УДК 004.942

Павлов Д.Г.

МОДЕЛЬ ПОВЕДІНКИ ЗЛОВМИСНИКІВ ПРИ РОЗМІЩЕННІ ІНТЕРНЕТ-РЕКЛАМИ ІЗ СХЕМОЮ ОПЛАТИ ЗА ТИСЯЧУ ПОКАЗІВ

Розглядається взаємодія суб'єктів в процесі створення та проведення рекламних кампаній в Інтернеті. Розроблена одна з можливих моделей поведінки зловмисників при розміщені реклами з схемою оплати за тисячу показів. Продемонстрована можливість застосування вейвлет-перетворення для аналізу отриманих часових рядів.

Ключові слова: *інтернет-реклама, плата за тисячу показів, CPM, вейвлет-перетворення.*

Рассматривается взаимодействие субъектов в процессе создания и проведения рекламных кампаний в Интернете. Разработана одна из возможных моделей поведения злоумышленников при размещении рекламы по схеме оплаты за тысячу показов. Продемонстрирована возможность применения вейвлет-преобразования для анализа получающихся временных рядов.

Ключевые слова: *интернет-реклама, плата за тысячу показов, CPM, вейвлет-превращение.*

Interaction between Internet-advertising participants is considered. One of the possible fraudster behavior models in cost-per-mille advertising system has been developed. Possibility of wavelet transform application for received time series analysis is shown.

Key words: *internet-advertising, paying for thousand shows, CPM, veyvlet-transformation.*

ВСТУП. ВЗАЄМОДІЯ УЧАСНИКІВ ПРОБЛЕМНОЇ ГАЛУЗІ

Реклама є одним із основних інструментів маркетингу. Існує багато різновидів реклами: реклама на телебаченні, радіо, в пресі тощо [1]. В останні роки високою популярністю серед рекламодавців та лояльністю серед споживачів користується Інтернет-реклама. Вважається, що доля ринку реклами в мережі Інтернет стрімко зростатиме [2].

В процесі створення та проведення рекламної кампанії в Інтернеті можуть бути задіяні наступні учасники: рекламодавець, рекламне агентство, пошукова мережа, рекламний майданчик та клієнт (людина, до якої адресовані всі рекламні повідомлення). Характер їх взаємодії відображено на рис. 1.

Якщо рекламодавець вирішує розмістити свої оголошення в Інтернеті, він може зробити це самостійно, використавши автоматизовані продукти, що надають такі рекламні мережі як Google та Яндекс. В цьому випадку йому необхідно самостійно розбиратися з налаштуваннями рекламних кампаній.

Альтернативним варіантом є використання послуг рекламних агентств. Головною перевагою такого підходу є те, що працівники спеціалізованих агентств володіють відповідними знаннями, тому можуть забезпечити проведення рекламної кампанії на високому рівні.

Оплата послуг розміщення реклами залежить від обраної моделі рекламної кампанії. Модель CPC (cost per click) передбачає плату за кожен клік (тобто перехід) по оголошенню. Обираючи модель CPM (cost per mille) рекламодавець оплачує кожну тисячу показів. Модель CPA (cost per action) гарантує, що оплачуватись буде тільки деяка, заздалегідь визначена дія відвідувача [3].

