Д. Н. Бирюков,
доктор технических наук, доцент;
О. О. Захаров;
П. В. Тимашов

ПОДХОД К СНИЖЕНИЮ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫХ С ПРИМЕНЕНИЕМ МАКРОСОВ В ОФИСНЫХ ДОКУМЕНТАХ

Рассмотрена проблема распространения вредоносного программного обеспечения с помощью макросов в офисных документах. Проанализированы существующие политики и механизмы безопасности офисных пакетов. Предложен подход к построению средства защиты, учитывающий недостатки в существующих механизмах. Реализован прототип, подтверждающий применимость подхода в реальных условиях. Выдвинуты предложения по настройке операционных систем семейства Windows для обеспечения безопасной работы с документами.

Ключевые слова: защита информации, вредоносное программное обеспечение, компьютерные атаки, информационная безопасность.

ВВЕДЕНИЕ

В повседневной жизни возникает множество рутинных задач, которые требуют автоматизации. Это касается и работы с офисными приложениями, например, при обработке внешних файлов, отправке документов через Интернет и др. Для их автоматизации в офисных пакетах (*Microsoft Office, LibreOffice* и т. д.) предусмотрены макросы – программные алгоритмы действий, записанные пользователем. Однако, как и любые технологии, макросы можно использовать как для полезной деятельности, так и для вредоносной, что открывает широкие возможности не только для рядовых пользователей, но и для нарушителей информационной безопасности.

Офисные документы широко используются злоумышленниками для распространения вредоносных программ по всему миру. Документы *Microsoft Office* являются наиболее применимым типом файлов для доставки вредоносного программного обеспечения под операционные системы семейства *Windows* [1]. Основная причина того, что эти файлы часто применяются в таких компаниях, заключается в том, что сотрудники в организациях постоянно обмениваются ими. Следовательно, пользователи с большей вероятностью загрузят и откроют полученный документ, даже от неизвестного отправителя, чем, например, файл исполняемого или «экзотического» формата. По этой причине злоумышленники применяют их для первоначального проникновения на целевую машину, а затем приступают к дальнейшему заражению хоста.

Вредоносные документы используют подсистему макросов для загрузки и выполнения полезной нагрузки. Некоторые защитные решения, несмотря на то, что учитывают этот вектор атаки, зачастую неэффективно блокируют его.

В данной статье рассматриваются возможности макросов, способы защиты от вредоносных макросов в документах, политики безопасности, написание собственного упрощенного макроса, подход к созданию программного комплекса обнаружения таких документов, полученных из сети Интернет.

ОБЗОР ВОЗМОЖНОСТЕЙ ПОДСИСТЕМЫ МАКРОСОВ И ВСТРОЕННЫХ МЕХАНИЗМОВ ЗАЩИТЫ НА ПРИМЕРЕ MICROSOFT OFFICE

Макросы представляют собой программы, написанные на интерпретируемом языке VBA, поддержка которого есть в линейке продуктов *Microsoft Office*. Кроме продуктов *Microsoft*, данный язык поддерживают *LibreOffice*, *CorelDraw*, *AutoCAD* и некоторые другие малоизвестные редакторы. По умолчанию VBA входит в набор устанавливаемых программ при установке *Microsoft Office*, но есть возможность отказаться от его поддержки.

Макросы позволяют получать доступ [2] к следующим объектам:

– содержимому документа;

– интерфейсу офисного приложения и действиям пользователя в нем (например, нажатиям клавиш);

– ресурсам операционной системы при помощи COM и WMI объектов

Указанные возможности подсистемы макросов позволяют автоматизировать рутинные задачи (например, для вставки шаблонов требуется доступ к содержимому документа). Записать макрос для взаимодействия с интерфейсом офисного приложения без разработки позволяют встроенные средства (рис. 1).

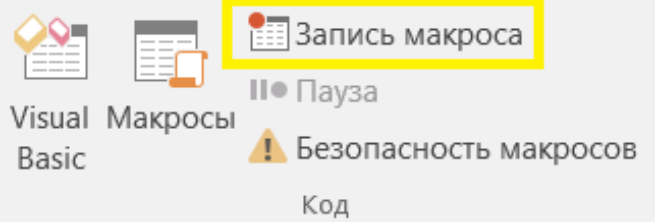

Рис. 1. Кнопка записи макросов на панели быстрого доступа

Доступ к ресурсам операционной системы позволяет сохранять файлы, автоматически отправлять документы по почте и выполнять другие задачи автоматизации. Именно доступ к данным ресурсам позволяет злоумышленникам запускать код на компьютере пользователя – скачивать, запускать и удалять файлы (т. е. *выполнять практически любые действия*).

