ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/3033-7097-2025-1-4-60-68
УДК 004.056.57(045)

Недекларируемые возможности файловой архитектуры. Автоматизированный офис, текстовый редактор, формат DOCX

А.А. Рыженко[a], С.И. Козьминых[b]
[a, b] Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация;
[b] Российский экономический университет им. Г.В. Плеханова, Москва, Российская Федерация

АННОТАЦИЯ

Вторая статья данного цикла работ предполагает приподнять завесу тайны форматов файлов автоматизированного офиса как контейнера для доработки вручную некоторых скрытых возможностей. **В статье рассмотрен** алгоритм реализации одной такой функции — перенаправление скрытой ссылки на активный интернет-ресурс. Как было упомянуто ранее в первой статье*, нарастающее количество недекларируемых функций в файловой архитектуре вызывает опасение у существующих спецслужб государств, что вполне обоснованно практическим отсутствием унифицированных программно-аппаратных комплексов аудита инъекций такого рода. Изучение простых программных инструментов, к сожалению, пропускаемых системами защиты на локальных ПК и в сетях, позволит построить более мощный закрытый контур на рабочих местах. Существующие системы управления информацией и событиями безопасности SIEM в унифицированном формате построения баз правил для аудита закрытого контура не содержат на данный момент готовых алгоритмов обнаружения посторонних файлов внутри файлов форматов автоматизированного офиса. Данный фактор необходимо исправлять с использованием самописных правил на рабочих местах индивидуально. В данном цикле статей не предполагаются практические инструкции, способные нанести вред цифровой среде корпоративного контура организаций. **Рассмотрен сценарий** простой инъекции с перенаправлением ссылки на интернет-ресурс (функция redirect), который предполагает исключительно образовательные функции и предупреждения для специалистов в сфере информационной безопасности.
Ключевые слова: инъекции; файловая система; текстовый редактор; безопасность; проникновение; глобальная сеть

Для цитирования: **Рыженко А.А., Козьминых С.И. Недекларируемые возможности файловой архитектуры. Автоматизированный офис, текстовый редактор, формат DOCX. *Цифровые решения и технологии искусственного интеллекта*. 2025;1(4):60-68. DOI: 10.26794/3033-7097-2025-1-4-60-68**

ORIGINAL PAPER

Undeclared File Architecture Features. Automated Office, Text Editor, Docx Format

A.A. Ryzhenko[a], S.I. Kozminych[b]
[a, b] Financial University under the Government of the Russian Federation, Moscow, Russian Federation;
[b] Plekhanov Russian University of Economics, Moscow, Russian Federation

ABSTRACT

The second paper of this series of articles suggests lifting the veil of secrecy of automated office file formats as a container for manually refining some hidden features. **The article discusses** an algorithm for implementing one such function — redirecting a hidden link to an active Internet resource. As mentioned earlier in the first part of the article, the increasing number of undeclared functions in the file architecture causes concern among the existing special services of states, which is fully justified by the practical lack of unified software and hardware systems for auditing injections of this kind. Studying simple software tools, unfortunately overlooked by security systems on local PCs and networks, will allow you to build a more powerful closed circuit in the workplace. The existing SIEM in a unified format for building rule bases for closed-circuit auditing does not currently contain ready-made algorithms for detecting extraneous files inside files of automated office formats. This factor needs to be corrected using self-written workplace rules individually. This series of articles does not provide practical instructions for harming the digital environment of the corporate circuit of organizations. **The considered scenario** of a simple injection with redirection of a link to an Internet resource (redirect function) assumes exclusively educational functions and warnings for information security specialists.
Keywords: injections; file system; text editor; security; penetration; global network

For citation: **Ryzhenko A.A., Kozminych S.I. Undeclared file architecture features. automated office, text editor, docx format. *Digital Solutions and Artificial Intelligence Technologies*. 2025;1(4):60-68. DOI: 10.26794/3033-7097-2025-1-4-60-68**

* Рыженко А.А., Козьминых С.И. Недекларируемые возможности файловой архитектуры: графические контейнеры. *Цифровые решения и технологии искусственного интеллекта*. 2025;1(3):55-61.

ВВЕДЕНИЕ

Массовый переход файловой архитектуры в кроссплатформенный формат в начале 2000-х гг. привел к тому, что многие популярные форматы файлов стали открытого типа как контейнеры [1]. С одной стороны, эффект унификации позволил без дополнительных конвертаций переносить файлы в абсолютно произвольную операционную систему со своими особенностями организации файловой архитектуры, с другой — файлы-контейнеры теперь открыты и доступны для злоумышленников. Программисты часто забывают, что криптозащита файла как целостной системы позволяет не только обезопасить данные, но и предотвратить заражение в форме инъекций.

Описанный в статье метод является отправной точкой для полноценного анализа существующих методов простых инъекций. В глобальной сети множество аналогичных статей и публикаций[1]. С научной точки зрения у правоохранительных органов есть множество вопросов к разработчикам, что также отражено в ряде статей [2, 3]. К сожалению, можно на данный момент уверенно констатировать тот факт, что унифицированных автоматизированных методов блокировки от данного метода инъекций (например, в базах правил SIEM) не существует [4].