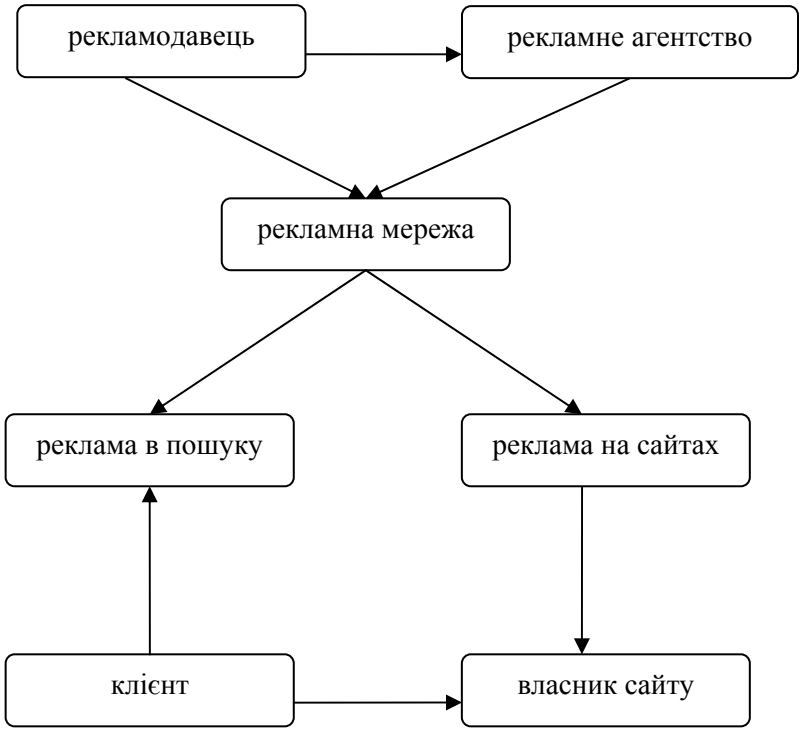

Рис. 1. Взаємодія учасників проблемної галузі Інтернет-реклами

В залежності від налаштувань рекламної кампанії оголошення будуть розміщуватися в якості результатів пошуку за деякими визначеними ключовими словами або на суміжних за тематикою сайтах. Власник сайту, на якому розміщені рекламні оголошення, отримує певну суму за переходи по оголошеннях або за тривалість їх розміщення на сайті.

Інтернет-реклама відкриває нові можливості для шахрайства [4]. Дійсно, генерація штучних кліків («склікування») або показів («споказування») не є важкою задачею. Проводити відповідні неправомірні дії може як людина, так і спеціальне програмне забезпечення.

Можна виділити ряд потенційних зловмисників в галузі Інтернет-реклами. Здійснювати «склікування» (при моделі CPC) або «споказування» (при моделі CPM) можуть різні групи учасників. Наприклад, власник сайту – з метою збільшення власних доходів, рекламодавець – для нанесення матеріальних збитків своїм конкурентам тощо.

Більшість алгоритмів виявлення недійсних кліків базуються на кількості показів оголошення між послідовними кліками [5], тому генерування штучних показів може також використовуватись як елемент склікування.

Визначення недійсних кліків є актуальною проблемою сьогодення Інтернет-реклами. Велика кількість робіт присвячена проблемі виявлення склікування, запропоновано декілька підходів: порівняння поточної активності відвідувачів з їх активністю в минулому, алгоритми, засновані на правилах [6], аналіз передісторії індивідуальної активності користувачів, використання альтернативних моделей рекламних кампаній, як то: плата за дію, плата за відсоток показів [7]. В той же час задача визначення недійсних показів привертає менше уваги дослідників.

ПОСТАНОВКА ЗАВДАННЯ

Метою даної роботи є побудова однієї із можливих моделей поведінки зловмисників при використанні моделі CPM, яку можна було б в подальшому використовувати для визначення недійсних показів.

МОЖЛИВА МОДЕЛЬ ПОВЕДІНКИ ЗЛОВМИСНИКІВ ПРИ ВИКОРИСТАННІ СХЕМИ CPM

Модель cost per mille була основною для першого покоління реклами в Інтернеті [5]. Хоча ця модель має деякі очевидні недоліки (рекламодавець змушений платити за кожну тисячу показів

не залежно від того, чи привернув хоча б один з них увагу потенційного клієнта), вона досі широко використовується.

Одним із можливих зловмисників за такої моделі є рекламодавець, який бажає підірвати рекламну кампанію своїх конкурентів. Його діяльність визначається такими елементами рекламної кампанії як позиція оголошення та розмір денного бюджету.

Позиція оголошення при показі залежить від показника якості CTR (click through rate – відношення кількості переходів до кількості показів) і ставки CPM (максимальна сума, яку рекламодавець згоден платити за тисячу показів). Чим вищі значення цих показників, тим більш високу позицію отримує оголошення. Кількість показів визначається розміром рекламного бюджету. Якщо він вичерпаний, то показ на поточний день припиняється. Оновлення бюджету відбувається в 00:00, тому після опівночі рекламне повідомлення знову з'явиться в мережі.

Метою шахрайства в даному випадку є вичерпання денного бюджету більш успішних підприємців для отримання вищої позиції при показі.

Зловмисник не може знати напевно розмір денного бюджету конкурентів, тому можливою є наявність підготовчого етапу, а саме: розвідувальних дій. Наприклад, деякого визначеного дня нападник може відключити свою рекламу та згенерувати серію штучних показів.

За наявності підготовчого етапу ця модель поведінки зловмисника буде певним аналогом інформаційної атаки [8]. Фазам «проби», «затишок» й «атака» відповідатимуть розвідувальні дії (оголошення зловмисника не демонструється, тобто кількість показів дорівнює нулю), природній рівень показів (тимчасове припинення впливу, для зниження ймовірності виявлення шахрайства) та напад.