В *Microsoft Office* существуют встроенные механизмы безопасности:

– защищенный режим просмотра;

– политики запрета исполнения макросов VBA;

– надежные расположения.

В защищенном режиме просмотра запрещается запуск любого содержимого, создается ряд ограничений на процесс, который открывает этот документ. После открытия создается дочерний процесс, аналогично – с рядом ограничений, в котором происходит просмотр документа (рис. 2).

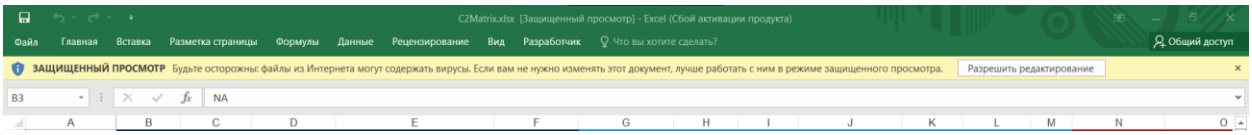

Рис. 2. Оповещение о работе в режиме защищенного просмотра

Политики запрета исполнения макросов VBA позволяют выбрать, какие действия необходимо произвести, как оповестить пользователя или заблокировать исполнение макроса (рис. 3).

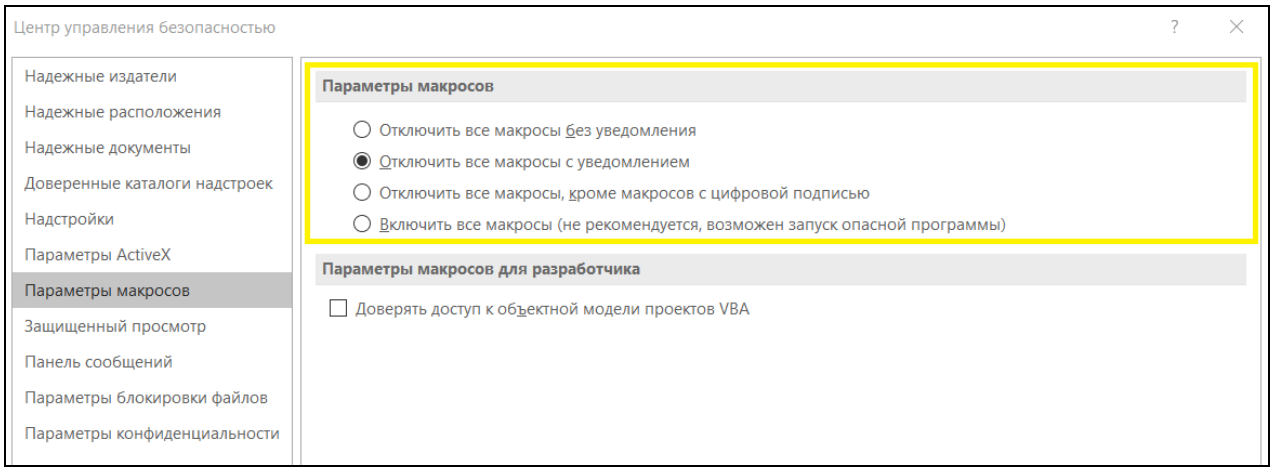

Рис. 3. Управление политикой запрета исполнения макросов

В случае использования опции по умолчанию «Отключить все макросы с уведомлением» при открытии документа с макросом пользователь будет оповещен (рис. 4).

Рис. 4. Предупреждение об отключенном запуске макросов

К файлам из надежных расположений не применяется проверка активного содержимого и режим защищенного просмотра, макросы и код выполняются *без предупреждения*.

ПОЛИТИКИ БЕЗОПАСНОСТИ И ОГРАНИЧЕНИЯ, СВЯЗАННЫЕ С БЕЗОПАСНОСТЬЮ MICROSOFT OFFICE

Операционные системы семейства *Windows* позволяют различным образом настраивать системы для уменьшения вероятности заражения через вредоносные документы *Microsoft Office*. Для этого используются групповые и облачные политики *Office*, некоторые из них могут соответствовать тем, что описаны выше. Рассмотрим их возможности и требования в табл. 1 и 2.

