НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«МОСКОВСКИЙ ЭНЕРГЕТИЧЕСКИЙ ИНСТИТУТ»

Лабораторная работа по ЗД №5

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

Группа: А-05-18

Выполнил: Крылов К.С.

Вариант 24

Проверил

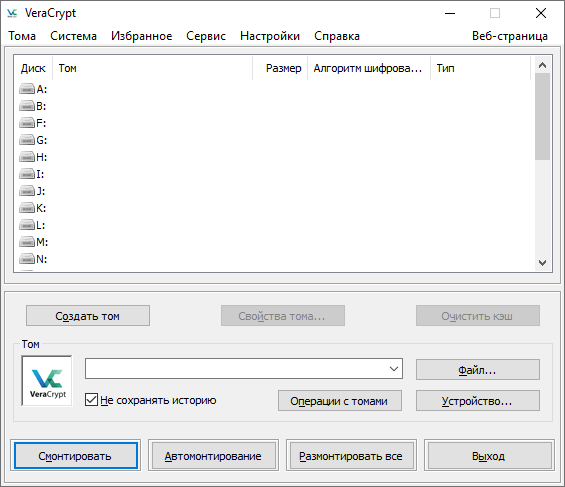
Хорев П.Б.

2021

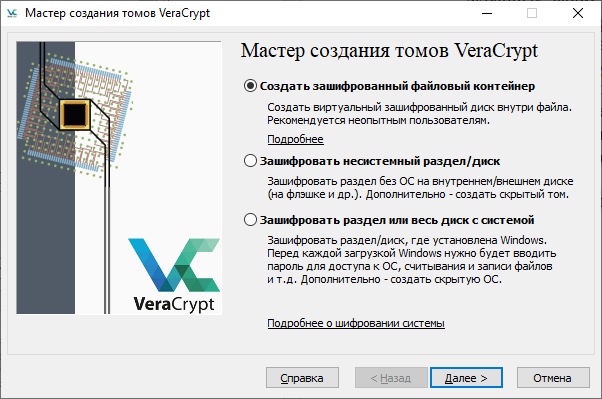
1. Этот пункт выполняется в виртуальной машине Windows XP (если работа выполняется в компьютерном классе кафедры) или с правами администратора (если работа выполняется на домашнем компьютере).

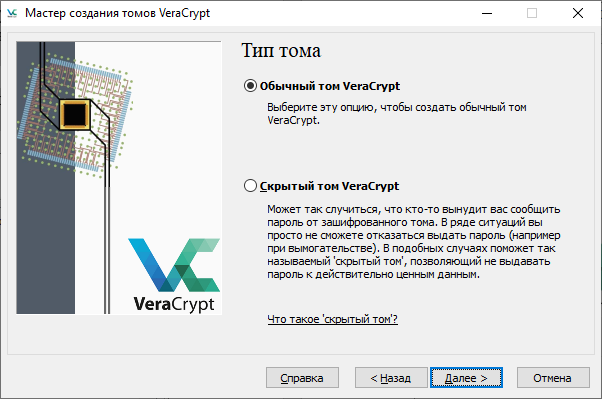
Если пункт выполняется в операционной системе Windows 7 или старше. Скопировать в произвольную папку на локальном жестком диске файл VeraCrypt Setup 1.17.exe.

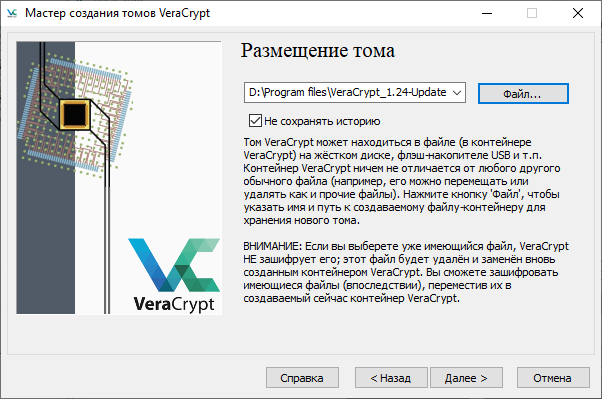
* 1. Если программа VeraCrypt не установлена (отсутствует соответствующий пункт в главном меню), выполнить установку программы VeraCrypt, согласившись со всеми параметрами установки по умолчанию.
  2. Для русификации интерфейса программы выполнить после ее первого запуска команду меню Settings | Language | Русский.

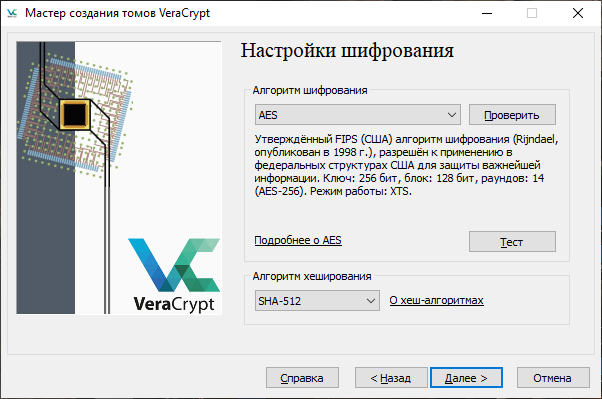


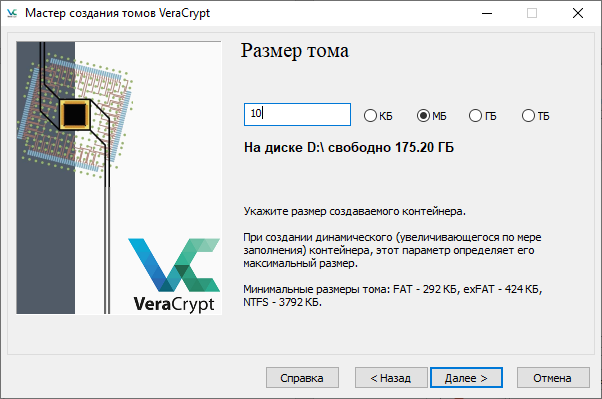
* 1. На примере работы с произвольными (несистемными) файлами различного типа изучить функции программы шифрования VeraCrypt, учитывая, что:
     + перед шифрованием файлов необходимо создать том (зашифрованный файловый контейнер) с помощью кнопки «Создать том» и мастера создания томов VeraCrypt: выбрать 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);

