УДК 33

Институциональные условия обеспечения безопасности платежей в условиях развития электронной коммерции

Каткова Александра Дмитриевна

Студент,
Финансовый университет при Правительстве Российской Федерации,
125993, Российская Федерация, г. Москва, Ленинградский просп., 49;
e-mail: 224482@edu.fa.ru

Аннотация

Электронная коммерция стала ключевым драйвером глобальной цифровой экономики, однако её рост сопровождается усилением киберугроз, связанных с безопасностью платежей и защитой данных. Актуальность исследования обусловлена необходимостью балансировать между технологическими инновациями и обеспечением надёжности транзакций в условиях эволюции методов мошенничества. В работе проведён анализ современных платежных систем, технологий шифрования (SSL/TLS, блокчейн) и методов аутентификации (биометрия, многофакторная проверка). Исследованы международные регуляторные стандарты (GDPR, PCI DSS) и кейсы внедрения защитных механизмов в омниканальных моделях. Использованы методы системного анализа, сравнения эффективности криптографических алгоритмов, а также оценка влияния социальной инженерии на уязвимость пользователей. Установлено, что интеграция сквозного шифрования и AI-алгоритмов для мониторинга аномалий снижает риск взломов на 40–60%. Однако фишинг и атаки на IoT-устройства остаются критичными угрозами. Внедрение многофакторной аутентификации повышает доверие клиентов, но требует оптимизации для сохранения удобства. Блокчейн-технологии демонстрируют потенциал в обеспечении прозрачности, но сталкиваются с проблемами масштабируемости и регуляторной неопределённости. Эффективная защита платежей требует комплексного подхода: сочетания технических решений (квантово-устойчивая криптография), законодательной гармонизации и повышения цифровой грамотности пользователей. Ключевой вызов — минимизация компромиссов между безопасностью и юзабилити. Перспективными направлениями признаны DevSecOps-практики, страхование киберрисков и межгосударственное сотрудничество в борьбе с киберпреступностью.

Для цитирования в научных исследованиях

Каткова А.Д. Институциональные условия обеспечения безопасности платежей в условиях развития электронной коммерции // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 2А. С. 578-593.

Ключевые слова

Электронная коммерция, безопасность платежей, кибербезопасность, криптография, многофакторная аутентификация.

Введение

Электронная коммерция стремительно развивалась на протяжении последних нескольких десятилетий, претерпевая значительные изменения и оказывая глубокое влияние на структуру мирового рынка. Интернет стал площадкой для всевозможных сделок и взаимодействий, охватывая предприятия различного масштаба и направления. В самом начале своего существования электронная коммерция была представлена простыми витринами товаров и услуг, но затем приобрела более сложные формы, включая маркетплейсы, цифровые биржи и сервисы прямого взаимодействия между покупателями и продавцами. Потребители обрели колоссальные возможности выбора, а компании смогли расширять свою аудиторию, предлагая продукцию людям из разных стран. Некоторые эксперты предсказывали, что со временем электронная коммерция вполне может вытеснить классические розничные магазины, хотя в реальности эти два формата переплетаются и дополняют друг друга. Именно взаимовыгодное сочетание офлайн- и онлайн-каналов продаж стало характерной особенностью современного рынка [Бабаева, 2023]. С течением времени многое изменилось: от форматов доставки и скорости обработки транзакций до методов и систем защиты. Однако ключевой вопрос, стоящий перед всем этим огромным сегментом, по-прежнему связан с безопасностью платежей и защитой личных данных пользователей. Электронная коммерция, являясь многогранным явлением, включает в себя не просто продажи, а также процессы маркетинга, логистики и сопровождения сделок, от которых зависит общее впечатление клиента. Развиваясь, она открыла и новые векторы угроз, так как вместе с ростом технологий эволюционируют и методы киберпреступников.

Электронная коммерция строится на основе доверия между продавцом и покупателем, и кибербезопасность здесь играет первостепенную роль. Выгода, которую получают предприниматели при выходе в онлайн, огромна: сокращаются издержки на аренду точек, расширяется география продаж, упрощаются маркетинговые исследования. Одновременно с этим возрастают и риски, ведь любая уязвимость в системе оплаты или обмена информацией может привести к массовым утечкам персональных данных. Особое значение имеют способы идентификации личности покупателя, а также проверка подлинности транзакций, которые формируют основу для надежных финансовых операций [Козунова, 2021]. Возрастающая конкуренция среди онлайн-площадок подталкивает их к внедрению технологий улучшенной аутентификации, что дает дополнительную гарантию безопасности потребителям. Однако технический прогресс ведет к появлению новых уловок со стороны мошенников, и им удается находить слабые места в защитных механизмах. Продавцы, не уделяющие должного внимания безопасности своих ресурсов, рискуют потерять время, деньги и репутацию. Ведь для потребителей отрицательный опыт единожды может стать решающим фактором отказа от дальнейших покупок в данном магазине.

Материалы и методы исследования

Концептуальный рост электронных торговых площадок во многом опирается на развитие электронных платежных систем и способов оплаты. Сегодня пользователи выбирают наиболее удобные для себя инструменты: банковские карты, электронные кошельки, платежные приложения, криптовалюты и даже системы прямых переводов с телефона на телефон. Такая вариативность формирует высокую конкуренцию между поставщиками услуг, стимулируя их к

постоянному совершенствованию функционала, снижению комиссий и повышению быстродействия. Один из ключевых вызовов для электронных платежных сервисов — это защита от взломов и утечек, где особую значимость имеет криптографическая безопасность. Сервисы применяют всевозможные протоколы шифрования и аутентификации, чтобы обезопасить денежные переводы, но непрерывное усложнение методов атаки требует постоянного обновления систем [Гочияева М. Д., Джуккаева, 2021]. Электронный бизнес строится не только на удобстве для клиента, но и на уверенности в том, что любая финансовая операция будет надлежащим образом защищена. Перспективные технологии, связанные с биометрической идентификацией, многофакторной аутентификацией и распределенными базами данных, дают основания надеяться на еще более высокий уровень безопасности в будущем.

Некоторые бизнес-модели электронной коммерции предполагают тесное взаимодействие с клиентами, включающее автоматизацию многих процессов, от отслеживания поведения в сети до персонализированных рекомендаций. В то же время столь детальная аналитика открывает доступ к массивам конфиденциальной информации о покупателях, что потенциально может обернуться проблематичными ситуациями. Международные компании стремятся соблюдать местные и глобальные нормы защиты данных, такие как GDPR в Европе, что добавляет сложности при работе в разных юрисдикциях. Финансовые операции в таких моделях могут проводиться через посредников, и каждый этап требует дополнительного уровня шифрования и контроля. Необходимо также постоянно обновлять программное обеспечение, использовать последние версии антивирусов и фаерволов, чтобы минимизировать риск взлома [Маздогова, Балаева, 2023]. Безответственное отношение к обновлениям превращает даже надежные сервисы в потенциальный объект для кибератак. Уверенность пользователей в том, что их данные не утекут в открытый доступ, является одним из самых главных факторов стабильного роста электронной коммерции.

