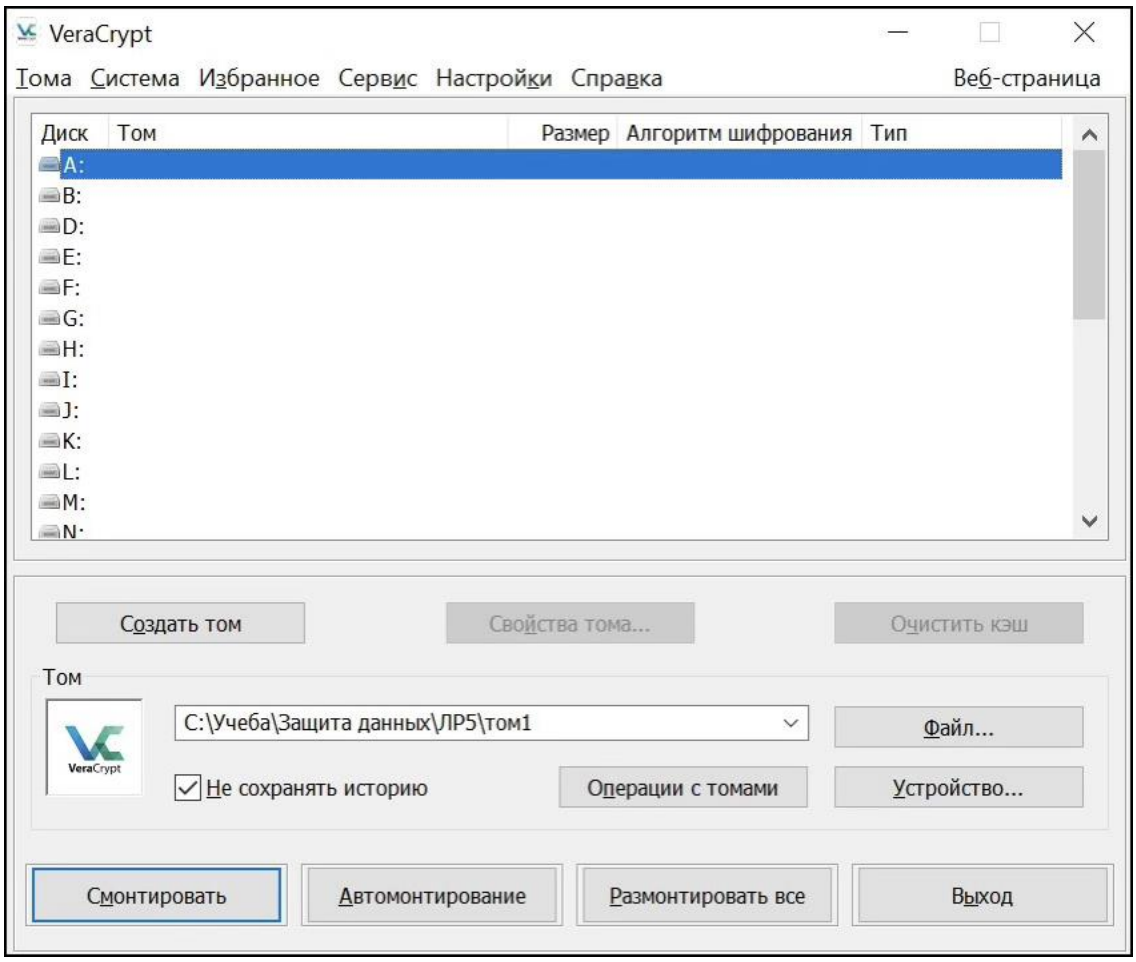


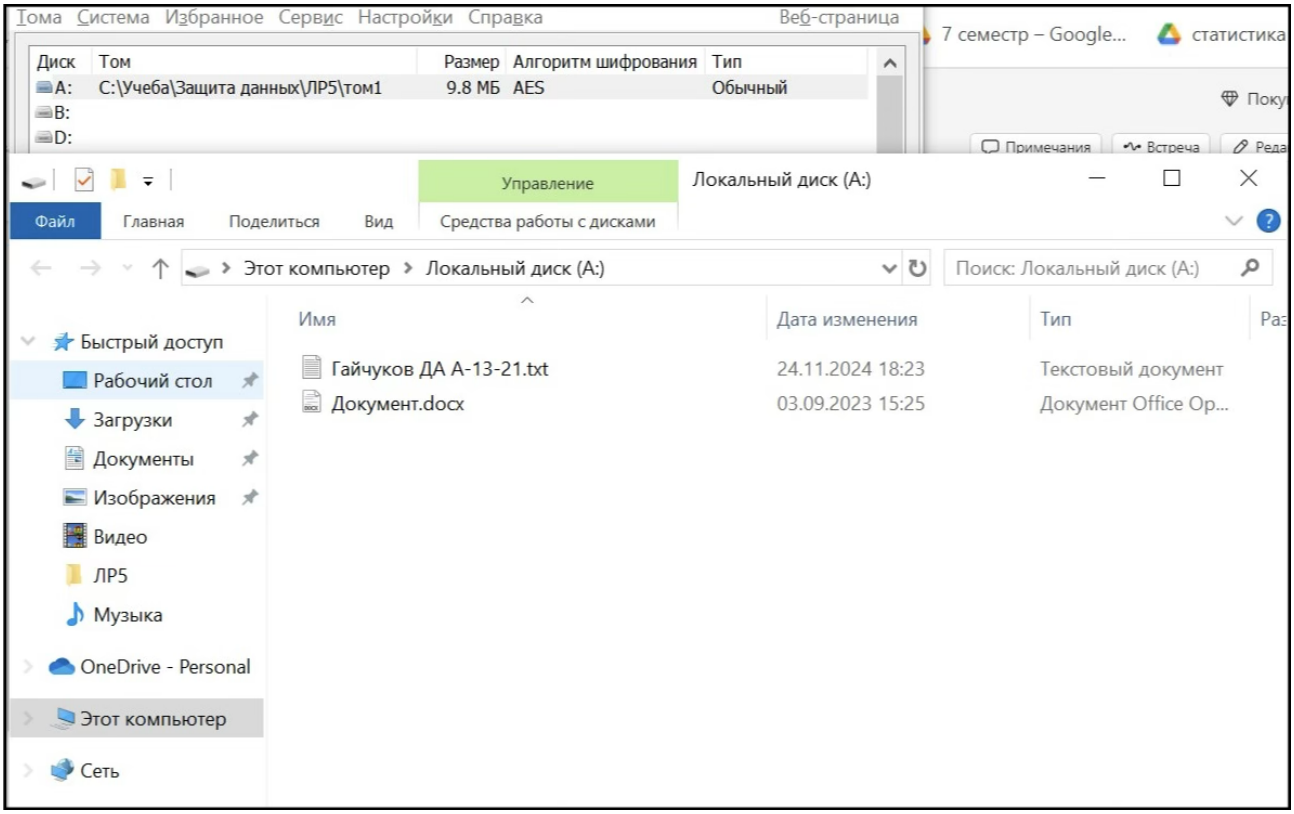
- выбрать незанятое имя (букву) для созданного тома и смонтировать его с помощью кнопки «Смонтировать», после чего ввести заданный при создании тома пароль;



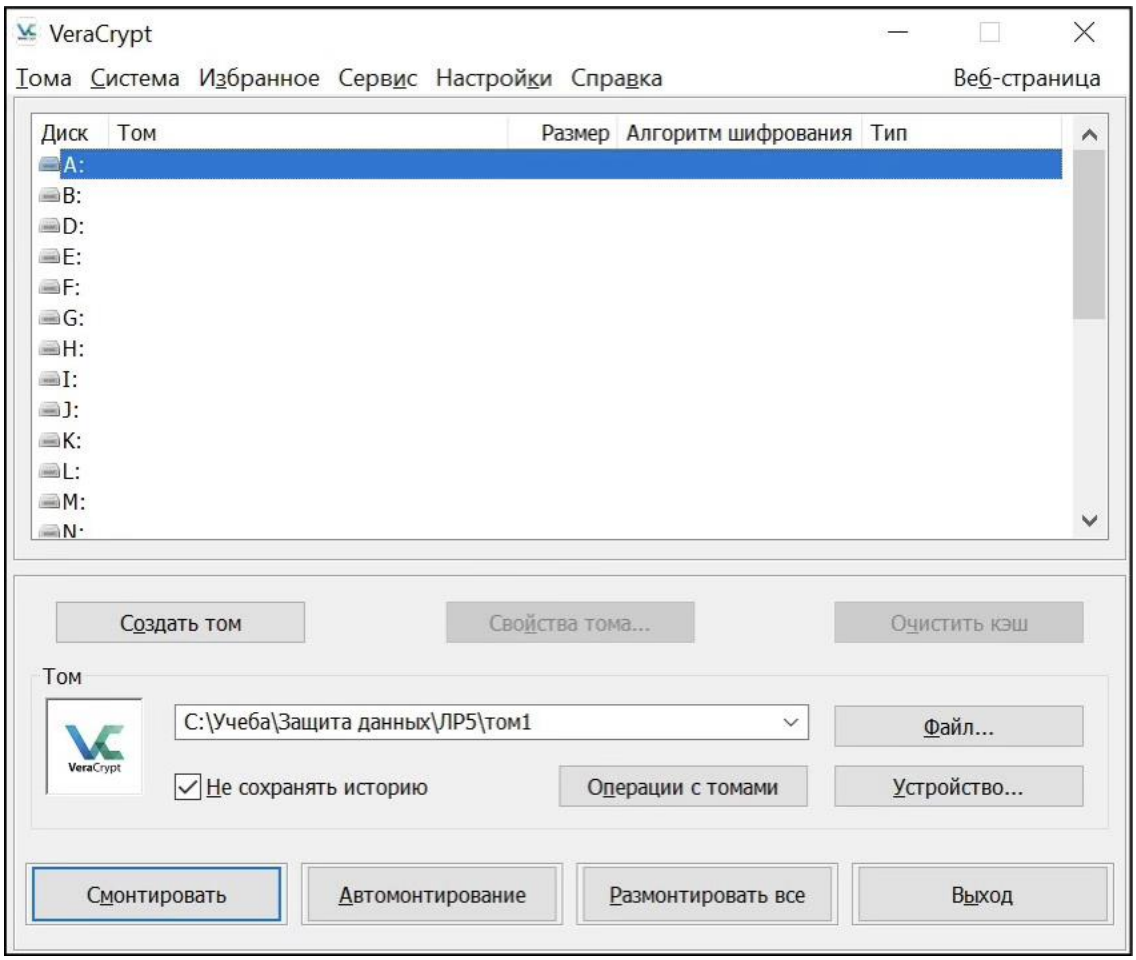


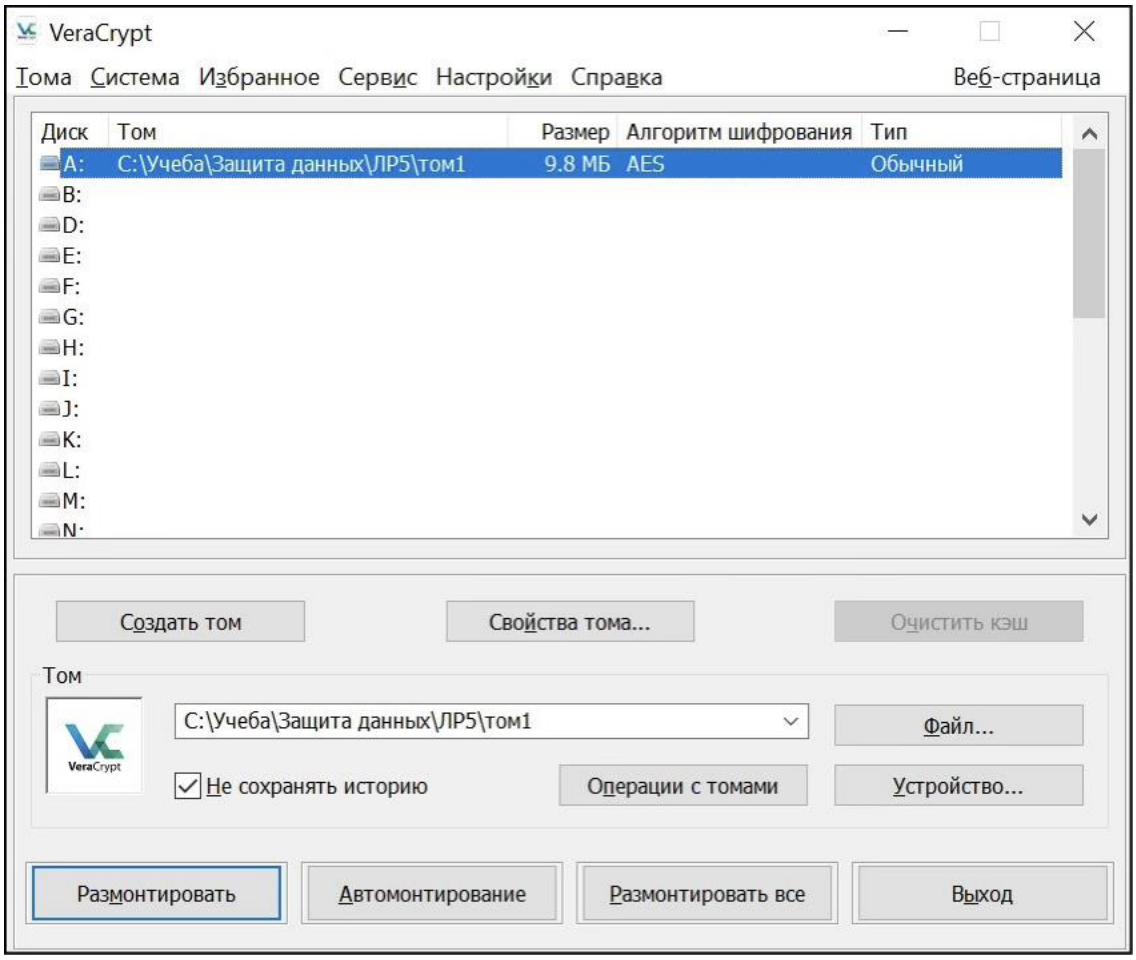
- с помощью команды «Открыть» контекстного меню имени (буквы) смонтированного тома открыть его в Проводнике, после чего добавить в него несколько файлов разного типа (один из них должен иметь имя, включающее фамилию студента);

