УДК 004.942

Павлов Д. Г.

ЗАХИСТ РЕКЛАМНОЇ ІНТЕРНЕТ-КАМПАНІЇ ВІД МЕРЕЖЕВОГО ШАХРАЙСТВА

В статті запропоновано архітектурну схему системи захисту від шахрайства в галузі Інтернет-реклами. Розроблено новий поведінковий шаблон нападу зловмисників.
Ключові слова: *Інтернет-реклама, склікування, споказування, шаблони атаки.*

В статье предложена архитектурная схема защиті от мошенничества в отрясли Интернет-реклами. Разработано новый поведенческий шаблон нападения злоумышленников.
Ключевые слова: *Интернет-реклама, скликивание, споказывание, шаблоны атаки.*

Paper proposes an architectural scheme of the fraud-defending system for the Internet-advertising area. A new behavioral pattern of the fraudster's attack is presented as well.
Key words: *Internet advertising, communication, spokazuvannya, templates attack.*

Вступ

Новітні інформаційні технології проникають все глибше в різноманітні сфери життя і господарської діяльності людини. Одним з прикладів подібних тенденцій є розвиток ринку Інтернет-реклами. Багато рекламодавців обирають рекламу в мережі, оскільки в порівнянні із традиційними ЗМІ, вона має такі перевагами:

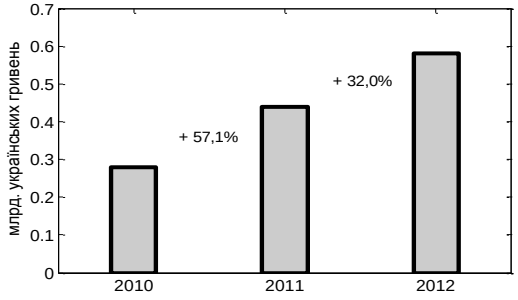
– відносно невисока вартість рекламної кампанії;

– більш точна орієнтація на потенційних клієнтів, можливість налаштувати рекламу відповідно до географічного положення, віку та мови користувачів тощо (для контекстної реклами);

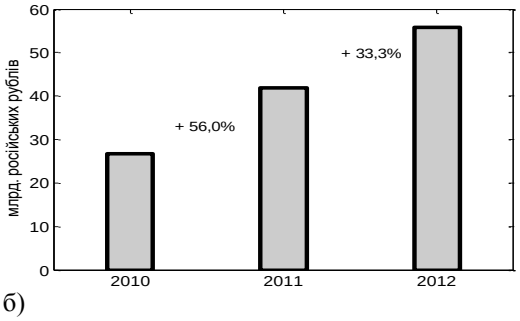
– більш швидкий старт рекламної кампанії;

– використання в якості рекламного майданчику найбільшого та найпопулярнішого в сучасному світі джерела інформації – глобальної мережі Інтернет.

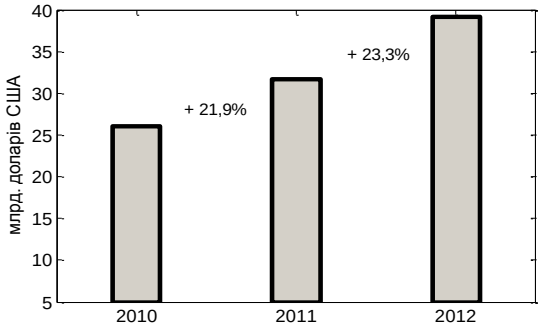
Ринок Інтернет-реклами показує стабільне зростання в більшості країн світу, що відображається у відповідних прогнозах його розвитку [1]. На рис. 1 наведено об'єми ринків реклами в мережі Інтернет в 2010 та 2011 роках, а також прогнози на 2012 рік для України, Росії та Сполучених Штатів Америки. За результатами досліджень [2] розмір грошового обігу в сфері Інтернет-реклами України склав 0,28 і 0,44 млрд. гривень в 2010 та в 2011 роках відповідно. В наступному році експерти прогнозують зростання об'єму ринку на 32%. На території Росії відповідні показники становлять 26,8 та 41,8 млрд. російських рублів [3], очікується зростання об'єму ринку на третину [4]. В Сполучених Штатах Америки прибутки від онлайн-реклами в 2010 р. склали 26,04 млрд. доларів США. В 2011 р. це значення зросло на 21,9% і досягло 31,74 млрд. доларів [5]. Очікується, що наступного року рівень зростання досягне 23,3% [6].