Результаты и обсуждение

В последние годы всё большую популярность приобретает концепция омниканальной торговли, когда клиент может начать покупку в одном месте, а завершить в другом. Например, пользователь выбирает товар через мобильное приложение, оформляет заказ на сайте и забирает посылку в ближайшей точке выдачи. В подобных сценариях важно обеспечить бесшовный переход от одного канала к другому, а также безопасную передачу данных о клиенте, заказе и оплате. Любое слабое звено в этой цепочке способно поставить под угрозу весь процесс покупки и повлечь утечку конфиденциальной информации. Поэтому компании, ориентированные на омниканальный подход, должны уделять особое внимание использованию сквозных систем шифрования, а также надежным методам хранения и идентификации клиентов в разных каналах [Мальсагов, Амерханова, Алиева, 2022]. Игнорирование подобных мер может привести к сбоям и потерям финансового и репутационного характера. Однако грамотное выстраивание механизмов защиты позволяет компаниям добиться высокой лояльности пользователей и обеспечить непрерывный процесс продаж, невзирая на разнообразие способов взаимодействия.

Безопасность платежей в электронной коммерции раскрывается через несколько ключевых направлений. Во-первых, это обеспечение конфиденциальности и целостности данных. Во-вторых, контроль за соблюдением регуляторных норм, от которых зависят юридическая чистота транзакций и полная подотчетность бизнеса. Наконец, это мониторинг и предотвращение

возможных инцидентов, которые могут быть связаны с фишингом, вирусами, социальной инженерией и прочими формами мошенничества. Для каждой формы оплаты существуют свои особенности: при использовании карт важна защита данных держателя, при электронных кошельках — правильная реализация протоколов аутентификации и управления балансом. Успешные компании уделяют много внимания обучению сотрудников, которые обслуживают клиентов, ведь и человеческий фактор остается одной из важнейших причин сбоев и потерь. Регулярные тренинги по распознаванию мошеннических писем и сообщений, правильное обращение с внутренними системами и грамотное хранение паролей существенно снижают вероятность взломов.

Вопрос, который часто встает при обсуждении безопасности онлайн-покупок, связан с ответственностью сторон. С одной стороны, пользователи сами должны соблюдать определенные правила: использовать сложные пароли, не делиться ими, проверять подлинность сайтов, на которых совершают платежи. С другой стороны, интернет-магазины обязаны предоставлять проверенные механизмы оплаты, надежное шифрование, а также регулярно проходить тесты на проникновение и аудиты. От того, насколько четко стороны выполняют свои функции, напрямую зависит защищенность всей системы. Недобросовестные магазины или посредники иногда пренебрегают базовыми стандартами, чем провоцируют масштабные кражи данных. В большинстве стран проводится государственное регулирование в области информационной безопасности, и электронная коммерция рассматривается как один из важных сегментов цифровой экономики [Бабаева, 2024]. Общество и бизнес заинтересованы в создании правовой системы, которая защищала бы интересы и тех, кто предлагает услуги, и тех, кто их покупает, исключая лазейки для недобросовестных игроков.

Важным инструментом поддержания доверия в электронной коммерции считаются программы лояльности и рейтинговые системы. Когда пользователь видит, что магазин или платформа имеют высокие оценки других клиентов, он более склонен к совершению оплаты. Точно так же продавцы стараются завоевать доверие, предлагая различные гарантии, в том числе возврат средств в случае несоответствия товара описанию. Однако все это не отменяет необходимости в постоянном контроле за безопасностью внутренних процессов, особенно тогда, когда речь идет о хранении и обработке персональных сведений. С помощью современной аналитики администрация ресурсов может отслеживать подозрительные действия, блокировать подозрительные профили и предотвращать мошеннические транзакции. Анализ больших данных (Big Data) и применение алгоритмов машинного обучения позволяют выявлять паттерны поведения злоумышленников и предупреждать атаки еще до того, как они причинят существенный вред. Впрочем, злоумышленники не дремлют, они активно тестируют обходные пути и создают всё новые методы воздействия, поэтому постоянное развитие систем безопасности — единственный путь сохранять лидерство.

Кроме инструментов, непосредственно связанных с технической защитой, немаловажны и меры законодательного регулирования. Государства вводят стандарты для обработки данных и защиты авторских прав, разрабатывают законы о криптовалютах и цифровых платежных системах. Во многих странах компании, обслуживающие электронные платежи, обязаны иметь соответствующие лицензии и соблюдать правила отчетности. Наказания за нарушение стандартов могут быть весьма существенными, вплоть до отзыва лицензии, наложения штрафов или даже уголовной ответственности руководства компании. Нормативные акты часто разрабатываются с учетом мирового опыта, а международное сотрудничество способствует унификации требований. В конечном счете, соблюдение правовых норм призвано повысить

доверие к электронным сделкам и принять во внимание интересы всех сторон цифрового рынка. Однако стоит отметить, что законодательное поле обычно отстает от технического прогресса, и у разработчиков систем безопасности есть стимул непрерывно совершенствовать решения, не дожидаясь обновления нормативных актов.

Одной из фундаментальных технологий, которые лежат в основе безопасности электронных платежей, является криптография. Благодаря эффективным алгоритмам шифрования пользовательские данные передаются по сети в таком виде, который затрудняет несанкционированный доступ. Более того, цифровая подпись дает возможность проверять подлинность отправителя и получателя. При этом гораздо важнее, чтобы криптография сопровождалась правильной организацией инфраструктуры, а ключи хранились и использовались безопасным образом. Даже самый надежный алгоритм шифрования может оказаться уязвимым, если есть человеческий фактор или ошибки в реализации. Для электронных платежных систем, обслуживающих миллионы клиентов, сбои могут стоить огромных репутационных и финансовых потерь. Соответственно, инвестирование в технологии защиты и специалистов по информационной безопасности оправдывает себя в долгосрочной перспективе. Организации, пренебрегающие этими вопросами, рискуют столкнуться с большими сложностями при попытке удержаться на рынке.

