УДК 004.056

Воєвода А.В.
Майданевич Л.О.

ФІЛЬТРАЦІЯ КОНТЕНТУ В РЕАЛЬНОМУ ЧАСІ: ЯК TELEGRAM-БОТИ ЗАХИЩАЮТЬ ВІД СПАМУ ТА ШАХРАЇВ

Вінницький національний технічний університет

Анотація

Зі зростанням популярності месенджера Telegram значно активізувалися спам- та шахрайські атаки, спрямовані на групові чати та публічні канали. У роботі розглянуто методи фільтрації контенту в реальному часі з використанням автоматизованих ботів-модераторів. Особливу увагу приділено аналізу можливостей таких ботів, як Group Help, Combot та Shieldy, які застосовують фільтрацію за ключовими словами, CAPTCHA-верифікацію, поведінковий аналіз та системи попереджень. Показано, що впровадження автоматичної модерації значно підвищує рівень інформаційної безпеки спільнот.

Ключові слова : Telegram, спам, фільтрація контенту, бот-модератор, кібербезпека.

Abstract

With the rapid growth of Telegram’s popularity, spam and fraud attacks targeting group chats and public channels have intensified. This paper examines real-time content filtering methods using automated moderation bots. Special attention is given to the capabilities of bots such as Group Help, Combot, and Shieldy, which apply keyword filtering, CAPTCHA verification, behavioral analysis, and warning systems. It is demonstrated that automated moderation significantly enhances the cybersecurity level of online communities.

Keywords: Telegram, spam, content filtering, moderation bot, cybersecurity

Вступ

Telegram став однією з найпопулярніших платформ для спілкування завдяки своїй швидкості, простоті використання та можливості створювати великі відкриті спільноти. Проте разом із зростанням популярності платформа стала привабливою для зловмисників, які використовують її для розсилки реклами, шахрайських схем, фішингових посилань або масового флуду. У великих чатах, де щоденно надсилаються сотні або тисячі повідомлень, ручна модерація є практично неможливою. Тому актуальним завданням є впровадження систем автоматичної фільтрації контенту, здатних у реальному часі виявляти небажані повідомлення та блокувати порушників. У цьому контексті особливу роль відіграють Telegram-боти, які виконують функції "цифрових охоронців" онлайн-спільнот.

Результати дослідження

Дослідження показало, що у Telegram доступні різні інструменти для контролю контенту, які можна умовно поділити на кілька груп. Одним із основних методів є фільтрація за ключовими словами та шаблонами. Так, бот Combot дозволяє створювати списки заборонених слів, емодзі, доменів або фраз, і при їхньому виявленні повідомлення автоматично видаляються. Іншим важливим інструментом є CAPTCHA-верифікація нових учасників. Бот Shieldy, наприклад, вимагає, щоб кожен, хто приєднується до чату, підтвердив свою присутність за допомогою кнопки або емодзі. Якщо цього не зроблено, акаунт видаляється, що ефективно запобігає спам-ботам. Також у Telegram використовуються методи поведінкового аналізу, або антифлуд. Боти, такі як Group Help, здатні

виявляти підозрілу активність, наприклад, надсилання великої кількості повідомлень або однотипних символів. При повторних порушеннях бот видає попередження або блокує користувача. Додатково модератори можуть використовувати списки репутації та глобальні чорні списки, які містять інформацію про відомі спамерські акаунти, що дозволяє швидко блокувати потенційно небезпечних користувачів. Нарешті, аналітика та звітність стають важливим інструментом для оцінки ефективності модерації. Бот Combot, наприклад, надає статистику щодо кількості заблокованих порушників, що допомагає керівникам груп коригувати налаштування фільтрів.

Рекомендації для користувачів Telegram

Для підвищення безпеки у групових чатах та каналах рекомендується обов'язково використовувати CAPTCHA або верифікацію нових учасників. Важливо налаштовувати фільтри за ключовими словами, особливо у технічних та фінансових групах. Замість миттєвих банів доцільно застосовувати систему попереджень, щоб уникати конфліктів з реальними користувачами. Правила фільтрації слід періодично оновлювати відповідно до нових шахрайських схем, а автоматичну модерацію поєднувати з людським наглядом для спірних випадків.

Висновки

Використання Telegram-ботів для фільтрації контенту є ефективним засобом протидії спаму та шахрайству. Завдяки автоматичній модерації адміністратори спільнот можуть зменшити навантаження на себе та захистити учасників від небажаного контенту. Найбільш результативними є комплексні рішення, що включають CAPTCHA, фільтри за ключовими словами та поведінкову аналітику.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Telegram Bot API Documentation. Офіційний портал для розробників. URL: [підозріле посилання видалено] (дата звернення: 18.10.2025).
2. Group Help Bot — Official Documentation. Інструкції з налаштування антифлуду та безпеки. URL: https://www.grouphelp.top/ (дата звернення: 20.10.2025).
3. Combot Moderation Platform. Аналітика та інструменти модерації для Telegram. URL: https://combot.org (дата звернення: 28.10.2025).
4. Shieldy Bot GitHub Repository. Відкритий вихідний код та логіка роботи CAPTCHA-верифікації. URL: https://github.com/backmeupplz/shieldy (дата звернення: 01.03.2026).
5. OWASP Automated Threat Handbook. Рекомендації щодо захисту від автоматизованих загроз (ботів). URL: https://owasp.org/www-project-automated-threat-handbook/ (дата звернення: 02.03.2026).
6. Cloudflare: What is a Content Moderation Bot? Огляд технологій фільтрації контенту в реальному часі. URL: https://www.cloudflare.com/learning/bots/what-is-content-moderation-bot/ (дата звернення: 03.03.2026).
7. IEEE Xplore: Machine Learning Techniques for Spam Detection in Instant Messengers. Наукова стаття про використання ШІ для виявлення спаму. URL: https://ieeexplore.ieee.org/ (пошук за темою: Spam Detection Telegram, дата звернення: 03.03.2026).
8. Telegram Anti-Spam (Internal) Logic Updates. Офіційний блог Telegram про впровадження системного антиспам-фільтра. URL: https://telegram.org/blog/ (дата звернення: 02.03.2026).
9. Cybersecurity & Infrastructure Security Agency (CISA): Phishing Infographic. Матеріали щодо розпізнавання фішингових посилань, що використовуються в месенджерах. URL: https://www.cisa.gov/resources-tools/resources/phishing-infographic (дата звернення: 01.03.2026).
10. Rose Bot Documentation. Посібник з налаштування одного з найпопулярніших ботів-адміністраторів Miss Rose. URL: https://missrose.org/guide/ (дата звернення: 03.03.2026).
11. Check Point Research: Telegram as a Command and Control Center. Дослідження про використання Telegram зловмисниками. URL: https://research.checkpoint.com/ (дата звернення: 02.03.2026).

Воєвода Аліна Віталіївна – студентка групи 1БКС-24б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: alinavoievoda77@gmail.com

Науковий керівник : **Майданевич Леонід Олександрович –** доцент кафедри ЗІ, к.філос.н., Вінницький національний технічний університет, Вінниця.