ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/3033-7097-2026-2-1-28-34
УДК 004.056.57(045)

Недекларируемые возможности файловой архитектуры. Уязвимость формата PPTX Microsoft PowerPoint

А.А. Рыженко[1], С.И. Козьминых[2]
[1,2] Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация;
[2] Российский экономический университет им. Г.В. Плеханова, Москва, Российская Федерация

АННОТАЦИЯ

Поскольку презентации прочно вошли в повседневную рабочую практику самых разных специалистов, форматы файлов для их создания неизбежно привлекают внимание злоумышленников — чем шире распространение, тем выше интерес к поиску уязвимостей. Что важно знать для эффективной защиты? **Предмет исследования** — уязвимость формата файлов PPTX (Microsoft PowerPoint), обусловленная его архитектурой как ZIP-контейнера с XML-компонентами. **Цель работы** — продемонстрировать возможность внедрения инъекций в PPTX-файлы без использования программирования, раскрыть механизмы эксплуатации и обозначить риски для информационной безопасности. **Основные аспекты анализа: а**рхитектурные особенности PPTX; механизм внешних ссылок через ActiveX-компоненты. Алгоритм инъекции: преобразование и модификация файла, маскировка подмены, восстановление исходного формата. Отражены практические риски, даны рекомендации по защите. **Научная и практическая значимость:** систематизация знаний о недекларированных возможностях PPTX; демонстрация реального сценария атаки; формирование базы для разработки контрмер (DLP-правила, настройки Office). **Целевая аудитория:** специалисты по ИБ, разработчики офисного ПО, преподаватели курсов кибербезопасности, продвинутые пользователи. **Вывод:** в данной статье аналогично предыдущим сочетаются техническая глубина и доступность, подчеркивается необходимость комплексного подхода к защите офисных документов. Статья несет исключительно образовательные функции и предупреждения для действующих специалистов, не предполагая инструкции для нанесения вреда* фирмам или организациям**.
Ключевые слова: инъекции; файловая система; презентации; безопасность; проникновение; глобальная сеть

Для цитирования: Рыженко А.А., Козьминых С.И. Недекларируемые возможности файловой архитектуры. Уязвимость формата PPTX Microsoft PowerPoint. *Цифровые решения и технологии искусственного интеллекта.* 2026;2(1):28-34. DOI: 10.26794/3033-7097-2026-2-1-28-34

ORIGINAL PAPER

Undeclared File Architecture Features. Vulnerability of Microsoft PowerPoint's PPTX Format

A.A. Ryzhenko[1], S.I. Kozminych[2]
[1,2] Financial University under the Government of the Russian Federation, Moscow, Russian Federation;
[2] Plekhanov Russian University of Economics, Moscow, Russian Federation

ABSTRACT

Presentations have become an integral part of the core processes of many areas of professional activity. Nevertheless, the market for professional software packages that allow you to create presentations that meet modern requirements is not so saturated with competition. Microsoft's software products are the undisputed leader. Competitors are much inferior in quality. But, as mentioned in previous articles in this series, cross-platform file formats are not protected from simple injections (without programming knowledge). A detailed example for a word processor was demonstrated in the second part. In this article, the PPTX format will be analyzed in a similar scenario. A simple injection with a hidden link to the active element is a demonstration of the undeclared capabilities of this type of file formats. It should be remembered that these files can be run or opened on absolutely any (including mobile) smart device. This article, like the previous ones, does not provide instructions for harming* firms or organizations**. The articles have exclusively educational functions and warnings for current specialists.
Keywords: injections; file system; presentations; security; penetration; global network

For citation: **Ryzhenko A.A., Kozminych S.I. Undeclared file architecture features. Vulnerability of Microsoft PowerPoint's PPTX format. *Digital solutions and artificial intelligence technologies.* 2026;2(1):28-34. DOI: 10.26794/3030-7097-2026-2-1-28-34**

* Бирюков А. О преступлениях в ИТ простым языком. URL: https://habr.com/ru/companies/otus/articles/804645/?ysclid=mlko2562y4238181887
** УК РФ, ст. 272. Неправомерный доступ к компьютерной информации; УК РФ, ст. 273. Создание, использование и распространение вредоносных компьютерных программ; УК РФ, ст. 274. Неправомерный доступ к компьютерной информации.

