

- [2] Brown, K., & Garcia, M. (2019). "Building Bridges: Leveraging Digital Platforms for Interdisciplinary Research in Computer Engineering Departments." Proceedings of the ACM Conference on Computer-Supported Cooperative Work and Social Computing, 255-268.
- [3] "Don't Make Me Think: A Common Sense Approach to Web Usability" - Steve Krug
- [4] "The Design of Everyday Things" - Don Norman
- [5] "About Face: The Essentials of Interaction Design" - Alan Cooper, Robert Reimann, David Cronin, Christopher Noessel
- [6] "Responsible Responsive Design" - Scott Jehl
- [7] "The Elements of User Experience: User-Centered Design for the Web and Beyond" - Jesse James Garrett
- [8] "Rosenfeld, L., & Morville, P. (2015). "Information Architecture: For the Web and Beyond." O'Reilly Media.
- [9] http://asoiu.edu.az/faculty_itif
- [10] <https://iconicdigitalworld.com/5-important-benefits-of-redesigning-a-website/>
- [11] <https://www.coursera.org/articles/ui-vs-ux-design>
- [12] <https://www.smashingmagazine.com/2011/01/guidelines-for-responsive-web-design/>

АТАКА СИСТЕМ ПОСРЕДСТВОМ МАКРОСОВ WORD ДОКУМЕНТОВ

Əsədov Əkbər, Əsgərov Taleh

Абстракт

Использование макросов в Microsoft Word может значительно упростить рутинные задачи для пользователей всех уровней навыков. От простого форматирования текста до более сложных операций, таких как слияние данных из различных источников или создание пользовательских функций. Макросы позволяют существенно повысить эффективность работы с документами. Как и любой мощный инструмент, использование макросов также может иметь свои риски. Некорректно написанные макросы или макросы с вредоносным содержимым могут представлять угрозу безопасности данных. Почему важно быть осторожным при загрузке и выполнении макросов из ненадежных источников покажет данная статья

Ключевые слова: Word документ, макрос, вредоносные документы, безопасность данных, социальная инженерия, компьютерный вирус

Введение

Приложения Microsoft Office, такие как Word и Excel, позволяют пользователям встраивать макросы[1], которые представляют собой серию команд и инструкций, сгруппированных вместе для программного выполнения задачи. Организации часто используют макросы для управления динамическим контентом и связывания документов с внешним контентом.

Макросы можно писать с нуля на Visual Basic для приложений (VBA)[2], мощном языке сценариев с полным доступом к объектам ActiveX[3] и узлу сценариев Windows, аналогичному JavaScript в HTML-приложениях.

В этой статье мы будем использовать встроенный макрос в Microsoft Word для запуска PowerShell при открытии документа. Макросы — один из старейших и наиболее известных векторов атак на стороне клиента. Они и сегодня хорошо работают, если нам удастся убедить жертву включить их.

Имейте в виду, что старые векторы атак на стороне клиента, включая динамический обмен данными (DDE)[4] и различные методы связывания и внедрения объектов (OLE)[5], сегодня не работают должным образом без существенной модификации целевой системы.

Цель

Целью данной статьи является демонстрация возможностей макросов в файлах Word для атаки на целевую систему с Windows. А так же в образовательных целях демонстрируется возможность создания Word файла с вписанным в него макросом исполняющим код для запуска PowerShell

Методология

Давайте углубимся и создадим макрос в Word. Мы создадим пустой документ Word с именем тутасго и сохраним его в формате .doc. Это важно, поскольку новый тип файла .docx не может сохранять макросы без прикрепления содержащего его шаблона. Это означает, что мы можем запускать макросы в файлах .docx, но не можем встраивать или сохранять макросы в документ. Другими словами, макрос не является постоянным. В качестве альтернативы мы также можем использовать тип файла .docm для нашего встроенного макроса.

