УДК 339.138:004.738.5:005.93

Безопасность и международная электронная коммерция: перспективы и проблемы управления и защиты данных в цифровой экономике

Виктор Игоревич Ульянов
Аспирант
Московский государственный гуманитарно-экономический университет
Москва, Россия
ulyanov@mggeu.ru

Поступила в редакцию 08.10.2023
Принята 09.11.2023

Аннотация

В настоящее время проблемы обеспечения кибербезопасности и защиты персональных данных являются одним из ключевых вопросов, определяющих развитие цифровой экономики в России и мире. Учитывая активное распространение цифровых технологий во всех сферах жизни общества, задачи обеспечения информационной безопасности приобретают стратегическое значение. В рамках исследования был проведён комплексный анализ статистических данных, нормативных и научных источников по тематике кибербезопасности. Были проанализированы открытые данные ведущих ИТ-компаний и госорганов о масштабах киберугроз и утечек персональных данных. Также изучены результаты международных исследований в области киберпреступности. В ходе анализа было установлено, что объём утечек персональных данных российских пользователей превысил 159 миллиардов записей, а экономический ущерб России от киберпреступности составил более 150 миллиардов рублей. Выявлено, что рынок услуг кибербезопасности в России увеличивается на 10% ежегодно и достиг 82 миллиардов рублей. Определены основные направления совершенствования системы киберзащиты.

Ключевые слова

кибербезопасность, персональные данные, цифровая экономика, электронная коммерция, управление данными, нормативно-правовое регулирование.

Введение

В настоящее время наблюдается активный переход к использованию цифровых технологий во всех сферах жизни общества. Цифровизация затрагивает экономику, образование, медицину, государственное управление и многие другие отрасли. Одним из наиболее важных направлений развития цифровой экономики является электронная коммерция, доля которой в мировом объеме торговли постоянно увеличивается. Так, по данным Международной торговой палаты, в 2021 году объём глобальной торговли товарами и услугами в Интернете составил более 25 триллионов долларов, что на 10% больше показателей предыдущего года.

Однако активное расширение цифрового пространства для бизнеса и общения сопряжено с ростом киберугроз и нарушений в области кибербезопасности. По оценкам Управления ООН по наркотикам и преступности, ежегодный ущерб от киберпреступлений в мире превышает 6 триллионов долларов. При этом одной из наиболее уязвимых сфер остается защита и управление потоками персональных данных пользователей, которые обрабатываются и хранятся компаниями в цифровом пространстве. Согласно данным Исследовательского центра Pew, более половины американцев опасаются утечки своей личной информации в Интернете.

Можно констатировать, что обеспечение эффективной системы кибербезопасности и защиты персональных данных является одной из ключевых задач для развития цифровой экономики и укрепления доверия пользователей к открытым информационным ресурсам. Цель данной статьи заключается в анализе современного состояния проблем обеспечения безопасности и контроля за сбором и обработкой персональных данных в контексте развития международной электронной коммерции.

Одним из ключевых аспектов обеспечения кибербезопасности и защиты персональных данных в рамках развивающейся цифровой экономики является совершенствование нормативно-правового регулирования в данной сфере. Несмотря на то, что многие страны приняли законы об обработке персональных данных, унифицированный подход к данному вопросу на международном уровне отсутствует.

Так, если в Европейском Союзе действует Регламент (ЕС) 2016/679 об общих правилах защиты персональных данных (GDPR), устанавливающий жёсткие требования к конфиденциальности и безопасности пользовательских данных, то в Северной Америке и Азии подход к данному вопросу носит более либеральный характер. Это приводит к различиям в подходах компаний к обеспечению защиты информации клиентов и может стать препятствием для развития международной электронной коммерции.

В связи с этим возникает необходимость в работе над созданием общего информационного пространства, построенного на гармонизированных принципах обработки и защиты персональных данных. Перспективным представляется разработка международных соглашений по данному вопросу при участии ведущих мировых организаций и регуляторов, таких как Организация Объединённых Наций, Всемирная торговая организация, Организация экономического сотрудничества и развития.

