УДК 004.056

ОБЗОР ПЕРСПЕКТИВ ИСПОЛЬЗОВАНИЯ СТЕГАНОГРАФИИ В КАЧЕСТВЕ ИНСТРУМЕНТА ОБМЕНА СКРЫТЫМИ ДАННЫМИ В ПРОЦЕССЕ ОСУЩЕСТВЛЕНИЯ НЕПРАВОМЕРНЫХ ДЕЙСТВИЙ

Федосенко М.Ю. (Университет ИТМО)
Научный руководитель – профессор, доктор технических наук, Беззатеев С.В.
(Университет ИТМО)

Введение. В настоящее время интернет становится всё более прозрачным и контролируемым сегментом современной ИТ инфраструктуры. Буквально несколько десятилетий назад практически не существовало структурированных возможностей для контроля обрабатываемых в его просторах потоков информации. Иначе говоря, можно было размещать что угодно (детскую порнографию, экстремизм, продажу запрещённых к обороту объектов) с сомнительной возможностью установить лицо это осуществляющее и воспрепятствовать ему. Однако ведётся большой пласт работ, чтобы взять данные процессы под контроль, воспрепятствовать им, иметь возможность использовать в цифровой криминалистике при расследовании преступлений. В свою очередь, это приводит к тому, что преступникам нужно искать новые способы защиты своих нелегитимных данных от контроля извне, а специалистам по информационной безопасности разрабатывать новые способы для получения контроля над потоками данной информацией. В данной работе будет рассмотрен такой инструмент как стеганография и возможность её потенциального использования для обмена данными злоумышленниками, а также перспективы противодействия данному обмену со стороны специалистов информационной безопасности.

Основная часть. Среди способов контроля обрабатываемых в сети Интернет данных, стоит выделить разработку нормативно-правовых актов и законодательных проектов. В подавляющем своём большинстве, это поправки в Федеральный закон "Об информации, информационных технологиях и о защите информации" (например, так называемый «пакет Яровой»). Также стоит выделить технические методы, такие как блокирование доступа к нелегитимных (запрещённым) ресурсам, обязанность владельцев ресурсов по хранению всех обрабатываемых на интернет-ресурсе данных за последние 6 месяцев. Всё это позволяет получить контроль над информацией злоумышленников и восстановить цепочку действий при расследовании правонарушений.

Что касается выбора стеганографии как объекта исследования и её роли среди злоумышленников, то он обусловлен прежде всего её концептуальной особенностью. Стеганография скрывает сам факт наличия информация, что позволит преступникам обмениваться информацией при использовании легитимных данных, тем самым, не вызывая подозрений у правозащитников. Отсюда, основный направлением при работе с данной гипотезой является установить технические и практические возможности реализации скрытого обмена данных у злоумышленников, возможные способы противодействия преступникам, изучить имеющиеся результаты работ в данном направлении в научном сообществе. Концептуально, это можно декомпозировать на следующий перечень задач:

- Исследование характеристик нарушителей, их целей, особенностей поведения, потенциального мотива использования стеганографии,
- Исследования инструментария для стегановложения и среды связи на возможность обмена скрытыми вложениями,
- Разработка методов стеганоанализа и защиты среды связи от возможности осуществления скрытого обмена данными.

Что касается первой задачи, то учёными были установлены случаи использования стеганографии с целью нарушения информационной безопасности. Например, в работе Cho D.

X. и др [1] описано применение стеганографии в сетевых пакетах для обмена вредоносными данными, Bassil Y. [2] представил реализацию сети даркнет при помощи текстовой стеганографии за счёт скрытия одной веб страницы внутри другой, Garcia N. [3] описывает тенденцию использования стеганографии злоумышленниками в киберпреступлениях, Никулина Т. В. [4] упоминает успешные атаки на компьютерные системы с применением методов стеганографии. Всё это говорит о том, что стеганография является востребованным инструментом среди нарушителей.