Таблица 1

Групповые политики*

Политика безопасности	Описание	Требования	Примечание
Настройка уведомлений о макросах VBA	Определяет вид предупреждений, отображаемых в случае наличия макросов	*Microsoft* Office 2003 и выше; *Windows* 2000 и выше; *Windows Server* 2000 и выше	Отключить все с уведомлением. Отключить все, кроме макросов с цифровой подписью. Отключить все без уведомления. Включить все макросы
Показывать вкладку «Разработчик» на ленте	Если этот параметр политики отключен, вкладка «Разработчик» не будет отображаться на ленте		

Окончание табл. 1

Политика безопасности	Описание	Требования	Примечание
Отключить команды	Если этот параметр включен, можно ввести идентификатор, чтобы отключить конкретную кнопку или пункт меню на панели команд		Идентификаторы кнопок и элементов меню, связанных с макросами, для каждого продукта доступны с целью скачивания на официальном сайте производителя [3]
Отключить VBA для приложений Office	Запрещает приложениям *Office* использовать компонент *Visual Basic* для приложений (VBA)		
Надежные расположения	К файлам в надежных расположениях не применяются проверка файлов, проверки активного содержимого и режим защищенного просмотра. Макросы и код в этих файлах будут выполняться без вывода предупреждений для пользователя	*Microsoft Office* 2007 и выше	
Блокирование запуска макросов в файлах *Microsoft Office*, полученных через Интернет	Если включить этот параметр политики, макросы будут блокироваться, даже если в разделе «Параметры макросов» в центре управления безопасностью выбран параметр «Включить все макросы»	*Windows Server* 2008 R2 и выше; *Windows* 7 и выше; *Microsoft Office* 2016 и выше	
Настройка правил уменьшения поверхности атаки	Позволяет предотвращать подозрительную активность от приложений Microsoft Office	*Windows* 10 *Pro*, корпоративная (версии 1709 и выше); *Windows Server* (версии 1803 и выше), 2012 R2, 2016, 2019, 2022	Блокировка запуска исполняемого контента приложениями из пакета *Office*. Блокировка внедрения кода в другие процессы приложениями из пакета *Office*. Блокировка вызовов Win32 API из приложений *Office*. Блокировка создания дочерних процессов приложениями *Office*. Уникальные идентификаторы для правил размещены на официальном сайте производителя [4]
Запускать антивирусную проверку во время выполнения	Определяет, когда файлы Office проверяются в среде выполнения с помощью установленной антивирусной программы	*Windows Server* 2016; *Windows* 10; Приложения *Microsoft* 365 для предприятий;	

* Для групповых политик требуются шаблоны (**.adm*, **.admx*). Данные файлы доступны на официальном сайте производителя [5].

Таблица 2

Сервис облачных политик для Office

Политика безопасности	Описание	Требования	Примечание
Отключение VBA для приложений *Office*	Отключает макросы для всех приложений из пакета *Microsoft Office*	*Microsoft* 365 *Apps* для корпораций 1808 версии и выше. Пользователи должны войти в *Microsoft* 365 *Apps* с *Azure Active Directory* аккаунтом. Разрешить доступ в Интернет ряду доменных имен и IP-адресов. С полным списком можно ознакомиться на официальном сайте производителя [6]	
Настройка уведомлений о макросах VBA	Определяет вид предупреждений, отображаемых в случае наличия макросов		Аналогично групповой политике
Запускать антивирусную проверку во время выполнения	Определяет, когда файлы *Office* проверяются в среде выполнения с помощью установленной антивирусной программы		

Кроме того, существует решение управления мобильными устройствами (MDM) на *Windows* 11, 10 в различных вариантах поставки. С его помощью появляется возможность настраивать правила *Windows* ASR. Также с апреля 2022 года начинается рассылка обновления для *Microsoft Office*, которое по умолчанию отключает все макросы в документах, полученных из Интернета [7]. Это существенный шаг на пути уменьшения количества атак, проводимых с помощью вредоносных документов.

Стоит упомянуть тот факт, что «**.docx*» не поддерживает макросы – только «**.docm*» [8]. Их значки (иконки) заметно различаются, и это может помочь пользователю распознать угрозу (рис. 5). Предыдущий формат «**.doc*» поддерживает макросы. Данная особенность присуща и другим типам документов *Microsoft Office*.

Рис. 5. Значки документов Microsoft Word («.docm», «*.docx», «*.doc»)*

ПРИМЕРЫ ОБХОДА ВСТРОЕННЫХ МЕХАНИЗМОВ ЗАЩИТЫ И ОГРАНИЧЕНИЙ

Несмотря на все применяемые меры по защите от вредоносных офисных документов, существуют способы обхода данных ограничений, которые позволяют выполнить код на компьютере.

Обходу ограничений может способствовать применение методов *социальной инженерии* (рис. 6).

Пользователь получает по почте или иному каналу связи документ, при открытии которого отражается уведомление, что он «защищен» или «для просмотра его содержимого необхо-

димо нажать на кнопку «Включить содержимое», что приведет к выполнению макроса. Обычно, для того, чтобы документ выглядел правдоподобно после выполнения макроса, злоумышленники предусматривают изменение содержимого документа – пользователь увидит, что документ изменился после нажатия кнопки, но никакой действительно важной информации находиться не будет.