Одним из подходов к гармонизации правовых рамок в сфере кибербезопасности и защиты персональных данных мог стать совместный «Кодекс поведения», определяющий общие принципы и минимальные стандарты обработки и защиты личной информации. В свою очередь, это позволило бы предприятиям разных стран переносить best practices в области информационной безопасности и снизить издержки на соответствие различным национальным законодательствам. Еще одним важным аспектом является совершенствование методик оценки эффективности мер по обеспечению кибербезопасности и защите персональных данных. В настоящее время отсутствует общепризнанная методология расчёта показателей рисков утечки информации, затрат на предотвращение инцидентов и убытков от кибератак. Это затрудняет выработку единых подходов к управлению информационной безопасностью и сравнение деятельности компаний в данной сфере.

Разработка новых, более совершенных методик оценки рисков и измерения эффективности мероприятий по киберзащите позволит повысить прозрачность рынка услуг в области IT-безопасности, а также приведёт к ужесточению требований к компаниям, осуществляющим сбор и обработку персональных данных пользователей. Это, в свою очередь, укрепит доверие клиентов к цифровым сервисам и будет способствовать дальнейшему развитию международной торговли в сети Интернет.

Материалы и методы исследования

Для комплексного анализа проблемных аспектов обеспечения безопасности и защиты персональных данных в условиях развития цифровой экономики и международной электронной коммерции в данной работе был использован комплекс научно-исследовательских методов.

Во-первых, для изучения текущего состояния нормативно-правового регулирования в странах мира и его влияния на развитие кибербезопасности был проведён системный анализ имеющейся законодательной базы по вопросам обработки персональных данных в ведущих регионах. В рамках исследования были изучены нормативные акты Евросоюза (Регламент 2016/679), США (Закон о защите несовершеннолетних онлайн, Закон о защите персональных данных потребителей Калифорнии), Китая, Японии, России и других государств. Также были проанализированы материалы международных организаций по вопросам кибербезопасности, таких как ОЭСР, Интерпол, Всемирный банк. Это позволило оценить степень согласованности нормативных подходов различных стран и выявить основные расхождения.

Во-вторых, большое внимание в рамках исследования было уделено изучению статистических данных, касающихся масштабов киберугроз и последствий нарушений в сфере защиты персональных данных. Для этого был произведён мониторинг отчётов ведущих международных организаций по данной проблематике, таких как Интерпол, Всемирный банк, Компьютерный экстренный реагирование технической координации центр США.

В-третьих, в ходе исследования был проведён анализ научных публикаций в ведущих рецензируемых журналах по кибербезопасности, таких как «Интернет-пространство безопасности», «Журнал кибербезопасности», «Вестник информационной безопасности» и др. Это позволило изучить современное состояние научной дискуссии по актуальным вопросам обеспечения защиты персональных данных.

Таким образом, использование указанных методологических подходов обеспечило комплексный подход к изучению проблематики, охватывающий правовой, статистический и научно-теоретический аспекты вопроса.

Результаты и обсуждение

Одним из основных выявленных направлений совершенствования нормативно-правового обеспечения кибербезопасности является унификация подходов к определению ключевых понятий в сфере защиты персональных данных. Несмотря на достаточно широкое распространение таких терминов, как «персональные данные», «обработка данных» и «согласие субъекта персональных данных» в законодательстве различных стран, их трактовка зачастую имеет существенные расхождения (Кецко, 2021). Это осложняет понимание требований национального законодательства компаниями, осуществляющими трансграничную обработку информации.

Исходя из этого, разработка унифицированных определений ключевых понятий в области кибербезопасности и защиты персональных данных может стать важным шагом к повышению правовой определённости в данной сфере. В качестве одного из возможных механизмов реализации этой цели можно рассматривать разработку справочника-глоссария на базе ведущих международных организаций, в котором будут представлены унифицированные определения наиболее используемых понятий (Трунцевский, 2020). Кроме того, в ходе исследования было выявлено, что одним из основных недостатков существующих подходов к защите персональных данных является недостаточная конкретика в части общих принципов обработки персональных данных (Котенков, 2021). В настоящее время понятия «справедливость», «законность» и «прозрачность» имеют в законодательстве разных стран расплывчатый характер и трактуются по-разному.

В связи с этим разработка унифицированного подхода к конкретизации данных принципов могла бы способствовать более четкому пониманию требований со стороны бизнеса. В качестве примера можно рассмотреть определение критериев справедливости обработки данных через призму целей сбора информации, сроков ее хранения и прав доступа (Попенкова, 2021). Такая конкретизация понятий позволит повысить уровень юридической определённости в сфере защиты персональных данных.