В статье рассмотрен сценарий простой корректировки вложенных в контейнер файлов автоматизированного офиса (на примере формата.docx) как пример простой инъекции произвольной информации в файловую архитектуру.

АЛГОРИТМ ИНЪЕКЦИИ В ПОПУЛЯРНЫЙ ФОРМАТ ТЕКСТОВОГО РЕДАКТОРА

Цифровая среда не очень любит открывать свои тайны и секреты. И если пользователь не знает, что может скрывать вроде бы обычный файл, то, как правило, действие такого рода приводит к заражению устройства вирусами с последующей утечкой информации. В качестве примера можно рассмотреть одно из новых направлений цифровизации банковской инфраструктуры. Летом 2025 г. юридическим отделом Банка России[2] было предложено упростить процесс подписания договоров при оформлении кредитов дистанционно с применением цифрового суррогата сопроводительных документов. Файлом-посредником для фиксации момента подписания выбран самый популярный формат файла автоматизированного офиса — DOCX. Данный формат содержит множество недекларированных возможностей, способствующих проникновению злоумышленника в закрытый контур банка. Далее будет рассмотрен один из известных в сети Интернет процессов перенаправления ссылки. Авторы специально не стали усложнять данный пример теми инструментами, которые позволяют еще глубже скрыть данный процесс с использование методов и алгоритмов социальной инженерии. Новое направление и возможные последствия будут рассмотрены в последующих статьях. Итак, процесс перенаправления ссылки состоит из следующих шагов.

Шаг 1. Заводим личный аккаунт в любом из IP-грабберов (*рис. 1*) [5]. В статье не предполагается отдельное описание функционала программных порталов такого рода, а также представление возможностей интернет-ресурсов, работающих на протоколах пятого уровня. Использование логгеров в цифровой среде нашего государства не запрещено законом, чем пользуются многие сотовые операторы для слежения за своими абонентами.

На втором шаге необходимо создать или использовать готовый файл в формате docx, на котором будем далее экспериментировать. При создании пустого нового файла не будет автоматически создана архитектура XDTO-контейнера. Страницы XML-кода добавляются в архитектуру контейнера только после открытия (или запуска) файла в активную фазу [6].

Шаг 2. Создаем документ в формате docx (*рис. 2*).

Далее используем ту самую недекларируемую функцию компонента ActiveX на примере «Видео из интернета». Особенностью активных элементов текстового редактора заключается в том, что они применяют встроенный макрос, который не фиксируется системами защиты на ПК как зловред. Именно этой особенностью часто пользуются злоумышленники при получении доступа изнутри в закрытом контуре организации. Чаще всего инструментарий ActiveX встроен в табличный процессор автоматизированного офиса. Почему до сих пор системы безопасности не научились запрещать инъекции такого рода, остается загадкой [7].

Шаг 3. Добавляем в документ компонент ActiveX на примере «Видео из интернета» (*рис. 3*).

Как уже было упомянуто ранее, обратимся к самому популярному примеру из интернет-среды. В 2025 г. Роскомнадзор запретил использование портала YouTube (запрещенный ресурс на терри-

[1] IP Логгер через Word, PDF или Excel файл. URL: https://teletype.in/@rightdecision/IP-Logger-cherez-Word-PDF-ili-Excel-fajl-03–31; IP Logger в Word. URL: https://lolz.live/threads/2431117/; Как нас могут логгировать общедоступными методами. URL: https://habr.com/ru/companies/tomhunter/articles/590633/

[2] Цифровизация банковской сферы в 2025 году: ключевые тренд. URL: https://contentai.ru/blog/tpost/34rlifhu21-tsifrovizatsiya-bankovskoi-sferi-v-2025

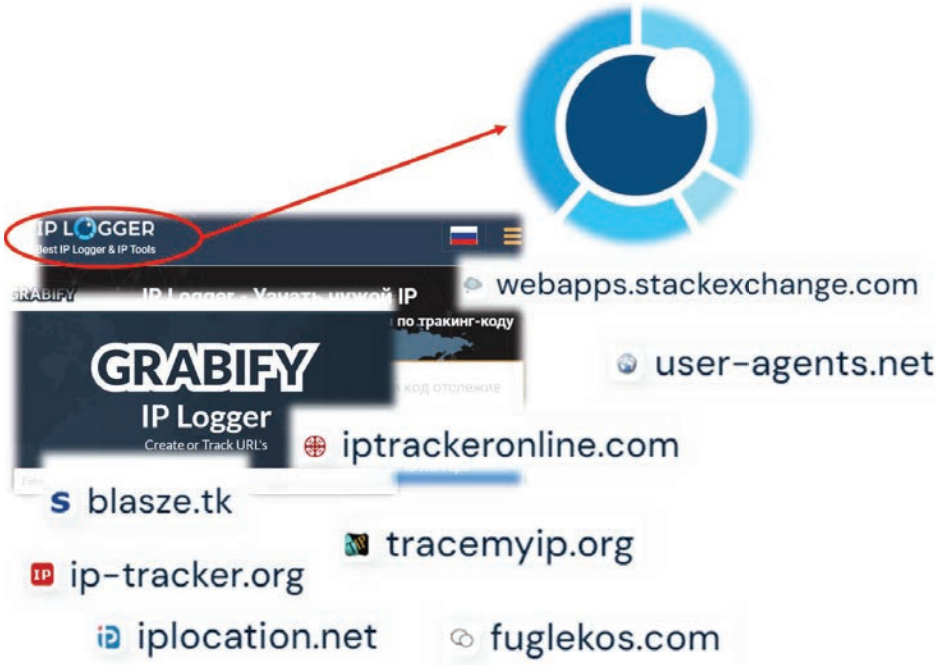

Рис. 1 / Fig. 1. **Варианты IP-грабберов / IP Grabber Options**

Источник / Source: открытая зона интернета / Open Internet Area.