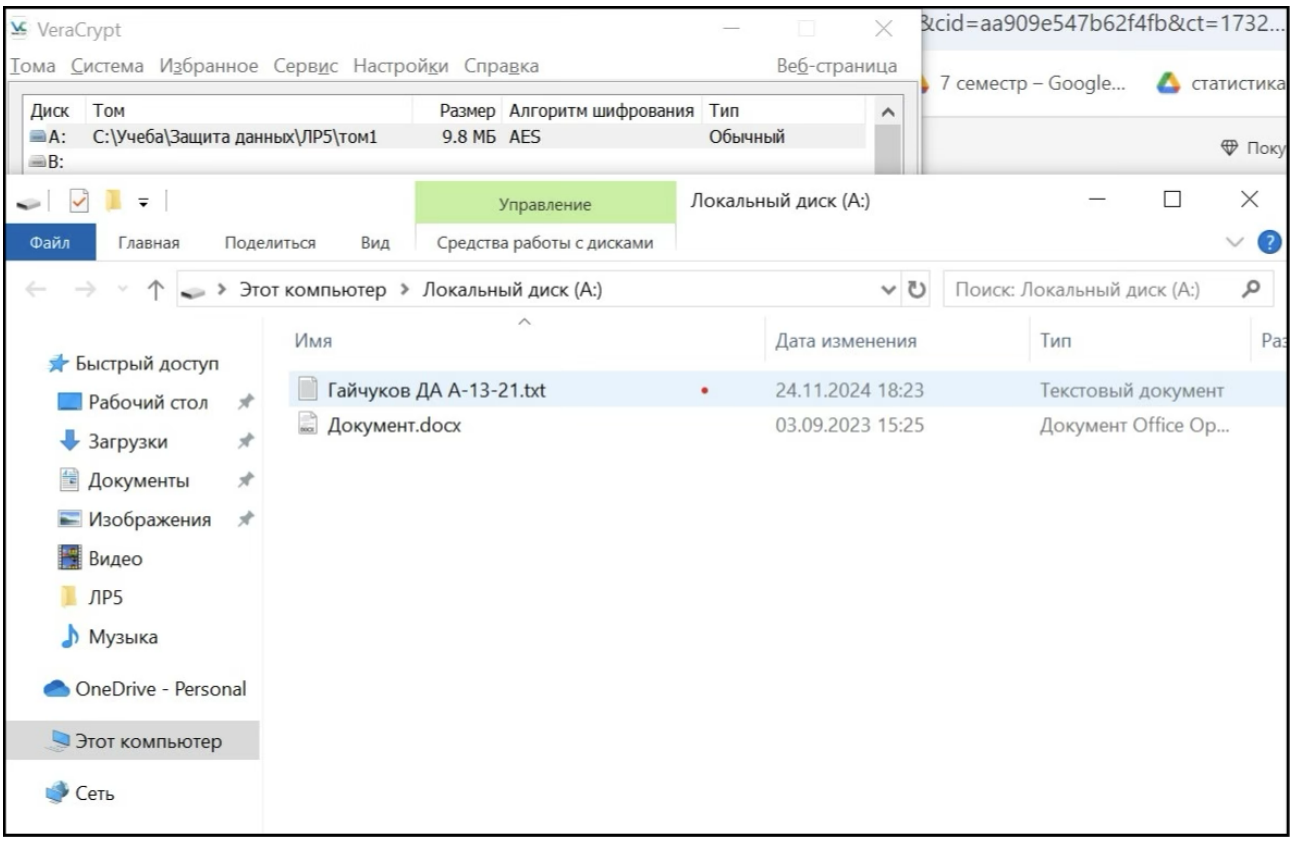




- размонтировать том с помощью соответствующей кнопки, после чего снова смонтировать и убедиться в наличии в нем добавленных ранее файлов.


VeraCrypt
Тома Система Избранное Сервис Настройки Справка Веб-страница
Диск Том Размер Алгоритм шифрования Тип
A:
B:
D:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
Создать том
Свойства тома...
Очистить кэш
Том
C:\Учеба\Защита данных\ЛР5\том1
Файл...
Не сохранять историю
Операции с томами
Устройство...
Смонтировать
Автомонтирование
Размонтировать все
Выход


VeraCrypt
Тома Система Избранное Сервис Настройки Справка Веб-страница
Диск Том Размер Алгоритм шифрования Тип
A: C:\Учеба\Защита данных\ЛР5\том1 9.8 МБ AES Обычный
B:
D:
E:
F:
G:
H:
I:
J:
K:
L:
M:
N:
Создать том
Свойства тома...
Очистить кэш
Том
C:\Учеба\Защита данных\ЛР5\том1
Файл...
Не сохранять историю
Операции с томами
Устройство...
Размонтировать
Автомонтирование
Размонтировать все
Выход



<u>При выполнении в любой операционной системе.</u>

1.4. Включить в электронную версию отчета о лабораторной работе копии экранных форм, полученных при использовании программы Citadel Safstor (VeraCrypt), после чего завершить работу с ней. Включить в отчет ответы на вопросы:

- какие криптоалгоритмы реализованы в использованной программе (назвать имя и тип алгоритмов);
  AES – симметричный (блочный)
  Serpent – симметричный (блочный)
  Twofish – симметричный (блочный)
  Camelia – симметричный (блочный)
  Kuznyechik – симметричный (блочный)
  AES(Twofish) – Каскадное (последовательное)
  AES(Twofish(Serpent) – Каскадное (последовательное)
  Serpent(AES) – Каскадное (последовательное)
  Serpent(Twofish(AES)) – Каскадное (последовательное)
  Twofish (Serpent)– Каскадное (последовательное)

- как генерируется и сохраняется ключ шифрования файла;

Ключ шифрования файла в программе VeraCrypt генерируется при создании нового зашифрованного тома или контейнера. Пользователь может выбрать различные методы генерации ключа, такие как пароль, ключевой файл или комбинация обоих. После выбора метода генерации ключа, пользователю необходимо ввести или создать соответствующий пароль или ключевой файл.

После этого ключ шифрования сохраняется в зашифрованном томе или контейнере, который затем может быть сохранен на компьютере или другом устройстве. Пользователь также может создать резервную копию ключа шифрования для безопасного хранения.

- изменяется ли (если да, то как) размер файла после шифрования;

Да, размер файла изменяется после шифрования в программе VeraCrypt. При шифровании файловой системы или контейнера VeraCrypt добавляет дополнительные данные, такие как заголовок шифрования, проверочные суммы и другую метаинформацию, что приводит к увеличению размера файла.

- возможен ли (если да, то как) совместный доступ к зашифрованному файлу);

Да, совместный доступ к зашифрованному файлу в программе VeraCrypt возможен. Для этого необходимо предоставить другим пользователям доступ к паролю или ключу шифрования, который используется для защиты файла. Также можно передавать зашифрованный файл между пользователями, предоставляя им доступ к программе VeraCrypt и необходимым ключам или паролям. Однако необходимо помнить о безопасности и контроле доступа к зашифрованным файлам, чтобы избежать утечки конфиденциальной информации.

- какие действия выполняет пользователь при установке программы.

Выбирает язык; соглашается с лицензией программы; выбирает режим (установить/извлечь); указывает место для установки программы.

2. Данный пункт выполняется 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 Свойства контекстного меню объекта, вкладка Общие, кнопка Другие, выключатель. Шифровать содержимое для защиты данных). Включить в отчет ответы на вопросы:

2.1. скрывается ли наличие в системе зашифрованных файлов и папок;

От пользователя, зашифровавший файл, зашифрованные файлы и папки не могут быть скрыты, в отличие от других пользователей.

2.2. где хранится ключ шифрования файла;

Ключ шифрования хранится в профиле пользователя и при входе в систему извлекается автоматически.

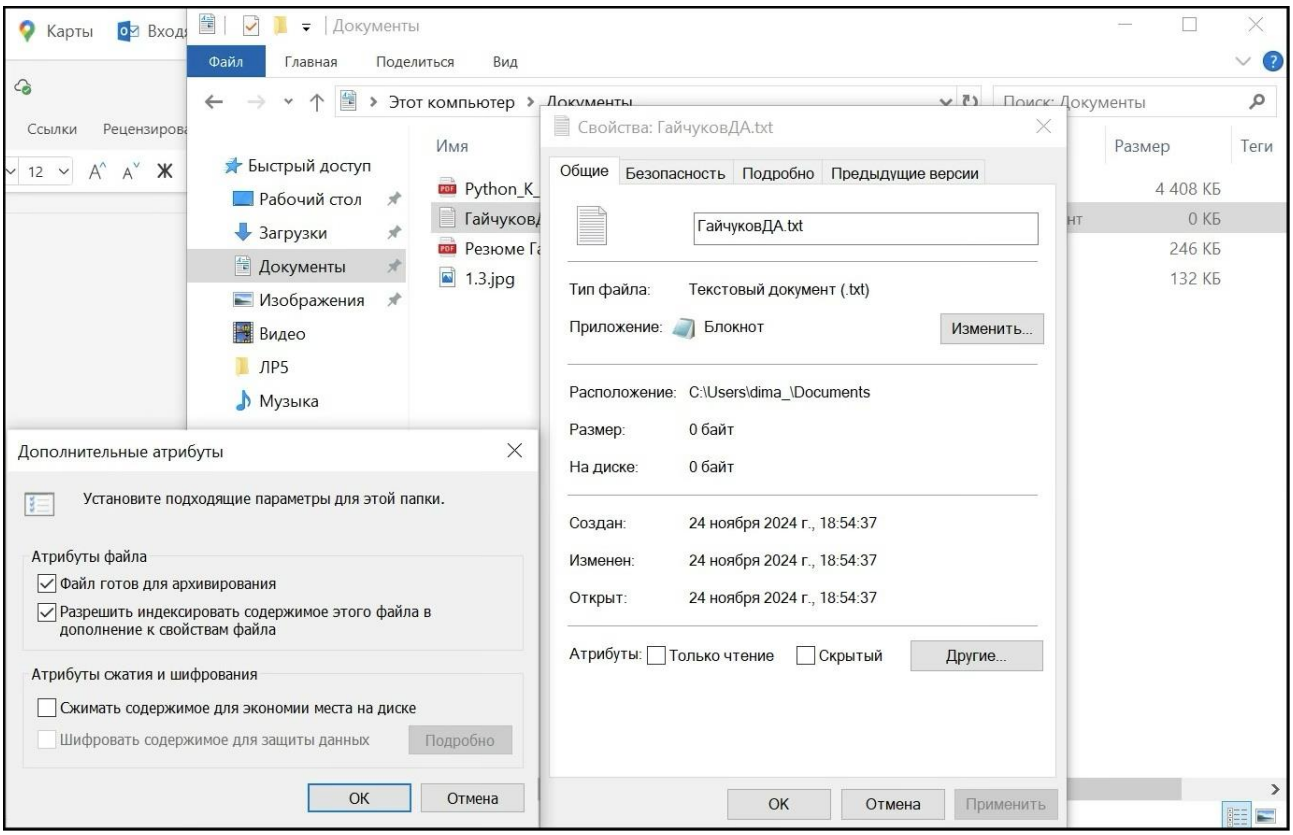
2.3. как обеспечивается в системе возможность восстановления зашифрованных файлов при невозможности входа пользователя в систему или при его отсутствии;

Возможность восстановления зашифрованных файлов определяется наличием учётных данных пользователя, который производил шифрование. При невозможности входа этого пользователя в систему или его отсутствия, восстановление может стать затруднительным.