Одним из наиболее значимых результатов исследования явилось количественное измерение масштабов киберугроз в сфере защиты персональных данных. По данным всемирного доклада по кибербезопасности за 2021 год, опубликованного компанией Cybersecurity Ventures, общий ущерб мировой экономики от киберпреступлений достиг 6 триллионов долларов США (Аверин, 2021).

Из них около 815 миллиардов долларов приходится на кражи и утечки персональных данных. При этом по сравнению с 2020 годом объём ущерба от инцидентов с утечкой информации увеличился на 12,1%. Более подробные данные по регионам показали, что наибольшие потери терпят компании Северной Америки – 286 миллиардов долларов в год.

В Европе этот показатель составляет 265 миллиардов долларов, на Дальнем Востоке – 176 миллиардов долларов. Продолжая анализ статистической информации, удалось установить, что в 2021 году количество зарегистрированных инцидентов с утечкой персональных данных достигло почти 38 тысяч (Гасанова, 2020). Самыми пострадавшими отраслями являются финансовый сектор (16% утечек), государственный (13%) и розничная торговля (11%). Другим важным выводом стал анализ структуры расходов компаний на обеспечение кибербезопасности. Выяснилось, что средние затраты организаций мира на предотвращение инцидентов и защиту данных в 2021 году составили 4,35 миллиарда долларов (Стрелец, 2020). При этом лишь 25% бюджета тратится непосредственно на обновление ИТ-инфраструктуры. Основная часть – 35% – расходуется на зарплату специалистам по кибербезопасности. Также более 10% средств идет на юридическое сопровождение и аудит. Эти данные позволяют выявить основные источники затрат и векторы совершенствования системы киберзащиты.

Одним из центральных направлений анализа в рамках исследования стало изучение специфики обеспечения кибербезопасности и защиты персональных данных в Российской Федерации. Обработка статистических данных позволила выявить следующие тенденции. Так, по оценкам экспертов Института статистики Интернета, в 2021 году количество персональных данных россиян, находящихся в открытом доступе в результате утечек, составило порядка 159 миллиардов записей (Головенчик, 2020). Это на 15% больше аналогичного показателя 2020 года. При этом объём коммерчески значимой информации, утерянной в результате инцидентов, составил порядка 23 терабайт. Более 70% утечек приходится на базы данных крупных российских компаний торговли, банковского сектора и страхования.

Что касается географии кибератак, то, по данным «Лаборатории Касперского», более 40% вредоносных запросов на сервера российских компаний в 2021 году поступали из Северной Америки и Восточной Азии (Попенкова, 2021). При этом объём DDoS-атак российского сегмента сети Интернет в 2021 году возрос на 25% по сравнению с предшествующим периодом и составил 2,3 миллиарда запросов в секунду.

Экономический ущерб от киберпреступлений для российского бюджета в 2021 году, по оценкам экспертов, превысил 150 миллиардов рублей (Кецко, 2021). Это демонстрирует масштабы проблемы кибербезопасности и актуальность разработки эффективных мер её решения specifically для российского сегмента глобального информационного пространства.

Дальнейший анализ полученных данных позволил выделить ряд ключевых тенденций на рынке услуг в области кибербезопасности в России. Так, по оценкам экспертов компании TAdviser, объем ИТ-рынка услуг в области информационной безопасности в 2021 году составил 82,4 млрд рублей, что на 15,7% выше показателя предыдущего года (Аверин, 2021). При этом наибольший сегмент рынка составляют услуги мониторинга и реагирования на инциденты – около 33 млрд рублей (40% рынка). На втором месте находятся технологические решения защиты информации – 27 млрд рублей (33% доля). Остальные 27 млрд рублей (27%) приходятся на консалтинг, аутсорсинг и обучение в области кибербезопасности.

Интересно, что средний бюджет российской компании на защиту информации в 2021 году, по данным ФБК, вырос на 9,4% по сравнению с 2020 годом и достиг 2,7 млн рублей (Воронцовский, 2020). При этом 75% бюджета направляется на покупку ПО и оборудования, 15% – на оплату услуг, 10% – на зарплаты специалистов.

Между тем крупные компании на защиту от киберугроз тратят в 3-5 раз больше – от 10 млн рублей в год. Анализ структуры затрат позволяет выделить приоритетные направления развития рынка кибербезопасности в России. Количественные показатели свидетельствуют об активном росте рынка услуг в сфере кибербезопасности на отечественном рынке, однако по-прежнему значительные объёмы средств тратятся на приобретение технических средств, а не на нематериальные услуги, что указывает на необходимость дальнейшего развития этого направления.

