Научно-технические ведомости СПбГПУ. Экономические науки. 2021, Том 14, № 6. С. 78–88.
St. Petersburg State Polytechnical University Journal. Economics. 2021, Vol. 14, No. 6. Pp. 78–88.

Экономика и менеджмент предприятия
Economy and management of the enterprise

Научная статья
УДК 338.28
DOI: https://doi.org/10.18721/JE.14606

ФОРМИРОВАНИЕ НАПРАВЛЕНИЙ СОВЕРШЕНСТВОВАНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

А.В. Бабкин[1,2], А.С. Лошаков[3] ✉

[1] Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербург, Российская Федерация;

[2] Псковский государственный университет, г. Псков, Российская Федерация;

[3] Московский университет МВД России имени В.Я. Кикотя, Москва, Российская Федерация

✉ Loshakov@inbox.ru

Аннотация. Цифровая трансформация – процесс перехода к цифровой экономике реализуемый как экономическими отраслями, так и отдельными предприятиями с целью получения конкурентных преимуществ. Хотя цифровая трансформация приносит новые возможности по повышению эффективности обеспечения безопасности предприятия, она также приводит и к возникновению новых угроз безопасности. Рассмотрены основные этапы системы обеспечения экономической безопасности предприятия (сбор и анализ информации; разработка, выбор и реализация мер обеспечения безопасности, контроль и совершенствование системы безопасности), перечислены угрозы экономической безопасности предприятия. Определены и проанализированы угрозы безопасности, отличающиеся степенью сформированности и последствиями воздействия. Изучены проблемы, возникающие при противодействии этим угрозам. Предлагается в рамках цифровой трансформации создание и внедрение информационных технологий устойчивых к киберугрозам, а также развитие механизмов обнаружения, предупреждения угроз с ликвидацией последствий их проявления. Сделан вывод о необходимости интеграции системы обеспечения безопасности предприятия в структуру деятельности самого предприятия путем выстраивания интегрированной системы сбора, передачи и анализа показателей деятельности предприятия, динамики внутренних и внешних угроз, ситуации на рынке и т.д. по цифровым каналам с целью использования данной информации для повышения уровня экономической безопасности предприятия. Экономическая безопасность максимально эффективна при цифровой трансформации всего предприятия, а не только системы обеспечения экономической безопасности предприятия. С целью повышения ее эффективности по минимизации (устранению) угроз определены приоритетные направления совершенствования системы обеспечения экономической безопасности предприятия: учет специфических факторов деятельности организации, активное использование предупредительных мер, координация деятельности службы безопасности и правоохранительных органов; расчет экономической целесообразности (эффективности) противодействия вызовам и угрозам, профессиональный аудит безопасности, экономический анализ реализации цифровых проектов в области обеспечения экономической безопасности.

Ключевые слова: угроза, противодействие, система экономической безопасности, направления совершенствования, повышение эффективности, цифровая трансформация

Для цитирования: Бабкин А.В., Лошаков А.С. Формирование направлений совершенствования экономической безопасности предприятия в условиях цифровой трансформации // Научно-технические ведомости СПбГПУ. Экономические науки. 2021. Т. 14, № 6. С. 78–88. DOI: https://doi.org/10.18721/JE.14606

Scientific article
DOI: https://doi.org/10.18721/JE.14606

WAYS TO IMPROVE ENTERPRISE ECONOMIC SECURITY IN THE CONDITIONS OF DIGITAL TRANSFORMATION

A.V. Babkin[1,2], A.S. Loshakov[3] ✉

[1] Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russian Federation;

[2] Pskov State University, Pskov, Russian Federation;

[3] Moscow University of the Ministry of Internal affairs of Russia named after V.Ya. Kikot, Moscow, Russian Federation

✉ Loshakov@inbox.ru

Abstract. Digital transformation is the process of transition to a digital economy implemented by both economic sectors and individual enterprises in order to gain competitive advantages. Although digital transformation brings about new opportunities to improve the efficiency of enterprise security, it also leads to the emergence of new security threats. The main stages of the enterprise's economic security system are considered (collection and analysis of information; development, selection and implementation of security measures, control and improvement of the security system), threats to the economic security of the enterprise are listed. Security threats, differing in the degree of formation and consequences of exposure are identified and analyzed. The problems arising in countering these threats have been studied. Within the framework of digital transformation, it is proposed to create and implement information technologies resistant to cyber threats, as well as develop mechanisms for detecting and preventing threats with the elimination of the consequences of their manifestation. The conclusions show that it is necessary to integrate the enterprise security system into the structure of the enterprise itself by building an integrated system for collecting, transmitting and analyzing enterprise performance indicators, dynamics of internal and external threats, market situation, etc. through digital channels in order to use this information to increase the level of economic security of the enterprise. Economic security is most effective in the digital transformation of the entire enterprise, and not just the economic security system of the enterprise. In order to increase its effectiveness in minimizing (eliminating) threats, priority directions for improving the economic security system of the enterprise have been identified. They include taking into account specific factors of the organization's activity, active use of preventive measures, coordination of the activities of the security service and law enforcement agencies, calculation of the economic feasibility (effectiveness) of countering challenges and threats, professional security audit, economic analysis of the implementation of digital projects in the field of economic security.