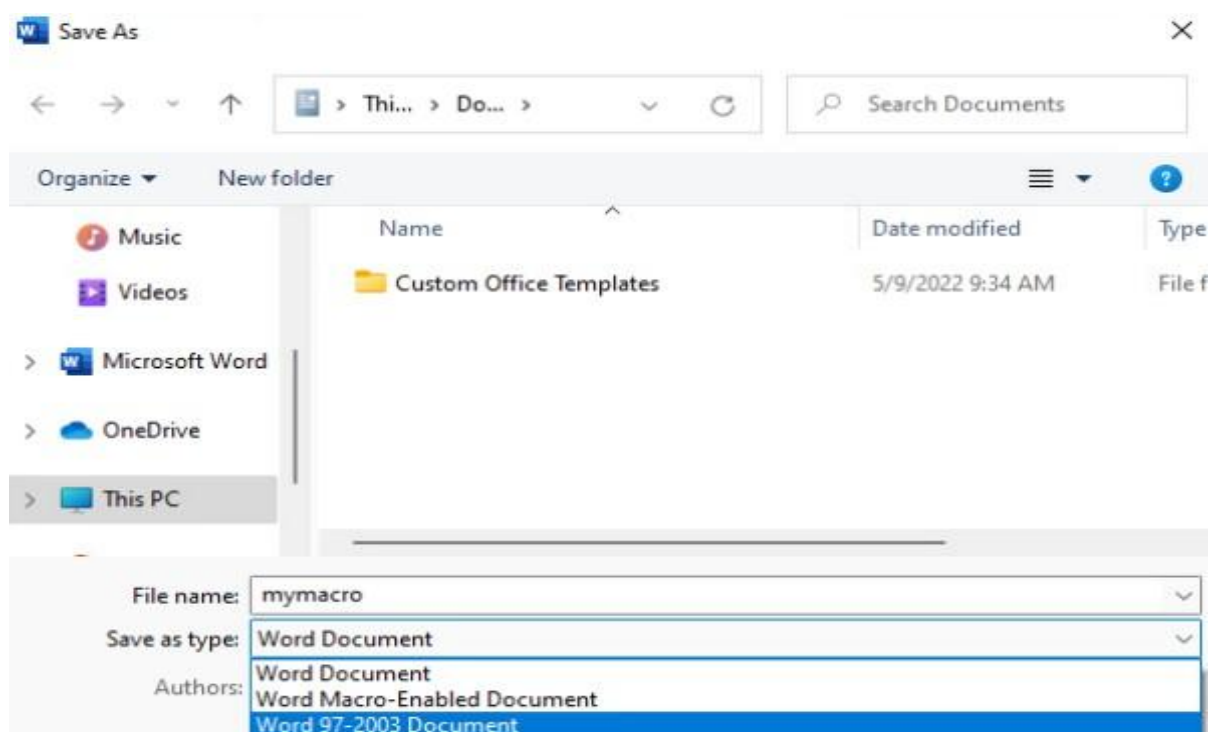


Рис. 1 – Создание документа.

После сохранения документа мы можем приступить к созданию нашего первого макроса. Чтобы перейти в меню макросов, мы щелкнем вкладку «Вид» в строке меню, где найдем и щелкнем элемент «Макросы»:

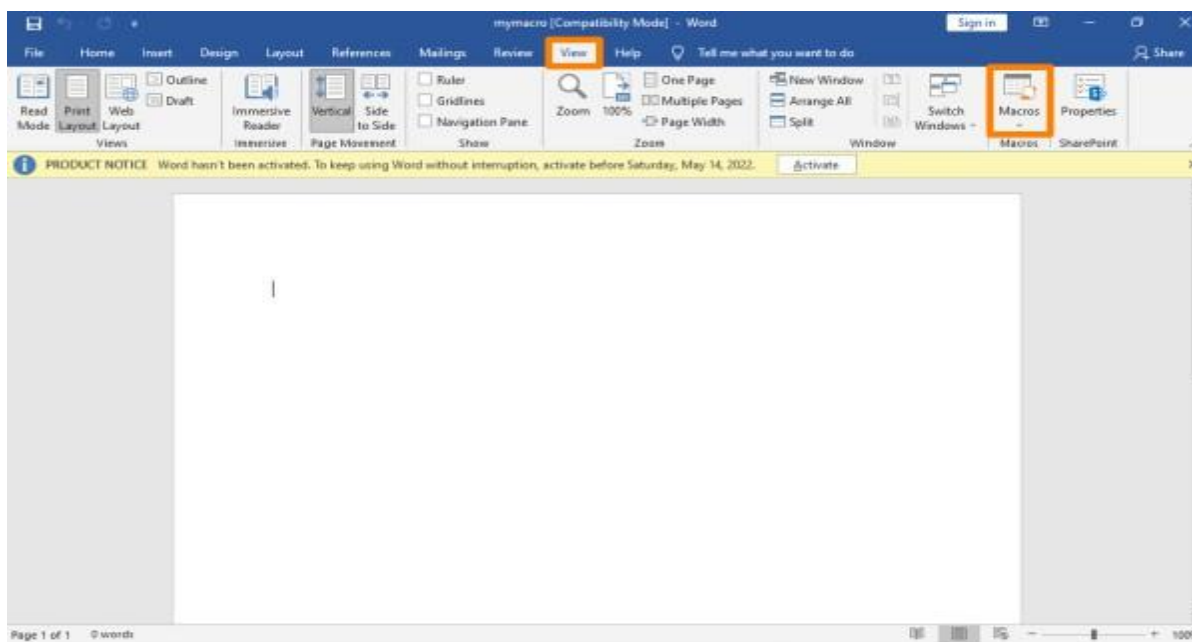


Рис. 2 – Расположение макросов в программе Word

Это открывает новое окно, в котором мы можем управлять нашими макросами. Давайте введем МуМасго в качестве имени в разделе «Имя макроса», а затем выберем документ тутасго в раскрывающемся меню «Макросы». Это документ, в котором будет сохранен макрос. Наконец, мы нажмем «Создать», чтобы вставить простую структуру макросов в наш документ.

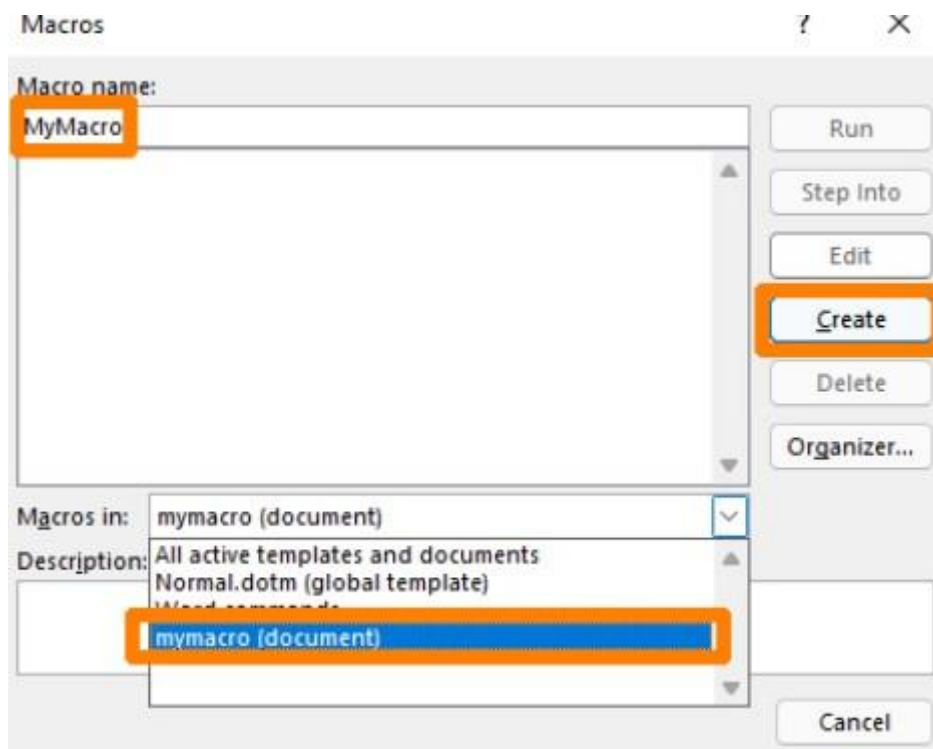


Рис 3. – Окно создания и редактирования макросов

Откроется окно Microsoft Visual Basic для приложений, в котором мы можем разработать макрос с нуля или использовать вставленный скелет макроса.

Давайте рассмотрим предоставленный скелет макроса. Основная процедура, используемая в нашем макросе VBA, начинается с ключевого слова Sub[6] и заканчивается End Sub. По сути, это обозначает тело нашего макроса.

