# РЕКЛАМА, КАК УГРОЗА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

*Институт информационных технологий БГУИР,*
*г.Минск, Республика Беларусь*

*Заяц И.Л., Лазаренко Р.А.*

*Савенко А.Г.- магистр технических наук, ассистент*

Информационно-психологическая безопасность личности в информационном пространстве рассматривается как одна из центральных ценностей современного общества. Одним из каналов воздействия на личность является реклама, влияние которой носит двойственный характер. Рекламная безопасность связана с проблемами свободы выбора и идентичности человека в современном информационном обществе. Общий источник внешних угроз информационно-психологической безопасности личности – та информация, которая не только вводит людей в заблуждение, в мир иллюзий, не позволяет адекватно воспринимать окружающее и самого себя, но и травмирует сознание индивида своим возрастающим количеством [1].

Интернет становится формой организации совместной информационно-познавательной и коммуникативной деятельности людей, выступая носителем нравственных ценностей [2]. Цель рекламы в интернете – умело скрыть недостатки и подчеркнуть достоинства товара или услуги. Поэтому большая часть рекламы – обман. Несмотря на внешнюю простоту, реклама использует достаточно сложные механизмы воздействия на человека. Риски для потребителя могут быть связаны не только с тем, что недобросовестная реклама намеренно вводит его в заблуждение, но и с тем, что она освобождает человека от необходимости мыслить самостоятельно, взвешивать соответствующие обстоятельства.

У большинства населения сознание постепенно начинает исполнять роль хранилища штампов и стереотипов, которые воспроизводятся в том же виде, в котором были получены. Процесс критического восприятия информации часто отсутствует.

Специалисты называют эти психологические изменения «руинизацией психики», при которой человеку становится все труднее использовать свои потенциальные интеллектуальные и волевые возможности. В постсоветских странах феномен руинизации особенно выражен у молодых поколений, у которых формирование сознания пришлось на последнее десятилетие.

Первопроходцами в блокировке рекламы стала компания Apple. В сентябре 2015 года компания представила iOS 9 — новую версию операционной системы для мобильных устройств. Тогда в браузере Safari появилась поддержка расширений, способных «блокировать контент». Adblock Plus и другие поставщики подобных расширений для десктопных браузеров смогли опубликовать в App Store свои продукты для Safari.

По данным счётчика «Рейтинг Mail.ru», 9,66% пользователей рунета используют блокировщики. При этом на пользователей такого ПО приходится 10,44% сессий и 11,92% просмотров, что подтверждает гипотезу: блокировщиками пользуется продвинутая и активная, наиболее интенсивно взаимодействующая с сайтами аудитория. Отсюда вытекает очевидное следствие, что аудитория, которая использует блокировщики, наиболее активна, потому что пользоваться интернетом без рекламы гораздо удобнее и приятнее.

С момента появление первых блокировщиков началась гонка вооружений между рекламщиками и блокировшиками. Рекламщики становились все изощрение в методах обхода блокировок. Большинство популярных «эдблокеров» сегодня умеют не только блокировать рекламу, но и запрещать рекламным системам собирать информацию о пользователе.

Самые первые блокировщики имели в основе следующий принцип: они скрывали от глаз пользователя рекламные элементы, которые уже были загружены на страницу. Сейчас этот способ используется в некоторых программах как вспомогательный. Также можно вспомнить браузерные расширения, которые скрывают с сайтов и соцсетей тексты на определенные тематики, ориентируясь по ключевому слову.

Современные «эдблокеры» препятствует коммуникации между отображающей веб-страницу программой, например, браузером, и серверами, с которых загружаются рекламные элементы (баннеры, объявления, видео, попапы и так далее). Или другие элементы, которые он призван блокировать (например, счетчики статистики или кнопки соцсетей).

Основной проблемой на данный момент является то, что в основе блокировки рекламы в интернете лежит не искусственный интеллект на самообучающихся нейросетях, а ручной труд, причем не только разработчиков, но и сообщества.

Продукт этого ручного труда – фильтры, то есть списки правил для определения рекламы и отделения её от полезного контента. Критерии отделения рекламы от всего остального обычно определяются волевым решением основателя того или иного фильтра с учётом мнения сообщества, которое помогает его формировать. Самый популярный набор фильтров называется EasyList. Он не принадлежит какому-то конкретному блокировщику, но используется в большинстве популярных продуктов (в том числе в Adblock Plus, uBlock Origin, AdGuard).

Именно от того, насколько оперативно обновляются фильтры, зависит качество блокировщика. Заинтересованные в показе рекламы компании постоянно работают над обходом блокировки. Они меняют все уже попавшие в фильтры идентификаторы рекламных элементов или шифруют запросы страниц к серверам рекламы, чтобы блокировщик их не остановил. Эта деятельность требует столь же постоянных контрмер.