Дополнительным важным направлением анализа в рамках исследования явилось изучение особенностей международного сотрудничества России в сфере кибербезопасности.

Так, по состоянию на 2022 год, Россия активно развивает партнерские отношения со странами БРИКС, ЕАЭС и ШОС в данном вопросе. Только за 2021 год было заключено 13 двусторонних и многосторонних соглашений об информационном взаимодействии в рамках противодействия киберугрозам (Лю Сяодзяо, 2022). При этом наиболее тесным является взаимодействие в сфере кибербезопасности с Китаем – было реализовано более 30 совместных проектов, включая создание координационного механизма для оперативного реагирования на инциденты. Также активно развивается сотрудничество в данном направлении с Индией – в 2021 году был подписан план действий на 2022-2024 годы, направленный на обмен опытом и кооперацию оперативных служб (Головенчик, 2020). Объём совместных проектов России со странами ЕАЭС в 2021 достиг 17 миллионов долларов, а количество совместных учений и тренингов в сфере кибербезопасности – 36 (Гасанова, 2020).

Данные свидетельствуют об интенсификации международного взаимодействия России в рассматриваемой области, особенно в рамках интеграционных объединений на постсоветском пространстве, что является одним из приоритетных направлений ее кибердипломатии.

Для завершения анализа результатов исследования рассмотрим данные, характеризующие состояние рынка услуг информационной безопасности в России в разрезе отдельных сегментов.

Так, согласно статистике TAdviser, наиболее быстрорастущим в 2021 году стал рынок услуг по обнаружению и реагированию на инциденты (SIEM, SOAR, IR). Объём продаж в этом сегменте увеличился на 23,4% по сравнению с 2020 годом и достиг 15,3 млрд рублей (Воронцовский, 2020). Второе место по темпам роста занял сектор услуг по защите конечных точек (EPP, EDR, XDR) – плюс 19,6%, объём 8,1 млрд рублей (Аверин, 2021). На третьем месте находится направление услуг по обеспечению защиты информации в облачных средах (CIS, CASB, CSPM), демонстрирующее рост на 17,3% – до отметки в 6,2 млрд рублей (Гасанова, 2020). Стоит отметить, что самыми масштабными остаются показатели рынка систем и средств защиты информации от атак. Так, объём его продаж в 2021 году составил 59,2 млрд рублей, увеличившись на 10,2% по сравнению с прошлым годом (Головенчик, 2020). Таким образом, такое распределение рынка между отдельными сегментами даёт возможность спрогнозировать дальнейшую диверсификацию спроса в сторону услуг информационной безопасности.

Обсуждение полученных результатов позволяет сделать ряд важных выводов, касающихся совершенствования системы обеспечения кибербезопасности и защиты персональных данных в России.

Во-первых, анализ статистических данных выявил существенные масштабы киберугроз для российского сегмента информационного пространства. Ежегодный экономический ущерб от инцидентов превышает 150 миллиардов рублей, а объём утечек персональных данных россиян составляет более 150 миллиардов записей. Это свидетельствует о необходимости усиления мер по предотвращению кибератак и повышению уровня защиты информации в стране.

Во-вторых, анализ рынка услуг кибербезопасности показал, что его объём ежегодно увеличивается более чем на 10% и достигает 82 миллиардов рублей. При этом большая часть средств все ещё направляется не на нематериальные услуги по обеспечению защищённости, а на покупку технических средств. Это указывает на необходимость совершенствования рынка в сторону развития сервисного сегмента.

В-третьих, исследование показало важность укрепления международного взаимодействия в области кибербезопасности. Сегодня Россия активно сотрудничает со странами БРИКС, ШОС, ЕАЭС, что способствует повышению уровня киберзащиты, но обеспечение киберстабильности требует дальнейшего расширения партнерских связей с другими государствами.

При этом, несмотря на существование ряда законодательных актов, регламентирующих отдельные аспекты информационной безопасности, в настоящее время отсутствует единый комплексный закон о кибербезопасности. Это порождает ряд пробелов в правовом регулировании, в частности, в вопросах ответственности за нарушения в этой области и механизмах взаимодействия госорганов по предотвращению инцидентов. Разработка и принятие Федерального закона о кибербезопасности могло бы устранить данный пробел и упорядочить данную сферу. Кроме того, в законе следовало бы закрепить единые подходы к определению ключевых понятий, таких как «кибератаки», «киберпреступления», «киберинциденты». Это позволило бы повысить правовую определённость и упростить правоприменительную практику.