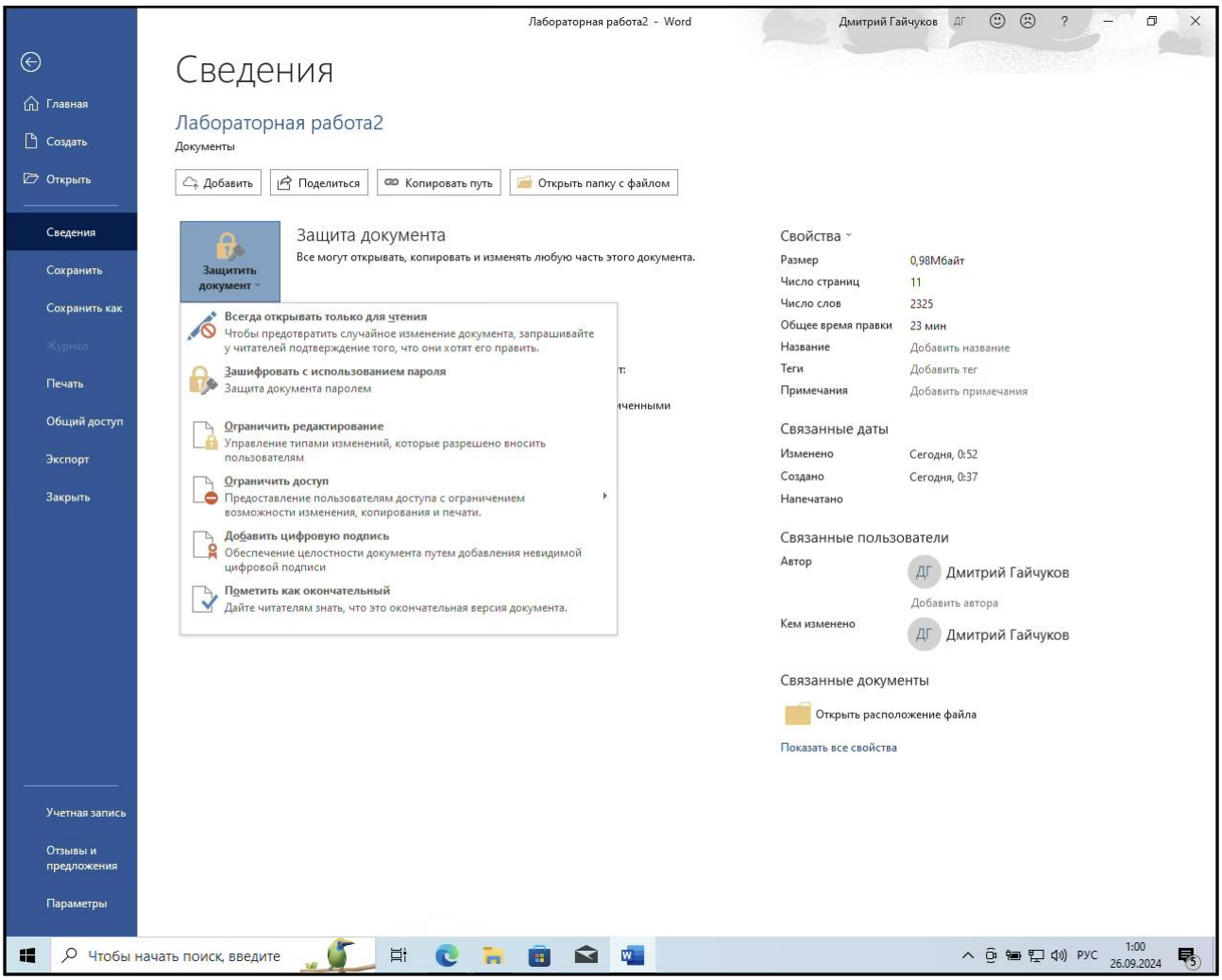
2.4. на дисках с какой файловой системой возможно использование функции шифрования файлов.

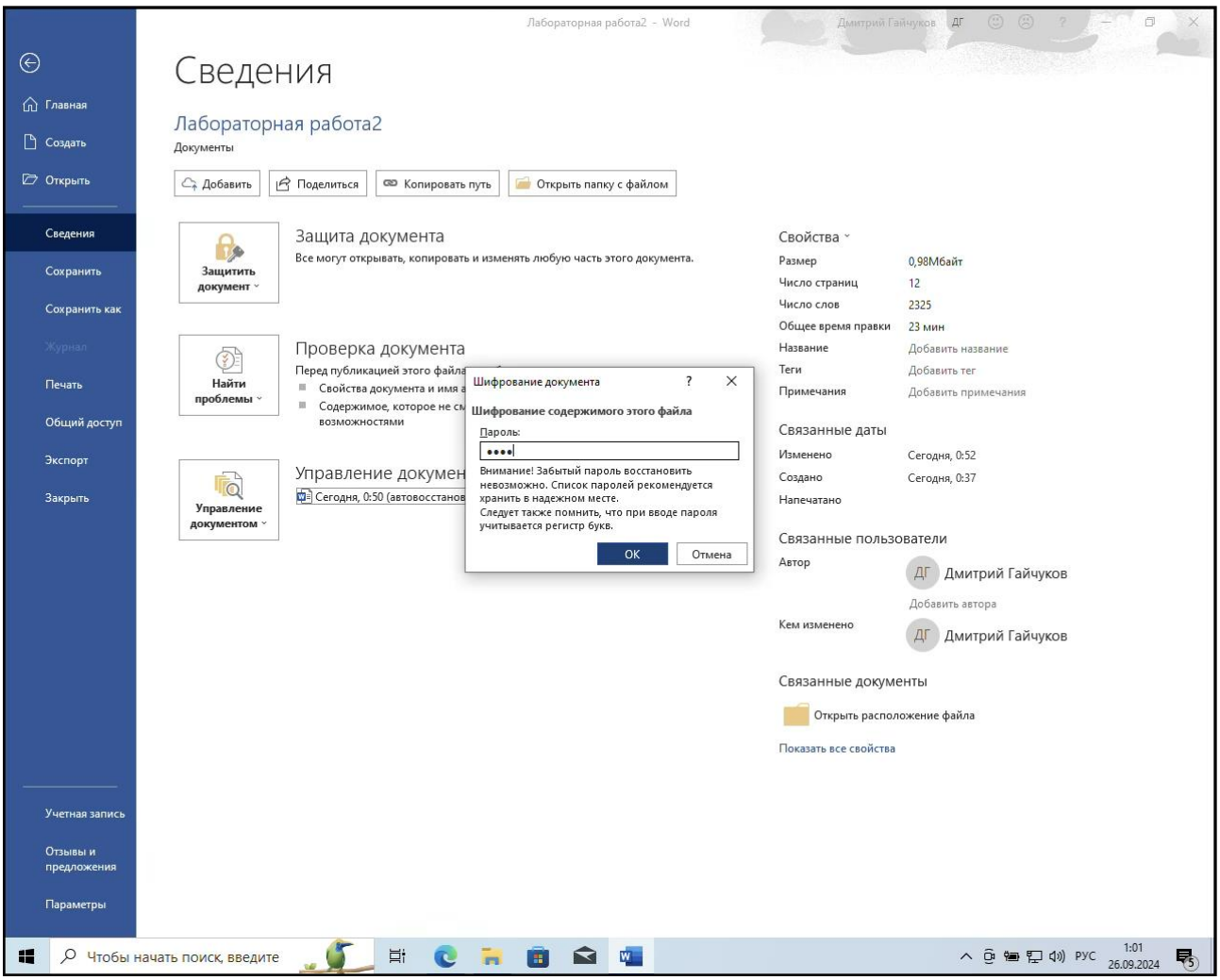
NTFS, но также и на других, например, FAT32.

2.5. Освоить средства обеспечения совместного доступа нескольких пользователей к зашифрованным файлам (с помощью кнопки Подробно окна его дополнительных атрибутов) 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.

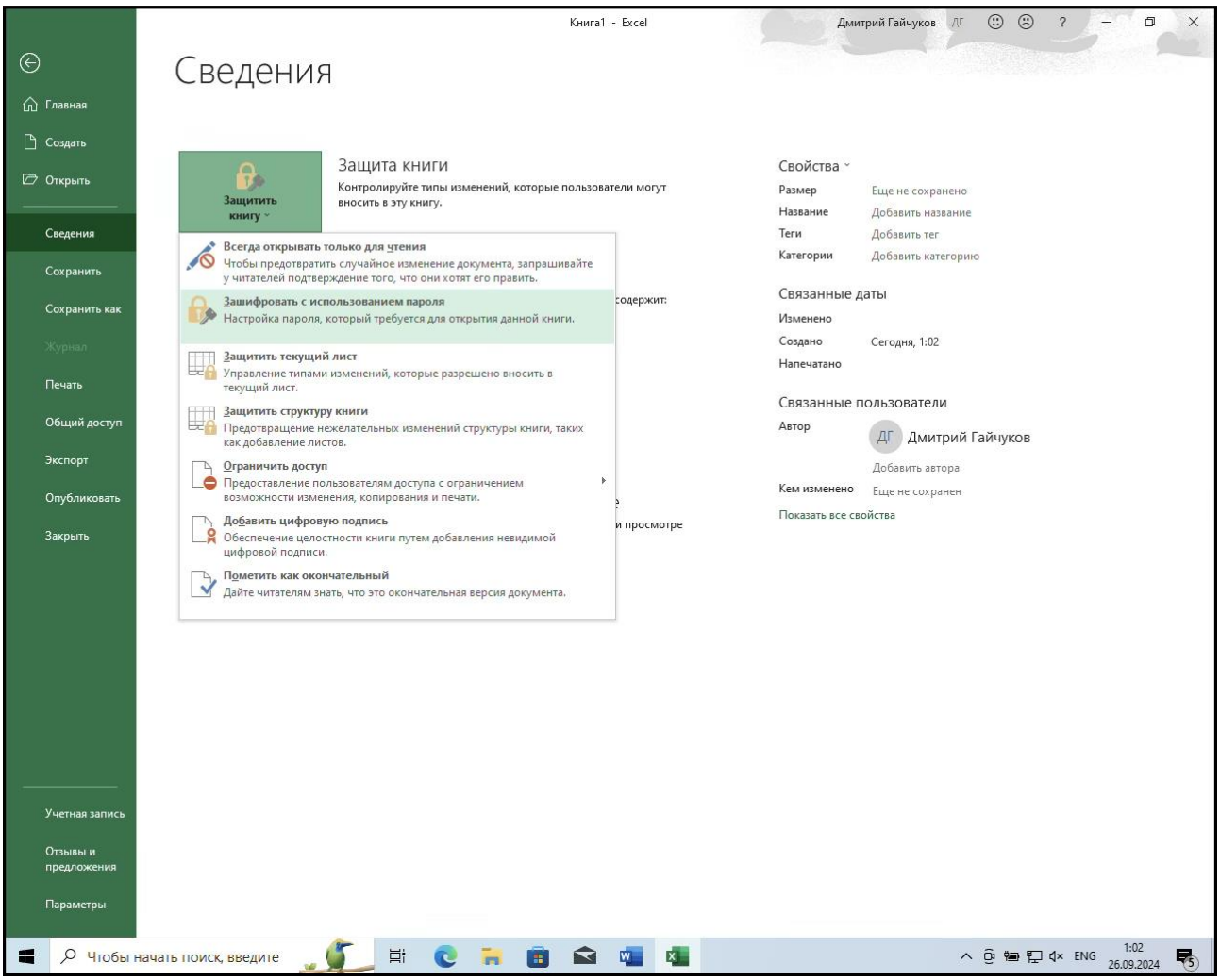


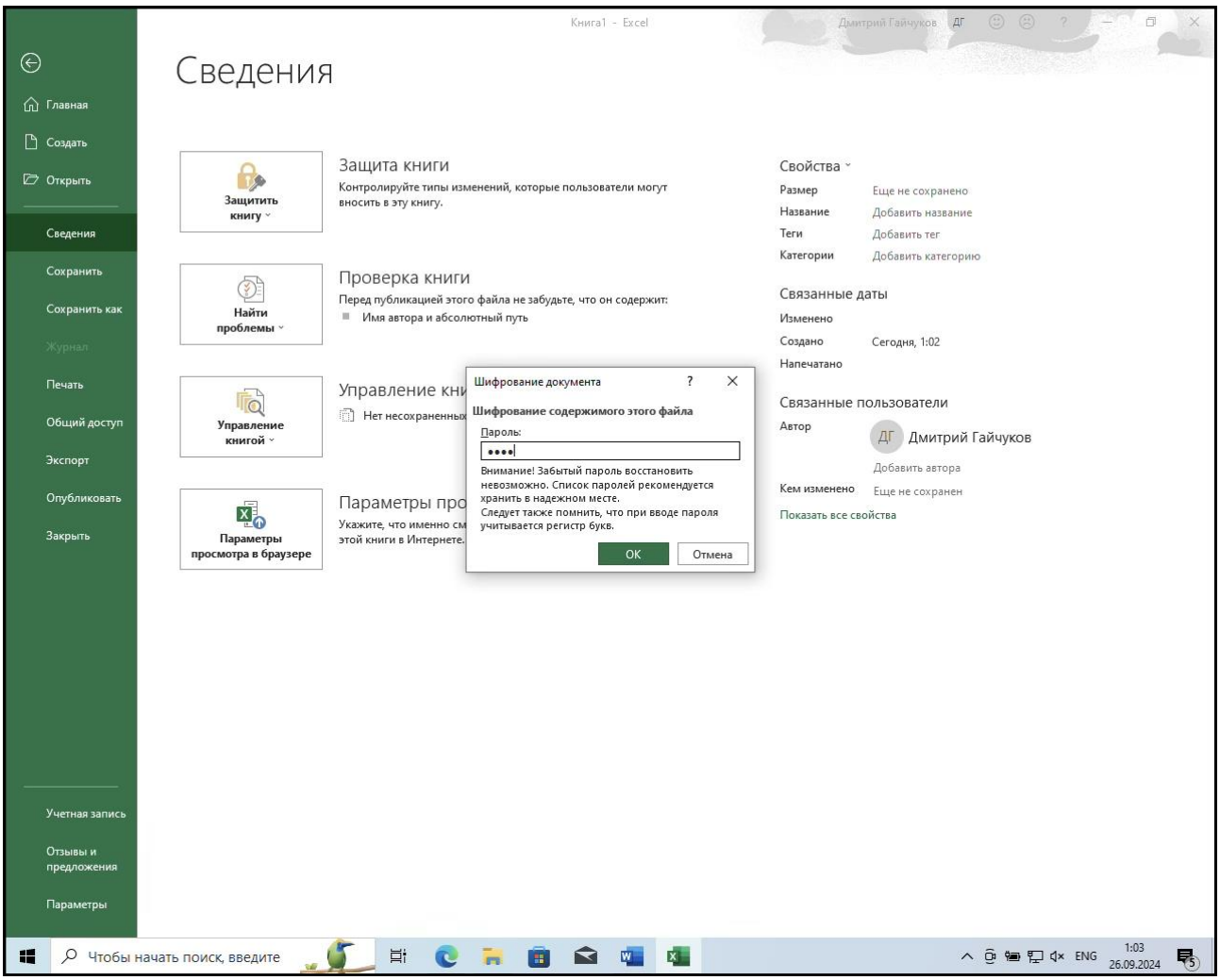
3. Начать работу с Microsoft Word из пакета Microsoft Office (версии XP или старше). Освоить средства шифрования конфиденциальных документов (команды Файл | Сведения | Защита документа | Зашифровать с использованием пароля в Office 2013, Файл | Сведения | Защитить документ | Зашифровать паролем в Office 2010, Кнопка Microsoft Office | Подготовка | Зашифровать документ в Office 2007, Сервис | Параметры | Безопасность и кнопка Дополнительно в Office 2003). Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.


