

*Дисциплина: МДК*

**Практическая работа**

# **«Изучение работы макровируса»**

**Выполнили:**

Нечаев А. Ю.

**Проверил:**

Возвахов Д.А.

Москва

2022

**Установка вируса**

Макровирусы чаще всего встречаются в документах или вставляются как вредоносный код в программы обработки текстов. Они могут содержаться в документах, прикрепленных к электронным письмам, или код может быть загружен после нажатия «фишинговых» ссылок в баннерной рекламе или URL-адресах.

Их трудно обнаружить, так как они не работают до тех пор, пока не будет запущен зараженный макрос - тогда они выполняют ряд команд.

Макровирус похож на троянскую программу: он может выглядеть вполне безопасным, и пользователи не сразу замечают какие-либо вредоносные последствия. Однако в отличие от [троянских программ](https://www.kaspersky.ru/resource-center/threats/trojans) макровирусы могут копировать самих себя и заражать другие компьютеры.

**Удаление макровируса**

Для удаления макровируса первое, что предлагает Microsoft, – это использование хорошего антивируса, чтобы макросы не могли загружать вредоносные программы или отправлять нежелательную информацию с вашего компьютера. Запустите антивирусное программное обеспечение, если вам это необходимо.

Открывая документы Word, которые, по вашему мнению, могут содержать макро-вирус, нажмите Shift при открытии документа. Это предотвратит запуск любых макросов, так как документы Office запускаются в безопасном режиме, когда вы нажимаете Shift и открываете их. Затем вы можете проверить, какие все макросы присутствуют в документе. Если что-то выглядит подозрительно, вы можете удалить его перед использованием документа.

В последнее время Microsoft демонстрирует скачок в распространенности макровируса, используя электронную почту и социальную инженерию. На самом деле, некогда смертоносное макро-вредоносное ПО VBA также недавно возродилось.

***Регулярно выполняйте сканирование***

Даже если вы осторожны в Интернете, вы все равно можете ошибиться или столкнуться с новой и сложной схемой, которая обманом заставит вас загрузить макровирус. Важно [***выполнять регулярные проверки***](https://www.makeuseof.com/scan-for-viruses-without-buying-antivirus-software/) всякий раз, когда вы не используете свое устройство, чтобы отсеять любые подозрительные файлы, прежде чем они станут проблемой

**Контрольные вопросы**

2. **Примечание:** Этот метод может быть недопустим в текущих версиях Word, но его можно использовать в Word 1997.

Выберите вариант ***Макрос*** в ***инструменты*** > ***Создать новый макрос*** > ***Звоните***: AutoExec где нужно написать:

***Sub Main DisableAutoMacros MSGBOX «AutoMacros теперь выключены.», «Защита от вирусов», 64 End Sub***

1. Word также обеспечивает уровни безопасности для снижения заражения ваших документов макровирусами. Чтобы увеличить или уменьшить уровень безопасности, выполните следующие действия:

Перейти в меню ***инструменты*** > ***Макрос*** >***Безопасность***, На вкладке ***Уровень безопасности*** выберите нужный уровень безопасности и нажмите ***Ok***, Затем у вас будет возможность выбрать один из четырех уровней: низкий, средний, высокий и очень высокий.

1. Этот третий способ заключается в блокировке вашего Normal.dot паролем. Это позволяет снизить риск доступа макровирусов к вашим документам.

Для этого перейдите в меню ***инструменты*** > Макрос > ***Редактор Visual Basic*** и выбрать ***Этот документ*** в окне проекта. Так же, перейдите к ***инструменты*** > ***Свойства проекта***.

На вкладке ***Защита***, активировать окно ***Заблокировать проект, чтобы увидеть***, Введите пароль (советую использовать комбинацию букв, цифр, + специальных символов и заглавных букв). Пример надежного пароля***: UmN4t%^^p2tL123!***.

Введите тот же пароль в поле. ***подтвердить пароль*** и нажмите на ***Ok***, Перейти в меню ***архив*** и нажмите на ***Закройте и вернитесь в***[***Microsoft Word***](https://paradacreativa.es/ru/%D0%BA%D0%B0%D0%BA-%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D1%8C-%D1%81%D0%BB%D0%BE%D0%B2%D0%BE-Microsoft/).

нажмите [***ключ***](https://paradacreativa.es/ru/%D0%B8%D0%B7%D0%BC%D0%B5%D0%BD%D0%B8%D1%82%D1%8C-%D0%BD%D0%B0%D0%B7%D0%BD%D0%B0%D1%87%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BA%D0%BB%D0%B0%D0%B2%D0%B8%D1%88%D0%B8-%D0%BA%D0%BB%D0%B0%D0%B2%D0%B8%D0%B0%D1%82%D1%83%D1%80%D1%8B/)***Обмен*** и удерживайте его> ***архив*** > ***Сохранить все***.

Если появится следующее сообщение: ***Изменения были внесены в глобальную модель***.

