1.7. ЭТИЧЕСКИЕ ПРОБЛЕМЫ СБОРА ДАННЫХ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ DOOH РЕКЛАМЫ

Глаз Р.А.[1], Шамаева Е.Ф.[2]
[1]Государственный университет «Дубна»
[2]Государственный университет управления

Одной из основных проблем современной цифровой трансформации является вопрос безопасности персональных данных. Работа посвящена этике сбора персональных данных рекламодателями в сфере наружной рекламы в целях последующей трансляции коммуникационного сообщения потребителю. В статье проанализированы основные критерии оценки эффективности работы цифровых щитов, выявлены измеряемые показатели. Далее проанализированы способы измерения этих показателей. Этим способам была дана правовая оценка. Изучены риски, связанные со сбором такой информации. В результате определяется этическая проблема и способ ее решения.

Введение

В 2020 году волна пандемии и карантинные режимы дали мощный толчок к цифровизации многих сфер, в том числе рекламы. Самым ярким примером цифровизации в рекламе служит рынок наружной рекламы, которая, фактически, разделилась на два больших направления OOH (out-of-home) и DOOH (digital-out-of-home) [Jefkins, 2000]. Причем второе направление имеет массу преимуществ по сравнению с первым:

1. На одном цифровом щите может показываться гораздо больше рекламы, чем на обычном в один период времени;
2. Изменение рекламного сообщения на щите требует значительно меньше человеческих усилий;
3. Цифровые щиты позволяют показывать рекламное сообщение в зависимости от погоды и времени суток;
4. Цифровые щиты могут автоматически собирать данные об аудитории, которые потом могут использоваться в других рекламных каналах;
5. На цифровых щитах можно использовать видео-сообщение;

И многие другие.

За счет своих очевидных преимуществ доля DOOH на рынке офлайн-рекламы постоянно растет и в перспективе полностью вытеснит традиционный формат OOH [9]. К 2021 году доля DOOH на рынке наружной рекламы составила 31% в России, годом ранее этот показатель был равен 25% [3]. Так как для оценки эффективности и дальнейшего ретаргетинга цифровые щиты с помощью технологий распознавания и wi-fi собирают и обрабатывает данные человека, все более остро стоит вопрос об этичности такой активности.

Из этого следует цель данной работы.

Цель: найти решение этической проблемы, возникающей при сборе данных цифровыми щитами.

Задачи:

- определить основные метрики для оценки эффективности наружной рекламы;
- изучить существующие методы сбора информации на рынке DOOH;
- проанализировать существующие нормативные документы в отношении собираемой информации;
- проанализировать возможности, которые дает собираемая цифровыми щитами информация для идентификации и деанонимизации потребителя.

1. Методология измерения эффективности цифровых щитов

Основным и наиболее важным показателем в оценке эффективности цифрового щита является OTS (opportunity to see) – это оценка количества контактов потенциальным потребителем с рекламой, включающая повторные контакты [4].

OTS за день считается по формуле:

$$OTS = Cov * ((T*Z)/3600)^n$$

Где:

Cov – общий суммарный охват пользователей задействованных рекламных носителей в день, тыс. человек;

T – длительность видеоролика, с;

Z – частота показа рекламы, р/ч.;

n – среднее количество цифровых щитов, которое видит потенциальный потребитель за 24 часа.

Общий охват будет равен сумме охватов всех цифровых щитов за вычетом пересечений. *Охват каждого конкретного щита определяется измерением.*

Для того, чтобы рассчитать OTS за весь период рекламной кампании, необходимо просто умножить OTS за день на количество дней рекламной кампании.

Также важным показателем оценки эффективности является частота (Fr). Частота – среднее число контактов, которое один человек имел с рекламным обращением за определенный промежуток времени. Частота равна отношению возможных контактов с рекламой к накопленной частоте за выбранный период:

Fr = (OTS(t)) / (Cov(t))

Другим важным показателем для расчета является Gross Rating Point. GRP – это суммарный рейтинг, показывающий процент населения, который был подвергнут рекламному воздействию или, другими словами, общую массу этого воздействия. GRP равен отношению возможных контактов с рекламой к общему населению выбранной области города, района:

GRP = OTS / S * 100%

где S – количество людей, проживающих на территории проведения рекламной кампании.

Когда произведен расчет GRP, можно вычислить долю базовой аудитории, имевшей возможность визуального контакта с рекламным сообщением хотя бы один раз в заданный промежуток времени – REACH (%).

REACH=GRP/Fr

Следующим важным показателем является CPT (cost per thousand). Он служит для расчета стоимости рекламной кампании и обозначает стоимость 1000 контактов с рекламой [Dahl, 2011]:

CPT = B / OTS * 1000

где B – это рекламный бюджет.

Таким образом, можно сделать вывод, что основным показателем для оценки является OTS, т.к. все остальные показатели рассчитываются на его основе. Поскольку переменные T (длина рекламного ролика) и Z (частота показа ролика в час) не связаны с аудиторией и зависят только от рекламного бюджета рекламодателя и заполняемостью времени работы цифрового щита, важнейшим показателем для определения эффективности является *Cov (охват пользователей).* Как сказано выше, этот показатель можно только измерить.