На часовому ряді кількості показів оголошень, які зазнали нападу, відповідні фази відобразяться у вигляді двох однакових за величиною екстремумів, адже кількість показів в обох випадках визначатиметься розміром денного бюджету (Рис. 2).

Рис. 2. Кількість показів оголошень щоденно

Використовуючи модель CPM, можна встановити часові рамки показу оголошення. Наприклад, якщо відомо, що загальна маса потенційних клієнтів знаходиться в мережі впродовж робочого дня, то доцільним є встановлення саме цього періоду в якості часового інтервалу показу оголошення.

В такому випадку зловмисник буде атакувати оголошення конкурентів тільки в той період, коли його власне рекламне повідомлення не демонструється, інакше буде вичерпуватись його власний рекламний бюджет. Очевидно, що конкуренти так само можуть встановити оптимальні часові рамки для показу своїх оголошень, які можуть співпадати з відповідними параметрами рекламної кампанії зловмисника. Тому, використання для атаки того проміжку часу, коли оголошення не демонструються через відсутність в мережі потенційних клієнтів, не може гарантувати успіх.

Зловмисник може зменшити часові рамки показу свого оголошення. Для нападу буде використовуватись той інтервал часу, коли реклама конкурентів вже демонструється, а реклама зловмисника – ще ні. На рис. 3 зображені часові ряди кількості показів по годинам оголошення зловмисника та одного з оголошень, що зазнало нападу.

Рис. 3. Часові ряди кількості показів по годинам

Перший максимум на часовому ряді оголошення, що зазнало нападу, відповідає розвідувальним діям, він більш пологий і не такий локалізований, як глобальний екстремум, що відповідає нападу. На графіку також видно, що під час «проби» та «атаки» оголошення зловмисника не демонструвалося, це свідчить про відключення показу реклами та зміщення часового інтервалу показу відповідно.

Отримані часові ряди можуть бути проаналізовані різними методами, але в якості найбільш перспективного нам видається вейвлет-перетворення. Особливістю даного методу є те, що він дозволяє виділяти різкі зміни. На рисунках 4 та 5 наведено результати неперервного вейвлет-перетворення кожного з часових рядів. На вейвлет-скейлограмах та скелетонах чітко відображаються локальні та глобальні екстремуми, які свідчать про наявність шаблону, характерного для розглянутого нападу зловмисника.

ВИСНОВКИ

В результаті аналізу взаємодії учасників процесу була запропонована модель поведінки однієї з груп зловмисників в рекламній моделі CPM, описані основні особливості цієї моделі. Для визначення наявності шахрайських дій пропонується використовувати вейвлет-аналіз як ефективний засіб виявлення аномалій в сигналах різноманітної природи.

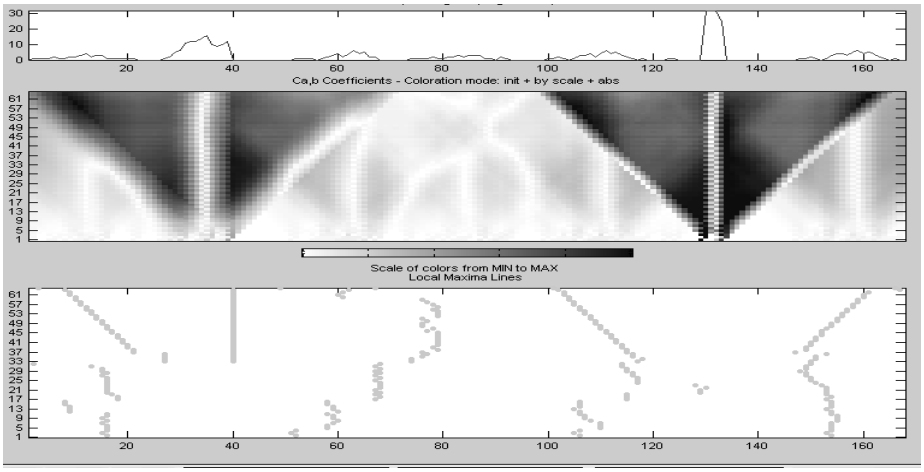

Рис. 4. Неперервне вейвлет-перетворення часового ряду кількості показів оголошення, що зазнало нападу