Keywords: threat, counteraction, economic security system, improvement directions, efficiency improvement, digital transformation

Citation: A.V. Babkin, A.S. Loshakov, Ways to improve enterprise economic security in the conditions of digital transformation, St. Petersburg State Polytechnical University Journal. Economics, 14 (6) (2021) 78–88. DOI: https://doi.org/10.18721/JE.14606

Введение

Развитие предприятия невозможно без знания достоверной, точной информации о его текущем экономическом состоянии, ситуации на рынке, конкурентных преимуществах с последующим анализом этой информации для прогнозирования угроз, определения степени их воздействия на бизнес с последующей выработкой мер противодействия. Все перечисленное осуществляется в создаваемой на предприятии системе обеспечения экономической безопасности. Данная система учитывает при обеспечении безопасности существенные структурные элементы

и связи между ними, организационную структуру управления, функцию и задачу каждого элемента; позволяет учесть будущую динамику угроз с целью прогнозирования и адаптации к ним деятельности предприятия. Помимо этого, функционально система безопасности зависит от типа деятельности, выпускаемой продукции или оказываемых услуг, а также уровня цифровой трансформации, определяющего особенности ведения бизнеса и экономическую эффективность бизнес процессов.

Цифровая трансформация в общем виде – работа сотрудников с использованием компьютерной техники (тренды с облачными технологиями, социальные сети, искусственный интеллект), при этом степень цифровой трансформации отличается от «цифровой обертки» (многие пытаются быть похожи на цифровой бизнес, ведь капитализация цифровых компаний растет быстрее «традиционных») до «полностью цифровой» вследствие преобразования структуры, процессов производства, продажи продукции и бизнес-модели предприятия. Цифровая трансформация неизбежна для компаний, стремящихся остаться на конкурентном рынке и затрагивает такие сферы деятельности предприятия, как работу с клиентами, работу сотрудников внутри предприятия, процессы производства (оказания услуг).

Цифровая трансформация меняет состав и структуру угроз: растут информационные угрозы, что усложняет деятельность службы безопасности предприятия в контексте необходимости повышения квалификации сотрудников, уровня технической базы и подходов к аналитической обработки данных для прогнозирования вариантов развития угроз, оптимизации деятельности службы безопасности предприятия по противодействию угрозам и т.д.

В работе Хачатурян М.В. [1] проводит анализ внедрения современных цифровых технологий, отмечая что значительное число российских организаций включает в свои стратегические планы цели цифровизации управления бизнес-процессов, но при этом лишь ограниченное число менеджеров и собственников как в России, так и в мире имеют четкое представление о том, как вести цифровую трансформацию и как управлять связанными с нею рисками. Коломыцева О.Ю., Плотников В.А. говорят об обеспечении экономической безопасности предприятия, которая сводится, по существу, к парированию угроз (совокупности условий и факторов, создающих прямую или косвенную возможность нанесения ущерба экономическим интересам предприятия) [2, с. 78]. Теневую экономику, как угрозу экономической безопасности, рассматривает Литвиненко А.Н., Грачев А.В. и др. [3] В тоже время Пузыревский Л.С., Бабкин А.В. показывают, что теневые практики хозяйствования не только деструктивно воздействуют на безопасность предприятий, но и реализуют функции по их защите, рассматривают различные формы реализации теневой экономикой функций безопасности [4].

Вопросы обеспечения экономической безопасности предприятия приобретают все большую значимость в связи с неустойчивыми динамичными тенденциями, событиями в современном мире, появлением новых вызовов и угроз при переходе к цифровой экономике.

Таким образом, помимо состава и структуры угроз, цифровая трансформация изменяет саму деятельность по обеспечению экономической безопасности предприятия и по ряду направлений упрощая работу и высвобождая ресурсы.

Перечисленные факторы обуславливают необходимость проведения дополнительных исследований по изучению и формированию направлений совершенствования экономической безопасности предприятия в условиях цифровой трансформации, что представляет собой актуальную научную задачу.

Объектом исследования являются предприятия среднего и крупного бизнеса, занимающиеся производством продукции (оказанием услуг) в условиях цифровизации экономики.

В качестве *предмета исследования* выступает система обеспечения экономической безопасности предприятия в условиях цифровой трансформации.