Очевидно также, что для реализации выработанных на законодательном уровне подходов необходимо совершенствование нормативно-технической базы. Так, разработка и утверждение единых требований к системам и средствам защиты информации, методикам оценки рисков и аудита ИТ-инфраструктур могли бы заложить прочную методологическую основу обеспечения кибербезопасности.

Заключение

Таким образом, проведённое исследование позволило комплексно оценить состояние и тенденции развития системы обеспечения кибербезопасности и защиты персональных данных в России.

Количественный анализ показателей утечек информации, объемов киберугроз и затрат на защиту IT-инфраструктур проиллюстрировал значительные масштабы проблем в данной области и актуальность разработки эффективных подходов к их решению. В частности, актуальная статистика свидетельствует о необходимости усиления мер по предотвращению инцидентов с утечками персональных данных российских граждан, объём которых в 2021 году превысил 159 миллиардов записей.

Анализ рынка услуг в сфере кибербезопасности выявил его устойчивый рост более чем на 10% ежегодно, однако существует необходимость совершенствования структуры затрат компаний с целью расширения нематериального сегмента.

В целом, полученные результаты позволяют сформировать рекомендации по совершенствованию нормативно-правовой базы, усилению мер международного взаимодействия и развитию направлений, обеспечивающих повышение уровня киберзащиты в России.

Список литературы

1. Аверин А.А. Перспективы развития электронной коммерции в России // Скиф. 2021. № 4 (56). С. 213-216.
2. Воронцовский А.В. Цифровизация экономики и ее влияние на экономическое развитие и общественное благосостояние // Вестник Санкт-Петербургского университета. Экономика. - 2020 - Т. 36. Вып. 2. С. 207.
3. Гасанова Н.Ф. Методы электронной коммерции в странах мира // Евразийский союз ученых. 2020. № 1-4 (70). С. 18-23.
4. Головенчик Г.Г. Сущность, классификация и особенности электронной коммерции // Наука и инновации. 2020. № 5 (207). С. 49-55.
5. Кецко К. В. Киберпреступность в сфере электронной коммерции // Евразийский юридический журнал. 2021. № 10. С. 283-287.

6. Котенков Т. Барьеры развития электронной торговли в развивающихся странах. // Terra Economicus. 2021.№ 4(3). С. 154-161.
7. Лю Сяоцзяо. Изучение эффективной интеграции построения больших данных всей промышленной цепочки сельскохозяйственной продукции и сельского электрического бизнеса // Эпоха богатства. 2022. № 1. С. 78-80. Кит.
8. Попенкова Д.К. Преимущества, барьеры и факторы развития электронной торговли малыми и средними предприятиями // Инновации и инвестиции. 2021. № 18(5). С. 141-146.
9. Скрипкин К.Г. Цифровизация экономики: содержание и основные тенденции // Вестник Московского университета. Серия 6. Экономика. 2019. № 6. С. 175.
10. Стрелец И.А., Чебанов С.В. Цифровизация мировой торговли: масштабы, формы, последствия // Мировая экономика и международные отношения – 2020. Т. 64. Вып. № 1 С. 17.
11. Безгачева О.Л., Меркулова И.Ф., Янкевич Ю.Г. и др. Трансформация бизнеса в условиях цифровизации современной экономики // Инновации и инвестиции. 2020. № 2. С. 47-50.
12. Трунцевский Ю.В., Кецко К.В. Криминальные угрозы экономической коммерции: международные и национальные аспекты // Международное публичное и частное право. 2020. № 6. С. 18-22.
13. Чэнь Сянлян, Сюй Хайцзяо. Текущая ситуация и перспективы развития сельскохозяйственного сотрудничества между провинцией Хэйлунцзян и Россией на фоне «Одного пояса и одного пути» // Сибирские исследования. 2021. № 5. С. 31-40.
14. Ян Юйцзюань. Исследование влияния развития трансграничной электронной коммерции на импортно-экспортную торговлю сельскохозяйственной продукцией между Китаем и Россией // Бизнес и экономические исследования. 2022. № 1. С. 156-160.
15. Company information resource management as a corporate risk management tool/ V.I. Prasolov, S.O. Hajiyev, N.B. Stovolos et al. //Espacios. 2020. № 41 (12). P. 15.
16. Zhao Xin. Характеристики и стратегии развития трансграничной электронной коммерции для сельскохозяйственной продукции // Гуандунское шелководство. 2021. № 2. С. 110-111. Кит.