Что касается второй задачи, то были проведены исследования возможностей использования стеганографических методов для скрытого обмена данными. Araujo I. I и др. [5] в своей работе исследует сокрытие данных в PDF файлах и возможности последующего их обмена по электронной почте. Mohd Hilal Muhammad и др. [6] описывают применение математических техник при разработке методов стеганографии, основанных на функциях текста, а также перспективы его дальнейшего практического применения. Смирнов В.А., и Ермошин А.В. [7] описывают возможности сокрытия архива внутри JPEG изображения и процесс его обмена в интернете. Рудниченко А. К [8] в своей статье демонстрирует возможности реализации простых методов стеганографии без использования дополнительного программного обеспечения.

Что касается третьей задачи исследования, то в настоящее время уже ведутся разработки методов противодействия скрытому обмену данных. В работе Сирота А.А. [9] и др. рассматривается применение машинного обучения при стеганоанализе с учётом математических особенностей различных классификаторов. Аналогичные исследовательские задачи с применением машинного обучения описывает в своей работе Ki-Hyun Jung [10], однако делает упор на обучение моделей с учётом особенностей стеганографических алгоритмов. О.О. Шумская и В.Ю. Будков. [11] представляют сравнительное исследование методов классификации в стегоанализе цифровых изображений, где основной упор сделан на предобработку наборов данных стеганоконтейнеров.

Выводы. Таким образом, проблема использования стеганографии в качестве инструмента обмена данными у злоумышленников является актуальной, и научное сообщество активно её исследует. Среди уже имеющихся результатов стоит подчеркнуть наличие возможностей реализации скрытого обмена, имеющиеся примеры успешной реализации при совершении преступлений, предлагаемые учёными методы для стеганоанализа данных в информационных системах. При разработке методов противодействия в рамках решения задач информационной безопасности основной упор необходимо делать на нормативно-правовые акты, программные методы стеганоанализа и возможности их совместного использования с технологиями искусственного интеллекта.

Список использованных источников:

1. Cho D. X., Thuong D. T. H., Dung N. K. A Method of Detecting Storage Based Network Steganography Using Machine Learning //Procedia Computer Science. – 2019. – Т. 154. – С. 543-548.]
2. Bassil Y. Text Steganography: The Deep Web in Plain Sight.
3. Garcia N. Digital steganography and its existence in cybercrime //dimensions. – 2018. – Т. 640. – С. 480.
4. Никулина Т.В. Выявление вредоносного кода в графических файлах, внедренного с помощью методов стеганографии / Никулина Т.В. – Текст: непосредственный // Матрица научного познания. - 2021. - № 1-2. - С. 62-67.
5. Araujo I. I. et al. Vulnerability exploitations using steganography in PDF files //International Journal of Computer Networks and Applications (IJCNA). – 2020. – Т. 7. – №. 1. – С. 10-18.

6. Muhammad M. H. et al. Review on feature-based method performance in text steganography //Bulletin of Electrical Engineering and Informatics. – 2021. – Т. 10. – №. 1. – С. 427-433.]

7. Ермошин А.В. Возможности использования методов стеганографии при публикации изображений в социальной сети Вконтакте / Ермошин А.В., Смирнов В.А. – Текст: непосредственный // Современные технологии в науке и образовании - СТНО-2020: тезисы III Международного научно-технического форума: 8-10 декабря 2020 года, Рязань - Рязань, 2020. - С. 145-149.

8. Рудниченко А.К. Применение простой стеганографии при передаче файлов в Интернете / Рудниченко А.К. – Текст: непосредственный // Молодой ученый. - 2017. -№ 3 (137). - С. 49-51.

9. Сирота А.А. Стегоанализ цифровых изображений с использованием методов поверхностного и глубокого машинного обучения: известные подходы и новые решения / Сирота А.А., Дрюченко М.А., Иванков А.Ю. . – Текст: непосредственный // Вестник Воронежского государственного университета. - Серия: Системный анализ и информационные технологии. - 2021. - № 1. - С. 33-52.

10. Jung K. H. A study on machine learning for steganalysis //Proceedings of the 3rd International Conference on Machine Learning and Soft Computing. – 2019. – С. 12-15.

11. Шумская О.О. Сравнительное исследование методов классификации в стегоанализе цифровых изображений / Шумская О.О., Будков В.Ю. . – Текст: непосредственный // Научный вестник Новосибирского государственного технического университета. - 2018. - № 3 (72). - С. 121-134.

Федосенко М.Ю. (автор) Подпись

Беззатеев С.В. (научный руководитель) Подпись