

Экономика личных данных в условиях цифровой трансформации

Петренко Мария Юрьевна

Приамурский государственный университет имени Шолом-Алейхема

Студент

Аннотация

Цель исследования – систематизировать теоретические подходы к анализу экономической ценности личных данных в условиях цифровой трансформации, а также выявить основные способы их сбора, монетизации и рыночного оборота. Результаты исследования показывают, что личные данные превратились в новый экономический ресурс, обладающий значительной рыночной стоимостью, однако их сбор и использование сопровождаются асимметрией информации и парадоксом конфиденциальности, когда потребители, несмотря на заявляемую важность приватности, продолжают бесплатно предоставлять свои данные.

Ключевые слова: личные данные, цифровая экономика, монетизация данных, рынок данных, конфиденциальность, парадокс конфиденциальности, цифровой след.

The personal data Economy in the context of digital transformation

Petrenko Maria Yuryevna

Sholom-Aleichem Priamursky State University

Student

Abstract

The purpose of the study is to systematize theoretical approaches to analyzing the economic value of personal data in the context of digital transformation, as well as to identify the main methods of collecting, monetizing, and marketing personal data. The results of the study show that personal data has become a new economic resource with significant market value, but its collection and use are accompanied by information asymmetry and the privacy paradox, where consumers continue to provide their data for free despite the importance of privacy.

Keywords: personal data, digital economy, data monetization, data market, privacy, privacy paradox, digital footprint.

В условиях цифровой трансформации экономики данные стали одним из ключевых факторов производства наряду с трудом, капиталом и землёй. Ежедневно каждый пользователь интернета генерирует огромное количество информации о себе: от демографических характеристик до поведенческих паттернов и предпочтений. Эта информация, известная как личные данные,

приобрела значительную экономическую ценность и превратилась в объект коммерческого оборота.

Актуальность исследования обусловлена тем, что рынок личных данных характеризуется глубокой асимметрией информации: пользователи зачастую не осознают реальную стоимость своих цифровых следов, а компании активно монетизируют эту информацию, используя её для таргетированной рекламы, поведенческого анализа и прогнозирования потребительского спроса. Парадокс конфиденциальности, при котором люди говорят об обеспокоенности защитой своих данных, но продолжают их бесплатно предоставлять, требует теоретического осмысления в рамках экономической науки.

Изучив научные работы по теме экономики личных данных, можно выделить следующие ключевые тезисы:

1. В статье К. В. Коробейниковой обосновывается, что цифровая экономика представляет собой сбор цифровых данных с помощью интернет-технологий, а создание прав на личную информацию стало неизбежным требованием в эпоху цифровой экономики [1];

2. Дэн МинФан в статье отмечает, что проблема защиты личной информации является одной из важнейших, нуждающихся в законодательном регулировании и контроле со стороны государства. В статье описываются исследования, проводимые в сфере цифровой безопасности, использования персональных данных, проводимые в различных странах [2];

3. В статье В. В. Каменновой указывается, что на «чёрном рынке» персональные данные стоят кратно больше, чем даже полные сведения банковской карты, а также приводятся данные о масштабных утечках информации в крупнейших российских компаниях [3];

4. В статье С. А. Моргуновой представлены результаты исследования отношения российских потребителей к сбору и анализу данных, выявлены основные противоречия и парадоксы конфиденциальности [4];

5. А. М. Кузьмин, Д. А. Свичкарь и П. В. Хенкин анализируют схемы создания несуществующих цифровых личностей на основе реальных и сфабрикованных данных, масштабы финансовых потерь и экономические последствия данного вида преступлений [5];

6. В исследовании А. В. Кириченко и Н. В. Ганженко рассматриваются проблемы обеспечения конфиденциальности при растущем объёме цифрового следа, оставляемого пользователями в сети Интернет, и описываются коммерческие механизмы использования этих данных [6].