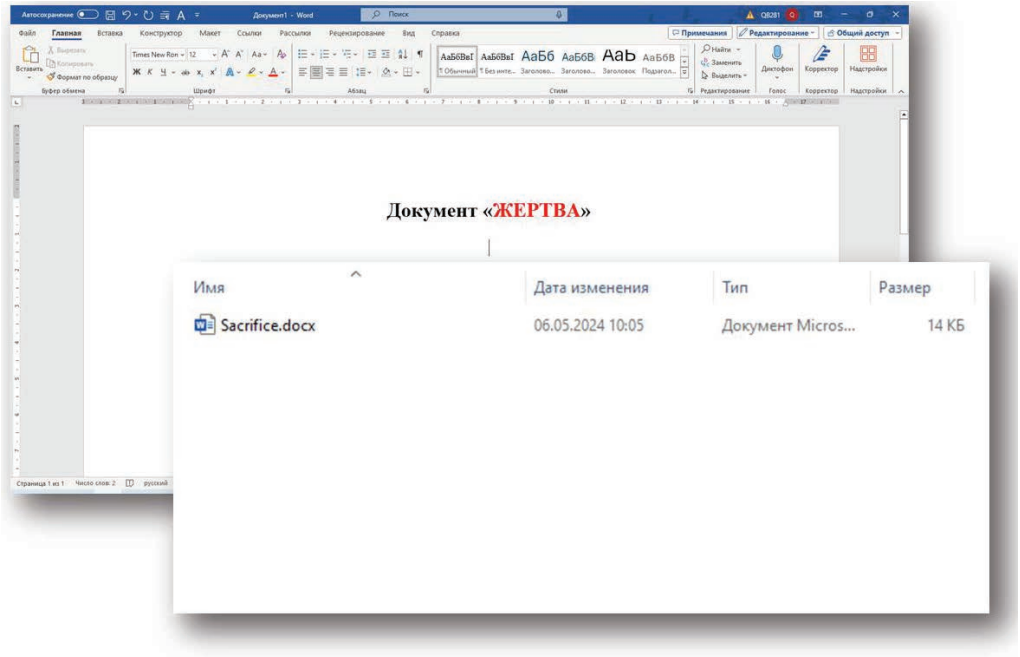

Рис. 2 / Fig. 2. **Подготовка файла для инъекции / Preparing the File for Injection**

Источник / Source: составлено авторами / Complied by the authors.

тории РФ) в цифровой зоне домена РУ. Попытки задействовать криптозащищенные каналы VPN для получения доступа к запрещенным ресурсам отслеживается специальными службами и, в случае необходимости, пользователь может быть привлечен к статьям УК РФ [8]. Как следствие, дальнейшая инструкция приводится только с целью обучения специалистов сферы информационной безопасности недекларированным возможностям автоматизированного офиса.

Шаг 4. Просто сохраняем файл с активной вставкой (*рис. 4*).

Шаг 5. В папке с файлом в формате docx открываем видимость расширений файлов. Меняем расширение docx на zip (*рис. 5*). Именно в этом начинается проблемный момент для любой службы безопасности. Все форматы с расширением X (extended) являются контейнерами и могут быть открыты как zip-архив. Содержимое контейнера в разных версиях автоматизированного офиса