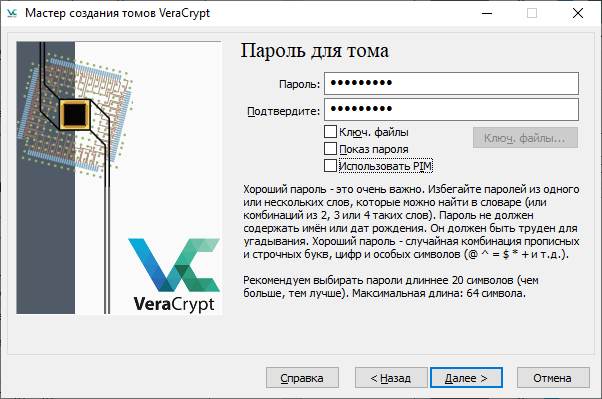


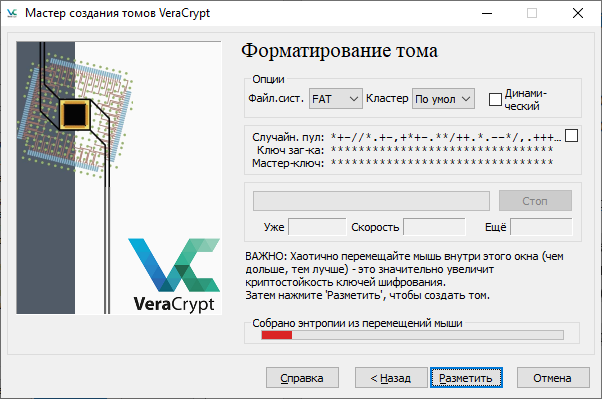


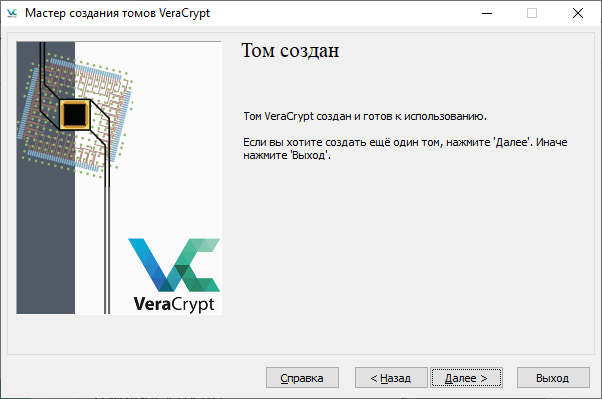




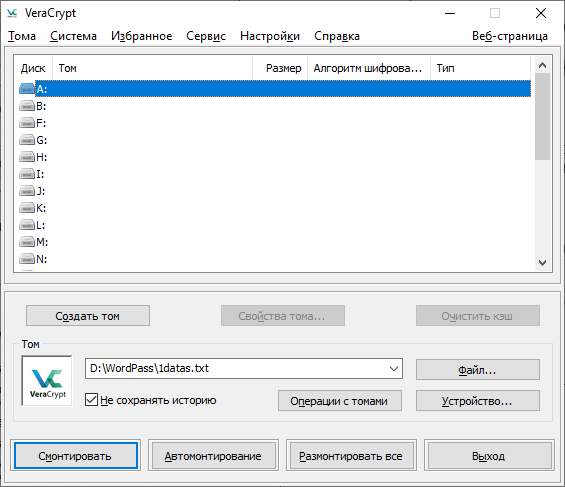


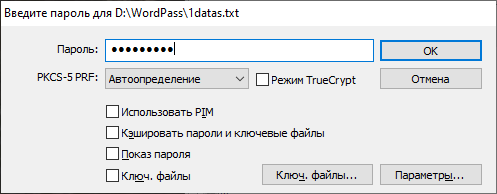


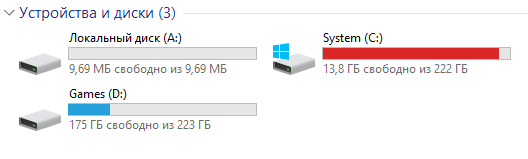




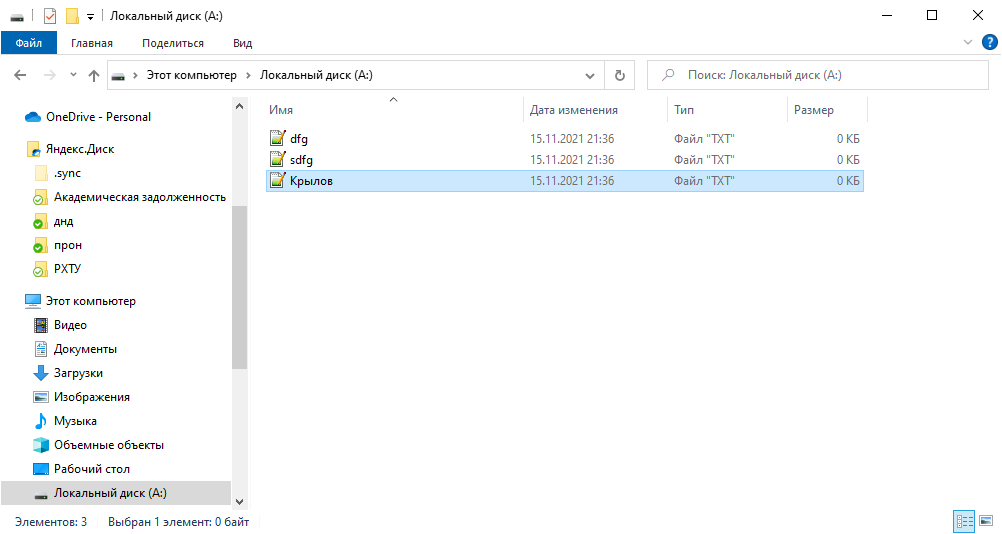
* + - выбрать незанятое имя (букву) для созданного тома и смонтировать его с помощью кнопки «Смонтировать», после чего ввести заданный при создании тома пароль;







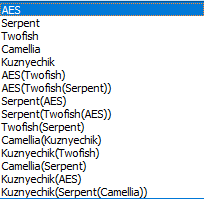
* + - с помощью команды «Открыть» контекстного меню имени (буквы) смонтированного тома открыть его в Проводнике, после чего добавить в него несколько файлов разного типа (один из них должен иметь имя, включающее фамилию студента);



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

При выполнении в любой операционной системе.

* 1. 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);



* + - как генерируется и сохраняется ключ шифрования файла;

В мастере создания томов, в окне диалога изменения пароля и в окне диалога Keyfile Generator можно выбрать алгоритм хэширования. Выбранный пользователем хэш-алгоритм используется генератором случайных чисел VeraCrypt в качестве псевдорандомной функции «смешивания», а функция производного ключа заголовка (HMAC на основе хэш-функции, как указано в PKCS #5 v2.0) в качестве функции псевдорандома. При создании нового тома генератор случайных чисел генерирует главный ключ, вторичный ключ (режим XTS) и соль.

Ключ шифрования данных MEK в обязательном порядке шифруется ключом шифрования ключа шифрования Key Encryption Key (KEK). Без KEK невозможно расшифровать MEK, а без MEK невозможно расшифровать данные. Для чего нужна такая сложная схема? Хотя бы для того, чтобы вы смогли сменить пароль от криптоконтейнера без обязательной расшифровки и перешифровки всего содержимого. Однако роль пары ключей MEK/KEK этим сценарием не ограничивается. Так, достаточно будет затереть несколько десятков байтов в заголовке контейнера (перезаписав область, в которой хранится MEK), и контейнер никто и никогда больше расшифровать не сможет, даже если точно известен пароль. Возможность моментального и безвозвратного уничтожения данных — важная часть общей стратегии безопасности.

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

Если брать файл, который используется в качестве хранилища тома, то он имеет постоянный объём, который пользователь задаёт при настройке тома, если брать файл, который пользователь шифрует, то файл не меняется.

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

Если есть необходимость организовать доступ к одному тому VeraCrypt одновременно с множества операционных систем, то для этого есть два вариант:

1. Контейнер VeraCrypt смонтирован только на одном компьютере (например, на сервере) и к содержимому смонтированного тома VeraCrypt (например, файловая система внутри тома VeraCrypt) раздается доступ по сети. Пользователи на других компьютерах или системах не будут монтировать том (он уже смонтирован на сервере).

Преимущества: Все пользователи могут записывать данные на том VeraCrypt. Том с общим доступом может быть как контейнером, так и разделом.

Недостатки: Данные, пересылаемые по сети, не будут зашифрованы. Тем не менее, всё же возможно их шифровать используя SSL, TLS, VPN или другие технологии.

2. Размонтированный файл контейнера VeraCrypt расположен на одном компьютере (например, на сервере). К этому зашифрованному файлу предоставлен общий доступ по сети. Пользователи на других компьютерах или системах будут монтировать его у себя. Таким образом, том будет смонтирован одновременно под множеством операционных систем.

Преимущества: Передаваемые по сети данные будут зашифрованы (тем не менее, всё равно рекомендуется шифровать их используя SSL, TLS, VPN или другие подходящие технологии, чтобы сделать анализ трафика более сложным и сохранить целостность данных).

Недостатки: Том с совместным доступом может быть только контейнером (не разделом). Этот том должен быть смонтирован в режиме только для чтения на каждой системе. Заметьте, что это требование применимо также и к незашифрованным томам. Одной из причиной этого, например, является то, что данные читаемые с обычной файловой системы под ОС, пока этот же файл модифицируется другой ОС, могут стать противоречивыми (что послужит причиной повреждения данных).

* + - какие действия выполняет пользователь при установке программы.

Вначале программе установки необходимо дать разрешение на необходимые права, после чего принять лицензионное соглашение и выбрать папку установки.

1. 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:
   1. скрывается ли наличие в системе зашифрованных файлов и папок;

Нет, не скрываются, но есть возможно скрыть файл или папку.

* 1. где хранится ключ шифрования файла;

FEK (случайный для каждого файла ключ симметричного шифрования) защищается путём асимметричного шифрования, использующего открытый ключ пользователя, шифрующего файл, и алгоритм RSA (теоретически возможно использование других алгоритмов асимметричного шифрования). Зашифрованный таким образом ключ FEK сохраняется в альтернативном потоке $EFS файловой системы NTFS.

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

Есть возможность записать ключ шифрования на съёмный носитель, поэтому даже при потере учётной записи пользователя, файл или папку можно будет восстановить.

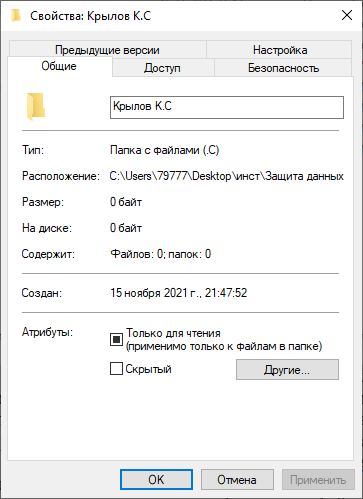
* 1. на дисках с какой файловой системой возможно использование функции шифрования файлов.

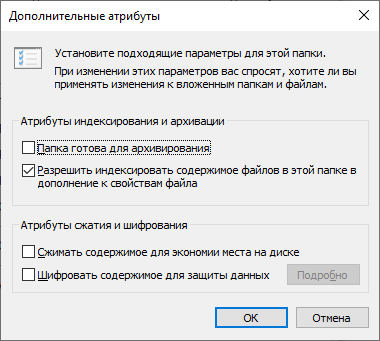
NTFS, и файловые системы съёмных носителей, такие как FAT, FAT32, exFAT.

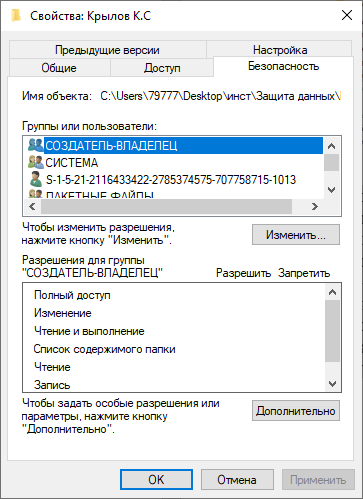
* 1. Освоить средства обеспечения совместного доступа нескольких пользователей к зашифрованным файлам (с помощью кнопки Подробно окна его дополнительных атрибутов) и включить в отчет сведения о порядке использования этих средств и ответ на вопрос, среди каких пользователей возможен выбор тех, кому будет разрешен доступ к зашифрованному файлу.