Цель данного исследования – систематизировать теоретические подходы к анализу экономической ценности личных данных в условиях цифровой трансформации, а также выявить основные способы их сбора, монетизации и рыночного оборота.

Цифровая экономика представляет собой динамичную концепцию, основу функционирования которой составляет сбор цифровых данных с помощью интернет-технологий. В отличие от традиционной формы сбора информации, скорость сбора цифровых данных в цифровой экономике имеет

большие преимущества, она может накапливать большое количество цифровых данных с помощью алгоритмов и формировать массивную базу данных, что стало внутренней движущей силой быстрого развития цифровой экономики [1].

По сравнению с традиционными данными, цифровые данные нельзя использовать напрямую. Их необходимо обрабатывать и интегрировать через платформу, чтобы иметь возможность преобразовывать их в информацию и затем использовать. Цифровая экономика может хранить большое количество экономической информации, а с помощью интернет-технологий цифровые данные могут храниться на облачном сервере платформы. Экономическая информация в эпоху цифровой экономики может сохраняться в больших количествах, что позволяет повысить коэффициент использования и коэффициент конверсии экономической информации [1].

Важным теоретическим положением является закон Меткалфа: «суммарное значение сети, сформированной пользователями, представляет собой квадрат количества пользователей: чем больше пользователей, тем выше значение сети, которое еще называют экстернальностью сети, а в цифровой экономике огромные данные заменяют пользователей, чем больше данных, тем большее значение может быть сгенерировано, что является «экстернальностью данных»» [1].

По сравнению с традиционной экономикой цифровая экономика предоставляет более широкие возможности для обмена информацией, что позволяет генерировать многократно возросшую стоимость, а при использовании масштабных данных активность экономической деятельности достигает новой высоты. В последние годы фокус крупных интернет-компаний и производителей постепенно сместился с утечки трафика на сбор данных, а интернет и даже всё общество вступили в эпоху «данных» [1].

Проблема защиты личной информации на современном этапе развития цифрового общества названа одной из важнейших, которая нуждается в законодательном регулировании и контроле со стороны государства. В контексте современной цифровизации и глобализации информация является, с одной стороны, одним из мощнейших ресурсов общественного развития, с другой – это эффективный инструмент управления отдельными людьми, группами и обществом в целом [2]. Особенно это важно по отношению к персональным и конфиденциальным данным, личной информации. Потенциал использования цифровых, компьютерных и интернет-технологий актуализирует вопросы обеспечения безопасности сбора, хранения и использования личной информации, а также её защиты от несанкционированного вторжения. В данном случае речь идёт об использовании технологий «больших данных» (Big Data), где имеется доступ к структурированным и неструктурированным данным практически неограниченных объёмов [2].

В контексте развития цифровых технологий и сбора данных вопрос приватности становится всё более актуальным. В результате исследования, проведённого компанией Kaspersky в 2020 году с привлечением 15000 человек

в возрастном диапазоне 18-55 лет, стало ясно, что 57% опрошенных понимают необходимость сбора данных о них для улучшения предоставляемых продуктов и услуг. Однако около трети (30%) относятся с недоверием к компаниям, собирающим их данные. Из этих тридцати процентов 43% отметили, что сомневаются в защите личной информации, а 30% подозревают, что их данные используются без их согласия. Выявлено, что молодые опрошенные более склонны к предоставлению информации о себе, чем старшее поколение. Помимо этого, больше половины (55%) хотели бы иметь выбор и контроль над способом сбора и обработки личных данных. Однако меньше трети (29%) знают, как управлять использованием информации о них. Это показывает, что потребители осознают необходимость сбора и анализа личной информации о них, но при этом хотят большего контроля и защиты в данном процессе [4].