Подпроцедура очень похожа на функцию в VBA. Разница заключается в том, что подпроцедуры нельзя использовать в выражениях, поскольку они не возвращают никаких значений, в отличие от функций. На данный момент наш новый макрос MyMacro() представляет собой просто пустую подпроцедуру, содержащую несколько строк, начинающихся с апострофа, который отмечает начало однострочного комментария в VBA.

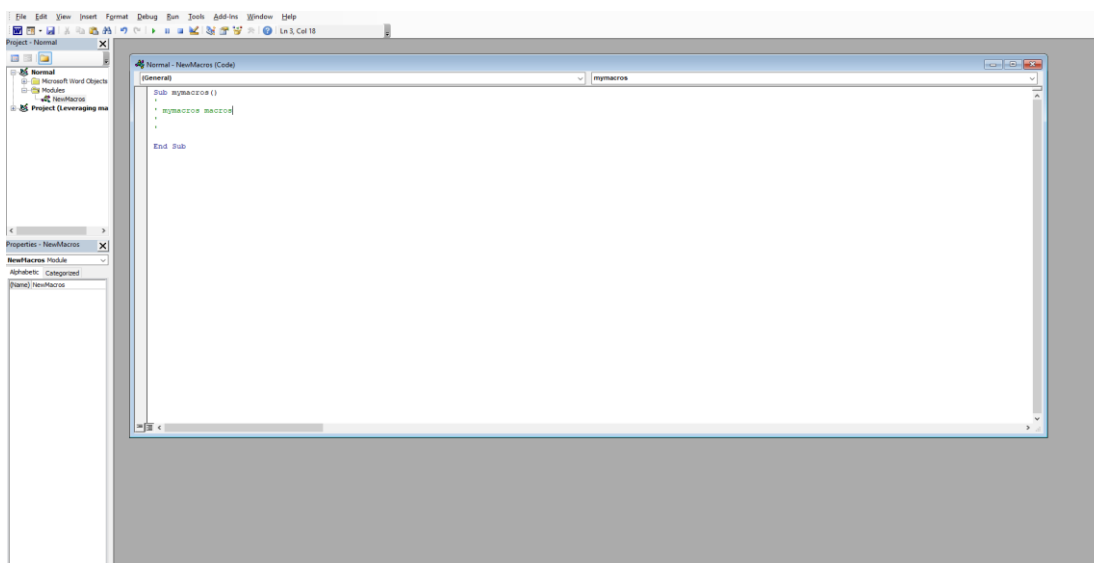


Рис 4. – Написание макроса

В этом примере мы будем использовать объекты ActiveX[7], которые обеспечивают доступ к базовым командам операционной системы. Этого можно достичь с помощью WScript[8] через объект Windows Script Host Shell[9]. Создав экземпляр объекта оболочки Windows Script Host Shell посредством CreateObject[10], мы можем вызвать метод Run[11] для Wscript.Shell, чтобы запустить приложение на целевом клиентском компьютере. Для нашего первого макроса мы запустим окно PowerShell. Код этого макроса показан ниже.