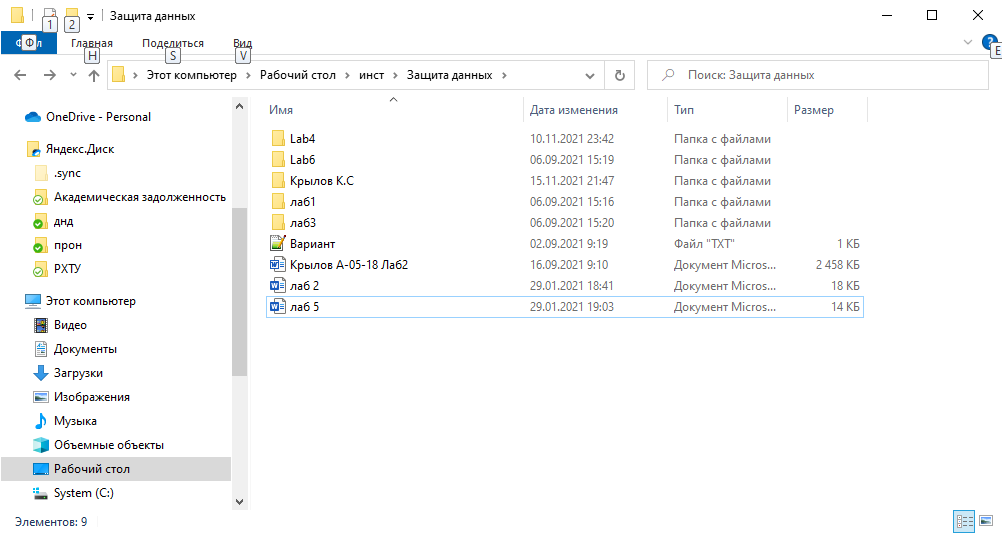
Среди пользователей, проведших проверку, а также доступ можно разрешить группе администраторы и группе все пользователи.

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

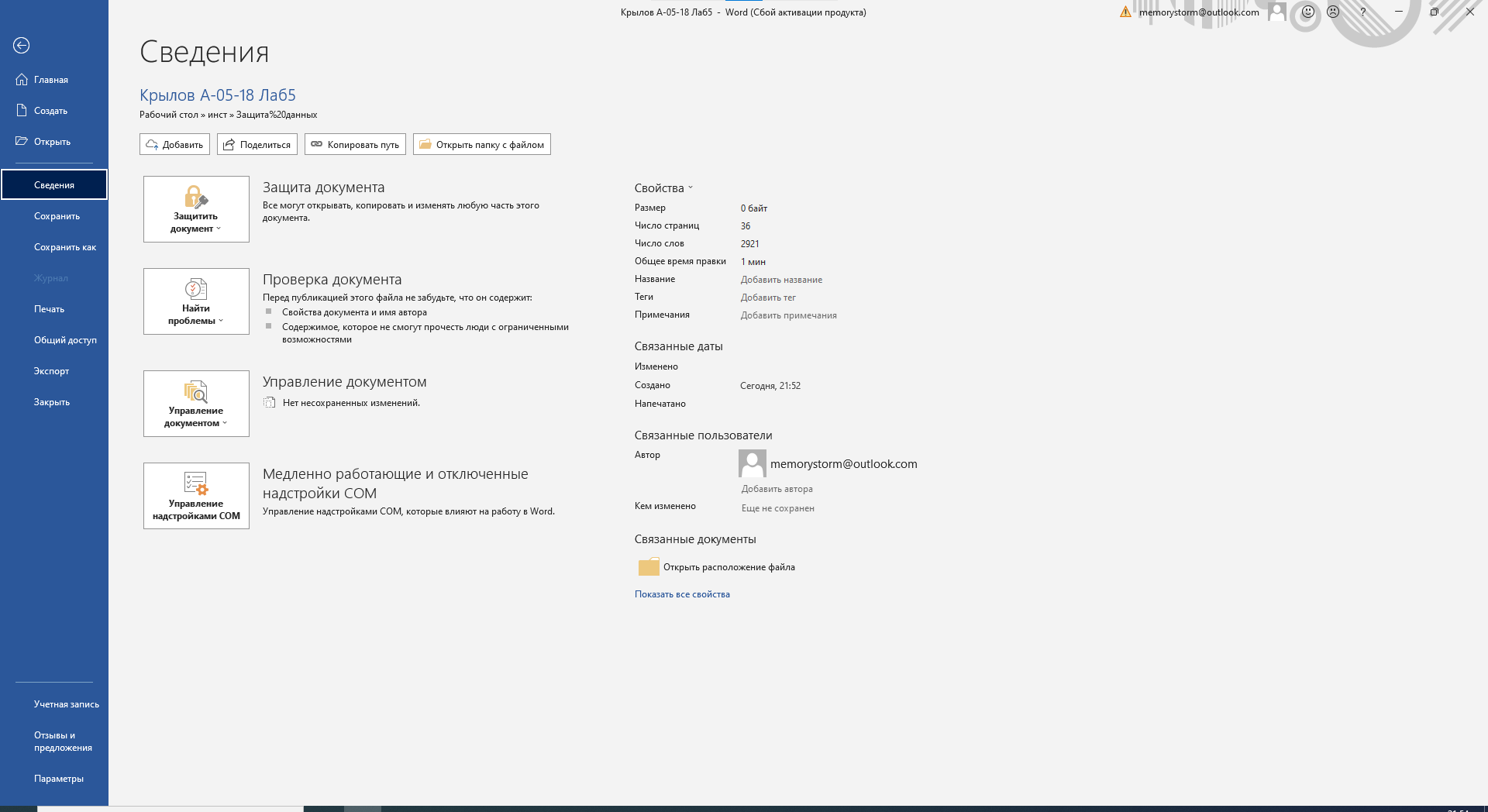


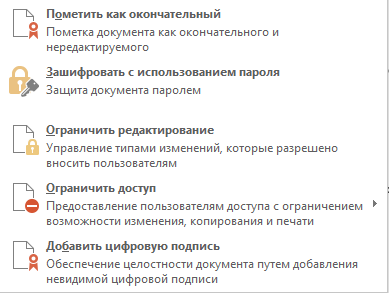


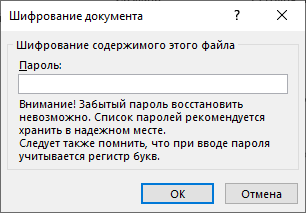
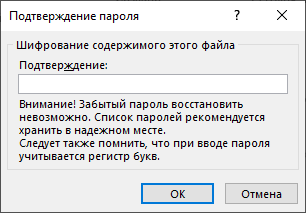




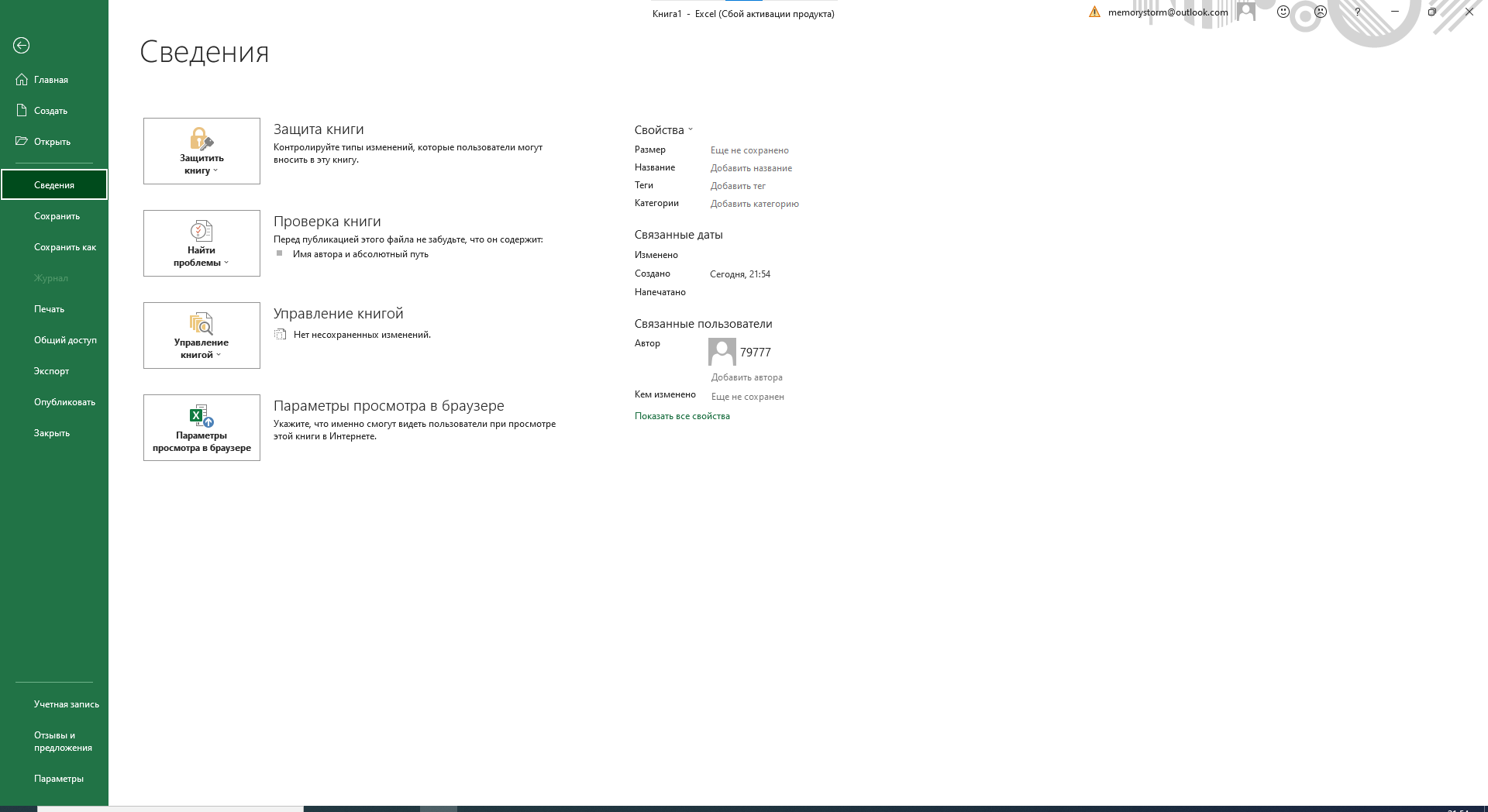
1. Начать работу с Microsoft Word из пакета Microsoft Office (версии XP или старше). Освоить средства шифрования конфиденциальных документов (команды Файл | Сведения | Защита документа | Зашифровать с использованием пароля в Office 2013, Файл | Сведения | Защитить документ | Зашифровать паролем в Office 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.



