Кибербезопасность куайринга для парковки автомобилей

Нугманова Айсина Минехатовна

Гейслер затрагивает проблему безопасности оплаты с помощью QR в работе «Зацепило: Реальное исследование фишинга с помощью QR-кодов». Использование кодов быстрого реагирования (QR) было ограничено до пандемии COVID-19. Из-за широкого распространения и частого применения с тех пор, это открыло привлекательную возможность для фишинга для злоумышленников. Они обманом заставляют пользователей сканировать коды и перенаправлять их на вредоносные веб-сайты. Чтобы выяснить, является ли фишинг с помощью QR-кодов еще одним успешным направлением атаки, авторы провели реальную фишинговую кампанию с использованием двух различных вариантов QR-кодов в исследовательском кампусе. Первая версия была довольно простой, в то время как вторая версия была более профессионально оформлена и включала возможность выиграть ваучер. После завершения исследования был проведен качественный опрос о фишинге и QR-кодах для проверки результатов фишинговой кампании. Как фишинговая кампания, так и опрос показывают, что профессиональному дизайну уделяется больше внимания. Они также показывают, что любопытные пользователи чаще используют QR-коды из-за их простой функциональности. Хотя результаты подтверждают, что технически подкованные пользователи лучше осведомлены о рисках, они также указывают на потенциальную опасность для нетехнически подкованных пользователей и предполагают дальнейшую работу по принятию контрмер [17].

Шаревски, Моссано и Вейт в исследовании обращают внимание на то, что QR-коды, предназначенные для удобного доступа к ссылкам, недавно были использованы в качестве векторов фишинговых атак. Поскольку этот тип фишинга является относительным, а многие аспекты угрозы в реальных условиях неизвестны, они провели исследование в естественных условиях (n=42), чтобы выяснить, как люди ведут себя с QR-кодами, которые могут содержать фишинговые ссылки. Авторы обнаружили, что 28 (67%) участников

открыли ссылку, встроенную в QR-код, не проверив URL на наличие потенциальных фишинговых подсказок. В качестве предлога они использовали плакат, который приглашал людей отсканировать QR-код и внести свой вклад на гуманитарную помощь. Выбор предлога был достаточно убедительным, и 22 (52%) участников указали, что это была основная причина, по которой они отсканировали QR-код и перешли по встроенной ссылке в первую очередь. Исследователи использовали три варианта ссылок, чтобы проверить, способны ли люди распознать потенциальную угрозу фишинга, связанную с QR-кодом плаката (каждый участник отсканировал только один вариант). В вариантах, где ссылка казалась подлинной или была скрыта сервисом сокращения ссылок, только двое из 26 участников (8%) отказались от ссылки, когда увидели, что предварительный просмотр в приложении для сканирования QR-кода. В варианте, когда ссылка явно содержала слово “фишинг” в доменном имени, это соотношение увеличилось до 7 из 16 участников (44%). Они используют результаты, чтобы предложить эффективные меры безопасности в приложениях для сканирования QR-кодов, предназначенные для предупреждения пользователей о потенциально фишинговых ссылках [45].

Цвитик и Перакович в работе «Исследование влияния технологий ближнего радиуса действия как вектора кибератак» говорят о том, что в сфере цифровых коммуникаций технологии ближнего действия, такие как NFC и QR-коды, легко интегрировались в повседневную жизнь, обеспечивая непревзойденное удобство и эффективность. Однако это удобство часто сопровождается недооцененными уязвимостями, что создает значительные риски для безопасности пользователей. Данное исследование направлено на изучение современных тенденций в области безопасности и потенциальных рисков, связанных с технологиями ближнего действия. Проводя это исследование, авторы стремятся внести свой вклад в разработку всеобъемлющей политики и стратегий, направленных на усиление защиты пользователей от угроз кибербезопасности. Важным аспектом исследования

также является информирование пользователей о важности онлайн-безопасности и практических мерах по защите от потенциальных киберугроз, исходящих от использования таких технологий, как NFC и QR-коды, как для мужчин, так и для женщин. Чтобы достичь глубокого понимания этих проблем, методология исследования включает количественный анализ, в ходе которого авторы собирали данные о количестве пользователей, взаимодействующих с определенными QR-кодами или NFC-метками. Этот подход позволяет получить количественное представление о распространенности киберугроз, связанных с этими технологиями. Кроме того, они провели подробный опрос пользователей на специальном веб-сайте. Результаты этого опроса дают более четкое представление о демографических и поведенческих характеристиках пользователей, которые более подвержены подобным кибератакам [12].