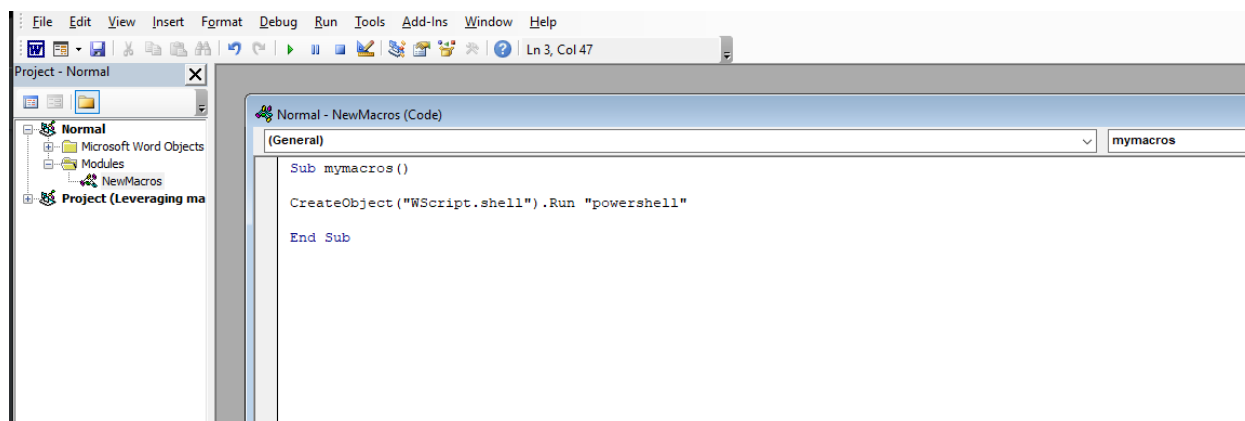
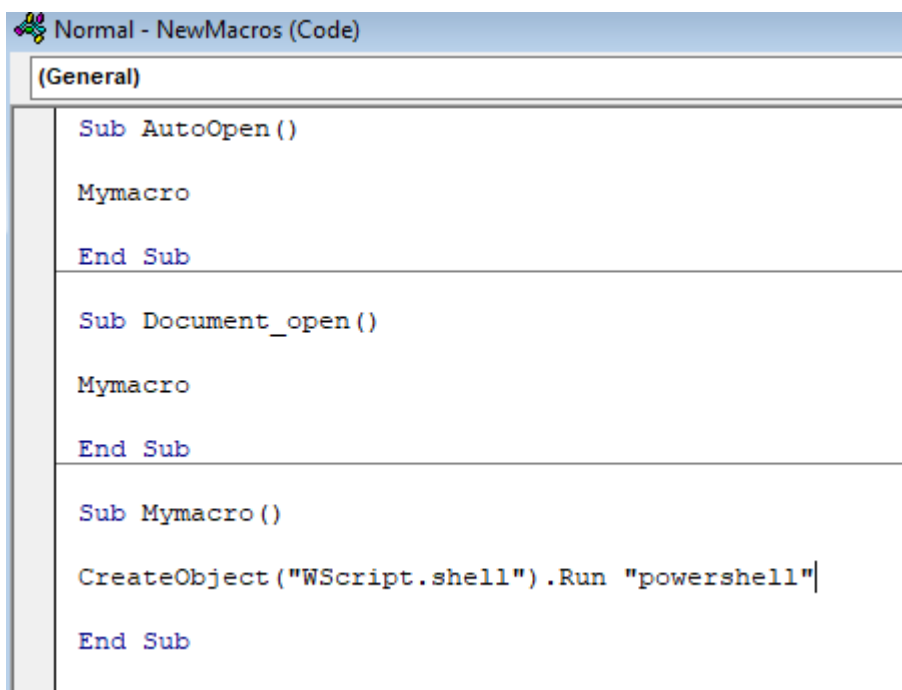


Рис 5. – Пример кода макроса.

Поскольку макросы Office не выполняются автоматически, мы должны использовать предопределенный макрос AutoOpen и событие Document_Open. Эти процедуры могут вызывать нашу пользовательскую процедуру и запускать наш код при открытии документа Word. Они незначительно отличаются в зависимости от того, как был открыт Microsoft Word и документ. Оба охватывают особые случаи, которых нет в другом, поэтому мы используем оба.

Наш обновленный код VBA показан ниже:



```
Sub AutoOpen()  
Mymacro  
End Sub  
  
Sub Document_open()  
Mymacro  
End Sub  
  
Sub Mymacro()  
CreateObject("WScript.shell").Run "powershell"  
End Sub
```

Рис 6. – Дописанный макрос, открывающийся при открытии документа.

Затем мы щелкнем значок «Сохранить» в окне Microsoft Visual Basic для приложений и закроем документ. После того, как мы снова откроем его, нам будет показано предупреждение системы безопасности, указывающее, что макросы отключены. Чтобы запустить наш макрос, мы нажмем «Включить контент».