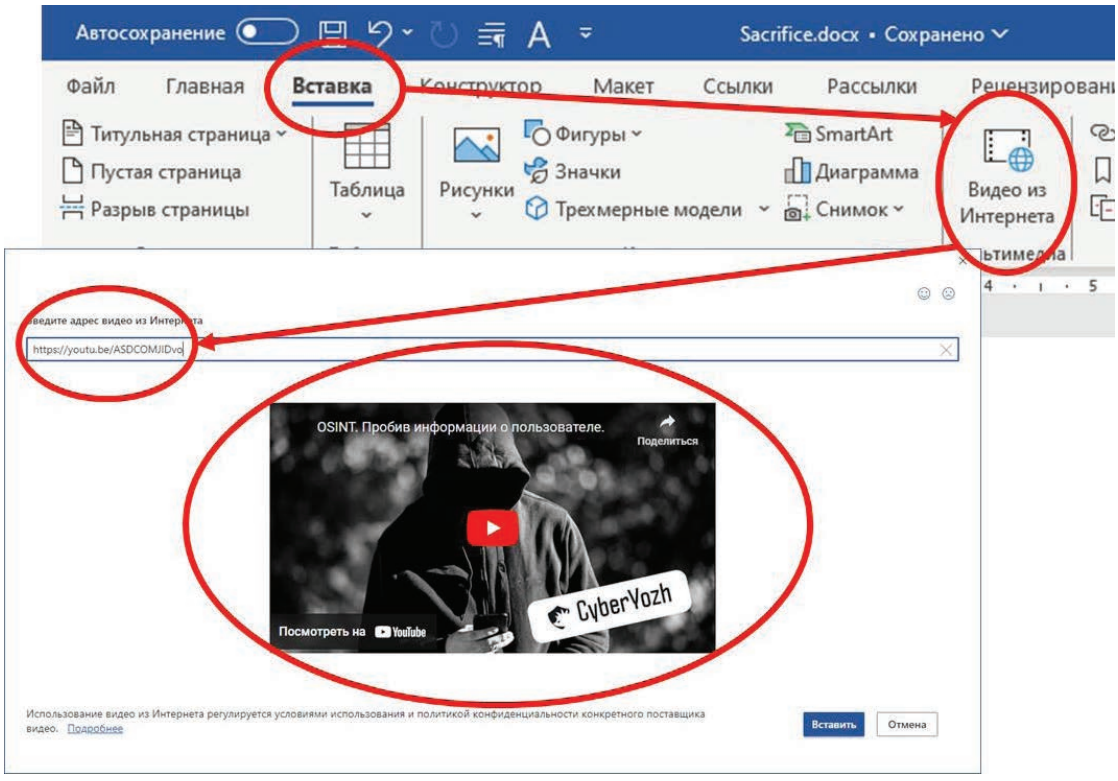

Рис. 3 / Fig. 3. **Добавление активного компонента / Adding an Active Component**

Источник / Source: составлено авторами / Complied by the authors.

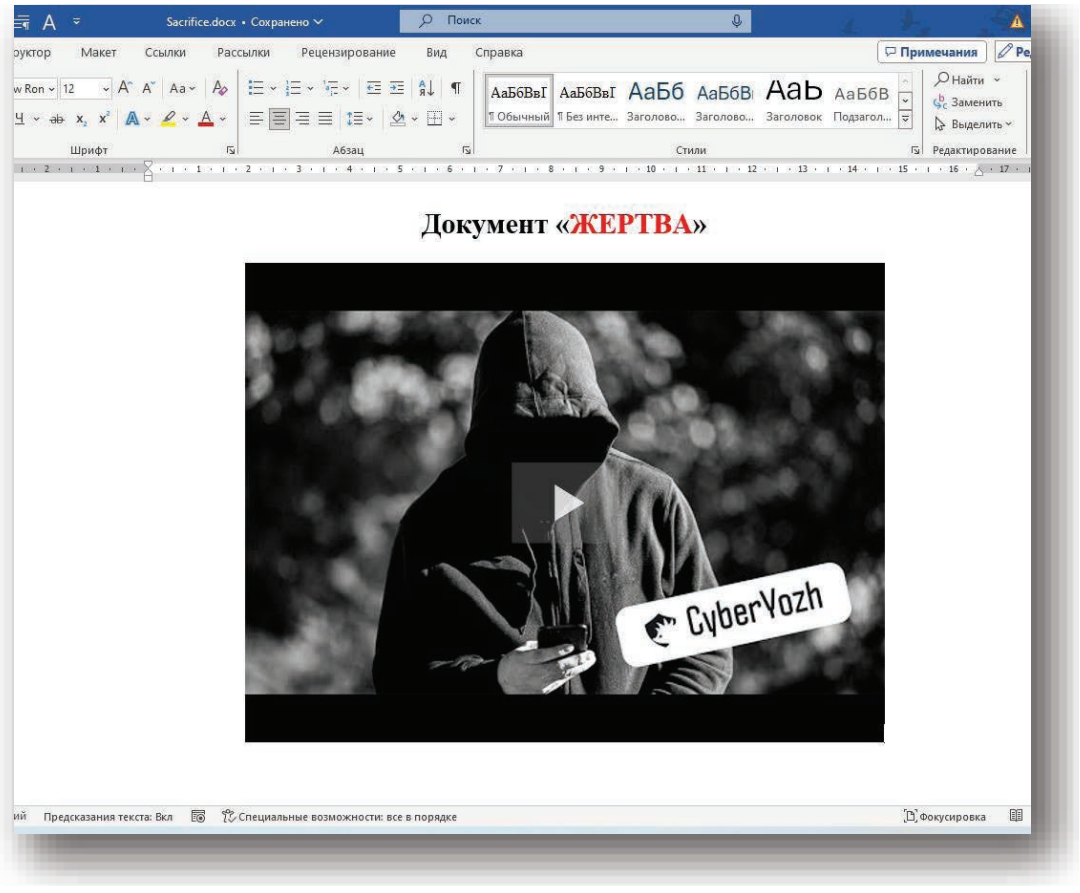

Рис. 4 / Fig. 4. **Файл с ключевой командой / The File with the Key Command**

Источник / Source: составлено авторами / Complied by the authors.

