Образец ссылки на эту статью: Измайлов М.К., Арбенина Е.А. Цифровые способы обеспечения экономической безопасности как основа устойчивого развития промышленного сектора // Бизнес и дизайн ревю. 2024. № 4 (36). С. 21-31.

УДК 338

ЦИФРОВЫЕ СПОСОБЫ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КАК ОСНОВА УСТОЙЧИВОГО РАЗВИТИЯ ПРОМЫШЛЕННОГО СЕКТОРА

Измайлов Максим Кириллович

Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Россия (195251, Санкт-Петербург, ул. Политехническая, д. 29), к.э.н., доцент Высшей школы производственного менеджмента, izmajlov_mk@spbstu.ru

Арбенина Евгения Андреевна

Воронежский государственный аграрный университет имени императора Петра I, Воронеж, Россия (394087, Воронеж, ул. Мичурина, 1), к.э.н., доцент кафедры экономики АПК, cneltyndufe@mail.ru

Аннотация. Исследование посвящено актуальной проблеме применения цифровых технологий для обеспечения экономической безопасности промышленных предприятий – ключевого фактора их устойчивого развития в современных условиях. В работе проведен комплексный анализ влияния цифровизации на повышение операционной эффективности, защищенности критических информационных активов, прозрачности цепочек поставок и финансовых операций промышленных компаний. Разработаны практические рекомендации по внедрению передовых решений в сфере управления информационной безопасностью, защиты «умных» производственных систем, шифрования данных, а также развития аналитических и прогностических возможностей. Показаны пути реализации предложенного комплексного подхода на уровне отдельных предприятий, отраслевых сообществ и промышленности в целом. Результаты исследования могут быть использованы руководителями и специалистами промышленных компаний при разработке и реализации стратегий обеспечения экономической безопасности в условиях цифровой трансформации.

Ключевые слова: цифровизация; экономическая безопасность; промышленность; устойчивое развитие; информационная безопасность; киберустойчивость.

DIGITAL WAYS OF ENSURING ECONOMIC SECURITY AS A BASIS FOR SUSTAINABLE DEVELOPMENT OF THE INDUSTRIAL SECTOR

Izmaylov Maxim Kirillovich

Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia (195251, St. Petersburg, Polytechnicheskaya, 29), Cand. Sc. (Economics), Associate Professor at the Graduate School of Industrial Management, izmajlov_mk@spbstu.ru

Arbenina Evgenia Andreevna

Voronezh State Agrarian University named after Emperor Peter the Great, Voronezh, Russia (394087, Voronezh, Michurina St., 1), Cand. Sc. (Economics), Associate Professor at the Department of Economics of Agroindustrial Complex, cneltyndufe@mail.ru

Abstract. The research is devoted to the urgent problem of using digital technologies to ensure the economic security of industrial enterprises, which is a key factor of their sustainable development in modern conditions. The paper provides a comprehensive analysis of the impact of digitalization on improving operational efficiency, security of critical information assets, transparency of supply chains and financial operations of industrial companies. Practical recommendations for the implementation of advanced solutions in the field of information security management, protection of «smart» production systems, data encryption, as well as the development of analytical and predictive capabilities are developed. The ways to implement the proposed integrated approach at the level of individual enterprises, industry communities and industry as a whole are shown. The results of the study can be used by managers and specialists of industrial companies in the development and implementation of strategies to ensure economic security in the conditions of digital transformation.

Keywords: digitalization; economic security; industry; sustainable development; information security; cyber resilience.

Введение

В современных условиях глобальной нестабильности проблема обеспечения экономической безопасности приобретает критическое значение для устойчивого развития промышленного сектора. Переход к цифровой экономике открывает новые возможности, но также несет серьезные риски кибератак, утечки конфиденциальной информации и других киберугроз, способных нанести значительный ущерб предприятиям, независимо от их отраслевой принадлежности [1]. Обеспечение надежной защиты информационных систем и данных становится ключевым фактором обеспечения экономической безопасности и сохранения конкурентоспособности промышленных компаний. Научная новизна работы заключается в комплексном анализе современных цифровых инструментов и технологий, позволяющих повысить уровень экономической безопасности промышленных предприятий. В работе выявляются наиболее перспективные цифровые решения в сфере кибербезопасности, защиты информации, мониторинга и управления рисками, а также оценивается их влияние на устойчивость развития промышленного сектора. Результаты исследования могут быть использованы руководителями промышленных предприятий, специалистами по информационной безопасности, а также органами государственного управления при разработке стратегий, программ и мероприятий, направленных на цифровую трансформацию промышленности и обеспечение ее экономической безопасности. Предложенные подходы и рекомендации будут способствовать повышению киберустойчивости, защищенности критически важных информационных активов и, как

