

# Макровирус

<https://habr.com/company/dsec/blog/353800/>

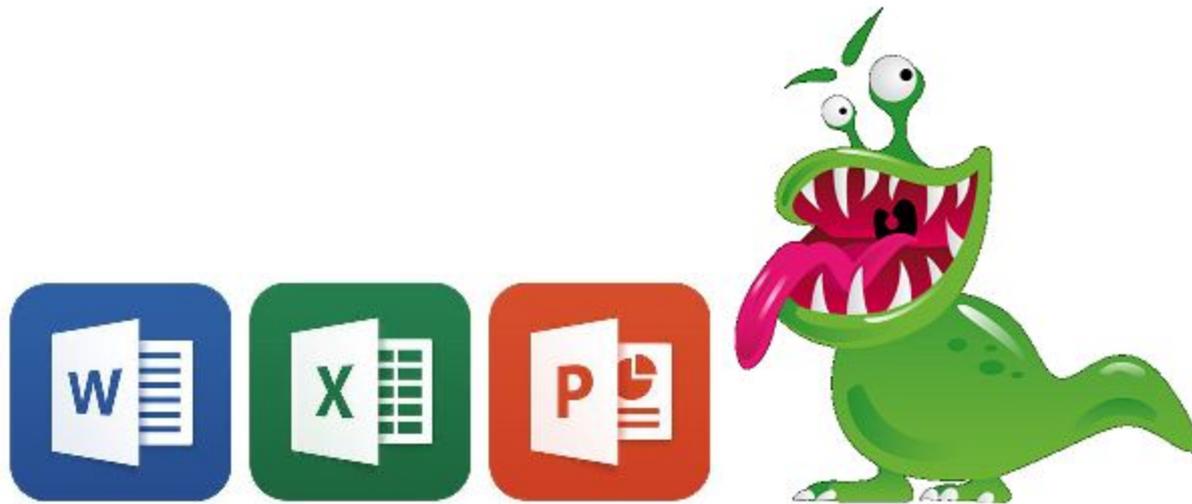
[Информационная безопасность,](#)  
[Блог компании «Digital Security»](#)

# Безопасность Microsoft Office: макросы VBA

- В 2016 году исследователи отметили всплеск активности, практически второе рождение, еще недавно казавшейся безнадежно устаревшей техники распространения нежелательного ПО — несущих злонамеренную нагрузку макросов в документах Microsoft Office, т.н. «**макровирусов**».

Самый знаменитый **макровирус, Melissa**, появился в марте 1999 года. Вирус поразил по крайней мере сто тысяч компьютеров по всему миру, парализовал работу сотен компаний, ущерб экономике составил 80 миллионов долларов в одних только США.

# Макровирусы «сегодня»



Судя по отчетам компаний, связанных с информационной безопасностью, на сегодняшний день макровирусы все еще занимают **верхние строчки в рейтингах по распространенности.**

# Что такое «макрос»

Так называемые «макросы» Microsoft Office представляют собой небольшие программы для интерпретируемого языка Visual Basic for Applications (VBA), поддержка которого встроена в линейку продуктов Microsoft Office.

Макросы в силу своих возможностей могут быть использованы для практически любой задачи автоматизации офисной работы.

# Какие программы поддерживают макросы VBA

- VBA охватывает все версии Microsoft Office для Windows, начиная с 1997г. и включая еще не вышедший 2019, а также некоторые другие приложения Microsoft, такие как MapPoint и Visio, и ПО других производителей: AutoCAD, CorelDraw, LibreOffice, Reflection, WordPerfect.

Реализована поддержка VBA и в Office for Mac OS X, за исключением 2008.

При выборочной установке Microsoft Office можно отказаться от поддержки VBA, но по умолчанию эта подсистема входит в набор устанавливаемых программ.