Конфиденциальность данных в digital-сфере имеет значение для пользователей, однако они могут быть готовы предоставить свои данные при определённых условиях. Компании должны активно работать над политиками конфиденциальности, обеспечивать прозрачность в отношении сбора и использования данных, а также строить доверие пользователей через надёжные системы защиты данных [4]. Исследование выявило, что пользователи обладают разной степенью осведомлённости о конфиденциальности данных и понимания о том, как компании используют их личную информацию. Репутация компании играет важную роль в восприятии пользователей о защите их данных. Утечка персональных данных может иметь негативные последствия для репутации компании: даже один случай утечки данных может вызвать недоверие и негативное отношение со стороны пользователей [4].

Согласно Федеральному закону № 152-ФЗ «О персональных данных» «персональные данные – это любая информация о физическом лице, в частности, фамилия, имя, отчество, место и дата рождения, место проживания и регистрации, социальное, имущественное и семейное положение, профессия, образование, доходы и другое» [3]. Сбором такой информации занимаются государственные или муниципальные органы, практически любые юридические лица, а также физические лица. Все они выступают в качестве операторов персональных данных и несут ответственность за их сохранность [3].

На «чёрном рынке» персональные данные стоят кратно больше, чем даже полные сведения банковской карты [7]. Масштаб проблемы подтверждается данными об утечках. В феврале 2021 года информационный сайт РИА Новости опубликовали список «громких» утечек 2020-2021 года. Среди источников утечек оказались такие крупнейшие организации, как Яндекс, Сбербанк, Россельхозбанк, Тинькофф банк, Райффайзенбанк, Авито, Юла и многие другие [3]. По данным РБК, «записи могут содержать полный набор персональных данных, которые требуются для оформления кредита: Ф.И.О., дата рождения, сумма и вид кредита, номер телефона, почтовый ящик, паспортные данные, ИНН, СНИЛС, домашний адрес, адрес места работы,

должность, размер дохода и другие сведения. Согласно объявлению, полная база стоит 100 тыс. руб. Отдельные строки с данными за 2021 год продаются за 15 руб., за вторую половину 2020 года – 10 руб., за первую половину 2020 года – 7 руб.» [3].

Всё это говорит о том, что даже сегодня при современном уровне развития технологий ни одна организация, включая органы государственной власти, не может гарантировать абсолютную защиту личных данных от мошенников и нелегальных учреждений [3].

Цифровой след является основным источником данных для коммерческого использования. Цифровой след – это информация, которая остаётся в сети после действий пользователя. Следы миллионов пользователей по всему миру представляют собой большие данные (Big Data) и являются целью обработки многих организаций, начиная монополями гигантами вроде Amazon и Google и заканчивая рекламными компаниями [6].

Цифровой след бывает активным и пассивным. Активный след – это сознательные действия пользователя в сети – посты в социальных сетях, комментарии, фотографии, переписка, лайки. Пассивный след – это непредумышленно оставленные данные – геолокация мобильного устройства, история посещений сайтов, IP-адрес устройства, с которого пользователь выходил в сеть [6].

На основе цифрового следа фильтруется и отбирается интересующий пользователя контент во Всемирной паутине. Рекламные компании идут тем же путём – анализируя деятельность пользователя в сети, они составляют его портрет как потребителя и предлагают те товары и услуги, что заинтересуют потребителя с большей вероятностью. Фильтрация контента и таргетированная реклама очень облегчает жизнь пользователя в сети. С другой стороны, интернет-площадки могут менять цены на свою продукцию в зависимости от истории покупок пользователей, повышать цены при увеличении количества заказов и наоборот, уменьшать цены при отсутствии заказов [6].

Большая часть цифровой информации визуальна: её составляют фотографии, видеоролики, данные с камер видеонаблюдения. На втором месте находится текстовая информация – электронная почта, электронные документы, переписки пользователей. Следом за текстовой информацией идёт голосовая информация – различные виды телефонной связи. Вся эта информация может быть использована недоброжелателями и злоумышленниками. Фото-, видео- и голосовые материалы могут быть использованы для уничтожения репутации одного человека или группы людей либо компрометации их тайной личной жизни. Текстовая информация из переписок может использоваться для тех же целей. Рабочие же переписки и документы, которые были получены путём несанкционированного доступа к учётной записи работника организации с использованием его цифрового следа, могут привести к серьёзным убыткам организации [6].