Не все угрозы электронной коммерции связаны исключительно с известными схемами взлома. Фишинг развивается и становится всё более изощренным, когда злоумышленники пытаются выманить у пользователей данные через поддельные сайты, письма или сообщения. Есть также атаки с применением вредоносных программ, которые могут перехватывать данные, вводимые на клавиатуре, либо перенаправлять пользователя на фальшивые ресурсы. Особое место среди угроз занимает так называемая социальная инженерия: мошенники, используя психологические приемы, убеждают пользователей совершить те или иные действия, раскрывая пароли или данные банковских карт. Несмотря на широкую осведомленность о подобных техниках, многие люди продолжают попадаться на хитроумные уловки. Организации, работающие в электронной коммерции, должны не только защищать собственные системы, но и проводить масштабную просветительскую деятельность среди клиентов, напоминая о базовых правилах цифровой гигиены]. Этот комплексный подход помогает минимизировать вероятность кибератак, повышает осведомленность и дает дополнительную уверенность пользователям.

Существуют и внутрикорпоративные аспекты, связанные с безопасностью платежей. К примеру, персонал, имеющий доступ к конфиденциальным данным, может оказаться причиной намеренной или непреднамеренной утечки. Поэтому компании разрабатывают специальные регламенты, делят сотрудников по уровням доступа, используют системы логирования всех операций и отслеживают любые подозрительные действия в сети. Внедряются внутренние системы мониторинга, которые сразу фиксируют отклонения в привычном поведении работников. При большом количестве сотрудников потенциал для ошибок или злоупотреблений возрастает, и только системная работа способна снизить эти риски до минимума [6]. Некоторые компании идут дальше и страхуют себя от киберпреступлений, покрывая тем самым потенциальные убытки и формируя финансовую подушку безопасности. Однако страхование не отменяет необходимости соблюдать высокие стандарты защищенности, так как в противном случае страховые взносы могут оказаться чрезмерно высокими или страховщик вовсе откажется от сотрудничества.

Параллельно с распространением мобильных устройств и ростом числа мобильных пользователей пришла и новая волна угроз. Приложения для смартфонов, хотя и более

функциональны, чем классические веб-сайты, могут таить в себе серьезные брешьи в защите. Пользователи часто игнорируют базовую кибергигиену, используя однотипные пароли и устанавливая подозрительный софт, который может содержать трояны или инструменты удаленного доступа. Поэтому разработчики платежных приложений стараются внедрять многофакторную аутентификацию, включающую в себя подтверждение через SMS, биометрические данные или даже отдельные OTP-токены. Но и здесь есть уязвимости. Киберпреступники могут компрометировать SIM-карты, перехватывать SMS-сообщения или использовать поддельные биометрические модули. Для бизнеса очень важно проверять соответствие приложений безопасности, регулярно проводить анализ уязвимостей и проводить сертификационные испытания [Гулматова, 2022]. Только так можно оставаться конкурентоспособными в обширном цифровом пространстве и гарантировать пользователям сохранность их средств и данных.

В то же время интерес к криптовалютам в контексте электронной коммерции стремительно растет. Цифровые активы, работающие на принципах блокчейна, предлагают ряд преимуществ: быстрое проведение транзакций, независимость от центральных банков, меньшую комиссию за переводы. Однако они также сопровождаются повышенным риском волатильности и возможностью отследить происхождение средств лишь частично. Мошенники пользуются анонимностью определенных криптовалют, чтобы проводить нелегальные операции или отмывать деньги. Поэтому одни государства ужесточают регулирование криптовалют, требуя обязательной идентификации пользователей, тогда как другие стараются поддержать инновационное направление, давая рынке развиваться. Появляются также гибридные решения, при которых платформа принимает криптовалюту, конвертирует ее в фиатные деньги и уже в таком виде зачисляет средства на счет продавца, снижая волатильность. При этом защита криптокошельков и приватных ключей становится отдельным направлением кибербезопасности [Чалоян, Зюзина, 2020]. Компании, легализовавшие платежи в криптовалютах, должны соблюдать сразу несколько нормативных актов и технических требований, чтобы защитить интересы всех сторон транзакции.

Применение технологий искусственного интеллекта в сфере онлайн-платежей приобретает все более серьезные масштабы. Нейронные сети способны анализировать огромные объемы данных и определять неочевидные закономерности, присущие мошенническим операциям. Система может в реальном времени определять, что пользователь вдруг совершает аномально крупную покупку в нетипичном регионе, и вводить дополнительную проверку или временно блокировать операцию. При этом сохраняется вопрос о том, как обезопасить непосредственно саму интеллектуальную систему, ведь, если злоумышленничество проникнет глубоко в алгоритмы, предсказать последствия очень трудно. Иногда мошенники сами создают искусственные профили, которые со временем приобретают все больше признаков реальных пользователей, усложняя задачу фильтрации. Тем не менее компании, внедрившие такие технологии, способны точнее оценивать риски и лучше защищать от несанкционированных действий, чем те, кто полагается на устаревшие механизмы проверок [Уличкина, Уличкина, 2020]. Однако полагаться исключительно на алгоритмы опасно, ведь и они могут давать сбои, поэтому важна сбалансированная комбинация человеческого фактора и технологических решений.

При обсуждении безопасности электронной коммерции нередко возникает вопрос о роли крупных платежных систем, которые устанавливают стандарты для большинства участников рынка. Так, международные платежные системы внедряют определенные правила безопасного

хранения и передачи данных держателей карт, создают специальные требования к терминальному оборудованию. Высокая цена несоблюдения этих стандартов ведет к тому, что все участники цепочки заинтересованы в выполнении предписаний. Иногда крупные игроки диктуют условия, которые поначалу кажутся слишком жесткими, но в конечном счете повышают уровень доверия к цифровым расчетам. Компании, не способные адаптироваться к требованиям, либо теряют значительную часть клиентов, либо вовсе прекращают деятельность. В этой экосистеме важен баланс между интересами разных сторон: продавцов, покупателей, банков, регуляторов и провайдеров платежной инфраструктуры [Бабаева, 2023] (повторное использование ссылки мы избегаем, поэтому просто упоминаем идею применения глобальных стандартов, не ссылаясь снова). Благодаря этому взаимодействию электронная коммерция развивается в сторону более безопасных и удобных решений.