а)



б)



в)

Рис. 1. Розвиток ринків Інтернет-реклами в 2010 і 2011 рр. та прогноз на 2012 р. для України (а), Росії (б) та Сполучених Штатів Америки (в)

Наведені цифри свідчать про високу і монотонно зростаючу популярність реклами в мережі Інтернет. Підвищення доступності Інтернет-послуг широкому колу користувачів зумовлює високі темпи зростання ринку в країнах, що розвиваються.

Рекламодавці оплачують рекламні послуги в мережі за однією з наступних схем: CPC (cost per click), CPM (cost per mille) або CPA (cost per action). Перша схема передбачає оплату кожного кліку (переходу) по рекламному оголошенню, друга – плату за кожну тисячу показів оголошення; використовуючи третю схему, рекламодавець платить лише тоді, коли користувач виконав певну заздалегідь визначену дію на сайті (наприклад, замовив продукцію або залишив контактну інформацію).

Схеми CPC та CPM є найпоширенішими, однак вони роблять рекламну кампанію вразливою до специфічного різновиду мережевого шахрайства – склікування та споказування. Склікування (споказування) – це процес генерації недійсних кліків (показів) з метою розтрати рекламного бюджету рекламодавця. Із збільшенням користувачів системи Інтернет-реклами та зростанням матеріальної зацікавленості сторін посилюється і ускладнюється конкуренція в галузі. Це призводить до появи більш складних та витончених схем недобросовісної конкуренції, що виражається не тільки в зростанні кількості спроб склікати оголошення, але й в ускладненні систем нападу, оскільки всі пошукові системи, що надають послуги Інтернет-реклами, намагаються захистити своїх клієнтів та відфільтрувати недійсний трафік. Тим не менш, якщо під час нападу зловмисник достатньо якісно імітує поведінку реальної людини на сайті, визначення факту дійсності чи недійсності показів та переходів стає дуже складною задачею. Тому актуальним залишається побудова таких методів фільтрації рекламного трафіку, які базувались би на врахуванні психології поведінки зловмисників.

Аналіз літератури по темі дослідження

Система захисту рекламодавців, що використовується одним з найбільших постачальників послуг Інтернет-реклами – компанією Google, складається з двох підсистем [7]. Перша підсистема проводить онлайн-фільтрацію. На цьому етапі всі характеристики трафіку аналізуються в режимі реального часу, визначаються як суто статистичні аномалії (кліки із переліку заблокованих IP-адрес), так і більш складні, наприклад, наявність відомих шаблонів нападу. Друга підсистема працює в режимі оффлайн та аналізує трафік, враховуючи його передісторію. На цьому етапі виділяються більш складні атаки. Також будь-який рекламодавець може особисто надіслати запит в службу підтримки компанії Google. Такі запити розглядаються людьми, які підтверджують або заперечують наявність шахрайства. У випадку позитивної відповіді компанія зобов'язується повернути кошти за недійсні кліки (покази). Деталі реалізації системи захисту компанії Google, а також шаблони, що використовуються для аналізу трафіку, не розголошуються.

Незважаючи на те, що система захисту Google постійно удосконалюється, вона є вразливою до деяких видів атак. Наприклад, в роботі [8] було запропоновано новий тип шаблону склікування, що базується на схемі інформаційної атаки, а в роботі [9] було показано, що цей вид шаблону не відфільтровується захисними системами Google. В статті [10] автори адаптували шаблон інформаційної атаки до випадку генерації недійсних показів. Запропонований шаблон є одновимірним в просторі кліків або показів. Також очевидно, що він не вичерпує всі можливі варіанти поведінки зловмисників.

