

**Лабораторная работа №2 «Макровирусы»**

**Выполнил:**

студент группы 2ИСП11-18

Порядный Д.А.

**Проверил**: преподаватель Возвахов Д. А.

Москва

2022

**Установка вируса**

Установка вируса производится путём открытия заражённого файла MS 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.

**Удаление макровируса**

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.