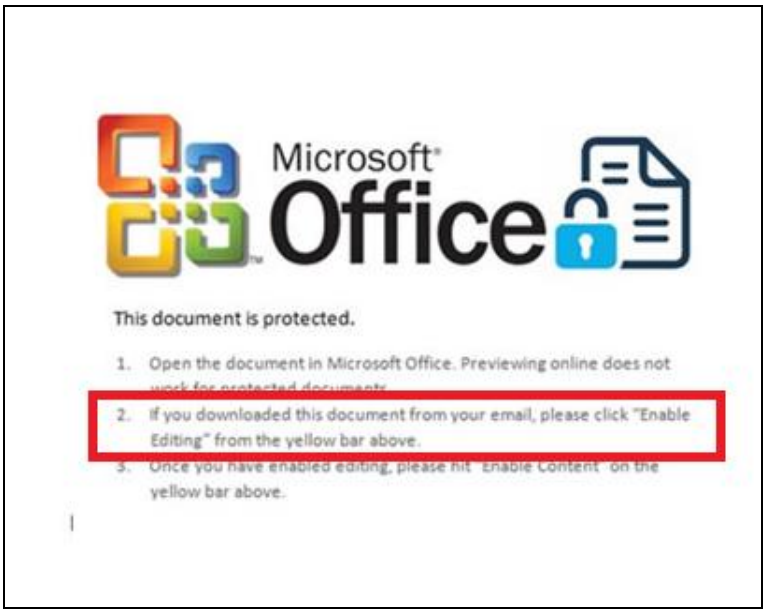

Рис.6. Пример содержимого вредоносного документа с макросом

С технической точки зрения социальная инженерия является самым действенным способом обхода ограничений на выполнение макросов. Но даже если у злоумышленника получилось убедить пользователя запустить макрос, есть вероятность того, что защитные средства определят макрос как вредоносное ПО. Для уменьшения шанса быть обнаруженными средствами защиты киберпреступники зачастую прибегают к обфускации кода макроса. Обфускация кода представляет собой изменение исходного текста программы к виду, сохраняющему функциональность, но затрудняющему анализ. На рис. 7,*а* и *б* представлен фрагмент кода на *JavaScript* для демонстрации возможностей обфускаторов кода.

```
function Hello() {
  console.log("Тест обфускации");
}
Hello();
```

```
(function(_0x3ff558,_0x2b8033){var _0x670285=_0x2c2f,_0x2bcaac=_0x3ff558();while(!![]){try{var _0x391e5c=-parseInt(_0x670285(0x8f))/0x1+-
parseInt(_0x670285(0x8c))/0x2+parseInt(_0x670285(0x92))/0x3+-parseInt(_0x670285(0x8e))/0x4+parseInt(_0x670285(0x88))/0x5*
(parseInt(_0x670285(0x90))/0x6)+parseInt(_0x670285(0x8a))/0x7*
(parseInt(_0x670285(0x8d))/0x8)+parseInt(_0x670285(0x91))/0x9;if(_0x391e5c===_0x2b8033)break;else _0x2bcaac['push'](_0x2bcaac['shift']
());}catch(_0x111faf){_0x2bcaac['push'](_0x2bcaac['shift']());}}}(_0x5e9f,0xc677a));function _0x5e9f(){var _0x3c1945=
['396560rEfwja','8UfljxJ','2755560cTpLPN','731655loGXAp','3714stZEID','917721HzEPXk','1726638hwAWoG','1475oxezOX','Тест\x20обфускации','
11001389oYcSMV','log'];_0x5e9f=function(){return _0x3c1945;};return _0x5e9f();}function _0x2c2f(_0x1b63ec,_0x47bef1){var
_0x5e9fec=_0x5e9f();return _0x2c2f=function(_0x2c2f54,_0x187964){_0x2c2f54=_0x2c2f54-0x88;var _0x416432=_0x5e9fec[_0x2c2f54];return
_0x416432;},_0x2c2f(_0x1b63ec,_0x47bef1);}function Hello(){var _0x14eda6=_0x2c2f;console[_0x14eda6(0x8b)](_0x14eda6(0x89));}Hello();
```

Рис. 7. Код до обфускации (*а*) *и после обфускации* (*б*)

Для обфусцирования кода макросов существует множество утилит, находящихся в открытом доступе. Примером подобной программы является *Macro Pack* [9].

Кроме того, исследователями были найдены недостатки в реализации технологии *Windows* ASR, упомянутой выше [10]. Несмотря на то, что корпорация *Microsoft* постоянно совершенствует данный механизм защиты, приведенные в исследовании способы позволяли успешно обходить ограничения и реализовывать различные вредоносные сценарии.

