ЭКОНОМИЧЕСКИЕ НАУКИ

УДК 339.138

О. А. Артемьева
Финансовый университет при Правительстве Российской Федерации, Москва,
e-mail: artemieva.o.a@mail.ru

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ЦИФРОВОГО МАРКЕТИНГА СОВРЕМЕННЫМ БИЗНЕСОМ

Ключевые слова: цифровой маркетинг, цифровая реклама, мошенничество, клик-спам, инъекция кликов, спуфинг, фермы устройств, фроды, антифрод-системы, бот, бренды, технология блокчейн.

В статье на основе систематизации теории и анализа опыта компаний российского рынка, приведены проблемы мошенничества в процессе применения цифровой рекламы. Определены виды и способы мошенничества, раскрыты признаки низкого качества трафика мошенника. Сделан вывод, что проблема мошенничества в сфере цифрового маркетинга в течение нескольких лет будет расти. В этой связи технология блокчейн как относительно новая технология предположительно сможет улучшить ситуацию. Использование технологии блокчейн позволит ослабить стремительно растущее проникновение интернет-мошенников в маркетинговую деятельность в банках. Концепция блокчейна может быть применена к некоторым видам маркетинговых технологий, так как она предлагает более прозрачный и эффективный способ управления игроками на рынке в режиме онлайн. Используя технологию блокчейн, рекламодателям станет проще проверять каждую рекламу по нескольким каналам и показывать ее без обмана.

O. A. Artemyeva
Financial University under the Government Russian Federation, Moscow,
e-mail: artemieva.o.a@mail.ru

PROBLEMS AND PROSPECTS OF USING DIGITAL MARKETING BY MODERN BUSINESS

Keywords: digital marketing, digital advertising, fraud, click-spam, click injection, spoofing, device farms, fraud, anti-fraud systems, bot, brands, blockchain technology.

Based on the systematization of the theory and analysis of the experience of Russian market companies, the article presents the problems of fraud in the process of using digital advertising. The types and methods of fraud are identified, and the signs of low quality of the fraudster's traffic are revealed. It is concluded that the problem of fraud in the field of digital marketing will grow over the next few years. In this regard, blockchain technology as a relatively new technology is expected to improve the situation. The use of blockchain technology will reduce the rapidly growing penetration of Internet fraudsters into marketing activities in banks. The concept of blockchain can be applied to some types of marketing technologies, as it offers a more transparent and efficient way to manage players in the market online. Using blockchain technology, it will become easier for advertisers to check each ad across multiple channels and display it without deception.

Введение

Цифровой маркетинг и цифровая реклама получила широкое распространение на современном этапе развития. Они характеризуется целенаправленностью, эффективностью, стремлением использованию максимального количества цифровых каналов. Применение цифрового маркетинга дает положительные результаты, выражающиеся в увеличении продаж через онлайн каналы. Современные компании выделяются большим количеством использования каналов и инструментов (SEO, Контекстная реклама, SMM, медийная реклама, E-mail-рассылки, адаптация, редизайн). Используют подходы к оценке эффективности цифрового маркетинга: коммерческий (экономический) и коммуникативный. Вместе с тем, многие крупные бренды призывают очистить рынок цифровой рекламы от мошенничества, который приобретает невиданные

масштабы. Мошенничество с цифровой рекламой является одной из наиболее серьезных проблем, которую всей маркетинговой индустрии необходимо решать. Мошенников привлекает неконтролируемый характер транзакций, как правило, непрозрачная деятельность посредников и возможность довольно быстро и легко изменять показатели. Игнорирование данного факта может привести к огромным потерям бюджета.

Цель исследования

На основе систематизации теории и анализа опыта компаний российского рынка, выявить проблемы применения цифровой рекламы, в том числе определить виды и способы мошенничества, раскрыть признаки низкого качества трафика мошенника, сформулировать перспективные рекомендации.

Материал и методы исследования

Существенный вклад в исследование цифровые технологии внесли зарубежные авторы В.П. Бауэр, М Свон, Д. Тапскотт, А. Тапскотт, К Скиннер, П. Винья, М. Кейси. Исследование вопросов, касающихся влияния цифровых технологий на маркетинговую деятельность, проводили отечественные ученые-экономисты М.М. Пряников, М.О. Пилипенко, В.В. Дорохов, С.А. Синягов, А.Л. Лысенко, В.К. Шаталов, П.Ю. Барышников. Информационной и нормативно-правовой базой данной работы являются федеральные законы, данные Банка России, годовые отчеты российских рейтинговых агентств (АКРА, Эксперт РА), Официальный сайт по финансовому анализу банков – «Куап.ру», исследования Гильдии маркетологов, данные аналитических агентств (Markswebb Rank & Report, Tadviser), а также официальные сайты кредитных организаций и финтех-компаний. При исследовании использовались методы теоретического анализа, эмпирического исследования, сравнительного анализа, статистический метод, а также методы синтеза и обобщения.