2. Методология сбора данных цифровыми щитами

Существует два наиболее распространенных способа собрать данные об охвате каждого цифрового щита [7].

Первый используется преимущественно для тех щитов, которые расположены рядом с автомобильными дорогами или трассами, где поток пешеходов очень маленький или вовсе отсутствует. На цифровой щит ставится видеокамера, которая анализирует поток машин, движущийся напротив щита с рекламным сообщением. Камера настраивается таким образом, что считывает данные только тех машин, водители которых теоретически могут увидеть рекламное сообщение.

Таким образом, камера считает количество автомобилей, которое проехало мимо цифрового щита и могло увидеть рекламное сообщение на нем. Поскольку в одном автомобиле может быть несколько людей, при расчете Cov (охвата рекламного носителя) используется коэффициент – среднее количество людей в автомобиле:

Cov = S(car) * k(p),

где:

S(car) – количество машин, зафиксированных видеокамерой за сутки;

k(p) – среднее количество людей в автомобиле.

Коэффициент k(p) равняется 1,4 [6]. Поскольку информации о расчете данного показателя нет, данное значение не может являться точным. В том числе это связано с:

1. Разной загрузкой автомобилей в разных местах считывания;
2. Разной загрузкой автомобилей в период разных погодных условий;
3. Разной загрузкой автомобилей в разное время суток.

Второй способ является более распространенным и чаще используется для тех цифровых щитов, которые находятся в пешеходных зонах, парках, тротуарах и аллеях. В каждом цифровом щите используется wi-fi ловушка [8], которая раздает незащищенный сигнал. Смартфон, планшет или ноутбук автоматически подключаются к сети, отдавая через wi-fi ловушку данные о физическом (MAC) адресе устройства, времени нахождения в зоне действия сигнала и т.д. В этом случае охват цифрового щита за сутки будет равен количеству уникальных значений MAC-адресов в собранной базе.

Cov = K(unicMAC)

Где K(unicMAC) – количество уникальных MAC-адресов, записанных за сутки

Такой способ сбора данных также связан с рисками искажения данных:

1. С 2014 года выпускаются устройства с рандомизированным MAC-адресом;
2. При выключенном доступе к wi-fi на устройстве такое устройство не будет считано ловушкой;
3. У одного человека может быть одновременно несколько устройств с разными MAC-адресами.

Исследований, связанных с определением погрешности такого способа подсчета охвата, не найдено.

Списки MAC-адресов служат не только для определения охвата цифрового щита, но и для ретаргетинга, путем загрузки базы физических адресов на рекламные площадки. *Т.е. в дальнейшем эта*

информация обрабатывается, передается, хранится и используется рекламодателем, причем есть возможность использовать ее в незашифрованном виде [10].

3. Законы, регулирующие сбор MAC-адресов

Основным законом, регулирующим сбор какой-либо информации о физических лицах в России, является Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ. В нем дается следующее определение персональным данным:

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) [1].

Данные, которые прямо или косвенно относятся к физическому лицу, а также в чем их разница, не уточняются в законе.

Однако вопрос MAC-адресов следует рассматривать в контексте Федерального закона "О связи" от 07.07.2003 N 126-ФЗ [2]. *Согласно закону «О связи», без сведений об абоненте MAC-адреса не относятся к персональным данным.*

С другой стороны, Генеральный регламент о защите персональных данных (GDPR) который является основным регулирующим законом в отношении персональных данных в Европейском союзе, определяет персональные данные так:

Персональные данные – любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу [13].

Идентифицируемое физическое лицо – это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, фамилия, идентификационный номер, данные о местоположении, онлайн-идентификатор или один или несколько характерных для указанного лица физических, физиологических, генетических, духовных, экономических, культурных факторов или ссылаясь на факторы социальной идентичности [13].

Из этого следует, что данные о местоположении пользователя и его идентификационный номер являются персональными данными, порядок хранения, обработки и передачи которых регламентирован GDPR.

4. Угрозы и риски, связанные со сбором MAC-адресов

Главным вопросом, связанным с рисками распространения и передачи MAC-адресов, является возможность деанонимизации с их помощью пользователя.

Любая wi-fi ловушка, с помощью которой отслеживаются MAC-адреса устройств, определяет и передает следующие данные:

1. MAC-адрес устройства;
2. Дата и время контакта с устройством;
3. Длительность контакта.

Некоторые wi-fi ловушки способны определяет расстояние от устройства до источника wi-fi сигнала.

Поскольку по состоянию на 13.02.22 в Москве находится более 500 рекламных цифровых щитов, которые собирают информацию о каждом устройстве, в т.ч. в метро, в торговых центрах, рядом с дорогами, тротуарами и т.д. [5], зная информацию о дате, времени и продолжительности подключения к wi-fi ловушке, можно установить местоположение каждого пользователя в момент времени. С помощью MAC-адреса данные, полученные с разных цифровых щитов, можно объединить и получить карту передвижений каждого конкретного MAC-адреса, в т.ч. можно установить:

1. Местоположение работы;
2. Местоположение дома;
3. Маршрут передвижения отдельно взятого MAC-адреса;
4. Из п. 1,2,3 можно определить уровень платежеспособности;
5. Из географии передвижений и посещений можно определить интересы пользователя;
6. Из карты MAC-адресов можно сделать вывод о семейном положении пользователя.