МЕХАНИЗМЫ БЕЗОПАСНОСТИ АНАЛОГОВ MICROSOFT OFFICE

Существуют аналоги *Microsoft Office*:

1. МойОфис.
2. *LibreOffice*.
3. *Open Office*.

Подсистема макросов пакета МойОфис не поддерживает взаимодействие с *Component Object Model* (COM) и внешними DLL [12]. Это позволяет избежать вредоносных воздействий на рабочую станцию посредством макросов. *LibreOffice* и *Open Office* имеют схожие механизмы безопасности:

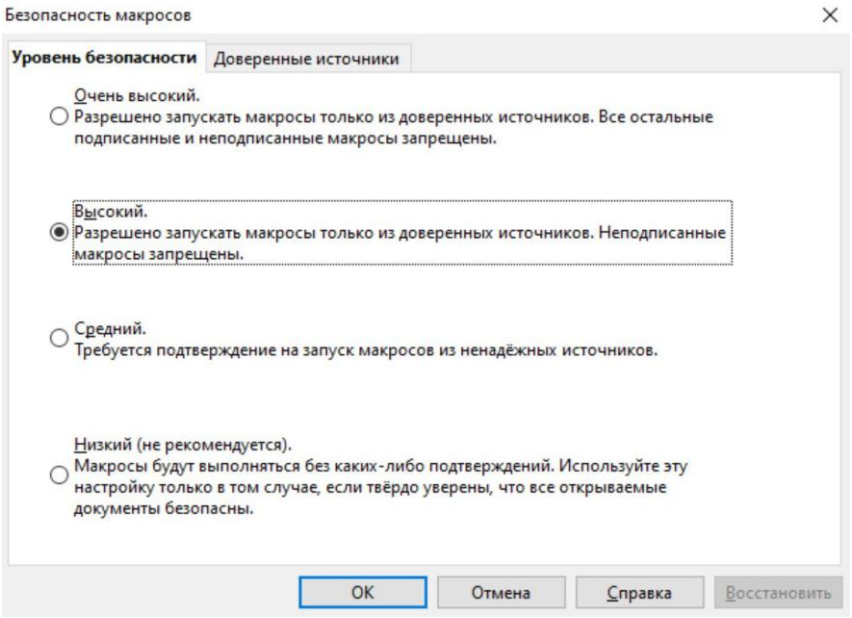

Рис. 8. Настройка уровней безопасности в LibreOffice/Open Office

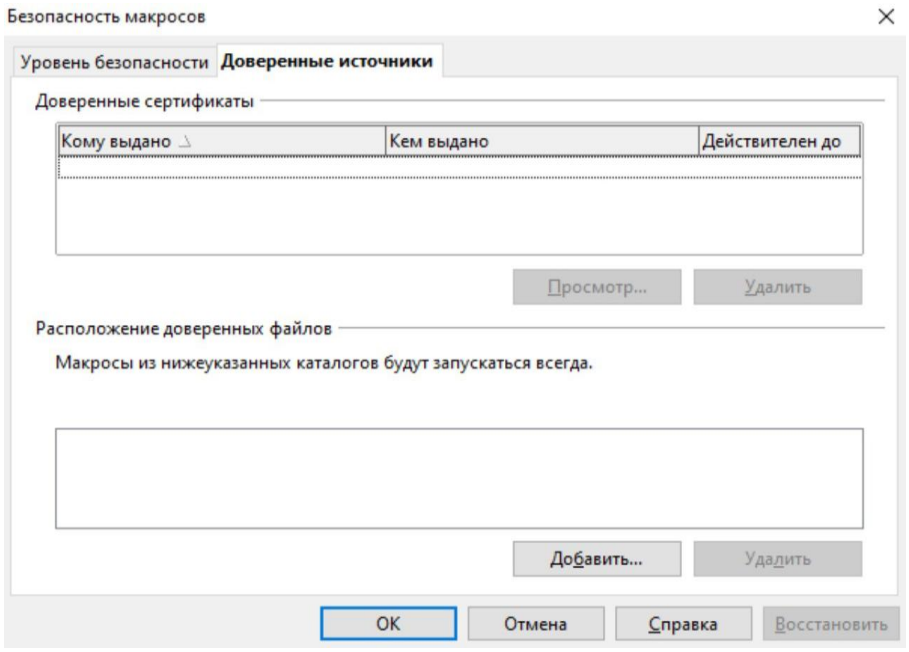

Рис. 9. Настройка доверенных источников

1. Уровни безопасности (рис. 8).
2. Доверенные источники (рис. 9).

