**Лабораторная работа**

**Защита документов в МS Offiсе и Windows**

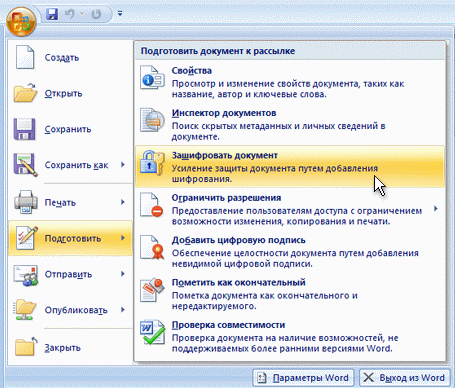
Задание 1.

Создать документ **Word, записать в него ФИО, выполнить действия по его защите при сохранении (см. Ниже)**

**Установка пароля для документа Word**

Чтобы зашифровать файл и задать пароль для его открытия, выполните указанные ниже действия.

1. Нажмите **кнопку Microsoft Office** Изображение кнопки и последовательно выберите команды **Подготовить** и **Зашифровать документ**.



1. В диалоговом окне **Шифрование документа** введите пароль в поле **Пароль** и нажмите кнопку **ОК**.

Можно ввести до 255 знаков. По умолчанию в этой функции применяется усиленное 128-разрядное шифрование по алгоритму AES. Шифрование – это стандартный метод, используемый для защиты файлов.

1. В диалоговом окне **Подтверждение пароля** введите пароль еще раз в поле **Подтверждение** и нажмите кнопку **ОК**.
2. Чтобы сохранить пароль, сохраните файл.

**Снятие защиты паролем для документа Word**

1. Введите пароль, чтобы открыть документ.
2. Нажмите **кнопку Microsoft Office** Изображение кнопки и последовательно выберите команды **Подготовить** и **Зашифровать документ**.
3. В диалоговом окне **Шифрование документа** удалите из поля **Пароль** зашифрованный пароль и нажмите кнопку **ОК**.
4. Сохраните файл.

**Установка пароля для защиты документа Word от изменения**

Помимо пароля на открытие документа Word также можно задать пароль для защиты файла от изменения другими пользователями.

1. Нажмите **кнопку Microsoft Office** Изображение кнопки, выберите команду **Сохранить как** и в нижней части диалогового окна "Сохранение документа" нажмите кнопку**Сервис**.
2. В меню "Сервис" выберите пункт **Общие параметры**. Откроется диалоговое окно "Общие параметры".
3. В разделе "Параметры совместного использования для данного документа" введите пароль в поле **пароль разрешения записи:**.
4. В диалоговом окне "Подтверждение пароля" введите пароль еще раз и нажмите кнопку **ОК**.
5. Нажмите кнопку **Сохранить**.

**Примечание.**  Чтобы удалить пароль, повторите описанную выше процедуру и удалите пароль из поля **пароль разрешения записи:**. Нажмите кнопку **Сохранить**.



1. Введите пароль в поле **Пароль** и нажмите кнопку **ОК**.