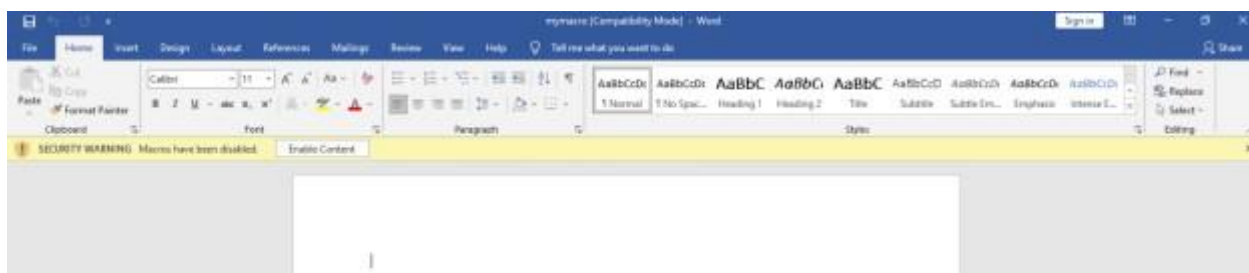


Рис 7. - Предупреждение о макросах Microsoft Word

После того, как мы нажмем «Включить контент», появится окно PowerShell:

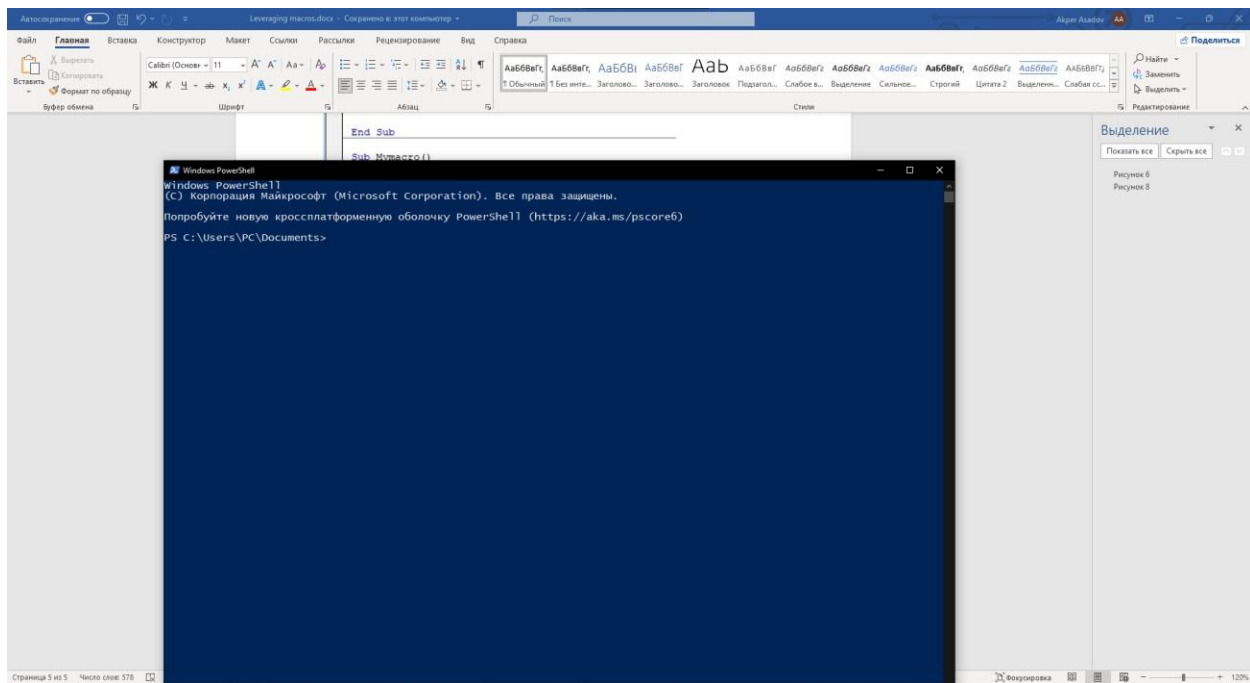


Рис 8. – Работа кода макроса при открытии Word документа.

Как показано на рис. 8, окно PowerShell было запущено с помощью нашего макроса.

Закключение

Важно соблюдать осторожность при работе с макросами, особенно при загрузке и выполнении их из ненадежных источников. Только при правильном и безопасном использовании макросы могут стать надежным помощником в повседневной работе с документами. Однако, несмотря на их потенциальную полезность, макросы также могут представлять серьезные угрозы для безопасности данных и системы в целом. Вредоносные макросы могут быть спрятаны в документах или электронных таблицах и запускаться автоматически при их открытии. Это может привести к заражению компьютера вредоносным программным обеспечением, краже личных данных или даже к разрушительным последствиям для всей сети. Поэтому очень важно доверять источникам, из которых вы загружаете макросы, и активировать их только в случае необходимости, а также иметь актуальное антивирусное программное обеспечение. Кроме того, следует быть внимательным при работе с макросами, особенно если они запрашивают доступ к важным системным ресурсам или файлам. Использование цифровой подписи или кодовой подписи для макросов может быть еще одним способом обеспечить их безопасность. Это позволит убедиться, что макросы были созданы и подписаны надежным источником, что уменьшит риск заражения вредоносным кодом.