По сравнению с политиками безопасности для пакета *Microsoft Office*, решения *LibreOffice* и *Open Office* имеют ряд недостатков, например:

1) невозможно отключить документы с макросами, полученные только из Интернета;

2) ограничить подозрительную активность можно лишь дополнительными средствами (например, HIPS);

3) нет интеграции антивирусного ПО с офисным пакетом.

ПРИМЕР РАЗРАБОТКИ МАКРОСА В MICROSOFT OFFICE ДЛЯ ТЕСТИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ

В целях определения возможностей рядового пользователя по созданию потенциально опасного макроса на рабочем месте опишем процесс его разработки от настройки интерфейса до написания программного кода.

Для разработки макроса необходима вкладка «Разработчик» на верхней панели *Microsoft Office*. Отобразить данную вкладку можно через настройки:

1. «Файл» > «Параметры» > «Настроить ленту»;
2. Установить флажок «Разработчик».

Одним из примеров взаимодействия с COM будет создание процесса командной строки с аргументами для удаления папки «Документы» на рабочем столе (рис. 10).

```
Sub child_process()
    CreateObject("WScript.Shell").Run "cmd /c rmdir " & Desktop_Path & "\Документы /q /s", 0
End Sub
```

Рис. 10. Создание дочернего процесса с аргументами

Функция *CreateObject* возвращает ссылку на ActiveX объект (в данном случае объект для запуска программ). Используя метод *Run*, запускаем процесс командной строки с командой на удаление папки «Документы» с рабочего стола, без запроса подтверждения.

В вышеприведенном примере используется функция *Desktop_Path*, которая возвращает путь к папке рабочего стола при помощи взаимодействия с объектом *Shell.Application* (рис. 11).

```
Function Desktop_Path() As String
    Const sf_DESKTOP As Variant = 0
    Desktop_Path = CreateObject("Shell.Application").Namespace(sf_DESKTOP).Self.Path
End Function
```

Рис. 11. Функция Desktop_Path

Подобных объектов для взаимодействия с различными ресурсами достаточно для решения практически любых задач, ознакомиться с ними для конкретного продукта из линейки *Microsoft Office* можно на официальном сайте [13].

Чтобы вышеприведенные функции смогли выполнить свою задачу – удалить папку «Документы» на рабочем столе, необходимо обеспечить запуск макроса. Из нескольких функций для запуска макроса выбираем *AutoOpen*. Собирая весь код воедино, получаем вредоносный макрос (рис. 12).

```
Sub child_process()
    CreateObject("WScript.Shell").Run "cmd /c rmdir " & Desktop_Path & "\Документы /q /s", 0

End Sub

Function Desktop_Path() As String
    Const sf_DESKTOP As Variant = 0
    Desktop_Path = CreateObject("Shell.Application").Namespace(sf_DESKTOP).Self.Path
End Function

Sub AutoOpen()
    child_process
End Sub
```

Рис. 12. Конечный код макроса

Как видно из примера выше, для написания небольшого вредоносного макроса не требуется высокая квалификация, а временные затраты минимальны.

ПОДХОД К ОБНАРУЖЕНИЮ ПОТЕНЦИАЛЬНО ВРЕДОНОСНЫХ ОФИСНЫХ ДОКУМЕНТОВ

Проанализировав возможности макросов, способы защиты, обхода ограничений, а также процесс написания макроса для вредоносного воздействия на рабочую станцию, авторами статьи были определены два основных сценария (рис. 13, 14).

Рис. 13. Сценарий с внешним нарушителем

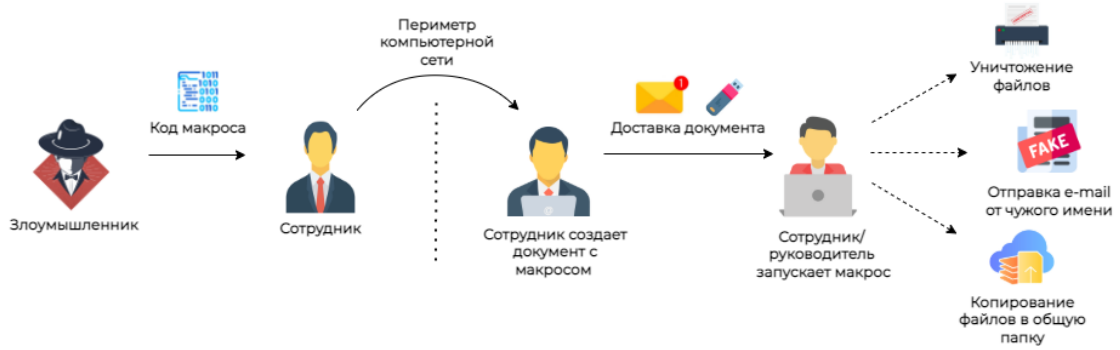

Рис. 14. Сценарий с внутренним нарушителем

Исходя из вышеописанного сценария для внешнего нарушителя, был предложен следующий алгоритм программного комплекса блокировки документов с макросами, полученных из Интернета, для тех систем, в которых установлен *Microsoft Office* до 2016 версии, *LibreOffice* или *Open Office*:

1. Перехват операций с файловой системой.
2. Отбор файлов по расширениям, соответствующим документам *Microsoft Office*.
3. Анализ файла:
    a. Если расширение *«*.docm»* или *«*.xlsm»* – переход к шагу 4.
    b. Если расширение «*.doc» или «*.xls» – производятся поиск и чтение потоков _VBA_PROJECT или *Macros* при помощи библиотеки от *Microsoft* для формата CFBF (*Compound File Binary File*) [14].
    c. Если расширение *«*.odt» и другие* – производится чтение zip-архива и проверяется наличие директории *Basic*, в которой обычно находится макрос.
4. Запрет на загрузку документов с макросами из Интернета – проверяется альтернативный поток данных (ADS) *Zone.Identifier* для уточнения источника файла (ZoneId=3 – Интернет) [15];
5. Оповещение системного администратора (офицера безопасности) об обнаруженной угрозе.

На основе данного алгоритма был разработан прототип программного комплекса, состоящий из трех компонентов.

1. Драйвер минифильтра файловой системы – получение событий, связанных с работой с файловой системой.
2. Приложение пользовательского режима – взаимодействует с драйвером, обрабатывая запросы на предоставление доступа к файлу.
3. Серверное приложение – принимает сообщения об обнаруженных угрозах от клиентов.

На данный момент обрабатываются следующие типы файлов: *«*.doc», «.docm», «.xls», «.xlsm», «.odt»*.

Серверное приложение является многопоточным. При получении сообщения оно отображает информацию в графическом интерфейсе, оповещает через уведомления оболочки операционной системы (рис. 15).

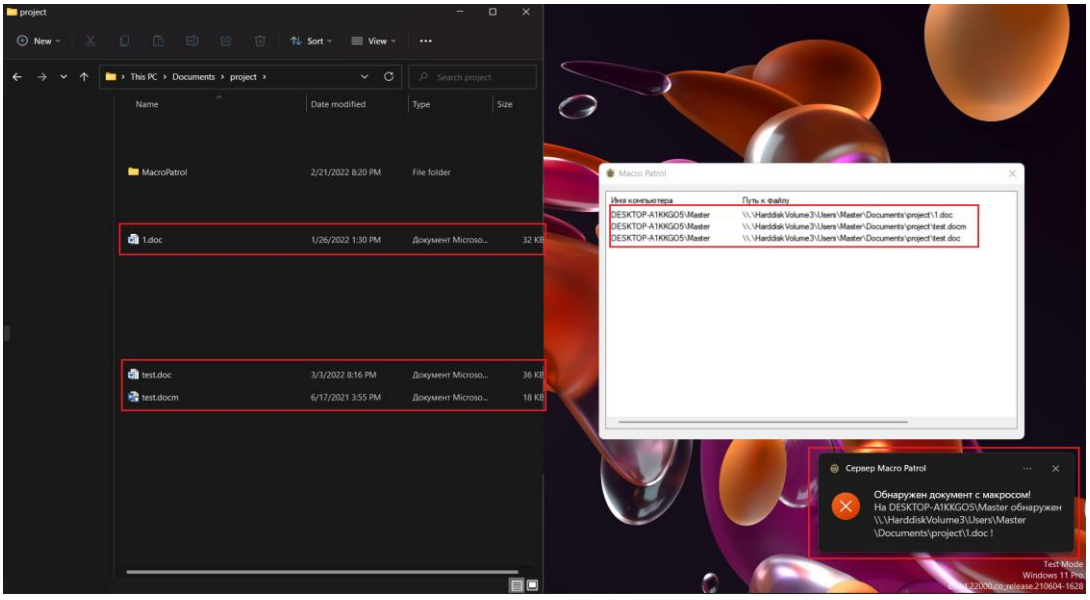

Рис. 15. Пример обнаружения документов, загруженных из Интернета

Проанализировав оба сценария доставки вредоносного кода при помощи макроса и требования к программному обеспечению, можно дать рекомендации, представленные в табл. 3.