следствие, обеспечению долгосрочной конкурентоспособности промышленных компаний.

Цель исследования

Настоящее исследование направлено на всесторонний анализ современных цифровых инструментов и технологий, которые способны повысить уровень экономической безопасности промышленных предприятий и, как следствие, обеспечить их устойчивое развитие. Для достижения поставленной цели в работе решается ряд ключевых задач. Первостепенное значение имеет изучение текущего состояния и ключевых тенденций в области применения цифровых технологий для обеспечения экономической безопасности промышленных предприятий. Это позволит сформировать комплексное представление о ведущих разработках и перспективных направлениях развития данной сферы. Отдельное внимание уделяется анализу наиболее перспективных цифровых решений и инструментов, применимых для повышения защищенности информационных систем, данных и критически важных активов промышленных компаний. Данный блок исследования предполагает оценку эффективности, функциональных возможностей и ключевых характеристик передовых цифровых технологий кибербезопасности, управления рисками, мониторинга и защиты информации. Важной составляющей работы является изучение влияния использования современных цифровых инструментов на повышение уровня экономической безопасности предприятий промышленного сектора. В этом контексте будет проанализирована роль цифровой трансформации в обеспечении киберустойчивости, сохранности критически важных активов и, в конечном счете, долгосрочной конкурентоспособности промышленных компаний. Результатом исследования является разработка практических рекомендаций по внедрению и эффективному применению цифровых инструментов обеспечения экономической безопасности для повышения устойчивости развития промышленных предприятий. Особое внимание будет уделено обоснованию путей реализации предложенных подходов на уровне отдельных компаний, отраслей и всего промышленного комплекса.

Методы исследования

Для реализации поставленных в работе целей и задач будет использован комплекс современных научных методов, включающих:

1. Системный анализ. Данный подход позволит исследовать экономическую безопасность промышленных предприятий как сложную многокомпонентную систему, находящуюся под влиянием разнообразных внутренних и внешних факторов. Применение системного анализа обеспечит целостное и структурированное изучение роли цифровых технологий в обеспечении экономической безопасности промышленности.

2. Сравнительный анализ. Метод сравнения будет использован для оценки эффективности различных цифровых инструментов и технологий, применяемых в сфере обеспечения экономической безопасности промышленных предприятий. Это позволит выявить наиболее перспективные решения, обладающие максимальным потенциалом для обеспечения устойчивого развития промышленности.

3. Методы группировки и классификации. Данные методы будут использованы для систематизации и группировки информации о существующих цифровых инструментах обеспечения экономической безопасности промышленных предприятий, а также для их классификации по ключевым признакам и характеристикам.

Комплексное применение указанных методов исследования позволит всесторонне изучить роль цифровых технологий в обеспечении экономической безопасности промышленного сектора, выявить наиболее перспективные решения и разработать практические рекомендации по их внедрению для достижения устойчивого развития предприятий.