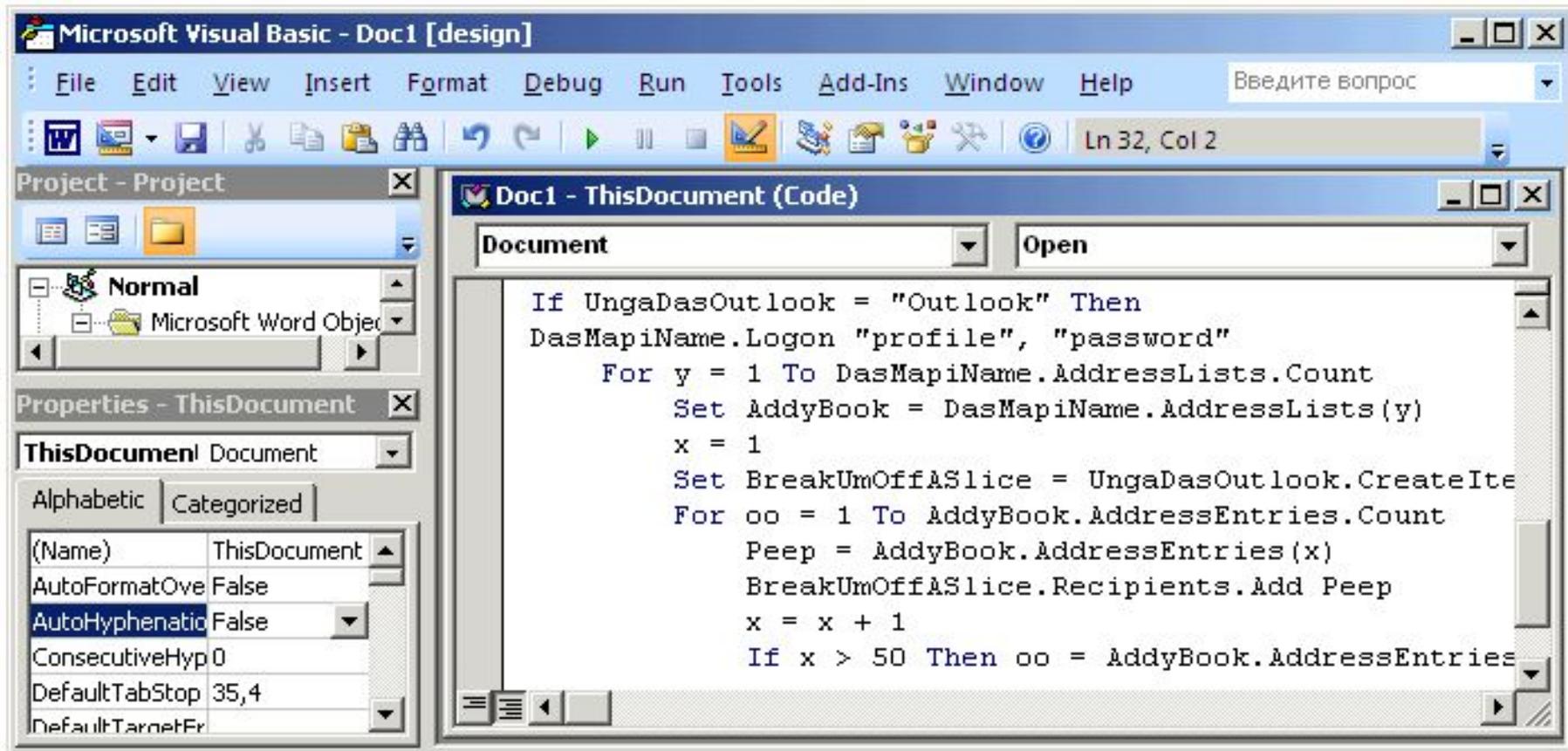
# Обход методов противодействия макровирусам

