Лабораторная работа № 3
По дисциплине «Основы информационной безопасности»
«Защита документов Microsoft Office программными методами»

Методические указания для обучающихся по прохождению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;
- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

- Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;
- ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;
- Итогом выполненной ЛР является отчет.

Структура и форма отчета о лабораторной работе

- Постановка задачи;
- Входные и выходные данные;
- Содержание этапов выполнения;
- Обоснование полученного результата (вывод);
- Список используемой литературы.

Требования к оформлению отчета о лабораторной работе

- Лабораторная работа (ЛР) предоставляется в печатном/или электронном виде;
- ЛР должна соответствовать структуре и форме отчета представленной выше;
- ЛР должна иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);
- Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

Теоретические сведения.

Основные принципы парольной защиты можно условно разделить на три типа:

- хранение пароля в документе в виде обычного текста;

- хранение в документе контрольного значения, тем или иным образом получаемого из пароля (например, при помощи хеш-функции);
- шифрование документа при помощи ключа, получаемого из пароля.

Первый способ парольной защиты является самым простым и соответственно самым ненадежным. Для восстановления пароля достаточно вычислить адрес, по которому он располагается в документе, и просто прочитать символы пароля. Тем не менее, многие уважаемые производители программного обеспечения, включая Microsoft, в некоторых случаях его применяют.

Способ, подразумевающий хранение в документе контрольного значения, более сложен, однако столь же легко поддается взлому, как и первый. Если для вычисления контрольного значения используется обратимая функция или функция, для которой легко подобрать одно из исходных значений, то пароль просто вычисляется. Если же функция необратима (например, криптостойкий хеш), то контрольное значение всегда можно подменить заранее вычисленным из известного пароля. Таким образом, нам остается лишь подменить в документе контрольное значение — и защита документа снята. Этот способ также применяется фирмой Microsoft для парольной защиты некоторых типов документов.

Третий способ защиты является самым сложным. Его криптографическая стойкость определяется лишь набором параметров, используемых для шифрования текста. При достаточной длине ключа шифрования гарантированный взлом защиты становится просто невозможным, даже если задействовать для этого все вычислительные мощности, существующие на земном шаре. Однако самым уязвимым местом этой защиты является сам пароль. Пользователю нужно не только защитить документ, но и придумать такой пароль, который он сможет вспомнить в любой момент. К сожалению, многие пользователи используют в качестве пароля короткие последовательности символов, слова из словаря или наборы цифр. При этом стойкость самой защиты уже не имеет значения — пароль можно найти очень быстро прямым перебором либо атакой по словарю.

Версии Microsoft Office

По способам парольной защиты можно выделить следующие группы версий Microsoft Office:

- ранние версии отдельных приложений: Word 2.0, 6.0; Excel 4.0, 5.0; Access 2.0.
- Microsoft Office 95;
- Microsoft Office 97/2000;
- Microsoft Office XP/2003;
- Microsoft Office 2010.

В MS Word 2013 предусмотрено несколько уровней защиты, позволяющих управлять доступом к документам (рис. 1):

- *Пометить как окончательный*. Это помогает пользователю сообщить о том, что он предоставляет для совместного использования окончательную версию документа. Кроме того, это позволяет предотвратить внесение в документ случайных изменений рецензентами или читателями.
- *Зашифровать паролем*. Это позволяет ограничить доступ к документу, предоставив его только «доверенным» пользователям.

Пароль – способ ограничения доступа к книге, листу или части листа. В MS Word длина пароля не должна превышать 255 букв, цифр, пробелов и других символов. При вводе пароля учитывается регистр букв.

- *Ограничить редактирование*. Чтобы предотвратить внесение редакторами содержимого случайных изменений в документ MS Word 2013, можно ограничить возможности форматирования и изменения файла.
- *Ограничить разрешения для пользователей*. Для ограничения разрешений позволяет использовать идентификатор Windows Live ID или учетную запись MS Windows.
- *Добавление цифровой подписи*. Цифровые подписи используются для проверки подлинности цифровых данных, например документов, сообщений электронной почты и макросов, с помощью криптографии. Они создаются путем ввода или на основе изображения и позволяют обеспечить подлинность, целостность и неотрекаемость.

Все уровни защиты являются не взаимоисключающими, а скорее взаимодополняющими друг друга.

