

«Практическая работа: *Лабораторная работа №2. Изучение работы макровируса*»

Выполнили:

студент группы 1ИСП11-18

Белякова А.А.

Ищенко Т.С.

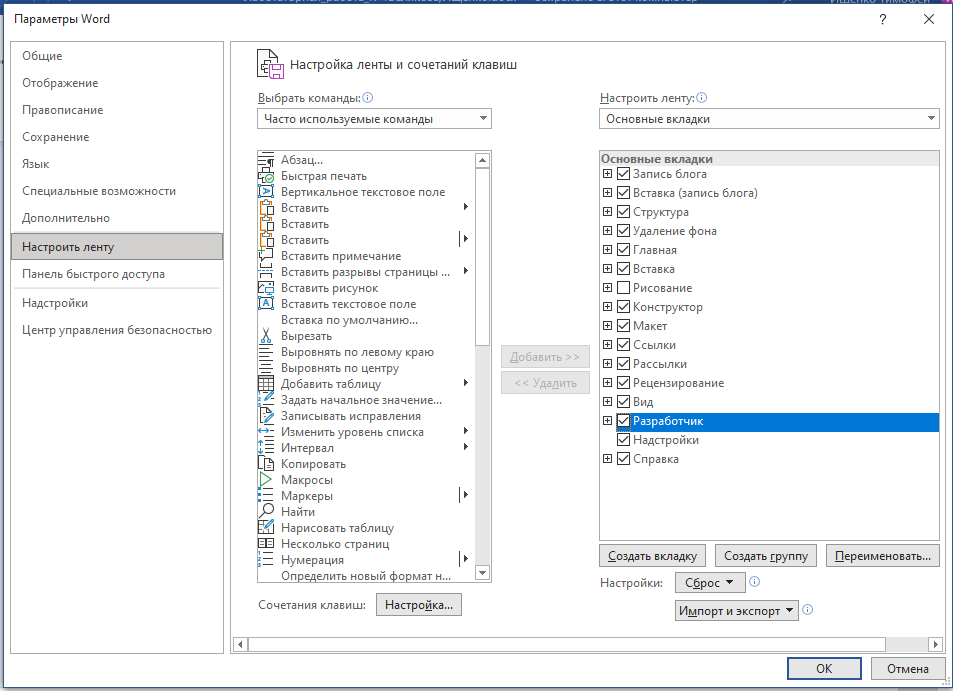
Проверил:

Возвахов Д.А.

Москва

2022

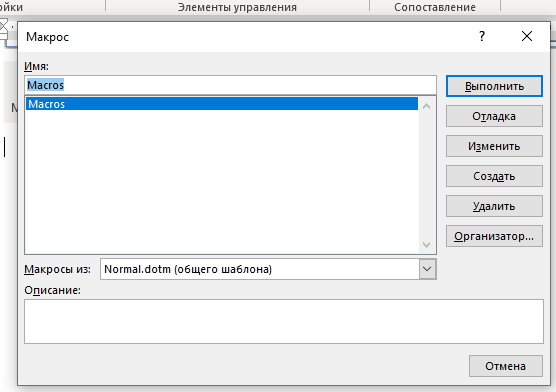
Включение панели “Разработчик” в MS Word.



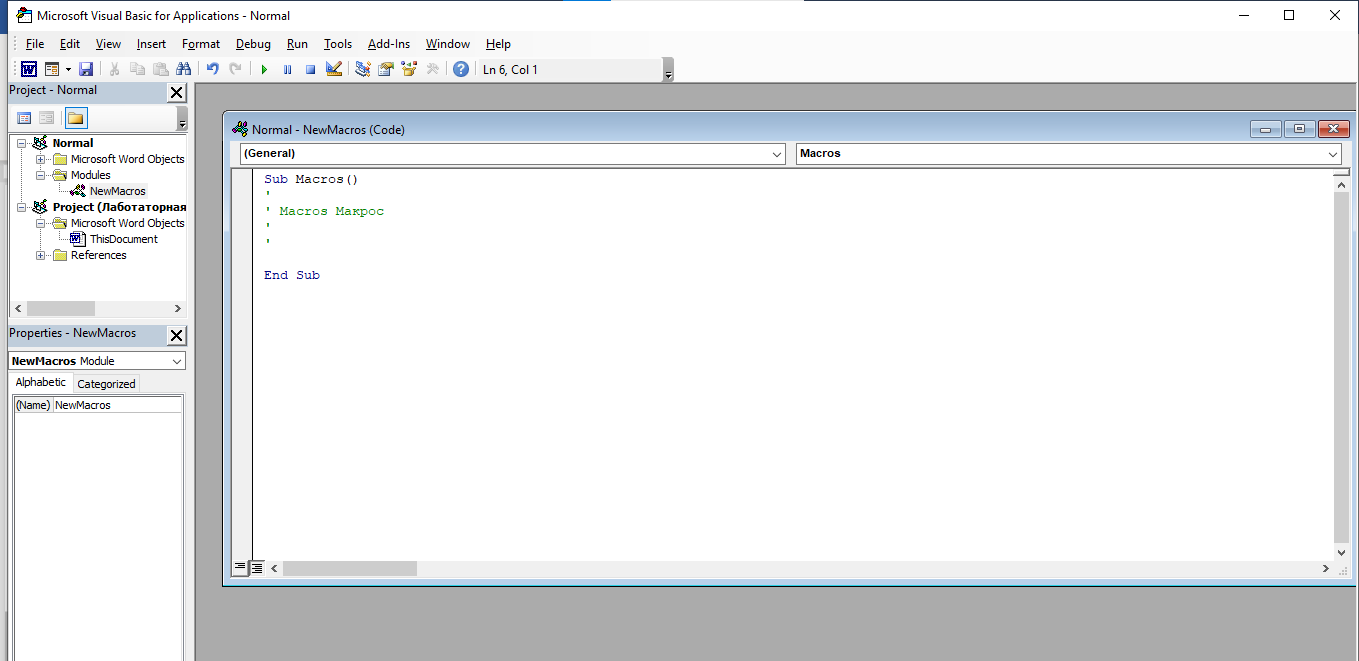
Нажимаем на вкладку “Макросы”.