- 

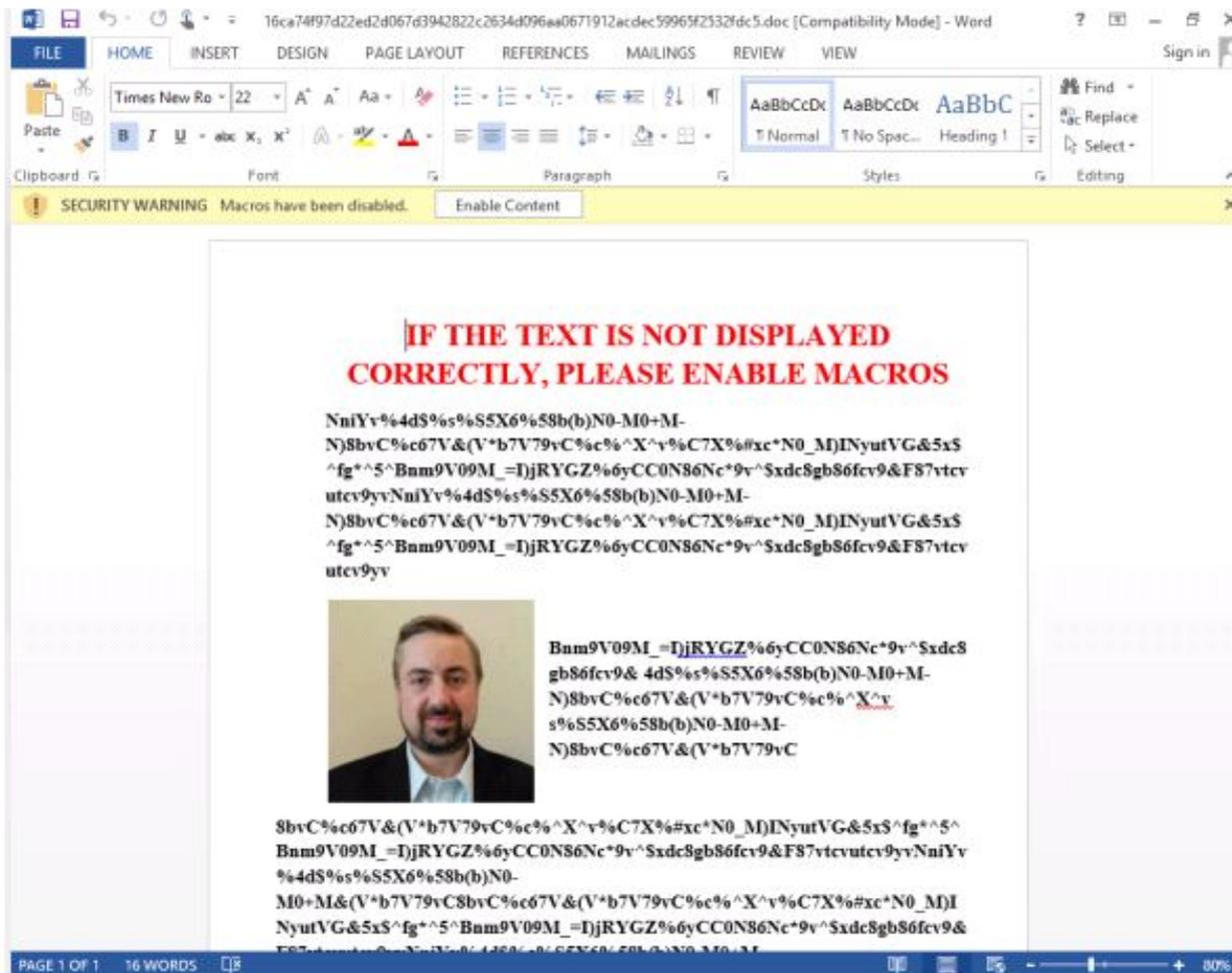
Большинство методов обхода механизмов безопасности строятся на **социальной инженерии**. Пользователи не воспринимают файлы Microsoft Office с макросами как исполняемые, поэтому легко вводятся в заблуждение демонстрацией ненормального открытия документа и приглашением пользователя включить макросы, чтобы устранить проблемы. Злоумышленники предоставляют подробные инструкции, на случай, если пользователи сами не могут догадаться как это сделать, и весомо выглядящее обоснование необходимости их включения.

На форумах соответствующей тематики можно встретить объявления о создании «индивидуальных дизайнерских решений» для оформления документов, призванных убедить пользователя включить активное содержимое. Стоимость таких решений может быть значительной, а эффективность, по мнению авторов, доходит до 60%.