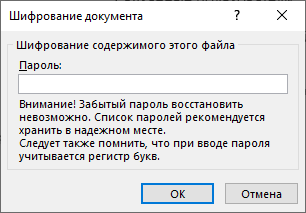
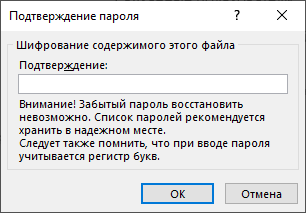


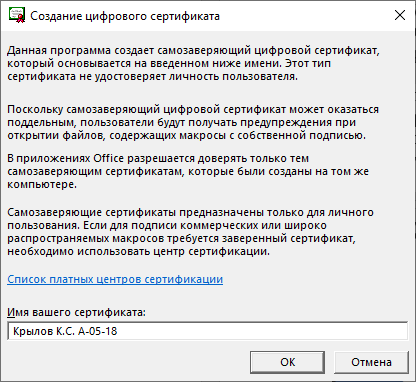
1. Повторить п. 3 для программы Microsoft Excel. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.

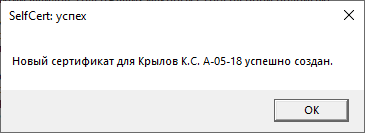




1. С помощью программы selfcert.exe из пакета Microsoft Office (вызов этой программы возможен через меню Пуск | Программы | Средства Microsoft Office | Средство создания цифровых сертификатов для проектов VBA) создать собственную пару ключей асимметричного шифрования и «самоподписанный» сертификат своего 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). Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.



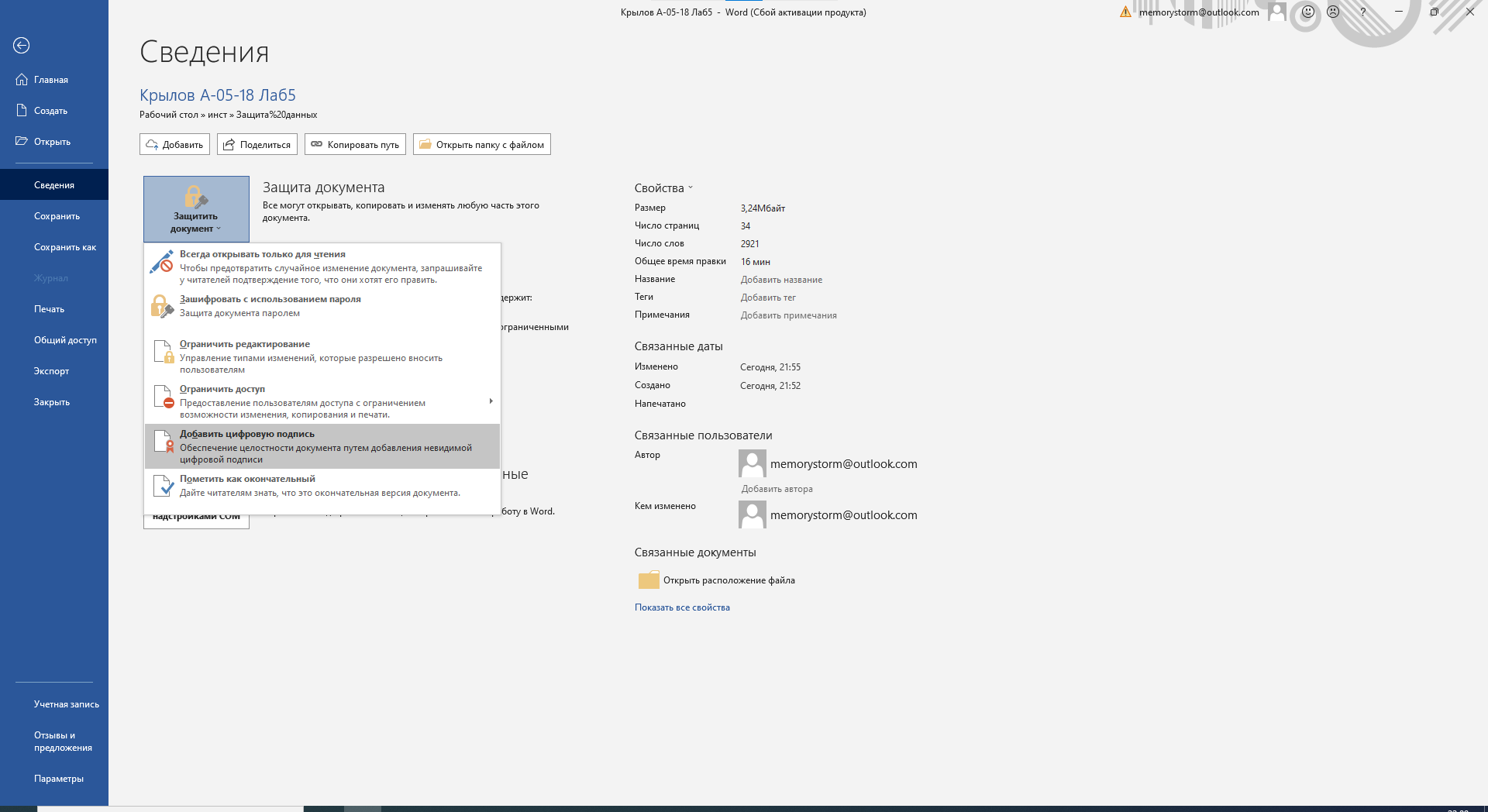
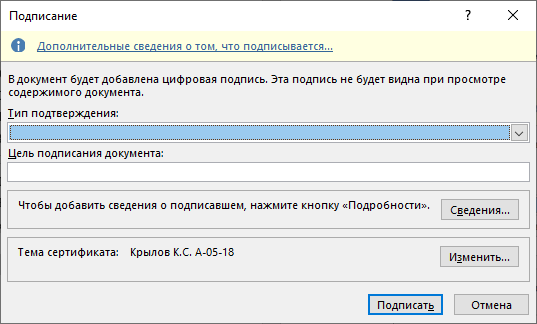


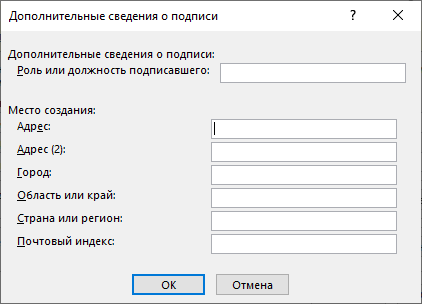
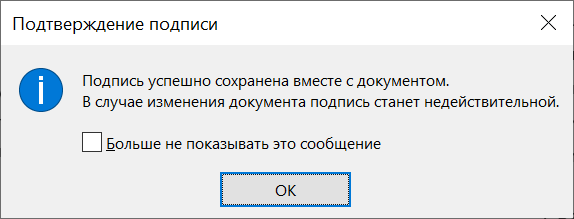
1. Освоить средства добавления электронной подписи к документам Microsoft Office на примере программы Microsoft Word (команды Файл | Сведения | Защита документа | Добавить цифровую подпись в Office 2013, Файл | Сведения | Защитить документ | Добавить цифровую подпись в Office 2010, Кнопка Microsoft Office | 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:
   1. какая информация содержится в сертификате открытого ключа;

* Системная дата и время
* Роль и должность подписавшего
* Адрес
* Адрес(2)
* Город
* Область или край
* Страна и регион
* Почтовый индекс
* Дополнительные сведения: Системная дата и время, Версия Windows, Версия Office, Версия Microsoft Word, Число мониторов, Основной монитор, Дата/время метки времени, Служба меток времени.
  1. что такое путь сертификации.

**Путь сертификации - у**порядоченная последовательность сертификатов объектов в иерархическом каталоге, которая вместе с открытым ключом начального объекта пути позволяет получить сертификат окончательного объекта пути.