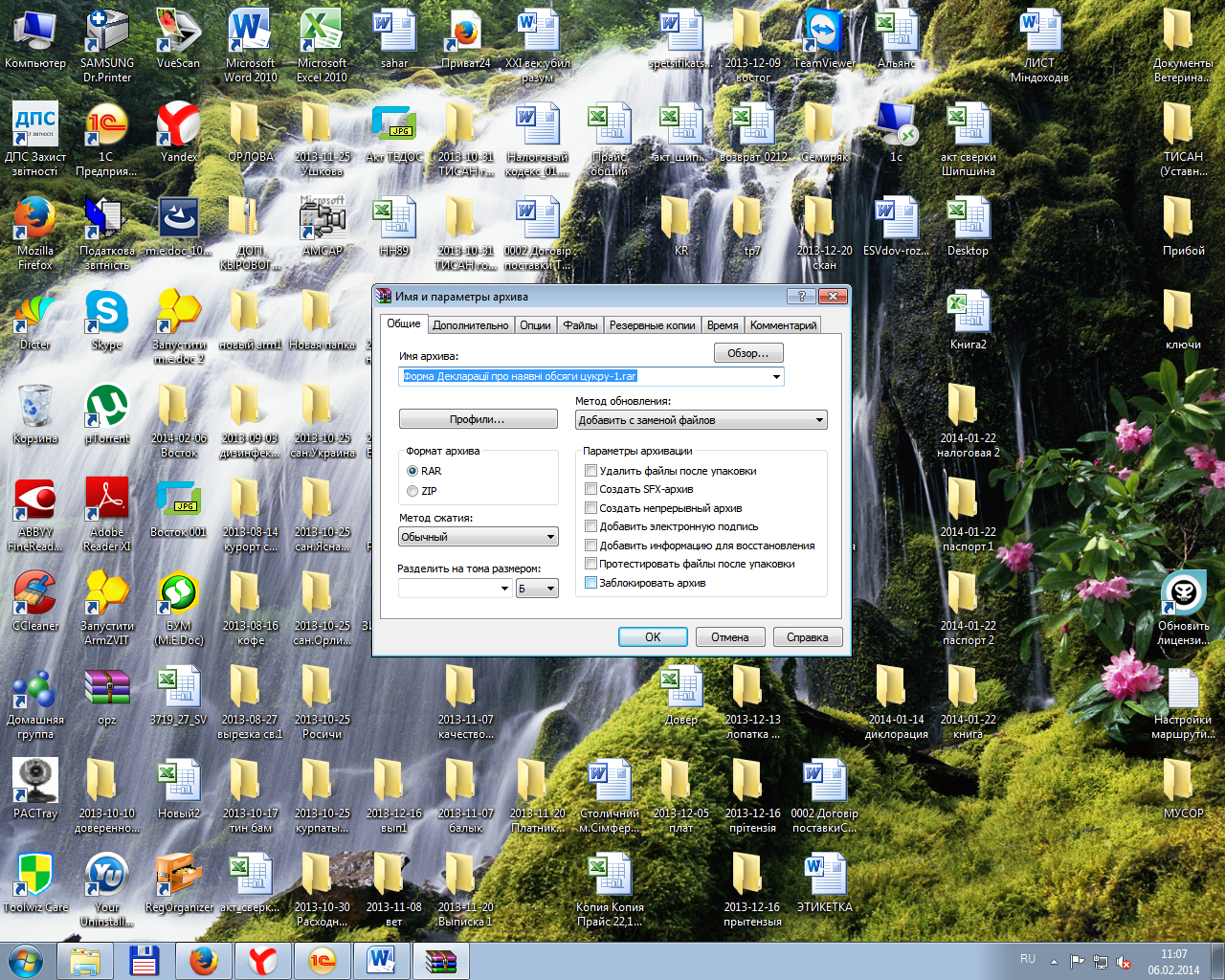
Можно ввести до 255 знаков. По умолчанию в этой функции применяется усиленное 128-разрядное шифрование по алгоритму AES. Шифрование – это стандартный метод, используемый для защиты файлов.

1. Введите пароль еще раз в поле **Подтверждение** и нажмите кнопку **ОК**.
2. Чтобы сохранить пароль, сохраните файл.