Бекавач и соавторы в работе «Целостность QR-кода по дизайну» подчеркивают - поскольку QR-коды становятся все более распространенными в различных приложениях и местах, их уязвимость к подделке, известная как удаление, представляет серьезную угрозу для безопасности пользователей. В этой статье исследователи представляют коды SafeQR, которые решают эту проблему путем внедрения инновационных стратегий проектирования для повышения безопасности QR-кодов. Используя визуальные элементы и принципы безопасного дизайна, проект направлен на то, чтобы сделать взлом более заметным, тем самым позволяя пользователям распознавать потенциальные угрозы фишинга и избегать их. Кроме того, авторы подчеркивают ограниченность существующих методов обучения пользователей в борьбе с кибератаками и предлагаем различные модели атак, адаптированные для противодействия кибератакам. Кроме того, авторы представляем многогранную стратегию защиты, которая сочетает в себе инновации в дизайне и бдительность пользователей. Проведя исследование с участием пользователей, они продемонстрировали эффективность QR-кодов "Целостность за счет дизайна". Эти инновационно разработанные QR-коды

значительно повышают подозрительность пользователей в случае подделки и эффективно снижают вероятность успешного завершения атак [6].

Исследователи Гимах, Офори-Менсах и Бувуо в работе «Расширение возможностей водителей транспортных средств с общей мобильностью, StoppingScams: цепочка кибератак и информационно-просветительский подход к написанию текстов в университетских городках» рассказывают о том, что QRishing, технология фишинга с использованием QR-кодов, представляет собой растущую угрозу в эпоху цифровых технологий. В этом исследовании рассматривается уязвимость мобильных устройств общего пользования в университетских городках США к атакам QRishing. В исследовании на примере крупного университета Среднего Запада проанализировано, как электронные велосипеды / скутеры могут быть использованы для размещения вредоносных QR-кодов. В исследовании рассматриваются распространенные тактики QR-поиска и их потенциальное влияние на студентов, сотрудников и сообщества. В нем рассматриваются технические аспекты имитируемой атаки QR-кодирования, в которой особое внимание уделяется использованию искусственного интеллекта (ИИ). Кроме того, в документе предлагаются контрмеры для программ проката электронных велосипедов и рекомендации для студентов, которые помогут им не стать жертвами. Подчеркивая важность сотрудничества между университетами, компаниями по аренде жилья и правоохранительными органами, этот документ направлен на снижение рисков, связанных с QRishing, и защиту студенческого сообщества. Полученные результаты подчеркивают необходимость проведения комплексных программ повышения осведомленности о кибербезопасности, безопасной генерации QR-кодов и повышения безопасности приложений для защиты пользователей от развивающихся киберугроз [21].

Ю. Блах и М. Климонтович, в работе «Факторы, определяющие успех PayTech на рынке мобильных платежей — на примере BLIK» Финтех и его взаимодействие с банковской деятельностью сегодня широко обсуждаются