ВВЕДЕНИЕ

Важность обсуждения темы недекларируемых возможностей файловой архитектуры и уязвимостей формата PPTX обусловлена следующими факторами:

1. Широкая распространенность формата. PPTX — де-факто стандарт для презентаций в бизнесе, образовании и госуправлении; его используют миллионы людей ежедневно, что многократно увеличивает потенциальный масштаб угроз.

2. Скрытость уязвимости. Архитектура PPTX как ZIP-контейнера с XML-файлами позволяет внедрять вредоносный код без видимых признаков заражения, из-за чего атаки остаются незамеченными для большинства пользователей и систем защиты.

3. Низкий порог эксплуатации. Описанные инъекции реализуемы без программирования — достаточно базовых навыков работы с архивами и текстовыми редакторами, что делает атаку доступной даже для неопытных злоумышленников.

4. Многовекторность угроз. Уязвимость позволяет не только собирать данные через IP-логгеры, но и распространять фишинг, вредоносные скрипты или конфиденциальные payload-компоненты, встраиваемые прямо в структуру файла.

Презентации стали неотъемлемой частью основных процессов многих направлений профессиональной деятельности. Тем не менее рынок профессиональных пакетов программных продуктов, позволяющий создавать презентации, соответствующие современным требованиям, не так насыщен конкуренцией.

Несомненным лидером является программная продукция Microsoft. Конкуренты сильно уступают в качестве. Но, как было упомянуто в предыдущих статьях [1, 2], кросс-платформенные форматы файлов не защищены от простых инъекций (без знания программирования). В настоящей статье аналогично предыдущим сценариям будет разобран формат PPTX. Простая инъекция со скрытой ссылкой на активный элемент является демонстрацией недекларированных возможностей форматов файлов такого типа. При этом необходимо помнить, что данные файлы можно запустить или открыть на абсолютно любом (в том числе и мобильном) смартустройстве. В данной статье, аналогично предыдущим, не предполагается инструкция для нанесения вреда[1] фирмам или организациям[2]. Статьи несут образовательные функции и предупреждения для действующих специалистов.

Современный Microsoft Office способен сохранять файлы как в старом формате PPT, так и в новом формате PPTX. Как заражать старый формат, будет рассмотрено в последующих статьях. Современный кросс-платформенный расширенный формат, аналогично DOCX, представляет не закрытый файл, а ZIP-контейнер [1, 2]. При переименовании расширения PPTX в ZIP появляется возможность просмотра структуры файла. Используя данную возможность, можно создавать простые инъекции. В статье рассмотрен алгоритм простой инъекции, позволяющий изменять атрибуты активных компонентов презентации на примере YouTube[3] ролика[4]. Данная технология широко используется до сих пор на практике несмотря на то, что прямого доступа к видеороликам непосредственно из презентации практически невозможно. Так как ссылки заведомо ложные и являются редиректом IP-логгера[5], сами видеоролики не запускаются.

АЛГОРИТМ ИНЪЕКЦИИ В ПОПУЛЯРНЫЙ ФОРМАТ PPTX

Аналогично предыдущим инъекциям, создаем отдельную пустую папку для дальнейших экспериментов. Воспользуемся одним из самых популярных и пока доступных веб-ресурсом IP LOGGER[6]. Здесь сразу необходимо сделать небольшую поправку. Логгеры запоминают всю историю и хранят в log-файлах[7]. Пользоваться одним и тем же временным адресом логгера не рекомендуется. При обнаружении редирект-ссылки[8] браузеры заносят в черный список адрес и могут закрыть доступ к ресурсу.

Шаг 1. Заводим личный аккаунт в любом из IP-логгеров. Даже бесплатный одноразовый режим предоставляет доступ к достаточно большому количеству встроенных ресурсов (*рис. 1*).

---

[1] Бирюков А. О преступлениях в ИТ простым языком. URL: https://habr.com/ru/companies/otus/articles/804645/?ysclid=mlko2562y4238181887

[2] УК РФ, ст. 272. Неправомерный доступ к компьютерной информации; УК РФ, ст. 273. Создание, использование и распространение вредоносных компьютерных программ; УК РФ, ст. 274. Неправомерный доступ к компьютерной информации.

