УДК 004.942

О. Р. Сташевська

ПРОЯВИ МЕРЕЖЕВОГО ШАХРАЙСТВА В СУЧАСНОМУ СВІТІ

Вінницький національний технічний університет

Анотація

Зроблено огляд проявів шахрайства в мережі Інтернет. Запропоновано виявлення мережевого шахрайства з використанням нечіткої логіки на прикладі шаблонів інформаційної атаки.

Ключові слова: мережеве шахрайство,шаблон інформаційної атаки, нечітка логіка,Інтернет-реклама.

Abstract

A review of the manifestations of fraud on the Internet is made. We propose to detect network fraud using fuzzy logic as an example of information attack templates.

Keywords: network fraud, an information attack template, fuzzy logic, Internet advertising.

Вступ

Реклама в мережі Інтернет є невід'ємною частиною багатьох сфер діяльності людини. Більшість рекламних Інтернет-оголошень оплачується за кліки. Кожного разу при натисканні на рекламне оголошення з рекламодавця стягується певна плата. Така модель породжує специфічний різновид мережевого шахрайства: склікування (споказування), коли зацікавлена особа генерує недійсні кліки (покази) з метою розтрати бюджету рекламодавця [1]. Постачальники послуг Інтернет-реклами постійно вдосконалюють свої системи захисту від склікування, однак рівень шахрайства в галузі Інтернет-реклами стрімко зростає.

Результати дослідження

На сьогоднішній день існує найпоширеніша система оплати рекламних послуг в мережі за схемами: CPC (плата за кожен клік та перехід по рекламному оголошенню) та CPM (плата за кожну тисячу показів оголошення) [2]. Дані схеми і роблять рекламну кампанію вразливою до склікування та споказування.

Аналізуючи існуючі методи для визначення мережевого шахрайства типів склікування та споказування, авторами в роботі [3] було запропоновано альтернативний підхід: проводиться аналіз інтернет-трафіку на стороні рекламодавця, тобто використовується тільки доступна йому інформація [1]. Запропонований підхід базується на визначенні типових шаблонів поведінки шахраїв. Одним з таких шаблонів є шаблон інформаційної атаки [4], що зображений на рис. 1 [1].

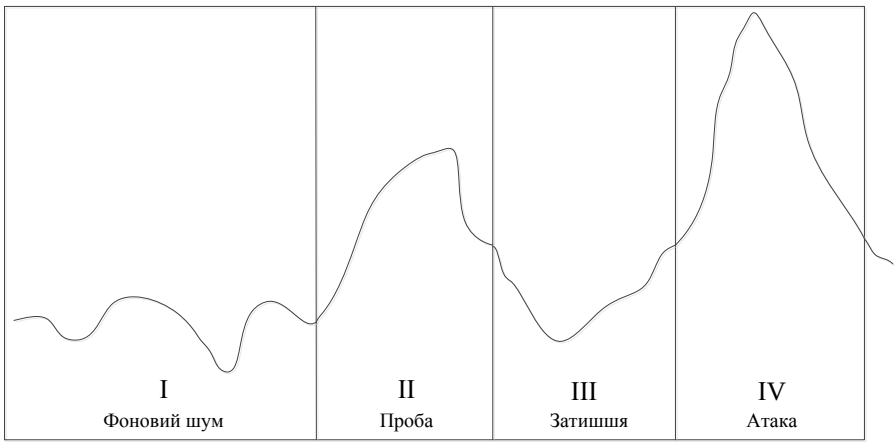

Рис. 1 – Шаблон інформаційної атаки

Шаблон має чотири фази, які у випадку склікування та споказування відповідають:

I. звичайній активності користувачів (природній рівень кліків);
II. першій спробі нападу;
III. вичікуванню результатів;
IV. склікуванню (споказування) оголошення.

Аналізуючи публікації по темі дослідження, існуючі методи виявлення мережевого шахрайства поділяються на три групи [5]:

1. методи, що базуються на пошуку відхилень від норми активності користувачів;
2. методи визначення шахрайства за допомогою класифікаторів;
3. алгоритми, які базуються на правилах.

Для роботи методів третьої групи важливим є визначення правил, які показують поведінку шахраїв, експертами. Алгоритми, що базуються на правилах є тотожними теорії нечітких обчислень, яка дозволяє оперувати поняттями подібними до людської мови та будувати логічні висновки, що наближені за своєю структурою та різноманітністю до тих, якими оперує людина [1]. Застосування теорії нечіткої логіки є актуальним для визначення мережевого шахрайства, а також для створення шаблонів інформаційної атаки.

Висновки

У ході дослідження було проаналізовано прояви мережевого шахрайства в сучасному світі. Виявлено актуальність використання інтелектуальних технологій для створення шаблонів інформаційної атаки на основі нечіткої логіки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Використання нечіткої логіки для визначення мережевого шахрайства на прикладі шаблону інформаційної атаки / Д. Г. Павлов, О. Р. Чертов // 20-th International conference on System Analysis and Information Technology SAIT 2018. – 2018. – С.142-143.
2. Павлов Д. Г. Захист рекламної Інтернет-кампанії від мережевого шахрайства / Д. Г. Павлов // Наукові праці. Комп'ютерні технології. — 2012. — Вип. 179. — Том 191. — С. 81—86.
3. О.Р. Чертов, Д.Г. Павлов, В.В. Мальчиков, and М.В. Александрова. "Виявлення аномальної поведінки користувача системи контекстної реклами" // Штучний інтелект, no. 4, pp. 476–483, 2010.
4. В.М. Фурашев, Д.В. Ланде. "Практичні засади прогнозування можливих загроз та ризиків шляхом аналізу взаємозв'язку подій з інформаційним простором" // Открытые информационные и компьютерные интегрированные технологии: сб. науч. трудов, no. 42, pp. 194–203, 2009.
5. Павлов Д. Г. Інформаційна технологія захисту від мережевого шахрайства на базі моделювання поведінки зловмисників / Д. Г. Павлов // Інформаційна безпека, №2. — 2013.— С. 109—116.

Сташевська Олена Русланівна — студентка групи 1БС-15б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: poleshkolena@gmail.com.

Науковий керівник: ***Кондратенко Наталія Романівна*** — канд. техн. наук, професор кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: kondrn2014@gmail.com.

Olena Stashevska - student of the group 1BS-15b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: poleshkolena@gmail.com.

Supervisor: ***Kondratenko Natalia Romanivna*** – Cand. tech Sciences, professor of information security, Vinnytsia National Technical University, Vinnytsya, e-mail: kondrn2014@gmail.com.