***Сохранить эти изменения?***Нажмите на ***YES***.

1. Носить хороший [***антивирус***](https://paradacreativa.es/ru/%D0%B1%D0%B5%D1%81%D0%BF%D0%BB%D0%B0%D1%82%D0%BD%D1%8B%D0%B9-%D0%B0%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81-2/) регулярно обновляется для удаления таких вирусов. Запустите полное сканирование системы с помощью антивируса, чтобы обнаружить зараженные макросы.
2. Самый простой способ лечения – запуск антивирусной программы. Как правило, современный антивирус в числе прочих модулей содержит антивирусный монитор, постоянно загруженный в оперативную память. При попытке запуска или проверки файла, зараженного макровирусом, антивирус попытается вылечить файл (при неудачной попытке лечения – блокирует доступ к нему, т. е. не даст его открыть или скопировать).  
     
   Можно также воспользоваться загрузочным «аварийным» диском, содержащим антивирус со свежими базами (предварительно в BIOS нужно установить загрузку с CD-ROM'а). Загрузить антивирус, просканировать винчестер, найденные вирусы будут обезврежены.  
     
   Если антивирус не смог вылечить файл, зараженный макровирусом (что бывает очень и очень редко!), или приходится временно работать на ПК без установленного антивируса, или нет под руками загрузочного «аварийного» диска, а зараженный документ Word’а содержит ценную информацию и необходим, как воздух, – есть очень эффективный способ ручного лечения.  
     
   Сохраняем (не открывая!) документ Word в формате.Rtf (Rich text format), т. е. нужно поменять расширение файла.Doc на.Rtf. Если у вас не отображаются расширения, нужно запустить Проводник Windows, открыв любую папку, например, щелкнув по значку Мой компьютер. Выберите меню Сервис – Свойства папки… В открывшемся диалоговом окне Свойства папки откройте вкладку Вид. В прокручиваемом списке Дополнительные параметры снимите флажок со строки Скрывать расширения для зарегистрированных типов файлов. Нажмите OK.  
     
   Найдите файл, который нужно вылечить. Теперь в его названии отображается расширение.Doc. Поменяйте в названии файла расширение.Doc на.Rtf (текстовый формат.Rtf позволит сохранить всю необходимую информацию, включая текст, рисунки, таблицы; при этом VBA – надстройка файла, в которой гнездятся макровирусы, будет вычищена от программного кода макровируса). Появится предупреждение системы: «После смены расширения имени файла этот файл может оказаться недоступным. Вы действительно хотите изменить расширение? Да/Нет». Санкционируйте смену расширения, нажав Да.  
     
   Далее нужно удалить зараженный шаблон Normal. dot (после лечения при запуске Word шаблон Normal. dot будет создан заново) и другие зараженные шаблоны \*.Dot в следующих папках (для ОС Windows XP):  
   1) C : \Documents and Settings\Имя\_пользователя\Application Data\Microsoft\Шаблоны  
   2) C : \Documents and Settings\Имя\_пользователя\Application Data\Microsoft\Word\STARTUP  
   3) C : \Documents and Settings\Имя\_пользователя\Шаблоны  
     
   Расположение шаблонов для Windows 98/ME:  
   1) C : \WINDOWS\Application Data\Microsoft\Шаблоны  
   2) C : \WINDOWS\Application Data\Microsoft\Word\STARTUP  
     
   Меняем расширение файла.Rtf на.Doc. Устанавливаем обратно флажок Скрывать расширения для зарегистрированных типов файлов (Мой компьютер – Сервис – Свойства папки… – Вид – Дополнительные параметры): это нужно для того, чтобы у Вас не было неудобств с переименованием файлов. Работаем с файлом по обычной схеме.
3. Макровирусы, поражающие файлы Word, Excel или Office 97, как правило пользуются одним из трех нижеперечисленных приемов:

в вирусе присутствует автомакрос (автофункция);

в вирусе переопределен один из стандартных системных макросов (ассоциированный с каким-либо пунктом меню);

макрос вируса автоматически вызывается при нажатии на какую-либо клавишу или комбинацию клавиш.

Бывают также полувирусы, которые не используют перечисленные приемы и размножаются, только если пользователь самостоятельно запускает их на выполнение.

Большинство макровирусов содержат все свои функции в виде стандартных макросов MS Word/Excel/Office 97. Существуют, однако, вирусы, использующие приемы скрытия своего кода и хранящие свой код в виде не-макросов. Известны три подобных приема. Все они используют возможность макросов создавать, редактировать и исполнять другие макросы. Как правило, подобные вирусы имеют небольшой (иногда полиморфный) макрос-загрузчик, который вызывает встроенный редактор макросов, создает новый макрос, заполняет его основным кодом вируса, выполняет и затем, как правило, уничтожает, чтобы скрыть следы присутствия вируса. Основной код таких вирусов присутствует либо в теле самого вируса в виде текстовых строк, либо хранится в области переменных документа или в области Auto-text.

1. **Макрос** — это **действие или набор действий, которые можно выполнить сколько угодно раз**. При создании макроса записуются щелчки мышью и нажатия клавиш. После создания макроса его можно отредактировать, чтобы внести незначительные изменения в его работу.