Результаты исследования и их обсуждение

Современные промышленные предприятия функционируют в условиях стремительных технологических изменений и нарастающей глобальной нестабильности [2]. Цифровая трансформация, охватывающая все сферы деятельности компаний, открывает широкие возможности для повышения операционной эффективности, гибкости и конкурентоспособности бизнеса. Вместе с тем, процесс цифровизации промышленности сопровождается появлением ранее не существовавших рисков и угроз экономической безопасности. Ключевым фактором, определяющим активное внедрение цифровых технологий в промышленности, является стремление компаний к повышению эффективности и гибкости производственных процессов, а также улучшению качества продукции и сервиса для клиентов. В этом контексте широкое распространение получают решения в области «умных» производственных систем, промышленного интернета вещей, роботизации, больших данных и аналитики. Однако, по мере расширения цифровизации производственной сферы, все более актуальными становятся вопросы обеспечения информационной и кибербезопасности предприятий [3]. Современные промышленные компании сталкиваются с растущими рисками хакерских атак, утечки конфиденциальной информации, нарушения работоспособности критически важных систем и других киберугроз. Подобные инциденты способны нанести колоссальный материальный и репутационный ущерб предприятиям, поставив под угрозу их операционную деятельность и финансовую устойчивость. В этих условиях защита информационных активов, систем управления и производственных процессов становится ключевым приоритетом в обеспечении экономической безопасности промышленности [4].

Анализ ключевых трендов развития цифровых технологий в данной сфере позволяет выделить следующие перспективные направления:

1) внедрение комплексных систем управления информационной безопасностью, интегрирующих средства защиты, мониторинга, анализа и реагирования на киберугрозы. Данные решения обеспечивают централизованный контроль и защиту критической сетевой инфраструктуры, промышленных систем управления, баз данных и других жизненно важных информационных активов предприятия;

2) развитие технологий индустриального интернета вещей (IIoT) и промышленной робототехники с повышенным уровнем кибербезопасности. Такие решения призваны гарантировать надежную защиту «умных» производственных систем и устройств от внешних и внутренних угроз;

3) применение продвинутых аналитических технологий, в том числе, на основе искусственного интеллекта, для мониторинга и автоматизированного реагирования на киберугрозы в режиме реального времени. Данные инструменты позволяют существенно повысить киберустойчивость промышленных предприятий;

4) внедрение решений для шифрования, идентификации и биометрической аутентификации, обеспечивающих защиту конфиденциальных данных, промышленных секретов и критически важных активов компаний;

5) развитие технологий распределенного реестра (блокчейн) для обеспечения неизменности и прослеживаемости информации об операциях, производственных процессах и транзакциях.

Таким образом, текущее состояние и ключевые тенденции развития цифровых технологий в сфере обеспечения экономической безопасности промышленности характеризуются растущей потребностью в комплексных решениях по защите информационных систем, данных и производственных процессов от киберугроз. Внедрение передовых цифровых инструментов становится критически важным фактором, определяющим киберустойчивость и долгосрочную конкурентоспособность современных промышленных компаний.

Обеспечение информационной безопасности и защита критически важных активов становятся ключевыми приоритетами для промышленных предприятий в условиях активного внедрения цифровых технологий. Для решения данной задачи компании внедряют широкий спектр перспективных цифровых инструментов и решений. Одним из ведущих направлений является разработка и внедрение комплексных систем управления информационной безопасностью (SIEM-систем). Такие решения интегрируют средства защиты, мониторинга, анализа и оперативного реагирования на киберугрозы в масштабах всего предприятия. SIEM-системы обеспечивают централизованный контроль и защиту корпоративной сетевой инфраструктуры, промышленных систем управления, баз данных и других ключевых информационных активов. Использование продвинутой аналитики

и машинного обучения в таких системах позволяет выявлять сложные, ранее неизвестные атаки, а также автоматизировать процессы реагирования в режиме реального времени. Технологии индустриального интернета вещей (IIoT) и промышленной робототехники также становятся объектом пристального внимания с точки зрения обеспечения кибербезопасности. Для повышения защищенности «умных» производственных систем и устройств активно разрабатываются специализированные решения, предусматривающие встроенные механизмы шифрования, аутентификации, целостности и разграничения доступа [5]. Кроме того, применение продвинутой аналитики позволяет осуществлять непрерывный мониторинг аномалий и вторжений в промышленные сети и системы. Важным направлением являются технологии шифрования, идентификации и биометрической аутентификации, применяемые для защиты критически важных данных, промышленных секретов и других конфиденциальных активов компаний. Использование современных криптографических алгоритмов, систем контроля доступа и многофакторной аутентификации позволяет обеспечить высокий уровень защищенности ключевой информации предприятий. Технологии распределенного реестра (блокчейн) также находят свое применение в сфере промышленной безопасности. Их использование дает возможность гарантировать неизменность и прозрачность данных об операциях, производственных процессах и транзакциях, повышая доверие и защищенность цифровых платформ и экосистем. Помимо этого, для противодействия современным киберугрозам активно применяются продвинутые аналитические решения, в том числе на основе искусственного интеллекта. Такие инструменты обеспечивают непрерывный мониторинг аномалий, выявление сложных атак и автоматизированное реагирование, что позволяет существенно повысить киберустойчивость промышленных предприятий. Другими словами, анализ наиболее перспективных цифровых решений и инструментов в сфере обеспечения экономической безопасности промышленности выявляет четкий тренд на комплексный подход, включающий защиту информационных систем, данных и критических активов на основе современных технологий шифрования, аналитики и управления доступом.