[3] YouTube — интернет-видеоплатформа и социальная сеть. Запрещена на территории Российской Федерации.

[4] Эксперты ответили на сообщения о полной блокировке YouTube в России. URL: https://www.rbc.ru/technology_and_media/10/02/2026/698b42499a79471c03a2bb74

[5] Лучшие IP Logger Альтернативы. URL: https://apkpure.net/ru/similar/com.linkslogger.iplogger

[6] IP Logger. Узнать чужой IP. URL: https://iplogger.org/ru/

[7] Как скрыться от IP логгеров? URL: https://www.securitylab.ru /blog/personal/xiaomite-journal/355293.php

[8] Что такое редирект. URL: https://help.reg.ru/support/hosting/ redirekty/chto-takoye-redirekt#0

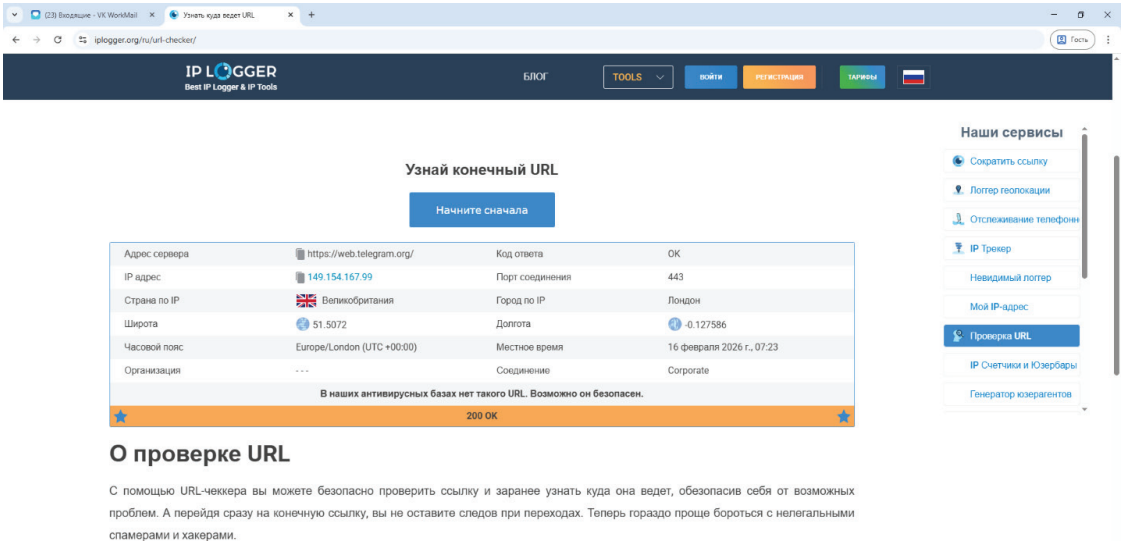

Рис. 1 / Fig. 1. **Примеры IP Logger / IP Logger Examples**

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

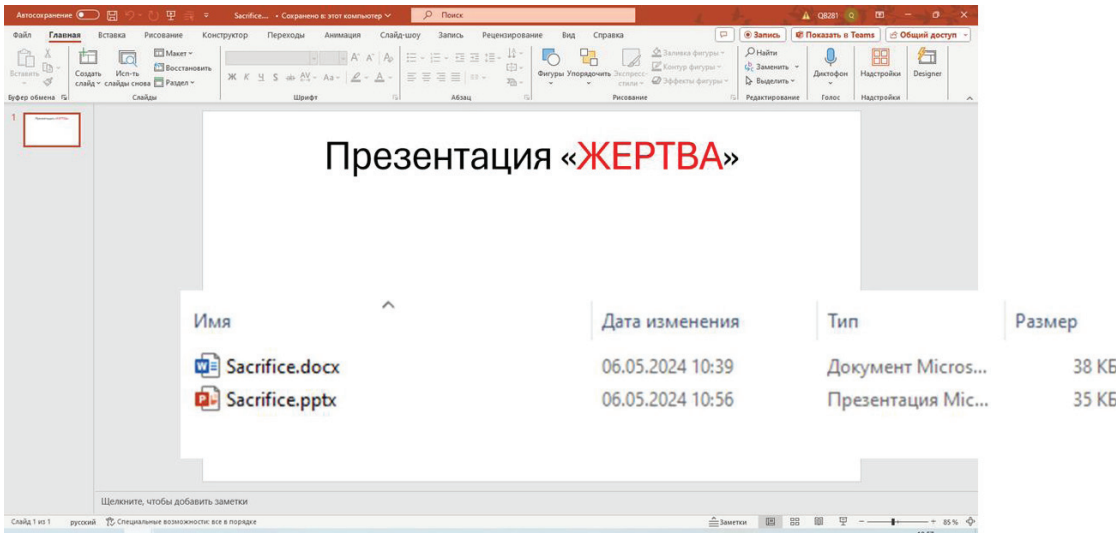

Рис. 2 / Fig. 2. **Подготовка файла для инъекции / Preparing the File for Injection**