Постановка завдання

Метою даної роботи є побудова принципової схеми системи фільтрації трафіку оголошень та знаходження нових шаблонів шахрайської поведінки, які наразі не відфільтровуються захисними системами Google. Вхідними даними для розроблюваної системи є статистичні дані про відвідування сайту та активність рекламної кампанії. Джерелом цих даних можуть бути звіти постачальника рекламних послуг. Так, наприклад, сервіс компанії Google надає своїм рекламодавцям доступ до агрегованої інформації про статистику рекламної кампанії (найбільший рівень деталізації – одна година). Інформацію про відвідування сайту можна дістати з таких сервісів як Google Analytics, Яндекс, Метрика, тощо.

Концептуальна архітектура системи фільтрації трафіку та знаходження нових шаблонів шахрайської поведінки

Принципова схема системи наведена на рис. 2. На протязі всього часу проведення рекламної кампанії накопичується статистична інформація про природну поведінку користувачів сайту (наприклад, найвірогідніший час перебування людини на сайті в окремі дні тижня та доби, розподіл інтенсивності переходів за рекламним посиланням впродовж дня, тижня, місяця тощо). З плином часу ці показники можуть змінюватися в результаті різкого підвищення або спаду попиту на деяку продукцію, зміни платоспроможності потенційних клієнтів. Тому базові характеристики оновлюють свої значення в залежності від передісторії кампанії та параметрів, які може вводити експерт. Наприклад, стало відомо, що виходить новий продукт, який, як очікується, буде дуже популярним. Експерт може внести відповідні корегування в систему з метою збільшення очікуваного значення деяких показників (інтенсивності переходів, часу перебування на сайті тощо).

Всі статистичні дані про трафік рекламної кампанії зберігаються в сховищі даних. Порівняння поточних значень параметрів трафіку із очікуваними дозволяє виділяти, наприклад, наступні аномалії: різкий необумовлений тенденціями ринку сплеск переходів, випадкове продовження часу перебування на сайті тощо. Дані можуть розглядатися в різному масштабі часу (година, день, тиждень, місяць). Оскільки кількість статистичних даних на найбільшому рівні деталізації (година) з часом стає дуже великою, а отже – ускладнює процес аналізу, початкове виділення аномальних періодів повинно проводитися щоденно або щотижнево. Виділений аномальний період після цього більш докладно розглядається на всіх інших доступних рівнях деталізації.