Банковские операции – ещё один источник достаточно большого пласта информации. При совершении операции банк получает точную информацию

о местоположении магазина или другого заведения, наименование и стоимость товара или услуги. Анализ этих данных может привести к компрометации адреса проживания, работы, уровня доходов, статей расходов и даже медицинских данных. Учитывая, как часто происходят утечки баз данных банковской информации, это довольно опасная информация в руках злоумышленников. Многим людям сразу после получения кредита или крупного перевода поступают звонки от мошенников, представляющихся службой безопасности банка и обманом пытающихся завладеть чужими средствами [6].

Особую опасность представляет использование цифровых данных для создания синтетических личностей. Синтетическая цифровая личность (далее – СЦЛ) представляет собой несуществующую цифровую личность, состоящую из набора данных, таких как имя, фамилия, телефон, адрес, сфабрикованных из вымышленных данных или скомпилированных из реальных и вымышленных данных [5].

Главным отличием и соответственно опасностью для атакуемой организации является отсутствие пострадавшего. В случае традиционного мошенничества злоумышленник использует реальные данные существующего человека и таким образом наносит ущерб конкретному человеку. Жертва обнаруживает мошеннические действия и обращается в организацию и правоохранительные органы, что зачастую позволяет оперативно расследовать инцидент. В случае мошенничества с использованием СЦЛ жертва, в традиционном понимании, отсутствует, что не позволяет оперативно установить факт преступления, и жертвой в данном случае становится сама организация [5].

По оценкам экспертов, потери от мошенничества с использованием СЦЛ в США достигли 20 млрд долларов в 2020 году. Финансовые организации, обнаруживающие активные поддельные аккаунты, закрывают их, а потери зачастую объясняются плохим андеррайтингом. По оценкам, за 12 месяцев с момента открытия счетов СЦЛ имеют возможность похитить около 90000 долларов США [5]. Мошенничество с СЦЛ стало самым быстрорастущим видом финансовых преступлений в США. Преступники используют автоматизацию для сбора элементов личности и создают миллионы синтетических профилей. Благодаря глубокому пониманию принципов работы платёжной системы и использованию специально разработанного программного обеспечения преступники имеют возможность создавать синтетические профили, которые очень сложно выявить. В отличие от кражи реальной личности, в данном случае нет пострадавшего, который может заметить мошенническую транзакцию в своей истории транзакций и обратиться в банк [5].

В Российской Федерации в силу принятых законов и выработанных процедур в финансовых организациях проверки персональных данных клиентов аналогичные мошеннические схемы с применением СЦЛ реализовать гораздо сложнее, но в случае сговора с сотрудником финансовой или другой организации такое становится возможным. Государственные

органы социальной защиты в России также подвержены риску мошенничества с СЦЛ. Некоторые случаи были зафиксированы на протяжении последних 10 лет [5]. Ряд других организаций также может быть подвержен данному виду мошенничества, но пока подобные случаи не выделены в отдельную категорию и не ведётся статистика потерь, поэтому оценить текущий уровень потерь в России от мошенничества с СЦЛ не представляется возможным [5].

Как отмечается в международных исследованиях, особенно остро проблема защиты личных данных стоит в развитых странах Европы, США, России и Востока. В 2016 году решением Европейского Парламента и Совета был принят Генеральный регламент по защите персональных данных (GDPR), регулирующий основные вопросы защиты личной информации и защищающий граждан от несанкционированного распространения личной информации, ограничения к ней доступа, а также обеспечения прав, которые определены более общими международными законодательными актами. В законодательстве различных стран акцент делается на совершенствовании международного сотрудничества в сфере трансграничного обмена цифровыми данными [2].