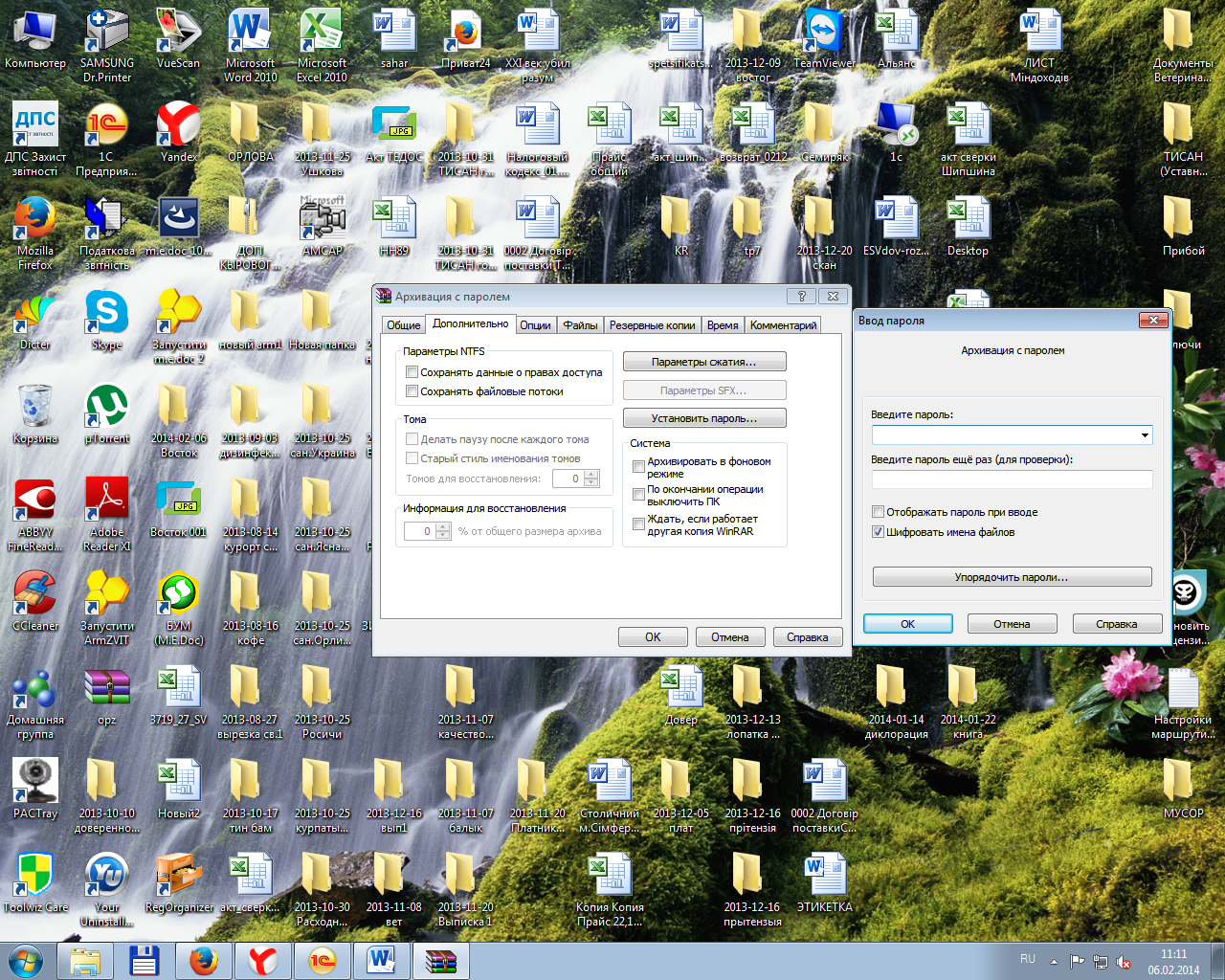
**Задание 2**

**Защита архивов**

Если все, что вам нужно — это зашифровать несколько файлов для отправки их кому-либо, для этой цели удобно пользоваться популярным архиватором WinRar (http://www.win-rar.ru/download/). После установки программы в системе вы получаете возможность создавать архивы, просто выделяя нужные файлы мышью и выполняя команду контекстного меню выделенного файла (или группы файлов, можно архивировать и папки) Добавить в архив. В появившемся после этого окне Имя и параметры архива, на закладке Общие, , можно задать имя архива, уровень сжатия, указать, нужно ли включать в архив информацию для восстановления. Это, кстати, полезный параметр. При передаче через Интернет большие архивы иногда доходят до получателя поврежденными. Использование информации для восстановления позволяет, до определенного уровня повреждений, восстанавливать архивы.