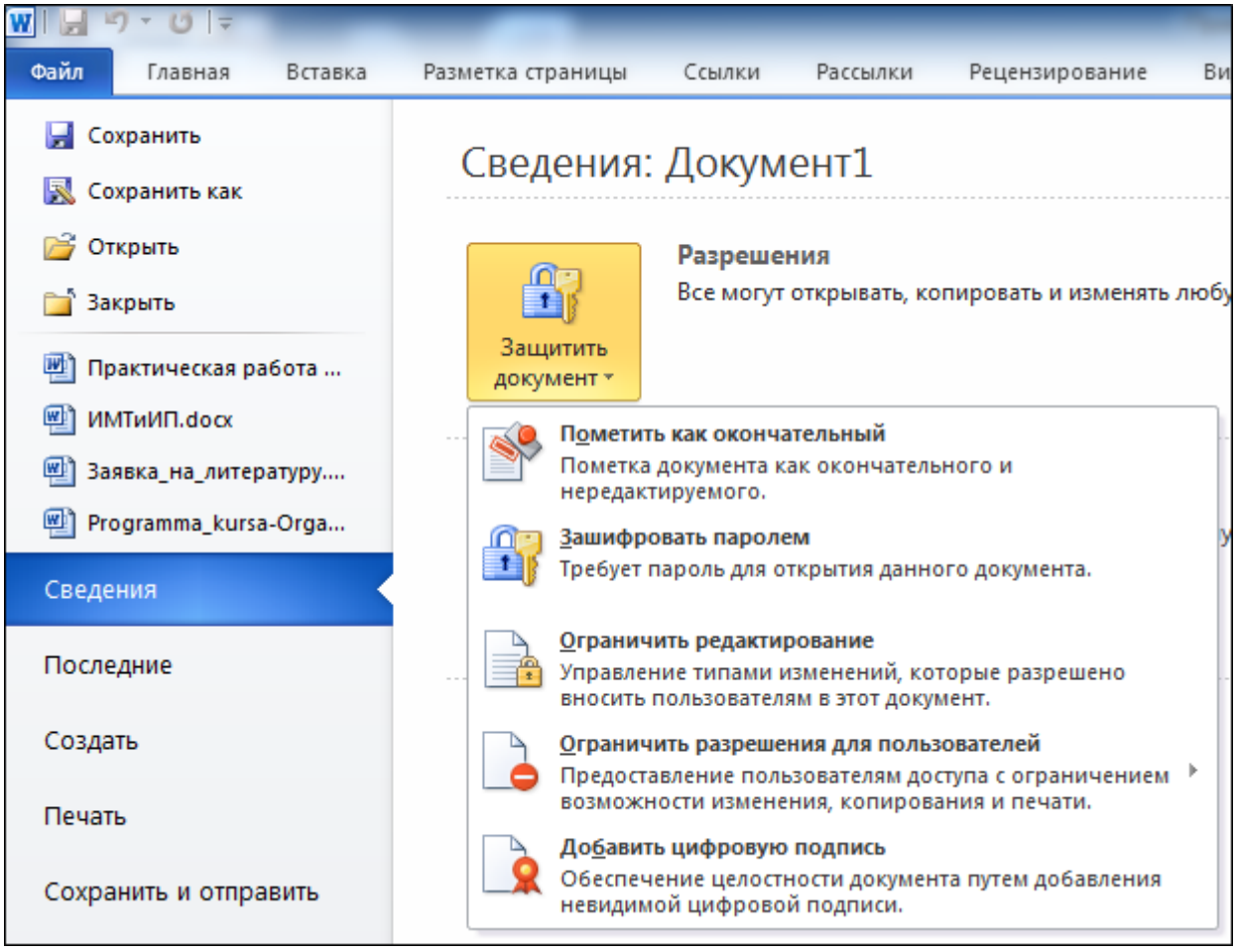


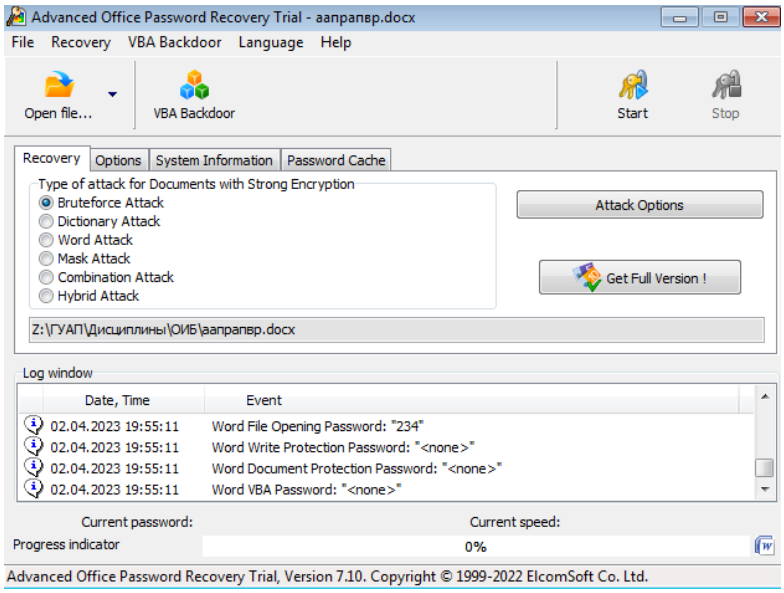
Рис. 1. Вкладка Файл / Сведения

Проверка стойкости паролей

Очень часто в организациях возникает проблема проверки стойкости паролей. Каждый сотрудник устанавливает пароли, исходя из своих личных предпочтений. Однако пароли, придуманные пользователями, могут оказаться нестойкими. Для проверки стойкости пароля можно использовать программу **Advanced Office Password Recovery** (https://www.elcomsoft.ru/aopr.html), поддерживающую документы всех версий Microsoft Office. При открытии документа программа автоматически определяет его версию и пароли, установленные в документе. Нестойкие пароли находятся мгновенно и отображаются, а для стойких паролей вначале применяется предварительная атака (preliminary attack), которая проверяет пароли по словарю, а также производит прямой перебор коротких паролей. Если пароль найден в результате этой атаки, он не является стойким. Далее надо проанализировать способ защиты, примененный к документу. Если защита совместима с Office , документ может быть расшифрован за несколько часов.

Восстановление забытых паролей

Очень часто пароли к документам теряются или забываются. Иногда уволившийся сотрудник оставляет набор документов, защищенных паролями. Для восстановления забытых паролей Microsoft Office можно использовать программы **Advanced Office Password Recovery и Elcomsoft Distributed Password