как новое явление, несмотря на то, что взаимосвязь между технологиями и финансовыми услугами не является новой темой. Большинство исследований посвящено инновациям и факторам, определяющим их внедрение, в том числе в платежной системе. Исследования, непосредственно посвященные платежным системам как особому виду финтех-компаний и их рыночной активности, являются относительно новой областью исследований. Данная статья призвана восполнить этот пробел. Многомерный характер этого исследовательского исследования обуславливает необходимость применения различных методов исследования, включая как индуктивный, так и дедуктивный методы, а также сравнительный анализ. Теоретический анализ, проведенный в статье для определения PayTechs с точки зрения бизнес-модели и поведения на рынке, был основан на подробном обзоре литературы. В этом разделе в основном применялись индуктивный метод и сравнительный анализ. Эмпирическая часть статьи включает анализ количественных данных, опубликованных Национальным банком Польши (NBP), Центральным статистическим управлением (GUS) и Банком международных расчетов (BIS). Предметом рассмотрения дела является польский платежный стандарт BLIK, внедренный в Польше в 2015 году для мобильных платежей. Распространение BLIK измеряется количеством участников и получателей, а также объемом транзакций, в то время как внедрение - количеством клиентов, использующих BLIK в повседневных транзакциях. Результаты представляют рыночное поведение BLIK как открытой бизнес-модели, а также ключевые факторы успеха внедрения и распространения BLIK и факторы, определяющие дальнейшее развитие инноваций в области открытых платежей. Недавно разработанное определение PayTechs, определение основных компонентов открытой бизнес-модели PayTech, а также указание на ключевые факторы успеха внедрения и распространения электронных платежей являются оригинальным вкладом в этот документ [8].

Стил, Морис и Морган говорят о том, что использование кодов быстрого реагирования (QR) представляет угрозу безопасности, существует мало

данных наблюдений, изучающих влияние информационных сигналов на взаимодействие. Хотя натуралистические наблюдения за использованием QR-кодов на территории кампуса и за его пределами, показали, что любопытство, а не информационные потребности мотивируют к участию, кажется, что информационные сигналы должны играть важную роль в принятии решений, основанных на безопасности. Более десяти лет спустя исследование посвящено натуралистическому использованию QR-кодов в кампусе с акцентом на информационные сигналы на листовках. Листовки были размещены в оживленных местах кампуса, и научные сотрудники регулярно проверяли их доступность. Исследователи подсчитали количество пользователей, которые использовали QR-код, по типу листовки (например, пустая, только логотип университета, фишинговое объявление о приеме на работу). Участникам исследования было предложено заполнить краткий опрос, в котором они поделились своим опытом в области безопасности, мотивацией и прогнозируемым поведением в будущем. Активность рекламодателей была низкой, особенно учитывая численность студентов в кампусе. Авторы показали, что вовлеченность во все типы рекламных листовок возрастала по мере увеличения количества информационных сигналов. Отрадно видеть низкий уровень вовлеченности, учитывая эти подозрительные рекламные листовки. Этот сдвиг в сторону поиска информации, а не простого любопытства, скорее всего, отражает большую осведомленность пользователей об атаках QRishing [48].

В статье «Разработка и внедрение безопасного Qr-платежа на основе визуальной криптографии» исследователи рассмотрели разработку и внедрение безопасной платежной системы, основанной на QR-кодах. В последние годы QR-коды получили широкое распространение благодаря их способности ускорять платежи и обеспечивать клиентам максимальный комфорт. Однако, какими бы удобными ни казались системы онлайн-платежей на основе QR- кода, они уязвимы для различных атак. Обработка транзакций должна быть достаточно безопасной, чтобы обеспечить конфиденциальность

и точность каждой платежной операции. Система онлайн-платежей должна также гарантируется легитимность каждой транзакции как для отправителя, так и для получателя. В этой статье предлагается система защиты на основе QR-кода с использованием визуальной криптографии. Рекомендуемое решение состоит из мобильного приложения и сервера платежного шлюза, использующего визуальную криптографию. Клиенты, использующие приложение, могут проводить финансовые операции в безопасной среде благодаря его понятному и удобному для пользователя интерфейсу [53].