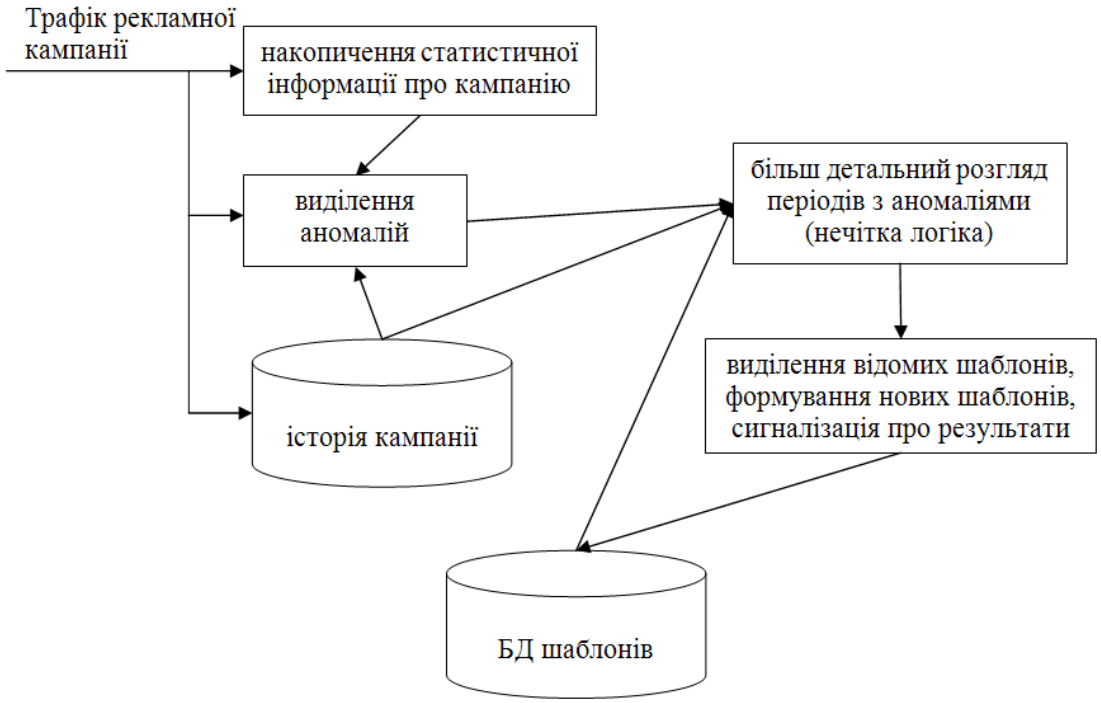


Рис. 2. Базова архітектура системи фільтрації тарфіку для виділення нових шаблонів шахрайської поведінки

На етапі детального аналізу система намагається відшукати в даних трафіку вже відомі шаблони шахрайської поведінки. Якщо такі були знайдені, генерується відповідний сигнал для рекламодавця. Після цього він може звернутися в сервісний центр Google (за умови вибору цієї компанії в якості постачальника Інтернет-послуг) і вимагати більш детального дослідження трафіку експертами, а також повернення коштів у випадку визнання наявності шахрайства. Шаблони зберігаються в базі даних у вигляді інформації про наявність локальних мінімумів та максимумів на графіках різних показників трафіку. Очевидно, що інтенсивність таких екстремумів може бути різною в кожному окремому випадку, тому для виділення шаблонів в поточному трафіку необхідно користуватися засобами теорії нечітких обчислень.

Якщо ж жодного відомого шаблону не було знайдено, однак існують підозри про наявність нападу, система генерує повідомлення про можливу атаку та надає всю необхідну інформацію на розгляд рекламодавця. Останній формує висновок про наявність або відсутність на його думку нападу та заносить характеристики нового шаблону в базу даних.

Експериментальні результати

Для апробації запропонованої принципової архітектурної схеми в напівавтоматичному режимі було проведено експеримент з метою виявлення можливого шаблону склікування оголошення. Розглядався трафік декількох рекламних кампаній з деталізацією в одну добу. В якості індикації підозрілого періоду використовувалось різке збільшення параметру CTR (click through rate), який представляє собою відношення кількості кліків до кількості показів оголошення. Зазвичай, параметр CTR лежить в межах декількох десятків відсотків. Різке збільшення значення CTR говорить про те, що рівень кліків збільшився в декілька разів без відповідного збільшення кількості показів, що може бути сигналом про наявність атаки. На Рис. 3 показано графік щоденного CTR для реальної Інтернет-кампанії в період з 15 квітня по 16 вересня 2010 року.