Результаты исследования и их обсуждение

Исследования показали, что мошенничество в цифровой среде осуществляется следующим образом:

● клик-спам – это имитация с реальных устройств определенно большого количества кликов, с целью получения денежных средств за органические установки и скачивания. Данный факт может привести к растрате рекламного бюджета на тех пользователей, которые и так бы установили сервис. Также клик-спам может быть опасен тем, что система заберет самых ценных пользователей, которые пришли целенаправленно, не под воздействием рекламы. Распознать клик-спам можно фиксируя длину времени между кликом и установкой.

● инъекция кликов – это усовершенствованная версия клик-спама, в основе которой лежит использование вредоносного программного обеспечения на устройстве пользователя. Создаются фальшивые клики, с помощью приложения в момент его установки пользователем, тем самым мошенник присваивает установку себе, получая за нее плату. В этом случае длина времени между кликом и установкой очень короткая.

● спуфинг – ситуация, в которой мошенники создают программу, которая с успехом маскируется под другую, фальсифицируя данные и получая несанкционированный доступ к определенному ресурсу. Программа отправляет данные о кликах пользователя уже в новых приложениях, которые считает их так, как если бы они были настоящими.

● фермы устройств – это сервис для тестирования приложений, который используют для нажатия на рекламу или установку приложений, с целью повышения производительности приложения. После чего все клики сбрасываются и процесс начинается по новому кругу. Обычно фермы устройств можно определить по уже известному шаблону действий.

● бот – это специальная программа, которая выполняет запрограммированные действия автоматически по заранее заданному алгоритму. Боты имитируют поведение настоящих пользователей. По сути, боты работают по тому же принципу, что и фермы устройств. Исключением является лишь использование не настоящих устройств, тем самым упрощая процесс очистки данных, но характерный шаблон действий остается.

Фермы устройств и боты являются наиболее используемыми формами мошенничества с цифровой рекламой. Если их рост продолжится, то можно ожидать, что этот фактор потери бюджета компаниями станет самым главным.

По оценкам консервативных экспертов, уровень потери бюджета достигнет 50 млдр. долларов к 2025 году, к этому времени это будет около 10% всего рынка цифровой рекламы. Маркетологи из крупных компаний полагают, что минимум 40% рекламных бюджетов в интернете и приложениях в мобильном телефоне подвержены риску мошенничества. При этом только 19% представителей брендов сообщают о наличии у себя системы предотвращения мошенничества, 92% участников опроса (это более 250 специалистов компаний с рекламными бюджетами от 1 млн. долл. в месяц) считают борьбу с фродом в мобильной рекламе главной задачей современности [9, 10].

Бренды несут экономические потери в результате поддельных конверсии и «пустого» трафика. Ожидается, что к 2021 году доля цифровой рекламы достигнет 50% всей рекламы, и отрасль готова к переменам. Также отчаянно нужно найти решения, которые создадут более здоровую экосистему для клиентов, рекламодателей и издателей. По оценкам AdAge, за мошенничество с рекламой требуется 1 доллар на каждые 3 доллара, потраченные на цифровую рекламу. К 2022 году, по подсчетам Juniper Research, индустрия может потерять на фроде до $44 млрд. Но деньги теряют не только рекламодатели. От мошенничества страдают все участники рынка (кроме самих фродеров): рекламодатели, маркетинговые агентства, рекламные сети, но агентствам в силу их промежуточного положения приходится особенно тяжело. С паблишерами и сетями они работают по предоплате, а потом ждут вознаграждения от рекламодателей, которые могут отказаться платить за часть работы.

В качестве примера можно привести несколько брендов, прекратившие свою рекламу на YouTube после отчета The Times of London, в котором подчеркивалось, «как их реклама отображалась на фоне экстремистского контента, размещенного на сайте для обмена видео». Случаи мошенничества с цифровой рекламой начинают появляться один за другим. Несмотря на то, что некоторые рекламодатели возвращают деньги (Google дал больший возврат средств рекламодателям, пострадавшим от мошенничества с рекламой), угрозу нужно обуздать раньше, чем позже. [7, 8].