М. Альджохани, С. Олариу и А. Алали в исследовании «Обзор парковочных решений для умных городов» Существующие исследования рассматривают решения для парковки с точки зрения датчиков, коммуникационных протоколов и аппаратно-программного интерфейса. Хотя это полезный подход, он страдает тремя очевидными недостатками, а именно тем, что современные датчики, скорее всего, устареют через несколько лет, протоколы связи будут сняты с производства, а современное программное обеспечение почти наверняка не будет работать на платформах завтрашнего дня. Следовательно, эти подходы не являются перспективными для создания "умных городов" ближайшего будущего. В отличие от предыдущих исследований, авторы рассматривают парковку в "умных" городах через призму рыночного распределения товаров и услуг. На конкурентных рынках цены выступают в качестве сигналов, используемых для распределения товаров среди тех, кто ценит их больше всего. Что касается парковочных мест, то некоторые водители готовы платить более высокие цены за пользование теми парковочными местами, которые предлагают им наибольшую выгоду. Уникальность исследования заключается в том, что они изучали новейшую литературу в поисках рыночно ориентированных решений, включая ценообразование как инструмент формирования трафика и стимулирования социально приемлемого поведения водителей. Исследователи считают, что одним из важных вкладов любой обзорной статьи, помимо того, что она представляет собой сборник известных работ, является предложение новых

направлений исследований. Эти перспективы призваны заставить задуматься и открыть новые пути для возможных расследований [4].

Тему безопасности куайринга для парковочных автомобилей в своих работах также поднимали: Рахман и Бахай в исследовании «Охраняемая система парковки и бронирования, интегрированная с распознаванием автомобильных номеров и QR-кодом» [1], Тота М. К., Пратибхавани П. М., Венугопал К. Р. Висследовании «Интеллектуальная система парковки: QR-код для определения устойчивости автомобиля в "умном городе"» [50].

Из отечественных исследователей похожие исследования проводили: Кемалов в исследовании «Блокчейн и Интернет вещей (IoT): Взаимодействие и перспективы интеграции» [60], Майдан С. Б. «Рекламные исследования как разновидность маркетинговых исследований: понятие, роль, цель и задачи» [62], Шарапова и Новикова «Privatebanking в практике российских банков» [69], Соснило А.И. «Атлас искусственного интеллекта для бизнеса и власти» [66] и Трощинский П.В. в работе «Цифровой Китай до и в период коронавируса: особенности нормативно-правового регулирования» [67].

Список использованной литературы

1. Abd Rahman N. A. et al. Secure parking and reservation system integrated with car plate recognition and qr code //2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). – IEEE, 2022. – С. 1-7.

2. Ahmadian M. M. et al. Retiring meters: a roadmap to encourage wider adoption of parking apps //Transportation. – 2024. – С. 1-29.

3. Ahmed T. et al. Assessing Heterogeneity Among Cyclists Towards Importance of Bicycle Infrastructural Elements in Urban Areas //Infrastructures. – 2024. – Т. 9. – №. 9. – С. 153.

4. Aljohani M. et al. A survey of parking solutions for smart cities //IEEE Transactions on Intelligent Transportation Systems. – 2021. – Т. 23. – №. 8. – С. 10012-10029.

5. Ari M. [NEOBHÁJENO] Impact of Smart Tourism Technologies on Tourist Experience Satisfaction and Sustainable Destination Image: Evidence from Istanbul. – 2022.

6. Bekavac L. J. L., Mayer S., Strecker J. QR-Code Integrity by Design //Extended Abstracts of the CHI Conference on Human Factors in Computing Systems. – 2024. – С. 1-9.

7. Bhatt R. et al. Equitable charging infrastructure for electric vehicles: access and experience //Progress in Energy. – 2024. – Т. 6. – №. 3. – С. 033006.

8. Błach J., Klimontowicz M. The Determinants of PayTech's success in the mobile payment market—the case of BLIK //Journal of Risk and Financial Management. – 2021. – Т. 14. – №. 9. – С. 422.

9. Blancaflor E. et al. Impact Analysis and Attack Simulation on Quishing (a QC Code Phishing) using QRLJacker //2024 International Conference on Electrical, Computer and Energy Technologies (ICECET. – IEEE, 2024. – С. 1-5.

10. Boz Y., Cay T. How smart and sustainable are the cities in Turkiye?-National policies and the enthusiasm level of the local governments //Heliyon. – 2024. – Т. 10. – №. 4.

11. Capaccioli A. et al. inclusive digital mobility. – 2024.

12. Cvitić I. et al. Research on the Impact of Short-Range Technology as Cyber Attack Vector //EAI International Conference on Management of Manufacturing Systems. – Cham : Springer Nature Switzerland, 2024. – С. 99-110.