Также с помощью MAC-адреса можно установить производителя устройства.

В сети Интернет существует множество сервисов, позволяющие определить вендора по MAC-адресу в режиме онлайн [11].

Динамический MAC-адрес, генерируемый на основе алгоритма рандомизации MAC-адреса, не является гарантом сохранения данных в безопасности, т.к. создан алгоритм обхода системы рандомизации. Специалистам, которые занимались данным исследованием [12], удалось достичь результата обхода системы с точностью 100%.

Таким образом сделан вывод, что информация о пользователе, которую можно узнать путем обработки MAC-адресов, является персональными данными согласно определению персональных данных GDPR [13].

Заключение

В ходе исследования были проанализированы способы оценки эффективности DOOH-рекламы и изучены существующие способы сбора данных для проведения оценок. На основе изучения законодательной базы и рисков, связанных со сбором такой информации, были сделаны следующие выводы:

1. MAC-адреса следует отнести к персональным данным физического лица;

2. Физическое лицо должно быть проинформировано о сборе, хранении и обработке MAC-адресов, которые проводятся цифровыми щитами. Также следует уведомлять о зоне действия ловушки для сбора;
3. Сбор, хранение и обработку MAC-адресов следует производить с согласия физического лица;
4. Физическое лицо должно иметь возможность отказаться от предоставления в систему своих персональных данных, либо отменить свое согласие;
5. Все операции, связанные со сбором, хранением, передачей, копированием, изменением и обработкой MAC-адресов следует производить в контексте Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ [1].

Данная работа может быть использована в рамках дальнейших исследований в области интернет-маркетинга, профессиональной этики и информационной безопасности.

Литература

1. Frank Jefkins. Advertising media: Above-the-line // Advertising / Daniel Yadin. — Pearson Education, 2000. — P. 74-122. — 394 p. — (Frameworks – Financial Times Management). — ISBN 9780273634355.
2. Gary Dahl. Advertising For Dummies. — 2. — John Wiley & Sons, 2011. — P. 190. — 336 p. — ISBN 9781118068090.

Стандарты, нормативные документы, методики

1. О персональных данных: федеральный закон от 27 июля 2006 г. N 152-ФЗ // Собрание законодательства Российской Федерации. — 2006. — № 31 (часть I). — Ст. 3451
2. Федеральный закон от 07.07.2003 №126-ФЗ (ред. от 13.07.2015) «О связи» (с изм. и доп., вступ. в силу с 10.01.2016) // Собрание законодательства РФ», 14.07.2003, №28, ст. 2895
3. Доля цифровых конструкций на рынке наружной рекламы. – URL: https://goo.su/azqJ
4. Измерение indoor-рекламы. – URL: https://goo.su/bg5l
5. Карта DOOH в России. – URL: https://dooh.ru/map
6. Методология измерений OTS. – URL: https://ppc.world/articles/na-ulicah-goroda-chto-izvestno-o-naruzhnoy-reklame-ot-yandeksa/
7. Принципы работы информационных цифровых экранов. – URL: https://habr.com/ru/post/539334/
8. Принципы работы Wi-Fi ловушек. – URL: https://goo.su/bmSF
9. Руководство IAB Europe по программной наружной рекламе. – URL: https://goo.su/ausl
10. Требования к данным MAC-адресов для загрузки аудиторий. – URL: https://yandex.ru/dev/audience/doc/intro/data-requirements.html
11. Сервис для определения производителя по MAC-адресу. – URL: https://2ip.ua/ru/services/information-service/mac-find
12. Способ обхода рандомизации MAC-адресов. – URL: https://arxiv.org/pdf/1703.02874v1.pdf
13. General Data Protection Regulation. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Глаз Роман Алексеевич,
аспирант Государственного университета «Дубна»,
roma_glaz@inbox.ru

Шамаева Екатерина Федоровна, к.т.н.,
руководитель Центра управления проектами,
Государственный университет управления,
shamef-kate@yandex.ru

Ключевые слова
Наружная реклама, информационная безопасность, профессиональная этика, персональные данные

Roman Glaz, Ekaterina Shamaeva, Ethical problems of data collection for evaluating the effectiveness of DOOH advertising

Keywords
Outdoor advertising, information security, professional ethics, personal data,

DOI: 10.34706/DE-2022-05-07
JEL classification M31 – Маркетинг, M37 – Реклама.

Abstract
The article analyzes the main criteria for evaluating the effectiveness of digital billboards, identifies measurable indicators. Further, the methods of measuring these indicators are analyzed. In this way, a legal assessment is given. The risks associated with the collection of such information have been studied. As a result, the ethical problem and the way to solve it are determined.