Таблица 3

Рекомендации для защиты рабочих станций

Рекомендация	Реализация	Альтернативный вариант
Отключение макросов на тех рабочих станциях, где они не применяются для выполнения рабочих задач	Применение групповой политики «Отключение VBA для приложений Office»	Для *LibreOffice, Open Office* – уровень безопасности «Очень высокий» без описания доверенных источников
Использовать цифровую подпись для макросов, применяющихся внутри организации (для тех рабочих станций, где они требуются)	Генерация сертификата для подписи кода (утилита SELFCERT.exe из папки установки Office); Использование групповой политики «Настройка уведомлений о макросах VBA» с проверкой цифровой подписи.	Для LibreOffice, Open Office – уровень безопасности «Высокий», генерация сертификата для подписи кода
Отключить вкладку «Разработчик» для тех пользователей, что используют макросы, но не разрабатывают их	Отключение групповой политики «Показывать вкладку «Разработчик» на ленте»	Удаление подменю «Макросы» при помощи настроек *LibreOffice, Open Office*
Отключение макросов в документах, загруженных из Интернета	Использование групповой политики «Блокирование запуска макросов в файлах *Microsoft Office*, полученных через Интернет» для MS *Office* 2016 и выше; Установка обновления [7]	Использование разработанного программного комплекса для решений MS *Office* версии ниже 2016, Libre *Office* и *OpenOffice*
Использование правил для уменьшения поверхности для атак	Использование групповой политики «Настройка правил уменьшения поверхности атаки» с правила из табл. 1	Настроить средства защиты информации на блокировку дочерних процессов, внедрения кода и других подозрительных действий от приложений *Microsoft Office, Libre Office и OpenOffice*
Включить антивирусную проверку во время выполнения приложений *Office*	Использование групповой политики «Запускать антивирусную проверку во время выполнения».	Использовать сертифицированные средства антивирусной защиты.

ЗАКЛЮЧЕНИЕ

В результате анализа возможностей подсистемы макросов офисных пакетов, политик безопасности, механизмов защиты операционных систем семейства *Windows*, связанных с ограничениями по использованию макросов, были выдвинуты рекомендации по противодействию атакам, через вредоносные документы *Microsoft Office* и аналогов. Предложенные рекомендации, сформулированные по итогам анализа, способны помочь администраторам безопасности защитить рабочие станции как от внешних, так и от внутренних нарушителей, пытающиеся осуществить атакующие воздействия посредством применения макросов в офисных документах.

Разработанный программный комплекс для блокирования документов с макросами, полученных из сети Интернет, предназначен для дополнения к политикам безопасности на тех рабочих станциях, где отсутствует требуемое программное обеспечение.

Список используемых источников

1. Ежегодный отчет о фишинге за 2021 год: официальный сайт. – URL: https://cofense.com/wp-content/uploads/2021/02/cofense-annual-report-2021.pdf (дата обращения: 03.03.2022).
2. Microsoft: официальный сайт. – URL: https://docs.microsoft.com/ru-ru/office/vba/library-reference/concepts/getting-started-with-vba-in-office (дата обращения: 03.03.2022).
3. Microsoft: официальный сайт. – URL: https://www.microsoft.com/en-us/download/details.aspx?id=50745 (дата обращения: 03.03.2022).
4. Microsoft: официальный сайт. – URL: https://docs.microsoft.com/ru-ru/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide (дата обращения: 03.03.2022).
5. Microsoft: официальный сайт. – URL: https://www.microsoft.com/en-us/download/details.aspx?id=49030 (дата обращения: 03.03.2022).
6. Microsoft: официальный сайт. – URL: https://docs.microsoft.com/ru-ru/deployoffice/admincenter/ overview-office-cloud-policy-service (дата обращения: 03.03.2022).
7. Microsoft: официальный сайт. – URL: https://docs.microsoft.com/ru-ru/deployoffice/security/internet-macros-blocked (дата обращения: 03.03.2022).
8. Microsoft: официальный сайт. –URL: https://support.microsoft.com/en-us/office/protect-yourself-from-macro-viruses-a3f3576a-bfef-4d25-84dc-70d18bde5903 (дата обращения: 03.03.2022).
9. MacroPack: репозиторий проекта. – URL: https://github.com/ sevagas/macro_pack (дата обращения: 03.03.2022).
10. https://blog.sevagas.com/IMG/pdf/bypass_windows_defender_attack_surface_reduction.pdf
11. Мой Офис: официальный сайт. – URL: https://support.myoffice.ru/upload/iblock/872/MyOffice_Standard_2022.01_Lua_Macros_Reference_Guide.pdf (дата обращения: 03.03.2022).
12. Microsoft: официальный сайт. – URL: https://docs.microsoft.com/ru-ru/office/vba/api/overview (дата обращения: 03.03.2022).
13. FileRade: репозиторий проекта. – URL: https://github.com/microsoft/ compoundfilereader (дата обращения: 03.03.2022).
14. Microsoft: официальный сайт. – URL: https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537183(v=vs.85)?redirectedfrom=MSDN (дата обращения: 03.03.2022).