Но нас в данный момент больше интересует следующая закладка окна настройки архива — Дополнительно. Здесь есть кнопка Установить пароль. Если нажать на нее, появляется окно установки пароля. Помимо полей для ввода пароля и подтверждения, здесь имеется флаг Шифровать имена файлов. Его установка приведет к тому, что без знания пароля не только нельзя будет распаковать архив, но и просмотреть его содержимое. Без установки этого флага при открытии архива в программе (например, двойным щелчком по архиву в системе, где установлен WinRar) будут видны содержащиеся в нем файлы. Но попытка распаковать архив или, выполнив двойной щелчок по файлу, открыть его прямо из архиватора, приведет к показу окна для ввода пароля. Без знания пароля открыть такой архив не получится.



Создать защищенный архив для созданного файла

**Задание 3**

**Создать на рабочем столе папку, поместить в нее документ**

Для шифрования файла выполните следующие действия:

1. В главном меню выберите пункт "Все программы", затем "Стандартные" и запустите приложение "Проводник".
2. Перейдите к файлу, который необходимо зашифровать. Щелкните по файлу правой кнопкой мыши и выберите из контекстного меню команду "Свойства".
3. На вкладке "Общие" нажмите кнопку "Другие".
4. В группе "Атрибуты сжатия и шифрования" установите флажок "Шифровать содержимое для защиты данных" и нажмите кнопку "ОК".
5. Нажмите кнопку "ОК". Если файл расположен в незашифрованной папке, Вы получите сообщение "Предупреждение при шифровании". Выполните одно из следующих действий:
   * Если необходимо зашифровать только текущий файл, установите переключатель "Зашифровать только файл" и нажмите кнопку "ОК".
   * Если необходимо зашифровать как файл, так и содержащую его папку, установите переключатель "Зашифровать файл и содержащую его папку" и нажмите кнопку "ОК".

Другие пользователи не имеют возможности работы с зашифрованными Вами файлами. При попытке другим пользователем открыть зашифрованный файл, например, документ Microsoft Word, будет выдано следующее сообщение:

Невозможно открыть документ, так как пользователь не обладает достаточными полномочиями.   
( *диск* :\ *имя\_файла* .doc)

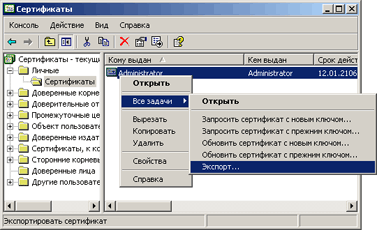
При попытке другим пользователем скопировать зашифрованный файл будет отображено следующее сообщение об ошибке:

Ошибка при копировании файла или папки   
Не удалось скопировать файл *имя\_файла* : Нет доступа.   
Диск может быть переполнен или защищен от записи, либо файл занят другим приложением.

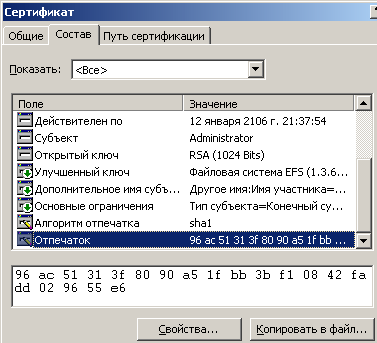
следует заранее экспортировать копии сертификатов и сохранить их в особо надежном месте (например, на CD-R, спрятанном в глухом и темном лесу). Расскажем, как это делается в Windows XP[1](http://old.computerra.ru/gid/rtfm/system/252505/" \l "fwd1).

**Экспорт сертификатов**

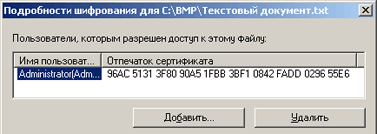
Идем в "Пуск -> Выполнить" и вводим там команду certmgr.msc для вызова консоли управления сертификатами.



Далее неспешно следуем в личные сертификаты, находим свой сертификат (если его нет, значит, вы еще ничего не шифровали, так как он создается при первом использовании этой функции). Убедиться, что это именно тот сертификат, который используется, можно по его отпечатку. Открываем его, проходим на вкладку "Состав" и смотрим "Отпечаток".