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

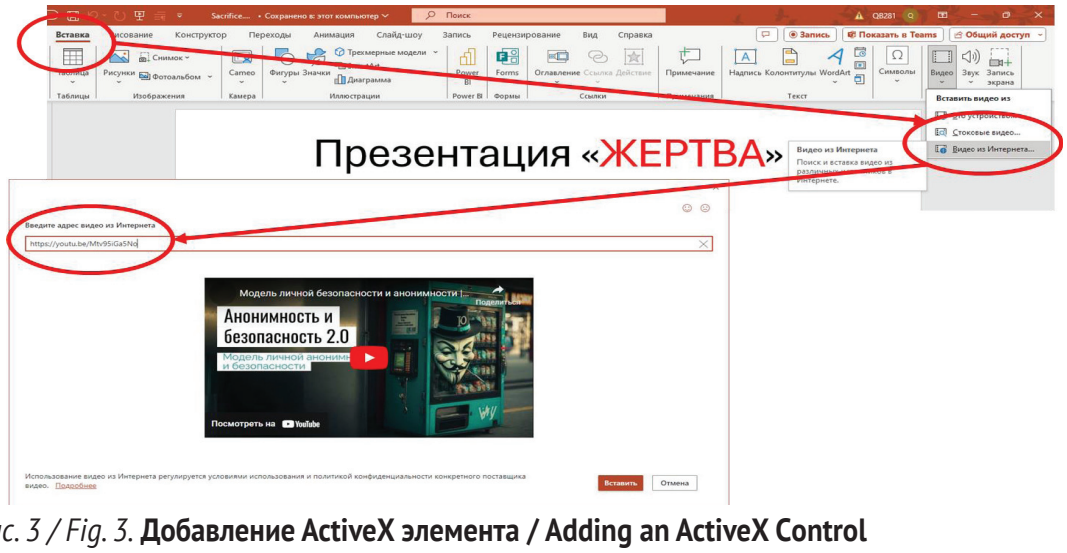

Рис. 3 / Fig. 3. **Добавление ActiveX элемента / Adding an ActiveX Control**

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

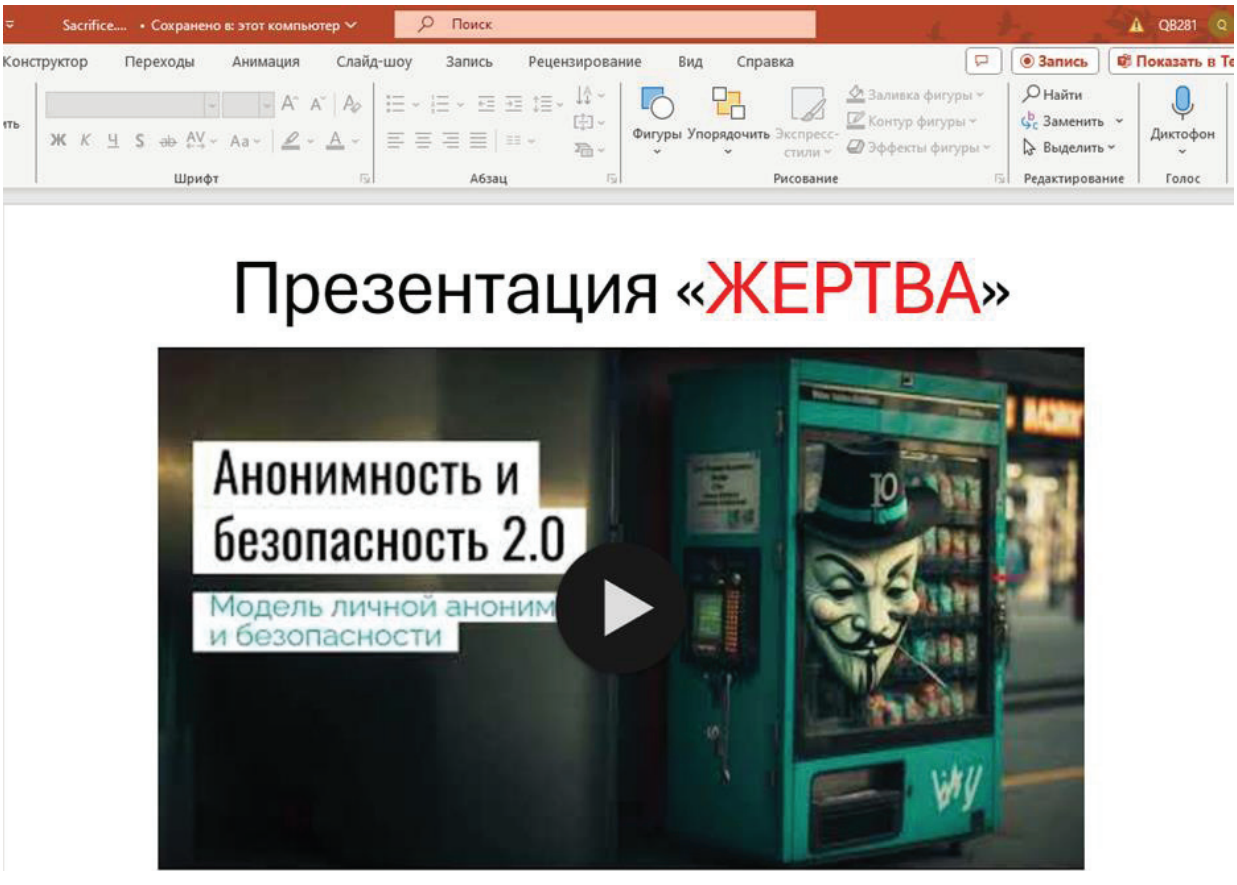

Рис. 4 / Fig. 4. **Файл с активным элементом / The File with the Active Element**

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

На втором шаге необходимо создать или использовать готовый.pptx файл, в который будем внедрять инъекцию. Можно использовать пустой файл без наполнения контентом. Интерес именно в файловой информации.

Шаг 2. Создаем документ жертву в формате.pptx (*рис. 2*)[9].

Далее необходимо добавить активный элемент ActiveX[10] на слайд презентации. Открываем закладку «Вставка», находим группу «Видео».

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

При подключении используем произвольную ссылку на видеоролик YouTube. Попытки подключить видео с других каналов, таких как VK Video[11], Yandex, RuTube[12] и т.д., потерпели неудачу. Данный элемент использует только один глобальный канал потоков видео данных.

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

Шаг 5. В папке с файлом открываем видимость расширений файлов. Меняем расширение.pptx на.zip (*рис. 5*).

Если открыть полученный архив как папку, получим доступ к ряду файлов и папок. Основное расширение файлов атрибутов контента слайдов.xml. Дополнительные атрибуты неосновных элементов слайда хранятся в резервной папке Rels.

Шаг 6. Открываем архив Sacrifice.zip. Открываем папку ppt, затем slides. Открываем папку _rels. Находим файл slide1.xml.rels (*рис. 6*).

Шаг 7. Находим в файле ссылку на Youtube-ролик и меняем на ссылку IP-ЛОГГЕР. Файл готов! (*рис. 7*).

Никаких нюансов здесь нет. Идет простая подмена ссылки. Можно ли скрыть подмену? Можно, воспользовавшись встроенной функцией «Подсказка». Если пользователь не выберет «Изменить ссылку», он никогда не узнает, что была подмена.

