ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 4
2012

Д. Г. Павлов (Киев, НТУУ «КПИ»). **Нечеткие шаблоны поведения злоумышленников при скликивании в системе контекстной рекламы.**

Благодаря возможности гибкой настойки рекламной кампании и четкой ориентации на круг потенциальных клиентов контекстная реклама становится все более популярной. Однако, поскольку зачастую рекламодатели используют схему оплаты за клик (CPC, «cost per click») в системе контекстной рекламы возникает такое явление, как скликивание — процесс генерации мошеннических кликов с целью растраты рекламного бюджета рекламодателя. Масштабы скликивания являются довольно широкими, известны случаи, когда поисковым системам было в судебном порядке присуждено возвращать деньги своим рекламодателям [1].

В работе [2] был введен новый шаблон скликивания, который соответствует схеме информационной атаки (см. рис.) и включает в себя фазы: «фоновый шум» (I), «проба» (II), «затишье» (III), «атака» (IV). Для определения факта наличия скликивания можно использовать нечеткие шаблоны. Предположим, что злоумышленник является конкурентом рекламодателя, цель его деятельности — преждевременное исчерпание рекламного бюджета. Пусть также были определены временные промежутки, которые являются кандидатами на соответствующие фазы информационной атаки. Тогда можно сформулировать такие правила определения степени вероятности наличия скликивания в текущем рекламном трафике:

- ЕСЛИ <в периоды 1, 3 бюджет не исчерпан> & <в периоды 2, 4 бюджет исчерпан> & <в периоды 1, 3 нет преждевременного прекращения демонстрации объявлений> & <в периоды 2, 4 преждевременное прекращение демонстрации объявлений> & <в периоды 1, 2, 3, 4 настройки рекламной кампании не менялись> ТО <вероятность атаки высокая>;

- ЕСЛИ <в периоды 1, 2, 3, 4 бюджет исчерпан> & <в периоды 1, 3 нет преждевременного прекращения демонстрации объявлений> & <в периоды 2, 4 преждевременное прекращение демонстрации объявлений> & <в период 3 настройки рекламной кампании менялись> ТО <вероятность атаки низкая>.

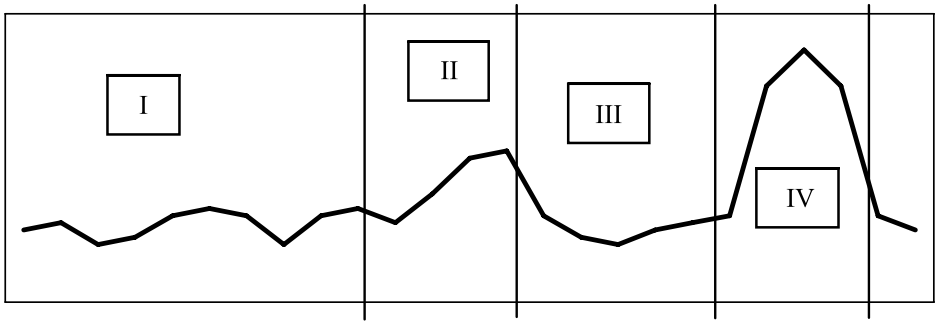

Рис. Модель информационной атаки

Использование нечетких шаблонов повышает эффективность защитных систем за счет более точной формализации процессов, содержащих в себе человеческий фактор.

СПИСОК ЛИТЕРАТУРЫ

1. *Сазанов В. М.* Виртуальная школа компьютерных технологий. Лекция 15. [Електронный ресурс]. Режим доступа: http://v-school.narod.ru/INI/ini.htm.
2. Чертов О. Р., Павлов Д. Г., Мальчиков В. В., Александрова М. В. Виявлення аномально» поведінки користувача системи контекстно» реклами. — Искусственный интеллект, 2010, № 4, с. 476–483.