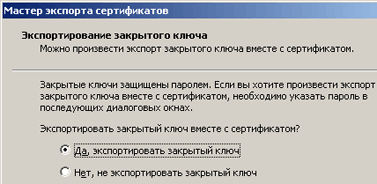


Параллельно идем в "Свойства" какого-нибудь зашифрованного файла, нажимаем "Дополнительно -> Атрибуты сжатия и шифрования -> Подробно" и там смотрим на отпечаток.

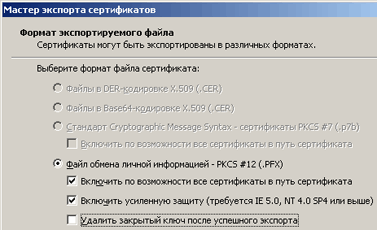


Если они совпадают, значит, этим ключом файл расшифровать можно. Дело в том, что, удалив в certmgr.msc свои сертификаты, Windows создаст их заново. При этом отпечаток у них будет уже другой, и старые файлы они расшифровывать не будут.

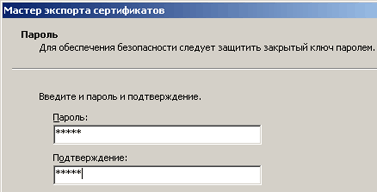
Итак, выбираем в certmgr.msc свой ключ, выбираем меню "Все задачи -> Экспорт".



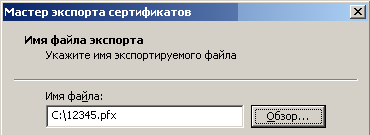
Указываем экспорт закрытого ключа.



Выбираем тип файла PFX и обязательно снимаем галочку на удалении закрытого ключа после экспорта (иначе вы сразу же потеряете доступ к ранее зашифрованным файлам).



Далее вводим пароль к экспортируемому файлу. Этот пароль очень важно потом не забыть, ибо он потребуется только для восстановления ключа в случае падения системы.



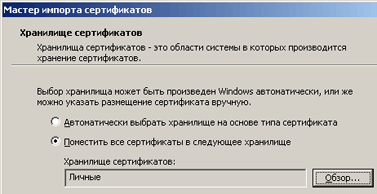
Сохраняем ключ в файл. Готово. Рекомендуем аналогично произвести экспорт не только используемого сертификата, но и остальных в разделе "Личные" и "Доверенные". Теперь эти файлы следует записать на надежный носитель.

**Восстановление данных**

Теперь, рассмотрим последовательность действий при восстановлении зашифрованной информации. Загружаемся в любой Windows XP Pro и открываем в "Проводнике" PFX-файл.

Если на этой машине необходимо только открыть (восстановить) зашифрованные файлы, то галочку на "Пометить этот ключ как экспортируемый" не ставим. Если на компьютере мы заново установили Windows и хотим продолжить обычную работу с зашифрованными файлами, то галочка нужна.

Теперь выбираем "Поместить все сертификаты в указанное хранилище" и при помощи кнопки "Обзор" указываем, куда их помещать. Если сертификат нужен только для чтения старых зашифрованных файлов, то помещаем в "Доверенные".



А вот если сертификат нужен, для того чтобы еще и создавать зашифрованные файлы, то указываем "Личные". Но здесь есть пара тонких моментов. Если вы только что установили Windows, то пока в ней нет сертификата (он создается при первом использовании шифрования файлов), можно смело импортировать старый сертификат в раздел "Личные". Но если вы уже успели воспользоваться шифрованием (или Windows работает давно), то чтобы у вас не возникло двух личных сертификатов и путаницы при шифровании новых файлов, запустите certmgr.msc и посмотрите в раздел "Личные". Если там уже есть сертификат, то следует подумать о возможных последствиях: если вы импортируете еще один сертификат, то вам при шифровании придется внимательно следить за тем, какой сертификат используется. Можно расшифровать файлы, удалить лишний сертификат, перезагрузиться[2](http://old.computerra.ru/gid/rtfm/system/252505/" \l "fwd2) и зашифровать заново оставшимся.

Готово. Теперь с зашифрованными данными можно работать.