# VBA



# Пример (ENABLE MACROS)



The screenshot shows a Microsoft Word window in Compatibility Mode. A yellow security warning banner at the top reads "SECURITY WARNING: Macros have been disabled." with an "Enable Content" button. The document content includes a red warning message: "IF THE TEXT IS NOT DISPLAYED CORRECTLY, PLEASE ENABLE MACROS". Below this, there are several paragraphs of text, some of which are partially obscured by a large, faint watermark. A small portrait photo of a man is visible, followed by more text. The status bar at the bottom indicates "PAGE 1 OF 1" and "16 WORDS".

**IF THE TEXT IS NOT DISPLAYED  
CORRECTLY, PLEASE ENABLE MACROS**

NniYv%4dS%\$%S5X6%58b(b)N0-M0+M-  
N)8bvC%c67V&(V\*b7V79vC%c%<sup>^</sup>X^r%<sup>^</sup>C7X%#xc\*N0\_M)INyutVG&5xS  
^fg\*^5^Bnm9V09M\_=IjjRYGZ%6yCC0N86Nc\*9v^Sxdc8gb86fcv9&F87vtcv  
utcv9yvNniYv%4dS%\$%S5X6%58b(b)N0-M0+M-  
N)8bvC%c67V&(V\*b7V79vC%c%<sup>^</sup>X^r%<sup>^</sup>C7X%#xc\*N0\_M)INyutVG&5xS  
^fg\*^5^Bnm9V09M\_=IjjRYGZ%6yCC0N86Nc\*9v^Sxdc8gb86fcv9&F87vtcv  
utcv9yv