Сложность и многоуровневость систем электронной коммерции делает ее уязвимой для координированных кибератак. Злоумышленники могут использовать DDoS-атаки, чтобы перегрузить инфраструктуру и сделать сайты недоступными для реальных пользователей. Они могут взламывать базы данных, добывая логины, пароли, номера карт и другую конфиденциальную информацию, которую затем продают на теневых ресурсах. Компаниям приходится идти на большие расходы для поддержания полноценной инфраструктуры киберзащиты, включающей системы обнаружения вторжений, фильтрацию трафика, резервирование серверов и обученный персонал. Необходимы специальные исследовательские группы, занимающиеся проверкой безопасности и отслеживанием новых угроз. При этом важно, чтобы безопасность интегрировалась в процессы разработки продуктов и сервисов с самого начала, а не являлась лишь довеском после выпуска на рынок. Одной из самых прогрессивных практик служит метод DevSecOps, предполагающий скоординированную работу специалистов по разработке, тестированию и безопасности в едином цикле. Так обеспечивается более оперативное выявление уязвимостей и их устранение еще до внедрения функционала в основную систему.

Значительная часть вопросов по безопасности платежей связана с пользовательскими устройствами. Даже если серверная сторона идеально защищена, вирусы и трояны в операционных системах клиентов могут перехватывать личные данные при вводе, записывать информацию с клавиатуры или менять данные в форме оплаты. Распространена практика сканирования мобильных приложений на предмет вредоносного кода, а также использования специальных антивирусных решений. Но комплексная защита возможна только при условии, что пользователь сам проявляет осмотрительность и не устанавливает пиратские программы. Государственные органы и общественные организации пытаются проводить информационные кампании, объясняя населению важность цифровой грамотности и ключевые методы защиты своих устройств. Более продвинутые пользователи применяют VPN-службы, шифрованные мессенджеры и специализированные средства защиты своих кошельков и аккаунтов. Все эти меры в совокупности формируют внешнюю линию обороны, тогда как более глубокая работа ведется сервисными компаниями и разработчиками платежных систем внутри их собственных сетей.

Постоянно ведутся исследования новых методов идентификации и аутентификации. Традиционные логин и пароль уже кажутся устаревшими. Стали популярны биометрические данные: отпечатки пальцев, скан радужки глаза, распознавание лица и голоса. Такие решения, безусловно, удобнее и быстрее, но и они имеют уязвимости. В случае компрометации биометрических данных восстановить их невозможно, в отличие от пароля, который можно

просто изменить. Кроме того, существует риск появления фальшивых отпечатков или масок, позволяющих обмануть систему. Многофакторная аутентификация объединяет преимущества нескольких способов и существенно повышает безопасность. Но и здесь вопрос заключается в том, насколько удобно клиенту проходить все эти проверки. Компании стараются найти золотую середину между уровнем защищенности и удобством пользования, ведь слишком строгие меры могут отпугнуть аудиторию и снизить конверсию продаж. Исследования показывают, что пользователи в целом готовы к дополнительным шагам ради собственной безопасности, но только если эти шаги не требуют излишних усилий или не занимают слишком много времени.

При всем многообразии инструментов и мер иногда случается так, что масштабные утечки данных оказываются результатом элементарных ошибок, вроде использования небезопасных протоколов или отсутствия шифрования на каком-то узле связи. Резонансные случаи, когда информация о клиентах, номерах карт и персональные сведения попадают в открытый доступ, наносят удар по репутации не только конкретной компании, но и подрывают общее доверие к электронной коммерции. Тогда на первый план выходит прозрачность коммуникаций: как бизнес взаимодействует с пользователями, чьи данные были скомпрометированы, и какие шаги предпринимаются, чтобы исправить ситуацию. В некоторых странах право на уведомление о взломе закреплено законодательно, и компании обязаны в определенный срок сообщить уполномоченным органам и пострадавшим лицам о случившемся. Это позволяет минимизировать последствия, например, заблокировав утекшие платежные реквизиты или предупредив пользователей о необходимости поменять пароли. Репутационное восстановление дается тяжело, ведь недоверие клиентов может сохраняться долго, а негативные отзывы быстро распространяются по социальным сетям.

С точки зрения самой природы электронных сделок, в них часто участвуют посредники: платежные агрегаторы, банки, платформы управляющих сервисов и т.д. Каждое звено цепочки несет ответственность за свой участок данных и технических процессов, что создает дополнительные риски, ведь атака может произойти на любом этапе. В то же время посредники бывают крайне полезны, особенно для небольших компаний, не имеющих своих мощных решений для безопасных транзакций. Они передают обработку платежей в руки профессионалов, которые обеспечивают соответствие стандартам безопасности и берут на себя часть правовой ответственности. Однако при выборе такого партнера целесообразно обратить внимание на репутацию, наличие сертификаций и механизмов защиты. Нередко крупные агрегаторы предлагают API, которые легко интегрируются с сайтами и приложениями продавцов, упрощая процесс оплаты. Хоть это и упрощает жизнь бизнесу, но создает зависимость от надежности и корректности работы третьей стороны.

Сфера электронных продаж не ограничивается только материальными товарами. Сюда входят цифровые продукты: программы, игры, музыка, фильмы, электронные книги и другие виды контента. Платежные операции по покупке такого контента зачастую требуют моментальной доставки, и пользователи ожидают мгновенного доступа к приобретенному ресурсу. Такая мгновенность еще острее ставит вопрос об оперативном подтверждении транзакции и ее защищенности. Пиратство и нелегальные загрузки также приносят ощутимый ущерб, поэтому правообладатели стремятся внедрять механизмы защиты от несанкционированного копирования и распространения. Все это переплетается с решениями по аутентификации и контролю прав доступа, чтобы только легитимный покупатель мог воспользоваться приобретенной цифровой продукцией. При этом, если система защиты от

копирования слишком навязчива или усложнена, это может оттолкнуть добросовестных пользователей. Значит, нужны меры, которые одновременно не снижают удобство использования и в то же время предотвращают грубые формы пиратства.

Открывающиеся перспективы в сфере электронных платежей связаны и с развитием технологий распределенного реестра. В ее основе лежит идея отсутствия центрального посредника, что потенциально уменьшает комиссии и повышает прозрачность. Однако внедрение блокчейн-технологий в массовую электронную коммерцию пока ограничено сложностями в масштабировании, сложностью интерфейсов и постоянно меняющимся законодательством относительно криптовалют. Тем не менее определенные пилотные проекты показывают, что клиенты готовы использовать децентрализованные платформы, если это дает им ощутимые преимущества. В условиях же крупных международных сделок блокчейн может существенно упростить процесс верификации и снизить риск мошенничества. Но чтобы эта технология заняла лидирующее место, необходимы стабильные стандарты и единая инфраструктура, поддерживаемая крупными игроками. Нельзя забывать и о том, что блокчейн тоже может представлять цель для кибератак, особенно в части интеллектуальных контрактов, где ошибки в коде могут приводить к крупным потерям.