Шаг 8. Переименовываем файл обратно.zip в.pptx. Запускаем (*рис. 8*).

[9] Extract files or objects from a PowerPoint file. URL: https://support.microsoft.com/en-us/office/extract-files-or-objects-from-a-powerpoint-file-85511e6f-9e76–41ad-8424-eab8a5bbc517

[10] Включение и отключение параметров элементов ActiveX в файлах Office. URL: https://support.microsoft.com/ru-ru/office/включение-и-отключение-параметров-элементов-office-f1303e08-a3f8–41c5-a17e-b0b8898743ed

[11] URL: https://vk.com/vkvideo

[12] URL: https://rutube.ru/

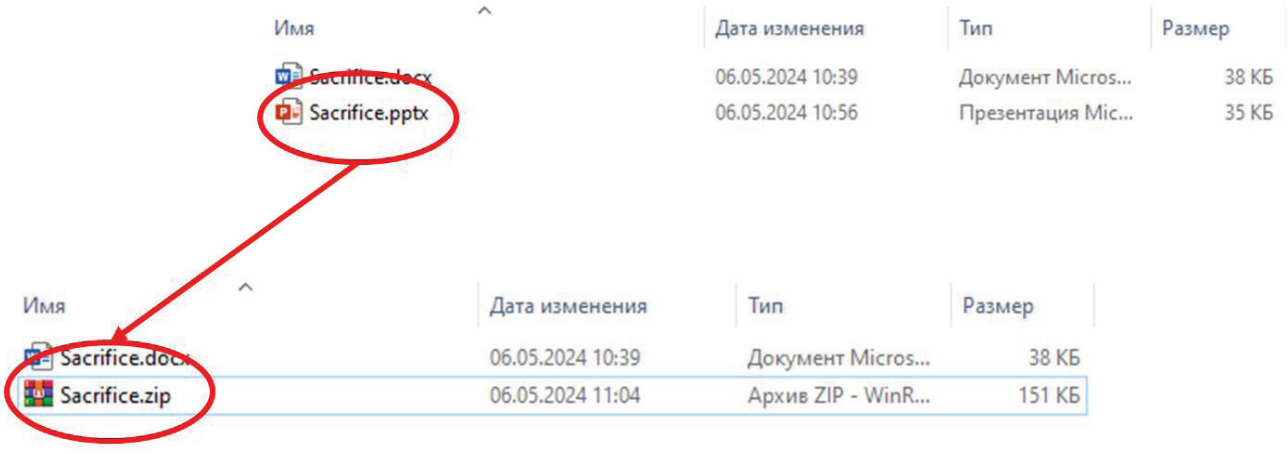

Рис. 5 / Fig. 5. **Меняем расширения презентации на расширение архиватора / Changing the Presentation Extensions to the Archiver Extension**

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

Рис. 6 / Fig. 6. **Содержимое файла slide1.xml.rels / Contents of the slide1.xml.rels File**