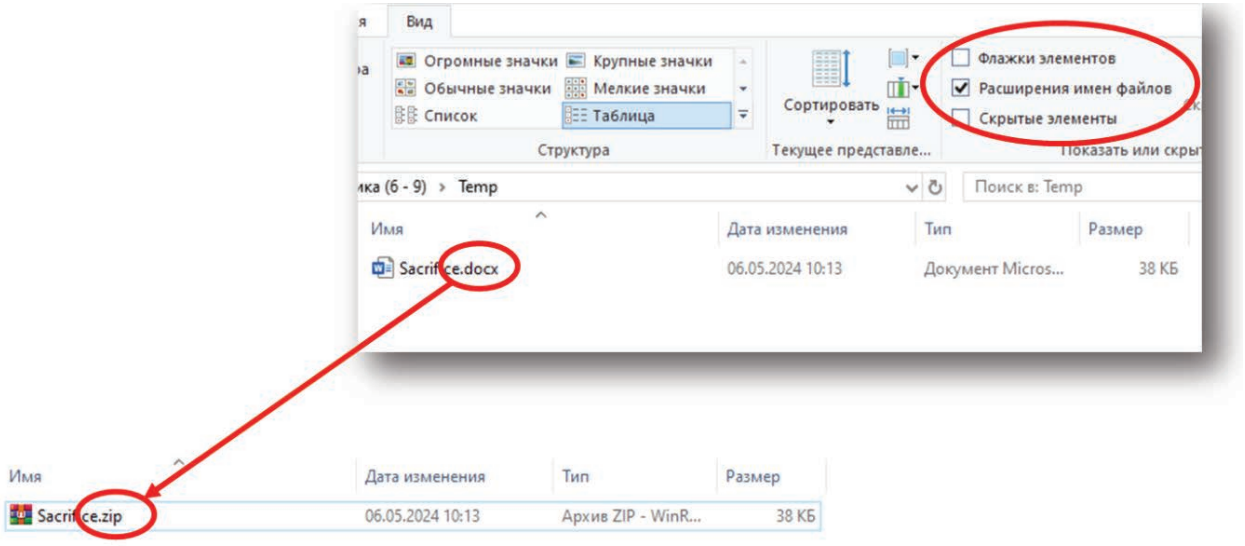

Рис. 5 / Fig. 5. **Меняем расширение docx на zip / Changing the Extension docx to zip**

Источник / Source: составлено авторами / Complied by the authors.

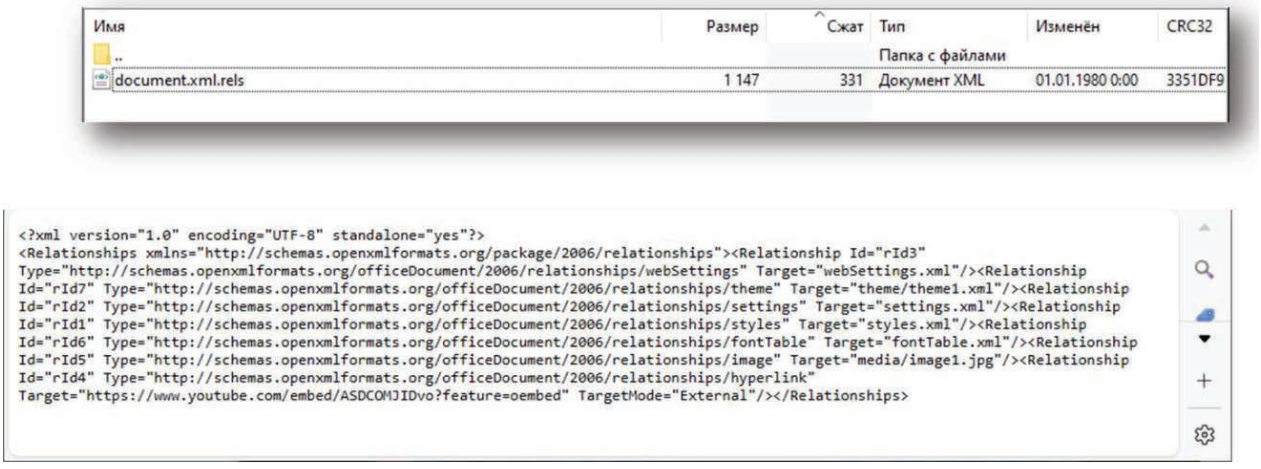

Рис. 6 / Fig. 6. **Текстовый формат файла, пример / Text File Format, Example**

Источник / Source: составлено авторами / Complied by the authors.

может изменяться, но суть от этого не меняется. Большая часть файлов — обычные XML-форматы, свободно читаемые произвольным текстовым редактором, о чем также будет сказано ниже.

В результате переименования автоматически создается файл как zip-архив, который можно открыть без нарушения целостности [9]!

Шаг 6. Запускаем архив Sacrifice.zip. Открываем папку word, затем папку _rels. Находим файл document.xml.rels. Открываем как обычный текстовый документ, например, в приложении «Блокнот» (*рис. 6*).

Шаг 7. Находим в файле ссылку на Youtube-ролик и меняем на ссылку-подсказку. Например, «https://www.ЖМИ!_НЕ_СТЕСНЯЙСЯ.ru». Первый файл готов! (*рис. 7*).

Шаг 8. Остаемся в архиве Sacrifice.zip. Переходим в папку word. Находим файл document.xml (*рис. 8*).

Шаг 9. Находим в файле ссылку на Youtube-ролик и меняем на ссылку IP-логгера (*рис. 9*). Второй файл готов!

Шаг 10. Переименовываем файл с расширением zip обратно в формат docx. Запускаем ссылку (*рис. 10*). Если пользователь нажмет на кнопку воспроизведения, то видео не запустится, но сработает логгер.