Современные промышленные предприятия активно внедряют передовые цифровые технологии и решения, добиваясь значительного повышения операционной эффективности, гибкости и конкурентоспособности. Однако этот процесс цифровой трансформации оказывает и более глубокое, комплексное влияние на обеспечение экономической безопасности компаний отрасли [6]. Одним из ключевых направлений воздействия цифровых технологий является значительное повышение производственных показателей. Использование «умных» производственных систем, промышленного интернета вещей и робототехники позволяет существенно улучшить эффективность, гибкость и качество выпускаемой продукции. Это, в свою очередь, укрепляет рыночные позиции и финансовую устойчивость

предприятий в долгосрочной перспективе, повышая их конкурентоспособность. Другим важным аспектом является обеспечение надежной защиты ключевых информационных активов и производственных процессов от киберугроз [7]. Внедрение комплексных систем управления информационной безопасностью, интегрирующих средства мониторинга, анализа и оперативного реагирования, позволяет минимизировать риски финансовых и репутационных потерь, вызванных кибератаками и утечками конфиденциальных данных. Применение современных технологий шифрования, идентификации и биометрической аутентификации также играет важную роль в повышении защищенности интеллектуальной собственности, ноу-хау и других критически важных данных компаний. Сохранность этих ключевых активов является базовым условием для обеспечения долгосрочной конкурентоспособности промышленных предприятий. Использование технологий распределенного реестра (блокчейн) способствует повышению прозрачности и защищенности цепочек поставок, производственных операций и финансовых транзакций. Это позволяет эффективно противодействовать рискам мошенничества, подлога и несанкционированного вмешательства. Наконец, внедрение продвинутых аналитических решений на основе искусственного интеллекта обеспечивает непрерывный мониторинг угроз, раннее выявление аномалий и автоматизированное реагирование на кибератаки. Данные технологии способствуют значительному укреплению киберустойчивости предприятий и минимизации связанных с ней финансовых и операционных рисков. На основании изложенного можно говорить о том, что использование современных цифровых технологий оказывает многогранное позитивное влияние на повышение экономической безопасности промышленных предприятий. Цифровая трансформация производственных процессов, информационных систем и бизнес-моделей создает условия для укрепления рыночных позиций, финансовой устойчивости и долгосрочной конкурентоспособности компаний. Одновременно внедрение передовых решений в сфере кибербезопасности, криптографии и аналитики гарантирует надежную защиту ключевых активов и производственной деятельности, нейтрализуя растущие риски и угрозы [8].

Цифровая трансформация производственных процессов, систем управления и бизнес-моделей стремительно меняет ландшафт экономической безопасности современных промышленных предприятий. Для успешного противодействия новым вызовам и рискам компаниям необходимо разрабатывать и реализовывать комплексные стратегии внедрения передовых цифровых решений и инструментов. Ключевым элементом такой стратегии должно стать формирование всеобъемлющей системы управления информационной безопасностью (SIEM). Внедрение интегрированной SIEM-платформы обеспечит централизованный контроль и защиту критически важных информационных активов предприятия - корпоративной сетевой инфраструктуры, промышленных систем управления, баз данных и так далее. Использование продвинутой аналитики и технологий машинного обучения в