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

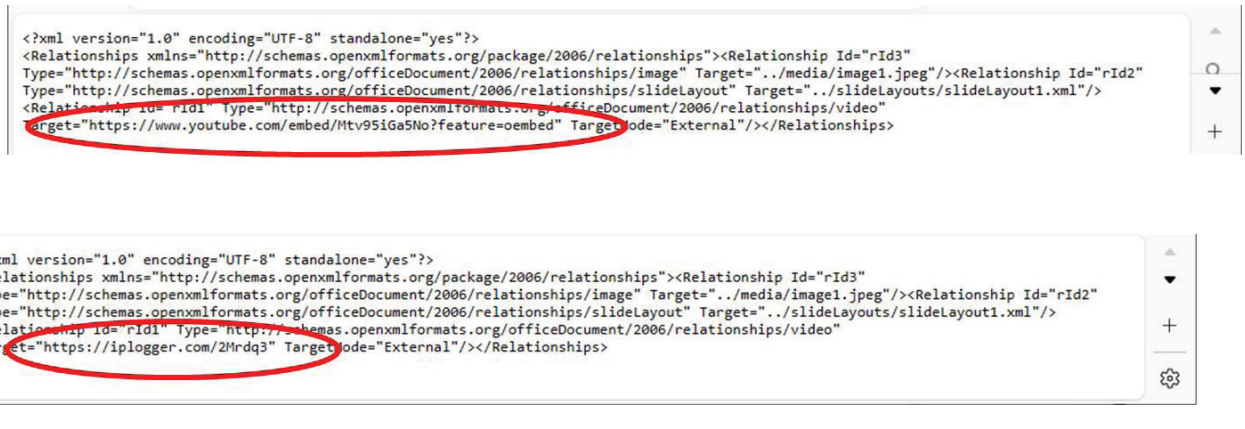

Рис. 7 / Fig. 7. **Подмена ссылки на редирект / Substitution of the Redirect Link**

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

На видеоролике нажимаем кнопку запуска PLAY. Система предложит запустить видео во внешнем браузере. Если пользователь согласится, то произойдет редирект IP-логгера на соответствующий ролик и система не «расскажет» про поддельную ссылку.

Аналогично предыдущим статьям, следует также обратить внимание на тот факт, что все манипуляции с целостностью файла.pptx не вызывали подозрения ни у одной установленной системы защиты информации.

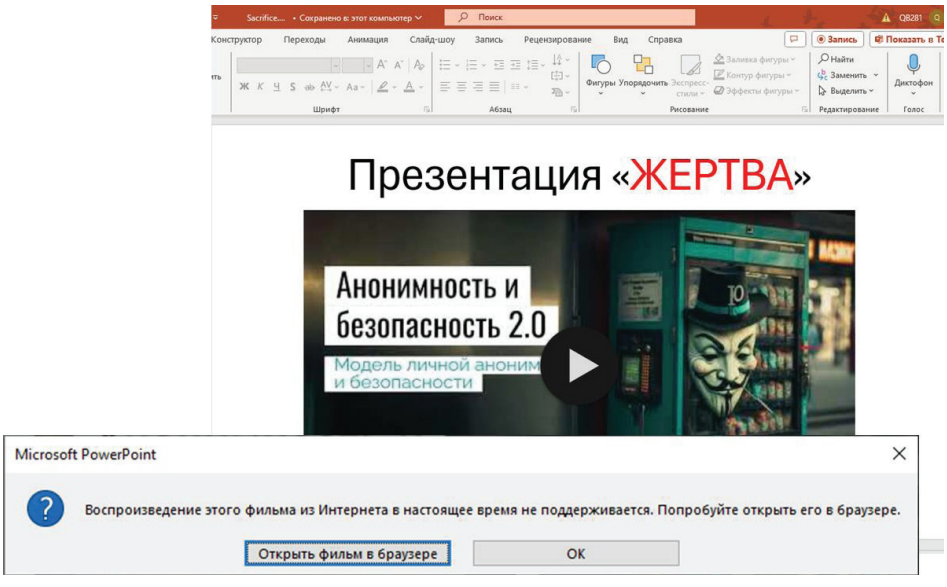

Рис. 8 / Fig. 8. **Запуск редирект ссылки / Launching a Redirect Link**

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

ВЫВОДЫ

В статье рассмотрен еще один механизм простой инъекции в популярный формат файлов[13] автоматизированного офиса. Забегая вперед, можно отметить, что это не единственный метод простой инъекции [3–8]. В следующих статьях будут рассмотрены «игры в прятки» непосредственно на файловом уровне. В саму структуру файла презентации можно добавлять произвольные ресурсы, несущие в себе вирусы, послания и прочую чуждую информацию.

