УДК 004.77 (045)

В.В. Шостак

В.В. Лукічов

Метод та засіб виявлення ознак кіберзлочинів в Телеграм каналах

Вінницький національний технічний університет

Анотація
Досліджено способи виявлення та аналізу кіберзлочинів в телеграм каналах.
Ключові слова: *моніторинг, кіберзлочини, Телеграм*

Abstract
Methods and analysis of cybercrimes in Telegram channels have been studied.
Keywords: *monitoring, cyber crimes, Telegram*

Інформаційна безпека стає ключовим фактором у боротьбі з кіберзлочинністю, зокрема в умовах активного поширення інформаційних технологій та соціальних мереж. Телеграм-канали, завдяки своїй відкритості та широкій аудиторії, стали платформою для здійснення різноманітних незаконних дій, включно з координацією кіберзлочинів. Виявлення таких загроз є важливим завданням для захисту суспільства від шкідливих дій, таких як фішинг, поширення шкідливих програм або дезінформація. Одним з ефективних підходів є розроблення методу та засобу для виявлення ознак кіберзлочинів у Телеграм-каналах. Це дозволяє автоматизувати моніторинг, збір і аналіз інформації для запобігання та своєчасного реагування на кіберзагрози.

Дослідження показало, що використання спеціалізованих засобів для моніторингу Телеграм-каналів може ефективно виявляти ознаки кіберзлочинів. Метод заснований на застосуванні сучасних технологій аналізу тексту, таких як обробка природної мови (NLP), машинне навчання та аналіз великих даних. Ці технології дозволяють системі ідентифікувати підозрілі патерни в поведінці учасників каналів, аналізувати зміст повідомлень та виявляти небезпечні або нелегальні активності. Вони мають такі ключові ознаки кіберзлочинів:

- Використання специфічних термінів, які часто зустрічаються в контексті злочинної діяльності (наприклад, "хак", "фішинг", "ддос").
- Посилання на нелегальні ресурси або файли, які можуть містити шкідливе програмне забезпечення.
- Координація дій, що може вказувати на підготовку до кібератак або інших злочинів.

Засіб, розроблений для виявлення таких ознак, може проводити автоматизований збір даних з Телеграм-каналів, зберігати ці дані в базі для подальшого аналізу та здійснювати фільтрацію повідомлень за ключовими словами, які можуть вказувати на кіберзлочини. Також інструмент дозволяє відстежувати шлях поширення повідомлень, що допомагає визначити джерело злочинної активності. Це особливо важливо для ідентифікації першоджерела фейкових новин або шкідливого програмного забезпечення.

Додатково було виявлено, що інтеграція засобу з системами штучного інтелекту може значно підвищити ефективність аналізу великих обсягів даних, що генеруються в Телеграм-каналах. Завдяки цьому можливо швидше ідентифікувати нові загрози, які з'являються в режимі реального часу, та відстежувати зміни в поведінкових патернах злочинних груп. Автоматизація процесів збору та аналізу інформації дозволяє зменшити навантаження на фахівців з безпеки та підвищити оперативність виявлення загроз.

Дослідження показало, що цей підхід дозволяє значно підвищити ефективність виявлення кіберзлочинів у порівнянні з традиційними методами, такими як OSINT. Тоді як OSINT фокусується переважно на загальнодоступних даних, моніторинг Телеграм-каналів дозволяє охоплювати ширше коло джерел, включно з приватними або закритими групами, які часто використовуються злочинцями для координації своїх дій.

Результати дослідження підтверджують, що метод та засіб для виявлення ознак кіберзлочинів у Телеграм-каналах є важливим інструментом у боротьбі з кіберзагрозами. Запровадження таких систем дозволяє ефективно виявляти потенційні загрози та своєчасно реагувати на них. Використання сучасних технологій аналізу тексту, машинного навчання та обробки даних значно підвищує точність та швидкість ідентифікації небезпечної активності. Це, в свою чергу, сприяє покращенню інформаційної безпеки та захисту суспільства від кіберзлочинів.

Такий засіб може бути корисним не лише для правоохоронних органів, а й для компаній, урядових установ та інших організацій, які зацікавлені в захисті своїх інформаційних ресурсів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Lawson R. Web Scraping With Python: Scrape Data from Any Website With the Power of Phython. 2015. P. 151
2. Al-Sakib K., Mohiuddin A. Data Analytics: Concepts, Techniques, and Applications. 2018. P. 450
3. Bielska A., Anderson N., Benetis V., Viehman C.. Open source intelligence tools and resources handbook [Електронний ресурс] – Режим доступу до ресурсу: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_June-2018_Final.pdf.

Шостак Володимир Володимирович *– студент групи 1БС-23м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vovkashostak@gmail.com*

Лукічов Віталій Володимирович *– к. т. н. , доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, lukichov.vitalyi@vntu.edu.ua*

Volodymyr Shostak – *student of group 1BS-23m, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vovkashostak@gmail.com*

Vitaliy Lukichov – *p. h. d., Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, lukichov.vitalyi@vntu.edu.ua*