рамках таких систем позволит непрерывно выявлять и пресекать сложные кибератаки в режиме реального времени, сводя к минимуму связанные с ними финансовые и репутационные риски. Не менее важным направлением является повышение защищенности «умных» производственных систем и устройств промышленного интернета вещей. Для этого необходимо внедрять специализированные решения со встроенными механизмами шифрования, аутентификации, контроля доступа и обеспечения целостности. Применение технологий биометрической идентификации персонала также будет способствовать надежной защите критически важных производственных активов. Кроме того, использование аналитических систем на базе машинного обучения позволит выявлять аномалии и вторжения в промышленные сети. Также не менее важным элементом комплексной стратегии обеспечения экономической безопасности должна стать надежная защита конфиденциальной информации и критически важных данных предприятия. Это достигается за счет внедрения систем шифрования, многофакторной аутентификации и технологий распределенного реестра, обеспечивающих неизменность и прозрачность информации о производственных операциях, цепочках поставок и финансовых транзакциях [9]. Решения на основе искусственного интеллекта также позволят эффективно выявлять и предотвращать инсайдерские угрозы и хищение данных. Развитие аналитических и прогностических возможностей является еще одним ключевым направлением повышения экономической безопасности. Передовые аналитические системы, интегрирующие данные из различных источников, будут способствовать всестороннему анализу рисков и угроз. Применение технологий искусственного интеллекта и машинного обучения позволит прогнозировать, выявлять на ранней стадии и автоматизированно реагировать на инциденты информационной безопасности. При этом обучение персонала навыкам работы с аналитическими инструментами крайне важно для вовлечения сотрудников в процессы обеспечения кибербезопасности. Наконец, комплексный подход к управлению рисками и обеспечению непрерывности бизнеса является неотъемлемой частью надежной системы экономической безопасности предприятия. Разработка актуальной стратегии управления рисками, внедрение систем резервирования и восстановления критически важных систем, а также регулярное тестирование сценариев реагирования на чрезвычайные ситуации позволят минимизировать негативное влияние возникающих угроз [10]. Комплексная реализация данных рекомендаций позволит промышленным предприятиям сформировать высокоэффективную систему обеспечения экономической безопасности на основе передовых цифровых технологий. Это, в свою очередь, станет фундаментом для устойчивого развития бизнеса, повышения конкурентоспособности и долгосрочной финансовой стабильности компаний в условиях стремительно меняющихся рисков и угроз цифровой эпохи.

Выводы

Предложенные рекомендации по внедрению и эффективному использованию передовых цифровых технологий в целях обеспечения экономической безопасности промышленных предприятий имеют высокую практическую значимость и широкие перспективы применения как на уровне отдельных компаний, так и в масштабах целых отраслей и промышленности в целом. На уровне отдельных предприятий комплексная реализация данных подходов позволит сформировать надежную защиту критически важных информационных активов, производственных процессов и финансово-хозяйственной деятельности. Внедрение интегрированных SIEM-платформ, специализированных решений для «умных» производственных систем, систем шифрования и биометрической идентификации персонала обеспечит высокую степень киберустойчивости компании и минимизацию рисков финансовых и репутационных потерь. Применение передовых аналитических инструментов на основе искусственного интеллекта и машинного обучения позволит предприятиям проводить всесторонний мониторинг рисков, осуществлять раннее выявление аномалий и автоматизированное реагирование на инциденты информационной безопасности. Это существенно повысит эффективность и оперативность управления экономической безопасностью в условиях постоянно растущих киберугроз. Реализация комплексного подхода к управлению рисками и обеспечению непрерывности бизнеса, включающая внедрение систем резервирования и восстановления, а также регулярное тестирование сценариев реагирования, станет прочным фундаментом для устойчивого развития предприятий в долгосрочной перспективе. На уровне отраслевых сообществ и промышленности в целом предлагаемые решения обладают высоким потенциалом для тиражирования и масштабирования. Разработка отраслевых стандартов и рекомендаций по внедрению передовых цифровых инструментов обеспечения экономической безопасности позволит сформировать целостную систему защиты от киберугроз в рамках всей производственной экосистемы. Кроме того, создание совместных центров мониторинга, анализа и реагирования на инциденты информационной безопасности, объединяющих усилия ключевых игроков отрасли, обеспечит синергетический эффект и повысит общий уровень киберустойчивости промышленности. Это также будет способствовать обмену передовым опытом и лучшими практиками в данной сфере. Таким образом, практическая реализация комплексного подхода к цифровизации экономической безопасности промышленных предприятий может осуществляться на нескольких уровнях: от внедрения передовых решений в рамках отдельных компаний до разработки и внедрения отраслевых стандартов и совместных инициатив. Это позволит сформировать надежную защиту ключевых активов, производственных процессов и финансово-хозяйственной деятельности, обеспечив устойчивое развитие промышленности в условиях нарастающих рисков цифровой трансформации.