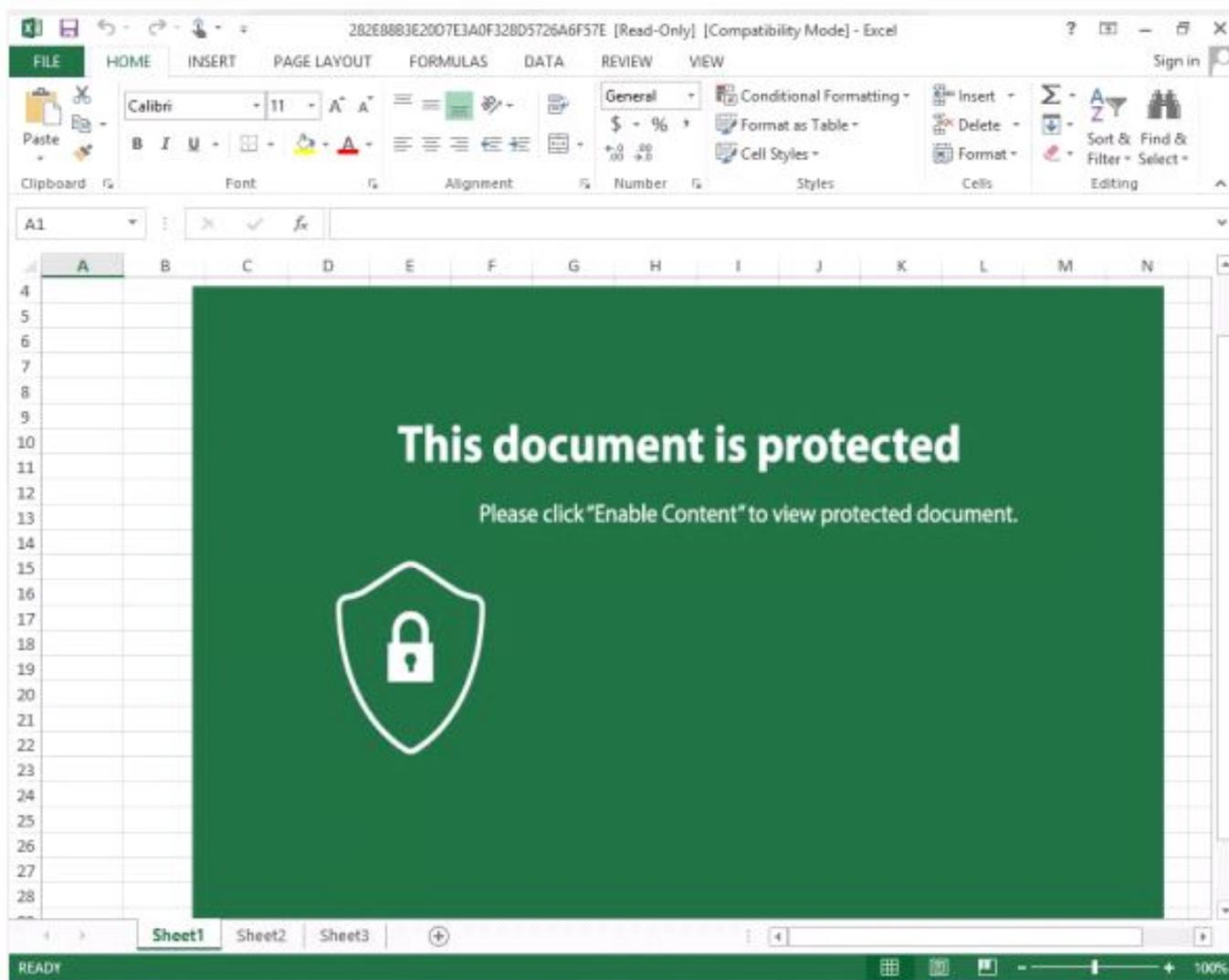


Bnm9V09M\_=IjjRYGZ%6yCC0N86Nc\*9v^Sxdc8  
gb86fcv9& 4dS%\$%S5X6%58b(b)N0-M0+M-  
N)8bvC%c67V&(V\*b7V79vC%c%<sup>^</sup>X^r  
s%\$S5X6%58b(b)N0-M0+M-  
N)8bvC%c67V&(V\*b7V79vC

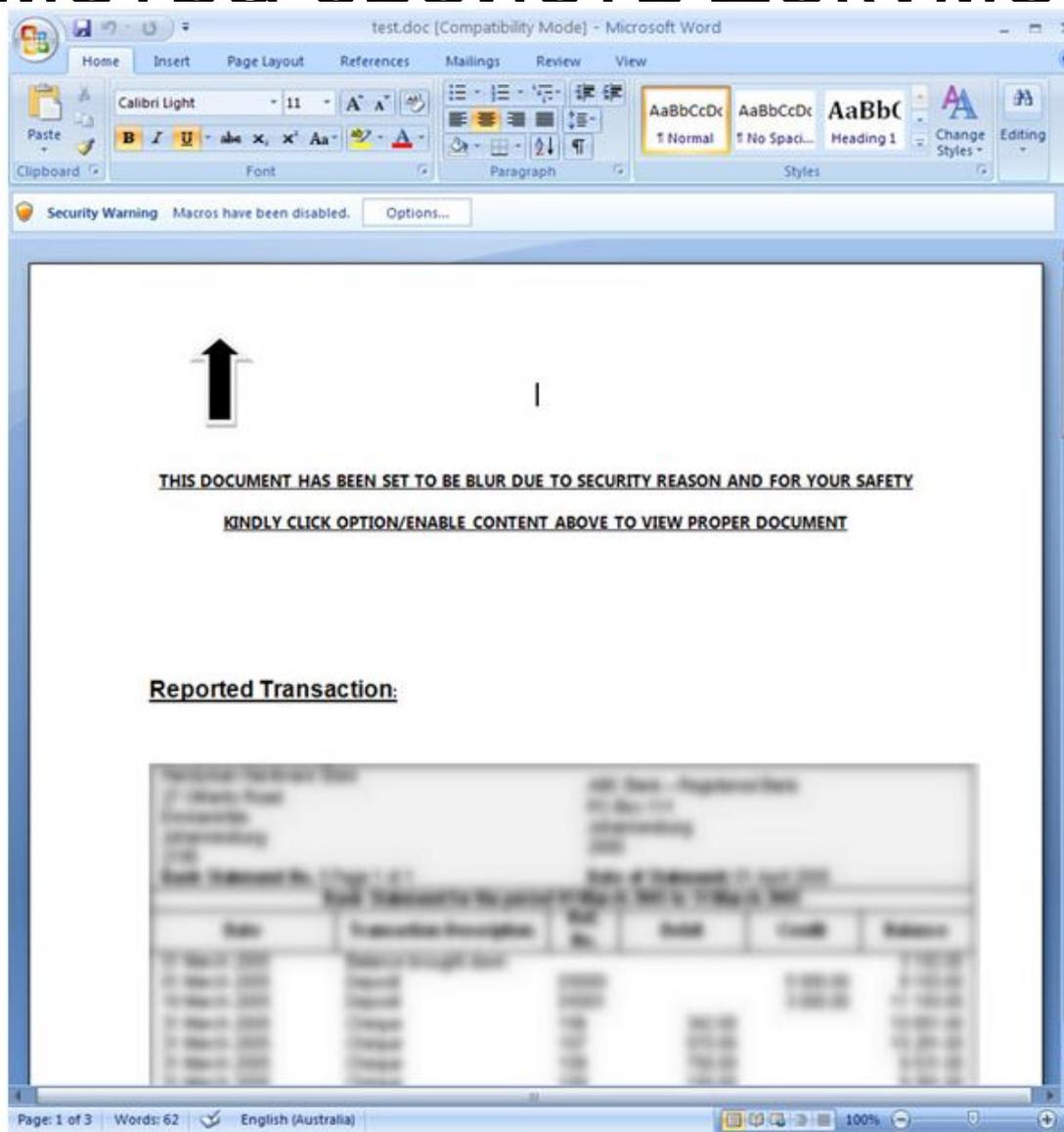
8bvC%c67V&(V\*b7V79vC%c%<sup>^</sup>X^r%<sup>^</sup>C7X%#xc\*N0\_M)INyutVG&5xS^fg\*^5^  
Bnm9V09M\_=IjjRYGZ%6yCC0N86Nc\*9v^Sxdc8gb86fcv9&F87vtcvutcv9yvNniYv  
%4dS%\$%S5X6%58b(b)N0-  
M0+M&(V\*b7V79vC8bvC%c67V&(V\*b7V79vC%c%<sup>^</sup>X^r%<sup>^</sup>C7X%#xc\*N0\_M)I  
NyutVG&5xS^fg\*^5^Bnm9V09M\_=IjjRYGZ%6yCC0N86Nc\*9v^Sxdc8gb86fcv9&  
F87vtcvutcv9yvNniYv%4dS%\$%S5X6%58b(b)N0-M0+M-