Recovery**, которые позволяют находить стойкие пароли, используя при этом вычислительные мощности компьютеров, объединенных в сеть. Также при помощи этих программ можно гарантированно расшифровать документ, к которому применена защита, совместимая с Office; при этом скорость восстановления паролей напрямую зависит от количества задействованных компьютеров.



Варианты индивидуальных заданий к лабораторной работе.

Задание 1. Создайте документ в текстовом процессоре MS Word.
1.Запустите MS Word. Сохраните файл под именем «Ваша фамилия» (например: Иванов).
2.Вставьте в созданный документ стихотворение автора Агнии Барто указанного в таблице прил.1 (согласно своему номеру по списку). Сохраните файл.

Задание 2. Защитите документ паролем**.**

Для этого выполните действия:

1. Для открытого документа выберите вкладку *Файл / Сведения / Защитить документ / Зашифровать паролем*.

2. В окне *Шифрование документа*
(рис. 2) введите пароль (**пароль берется из приложения 2!!!).** Нажмите кнопку *ОК*.

Примечание: при вводе пароля следует строго следить за регистром и раскладкой клавиатуры нажатие на одни и те же клавиши клавиатуры в русской и английской раскладке вводит различные символы. Убедитесь в том, что при первом вводе пароля не нажата клавиша **[CAPS LOCK]**.

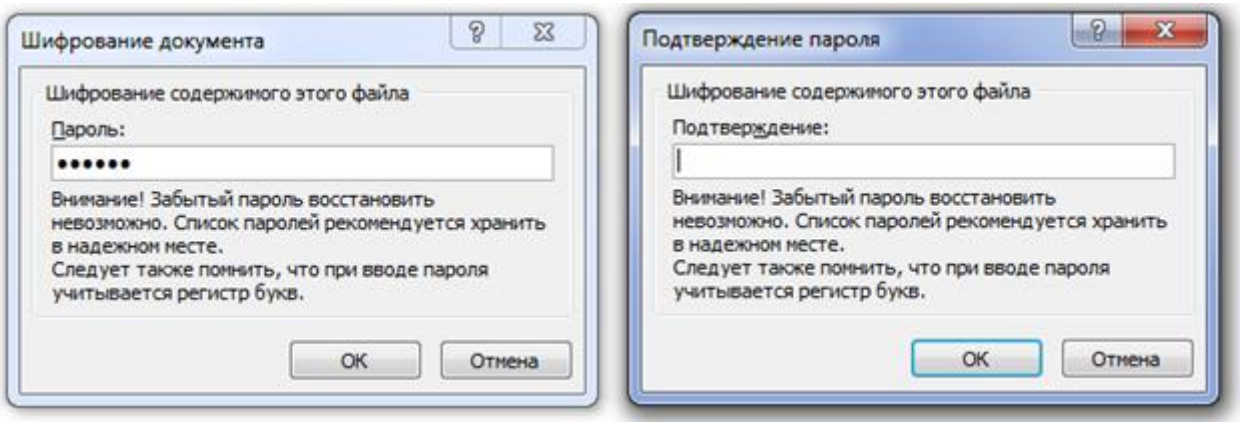


Рис. 2. Ввод и подтверждение пароля

3. В окне *Подтверждение пароля*
(рис. 2) введите пароль еще раз и нажмите кнопку ОК.