Список литературы

1. Талерчик С.М., Зайцев А.А., Шаванов М.В. Обеспечение экономической безопасности в контексте устойчивого инновационного развития агропромышленного комплекса в регионах России // Фундаментальные исследования. 2021. № 2. С. 57-65. DOI 10.17513/fr.42966.

2. Кержина Ю.О., Вострикова Е.О. Устойчивое развитие как фактор экономической безопасности // Проблемы комплексной безопасности Каспийского макрорегиона: Материалы Международной научно-практической конференции, Астрахань, 27–28 октября 2022 года / Под общей редакцией А.П. Романовой, Д.А. Черничкина. Астрахань: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Астраханский государственный университет», 2022. С. 142-147.

3. Сигова М.В., Супатаев Т.М. Система экономической безопасности предприятий нефтегазовой отрасли, ее особенности и ориентация на цифровизацию, эффективность, конкурентоспособность и устойчивое развитие бизнеса // Ученые записки Международного банковского института. 2021. № 1(35). С. 98-117.

4. Измайлов М.К., Арбенина Е.А. Приоритетные направления снижения уровня теневого сектора экономики: зарубежный опыт и российская практика // Бизнес и дизайн ревю. 2022. № 4(28). С. 19-30. DOI 10.56565/25419951_2022_4_19.

5. Белоусов А.В. Об устойчивом развитии как основе экономической безопасности // Экономическая безопасность: правовые, экономические, экологические аспекты: сборник научных трудов 6-й Международной научно-практической конференции, Курск, 09 апреля 2021 года. Курск: Юго-Западный государственный университет, 2021. С. 46-50.

6. Харламова Е.Е., Кондакова Е.Е., Ермилова И.А. Устойчивое развитие промышленных предприятий Волгоградской области как основное направление экономической политики региона // Управление устойчивым развитием. 2021. № 2(33). С. 22-27.

7. Устинова Л.Н. Устойчивое развитие промышленных предприятий и комплексов в условиях внешних вызовов // Устойчивое развитие цифровой экономики и кластерных структур: теория и практика: монография / Санкт-Петербургский политехнический университет Петра Великого. Санкт-Петербург: Политех-Пресс, 2020. С. 341-362. DOI 10.18720/IEP/2020.8/14.

8. Громова Е.А., Кудряшов В.С. Концептуальная модель активного производства // Вестник Академии знаний. 2023. № 5(58). С. 136-138.

9. Имамвердиева М.И. Особенности устойчивого развития промышленных предприятий в условиях структурно-динамической трансформация экономики // Экономика, предпринимательство и право. 2021. Т. 11. № 9. С. 2133-2146. DOI 10.18334/epp.11.9.113455.

10. Кравченко В.А. Концептуальные основы устойчивого развития // Новое в экономической кибернетике. 2021. № 1. С. 219-227.

References

1. Talerchik S.M., Zajcev A.A., Shavanov M.V. Obespechenie e`konomicheskoj bezopasnosti v kontekste ustojchivogo innovacionnogo razvitiya agropromy`shlennogo kompleksa v regionax Rossii (Ensuring economic security in the context of sustainable innovative development of the agro-industrial complex in the regions of Russia), *Fundamental'ny`e issledovaniya*, 2021, no 2, pp. 57-65. DOI 10.17513/fr.42966.