Лабораторная работа2 - Word
Дмитрий Гайчуков
Сведения
Лабораторная работа2
Документы
Главная
Создать
Открыть
Сведения
Сохранить
Сохранить как
Журнал
Печать
Общий доступ
Экспорт
Закрыть
Учетная запись
Отзывы и предложения
Параметры
Добавить
Поделиться
Копировать путь
Открыть папку с файлом
Защитить документ
Защита документа
Все могут открывать, копировать и изменять любую часть этого документа.
Всегда открывать только для чтения
Чтобы предотвратить случайное изменение документа, запрашивайте у читателей подтверждение того, что они хотят его править.
Зашифровать с использованием пароля
Защита документа паролем
Ограничить редактирование
Управление типами изменений, которые разрешено вносить пользователям
Ограничить доступ
Предоставление пользователям доступа с ограничением возможности изменения, копирования и печати.
Добавить цифровую подпись
Обеспечение целостности документа путем добавления невидимой цифровой подписи
Пометить как окончательный
Дайте читателям знать, что это окончательная версия документа.
Свойства
Размер 0,98Мбайт
Число страниц 11
Число слов 2325
Общее время правки 23 мин
Название Добавить название
Теги Добавить тег
Примечания Добавить примечания
Связанные даты
Изменено Сегодня, 0:52
Создано Сегодня, 0:37
Напечатано
Связанные пользователи
Автор ДГ Дмитрий Гайчуков
Добавить автора
Кем изменено ДГ Дмитрий Гайчуков
Связанные документы
Открыть расположение файла
Показать все свойства
Чтобы начать поиск, введите
РУС
1:00
26.09.2024

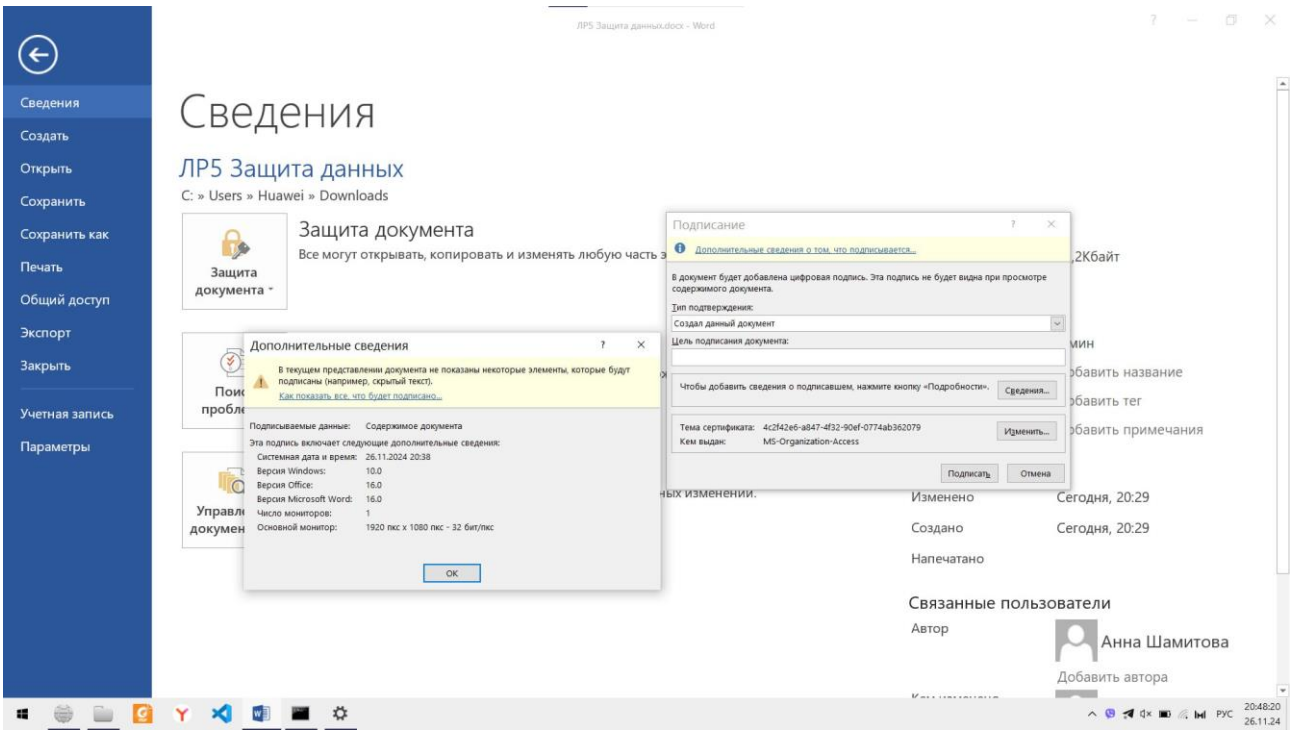


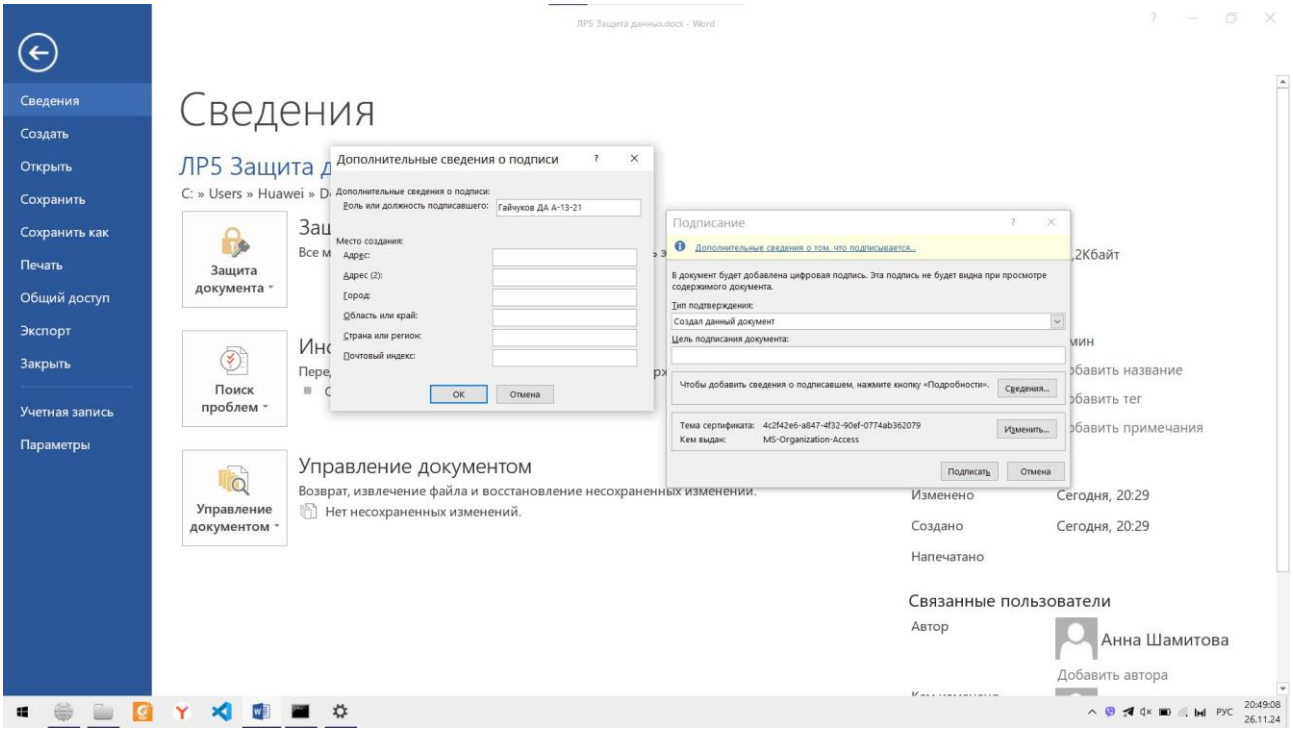
4. Повторить п. 3 для программы Microsoft Excel. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.

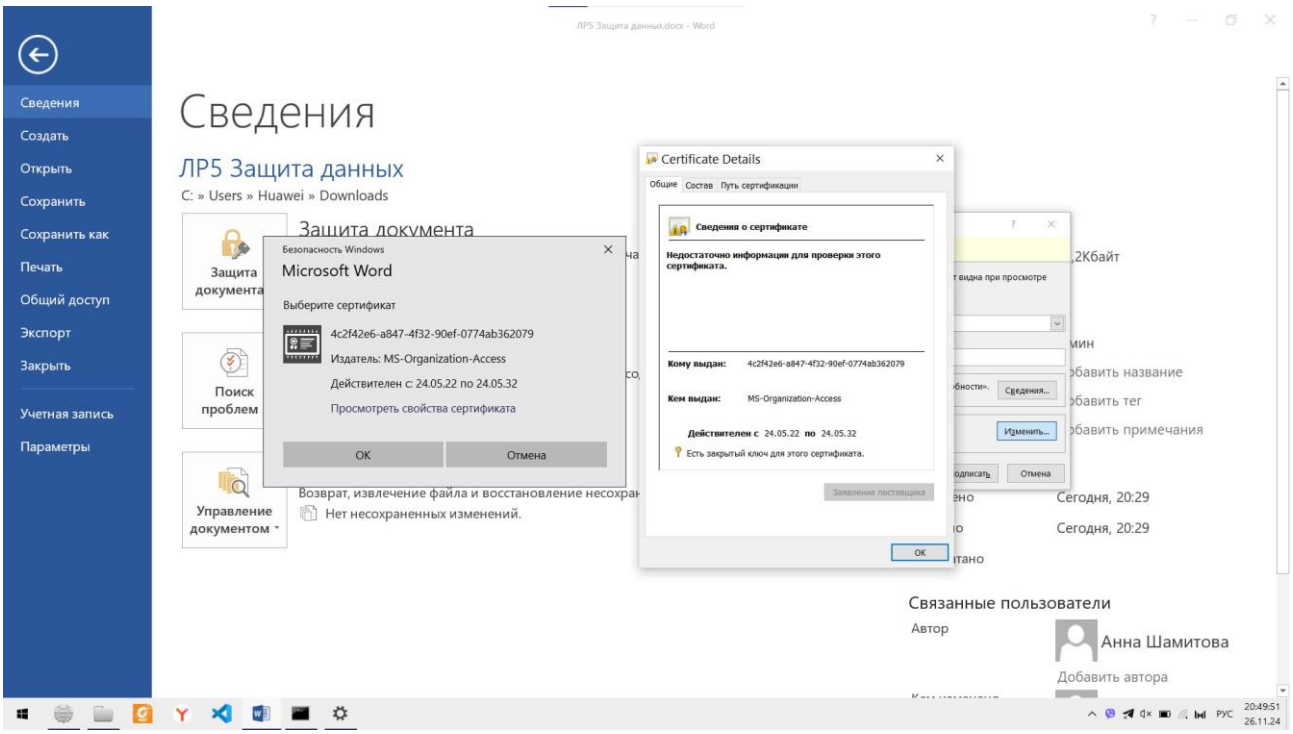

Книга1 - Excel
Дмитрий Гайчуков
Сведения
Главная
Создать
Открыть
Сведения
Сохранить
Сохранить как
Журнал
Печать
Общий доступ
Экспорт
Опубликовать
Закрыть
Учетная запись
Отзывы и предложения
Параметры
Защитить книгу
Защита книги
Контролируйте типы изменений, которые пользователи могут вносить в эту книгу.
Всегда открывать только для чтения
Чтобы предотвратить случайное изменение документа, запрашивайте у читателей подтверждение того, что они хотят его править.
Зашифровать с использованием пароля
Настройка пароля, который требуется для открытия данной книги.
Защитить текущий лист
Управление типами изменений, которые разрешено вносить в текущий лист.
Защитить структуру книги
Предотвращение нежелательных изменений структуры книги, таких как добавление листов.
Ограничить доступ
Предоставление пользователям доступа с ограничением возможности изменения, копирования и печати.
Добавить цифровую подпись
Обеспечение целостности книги путем добавления невидимой цифровой подписи.
Пометить как окончательный
Дайте читателям знать, что это окончательная версия документа.
Свойства
Размер
Еще не сохранено
Название
Добавить название
Теги
Добавить тег
Категории
Добавить категорию
Связанные даты
Изменено
Создано
Сегодня, 1:02
Напечатано
Связанные пользователи
Автор
ДГ
Дмитрий Гайчуков
Добавить автора
Кем изменено
Еще не сохранен
Показать все свойства
Чтобы начать поиск, введите
ENG
1:02
26.09.2024



5. С помощью программы selfcert.exe из пакета Microsoft Office (вызов этой программы возможен через меню Пуск | Программы | Средства Microsoft Office | Средство создания цифровых сертификатов для проектов VBA или с помощью ссылки https://disk.yandex.ru/d/0rJE5ahy_swfog) создать собственную пару ключей асимметричного шифрования и «самоподписанный» сертификат своего открытого ключа на имя, содержащее фамилию и инициалы студента. Если эта программа не установлена или создание сертификатов невозможно в соответствии с выбранной в системе политикой безопасности, 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 или с помощью ссылки https://disk.yandex.ru/d/nGm-Xlu_tuvzAw). Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.
6. Освоить средства добавления электронной подписи к документам Microsoft Office на примере программы Microsoft Word (команды Файл | Сведения | Защита документа | Добавить цифровую подпись в Office 2013, Файл | Сведения | Защитить документ | Добавить цифровую подпись в Office 2010, Кнопка Microsoft Office | Подготовка | Добавить цифровую подпись в Office 2007, Сервис | Параметры | Безопасность, кнопки Цифровые подписи и Добавить). С помощью кнопки Просмотреть свойства сертификата ознакомиться с содержанием сертификата открытого ключа. Включить в отчет ответы на вопросы:


ЛР5 Защита данных.docx - Word
Сведения
Создать
Открыть
Сохранить
Сохранить как
Печать
Общий доступ
Экспорт
Закрыть
Учетная запись
Параметры
Сведения
ЛР5 Защита данных
C: » Users » Huawei » Downloads
Защита документа
Все могут открывать, копировать и изменять любую часть э
Защита документа
Подписание
Дополнительные сведения о том, что подписывается...
В документ будет добавлена цифровая подпись. Эта подпись не будет видна при просмотре содержимого документа.
Тип подтверждения:
Создал данный документ
Цель подписания документа:
Чтобы добавить сведения о подписавшем, нажмите кнопку «Подробности».
Сведения...
Тема сертификата: 4c2f42e6-a847-4f32-90ef-0774ab362079
Кем выдан: MS-Organization-Access
Изменить...
Подписать
Отмена
Дополнительные сведения
В текущем представлении документа не показаны некоторые элементы, которые будут подписаны (например, скрытый текст).
Как показать все, что будет подписано...
Подписываемые данные: Содержимое документа
Эта подпись включает следующие дополнительные сведения:
Системная дата и время: 26.11.2024 20:38
Версия Windows: 10.0
Версия Office: 16.0
Версия Microsoft Word: 16.0
Число мониторов: 1
Основной монитор: 1920 пкс x 1080 пкс - 32 бит/пкс
OK
Управление документом
Изменено Сегодня, 20:29
Создано Сегодня, 20:29
Напечатано
Связанные пользователи
Автор
Анна Шамитова
Добавить автора
20:48:20
26.11.24


ЛР5 Защита данных.docx - Word
Сведения
Создать
Открыть
Сохранить
Сохранить как
Печать
Общий доступ
Экспорт
Закрыть
Учетная запись
Параметры
Сведения
Дополнительные сведения о подписи
Дополнительные сведения о подписи:
Роль или должность подписавшего: Гайчуков ДА А-13-21
Место создания:
Адрес:
Адрес (2):
Город:
Область или край:
Страна или регион:
Почтовый индекс:
OK
Отмена
Защита документа
Поиск проблем
Управление документом
Управление документом
Возврат, извлечение файла и восстановление несохраненных изменений.
Нет несохраненных изменений.
Подписание
Дополнительные сведения о том, что подписывается...
В документ будет добавлена цифровая подпись. Эта подпись не будет видна при просмотре содержимого документа.
Тип подтверждения:
Создал данный документ
Цель подписания документа:
Чтобы добавить сведения о подписавшем, нажмите кнопку «Подробности».
Сведения...
Тема сертификата: 4c2f42e6-a847-4f32-90ef-0774ab362079
Кем выдан: MS-Organization-Access
Изменить...
Подписать
Отмена
Изменено Сегодня, 20:29
Создано Сегодня, 20:29
Напечатано
Связанные пользователи
Автор
Анна Шамитова
Добавить автора
20:49:08
26.11.24

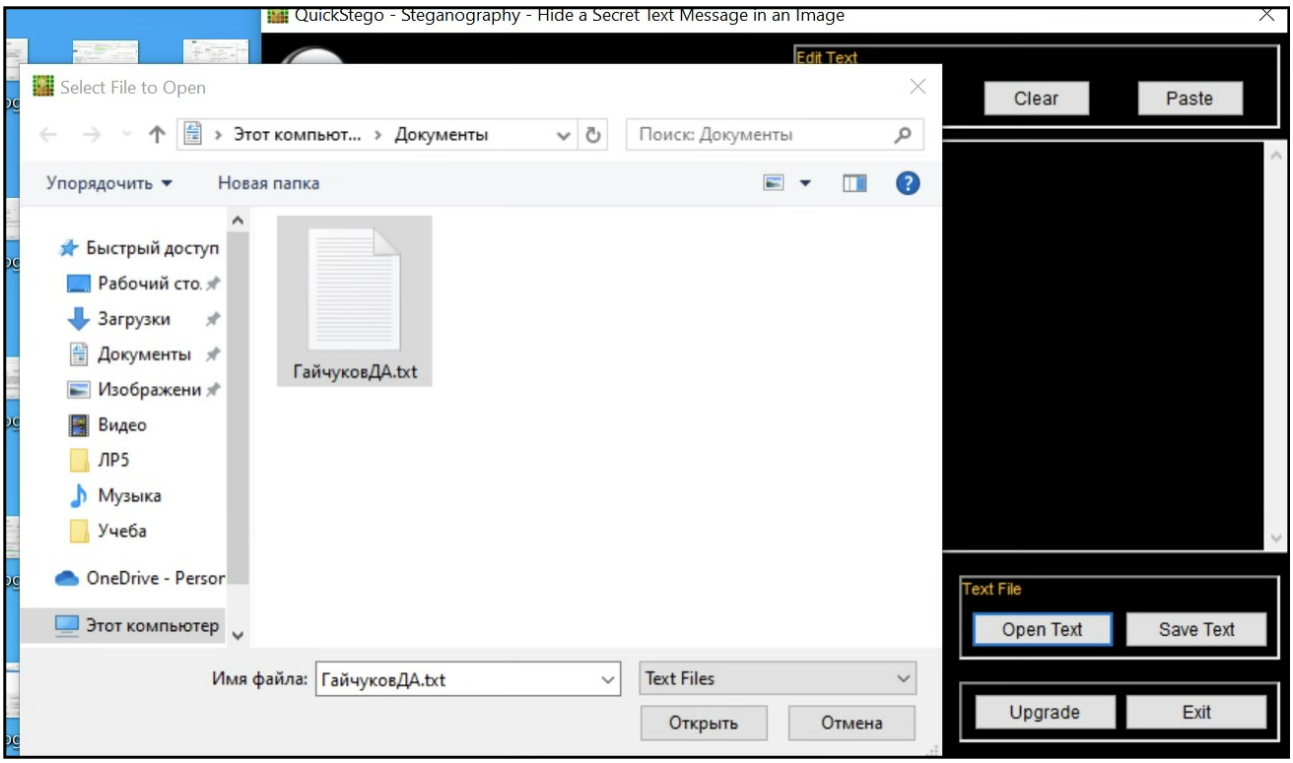


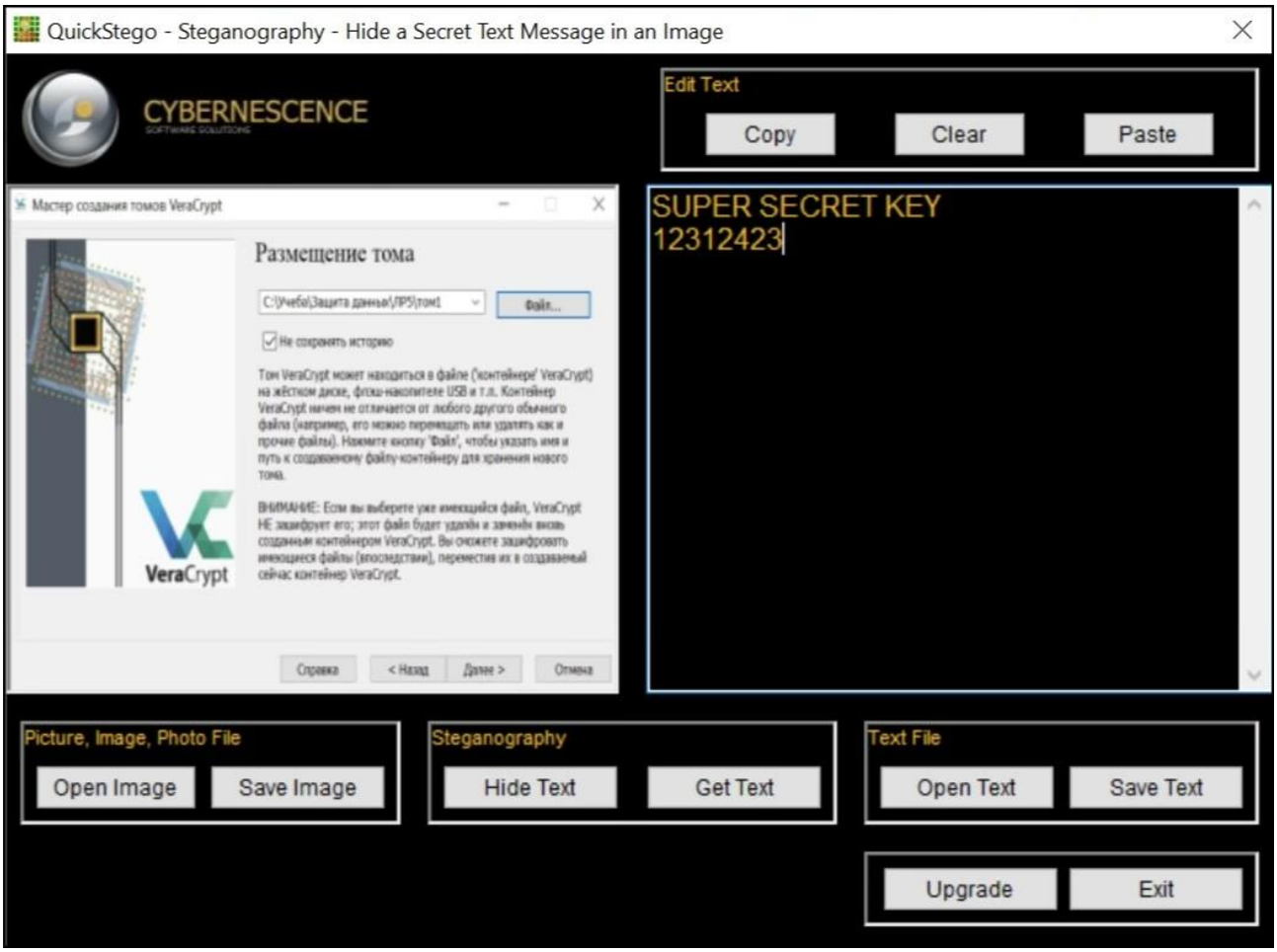
6.1. какая информация содержится в сертификате открытого ключа;
Имя владельца сертификата.
Публичный ключ владельца.
Информация о центре сертификации.
Срок действия сертификата.
Идентификатор сертификата и т.д.

6.2. что такое путь сертификации.
Это последовательность центров сертификации, подписывающих друг друга, вплоть до корневого центра.
Используется для проверки подлинности сертификата.

6.3. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.

7. Скопировать в произвольную папку на локальном жестком диске файл QS12Setup.zip.
   7.1. Если программа QuickStego не установлена (отсутствует соответствующий пункт в главном меню), то запустить программу QS12Setup.exe для установки стеганографической программы QuickStego.
   7.2. Запустить стеганографическую программу QuickStego. С произвольными файлами контейнеров (изображений) и сообщений (текстовых файлов, которые можно выбирать или создавать непосредственно в окне программы) изучить функции программы и включить в электронную версию отчета копии экранных форм, полученных при использовании этой программы, после чего завершить работу с ней.





<u>При выполнении в любой операционной системе.</u>

7.3. Включить в отчет ответы на вопросы:

- как происходит скрытие и извлечение сообщений из контейнеров;

Самым простым и распространенным методом стеганографического скрытия является LSB, в

Котором скрываемое сообщение заменяет младшие биты оттенков точек изображения. Такой метод в чистом виде сейчас практически не используется, т.к. его слабой стороной является незащищенность и доступность сообщения, позволяющие без труда получить и изменить скрытое сообщение любому человеку. Существует достаточно способов, так или иначе использующих идеи LSB, но значительно затрудняющих обнаружение факта передачи скрытой информации.

- в чем разница между методами криптографии и стеганографии;

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо или судоку. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

- каким должно быть соотношение между размерами файла-контейнера и файла-сообщения при использовании программы contrab.exe (QuickStego) и почему.

Соотношение между размерами файла-контейнера и файла-сообщения при использовании программы contrab.exe (QuickStego) должно быть таким, чтобы файл-сообщение можно было полностью вместить в файл-контейнер. Это означает, что размер файла-контейнера должен быть больше или равен размеру файла-сообщения. Если размер файла-контейнера меньше размера файла-сообщения, то сообщение не сможет быть полностью скрыто в контейнере, что может привести к потере данных или искажению сообщения.
Поэтому важно выбирать файл-контейнер достаточного размера, чтобы вместить в него весь файл-сообщение.