13. Edsgård E. et al. The effects of and attitudes toward mobility-and parking measures in Gothenburg. – 2024.

14. Ergün G., Akman Ç. Local Digital Transformation Studies in the Case of Konya Metropolitan Municipality //Digital Competency Development for Public Officials: Adapting New Technologies in Public Services. – IGI Global Scientific Publishing, 2025. – С. 453-474.

15. Farhana A. T. et al. Uses, constraints, and benefits of QRIS for merchants in PondokCina Station //JurnalStudiKomunikasi. – 2025. – Т. 9. – №. 1. – С. 054-066.

16. Fatimah S., Setiyawan W. B. M., Virdaus S. Dignified economic development by the implementation of electronic payment systems in the post of COVID-19 pandemic: Pembangunan ekonomi yang bermartabatdenganpenerapansistempembayaranelektronikpascapandemi COVID-19 //Constitutional Law Society. – 2023. – Т. 2. – №. 2. – С. 178-196.

17. Geisler M., Pöhn D. Hooked: A Real-World Study on QR Code Phishing //arXiv preprint arXiv:2407.16230. – 2024.

18. Geurs K., Grigolon A. B., Garritsen K. E. Making mobility hubs smarter: 10 recommendations for practitioners & policy makers. – 2024.

19. Godber A. What are the Motivators and Deterrents that Contribute to Women's Decision to Cycle as a Mode of Transportation: Exploring Gender Differences in Cycling Behaviour //Journal of Integrated Studies. – 2024. – Т. 15. – №. 1.

20. Goh Y. A study on smart parking system using IOT technology in shopping mall :дис. – UTAR, 2023.

21. Gyimah F. O. et al. Empowering Shared Mobility Vehicle Riders, Stopping Scams: A Cyber Kill Chain and Awareness Approach to QRishing on College Campuses //2024 Cyber Awareness and Research Symposium (CARS). – IEEE, 2024. – С. 1-7.

22. Habib N. et al. Smart parking for smart drivers using QR codes //Artificial Intelligence &Blockchain in Cyber Physical Systems. – CRC Press, 2023. – С. 22-47.

23. Hamiri M. H., Abu Mangshor N. N. Enhanced car park security through an Automatic Plate Number Recognition (APNR) system featuring QR code generation. – 2023.

24. Hendrawan A., Abdussalam F. Evaluation of user satisfaction on QRIS e-payment application at bank XYZ //International Research Journal of Economics and Management Studies IRJEMS. – Т. 3. – №. 1.

25. How C. C. et al. Smart parking reservation mobile application //2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). – IEEE, 2022. – С. 1-5.

26. HusnaZakaria M., Rohani M. D., Mohd M. F. On the road to sustainability: insights from Johor's free bus services //Journal of Sustainability Science and Management. – 2025. – Т. 20. – №. 1. – С. 23-40.

27. Irraivan E., Phang S. K., Gudipalli A. Automatic Number Plate Recognition and QR Code Double Authentication System for a Carpark //2023 Innovations in Power and Advanced Computing Technologies (i-PACT). – IEEE, 2023. – С. 1-6.

28. Kaim S. et al. From Cash to Clicks: The Impact of Touch'n Go on Student Financial Behaviors //Advances in Global Economics and Business Journal. – 2024. – Т. 5. – №. 2. – С. 107-121.

29. Kalaiselvi T. C. et al. Smart Car Parking System //2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE). – IEEE, 2024. – С. 1-8.

30. Karim R. The Electric Scooter: a sustainable form of urban micro-mobility transport? A Geographical Overview :дис. – The University of Bergen, 2024.

31. Krishnan R. S. et al. Machine Learning Based Efficient and Secured Car Parking System //Recent Advances in Internet of Things and Machine Learning: Real-World Applications. – Cham : Springer International Publishing, 2022. – С. 129-145.

32. Kumar A., Hussain J., Chun A. Wi-Fi //Connecting the Internet of Things: IoT Connectivity Standards and Solutions. – Berkeley, CA :Apress, 2023. – С. 145-213.