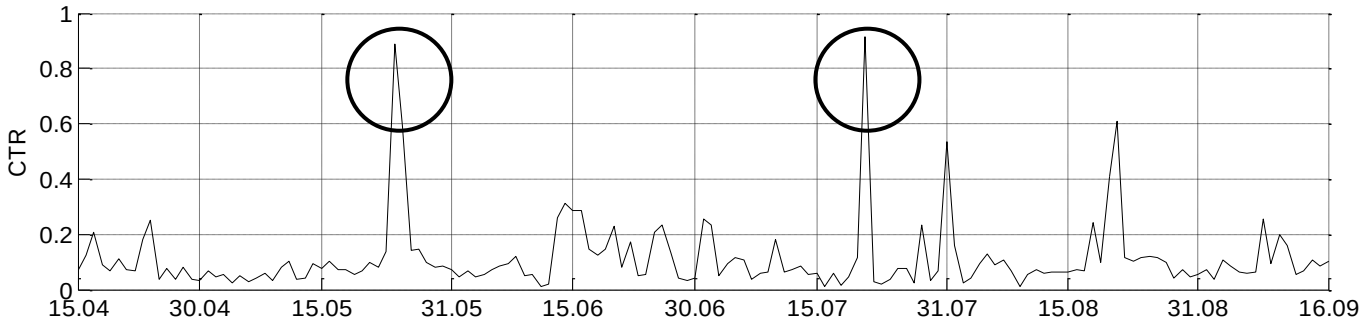


Рис. 3. Графік щоденного CTR

На графіку чітко виділяються два локальні максимуми в другій половині травня та липня. Після більш детального аналізу погодинних розподілів різних параметрів трафіку в періоди 01-30.05.2010 р. та 01-31.07.2010 р. виявилось, що ці часові проміжки мають деяку закономірність в розподілі кількості кліків,

кількості показів, CTR та середньої тривалості перебування користувачів на сайті. Графіки цих параметрів наведено на рис. 4 та 5.

В обох випадках спостерігається наступна послідовність подій:

1) короткострокове збільшення тривалості перебування людей на сайті;

2) підвищена кількість показів впродовж декількох днів;

3) збільшення кількості кліків та значення показника CTR (безпосередня атака), причому дострокове вичерпання бюджету кампанії не спостерігалося.

Атаці такого вигляду можна дати наступну психологічну інтерпретацію. Припустимо, що на ринку існує декілька конкуруючих фірм. Одна з фірм планує вивести на ринок новий вид товару і хоче зменшити конкуренцію на декілька перших днів появи продукції. Отже, спочатку необхідно докладно дослідити сайт конкурента. Це відображається у збільшенні середньої тривалості перебування користувачів на сайті та відповідає першому пункту запропонованої схеми атаки.

