УДК 004.021

ПРИМЕНЕНИЕ МЕТОДОВ СТЕГАНОГРАФИИ ПРИ ОСУЩЕСТВЛЕНИИ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ

Щербакова Е.Д. (СПбГУТ)
Научный руководитель – начальник отдела развития профессиональных компетенций Кривоносова Н.В.
(СПбГУТ)

Введение. Стеганография – один из распространённых способов при осуществлении противоправных действий. Данный способ имеет много видов, что дает большие возможности злоумышленникам создать иллюзию, что файл безопасен. В этой работе будут рассмотрены основные причины выбора стеганографии злоумышленниками для осуществления противоправных действий и методы, которыми чаще всего происходят такие кибератаки.

Основная часть. Большинство злоумышленников используют методы стеганографии по двум основным причинам: передача информации, команд, инструкций по скрытым каналам, которые помогают злоумышленникам уклоняться от наблюдения правоохранительных органов, и встраивание вредоносных вирусов или программ в файлы. Во многих случаях для сокрытия вредоносного кода используются методы стеганографии, которые связаны с изображениями, так как имеют высокую степень защищённости от стегоанализа, из-за чего многие инструменты безопасности не видят в графических файлах опасность. Этот вид стеганографии позволяет отправлять большую информацию или загружать вредоносные программы, которые дают возможность подключиться к компьютеру жертвы или украсть учётные данные. Одним из векторов атак также стала текстовая стеганография, которая часто встречается в файлах .xlsx и .txt. Данные файлы могут хранить в себе как вредоносный код, так и изображение, которое облегчает атакующему получить доступ к системе. Вредоносные программы могут скрываться не только в файлах, но и на веб-страницах. Одним из примеров являются рекламные баннеры на экране компьютера, планшета или смартфона. В них встраивается вредоносный код, после загрузки которого пользователя перенаправляет на страницу, содержащую набор эксплойтов. Таким кибератакам можно противостоять, зная несколько способов защиты. Один из самых известных способов – никогда не нажимать/не открывать/не загружать подозрительные текстовые/аудио/графические файлы из неизвестных источников. Также можно установить антивирусные продукты, которые обеспечивают защиту от новейших вирусов и других видов вредоносного ПО.

Выводы. Использование методов стеганографии в противоправных действиях демонстрирует значительную угрозу интернет-пространству. Скрытие данных, взлом систем позволяют злоумышленникам успешно обходить системы безопасности и осуществлять незаконные операции с минимальными рисками быть выявленными. Это подчеркивает необходимость развития методов киберзащиты, а также повышения осведомлённости о рисках, связанных со стеганографией, как формой кибератак.

Список использованных источников:

1. Steganography: The Undetectable Cybersecurity Threat – URL: https://builtin.com/articles/steganography (дата обращения 23.01.2025).
2. Что такое стеганография? Определение и описание – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-steganography (дата обращения 23.01.2025).
3. Частикова Вера Аркадьевна, Аббасов Тимур Олегович, Аббасова Светлана

Станиславовна // МЕТОДИКА РАСПОЗНАВАНИЯ СКРЫТОЙ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ НА ОСНОВЕ АЛГОРИТМОВ СТЕГАНОГРАФИИ // Компьютерные и информационные науки, 2020 - URL: https://cyberleninka.ru/article/n/metodika-raspoznavaniya-skrytoy-informatsii-v-izobrazheniyah-na-osnove-algoritmov-steganografii (дата обращения 23.01.2025).

4. Вадим Гребенников // СТЕГАНОГРАФИЯ. ИСТОРИЯ ТАЙНОПИСИ // 2019 – URL:https://onlinelit.net/book/steganografiya-istoriya-taynopisi?ysclid=m6fjckcxq0438787265 (дата обращения 23.01.2025).