33. Kumar V. Secondary Data //International Marketing Research: A Transformative Approach. – Cham : Springer Nature Switzerland, 2024. – С. 135-160.

34. Lättman K., Olsson L. E., Friman M. Perceived accessibility: unveiling inequalities in transport justice //Sustainable Transport and Livability. – 2024. – Т. 1. – №. 1. – С. 2373050.

35. Marres N. et al. Infrastructural Participation in Digital Societies: Challenges and Alternatives //Science & Technology Studies. – 2025.

36. McKay T. J. M., Duri B., Gunter A. Navigating the challenges of public transport and urban mobility in Thohoyandou, South Africa //Journal of Transport and Supply Chain Management. – 2024. – Т. 18. – С. 1054.

37. Meloni I. et al. Mobility as a Service: Insights from pilot studies across different Italian settings //Transportation Engineering. – 2024. – Т. 18. – С. 100294.

38. Mock M., Wankat K. Why do sustainable shared mobility practices not proliferate more widely? Insights from digital mobility diaries //Journal of Cleaner Production. – 2024. – Т. 475. – С. 143582.

39. Muchtar E. H. et al. Quick response code Indonesia standard (QRIS) E-payment adoption: customers perspective //Cogent Business & Management. – 2024. – Т. 11. – №. 1.

40. Najib M. F. et al. Exploring Traditional Market Merchants' Payment Acceptance using QRIS in Indonesia //Proceeding of the International Conference Economic Management Accounting (ICEMA). – 2024. – Т. 2. – №. 1. – С. 1021-1036.

41. Nasr O. et al. Designing an intelligent QR code-based mobile application: A novel approach for vehicle identification and authentication //Indian Journal of Science and Technology. – 2023. – Т. 16. – №. 37. – С. 3139-3147.

42. Özkan R. T., Alpullu A., Ramos W. The Contribution of Applicable Smart and Sustainable Technologies in Recreation to City Happiness

//International Journal of Recreation and Sports Science. – 2024. – Т. 8. – №. 1. – С. 57-77.

43. Prabandari A., Pandawani N. P., Maba W. Effectiveness of Using Quick Response Code Indonesian Standard (QRIS) as a Parking Paying Tool (Case Study in Gianyar District) //Ajhssr. Com UniversitasMahasaraswati Denpasar. – 2023. – Т. 4. – С. 61-71.

44. Ramzan S. R. S. et al. Smart and Secure Vehicle Parking System to Avoid Theft Using Deep Image Recognition //Journal of Innovative Computing and Emerging Technologies. – 2024. – Т. 4. – №. 1.

45. Sharevski F. et al. Exploring Phishing Threats through QR Codes in Naturalistic Settings //Symposium on Usable Security and Privacy (USEC) 2024. – 2024. – Т. 208. – С. 1-25.

46. Song J. et al. The influence of gender driving stereotype threat on the driving performance of female drivers and its mechanism //Current Psychology. – 2024. – Т. 43. – №. 19. – С. 17213-17224.

47. Sousa A. E., Cardoso P., Dias F. The use of artificial intelligence systems in tourism and hospitality: the tourists' perspective //Administrative Sciences. – 2024. – Т. 14. – №. 8. – С. 165.

48. Still J. D., Morris T., Edwards M. Investigating University QR Code Interactions //International Conference on Human-Computer Interaction. – Cham : Springer Nature Switzerland, 2024. – С. 204-214.

49. Tang Z., Hao J., Wang X. Park smart or face the music: Understanding users' orderly parking behavior of dockless shared bikes from the perspective of deterrence theory //Transportation Research Part F: Traffic Psychology and Behaviour. – 2024. – Т. 107. – С. 507-520.

50. Thota M. K., Prathibhavani P. M., Venugopal K. R. Intelligence in Parking: QR based earmarking vehicle Stability in smart-city //2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT). – IEEE, 2024. – С. 1-5.