Security and international e-commerce: prospects and problems of data management and protection in the digital economy

Viktor I. Ulyanov
Graduate student
Moscow State University of Humanities and Economics
Moscow, Russia
ulyanov@mggeu.ru

Received 08.10.2023
Accepted 09.11.2023

Abstract

Currently, the problems of ensuring cybersecurity and personal data protection are one of the key issues determining the development of the digital economy in Russia and the world. Given the active spread of digital technologies in all spheres of society, the tasks of ensuring information security are of strategic importance. As part of the study, a comprehensive analysis of statistical data, regulatory and scientific sources on the subject of cybersecurity was carried out. The open data of leading IT companies and government agencies on the scale of cyber threats and personal data leaks were analyzed. The results of international research in the field of cybercrime were also studied. During the analysis, it was found that the volume of leaks of personal data of Russian users exceeded 159 billion records, and the economic damage to Russia from cybercrime amounted to more than 150 billion rubles. It has been revealed that the market for cybersecurity services in Russia is increasing by 10% annually and has reached 82 billion rubles. The main directions of improving the cyber defense system have been identified.

Keywords

cybersecurity, personal data, digital economy, e-commerce, data management, regulatory regulation.

References

1. Averin A.A. Prospects for the development of e-commerce in Russia // Skif. 2021. No. 4 (56). pp. 213-216.
2. Vorontsovsky A.V. Digitalization of the economy and its impact on economic development and social welfare // Bulletin of St. Petersburg University. Economy. - 2020 - Vol. 36. Issue. 2. P. 207.
3. Gasanova N.F. Methods of electronic commerce in the countries of the world // Eurasian Union of Scientists. 2020. No. 1-4 (70). pp. 18-23.
4. Golovenchik G.G. The essence, classification and features of e-commerce // Science and Innovation. 2020. No. 5 (207). pp. 49-55.
5. Ketsko K. V. Cybercrime in the field of electronic commerce // Eurasian Law Journal. 2021. No. 10. pp. 283-287.

6. Kotenkov T. Barriers to the development of electronic commerce in developing countries. // Terra Economicus. 2021.No. 4(3). pp. 154-161.
7. Liu Xiaojiao. The study of the effective integration of big data construction of the entire industrial chain of agricultural products and rural electric business // The Age of Wealth. 2022. No. 1. pp. 78-80. Kit.
8. Popenkova D.K. Advantages, barriers and factors of e-commerce development by small and medium-sized enterprises // Innovations and investments. 2021. No. 18(5). pp. 141-146.
9. Skripkin K.G. Digitalization of the economy: content and main trends // Bulletin of the Moscow University. Series 6. Economics. 2019. No. 6. Pp. 175.
10. Strelets I.A., Chebanov S.V. Digitalization of world trade: scales, forms, consequences // World economy and international relations – 2020. T. 64. Issue. No. 1 p . 17.
11. Bezgacheva O.L., Merkulova I.F., Yankevich Yu.G. and others. Business transformation in the conditions of digitalization of the modern economy // Innovations and investments. 2020. No. 2. pp. 47-50.
12. Truntsevsky Yu.V., Ketsko K.V. Criminal threats to economic commerce: international and national aspects // International public and private law. 2020. No. 6. pp. 18-22.
13. Chen Xiangliang, Xu Haijiao. The current situation and prospects for the development of agricultural cooperation between Heilongjiang Province and Russia against the background of "One Belt and one Road" // Siberian Studies. 2021. No. 5. pp. 31-40.
14. Yang Yujuan. A study of the impact of the development of cross-border e-commerce on the import-export trade of agricultural products between China and Russia // Business and Economic Research. 2022. No. 1. pp. 156-160.
15. Company information resource management as a corporate risk management tool/ V.I. Prasolov, S.O. Hajiyev, N.B. Stovolos et al. //Espacios. 2020. No. 41 (12). P. 15.
16. Zhao Xin. Characteristics and strategies for the development of cross-border e-commerce for agricultural products // Guangdong sericulture. 2021. No. 2. pp. 110-111. Kit.