8. 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
8.1. сведения о назначении и основных функциях программы, а также ответы на вопросы:
Функции:
   - В антивирусе присутствует: антивирусный сканер и антивирусный монитор
   - Защита персональных данных
   - Защита электронной почты
   - Система обнаружения и предотвращения угроз
   - Система обновлений
   - Веб-защита

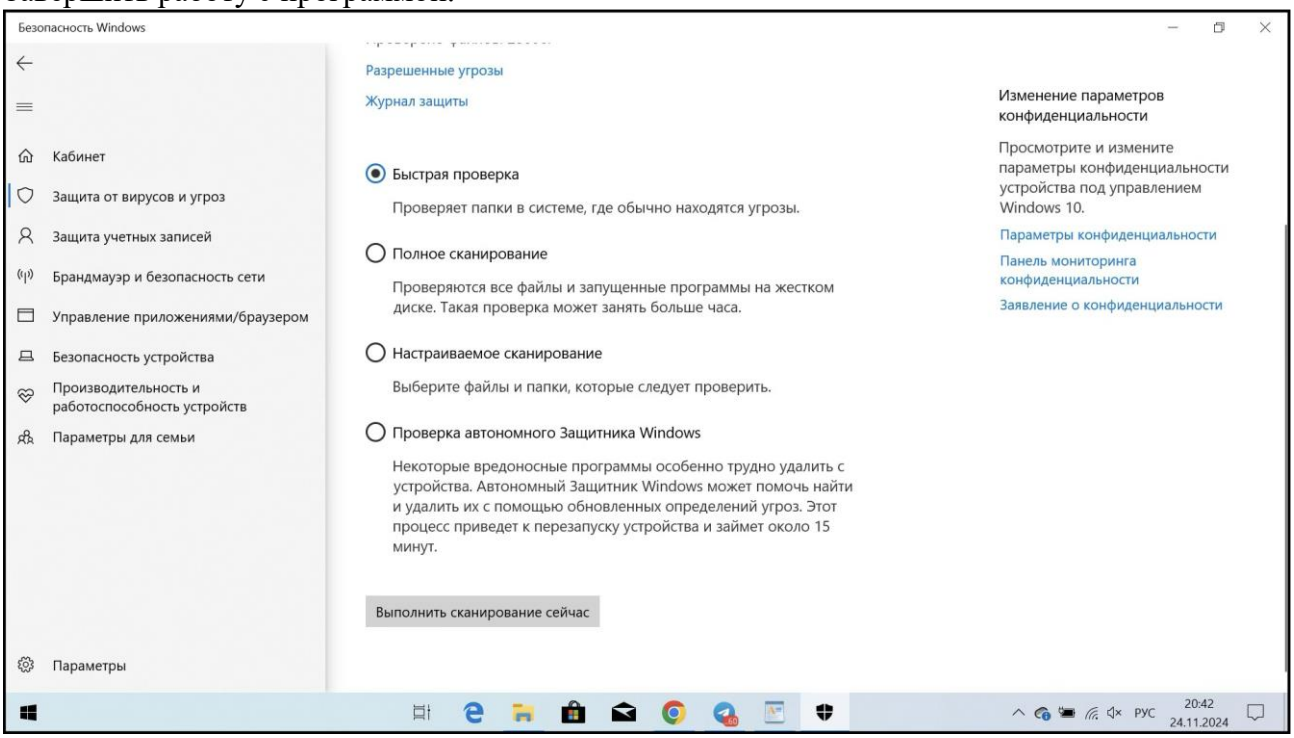
8.2. как задаются области сканирования (диски, папки и т.п.);
В антивирусе области сканирования (диски, папки и т.п.) задаются через настройки сканирования. Обычно пользователь может выбрать конкретные диски, папки или файлы для сканирования, а также настроить расписание сканирования и типы файлов, которые нужно сканировать. Также можно задать исключения для определенных файлов или папок, которые не нужно сканировать.
Для задания областей сканирования в антивирусе обычно используется графический интерфейс пользователя, где доступны различные опции и настройки сканирования.

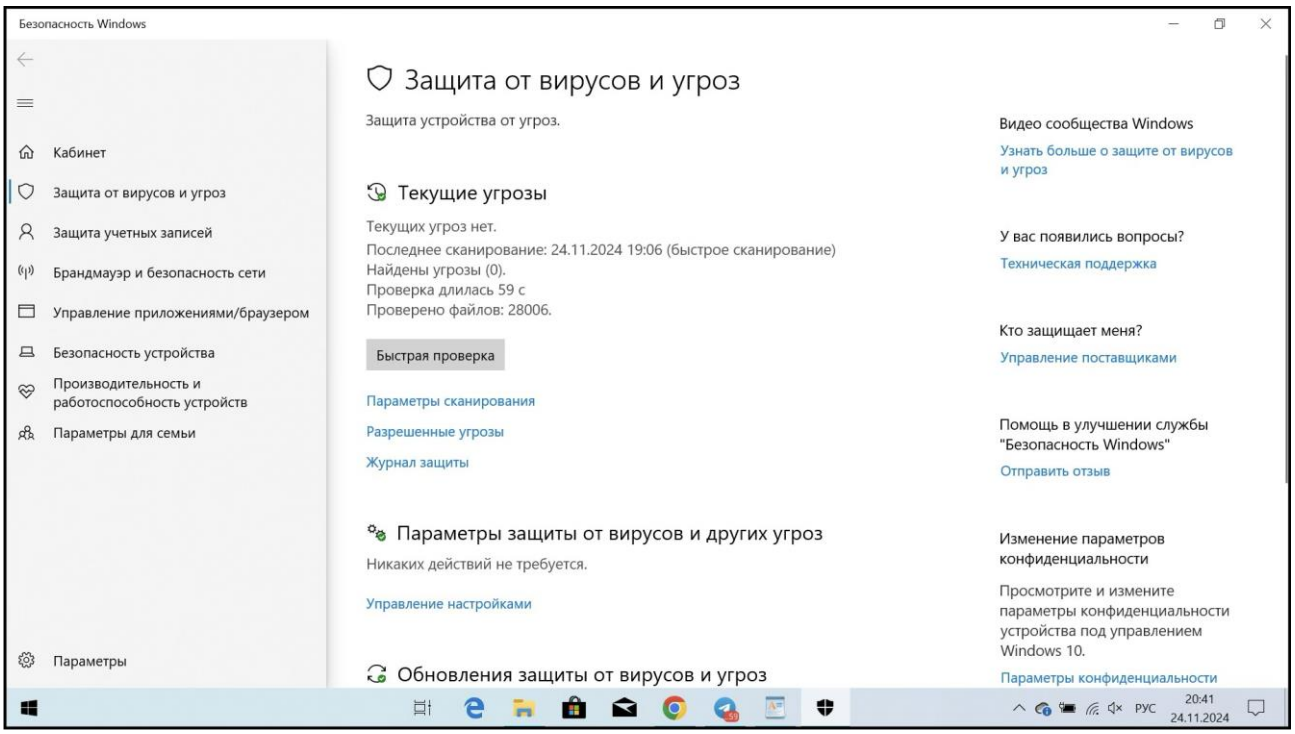
8.3. как задаются объекты проверки на наличие вирусов (типы (расширения имен) сканируемых файлов);
Для задания объектов проверки на наличие вирусов в антивирусе обычно используется меню настроек сканирования. Пользователь может выбрать типы файлов, которые нужно сканировать, например, исполняемые файлы, документы, архивы и т.д. Также

можно указать конкретные расширения файлов, которые следует сканировать или исключить из сканирования. Например, пользователь может задать сканирование только файлов с расширением .exe, .docx, .pdf и т.д. Такие настройки позволяют пользователю более гибко управлять процессом сканирования и оптимизировать его для конкретных нужд и требований.

8.4. как определяется реакция сканера в случае обнаружения зараженного файла. Когда сканер антивируса обнаруживает зараженный файл, он обычно предлагает пользователю несколько вариантов действий. Эти варианты могут включать в себя удаление зараженного файла, помещение его в карантин, а также возможность попытки восстановления файла, если это возможно. Пользователь может выбрать подходящий вариант действий в зависимости от своих предпочтений и уровня угрозы, представленной зараженным файлом.

Завершить работу с программой.





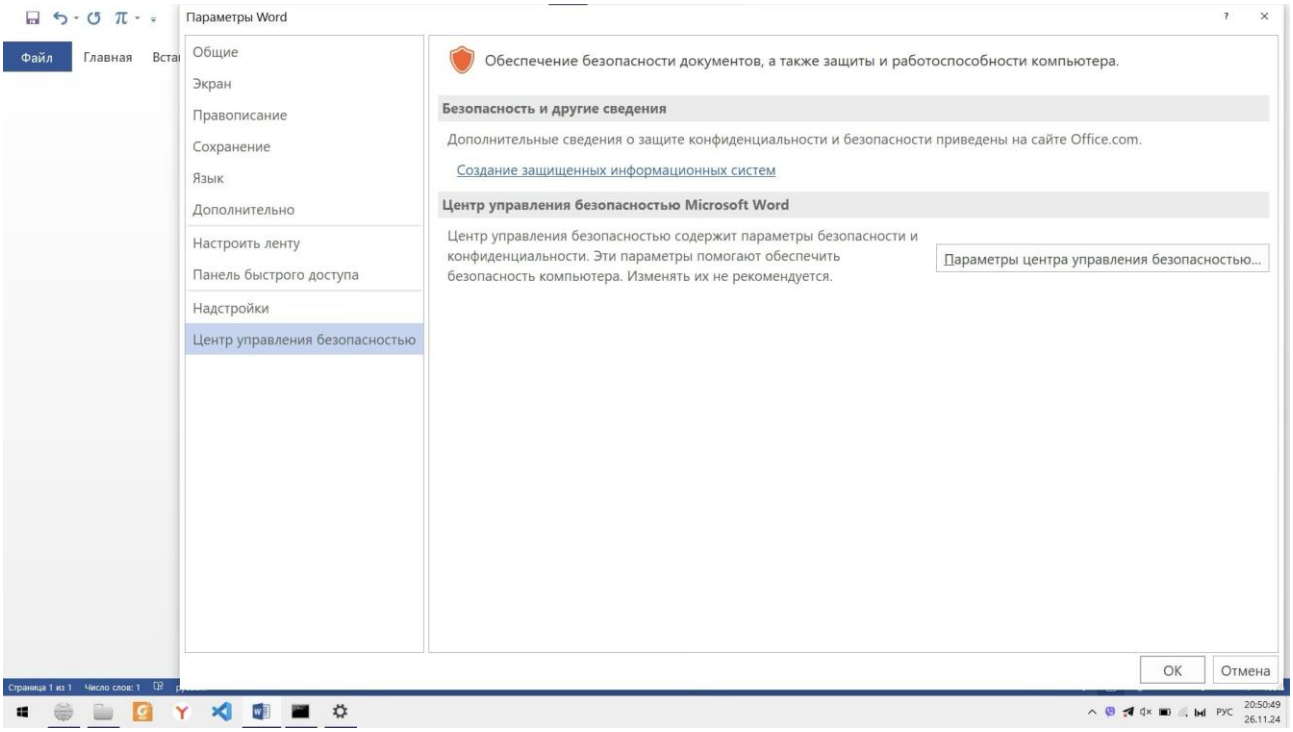
9. Начать работу с Microsoft Word. Включить средства защиты от вирусов в макросах в документах Word (команды Файл или кнопка Microsoft Office | Параметры | Центр управления безопасностью | Параметры центра правления безопасностью | Параметры макросов в Office 2013, 2010 или 2007, Сервис | Параметры | Безопасность в Office 2003). Завершить работу с Word.

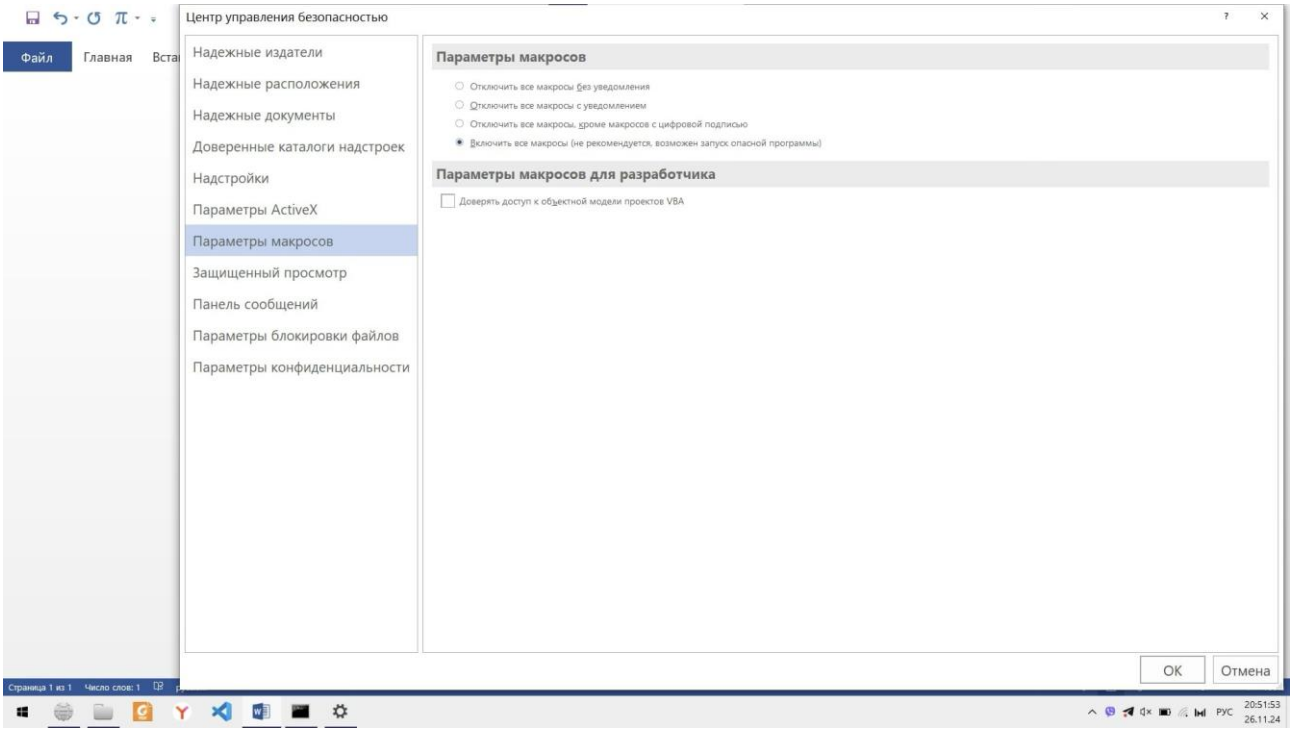
9.1. Включить в отчет сведения о способах защиты от вредоносных макросов в документах Word.