51. Uz V. E., Kesmez F. E. Micromobility Data Need and Data Use //Micromobility: Perspectives from Engineering, Urban Planning, Health Sciences and Social Sciences. – 2025. – С. 225-262.

52. Vales J. P. R. et al. Small-Medium Enterprises Owners' Preference for E-Wallet Payment in Transactions. – 2025.

53. Vineetha K. R., Sinu H. Design And Implementation of Secure Qr Payment Based on Visual Cryptography.

54. Wahyu S., Nasrullah N., Sahrullah S. The effect of ease and speed on interest in using the QRIS payment system on students majoring in management, faculty of economics and business, university of Muhammadiyah Makassar //International Journal of Economic Research and Financial Accounting. – 2024. – Т. 2. – №. 3.

55. Xu Q. et al. Payment behavior prediction on shared parking lots with TR-GCN //The VLDB Journal. – 2022. – С. 1-24.

56. Yu T. S., Islam S., Thong C. L. An Enhanced QR Code-Based Smart Parking System for Mobile Environment //Proceedings of International Conference on Computing and Communication Networks: ICCCN 2021. – Singapore : Springer Nature Singapore, 2022. – С. 59-75.

57. Zhang Y. et al. Can Relocation Influence Human Acceptance of Connected and Automated Vehicles? //Systems. – 2024. – Т. 12. – №. 8. – С. 296.

58. Zhu M. et al. Parking choice behaviour analysis of rural residents based on the latent variable random forest model //Transportation Safety and Environment. – 2024. – Т. 6. – №. 3. – С. tdad045.

59. Zulfiqar H. et al. A survey on smart parking systems in urban cities //Concurrency and Computation: Practice and Experience. – 2023. – Т. 35. – №. 15. – С. e6511.

60. Кемалов О. А. Блокчейн и Интернет вещей (IoT): Взаимодействие и перспективы интеграции //Инновации и инвестиции. – 2024. – №. 8. – С. 393-397.

61. Логинова И. А., Мальцев Н. В. Технология оплаты с помощью QR-кодов: правовое регулирование и экономическая безопасность // Оргкомитет конференции. – 2023. – С. 134.

62. Майдан С. Б. Рекламные исследования как разновидность маркетинговых исследований: понятие, роль, цель и задачи //Экономика и современный менеджмент: теория, методология, практика. – 2022. – С. 50-52.

63. Медяник О. В., Легостаева Н. И. Трансформация финансового поведения россиян в условиях цифровизации рынка финансовых услуг //Вестник Пермского национального исследовательского политехнического университета. Социально-экономические науки. – 2022. – №. 4. – С. 22-37.

64. Пашинина Н. И., Юхина Т. А. Особенности использования QR-кода в реалиях современной экономики // Качество продукции: контроль, управление, повышение, планирование. – 2022. – С. 159-163.

65. Пыхтин С. В. Оплата по QR-коду как способ безналичных расчетов //Вестник Университета имени ОЕ Кутафина. – 2023. – №. 1 (101). – С. 104-110.

66. Соснило А. И. Атлас искусственного интеллекта для бизнеса и власти //СПб.: Университет ИТМО. – 2022. – Т. 98.

67. Трощинский П. В. Цифровой Китай до и в период коронавируса: особенности нормативно-правового регулирования //Право и цифровая экономика. – 2021. – №. 1. – С. 44-58.

68. Фаткуллина Р. Р. Критерии оценки спроса в сервисе и цифровизация// Сервис в России и за рубежом. 2023. №3 (105). URL: https://cyberleninka.ru/article/n/kriterii-otsenki-sprosa-v-servise-i-tsifrovizatsiya (дата обращения: 03.05.2025).

69. Шарапова В. А., Новикова А. С. Privatebanking в практике российских банков // Финансовый университет при правительстве Российской федерации Алтайский филиал. – 2024. – С. 85.

70. Шувалова Н. А. Методические основы разработки финансовых моделей монетизации стартапов // Экономические системы. 2023. №2. URL: https://cyberleninka.ru/article/n/metodicheskie-osnovy-razrabotki-finansovyh-modeley-monetizatsii-startapov (дата обращения: 04.05.2025).