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

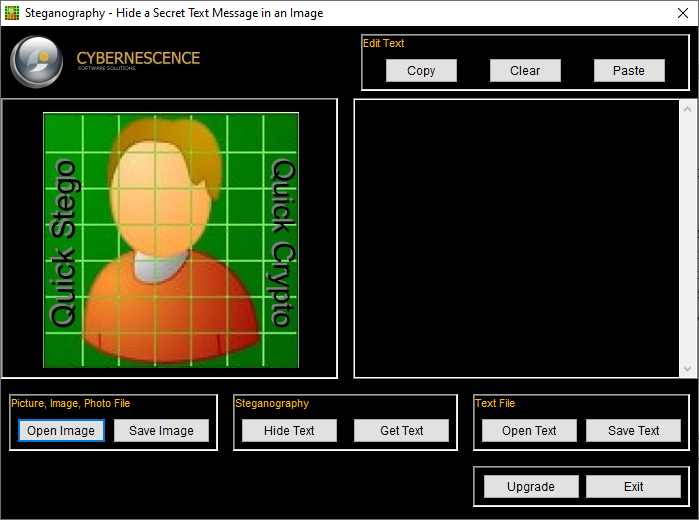
 

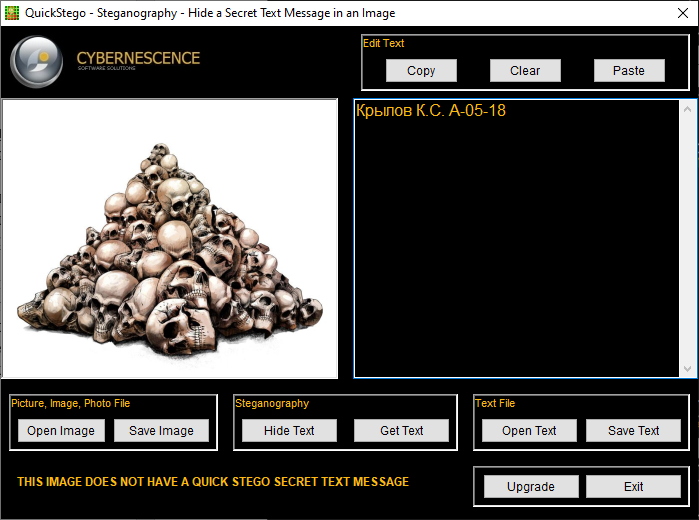
 

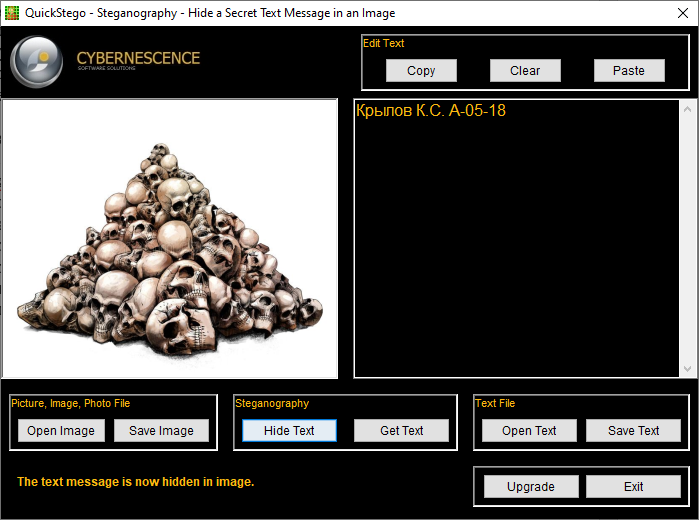
1. Этот пункт выполняется в виртуальной машине Windows XP или с правами администратора.

Если пункт выполняется в операционной системе Windows 7 или старше. Скопировать в произвольную папку на локальном жестком диске файл QS12Setup.zip и извлечь файлы из этого архива.

* 1. Если программа QuickStego не установлена (отсутствует соответствующий пункт в главном меню), то запустить программу QS12Setup.exe для установки стеганографической программы QuickStego.
  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.







При выполнении в любой операционной системе.

* 1. Включить в отчет ответы на вопросы:
     + как происходит скрытие и извлечение сообщений из контейнеров;

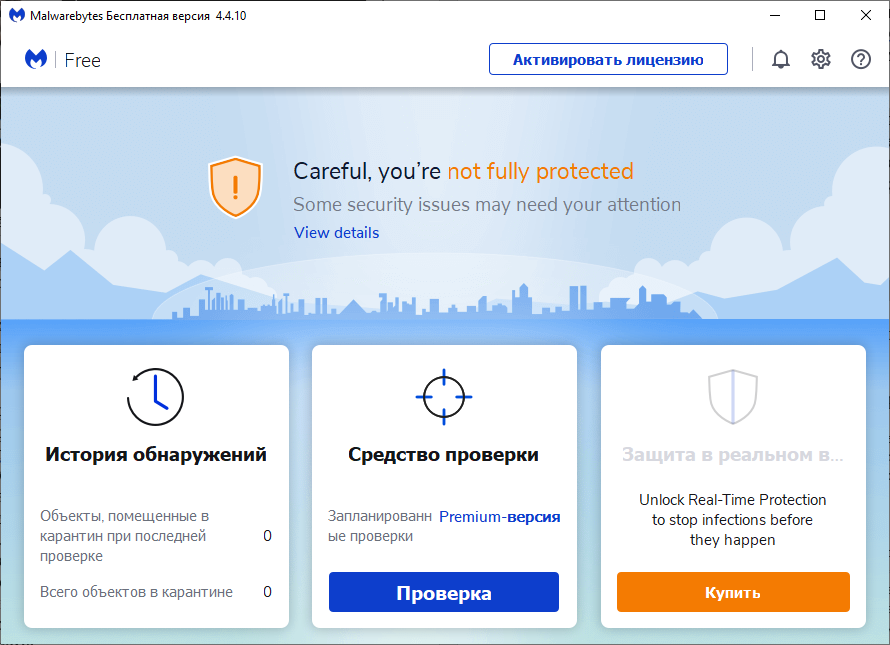
Все происходит по принципу замены цвета в изображении, на близкий к нему. Программа заменяет некоторые пиксели, положение которых вычисляет сама. Этот подход работает не только с текстовой информацией, но и с изображениями.

* + - в чем разница между методами криптографии и стеганографии;

1. Значение стеганографии - «скрытое или скрытое письмо», в то время как криптография означает «секретное письмо».
2. Стеганография - это попытка достичь безопасного и необнаружимого общения. С другой стороны, криптография намеревается сделать сообщение читаемым только для целевого получателя, но не для других путем получения замаскированной формы сообщения.
3. В стеганографии основная структура сообщения не изменяется, тогда как криптография налагает изменение на секретное сообщение перед его передачей по сети.
4. Криптография широко используется в отличие от стеганографии, которая не так знакома.
5. Степень защиты секретных данных измеряется длиной ключа, что делает алгоритм надежным и нерушимым. И наоборот, в стеганографии такого нет.
6. Стеганография обеспечивает только конфиденциальность и аутентификацию. Наоборот, принципами безопасности, обеспечиваемыми криптографией, являются конфиденциальность, целостность, аутентификация и отсутствие отказа от авторства.
   * + каким должно быть соотношение между размерами файла-контейнера и файла-сообщения при использовании программы contrab.exe (QuickStego) и почему.

Размер файла-сообщения не должен превышать размер файла контейнера, так как в противном случае будет заметен факт изменения изображения. Но разумеется, чем больше размер контейнера и чем меньше размер сообщения, тем лучше.

1. 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



* 1. сведения о назначении и основных функциях программы, а также ответы на вопросы:

Основное назначения антивирусных программ - это борьба с различными вирусами.

Основные функции:

* **Защита от вирусов в реальном времени.**

Большинство антивирусов предлагает защиту в режиме реального времени. Это означает, что антивирусная программа ежесекундно защищает компьютер от всех поступающих угроз. Таким образом, даже если вирус не заразил ваш компьютер, вы должны рассмотреть установку антивируса с режимом защиты в реальном времени с целью предотвращения дальнейшего распространения инфекции.

* **Обнаружение угроз.**

Антивирусное ПО может сканировать весь компьютер в поисках вирусов. Прежде всего сканируются наиболее уязвимые области, системные папки, оперативная память. Вы также можете сами выбирать сектора сканирования, или выбрать, например, проверку конкретного жесткого диска. Однако, не все антивирусы одинаковы в своих алгоритмах, и некоторые антивирусы имеют более высокий уровень обнаружения, чем другие.

* **Автоматические обновления.**

Новые вирусы создаются и появляются каждый день. Поэтому, крайне важным для антивирусных программ является возможность обновления баз (списка всех известных вирусов, как старых, так и новых). Автоматическое обновление является необходимым, потому что устаревший антивирус не может обнаруживать новые вирусы и угрозы.

Кроме того, если антивирусный софт предлагает только ручное обновление, вы можете забывать обновлять базы, а ваш компьютер может заразиться новым вирусом. Постарайтесь выбрать антивирус с автоматическим обновлением.

* **Оповещения.**

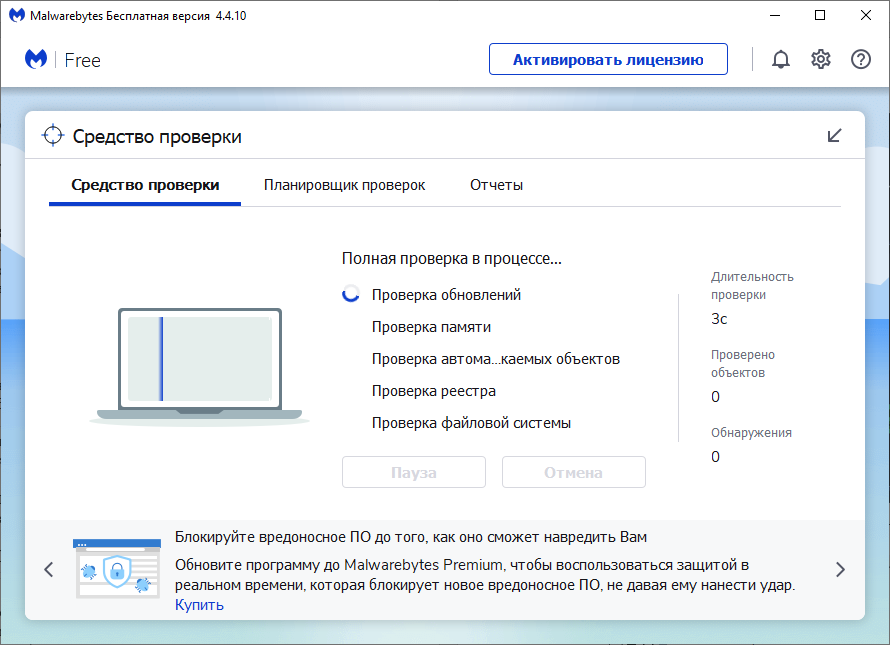
Антивирус предупредит вас, когда какая-либо программа попытается получить доступ к вашему компьютеру. Примером могут служить Интернет-приложения. Многие из них, которые пытаются получить доступ к ПК, безвредны или же вы загрузили их добровольно и, таким образом, антивирусы дают вам возможность принять решение самим — разрешать или блокировать их установку или работу.