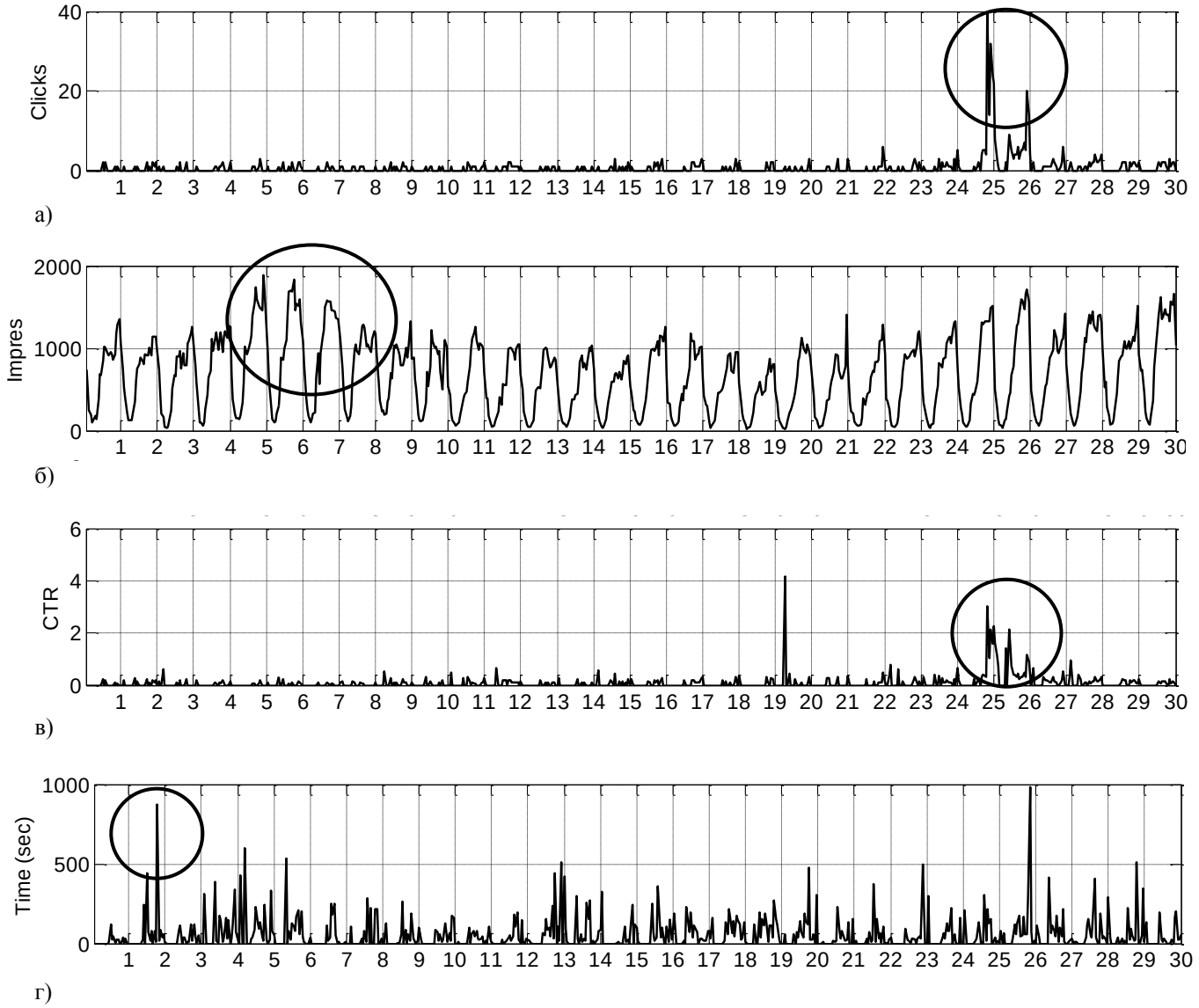


Рис. 4. Погодинний розподіл деяких параметрів трафіку сайту в період 01-30.05.2010 р.: а) кількість кліків по оголошенню, б) кількість показів оголошення, в) значення CTR, г) середня тривалість перебування користувачів на сайті в секундах

Зловмисник не може знати заздалегідь, яку схему оплати використовує його конкурент: CPC чи CPM (варіант оплати за схемою CPA не розглядається, оскільки вона використовується набагато рідше за попередні). Для того, щоб визначити, якою схемою користується конкурент, можна провести серію споказувань (генерування штучних показів оголошення) та подивитися на реакцію системи. Це відповідає другому пункту нападу. Визначившись, що використовується схема плати за клік (в досліджуваній рекламній кампанії використовується саме CPC), проводиться склікування (третій пункт атаки).

