РОЛЬ СОТРУДНИКОВ АГЕНСТВА ИНТЕРНЕТ-МАРКЕТИНГА В ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

М.Н. КУРЛОВИЧ, Т.А. ПАРАФИЯНОВИЧ
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Аннотация: В статье рассматривается роль сотрудников агентств интернет-маркетинга по защите конфиденциальной информации в условиях растущих угроз кибербезопасности. Обсуждаются риски, связанные с утечкой данных, и подчеркивается необходимость внедрения концепции нулевого доверия. Особое внимание, уделяется обучению сотрудников в области кибербезопасности, способствующему минимизации риска утечек.

Современный мир характеризуется стремительным ростом объемов данных, которые ежедневно генерируются всеми пользователями в сети Интернет. Каждый шаг пользователя в сети оставляет «цифровой след», который может быть использован для анализа его поведения, предпочтений и потребительских привычек. Данная информация стала важнейшим ресурсом для множества организаций, работающих в сфере интернет-маркетинга. Однако при увеличении объемов данных возникает ряд вопросов, касающихся их сбора, конфиденциальности и этичного использования.

Согласно закону Республики Беларусь «О защите персональных данных» персональные данные – это «любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано» [1]. К персональным данным относятся: Ф.И.О., идентификационный код, номер паспорта, место рождения и проживания, другие характеристики человека, касающиеся физического, физиологического, генетического, умственного, финансового, культурного и социального состояния. Для маркетинговых целей также важны номер телефона, электронная почта, информация о банковских картах, предыдущие заказы, IP-адрес, сведения о расписании дня, информация об интересах и предпочтениях [2].

Под обработкой персональных данных подразумеваются любые действия, совершаемые с ними, а именно сбор, систематизации, хранение, изменение, использование, обезличивание, блокирование, распространение, предоставление, удаление. Этичный сбор данных для анализа и последующей реализации маркетинговых стратегий требует получения свободного, однозначного, информированного согласия на обработку личной информации от каждого пользователя в письменной или электронной форме. Для получения согласия от субъекта, организация должна предоставить информацию о своем наименовании и месте нахождения, целях и сроках обработки данных, перечне данных и действиях с ними, иную необходимую информацию. Этот документ может быть отозван в любое время по требованию пользователя без объяснения причин [1]. Однако на практике многие организации используют сложные и запутанные условия соглашений, что затрудняет у пользователей понимание того, на что они соглашаются и какие у этого могут быть последствия. Компании

могут извлечь выгоду из неэтичного поведения, получив краткосрочную прибыль, но нужно задуматься и о долгосрочных последствиях своих действий для общества [3].

Одной из важнейших проблем в соблюдении принципов этичного маркетинга остается возможность утечки конфиденциальных данных. Основные причины утечек заключаются в действиях как внешних, так и внутренних нарушителей. Сотрудники, зачастую, представляют собой большую угрозу, чем внешние злоумышленники. Особенно опасны увольняющиеся сотрудники, которые могут использовать доступ к конфиденциальной информации в своих интересах, что приводит к значительным потерям для организаций – они знакомы с внутренними процессами и системами безопасности, поэтому их действия могут быть более продуманными и разрушительными.

В ответ на растущие угрозы кибербезопасности многие организации начинают применять концепцию нулевого доверия, рассматривающую каждого сотрудника как потенциальную угрозу, вследствие чего требующую от него постоянной верификации при доступе к данным [4]. Стратегия нулевого доверия предполагает, что, даже если человек, устройство или программный компонент работают в цифровой среде на законных основаниях, необязательно доверять им во всем, что они делают. По этой причине следует ограничить их полномочия до абсолютного минимума, необходимого для того, чтобы они могли выполнить свою задачу. Для внедрения концепции нулевого доверия компании должны пересмотреть свои внутренние процессы и системы контроля доступа, а также усилить меры по защите данных. Каждое взаимодействие с конфиденциальной информацией должно быть тщательно проверено, что требует дополнительных ресурсов и времени [3]. Успешное применение концепции нулевого доверия может значительно повысить защиту данных и создать более безопасную цифровую среду для всех.