Однако ещё до того, как началась эта борьба, началась саморегуляция. В 2011 году Adblock Plus объявил о запуске программы Acceptable Ads. Рекламодатели и площадки, согласившиеся адаптировать свою рекламу

под критерии допустимости и качества, помещались в «белый список», а пользователи Adblock Plus видели их рекламу (если не отключали это в настройках).

Учитывая, как быстро происходит смена подходов к отображения рекламных объявления и нахождение способов борьбы с ней, современные способы блокирования рекламы являются неудовлетворительными. Сервисы не могут реагировать достаточно быстро на обратную связь пользователей, в следствие чего новая реклама появляется быстрее, чем блокируют старую.

Для обеспечения безопасности ментального здоровья следует разработать нейронную сеть, с возможностью настройки отображаемой рекламы. Система будет сама подстраиваться под предпочтения пользоваться, и отталкиваясь от них, будет блокировать ту или иную рекламу. Этот подход обеспечит своевременную реакцию на новые угрозы.

Автоматизировать распознавание рекламы сложно, помимо прочего, еще и потому, что даже у людей нет единого мнения насчет того, что является рекламой, а что нет. Поэтому приложение будет отслеживать поведение конкретного пользователя на странице.

После установки приложения пользователю предлагается выбрать определенный паттерн блокировки рекламы. В него будут включаться сайты из «белого списка», а также наиболее приемлемые паттерны рекламы по отзывам других пользователей.

Основываясь на общей статистике, приложение будет скрывать ту рекламу, которая оказалась наиболее неприемлемой, по мнению других пользователей. Рейтинг неодобрения пользователей будет основываться на использовании пользователями одного из способов защиты от негативного информационного влияния – «ухода». Приложение будет отслеживать положение курсора, клики и окна, которые будут активно использоваться. Будет отслеживаться насколько долго реклама находилась на странице, пока пользователь ее не зарыл. Чем это время больше – тем выше лояльность пользователей к данному типу рекламы.

Также активно будет использоваться технология аиртрекинга [3]. Она будет отслеживать на сколько долго пользователь фокусировал внимание на блоках рекламы. Также, как и в случаях с пользовательским вводом, чем выше это время – тем выше лояльность пользователей.

Основываясь на этих данных, приложение будет скрывать «неугодную» для пользователя рекламу. Однако полностью скрыть всю рекламу не представляется возможным. Это происходит потому, что реклама является, в большинстве своем, основным источников доходов для владельцев сайта и крупных поисковых систем.

Постепенно накапливая и анализируя информацию, будут приниматься соответствующие меры по блокированию рекламы.

Список использованных источников:

1. Дроздова, А. В. Воздействие рекламы на безопасность личности в современном информационном обществе: социально-психологический аспект /А. В. Дроздова // Вестник Московского университета. Серия 14. Психология – Москва: МГУ, 2011. – с. 58-65.

2. Филиппова, Т.В. Интернет как инструмент социологического исследования / Т.В. Филиппова, Т.В.Дроздова // Социологические исследования. Выпуск 4 – Красноярск: КГАУ, 2001. – с. 115-122.

3. Окулография. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Окулография. – Дата доступа: 20.03.2018.

# ЗАЩИТА ОТ АВТОМАТИЧЕСКОГО ТРАФИКА

*Институт информационных технологий БГУИР,*
*г.Минск, Республика Беларусь*

*Казанок Д.Ю., Новохрестова А.О.*

*Савенко А.Г.- ассистент каф ПЭ, м.т.н.*

При построении информационных систем различного уровня сложности нередко является актуальным вопрос защиты сервиса от различного рода нежелательных внешних воздействий. Отдельно хотелось бы остановиться на мобильных- и веб-приложениях. В обоих случаях они могут быть тонкими клиентами над серверными приложениями, работающими в облаке. Соответственно, при разработке таких приложений возникает вопрос безопасности серверных приложений против различных форм автоматических запросов, направленных через или в обход разработанного клиентского приложения.

Отсутствие защиты от автоматического трафика при его регулярном поступлении приводит к затратам рабочего времени, оплачиваемого работодателем, на ликвидацию нанесенного ущерба. Так же автоматический трафик значительно увеличивает нагрузку на коммуникации и снижает эффективность работы сервера. Резюмируемый итог: дополнительные финансовые расходы и угроза целостности пользовательских данных (в том числе, при устранении последствий).

Для решения такого рода задач существует понятие CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). Как следует из названия, задача состоит в том, чтобы отличить роботов от человека во время работы приложения [1]. Заметим, что в мобильных приложениях такая задача обретает свою специфику реализации и влияния на пользовательский опыт, что, в свою очередь, оказывает влияние на выбор того или иного способа реализации. Приведем самые актуальные варианты реализации CAPTCHA и особенности их интеграции:

1) Google reCAPTCHA V2

При этом способе анализируются показатели движения мыши, траектория ее движения и отклонения, а также наличие человеческой активности в файлах cookie. Отслеживание данных пользователя покажет, человек