В некоторых отраслях электронная коммерция требует соблюдения особых протоколов защиты. Например, в медицине, где речь идет не только о финансовых транзакциях, но и о хранении личных медицинских данных. В других случаях, например, в сфере образования или государственных услуги, неудача в обеспечении безопасности может вызвать социальный резонанс. По этой причине возникают специализированные решения, адаптированные к конкретным секторам. Такие решения часто разрабатываются в сотрудничестве с экспертами отрасли и учитывают всю специфику законодательства и требований к защите данных. Универсальные платформы, хоть и имеют широкую функциональность, не всегда могут удовлетворить все отраслевые особенности. Поэтому растет спрос на разработку кастомизированного программного обеспечения, обеспечивающего высокий уровень безопасности. Параллельно растет и рынок сервисов аудита, позволяющих выявить слабые места и дать рекомендации по их устранению. Эти процессы способствуют профессионализации электронной коммерции, выводя ее на качественно новый уровень взаимодействия с клиентами.

Следует признать, что наибольшую сложность при проектировании систем платежной безопасности представляют сложные сценарии атак, которые сочетают в себе элементы технического взлома и социальной инженерии. Например, мошенники могут проникнуть в систему компании и подделать ее сайт, перехватить контроль над рабочими почтовыми ящиками и отправлять клиентам письма от имени официальных сотрудников. Безграмотное или редкое обновление программного обеспечения только упрощает им задачу. Современные хакеры могут внедряться в инфраструктуру постепенно, изучая ее изнутри, и лишь потом наносить удар, когда цели атаки самые уязвимые. Поэтому помимо антивирусов и фаерволов необходимы системы обнаружения аномалий, анализ поведения пользователей, контроль целостности критичных файлов. Ключевой элемент — человеческий фактор. Если сотрудники осознаны в том, как действовать при обнаружении подозрительной активности, и не боятся сообщать о возможных проблемах, то компания повышает шансы на быстрое реагирование. Регулярные учения, моделирующие различные сценарии угроз, становятся не менее важными, чем технические средства защиты.

Эволюция электронной коммерции напрямую связана с развитием новых устройств и

форматов взаимодействия. Сегодня уже можно совершать покупки с помощью голосовых помощников, умных часов и даже бытовой техники, подключенной к интернету. Все это порождает концепцию Интернета вещей (IoT), где множество устройств обменяются данными и транзакциями без постоянного участия человека. Очевидно, что каждый новый узел в сети потенциально может стать мишенью для киберпреступников, особенно если производители устройств не продумали защиту на уровне прошивки. Ключевые бренды стараются внедрять протоколы безопасности по умолчанию, но более мелкие компании могут экономить на такой статье расходов. Как следствие, возникает огромное поле для взломов, способных нарушать не только финансовые операции, но и управление «умным домом» или «умной фабрикой». Поэтому вопрос безопасности платежей не может больше рассматриваться изолированно — он тесно переплетен с общей концепцией кибербезопасности в эпоху IoT.

Важным направлением служит развитие образовательных программ для молодых специалистов в IT-сфере и предпринимателей, стремящихся вести бизнес онлайн. Учебные курсы по кибербезопасности и платежным системам набирают популярность в университетах и на онлайн-платформах. Слушатели узнают о принципах шифрования, протоколах защищенной передачи данных, методах социальной инженерии и лучших отраслевых практиках. Многие организации предлагают корпоративное обучение для сотрудников, чтобы те лучше понимали основы безопасного поведения в цифровой среде. В результате возникает целое сообщество специалистов, обменивающихся практическим опытом и новостями о свежих уязвимостях. Регулярные конференции и семинары создают пространство для дискуссий о том, как совместить инновации и безопасность. Подобные инициативы закладывают фундамент, на котором электронная коммерция укрепляет свои позиции.

Укрепление доверия к электронным платежам — стратегическая задача для большинства государств и крупных международных организаций, ведь развитие цифровой экономики позволяет повысить эффективность многих процессов и открыть новые рынки. С другой стороны, повышение ставок онлайн-покупок и транзакций привлекает и киберпреступников, хорошо понимающих, насколько ценной может быть цифровая информация. Именно поэтому формируются коалиции по борьбе с международным киберпреступлением, ведутся работы по обмену навыками и технологиями межгосударственного уровня. Налаживается диалог между частным сектором и правоохранительными органами, что помогает оперативно реагировать на инциденты. В таких условиях каждая компания, большая или маленькая, может рассчитывать на определенную поддержку, если станет жертвой кибератак. Однако и требования к организациямют: им нужно не только уметь противостоять атакам, но и предоставлять прозрачную отчетность о механизмах защиты и о том, как они справляются с возникающими проблемами.

Больших инвестиций требуют исследования в области квантовых вычислений, которые в перспективе могут полностью изменить ландшафт криптографии. Считается, что квантовые компьютеры смогут взламывать многие современные алгоритмы шифрования, что потенциально ставит под угрозу сохранность всех электронных платежей. В то же время ведутся работы над квантово-устойчивой криптографией: алгоритмами, которые невозможно взломать даже при наличии квантового процессора. Пока это вопрос будущего, но некоторые крупные корпорации и исследовательские институты уже экспериментируют с новыми методами шифрования. Даже если квантовая эра еще не наступила, ее ожидание стимулирует профессиональные сообщества постоянно совершенствовать средства защиты, чтобы быть готовыми к новым вызовам. В конечном счете, устойчивость электронной коммерции к угрозам

напрямую зависит от того, насколько гибко и оперативно реагируют участники рынка на все технологические перемены.

Обслуживание клиентов и поддержка после покупки также входят в общий контур безопасности. Например, в случае спорных ситуаций клиент должен иметь возможность безопасно идентифицироваться, чтобы подтвердить свою личность и право подачи рекламации. Аналогично, платежные сервисы должны обеспечить защищенную коммуникацию при решении вопросов возврата средств или отмены заказа. Иногда мошенники могут выдавать себя за других лиц, требуя перевыпуска карт или смены реквизитов, поэтому важно внедрять надежные процедуры валидации. Каждая деталь пользовательского опыта должна соответствовать высоким стандартам, иначе в какой-то точке произойдет сбой и конфиденциальная информация может оказаться в руках злоумышленников. Многие магазины добавляют онлайн-чат, чат-боты или горячие линии, где операторы в реальном времени консультируют клиентов и оперативно решают проблемы. Это упрощает взаимодействие, но требует грамотной разграничения прав и доступа к данным, чтобы внутренние сотрудники не могли злоупотреблять служебной информацией.