Мошенники используют несколько способов имитации поведения людей, включая доступ к социальным сетям, заполнение форм и движения курсора. Они избегают обнаружения, манипулируя данными геолокации. Также в 2017 году компания Uber подала иск в суд на Fetch Media в Dentsu, обвинив его в применении нечестных методов рекламы. Среди них считалось использование невидимых баннеров, закупка рекламы на нерелевантных площадках, а также попытка выдать естественные установки за рекламные. Агентство в свою очередь заявило, что Uber еще за несколько месяцев до этого отказал ему в выплатах. Этот случай стал наиболее резонансным из-за масштаба бренда и бюджета (годовые расходы Uber на мобильную рекламу в 2017 составили более $82,5 млн.). Но он далеко не единичный: в меньших объемах маркетинговые агентства сталкиваются с отказами в оплате конверсий постоянно. Самое неприятное заключается в том, что финансовые потери сваливаются на них непредвиденно, когда бюджеты уже потрачены и ничего исправить нельзя.

Крупнейшее в последнее время мошенничество фальсификации кликов по видео объявлениям. Разработчики ботов Methbot приносят своим владельцам по нескольку миллионов долларов США в день. Авторы Methbot работают по оригинальной схеме: они делают замену адресов своих собственных сайтов. Сначала бот в автоматическом режиме выбирает домен из списка премиум публикаторов, после чего создается подставная страница, где есть все необходимые для генерации рекламы и запросов видео рекламы из различных рекламных сетей. При этом используются приемы, помогающие ботнету имитировать работу обычного пользователя.

Мошенничество с помощью автоматизированных систем (ботов) – не един-

ственный вид мошенничества, от которого страдают рекламная и издательская деятельность. Существуют и другие проблемы, такие как видимость 0 % и преднамеренное неправильное истолкование, которые в равной степени несут ответственность за то, что не получают своих денег.

Теоретически определить фрод можно вручную, но на практике делать это не целесообразно. Хотя 100 % панацеи от мошенничества не существует, были разработаны анти-фрод системы, с помощью которых можно определить и пресечь некачественный трафик, не допуская серьезных потерь. Они отлавливают ботов и фильтруют трафик. Алгоритм пропускает через себя данные. Программа фиксирует аномалии, а также сравнивает ID и IP с уже имеющимися в базе. Если атипичные действия повторяются или ID/IP есть в блеклисте, то трафик признается фродовым [1, 3, 4].

Обнаружить низкое качество трафика можно, если обратить внимание на такие моменты, как:

- аномально большая скорость загрузки/переходов с одного источника;
- маленький промежуток времени между кликом по объявлению и целевым действием;
- очевидно шаблонное поведение (например, равные временные промежутки между кликами);
- разное ГЕО клика и установки для одного и того же пользователя;
- много кликов с одного IP/ID;
- конверсия ниже 0,1 % при большом потоке трафика или конверсия 100 %;
- время жизни пользователя – до 3 дней;
- подозрительная активность в ночные часы [2, 5, 6].

Маркетинговые агентства нередко сталкиваются с требованием клиента раскрыть источники трафика. Крупным брендам, которые дорожат репутацией, важно знать, на каких площадках они рекламируются. Никто из них не хочет обнаружить свои баннеры на сайтах адалт-тематики или с экстремистским контентом. В связи с этим они могут предложить своим подрядчикам работать в формате полной прозрачности. Маркетинговые агентства противостоят раскрытию информацию о своих источниках, ссылаясь на коммерческую тайну. На раскрытие информации агенства соглашаются только в случае необходимости подписания контракта с крупным брендом. Но и в этом случае они заключают с клиентом договор о неразглашении данных.

В 2020 году бренды продолжат внедрять антифрод-системы, при этом будут стремиться к стандартизации своих KPI и параметров по мошенничеству. Количество невыплат за подозрительный трафик будет расти, поэтому в выигрыше окажутся те, кто сделает ставку на оперативность в предотвращении мошенничества с помощью антифрод-систем. Лучше других сократить потери смогут те агентства, которые договорятся с клиентами о совместном доступе к анализу трафика и конверсий.

Вывод

Таким образом, методы, которые существуют в настоящее время не могут справиться с мошенничеством, поскольку постоянно разрабатываются технологии, которые способны находить лазейки. Учитывая серьезность ситуации, они должны опираться на более надежные, более футуристической технологии – такие, как блокчейн. В настоящее время для цифровой рекламы на блокчейне существует не менее пяти потенциальных приложений: больше прозрачности, меньше мошенничества, лучшее управление данными на потребительском уровне, автоматизация торгов и аукционы в режиме реального времени.