Примечание: пароль начнет действовать после сохранения и закрытия файла. В случае утраты пароля приложению MS Word не удастся восстановить данные. При открытии защищенного файла или снятии защиты выводится окно для ввода пароля, в котором необходимо ввести пароль. В случае неправильного ввода пароля выводится соответствующее сообщение. Следует нажать кнопку *ОК* и попытаться ввести правильный пароль.

4. Сохраните файл и закройте MS Word.

5. Проверьте успешность защиты документа паролем. Для этого:

– откройте ваш документ и введите неверный пароль в окне П*ароль* (рис. 3);

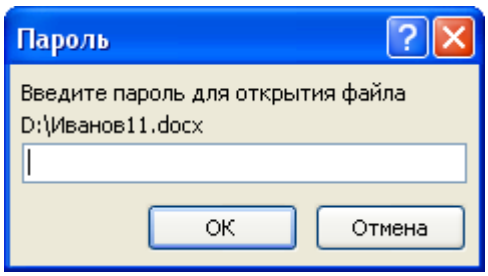


Рис. 3. Окно Пароль

– в ответ на ввод неправильного пароля проявить ошибка «Указан неверный пароль» (рис. 4). Нажмите кнопку *ОК* и закройте MS Word;

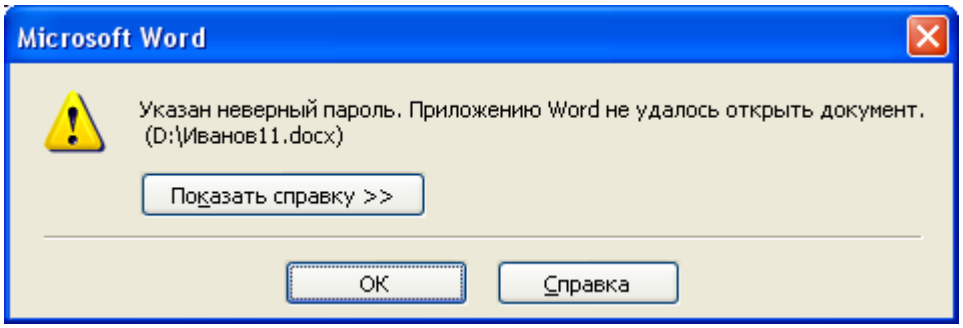


Рис. 4. Сообщение об ошибке

– откройте ваш документ и введите верный пароль в окне *Пароль* (рис. 4). При правильности ввода документ будет успешно открыт.

Задание 3. Снятие пароля с документа

Используя программы для восстановления забытых паролей Microsoft Office, например, **Advanced Office Password Recovery** **https://www.elcomsoft.ru/aopr.html** **(бесплатная версия)** или любые другие, попытаться восстановить «забытый» пароль от файла. Привести скриншоты работы программы. Проанализировать полученный результат.

Ответить на контрольные вопросы.

1. Можно ли распечатать документ с пометкой «Только для чтения»?
2. Можно ли скопировать фрагмент текста из документа, открытого как «Только для чтения» и сохранить его в новом документе без каких-либо паролей?
3. Что означает правило «нет чтения вверх»?
4. Как сохранить файл, открытый как документ «Только для чтения» после отказа от пароля на запись?
5. Какие используются криптоалгоритмы в Word/Excel 2007/2013?
6. Какова длина хеша пароля в данных программных продуктах Word/Excel 2007/2013?
7. Какие уязвимости шифрования Word/Excel 2007/2013 вы можете назвать?
8. Перечислите возможные атаки на Word/Excel/PowerPoint 2007/2013.
9. Назовите уязвимости шифрования Word/Excel/PowerPoint 2007/2013.
10. Как оценить время перебора паролей длины n?

Приложение 1

№ п/п	Название стихотворения
1.	Блинчики
2.	Болтунья
3.	Ботаника больна
4.	Буква «Р»
5.	Бычок
6.	В пустой квартире
7.	В театре
8.	В школу
9.	Важный пленник
10.	Веревочка
11.	Вот так защитник!
12.	Всё на всех
13.	Выборы
14.	Гуси-лебеди
15.	Две бабушки
16.	Две сестры глядят на братца
17.	Двояшки
18.	Дедушкина внучка
19.	Дело было в январе...
20.	Дикарка
21.	Докладчик
22.	Дом переехал
23.	Его семья
24.	Есть такие мальчики
25.	Жадный Егор
26.	Завитушки
27.	Зайка
28.	Зарядка
29.	Звенели птичьи голоса...
30.	Звонки

Приложение 2

№ п/п	Пароль
1.	123
2.	432
3.	134
4.	124
5.	112
6.	234
7.	421
8.	213
9.	214
10.	142
11.	114
12.	132
13.	223
14.	234
15.	456
16.	467
17.	456
18.	423
19.	345
20.	364
21.	245
22.	324
23.	456
24.	125
25.	237
26.	432
27.	345
28.	345
29.	222
30.	346