Европейская модель правовой защиты вызывает интерес в контексте использования практики применения законодательства в данной сфере, а также может служить примером для различных стран, в которых актуальна данная тематика [2]. В России нормативно-правовая база позволяет определить понятие, содержание персональных данных и степень защиты в зависимости от уровня конфиденциальности. Основной проблемой является сложность разграничения личной информации и конфиденциальной, касающейся не отдельных лиц, а отраслей, учреждений, предприятий. Это обусловлено тем, что защита личной информации регулируется нормами гражданского законодательства и не имеет определённой специализации [2]. Совершенствование законодательной базы различных государств сводится к единой идее выделения цифрового права в отдельную отрасль либо подотрасль, регулируемую гражданским правом. Современные правовые системы Европы, России, Азии и США имеют недостаточную разработанность и не всегда могут справляться с защитой предоставляемого объёма личной информации [2].

Подводя итог исследованию, можно сделать вывод, что личные данные в условиях цифровой трансформации превратились в новый экономический ресурс, обладающий значительной рыночной стоимостью. Отношение потребителей к сбору данных имеет двойственный характер: большинство пользователей осознают необходимость предоставления информации для улучшения сервисов, но при этом испытывают недоверие к компаниям, а доля тех, кто знает, как управлять использованием своих данных, остаётся невысокой. Рынок личных данных существует как в легальной форме (таргетированная реклама, поведенческий анализ), так и в теневой – через продажу баз на «чёрном рынке», а синтетические цифровые личности стали новым инструментом финансовых преступлений.

Дальнейшие исследования в этой области должны быть направлены на количественную оценку экономической ценности личных данных, разработку механизмов справедливого распределения выгод от их коммерческого использования и совершенствование правового регулирования в условиях цифровой трансформации.

Библиографический список

1. Коробейникова К. В. Использование данных в цифровой экономике с точки зрения защиты личной информации // Модернизация российского общества и образования: новые экономические ориентиры, стратегии управления, вопросы правоприменения и подготовки кадров. Таганрог: Таганрогский институт управления и экономики, 2023. С. 264-266. URL: <https://www.elibrary.ru/item.asp?id=54388512>
2. Дэн М. Исследования по защите личной информации в различных странах цифровой эпохи // Современные исследования и научные достижения в эпоху цифровизации: новые ориентиры и возможности. Ставрополь: Общество с ограниченной ответственностью «Ставропольское издательство «Параграф», 2023. С. 77-79. URL: <https://www.elibrary.ru/item.asp?id=50282271>
3. Каменнова В. В. Защита персональных данных // Развитие современной юриспруденции: актуальные вопросы теории и практики. Пенза: Общество с ограниченной ответственностью «Наука и Просвещение», 2021. С. 204-206. URL: <https://www.elibrary.ru/item.asp?id=45786225>
4. Моргунова С. А. Конфиденциальность данных в Digital: отношение потребителей к сбору и анализу данных цифровыми компаниями // Студент и наука: актуальные вопросы современных исследований. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2023. С. 89-92. URL: <https://www.elibrary.ru/item.asp?id=54224238>
5. Кузьмин А. М., Свичкарь Д. А., Хенкин П. В. Мошенничество с использованием синтетических цифровых личностей // Современные информационные технологии и ИТ-образование. 2023. № 2. С. 251-261. URL: <https://www.elibrary.ru/item.asp?id=65663434>
6. Кириченко А. В., Ганженко Н. В. Влияние цифрового следа на обеспечение конфиденциальности информации // Безопасность информационного пространства. Екатеринбург: Уральский государственный экономический университет, 2021. С. 101-104. URL: <https://www.elibrary.ru/item.asp?id=46636185>
7. Батыгова Г. Б. Защита персональных данных // Синергия наук. 2021. № 62. С. 161-165. URL: <https://www.elibrary.ru/item.asp?id=46694732>