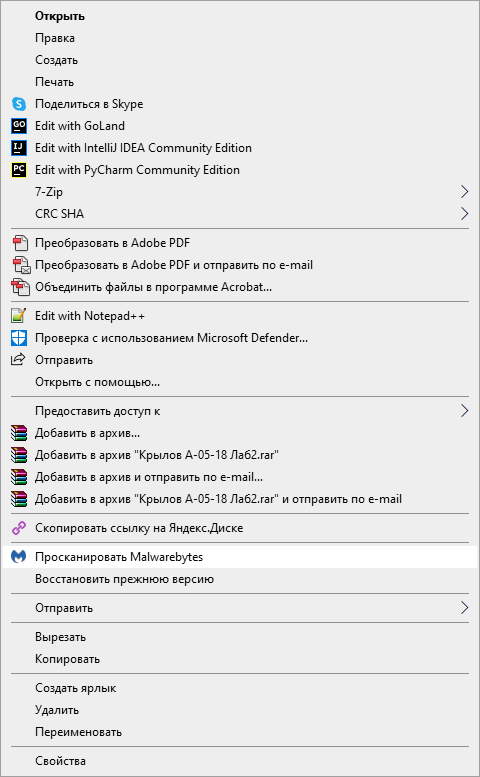
* **Дополнительные функции антивирусов.**

В зависимости от антивирусного программного обеспечения, оно может выполнять множество дополнительных функций. Они могут включать в себя защиту входящей и исходящий электронной почты, защиту мгновенного обмена сообщениями и чатов, защиту интернет-серфинга и мн. др.

* 1. как задаются области сканирования (диски, папки и т.п.);

Как видно по скриншоту ниже, мы можем выбрать конкретную папку или файл для сканирования из контекстного меню. Такая функция есть практически у всех популярных антивирусов.



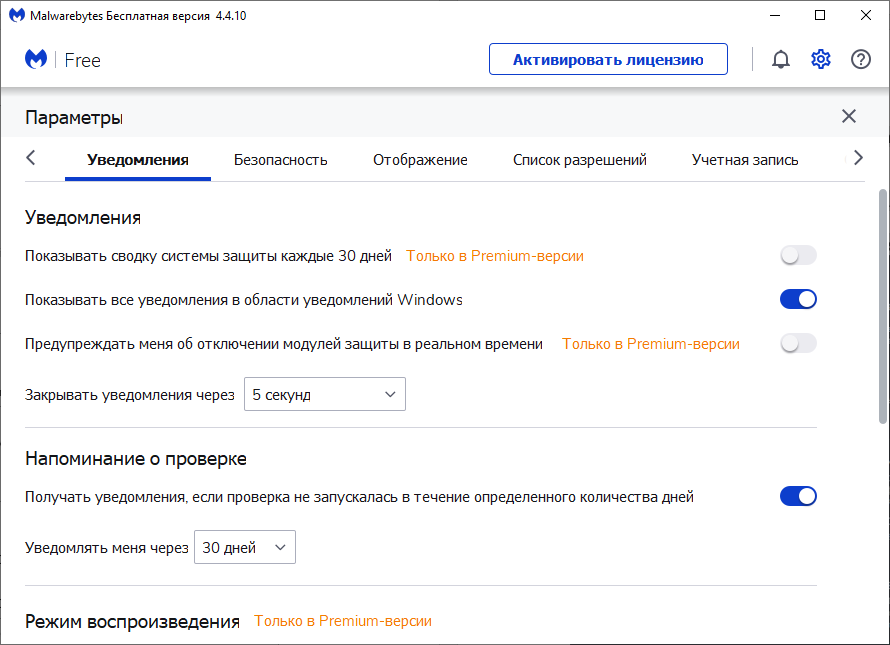


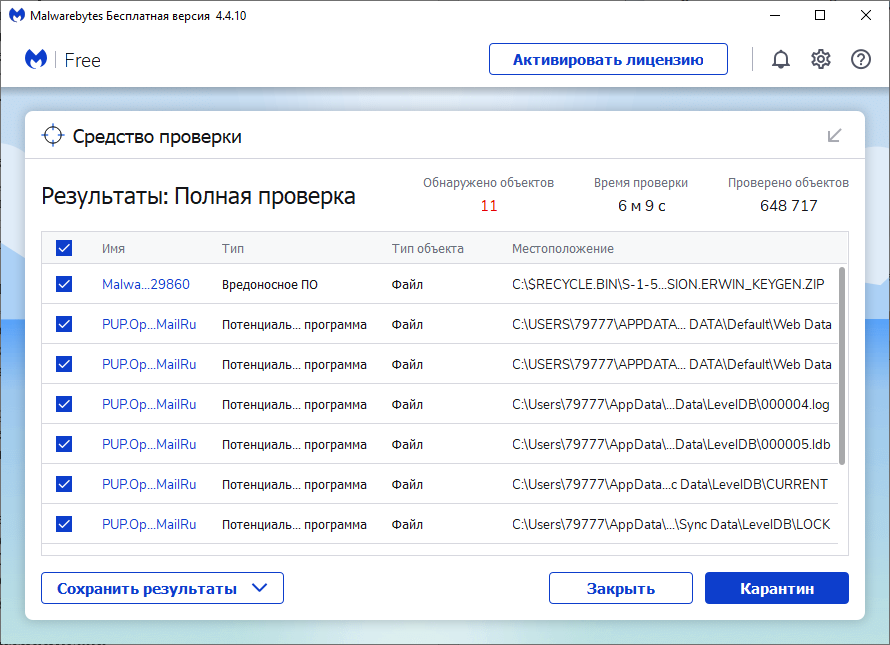
* 1. как задаются объекты проверки на наличие вирусов (типы (расширения имен) сканируемых файлов);

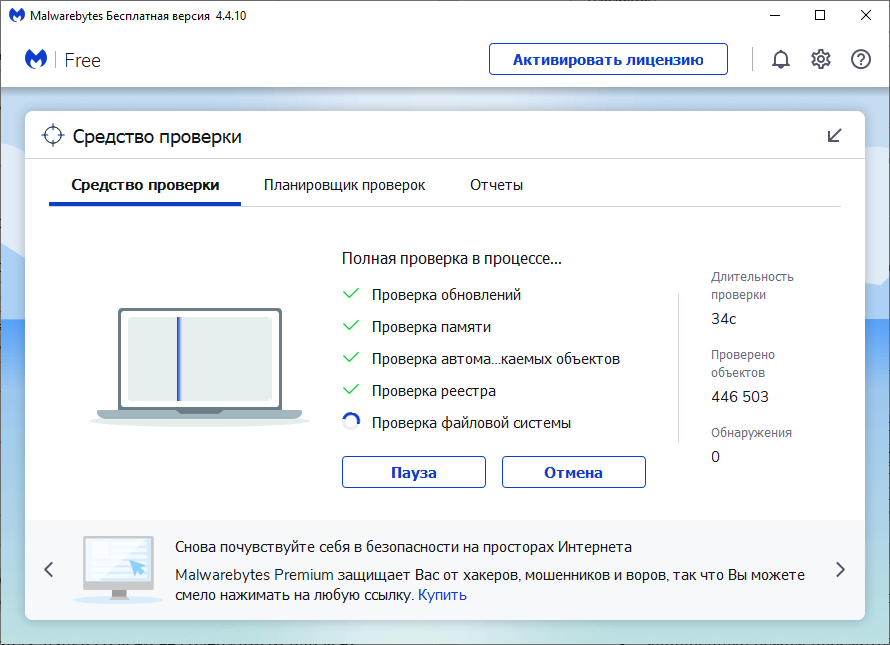
В данном случае нельзя выбрать конкретные расширения файлов. Возможно сканирование файла, папки со всем ее содержимым или всех файлов и папок целиком.

* 1. как определяется реакция сканера в случае обнаружения зараженного файла.

Возможен лишь выбор длительности уведомления. При обнаружении вируса возможно добавить его в карантин или оставить.







Завершить работу с программой.

1. 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.
   1. Включить в отчет сведения о способах защиты от вредоносных макросов в документах Word.

Два механизма безопасности интегрированы непосредственно в приложения Microsoft Office:

* Защищенный режим просмотра
* Политики запрета исполнения макросов VBA.

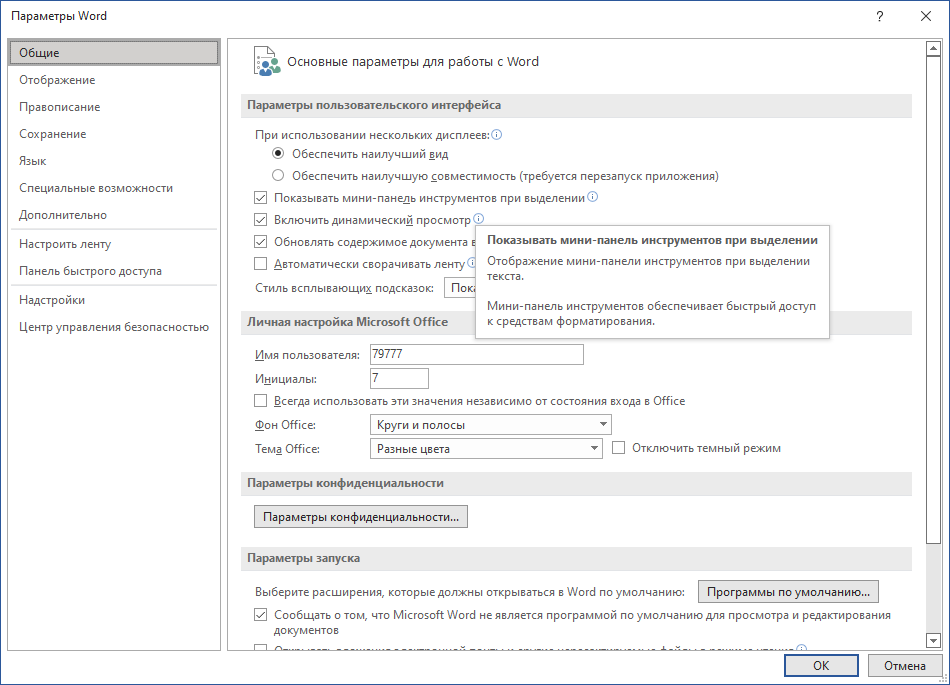
В Microsoft Office есть защищенный режим, который активируется при просмотре файлов, загруженных из интернета, запрещает запуск любого активного содержимого (в том числе, и макросов) и создает ряд ограничений для процесса, который открывает этот документ. При открытии документа в таком режиме создается дочерний процесс (в котором и происходит просмотр документа) с пониженным уровнем целостности и ограничением Job на создание дочерних процессов (делается ограничением одного активного процесса в Job).