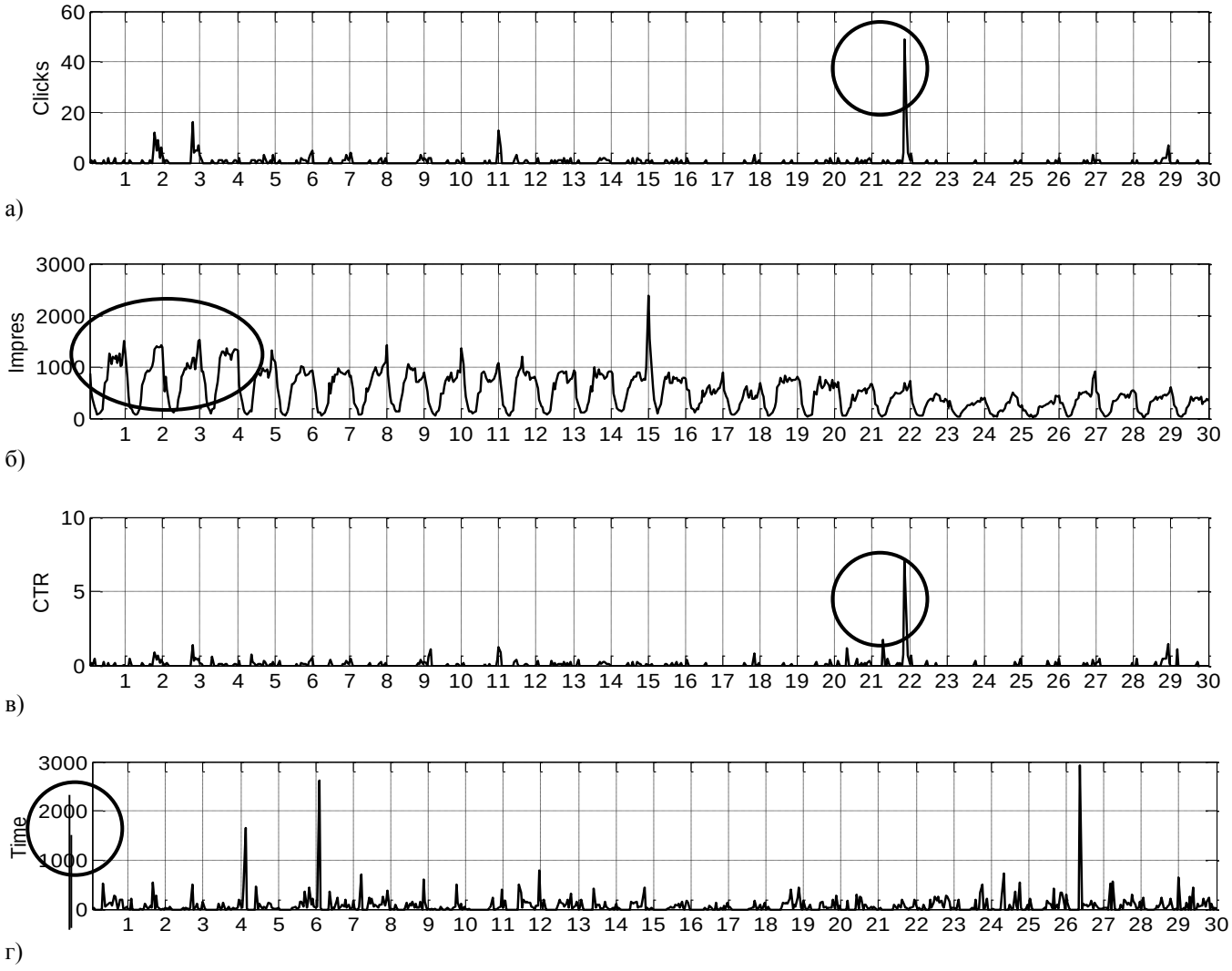


Рис. 5. Погодинний розподіл деяких параметрів трафіку сайту в період 01-30.07.2010 р.: а) кількість кліків по оголошенню, б) кількість показів оголошення, в) значення CTR, г) середня тривалість перебування користувачів на сайті в секундах

Частота показів рекламного оголошення встановлюється рекламодавцем та може приймати одне з двох значень:

– «прискорений показ» – оголошення демонструється по кожному релевантному запиту; якщо денний бюджет кампанії вичерпується раніше, оголошення не демонструється до кінця доби;

– «рівномірний показ» – оголошення демонструються рівномірно впродовж доби; якщо спостерігається швидке вичерпування денного бюджету, показ оголошення припиняється на деякий час, а потім поновлюється.