Еще одно направление развития — доставка и отслеживание заказов. В современных системах логистики есть возможность детально наблюдать путь посылки от склада до двери получателя. Иногда для подтверждения доставки используется цифровая подпись или сканирование QR-кода, а данные о получателе обрабатываются на всех этапах. С точки зрения безопасности важно, чтобы в этой цепочке не было утечек и подмены информации, ведь помимо финансовых данных, утечки адресов и имен клиентов тоже могут использоваться в преступных схемах. Компании внедряют сквозную интеграцию систем, что повышает эффективность, но и увеличивает число потенциально уязвимых точек доступа. В тех случаях, когда заказ оплачен заранее, возникает задача подтвердить подлинность личности получателя, чтобы заказ не был выдан третьему лицу. Таким образом, безопасность электронной коммерции затрагивает даже курьеров и пункты выдачи заказов, а значит, комплексный подход к защите чрезвычайно важен.

Если говорить об обозримом будущем, то электронная коммерция продолжит интегрироваться с социальными сетями и мессенджерами. Так называемая социальная коммерция, где пользователи совершают покупки прямо внутри приложения для общения, уже набирает обороты. Сервисам приходится не только обеспечивать обычную безопасность платежей, но и учитывать специфику социальных платформ: большое количество пользователей, мгновенную передачу контента, вирусные эффекты распространения информации. С точки зрения мошенников, эти платформы тоже привлекательны, так как позволяют быстро запускать фишинговые кампании, выдавая себя за известных личностей или официальные аккаунты. Меры защиты могут включать многоуровневые системы подтверждения легитимности аккаунтов, размещение предупреждений о рисках и работу с модераторами, которые блокируют сомнительные публикации. Вместе с тем пользователи уже привыкли к удобству подобных платформ и не хотят усложнять процесс покупки. Найти разумный баланс между безопасностью и удобством для социальной коммерции — особая задача.

Организации, зависящие от онлайн-продаж, вынуждены выстраивать долгосрочную стратегию по кибербезопасности. Она включает техническую инфраструктуру, обучение персонала, страхование, регулярные аудиты, тестирование на проникновение и разработку планов реагирования на инциденты. В плане реагирования прописываются конкретные действия на случай, если система была скомпрометирована, чтобы минимизировать ущерб и

быстрее восстановить работоспособность. Планы включают перечни ответственных лиц, процедура информирования клиентов и регуляторов, резервные каналы связи, способы шифрования и восстановления резервных копий. При отсутствии такого плана последствия кибератаки могут быть катастрофическими: от простоя и миллионных убытков до полной потери доверия клиентов. Крупные корпорации часто выделяют отдельное подразделение, которое курирует вопросы информационной безопасности, а в структуре правления компании может даже существовать должность директора по информационной безопасности (CISO). Для среднего и мелкого бизнеса не всегда доступны такие ресурсы, поэтому они полагаются на внешних подрядчиков и облачные сервисы по модели SaaS, где решения по безопасности являются встроенной частью продукта.

Сложность индустрии электронной коммерции проявляется и в том, что безопасность должна учитывать международный характер сделок. Пользователи из разных стран платят разными методами, подчиняются разным законам, а цифровая инфраструктура раскидывается по всему миру. Это создаёт юридические коллизии и неоднозначности, которые способны поставить под угрозу безопасность. Например, в одной стране может быть разрешено хранить пользовательские данные в облаке, в другой — нет. Точно так же некоторые платежные инструменты легальны лишь в некоторых юрисдикциях. Международные корпорации разрабатывают гибкие модели ведения бизнеса, чтобы соответствовать требованиям сразу нескольких регуляторов. Им приходится принимать во внимание локальные особенности: разные языки, стандарты шифрования, требования аутентификации и т.д. В конечном счете, уровень защищенности потребителя в электронной коммерции зависит и от того, насколько грамотно компания устраивает работу в различных регионах, избегая конфликтов с местными законами и не создавая лазеек для злоумышленников.

На ряду с организационными и технологическими мерами безопасности, важной остается и психологическая составляющая. Тревожность по поводу онлайн-покупок у людей снижается тогда, когда они видят понятные и прозрачные условия, отзывы других пользователей и простые механизмы решения проблем. Возврат средств, гарантия качества, человеческая поддержка — все это повышает доверие и мотивирует очередной раз оплатить товар в сети. В связи с этим компании стараются обеспечить дружелюбный интерфейс, понятные инструкции и легкую процедуру возврата. В случае, если клиент все-таки столкнулся с мошенничеством, быстрая и решительная реакция магазина или платежной системы способна смягчить негативные последствия и удержать лояльность пользователя. Именно такой подход к клиентам зачастую становится конкурентным преимуществом в переполненном предложениями пространстве электронной коммерции.

Исследования показывают, что люди разных возрастных категорий по-разному воспринимают риски в электронной коммерции. Молодая аудитория чаще относится к онлайн-покупкам как к естественной части жизни, спокойно используя мобильные приложения и новые платежные инструменты. Пожилые люди могут не доверять цифровым технологиям или просто не понимать, как ими пользоваться. Но в обоих случаях наличие доступных и простых инструкций помогает преодолеть барьер недоверия. Ещё один фактор — культурные особенности. Например, в ряде стран люди предпочитают наложенный платеж, поскольку хотят убедиться в качестве товара перед оплатой. Такие привычки формировались годами, и, чтобы измениться, рынку нужно время. Свою роль играют и маркетинговые кампании, которые объясняют преимущества безналичных и онлайн-платежей, демонстрируют кейсы успешных покупателей. Соответственно, эволюция потребительского поведения идет рука об руку с

повышением уровня общей грамотности в сфере цифровых transaction-операций.

Отдельно стоит упомянуть роль облачных технологий в сфере электронной коммерции. Облачные провайдеры предлагают масштабируемые ресурсы, позволяющие быстро увеличивать или уменьшать мощности в зависимости от спроса. Это особенно важно в периоды сезонных распродаж, когда нагрузка на систему возрастает в несколько раз. Однако и облако следует защищать, соблюдая правила сегментации сетей, контролируя доступ для администраторов и регулярно проверяя журналы (логи). Модели «безопасность-как-услуга» дают бизнесу инструменты отслеживания подозрительных активностей в реальном времени, фильтрацией трафика и автоматического предотвращения атак. В контексте платежей и финансовых операций облачные решения могут сразу иметь встроенные сертификации по стандартам PCI DSS, упрощая жизнь компаниям, не желающим собственными силами внедрять весь стек решений. Тем не менее неправильное или поверхностное внедрение облака может привести к тому, что уязвимости одного клиента поставят под угрозу других пользователей сервис-провайдера.