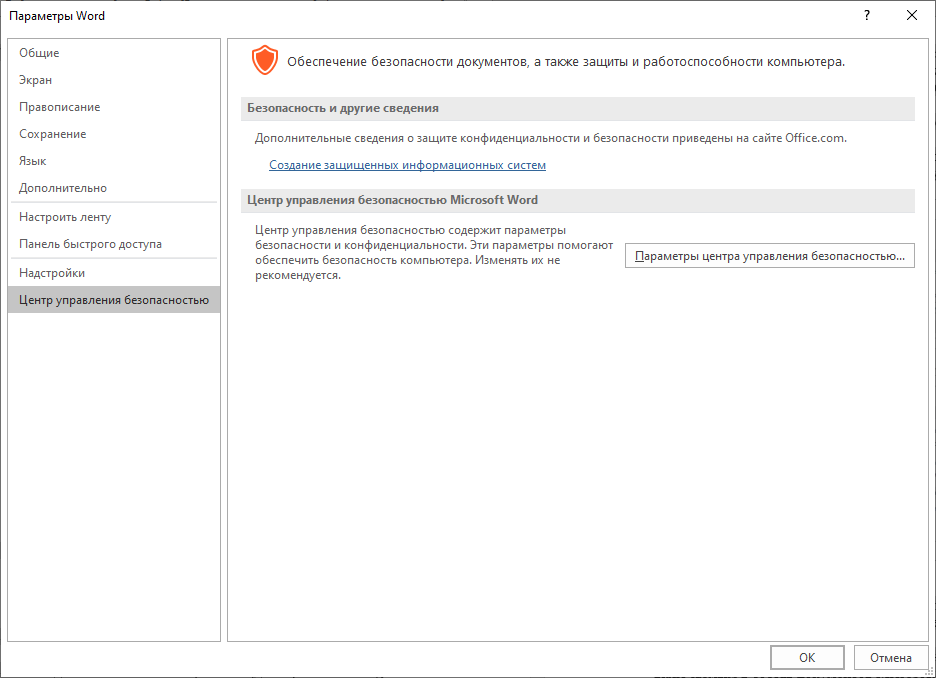
Эти ограничения, в первую очередь, направлены на предотвращение эксплуатации обычных бинарных уязвимостей в самом офисном приложении.  
  
Изоляция процесса, отображающего документ в защищенном режиме, реализована в целом хорошо и заслуживает отдельного упоминания.  
  
На уровне приложения в ОС Microsoft Windows предоставляет следующие возможности изоляции процесса:

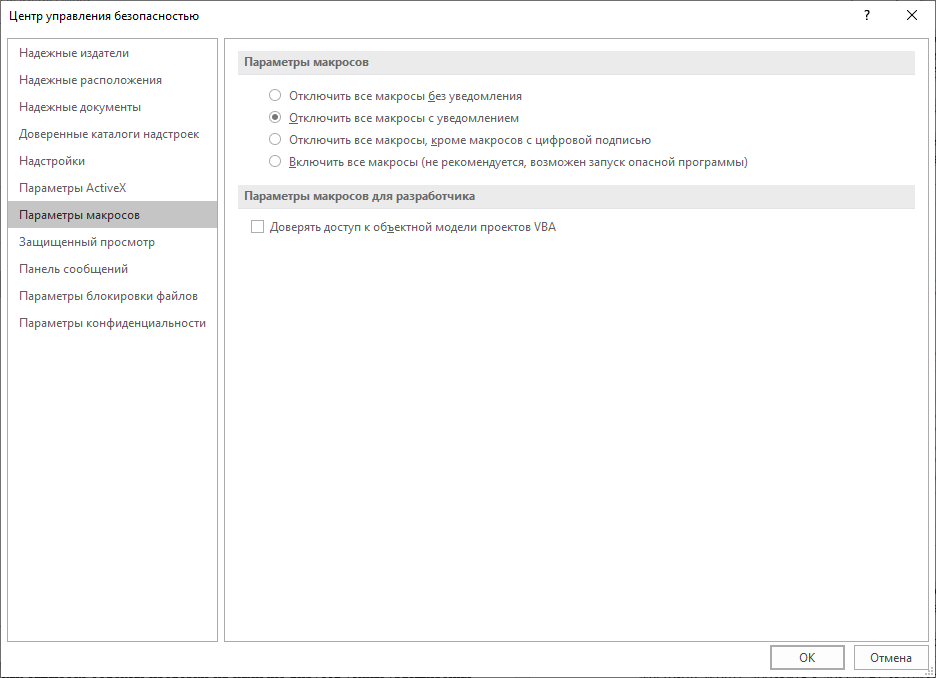
* Ограничения токена (маркера доступа) процесса
* Ограничения GUI-подсистемы
* Ограничения объекта Job для процесса.

Изоляция процесса офисного приложения, отображающего документ, реализуется при помощи всех этих трех механизмов.

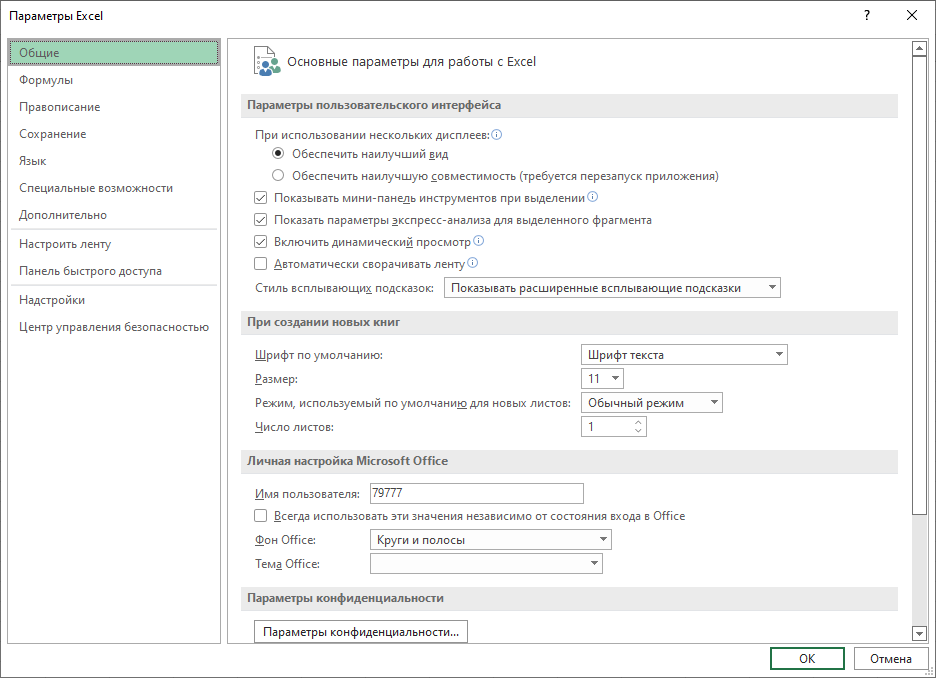
* 1. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.