В першому випадку нападникові для досягнення бажаного результату (припинення демонстрації оголошення конкурента) необхідно згенерувати достатню кількість кліків в першій половині дня. В другому випадку достатньо періодично генерувати недійсні кліки впродовж доби. В результаті, оголошення конкурента буде автоматично зникати з поміж результатів пошуку, а через деякий час з'являтися знову. В досліджуваній рекламній кампанії було встановлено рівномірний показ, тобто має місце другий варіант. Це пояснює відсутність факту дострокового вичерпання бюджету в період безпосередньої атаки.

Оскільки вхідні експериментальні дані були взяті з таких сервісів компанії Google як AdWords та Analytics, де міститься інформація з урахуванням відфільтрованих недійсних кліків, можна стверджувати, що даний різновид атаки не був розпізнаний існуючими захисними системами.

Висновки

В рамках даної роботи була розроблена принципова схема системи фільтрації трафіку Інтернет-оголошень та формування нових шаблонів нападу. Передбачається, що запропонована система працюватиме із даними, що надаються постачальником Інтернет-послуг (тобто агрегованими даними, з відфільтрованою інформацією про виявлені недійсні кліки). Також для отримання додаткової даних можуть застосовуватися аналітичні системи сайтів (Google Analytics, Яндекс Метрика тощо).

В результаті експериментальної апробації запропонованої архітектурної схеми було виявлено новий різновид психологічного шаблону нападу, який наразі не визначається захисними системами компанії Google.

Перспективами подальших досліджень є пошук нових шаблонів нападу для наповнення бази даних типових шаблонів (з урахуванням нечіткості критеріїв їх визначення) і розробка запропонованої системи.

ЛІТЕРАТУРА

1. Year-over-year change of advertising expenditure in selected countries in 2011 and 2012 [Електронний ресурс]. – Режим доступу : http://www.statista.com/statistics/215045/global-advertising-market-forecast/
2. Украинский рынок интернет-рекламы в 2011 г. вырос на 57% до 440 млн грн [Електронний ресурс]. – Режим доступу : http://ko.com.ua/ukrainskij_rynok_internet-reklamy_v_2011_g_vyros_na_57_do_440_mln_grn_59758
3. Объем рекламного рынка России в 2011 году [Електронний ресурс]. – Режим доступу : http://www.akarussia.ru/press_centre/news/id1864
4. In 2012 Runet advertising market will increase by a third [Електронний ресурс]. – Режим доступу : http://begingroup.com/en/top/news/market_news/1374
5. IAB Internet Advertising Revenue Report [Електронний ресурс]. – Режим доступу : http://www.iab.net/media/file/IAB_Internet_Advertising_Revenue_Report_FY_2011.pdf
6. US Online Ad Spend to Grow 23.3% in 2012 [Електронний ресурс]. – Режим доступу : http://www.marketingcharts.com/direct/internet-advertising-revenues-continue-growth-20257/
7. How does Google detects invalid clicks? [Електронний ресурс]. – Режим доступу: http://adwords.google.com/support/aw/bin/answer.py?hl=en&answer=6114
8. Виявлення аномальної поведінки користувача системи контекстної реклами / О. Р. Чертов, Д. Г. Павлов, В. В. Мальчиков, М. В. Александрова // Искусственный интеллект. – 2010. – № 4. – С. 476–483.
9. Chertov O. Non-Dyadic Wavelets for Detection of Some Click-Fraud Attacks / O. Chertov, V. Malchykov, D. Pavlov // Proc. International Conference on Signals and Electronic Systems (ICSES-2010), (September 7-10, 2010, Gliwice, Poland). – 2010. P. – 401–404.
10. Павлов Д. Г. Модель поведінки зловмисників при розміщенні Інтернет-реклами з схемою оплати за тисячу показів / Д. Г. Павлов // Наукові праці. Комп'ютерні технології. – 2010. – Вип. 121. – Т. 134. – С. 220-224.

Дата надходження статті до редколегії 03.05.2012 р.

ПАВЛОВ Д. Г. – аспірант кафедри прикладної математики Національного технічного університету України «Київський політехнічний інститут».