Аналогично первой статье этой серии следует обратить внимание на тот факт, что все действия с целостностью файла не вызывали подозрения ни у одной установленной системы защиты информации [10].

ВЫВОДЫ

Сценарий простой инъекции с перенаправлением ссылки на интернет-ресурс (функция redirect), рассмотренный в данной статье, представлен исклю-

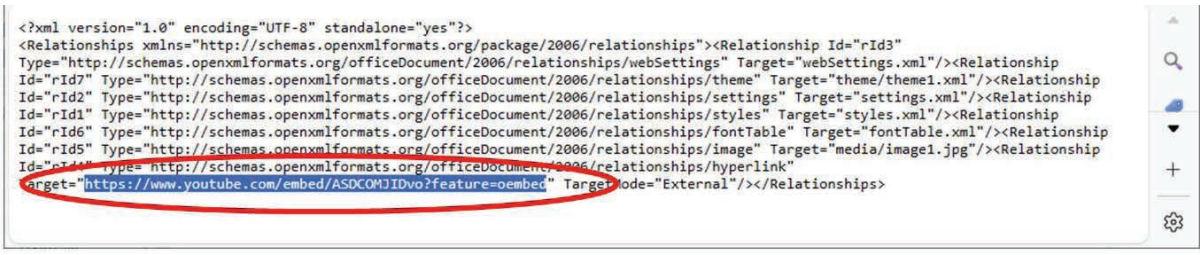

Рис. 7 / Fig. 7. **Замена всплывающей подсказки на поддельную / Replacing the Popup Hint with a Fake One**

Источник / Source: составлено авторами / Complied by the authors.

Рис. 8 / Fig. 8. **Активный файл со ссылками / Active File with Links**

Источник / Source: составлено авторами / Complied by the authors.

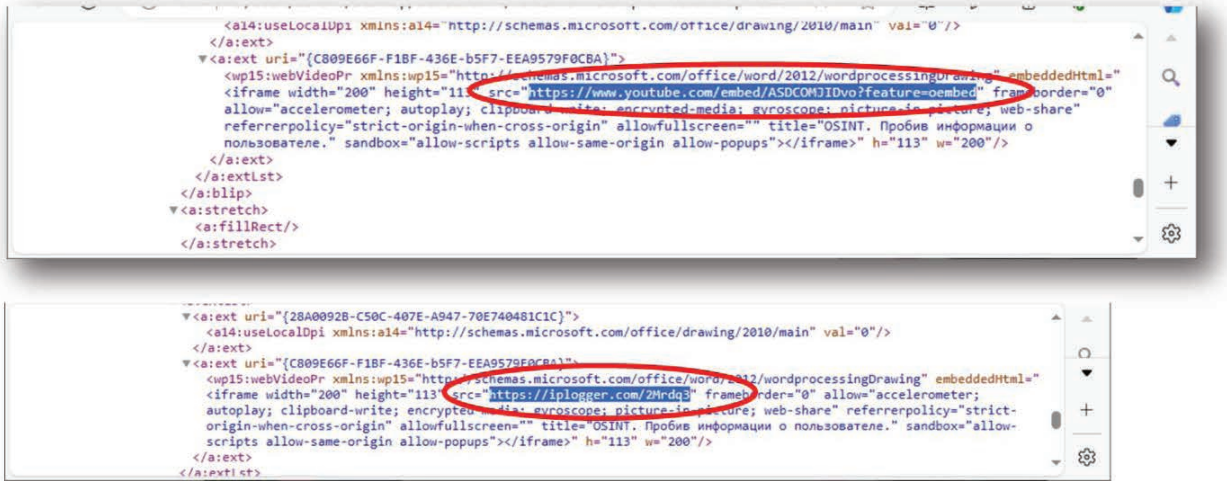

Рис. 9 / Fig. 9. **Фиктивная скрытая активная ссылка / Fictitious Hidden Active Link**

Источник / Source: составлено авторами / Complied by the authors.