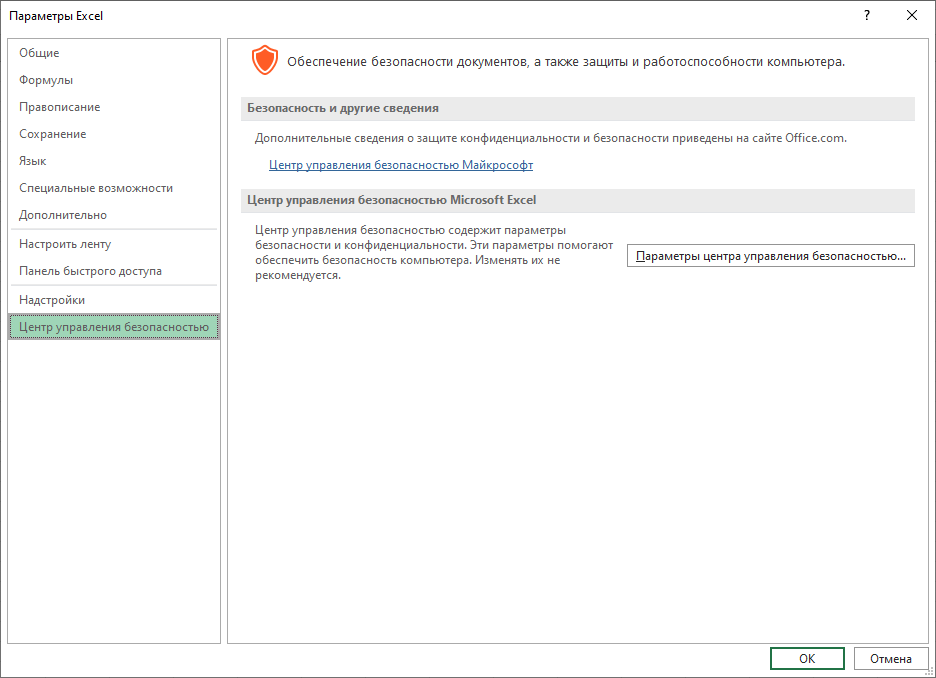


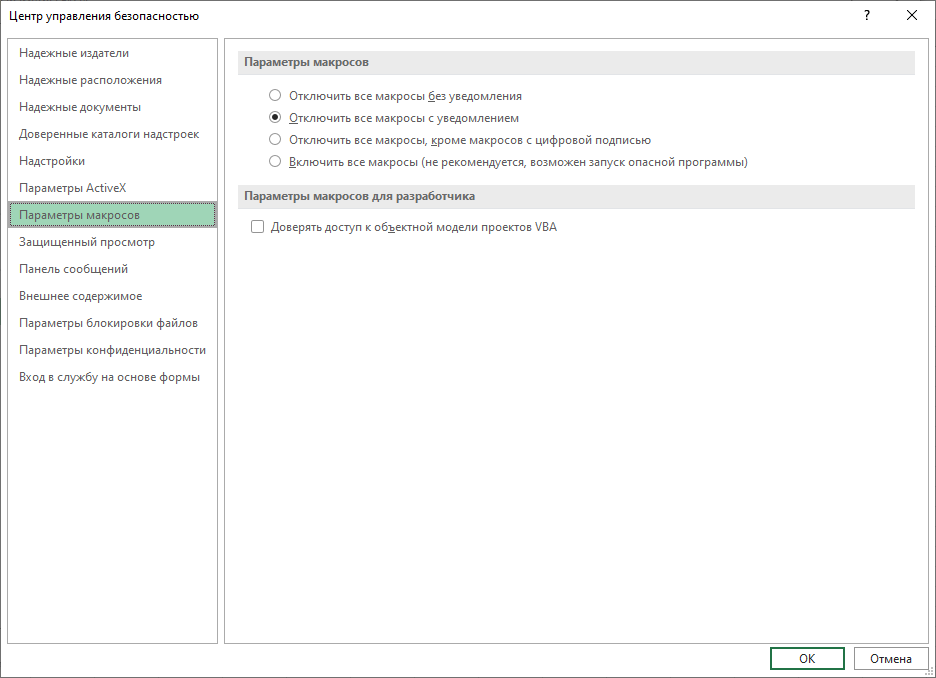




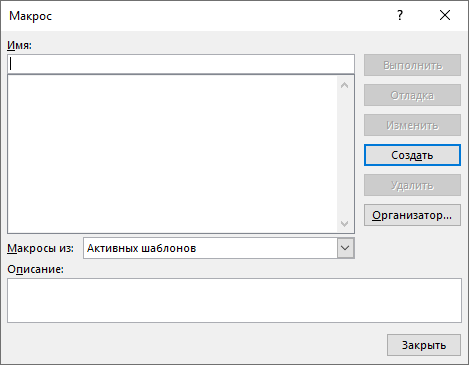
1. Повторить п. 9 для программы Microsoft Excel. Включить в электронную версию отчета копии экранных форм, полученных при выполнении данного пункта.

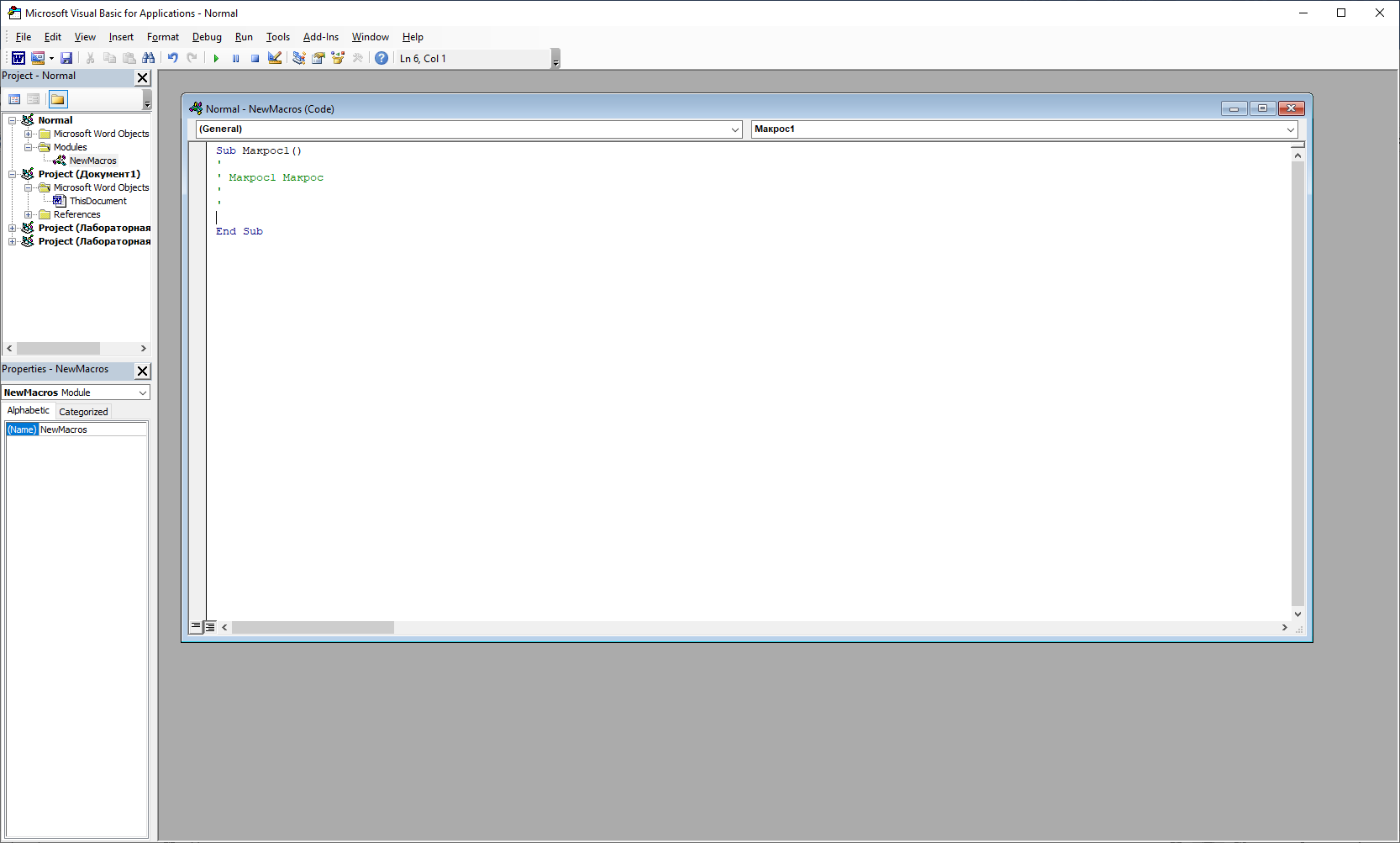


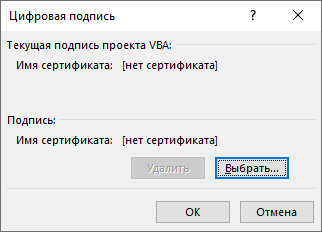




1. Освоить средства добавления электронной подписи к макросам, включаемым в состав документов Microsoft Office (на примере программы Microsoft Word): добавить в документ автоматически выполняющийся при его открытии макрос (команды Вид | Макросы | Макросы в Office 2013, 2010 и 2007, Сервис | Макрос | 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.







Ответы на контрольные вопросы:

4. В чем заключается основная проблема при использовании симметричной криптографии?

Т.к. для шифрования и расшифрования применяется один и тот же ключ, если он будет скомпрометирован третьи лица смогут получить полный доступ ко всей зашифрованной информации. Этого недостатка нет в ассиметричном шифровании, знание открытого ключа не упростит задачу расшифрования зашифрованного текста.

14.Что происходит при шифровании и расшифровании данных при использовании шифрующей файловой системы ОС Windows?

При шифровании файл шифруется с открытым ключем. Для шифрования применяется алгоритм шифрования DESX. Незашифрованный файл пользователя шифруется при помощи случайно сгенерированного ключа FEK. Этот ключ записывается вместе с файлом, файл дешифруется при помощи общего ключа пользователя (записанного в DDF), а также при помощи общего ключа агента восстановления (записанного в DRF).

Файл дешифруется при помощи общего ключа пользователя (записанного в DDF), а также при помощи общего ключа агента восстановления (записанного в DRF). Сначала используется личный ключ пользователя для дешифрации FEK — для этого используется зашифрованная версия FEK, которая хранится в DDF. Расшифрованный FEK используется для поблочного дешифрования файла. Если в большом файле блоки считываются не последовательно, то дешифруются только считываемые блоки. Файл при этом остается зашифрованным.

24. Как обеспечивается подлинность и целостность документов в пакете Microsoft Office?

Подлинность и целостность документов Microsoft Office обеспечивается за счёт наличия у документа электронной подписи с сертификатом автора документа. Также сюда можно отнести шифрования документов, но это скорее относится к защите документов.

30. Для решения каких задач защиты информации применяются функции хеширования?

Хеширование применяется для сокрытия информации, доступ к которой может быть получен нежелательными лицами. Например, базу данных паролей стоит хранить в захешированном виде, т.к. знание хеша пароля не упростит преступникам задачу его перебора.

34. Как осуществляется скрытие конфиденциальных файлов при использовании программы Contraband (QuckStego)?

Программа зашифровывает текстовые файлы в изображениях путем замены цвета в некоторых его(изображения) пикселях. Это позволяет прочитать текст при помощи программы, но с точки зрения человека изображение не меняется.

44. Какие существуют методы защиты от вредоносных макросов документов Microsoft Office?

Два механизма безопасности интегрированы непосредственно в приложения Microsoft Office:

* Защищенный режим просмотра
* Политики запрета исполнения макросов VBA.

То есть при открытии файла, Microsoft Office спрашивает разрешение на редактирования, до подтверждения этого разрешения пользователем, файл открыт в защищенном режиме. А также запретить в настройках Microsoft Office выполнять макросы.