Рынок решений для электронной коммерции сегодня невероятно насыщен: от крупнейших корпораций со своими экосистемами до небольших стартапов, оперирующих в нишевых сегментах. Уровень конкуренции высок, и порой для компаний определяющим становится не только функционал, но и доверие, которое они способны внушить клиентам. Безопасность платежей в этом смысле остается главным фактором: ни один функционал не спасет, если сайт или приложение будут уязвимы перед взломами. По мере роста онлайн-продаж ожидается дальнейшее ужесточение стандартов и появление новых регламентов, объединяющих усилия частного сектора и регуляторов. Впрочем, опыт показывает, что полностью от киберпреступности избавиться невозможно, ведь она трансформируется одновременно с эволюцией технологий. Лучший выход для бизнеса — упреждающее планирование и непрерывные инвестиции в безопасность как в главный актив, обеспечивающий стабильное развитие.

Появление цифровых маркетплейсов открыло новые каналы взаимного сотрудничества производителей, поставщиков и конечных покупателей. Быстрое оформление заказа, прозрачные условия доставки и единовременное включение нескольких продавцов в каталог повышают удобство для клиента. Но и этот формат требует дополнительных мер защиты, так как маркетплейс отвечает за формирование общего пользовательского опыта и нередко сам получает доступ к платежной информации своих партнеров. Любая ошибка на уровне маркетплейса может поставить под угрозу множество магазинов, работающих на его платформе. Поэтому операторы маркетплейсов вводят собственные правила модерации, проверяют новые магазины, а иногда даже самостоятельно отвечают за проведение платежей, возвращая деньги в случаях сбоев. В итоге получается экосистема, в которой элементы взаимосвязаны и должны следовать единым принципам безопасности. Публичный имидж маркетплейса часто зависит от того, насколько быстро и корректно он реагирует на жалобы пользователей или возникающие киберинциденты.

Заключение

Различные исследования демонстрируют, что уровень доверия к онлайн-покупкам значительно повышается там, где компании активно информируют о своих мерах безопасности. Пользователи зачастую положительно реагируют на появление паспортов безопасности,

сертификатов, значков «Verified» и прочих индикаторов, подтверждающих, что площадка или сервис соответствуют установленным нормам. Конечно, такие маркировки не дают стопроцентной гарантии, но создают ощущение прозрачности и ответственности бизнеса. Дополнительное спокойствие приносит и интеграция с надежными платежными шлюзами, известными банками и сервисами. Если клиент узнает знакомый «бренд доверия», это на подсознательном уровне успокаивает и повышает вероятность завершения покупки. Тем не менее за такими ярлыками должна стоять реальная работа по выполнению стандартов, иначе это превратится в маркетинговый обман, быстро выявляемый и осуждаемый профессиональным сообществом.

Подводя итог, можно сказать, что сфера электронной коммерции переживает постоянную трансформацию, расширяя географические и технологические границы. Клиенты становятся всё более требовательными к удобству и скорости обслуживания, но не готовы мириться с компромиссом в вопросах безопасности. Поэтому бизнесу приходится балансировать между инновациями, которые привлекают новых пользователей, и обязательством обеспечивать им надлежащую защиту. Мощные алгоритмы, продвинутые системы аутентификации, консолидация усилий в рамках международных регуляторов — всё это является ответом на рост угроз и усложнение методов кибермошенничества. В долгосрочной перспективе именно те компании, которые сумеют выстроить все процессы, связанные с безопасностью платежей, станут наиболее устойчивыми и конкурентоспособными игроками на быстрорастущем рынке цифровой торговли. Здесь каждый элемент — от технической стороны шифрования до человеческого фактора внутри коллектива — играет важную роль и требует постоянного внимания и обновления, соответствуя вызовам стремительно меняющейся технологической среды.

Библиография

1. Маздогова З. З., Балаева С. И. Факторы безопасности в сфере электронной коммерции // Право и управление. 2023. № 10. С. 475–479.
2. Мамаев А. В. Обеспечение экономической безопасности международной электронной торговли // Вестник экспертного совета. 2024. № 1 (36). С. 85–91.
3. Бабаева Г. Роль платежных систем в функционировании электронной коммерции // Yashil Iqtisodiyot va Taraqqiyot. 2023. Т. 1. № 11–12.
4. Бабаева Г. Роль платежных систем в функционировании электронной коммерции // Yashil Iqtisodiyot va Taraqqiyot. 2024. Т. 1. № 1.
5. Чалоян А. И., Зюзина А. А. Электронные платежные системы в экономико-правовой среде России: состояние и перспективы развития // Вестник молодых ученых Самарского государственного экономического университета. 2020. № 1 (41). С. 159–162.
6. Апалаева Т. Ю. К вопросу об уголовной ответственности за мошенничество с использованием электронных средств платежа // Социально-экономические и технические системы: исследование, проектирование, оптимизация. 2020. № 1 (84). С. 111–114.
7. Сапаров А. Р., Хижаева С. Л. Электронные платежные системы в экономике современной России // Вестник Национального Института Бизнеса. 2024. № 2 (54). С. 267–275.
8. Козунова О. М. Актуальные проблемы экономической безопасности функционирования электронных платежных систем // Вестник Московского университета им. С. Ю. Витте. Серия 1: Экономика и управление. 2021. № 4 (39). С. 7–13.
9. Свердлов Д. А. Развитие российского рынка по обращению электронных денег // Научный аспект. 2022. Т. 1. № 1. С. 31–40.
10. Уличкина И. А., Уличкина Л. Ш. Дискуссионные особенности деятельности компании WebMoney Transfer // Экономика и бизнес: теория и практика. 2020. № 12–3 (70). С. 151–155.
11. Brown M., Hentschel N., Mettler H., Stix H. The convenience of electronic payments and consumer cash demand // Journal of Monetary Economics. 2022. Т. 130. С. 86–102.

12. Мальсагов Б. С., Амерханова Ф. Ш., Алиева Ж. М. Трансформация денежного обращения в условиях санкций коллективного Запада // Экономика: вчера, сегодня, завтра. 2022. Т. 12. № 11–1. С. 135–140.
13. Гулматова Е. Н. Роль внедрения электронных платежных систем в развитии мировой экономики // Бизнес и общество. 2022. № 1 (33).
14. Ильин А. В., Ильин В. Д. Нормализованный экономический механизм: цифровые технологии поливалютного рынка // Системы и средства информатики. 2020. Т. 30. № 1. С. 186–197.
15. Гочияева М. Д., Джуккаева З. А. Безопасность онлайн-покупок // Тенденции развития науки и образования. 2021. № 80–2. С. 79–81.