Основной функционал внутри Word представлен на оконной форме, однако вот дополнительная информация о способах защиты от вредоносных макросов в документах Word:

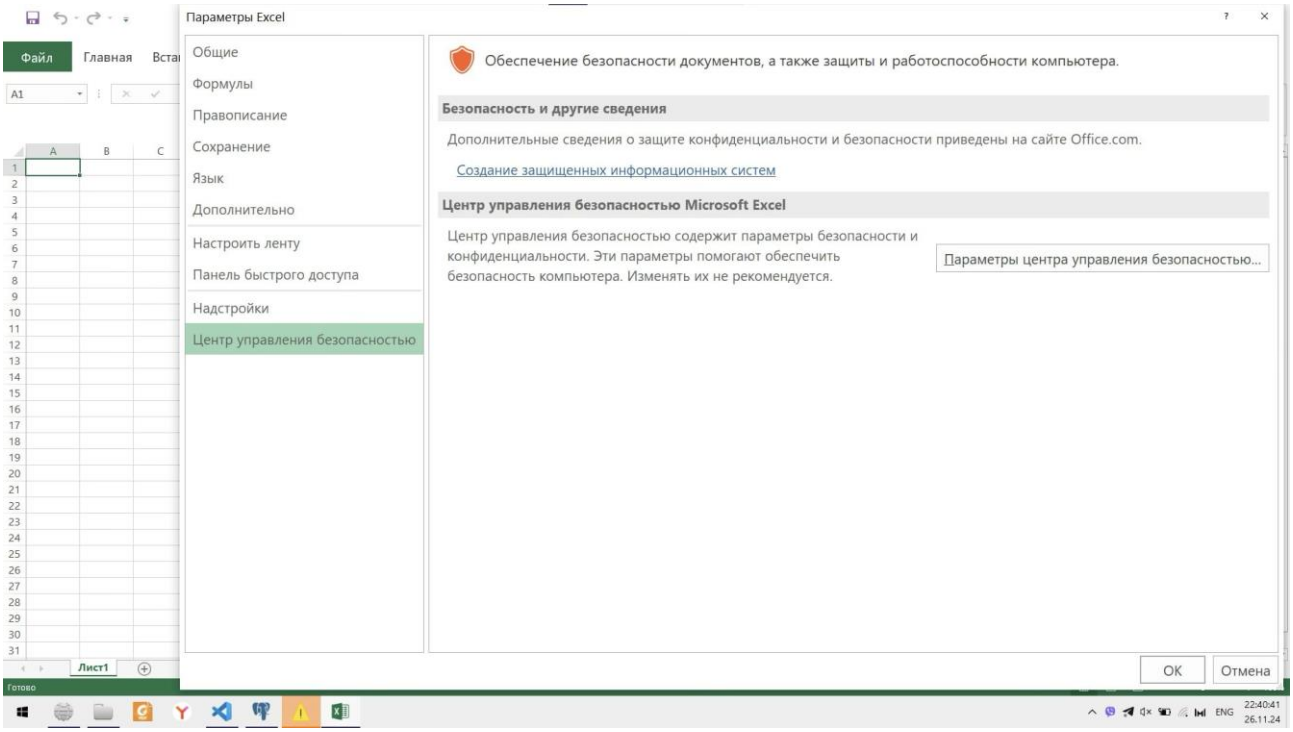
1. Включение защиты от макросов в настройках Microsoft Word. Это позволит предотвратить выполнение вредоносных макросов при открытии документов.
2. Обновление антивирусного программного обеспечения и регулярное сканирование документов Word перед их открытием.
3. Осторожность при открытии вложений в электронных письмах и загрузке файлов из интернета, особенно если они поступают из ненадежных источников.
4. Использование дополнительных инструментов для защиты от вредоносных макросов, таких как антивирусные программы с функцией обнаружения и блокировки макросов.
5. Обучение пользователей о возможных угрозах, связанных с вредоносными макросами, и о том, как избегать их использования или активации.

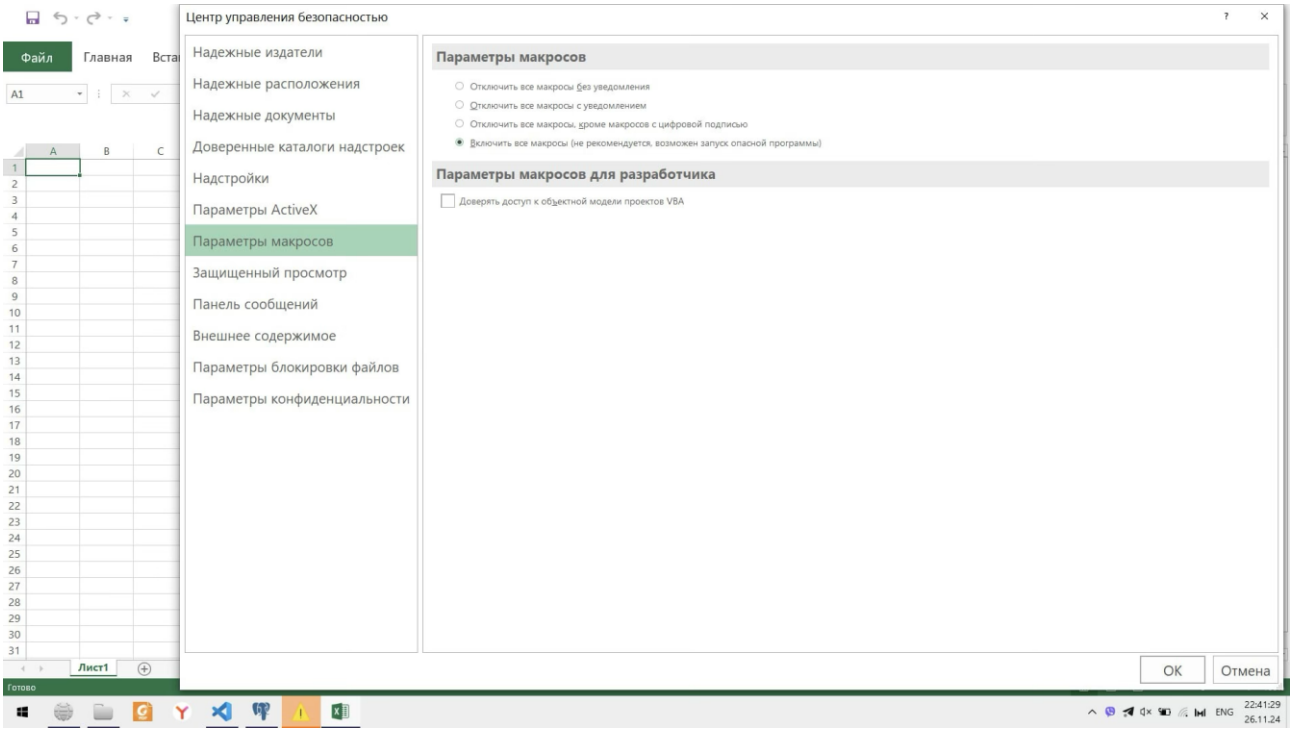
9.2. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.



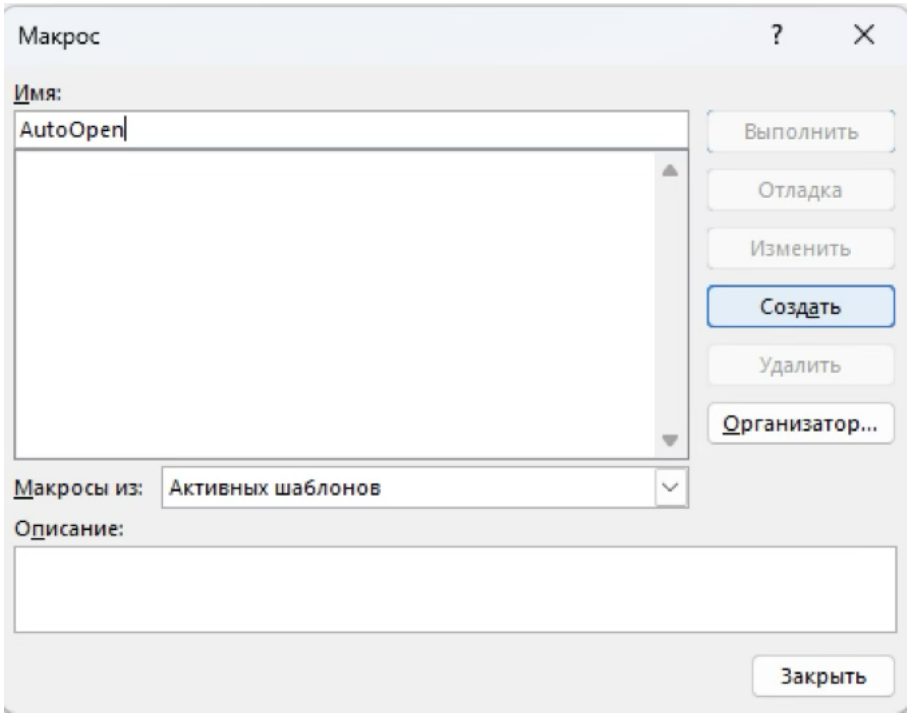


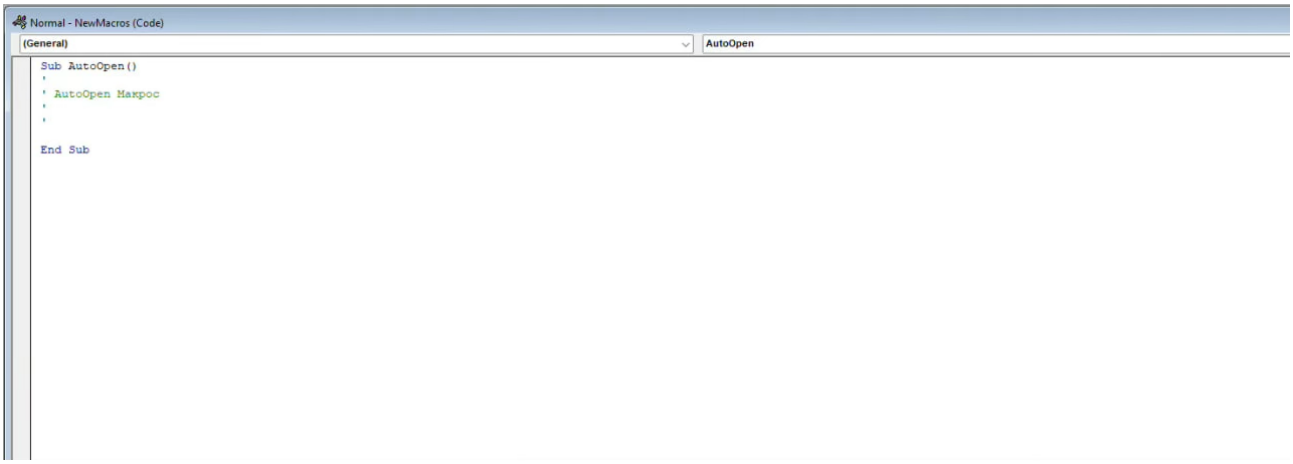
10. Повторить п. 9 для программы Microsoft Excel. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.