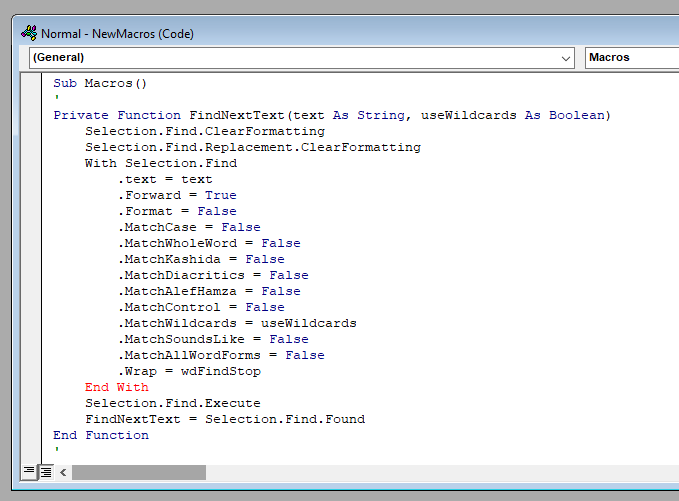
Создаём макрос.



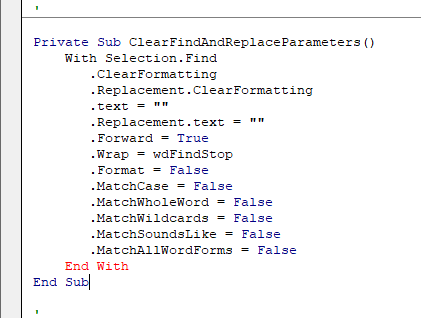
Открываем VBA редактор.



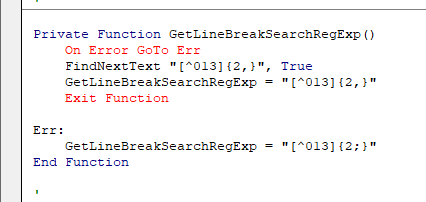
Создаём функцию FindNextText.



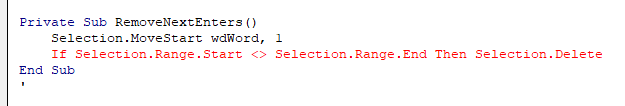
Создаём функцию ClearFindAndReplaceParameters.



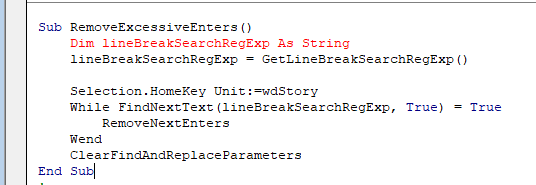
Создаём функцию GetLineBreakSearchRegExp.



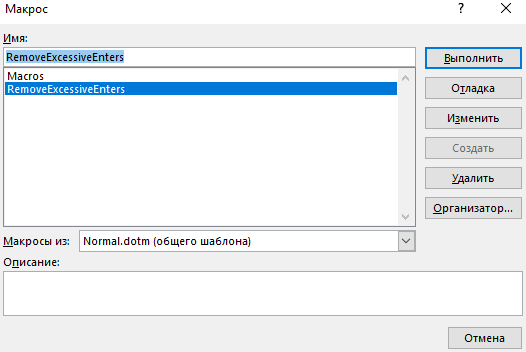
Создаём функцию RemoveNextEnters.



Создаём функцию RemoveExcessiveEnters.