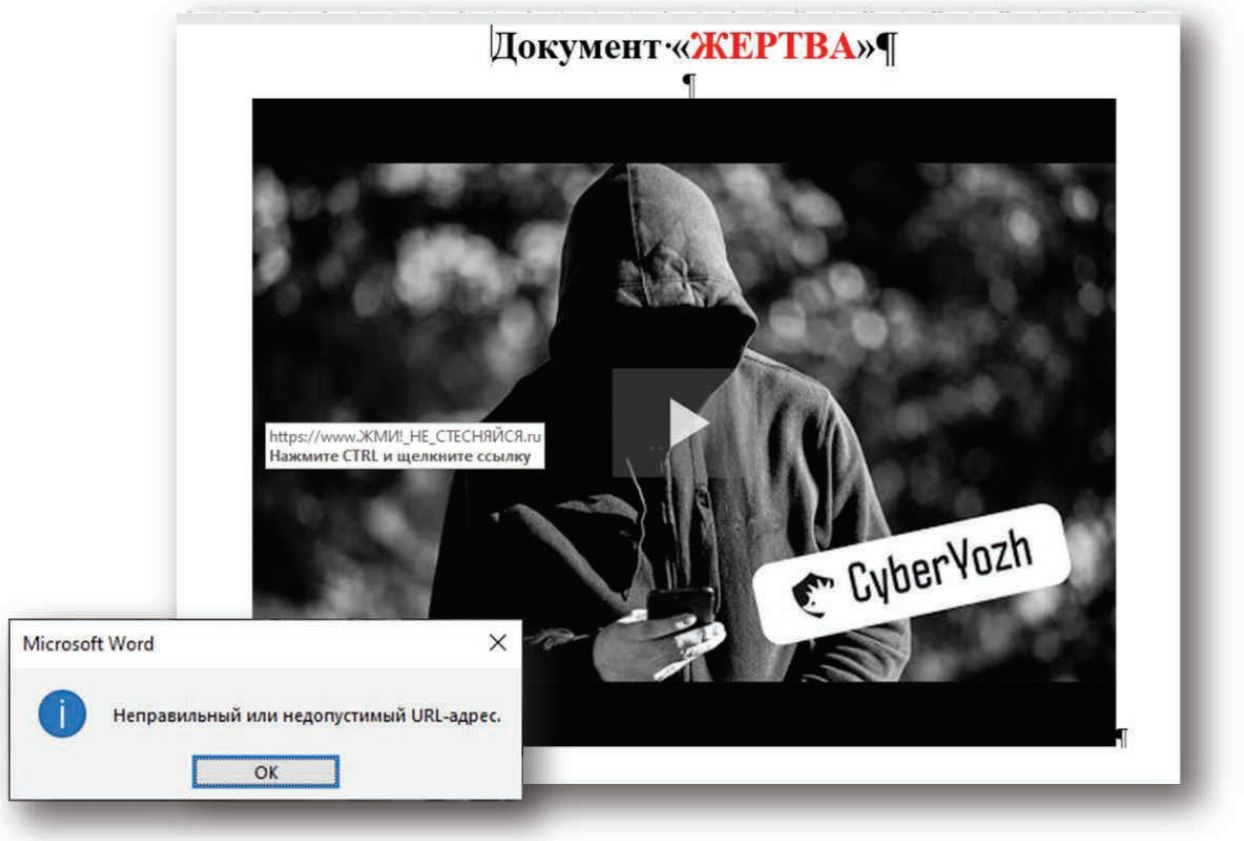

Рис. 10 / Fig. 10. **Активная фиктивная ссылка в скрытом виде / An Active Dummy Link in a Hidden Form**

Источник / Source: составлено авторами / Complied by the authors.

чительно в образовательных и предупредительных целях для специалистов в сфере информационной безопасности.

В последующих статьях будут описаны и расшифрованы уязвимости файлов автоматизированного офиса, не представленных в сети Интернет в открытых источниках. Также будут рассматриваться методы простых инъекций во все унифицированные форматы медиафайлов, распространенных в сети Интернет. Например, такие форматы, как: mp3, mp4, avi, mov, pdf, jpg, bmp, gif, tif и т.д. Сколько еще содержат существующие файлы контейнеры ошибок и недочетов будет также детально рассматриваться и далее.

СПИСОК ИСТОЧНИКОВ

1. Трусов А.Н., Иванченко П.Ю., Кацуро Д.А. Редактирование и внесение информации в XML-документы автоматизированных информационных систем. *Программные продукты и системы*. 2017;30(1):81–84. DOI: 10.15827/0236-235X.030.1.081-084
2. Сутыркина Е.А., Бурмистров А.Н. Исследование файлов журнала веб-сервера на предмет активности ботнетов с целью совершенствования технологии защиты веб-серверов. *Ученые записки УлГУ. Серия «Математика и информационные технологии».* 2021;2:63–74. URL: https://elibrary.ru/nliwpa
3. Смольянинов В.А. Программные способы определения метаположения пользователей социальных сетей. Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем. Сборник материалов конференции, Воронеж, 09 июня 2022 г. Воронеж: Воронежский институт Министерства внутренних дел Российской Федерации; 2022;51–53. URL: https://www.elibrary.ru/qyardw
4. Куприяновская Ю.В., Куприяновский В.П., Климов А.А., Намиот Д.Е., Долбнев А.В. и др. Умный контейнер, умный порт, BIM, интернет вещей и блокчейн в цифровой системе мировой торговли. *International Journal of Open Information Technologies*. 2018;6(3):49–94. URL: https://www.elibrary.ru/yrysiu
5. Бахтеев Д.В., Шевырталов Е.П. Способы нейтрализации штатных и нештатных средств защиты автомобиля как элемент совершения угонов и хищений транспортных средств. *Вестник Уральского юридического института МВД России*. 2024;1(41):74–79. URL: https://cyberleninka.ru/article/n/sposoby-neytralizatsii-shtatnyh-i-neshtatnyh-sredstv-zaschity-avtomobilya-kak-element-sovershheniya-ugonov-i-hischeniy-transportnyh/viewer