Прогнозируется, что технология блокчейн в целом сможет уменьшить потери от мошенничества в цифровом маркетинге более чем на 10 млрд. долларов к 2022 году. В реальных условиях данная технология не будет передовой и востребованной, поскольку базовая инфраструктура еще не готова, и я согласна с ним. На этом этапе развития блокчейн, много времени требуется для проведения транзакций, и для того, чтобы блокчейн смог бы обрабатывать и проверять несколько транзакций в секунду, поэтому необходимо многое сделать прежде, чем блокчейн можно будет эффективно использовать для решения задач рекламы.

Основная проблема, с которой сталкиваются маркетологи – это прозрачность и мошенничество в цифровой рекламе. Блокчейн может помочь во власти этого в значительной степени потому, что он работает в качестве старой школьной книги в распределенном цифровом формате. Концепция блокчейна может быть применена к рекламным технологиям, так как она предлагает более прозрачный и эффективный способ управления онлайн-рынками. Используя распределенные системы и децентрализованную бухгалтерскую книгу, рекламодателям станет проще проверять каждую рекламу и показ без обмана.

Революция уже происходит с компаниями, производящими передовые изобретения и издателями / покупателями / рекламодателями, использующими торговые площадки, которые подпитываются блокчейном. Это позволяет им использовать шифрование для максимальной безопасности. Они признают блокчейн как крайне необходимый компонент, обеспечивающий высочайший уровень прозрачности, чего очень не хватает в цифровом рекламном пространстве.

В настоящее время IAB (Техническая лаборатория Бюро интерактивной рекламы) и Ассоциацию данных и маркетинга пытаются принять определенные меры против мошеннических действий, которые охватывают цифровую рекламу. IAB работает над созданием рабочей группы по блокчейну, чтобы выяснить, как она может помочь рекламодателям [53]. Однако, поскольку блокчейн требует участия всех сторон, издатели и рекламодатели должны будут объединить усилия, чтобы установить правила игры и согласовать стандарт. Некоторые первопроходцы делают успехи при работе в области блокчейн технологии. Например, японский производитель автомобилей Toyota объявил о партнерстве с фирмой Lucidity, занимающейся рекламной аналитикой блокчейнов, с целью сокращения мошенничества при покупке цифровой рекламы. Результаты их первоначального пилотного проекта первой в истории проверенной программной рекламной кампании в автомобильной промышленности на блокчейне были впечатляющими – они продемонстрировали повышение эффективности кампании на 21%.

Библиографический список

1. Данько Т.П., Китова О.В. Вопросы развития цифрового маркетинга // Проблемы современной экономики. 2019. № 3 (47).

2. Егорян Л.Б. «Клик-фрод», как актуальная проблема оценки эффективности Интернет-рекламы: методики выявления и пути решения // Транспортное дело России. 2015. № 1-2. С. 31-35.

3. Стыцюк Р.Ю., Артемьева О.А., Рожков И.В. Маркетинговая ценность символического сообщения в обществе постмодерна // Экономика и управление в машиностроении. 2014. № 6. С. 72-74.

4. Стыцюк Р.Ю., Артемьева О.А. Методы и критерии оценки эффективности цифровой рекламы с учетом поведенческих характеристик // В сборнике: форсайт образования. Сборник материалов по итогам Международных научно-методических конференций. Под общей редакцией Е.А. Каменевой. 2018. С. 314-317.

5. Стыцюк Р.Ю. Особенности маркетинговых коммуникаций компаний на ИТ-рынке // Экономика и управление в машиностроении. 2020. № 1. С. 50-52.

6. Геращенко И.В., Стыцюк Р.Ю. Предпосылки развития клиенто-ориентированного HR-маркетинга // Научные труды Вольного экономического общества России. 2013. Т. 179. С. 216-221.

7. Розанова Т.П., Стыцюк Р.Ю., Артемьева О.А. Роль и эффективность маркетингового управления на разных уровнях маркетинговой стратегии. // Экономика и управление в машиностроении. 2016. № 4. С. 47-50.

8. Стыцюк Р.Ю., Иванова Ю.О. Университетский центр трансфера технологий как конкурентное преимущество // Научные труды Вольного экономического общества России. 2013. Т. 179. С. 394-398.

9. New professions emerging out of the development of robotics. Maimina E., Puzynya T., Grishina T., Psareva N., Stytsyuk R. Espacios. Издательство: Sociacion de Profesionales y Tecnicos del CONICIT, 2019. Т. 40. № 10. С. 16.

10. Гетьман Я. Плохие и хорошие методы SEO: 10 практик. [Электронный ресурс]. URL: https://imagecms.net (дата обращения: 10.07.2020).