PAGE 1 OF 1 16 WORDS 80%

# Пример (click “Enable Content”) для просмотра защищенного



# Пример (click “Enable Content”) для просмотра свойств документа



# Как реализована поддержка VBA

- Код, созданный в редакторе VBA, сохраняется внутри файла документа. Документы современного формата Office Open XML, содержащие макросы, должны иметь специальное расширение (".docm", ".dotm", ".xlm", ".xlsm", ...), в противном случае приложение откажется их открывать. Внутри zip-архива документа проект VBA хранится в [файле-хранилище CFBF](#).

# Встроенные механизмы противодействия макровирусам

- Два механизма безопасности интегрированы непосредственно в приложения Microsoft Office:
  - \* Защищенный режим просмотра
  - \* Политики запрета исполнения макросов VBA.

# Защищенный режим просмотра

- В Microsoft Office есть защищенный режим, который активируется при просмотре файлов, **загруженных из интернета, запрещает запуск любого активного содержимого (в том числе, и макросов)** и создает ряд ограничений для процесса, который открывает этот документ. При открытии документа в таком режиме создается дочерний процесс (в котором и происходит просмотр документа) с пониженным уровнем целостности и ограничением Job на создание дочерних процессов (делается ограничением одного активного процесса в Job).

Эти ограничения, в первую очередь, направлены на предотвращение эксплуатации обычных бинарных уязвимостей в самом офисном приложении.

Изоляция процесса, отображающего документ в защищенном режиме, реализована в целом хорошо и заслуживает отдельного упоминания.

# Задание

- 1) Изучите методы защиты от макровирусов на сайте <https://habr.com/company/dsec/blog/353800>
- 2) Какие методы обхода защиты от макровирусов существуют?