Существует ряд причин, которые делают утечку конфиденциальной информации возможной:

– отсутствие в организации строгой политики безопасности: ограничение прав доступа сотрудников, шифрование данных, использование антивирусных программ и виртуальной частной VPN-сети, резервное копирование информации, регулярный аудит [5];

– использование нелицензионного программного обеспечения;

– недостаточное инвестирование средств в цифровую грамотность сотрудников и профилактику киберугроз;

– нежелание компаний раскрывать информацию о произошедшей утечке, затрудняет анализ ситуации и мешает предотвращению будущих инцидентов;

– высокий уровень уязвимости населения к утечке персональных данных в социальных сетях или при регистрации на различных платформах.

Проблема недостаточной осведомленности сотрудников о правилах обращения с конфиденциальной информацией приводит к неумышленной утечке данных. Для того, чтобы минимизировать риски, связанные с человеческим фактором, необходимо систематически развивать компетенции сотрудников, проводя регулярные тренинги и семинары по следующим

тематикам: общие требование безопасности, хранение резервных копий важных данных, безопасная работа с мобильными устройствами, создание персональных учетных записей для каждого сотрудника с разграничением прав доступа, подключение и работа с частной сетью VPN [6]. Инвестиции в обучение сотрудников не только оправданы, но и необходимы для создания более безопасной профессиональной среды. Применение полученных знаний на практике не должно носить рекомендательный характер. Руководству компании и специалистам по кибербезопасности необходимо выполнять регулярные проверки уязвимости системы и оперативно устранять найденные замечания.

В условиях стремительного роста объемов данных и увеличения угроз кибербезопасности возрастает роль сотрудников агентств интернет-маркетинга в защите конфиденциальной информации. Сотрудники представляют собой как ресурс, так и потенциальную угрозу для безопасности компании. Поэтому важно внедрять концепцию нулевого доверия и пересматривать внутренние рабочие процессы. Ключевым аспектом защиты конфиденциальной информации остается обучение сотрудников.

Список использованных источников:

1. О защите персональных данных: Закон Республики Беларусь, 7 мая 2021 г., № 99-З // Национальный правовой интернет-портал Республики Беларусь [Электронный ресурс]. – Дата доступа: 09.05.2025. – Режим доступа: https://pravo.by/document/?guid=3871&p0=H12100099.

2. Кузнецова, Е. Защита данных в digital-marketing: информационная безопасность маркетинга в интернете / Е. Кузнецова // Агентство «Semantica» [Электронный ресурс]. – Дата доступа: 10.05.2025. – Режим доступа: https://semantica.in/blog/zashhita-dannyh-v-digital-marketing-informaczionnaya-bezopasnost-marketinga-v-internete.html.

3. Швыряев, П. С. Утечки конфиденциальных данных: главный враг внутри / П. С. Швыряев // Государственное управление. Электронный вестник. – 2022. – №91. – С. 226 – 240.

4. Ховард, Р. Кибербезопасность: главные принципы / Р. Ховард. – СПб, 2024.

5. Яковук, А. Н. Кибербезопасность в маркетинге / А. Н. Яковук // Электронный сборник трудов молодых специалистов Полоцкого государственного университета имени Евфросинии Полоцкой / ред. кол.: Ю. Я. Романовский (пред.) [и др.]. – Новополоцк: Полоцкий государственный университет имени Евфросинии Полоцкой, 2023. – Вып. 46 (116): Экономические науки. – С. 87-89.

6. Мальгина, И. В. Кибербезопасность бизнеса: зарубежный опыт / И. В. Мальгина // Технологическая независимость и конкурентоспособность Союзного государства, стран СНГ, ЕАЭС и ШОС: сборник статей VI Международной научно-технической конференции "Минские научные чтения – 2023", Минск, 06-08 декабря 2023 г. – Минск : БГТУ, 2023. – Т. 1. – С. 294-296.