6. Еремченко В.И. Современные проблемы свободного оборота средств совершения и сокрытия преступлений. *Общество и право*. 2017;2(60):195–197. URL: https://cyberleninka.ru/article/n/sovremennye-problemy-svobodnogo-oborota-sredstv-sovershheniya-i-sokrytiya-prestupleniy/viewer
7. Никифорова К.В., Окладова И.М. Обзор технологий com. разработка сервера автоматизации. *Форум молодых ученых*. 2019;4(32):791–797. URL: https://elibrary.ru/vuzifo
8. Авласевич Д.В., Дмитриев Н.А., Кириллов А.А., Бачинский А.Г. Использование технологии VPN для обеспечения информационной безопасности. *Форум молодых ученых*. 2020;3(43):12–18. URL: https://elibrary.ru/etgkxb
9. Жуйков Е.А. Разработка математической модели обнаружения программных закладных устройств. *НБИ технологии*. 2023;17(1):17–23. DOI: 10.15688/NBIT.jvolsu.2023.1.3
10. Тихомиров Н.А., Ключарёв П.Г. Проблема мониторинга информационных потоков, возникающих в ходе сборки программного обеспечения. *Вопросы кибербезопасности*. 2025;1(65):128–135. DOI: 10.21681/2311-3456-2025-1-128-135

REFERENCES

1. Trusov A.N., Ivanchenko P.Y., Katsuro D.A. Editing and entering information into XML documents of automated information systems. *Software Products and Systems*. 2017;30(1):81–84. DOI: 10.15827/0236-235X.030.1.081-084
2. Sutyrkina E.A., Burmistrov A.N. Botnet detection via server logs analysis. *Bulletin of the USU. The series "Mathematics and Information Technology"*. 2021;2:63–74. URL: https://elibrary.ru/nliwpa
3. Smolyaninov V.A. Software methods for determining the meta-position of users of social networks. Current issues of the operation of security systems and secure telecommunication systems: Conference proceedings, Voronezh, June 09, 2022. Voronezh: Voronezh Institute of the Ministry of Internal Affairs of the Russian Federation; 2022:51–53. URL: https://www.elibrary.ru/qyardw
4. Kupriyanovskaya Yu.V., Kupriyanovsky V.P., Klimov A.A., Namiot D.E., Dolbnev A.V. et al. Smart container, smart port, BIM, Internet of Things and blockchain in the digital world trade system. *International Journal of Open Information Technologies*. 2018;6(3):49–94. URL: https://www.elibrary.ru/yrysiu
5. Bakhteev D.V., Shevyrtalov E.P. Methods of neutralizing standard and non-standard means of protecting a car as an element of committing theft and theft of vehicles. *Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia*. 2024;1(41):74–79. URL: https://cyberleninka.ru/article/n/sposoby-neytralizatsii-shtatnyh-i-neshtatnyh-sredstv-zaschity-avtomobilya-kak-element-sovershheniya-ugonov-i-hischeniy-transportnyh/viewer
6. Eremchenko V.I. Modern problems of free trafficking of the means of committing and concealing crimes. *Society and Law*. 2017;2(60):195–197. URL: https://cyberleninka.ru/article/n/sovremennye-problemy-svobodnogo-oborota-sredstv-sovershheniya-i-sokrytiya-prestupleniy/viewer
7. Nikiforova K.V., Okladova I.M. Overview technology com. development of an automation server. *Forum of Young Scientists*, 2019;4(32):791–797. URL: https://elibrary.ru/vuzifo
8. Avlasevich D.V., Dmitriev N.A., Kirillov A.A., & Bachinsky A.G. Using VPN Technology to Ensure Information Security. *Forum of Young Scientists*. 2020;3(43):12–18. URL: https://elibrary.ru/etgkxb
9. Zhuikov E.A. Development of a mathematical model for detecting software embedded devices. *NBI Technologies*. 2023;17(1):17–23. DOI: 10.15688/NBIT.jvolsu.2023.1.3
10. Tikhomirov N.A., Klyucharev P.G. The problem of monitoring information flows that occur during software assembly. *Cybersecurity Issues*, 2025;1(65):128–135. DOI: 10.21681/2311-3456-2025-1-128-135

ИНФОРМАЦИЯ ОБ АВТОРАХ / ABOUT THE AUTHORS

Алексей Алексеевич Рыженко — кандидат технических наук, доцент, доцент кафедры информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

Alexey A. Ryzhenko — Cand. Sci. (Tech.), Assoc. Prof. of the Information Safety Department, Financial University under the Government of the Russian Federation, Moscow, Russian Federation

https://orcid.org/0000-0002-7279-9929

Автор для корреспонденции / Corresponding author:

AARyzhenko@fa.ru

Сергей Игоревич Козьминых — доктор технических наук, доцент, профессор кафедры прикладной информатики и информационной безопасности, Российский экономический университет им. Г.В. Плеханова, Москва, Российская Федерация; профессор кафедры информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация
Sergey I. Kozminykh — Dr. Sci. (Tech.), Assoc. Prof., Prof. of the Department of Applied Informatics and Information Security, Plekhanov Russian University of Economics, Moscow, Russian Federation; Professor of Information Security Department, Financial University under the Government of the Russian Federation, Moscow, Russian Federation
https://orcid.org/0000-0003-3903-9562
kozminyh.si@rea.ru;
SIKozminykh@fa.ru

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.
Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

Статья поступила в редакцию 13.10.2025; принята к публикации 24.11.2025.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 13.10.2025; accepted for publication on 24.11.2025.
The authors read and approved the final version of the manuscript.