2. Kerzhina Yu.O., Vostrikova E.O. Ustojchivoe razvitie kak faktor e`konomicheskoj bezopasnosti (Sustainable development as a factor in economic security), Problemy` kompleksnoj bezopasnosti Kaspijskogo makroregiona: Materialy` Mezhdunarodnoj nauchno-prakticheskoj

konferencii, Astraxan', 27–28 oktyabrya 2022 goda / Pod obshhej redakciej A.P. Romanovoj, D.A. CHernichkina. Astraxan': Federal'noe gosudarstvennoe byudzhetnoe obrazovatel'noe uchrezhdenie vy`sshego professional'nogo obrazovaniya «Astraxanskij gosudarstvenny`j universitet», 2022, pp. 142-147.

3. Sigova M.V., Supataev T.M. Sistema e`konomicheskoj bezopasnosti predpriyatij neftegazovoj otrasli, ee osobennosti i orientaciya na cifrovizaciyu, e`ffektivnost', konkurentosposobnost' i ustojchivoe razvitie biznesa (The system of economic security of enterprises in the oil and gas industry, its features and focus on digitalization, efficiency, competitiveness and sustainable business development), *Ucheny`e zapiski Mezhdunarodnogo bankovskogo instituta,* 2021, no 1(35), pp. 98-117.

4. Izmajlov M.K., Arbenina E.A. Prioritetny`e napravleniya snizheniya urovnya tenevogo sektora e`konomiki: zarubezhny`j opy`t i rossijskaya praktika (Priority areas for reducing the level of the shadow sector of the economy: foreign experience and Russian practice), *Biznes i dizajn revyu,* 2022, no 4(28), pp. 19-30. DOI 10.56565/25419951_2022_4_19.

5. Belousov A.V. Ob ustojchivom razvitii kak osnove e`konomicheskoj bezopasnosti (On Sustainable Development as the Basis of Economic Security), E`konomicheskaya bezopasnost': pravovy`e, e`konomicheskie, e`kologicheskie aspekty`: sbornik nauchny`x trudov 6-j Mezhdunarodnoj nauchno-prakticheskoj konferencii, Kursk, 09 aprelya 2021 goda. Kursk: Yugo-Zapadny`j gosudarstvenny`j universitet, 2021, pp. 46-50.

6. Xarlamova E.E., Kondakova E.E., Ermilova I.A. Ustojchivoe razvitie promy`shlenny`x predpriyatij Volgogradskoj oblasti kak osnovnoe napravlenie e`konomicheskoj politiki regiona (Sustainable Development of Industrial Enterprises in the Volgograd Region as the Main Direction of the Region's Economic Policy), *Upravlenie ustojchivy`m razvitiem*, 2021, no 2(33), pp. 22-27.

7. Ustinova L.N. Ustojchivoe razvitie promy`shlenny`x predpriyatij i kompleksov v usloviyax vneshnix vy`zovov (Sustainable Development of Industrial Enterprises and Complexes in the Context of External Challenges), Ustojchivoe razvitie cifrovoj e`konomiki i klasterny`x struktur: teoriya i praktika: monografiya / Sankt-Peterburgskij politexnicheskij universitet Petra Velikogo. Sankt-Peterburg: Politex-Press, 2020, pp. 341-362. DOI 10.18720/IEP/2020.8/14.

8. Gromova E.A., Kudryashov V.S. Konceptual'naya model' aktivnogo proizvodstva (Conceptual model of active production), *Vestnik Akademii znanij,* 2023, no 5(58), pp. 136-138.

9. Imamverdieva M.I. Osobennosti ustojchivogo razvitiya promy`shlenny`x predpriyatij v usloviyax strukturno-dinamicheskoj transformaciya e`konomiki (Features of sustainable development of industrial enterprises in the context of structural and dynamic transformation of the economy), *E`konomika, predprinimatel'stvo i pravo*, 2021, Vol. 11, no 9, pp. 2133-2146. DOI 10.18334/epp.11.9.113455.

10. Kravchenko V.A. Konceptual'ny`e osnovy` ustojchivogo razvitiya (Conceptual foundations of sustainable development), *Novoe v e`konomicheskoj kibernetike*, 2021, no 1, pp. 219-227.

Статья поступила в редакцию 02.09.2024