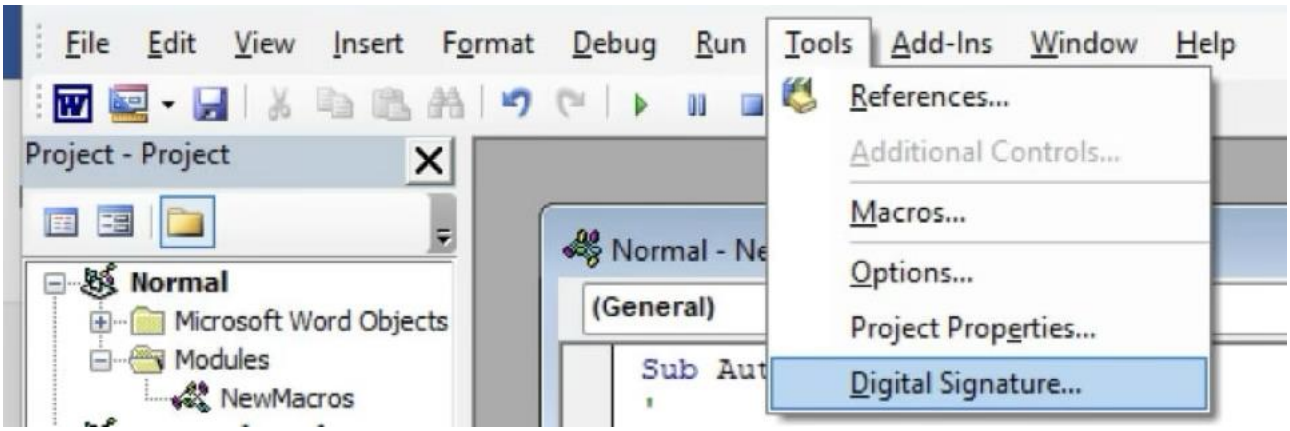


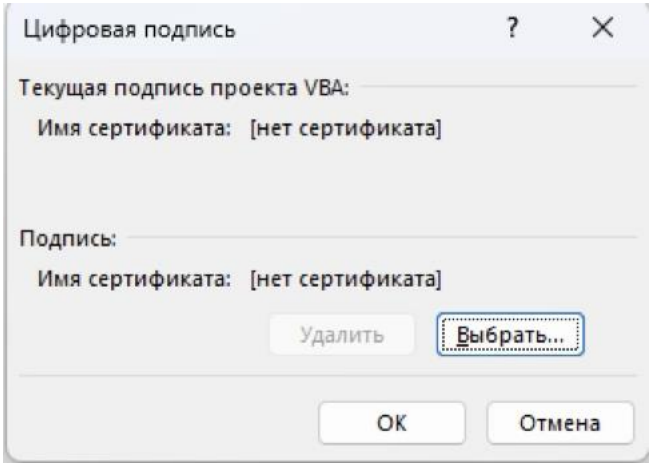


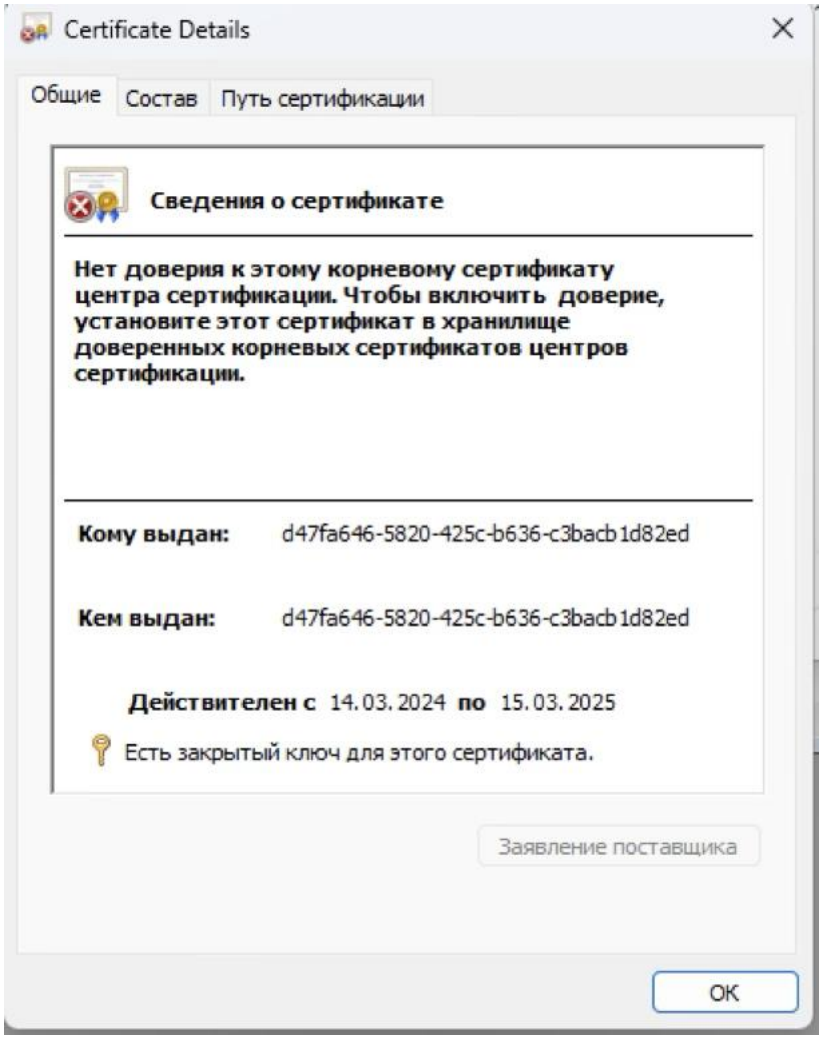
11. Освоить средства добавления электронной подписи к макросам, включаемым в состав документов Microsoft Office (на примере программы Microsoft Word): добавить в документ автоматически выполняющийся при его открытии макрос (команды Вид | Макросы | Макросы в Office 2013, 2010 и 2007, Сервис | Макрос | Макросы в Office 2003) с именем AutoOpen и воспользоваться командой Редактора Visual Basic for Application Tools | Digital Signature. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.

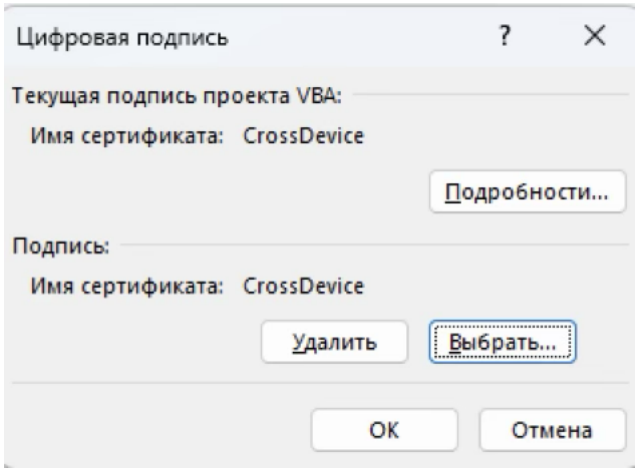

Макрос
Имя:
AutoOpen
Выполнить
Отладка
Изменить
Создать
Удалить
Организатор...
Макросы из:
Активных шаблонов
Описание:
Закрыть


Normal - NewMacros (Code)
(General)
AutoOpen
Sub AutoOpen()
' AutoOpen Макрос
End Sub


File
Edit
View
Insert
Format
Debug
Run
Tools
Add-Ins
Window
Help
References...
Additional Controls...
Macros...
Options...
Project Properties...
Digital Signature...
Project - Project
Normal
Microsoft Word Objects
Modules
NewMacros
(General)


Цифровая подпись
Текущая подпись проекта VBA:
Имя сертификата: [нет сертификата]
Подпись:
Имя сертификата: [нет сертификата]
Удалить
Выбрать...
OK
Отмена


Certificate Details
Общие
Состав
Путь сертификации
Сведения о сертификате
Нет доверия к этому корневому сертификату центра сертификации. Чтобы включить доверие, установите этот сертификат в хранилище доверенных корневых сертификатов центров сертификации.
Кому выдан: d47fa646-5820-425c-b636-c3bacb1d82ed
Кем выдан: d47fa646-5820-425c-b636-c3bacb1d82ed
Действителен с 14.03.2024 по 15.03.2025
Есть закрытый ключ для этого сертификата.
Заявление поставщика
OK



12. Включить в отчет титульный лист и сохранить файл с электронной версией отчета.
13. Предъявить преподавателю электронную версию отчета о лабораторной работе с копиями использовавшихся экранных форм и соответствующими им номерами пунктов задания.
14. После проверки электронной версии отчета о выполнении лабораторной работы преподавателем удалить файл с отчетом о лабораторной работе. Удалить программы Citadel Safstor (VeraCrypt) и Contraband (QuickStego) с помощью Панели управления Windows.
15. Включить в отчет ответы на контрольные вопросы, номера которых выбираются в соответствии с номером варианта и прилагаемой ниже таблицей.
16. Предъявить преподавателю для защиты лабораторной работы отчет на твердом носителе, содержащий
    - титульный лист,
    - сведения, полученные при выполнении работы, и ответы на общие вопросы с указанием пунктов задания, в которых они содержатся;
    - ответы на контрольные вопросы.

Контрольные вопросы

1. В чем разница между симметричной и асимметричной криптографией?

Основное различие между симметричной и асимметричной криптографией заключается в том, как используются ключи для шифрования и расшифровки данных:

Симметричная криптография:

• Один ключ: использует один и тот же секретный ключ как для шифрования, так и для расшифровки данных. Представьте себе замок с одним ключом: тот, кто имеет ключ, может как закрыть, так и открыть замок.
• Быстрая: гораздо быстрее асимметричной криптографии. Это делает её подходящей для шифрования больших объемов данных.
• Проблема распределения ключей: Основной недостаток – безопасная передача ключа получателю. Если злоумышленник перехватит ключ, он сможет расшифровать все зашифрованные с его помощью данные.

Асимметричная криптография:

• Два ключа: использует пару ключей: публичный (открытый) и приватный (секретный). Публичный ключ можно свободно распространять, а приватный ключ должен храниться в секрете.

• Медленная: гораздо медленнее симметричной криптографии. Поэтому она обычно не используется для шифрования больших объемов данных.
• Решение проблемы распределения ключей: Публичный ключ можно свободно распространять, устраняя проблему безопасной передачи секретного ключа. Только владелец приватного ключа может расшифровать данные, зашифрованные с помощью соответствующего публичного ключа.
• Цифровая подпись: позволяет подтвердить подлинность и целостность данных. Данные, подписанные приватным ключом, могут быть проверены с помощью соответствующего публичного ключа.

10. Как осуществляется совместный доступ к зашифрованным файлам при использовании программы Citadel Safstor (VeraCrypt)?

1. Использование сетевого хранилища (NAS)
Если у нас есть сетевое хранилище (NAS), мы можем создать зашифрованный контейнер на NAS и предоставить доступ к этому контейнеру нескольким пользователям.

1. Создание зашифрованного контейнера:
   - Устанавливаем VeraCrypt на компьютер.
   - Создаем новый зашифрованный контейнер на NAS.
   - Указываем пароль и другие параметры шифрования.
2. Монтирование контейнера:
   - Каждый пользователь, имеющий доступ к NAS, устанавливает VeraCrypt на свой компьютер.
   - Пользователи могут монтировать зашифрованный контейнер, используя общий пароль.

2. Использование облачного хранилища
Мы можем использовать облачное хранилище (например, Google Drive, Dropbox) для хранения зашифрованного контейнера.

1. Создание зашифрованного контейнера:
   - Создаем зашифрованный контейнер на локальном компьютере.
   - Загружаем этот контейнер в облачное хранилище.
2. Доступ к контейнеру:
   - Пользователи могут скачать контейнер из облачного хранилища.
   - Монтировать контейнер с помощью VeraCrypt, используя общий пароль.

3. Использование сетевых разделов
Если у нас есть сетевой раздел, доступный нескольким пользователям, мы можем создать зашифрованный контейнер на этом разделе.

1. Создание зашифрованного контейнера:
   - Создаем зашифрованный контейнер на сетевом разделе.
   - Указываем пароль и другие параметры шифрования.
2. Монтирование контейнера:
   - Пользователи могут монтировать контейнер, используя общий пароль.

4. Использование ключевых файлов
Для повышения безопасности мы можем использовать ключевые файлы вместо или в дополнение к паролям.

1. Создание ключевого файла:
   - Создаем ключевой файл с помощью VeraCrypt.
   - Распространяем ключевой файл среди пользователей, которым нужен доступ к зашифрованному контейнеру.
2. Монтирование контейнера:
   - Пользователи могут монтировать контейнер, используя ключевой файл и, при необходимости, пароль.

19. Как обеспечивается защита конфиденциальных документов в пакете Microsoft Office?

Microsoft Office предоставляет несколько методов для защиты конфиденциальных документов:

- Парольная защита: можно установить пароль для открытия документа или для его редактирования. Это предотвращает несанкционированный доступ и изменение документа.
- Шифрование: Встроенные функции шифрования позволяют зашифровать документ, что делает его нечитаемым без соответствующего ключа.
- Цифровые подписи: Использование цифровых подписей позволяет подтвердить подлинность документа и его автора, а также гарантировать, что документ не был изменен после подписания.
- Ограничение доступа: Функции управления правами (IRM) позволяют ограничить доступ к документу, запретить его копирование, печать или отправку по электронной почте.
- Защита информации: Встроенные функции защиты информации (Information Protection) позволяют классифицировать документы и применять соответствующие политики безопасности.

33. Для чего могут применяться методы компьютерной стеганографии?

Компьютерная стеганография используется для скрытия информации внутри других данных, таких как изображения, аудио или видео файлы. Основные области применения включают:

- Защита конфиденциальной информации: Скрытие важной информации от несанкционированного доступа.
- Цифровые водяные знаки: Внедрение водяных знаков для защиты авторских прав и предотвращения нелегального копирования.
- Секретная передача данных: Использование стеганографии для передачи секретных сообщений через общедоступные каналы связи.
- Форензика: Анализ стеганографических методов для обнаружения скрытой информации в ходе расследований.

41. Какие существуют методы обнаружения вредоносных программ?

Существует несколько методов обнаружения вредоносных программ:

- Сигнатурный анализ: Сравнение файлов с базой данных известных сигнатур вредоносного ПО. Этот метод эффективен против известных угроз, но менее эффективен против новых или модифицированных вредоносных программ.
- Эвристический анализ: Использование алгоритмов для обнаружения подозрительного поведения, которое может указывать на наличие вредоносного ПО. Этот метод может обнаруживать новые угрозы, но может также давать ложные срабатывания.
- Поведенческий анализ: Мониторинг поведения программ и процессов в реальном времени для обнаружения аномалий, которые могут указывать на вредоносную активность.
- Машинное обучение и искусственный интеллект: Использование алгоритмов машинного обучения для анализа больших объемов данных и обнаружения паттернов, характерных для вредоносного ПО.
- Сетевой анализ: Мониторинг сетевого трафика для обнаружения подозрительной активности, такой как попытки подключения к командным серверам или передача данных на подозрительные IP-адреса.

45. Как добавить электронную подпись к макросу в документе Microsoft Office?

Для добавления электронной подписи к макросу в документе Microsoft Office необходимо выполнить следующие шаги:

1. Создание сертификата

Если у меня еще нет цифрового сертификата, его нужно создать. Это можно сделать через центр сертификации или использовать самоподписанный сертификат для тестирования.

2. Открытие VBA-редактора

В Microsoft Office (например, Excel или Word) я открываю документ, содержащий макрос. Затем нажимаю **Alt + F11**, чтобы открыть редактор VBA.

3. Подписание макроса

В редакторе VBA я выбираю **Tools** (Инструменты) -> **Digital Signature** (Цифровая подпись). В открывшемся окне нажимаю **Choose** (Выбрать) и выбираю свой сертификат. После этого нажимаю **OK**, чтобы подписать макрос.

4. Сохранение документа

Сохраняю документ с подписанным макросом.

5. Проверка подписи

Возвращаюсь в основное окно Microsoft Office. Перехожу в **File** (Файл) -> **Info** (Информация) -> **View Signatures** (Просмотр подписей). Убеждаюсь, что моя подпись отображается и является действительной.