Запускаем макрос.



Контрольные вопросы.

1. Назовите основные способы защиты от макровирусов.

Защита от макровирусов:

* Пользуйтесь надежными антивирусными программами с регулярно обновляемыми базами.
* Не полагайтесь на антивирусный монитор: всегда перед копированием и открытием проверяйте антивирусным сканером все исполняемые файлы и документы (особенно файлы на дискетах, флешки, компакт-дисках, полученные по Интернету).
* Почаще делайте резервное копирование, храните копии наиболее ценной информации на разных носителях (например, диски CD-RW, флешки и т.д.).
* Если вы работаете на ПК без антивируса, то рекомендуется сохранять и переносить Word’овские файлы в формате .rtf .
* Найдите шаблон Normal.dot, щелчком правойкнопки мыши вызовите контекстное меню, установите атрибут Только чтение –> OK. Это защитит шаблон от перезаписи (и заражения) макровирусами.
* Имейте в виду, что рекомендуемый некоторымиавторами запрет запуска макросов (меню Сервис –> Макрос –>Безопасность... –> диалоговое окно Безопасность –> вкладка Уровень безопасности –> Очень высокая –> OK) является полумерой, так как при этом не запрещается запуск макросов со стандартными именами (FileOpen, FileSave, FileSaveAs, FilePrint, AutoExec), то есть остается лазейка для макровирусов.

1. Опишите алгоритм, позволяющий обезвредить макровирус.

Как обезвредить макровирус.

Опишем алгоритм, позволяющий в большинстве

случаев обнаружить и обезвредить макровирус в MS Word.

Шаг 1. Лечение необходимо производить в "чистой",

т.е. заведомо не зараженной макровирусами среде MS Word. Для

этого завершим работу MS Word и при помощи какого-нибудь

файлового менеджера переименуем (или даже удалим) файл

NORMAL.DOT из каталога WINWORD.

Шаг 2. Вновь запустим MS Word. Программа

обнаружит отсутствие файла NORMAL.DOT и предложит

создать новый, "чистенький". Естественно, согласимся.

Шаг 3. В меню Файл (File) выберем альтернативу

Шаблоны (Template). Далее на последовательно появляющихся

окнах нажмем кнопки Организатор, Закрыть Файл и Открыть

Файл. В результате чего MS Word предложит загрузить один из

документов-шаблонов, в роли которых может выступать как

документ, предназначенный для лечения, так и

переименованный во время Шага 1 старый "главный" шаблон.

Загружаем.

Шаг 4. Выберем вкладку Макро и обнаружим на

экране список макросов, заключенных внутри загруженного

шаблона. Вирус (если он есть) скрывается именно среди них.

Если список пуст, значит вирус отсутствует.

Шаг 5. Если список не пуст, внимательно изучим его

содержимое. О наличии вируса с большой долей вероятности

свидетельствуют:

• макросы со "странными" именами, типа AAAZAO,

Cap, Mtfl и пр.;

• макросы со "стандартными" именами: AutoOpen,

AutoClose, AutoExec, AutoNew и пр.;

• макросы с "автоматическими" именами: FileOpen,

FileSave, FileSaveAs, FilePrint, FileExit, FileClose и пр.

Шаг 6. Обнаружив вирусные макросы, ликвидируем

их, поочередно отмечая мышью и нажимая кнопку [Удалить].

Шаг 7. Имеем прооперированный и теперь абсолютно

здоровый файл. Единственный недостаток (если мы лечили

документ, а не NORMAL.DOT) в том, что файл по-прежнему

остался шаблоном, и для него недоступна операция FileSaveAs.

1. Как происходит заражение компьютера макровирусом?

Когда мы открываем зараженный документ Word,

макровирус копирует свой код в область глобальных макросов

документа. А при выходе из Word глобальные макросы (включая

макросы вируса) автоматически записываются в dot-файл

глобальных макросов (шаблон Normal.dot). Затем вирус

переопределяет стандартные макросы (например, FileOpen,

FileSave, FileSaveAs, FilePrint) и с их помощью перехватывает

команды работы с файлами. При вызове этих команд заражается

файл, к которому идет обращение.

Для создания макровируса нужно запустить

Word, выбрать меню Сервис –> Макрос –> Редактор Visual

/Word Basic.

1. Что такое макрос?

Макрос - это программа, написанная на некотором

языке, которая используется обычно для автоматизации

определенных процессов внутри приложений. В настоящее

время большинство известных макровирусов написано на

Microsoft Word Basic и на Visual Basic for Application (VBA).

Microsoft Word Basic - это внутренний язык программирования

текстового процессора Windows Word (для версии 6.0 и 7.0) и

Word 6.0 for Macintosh. Макровирус, созданный с помощью

VBA, может заражать программы из пакета Microsoft Office

(таблицы Excel, базы данных Access, презентации PowerPoint).