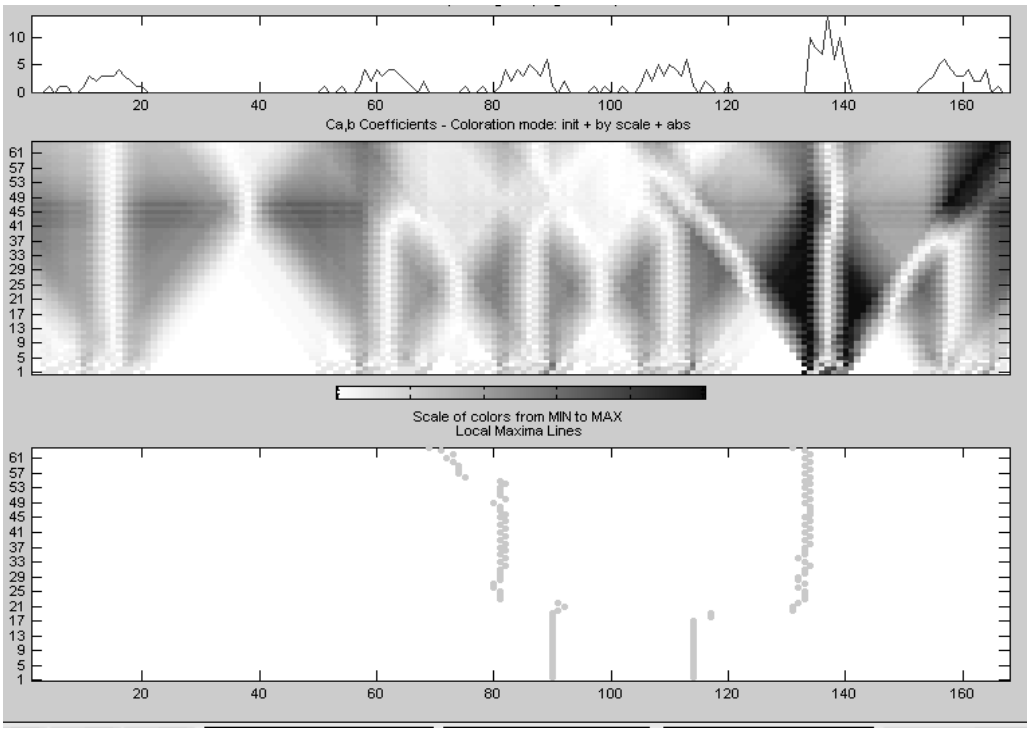

Рис. 5. Неперервне вейвлет-претворення часового ряду кількості показів оголошення зловмисника

ЛІТЕРАТУРА

1. Gandhi M., Jakobsson M., Ratkiewicz J. Badvertisements: Stealthy Click-Fraud with Unwitting Accessories // Journal of Digital Forensic Practice. – 2005. – Vol. 1, № 2. – P. 131-142.
2. Chen J., Liu D., Whiston A.B. Auctioning Keywords in Online Search // Journal of Marketing. – 2009. – Vol. 22, № 4. – P. 125-141.
3. Fain D.C., Pedersen J.O. Sponsored Search: A Brief History // Bulletin – American Society for Information Science and Technology. – 2006. – Vol. 32. – P. 12-13.
4. Daswani N., Mysen C., Rao V., Weis S., Gharachorloo K., Ghosemajumder S., the Google Ad Traffic Quality Team. Online Advertising Fraud [Електронний ресурс]. – Режим доступу: http://www.neildaswani.com/?page_id=15.
5. Matin S. Click Ahoy! Navigation Online Advertizing in a Sea of Fraudulent Clicks // Berkeley Technology Low Journal, Annual Review. – 2007. – Vol. 22, № 1. – P. 533-554.
6. Asdemir K., Yahya, M.A. Legal and Strategic Perspectives on Click Measurement // SEMPO Institute Opinions and Editorials. – 2006. – 11 p.
7. Goodman J. Pay-per-percentage of Impressions: An Advertising Method that is Highly Robust to Fraud [Electronic Resource]. – Режим доступу: http://research.microsoft.com/en-us/um/people/joshuago/publications.htm
8. Фурашев В.М., Ланде Д.В. Практичні засади прогнозування можливих загроз та ризиків шляхом аналізу взаємозв'язку подій з інформаційним простором // Открытые информационные и компьютерные интегрированные технологии: сб. науч. трудов. Вып. 42. – Харьков: Нац. аэрокосм. ин-т «ХАИ», 2009. – С. 194-203.

© Павлов Д.Г., 2010

Стаття надійшла до редколегії 22.03.10 р.