Литература

- [1] Microsoft Support, 2019 // <https://support.office.com/en-us/article/Create-or-run-a-macro-C6B99036-905C-49A6-818ADFB98B7C3C9C>
- [2] Microsoft Documentation, 2021 // <https://docs.microsoft.com/en-us/office/vba/api/overview/>
- [3] Wikipedia, 2022 // <https://en.wikipedia.org/wiki/ActiveX>
- [4] Microsoft, 2020 // <https://docs.microsoft.com/en-us/windows/win32/dataxchg/about-dynamic-dataexchange?redirectedfrom=MSDN>

- [5] Wikipedia, 2021 // https://en.wikipedia.org/wiki/Object_Linking_and_Embedding
- [6] Microsoft Documentation, 2022 // <https://docs.microsoft.com/en-us/office/vba/Language/Concepts/Getting-Started/calling-suband-function-procedures>
- [7] Microsoft Documentation, 2018 // <https://docs.microsoft.com/en-us/previous-versions/windows/desktop/automat/activex-objects>
- [8] Microsoft Documentation, 2015 // [https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/iedeveloper/windows-scripting/at5ydy31\(v=vs.84\)](https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/iedeveloper/windows-scripting/at5ydy31(v=vs.84))
- [9] Microsoft Documentation, 2015 // [https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/iedeveloper/windows-scripting/aew9yb99\(v=vs.84\)](https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/iedeveloper/windows-scripting/aew9yb99(v=vs.84))
- [10] Microsoft Documentation, 2022) // <https://docs.microsoft.com/en-us/office/vba/Language/Reference/User-InterfaceHelp/createobject-function>
- [11] Adersoft VBSEdit, 2022 // <http://www.vbsedit.com/html/6f28899c-d653-4555-8a59-49640b0e32ea.asp>

DEVELOPMENT OF AN INFORMATION SYSTEM FOR AN OIL PRODUCING ENTERPRISE

Asif Huseynov Etibar
Azerbaijan State Oil and Industry University

Abstract

The process of developing a study has been laid that covers the deep analysis of the entity's workflow, obstacles, and goals followed by the development of an informational system architecture. By applying sophisticated technologies like cloud computing, big data analytics, and IoT integration the system attempts to enhance the efficiency of oil and gas producing processes, including exploration scouting, drilling, extraction, refining, distribution and maintenance. Main functionalities of the system include real-time monitoring and production process control, predictive maintenance to render the downtimed small and resources' utilization criteria as enhanced, intelligent reservoir management for high production, supply chain optimization for efficient resource distribution, and compliance for meeting industry regulations and standards.

Introduction

The world's economy is largely based on oil that is a nerve of transport, manufacturing and invisibility, and this is the surest evidence that all the sectors are dependent on the oil industry. With the increase in global population and industrialization, the demand of oil and its derivatives increasingly raises as it becomes the main source for driving the engines of economic motor. Due to this, most international oil corporations need to turned toward the technology of efficiency, sustainability, and profitability. In this light, the creation of information technology which would provide an efficient solution addressing the unique problems and unwieldy task of oil production becomes indispensable. It is about efficient control of all stages of the production of oil on a drilling rig by offering such solutions as exploration, drilling, extraction, and refining. Through implementing of advanced technology and data analytics and information management methodologies the oil & gas companies may gain totally new capabilities which will enable the country to face all the challenges of market changes, regulatory requirements, and environment constraints. As oil production ultimately evolve into sophisticated information system as opposed to a mere technological upgrade, it displays a fundamental power towards an adaptive, data-centric and sustainable energy production. The world in the process of replacing conventional energy sources with the cleaner and more effective ones, the oil companies that lead in innovation and utilize information technology will become the champions of energy.

Major challenges in oil production