[13] Спрятать файл внутри другого файла без потери работоспособности обоих. URL: https://programmersforum.ru/showthread.php?t=48995; Как спрятать файл внутри изображения. URL: https://ru.wikihow.com/спрятать-файл-внутри-изображения

СПИСОК ИСТОЧНИКОВ

1. Рыженко А.А., Козьминых С.И. Недекларируемые возможности файловой архитектуры: графические контейнеры. *Цифровые решения и технологии искусственного интеллекта.* 2025;1(3):55-61. DOI: 10.26794/3033-7097-2025-1-3-55-61
2. Рыженко А.А., Козьминых С.И. Недекларируемые возможности файловой архитектуры: Автоматизированный офис, текстовый редактор, формат Doc X. *Цифровые решения и технологии искусственного интеллекта.* 2025;1(4):60-68. DOI: 10.26794/3033-7097-2025-1-4-60-68
3. Petrosyan M.A., Usenko A.S. The concept and elements of criminalistics characteristics of unauthorized access to computer information. *Epomen. Global.* 2023;43:123-140. URL: https://elibrary.ru/mfcqwu
4. Елизаров М.М. Выявление уязвимостей и недекларированных возможностей в программном обеспечении. *Интернаука.* 2024;21-1(338):60-61. URL: https://elibrary.ru/DLCUNL
5. Бегаев А.Н., Кашин С.В., Маркевич Н.А., Марченко А.А. Выявление уязвимостей и недекларированных возможностей в программном обеспечении. СПб.: Университет ИТМО; 2020. 38 с. URL: https://elibrary.ru/xfaznp
6. Маркин Д.О., Макеев С.М., Санников И.А., Чунг Х.Т. Методика исследования системного программного обеспечения сетевого оборудования семейства Cisco на предмет наличия недекларируемых возможностей. *Ученые записки Орловского государственного университета.* 2020;3(88):215-221. URL: https://elibrary.ru/xyjmtf
7. Markin D.O., Makeev S.M., Ho Thaj Trung. Security threat level estimation for untrusted software based on TrustZone technology. *Proceedings of the Institute for System Programming of RAS.* 2022;34(1):35-48. DOI: 10.15514/ISPRAS-2022-34(1)-3
8. Жук Р.В. Методика и алгоритмы определения актуальных угроз информационной безопасности в информационных системах персональных данных. Дис. … канд. техн. наук. СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича; 2021. URL: https://elibrary.ru/prxzhx

REFERENCES

1. Ryzhenko A.A., Kozminykh S.I. Undeclared file architecture features: graphical containers. *Digital solutions and artificial intelligence technologies.* 2025;1(3):55-61. (In Russ.). DOI: 10.26794/3033-7097-2025-1-3-55-61
2. Ryzhenko A.A., Kozminykh S.I. Undeclared file architecture features: Automated office, text editor, DocX format. *Digital solutions and artificial intelligence technologies.* 2025;1(4):60-68. (In Russ.). DOI: 10.26794/3033-7097-2025-1-4-60-68
3. Petrosyan M.A., Usenko A.S. The concept and elements of criminalistics characteristics of unauthorized access to computer information. *Epomen. Global.* 2023;43:123-140. URL: https://elibrary.ru/mfcqwu
4. Elizarov M.M. Identification of vulnerabilities and undeclared features in software. *Internauka.* 2024;21-1(338):60-61. URL: https://elibrary.ru/DLCUNL (In Russ.).
5. Begaev A.N., Kashin S.V., Markevich N.A., Marchenko A.A. Identification of vulnerabilities and undeclared features in software. Saint Petersburg: ITMO University; 2020. 38 p. URL: https://elibrary.ru/xfaznp (In Russ.).
6. Markin D.O., Makeev S.M., Sannikov I.A., Chung H.T. Methodology for investigating the system software of Cisco network equipment for undeclared capabilities. *Scientific notes of the Orel State University.* 2020;3(88):215-221. URL: https://elibrary.ru/xyjmtf (In Russ.).
7. Markin D.O., Makeev S.M., Ho Thaj Trung. Security threat level estimation for untrusted software based on TrustZone technology. *Proceedings of the Institute for System Programming* of RAS. 2022;34(1):35-48. DOI: 10.15514/ISPRAS-2022-34(1)-3
8. Zhuk R.V. Methodology and algorithms for determining actual threats to information security in personal data information systems. Cand. Sci. (Tech.) thesis. St. Petersburg: St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch Bruevich, 2021. URL: https://elibrary.ru/prxzhx (In Russ.).

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 19.12.2025; после рецензирования 12.01.2026; принята к публикации 26.01.2026.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 19.12.2025; revised on 12.01.2026 and accepted for publication on 26.01.2026.
The authors read and approved the final version of the manuscript.