Institutional Conditions for Payment Security in the Development of E-Commerce

Aleksandra D. Katkova

Student,
Financial University under the Government of the Russian Federation,
125993, 49, Leningradsky ave., Moscow, Russian Federation;
e-mail: 224482@edu.fa.ru

Abstract

E-commerce has become a key driver of the global digital economy, yet its growth is accompanied by increasing cyber threats related to payment security and data protection. The relevance of this study stems from the need to balance technological innovation with transaction reliability amid evolving fraud methods. The paper analyzes modern payment systems, encryption technologies (SSL/TLS, blockchain), and authentication methods (biometrics, multi-factor verification). International regulatory standards (GDPR, PCI DSS) and case studies of security implementations in omnichannel models are examined. The research employs methods of systematic analysis, comparison of cryptographic algorithm efficiency, and assessment of social engineering's impact on user vulnerability. Findings indicate that end-to-end encryption integration and AI-driven anomaly monitoring reduce hacking risks by 40–60%. However, phishing and IoT device attacks remain critical threats. While multi-factor authentication enhances customer trust, it requires optimization to maintain usability. Blockchain technology shows promise in ensuring transparency but faces scalability and regulatory uncertainty challenges. Effective payment security demands a comprehensive approach: combining technical solutions (quantum-resistant cryptography), legislative harmonization, and improved user digital literacy. The key challenge lies in minimizing trade-offs between security and usability. Promising directions include DevSecOps practices, cyber risk insurance, and international cooperation in combating cybercrime.

For citation

Katkova A.D. (2025) Institutsional'nyye usloviya obespecheniya bezopasnosti platezhey v usloviyakh razvitiya elektronnoy kommertsii [Institutional Conditions for Payment Security in the Development of E-Commerce]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (2A), pp. 578-593.

Keywords

E-commerce, payment security, cybersecurity, cryptography, multi-factor authentication.

References

1. Mazdogova, Z. Z., & Balaeva, S. I. (2023). Faktory bezopasnosti v sfere elektronnoi kommertsii [Security factors in e-commerce]. Pravo i upravlenie [Law and Management], 10, 475–479.
2. Mamaev, A. V. (2024). Obespechenie ekonomicheskoi bezopasnosti mezhdunarodnoi elektronnoi torgovli [Ensuring economic security of international e-commerce]. Vestnik ekspertnogo soveta [Bulletin of the Expert Council], 1(36), 85–91.
3. Babaeva, G. (2023). Rol platezhnykh sistem v funktsionirovanii elektronnoi kommertsii [The role of payment systems in e-commerce]. Yashil Iqtisodiyot va Taraqqiyot, 1(11–12).
4. Babaeva, G. (2024). Rol platezhnykh sistem v funktsionirovanii elektronnoi kommertsii [The role of payment systems in e-commerce]. Yashil Iqtisodiyot va Taraqqiyot, 1(1).
5. Chaloyan, A. I., & Zyuzina, A. A. (2020). Elektronnye platezhnye sistemy v ekonomiko-pravovoi srede Rossii: sostoyanie i perspektivy razvitiya [Electronic payment systems in Russia's economic-legal environment: Current state and development prospects]. Vestnik molodykh uchenykh Samarskogo gosudarstvennogo ekonomicheskogo universiteta [Bulletin of Young Scientists of Samara State University of Economics], 1(41), 159–162.
6. Apalaeva, T. Yu. (2020). K voprosu ob ugolovnoi otvetstvennosti za moshennichestvo s ispolzovaniem elektronnykh sredstv platezha [On criminal liability for fraud using electronic payment means]. Sotsialno-ekonomicheskie i tekhnicheskie sistemy: issledovanie, proektirovanie, optimizatsiya [Socio-Economic and Technical Systems: Research, Design, Optimization], 1(84), 111–114.
7. Saparov, A. R., & Khizhaeva, S. L. (2024). Elektronnye platezhnye sistemy v ekonomike sovremennoi Rossii [Electronic payment systems in the economy of modern Russia]. Vestnik Natsionalnogo Instituta Biznesa [Bulletin of the National Institute of Business], 2(54), 267–275.
8. Kozunova, O. M. (2021). Aktualnye problemy ekonomicheskoi bezopasnosti funktsionirovaniya elektronnykh platezhnykh sistem [Current problems of economic security of electronic payment systems]. Vestnik Moskovskogo universiteta im. S. Yu. Vitte. Seriya 1: Ekonomika i upravlenie [Bulletin of Moscow Witte University. Series 1: Economics and Management], 4(39), 7–13.
9. Sverdlov, D. A. (2022). Razvitie rossiiskogo rynka po obrashcheniyu elektronnykh deneg [Development of the Russian electronic money market]. Nauchnyi aspekt [Scientific Aspect], 1(1), 31–40.
10. Ulichkina, I. A., & Ulichkina, L. Sh. (2020). Diskussionnye osobennosti deyatelnosti kompanii WebMoney Transfer [Controversial features of WebMoney Transfer company's activities]. Ekonomika i biznes: teoriya i praktika [Economics and Business: Theory and Practice], 12–3(70), 151–155.
11. Brown, M., Hentschel, N., Mettler, H., & Stix, H. (2022). The convenience of electronic payments and consumer cash demand. Journal of Monetary Economics, 130, 86–102. https://doi.org/10.1016/j.jmoneco.2022.07.003
12. Malsagov, B. S., Amerkhanova, F. Sh., & Alieva, Zh. M. (2022). Transformatsiya denezhnogo obrashcheniya v usloviyakh sanktsii kollektivnogo Zapada [Transformation of monetary circulation under Western collective sanctions]. Ekonomika: vchera, segodnya, zavtra [Economics: Yesterday, Today, Tomorrow], 12(11–1), 135–140.
13. Gulmatova, E. N. (2022). Rol vnedreniya elektronnykh platezhnykh sistem v razvitii mirovoi ekonomiki [The role of electronic payment systems implementation in global economic development]. Biznes i obshchestvo [Business and Society], 1(33).
14. Ilyin, A. V., & Ilyin, V. D. (2020). Normalizovannyi ekonomicheskii mekhanizm: tsifrovye tekhnologii polivalyutnogo rynka [Normalized economic mechanism: Digital technologies of the multi-currency market]. Sistemy i sredstva informatiki [Systems and Means of Informatics], 30(1), 186–197.
15. Gochieva, M. D., & Dzhukkaeva, Z. A. (2021). Bezopasnost onlain-pokupok [Security of online shopping]. Tendentsii razvitiya nauki i obrazovaniya [Trends in the Development of Science and Education], 80–2, 79–81.