Литературный обзор

Теоретический анализ сущности и содержания категории «экономическая безопасность» проводит Ю.В. Быковская. [5] Структуру экономической безопасности по уровням (организационная структура) и видам (функциональная структура) рассматривает Кузнецова Е.И. [6, с. 24]. Разбирая сектор финансовых учреждений Дианов Д.В., дает прогноз материального ущерба от противоправных действий в банковском секторе и сфере страхования, который позволяет смоделировать ряд мероприятий по недопущению ухудшения экономической обстановки, а также меры активного противодействия существующим угрозам. [7] Бобошко В.И. проводит анализ рентабельности активов, являющихся инструментом обеспечения безопасности предприятия, так как позволяет определить оптимальные методы применения ресурсов и сформировать структуру средств предприятия, а также выявить резервы увеличения прибыли, что будет способствовать устойчивому выходу на новый уровень экономического развития предприятия. [8, с. 329]

Клычова Г.С., Закирова А.Р. раскрывают методологический инструментарий обеспечения экономической безопасности в системе управления персоналом предприятий. [9]

Васильев Д.В., Кравец Е.Г. обосновывают использование технологии больших данных для борьбы с экономическими преступлениями в топливно-энергетическом комплексе. Интеллектуальный мониторинг нефтепродуктов создает условия для предотвращения преступлений в топливно-энергетическом комплексе, повышая тем самым уровень экономической безопасности предприятия. [10] Бабкин А.В. рассматривает возможность оценки уровня экономической безопасности предприятия через экономический потенциал предприятия, включающего производственную структуру, уровень техники и технологии производства, другие показатели. [11, с. 125]

Суглобов А.Е., Кузьмина Т.И. изучают эффективность представления российской государственной поддержки для поддержания экономической безопасности малого и среднего бизнеса в условиях пандемии COVID-19. Основываясь на статистических данных и экономических фактах, ими было подтверждено, что государственная поддержка, оказанная в условиях пандемии, оказалась небольшой и недостаточной. [12, с. 1]

Проведенный анализ публикаций показал, что многие вопросы в области обеспечения экономической безопасности предприятия изучены. Однако, в литературе недостаточно освещены вопросы совершенствования обеспечения экономической безопасности предприятия в условиях цифровой трансформации, что обуславливает необходимость формирования направлений повышения экономической безопасности и позволяет сформулировать цель и задачи исследования.

Цель и задачи исследования

Цель исследования – формирование направлений совершенствования экономической безопасности предприятия в условиях цифровой трансформации за счет поиска и создания условий для поступательного развития предприятия за счет выстраивания эффективной системы экономической безопасности предприятия позволяющей своевременно выявлять угрозы; их устранять; целесообразно использовать потенциал, сохранять и высвобождать ресурсы в условиях цифровой трансформации.

Задачи исследования:

– оценка ситуации в области обеспечения экономической безопасности предприятия в современных условиях;

– определение и анализ угроз, вызывающих наибольшие сложности в развитии предприятия в условиях цифровой трансформации;

– оценка возможности использования цифровизации в обеспечении экономической безопасности предприятия, находящегося в процессе цифровой трансформации.

Методы исследования

Использовались общенаучные методы как научная абстракция, обобщение, синтез, а также специальные и другие методы научного исследования.

Сбор информации по тенденциям, факторам и условиям цифровизации в развитых странах свидетельствует о ее неоднозначном влиянии на предприятие (растет скорость принятия решений на основе «цифры», конкуренция), вызывая необходимость разработки методики, формирования инструментария выявления возникающих при этом рисков [13], угроз с целью их минимизации для последующего получения ожидаемых положительных результатов цифровизации.

Полученные результаты и обсуждение

Сегодня цифровая экономика опирается на сложную экосистему взаимосвязанных информационных и коммуникационных технологий, основанную на обработке «больших данных», обеспечиваемых сложным аналитическим инструментарием. В такой многоуровневой взаимозависимой структуре существуют риски, представляющие собой проблему многостороннего характера. То, что происходит в малом бизнесе, может оказать влияние на крупный бизнес и всех участников цепочки создания стоимости. Верно и обратное: системный сбой в цифровой системе страны поставит под угрозу существование отдельных предприятий, банков, организаций государственного сектора. [14, с. 95]

С целью снижения уровня этих угроз выстраивается на двух уровнях система обеспечения экономической безопасности предприятия:

– на макроуровне экономическая безопасность обеспечивается государством за счет общей организации деятельности субъектов в области экономической безопасности (законодательной, исполнительной власти, правоохранительных органов, общественных организаций и т.д.). Наличие этого уровня следует из того что не всем угрозам может противостоять система обеспечения экономической безопасности организации, и поэтому государство участвует в этом процессе, помогая организациям и противодействуя части угроз (снижая уровень коррупции, криминализацию, экономическую нестабильность, а также формирует благоприятную для предпринимательства институциональную среду и др.);

– на уровне предприятия экономическая безопасность обеспечивается самой организацией за счет работы службы безопасности, привлечения охранных подразделений и т.д. Система функционирует в рамках разработанной и принятой Концепции безопасности предприятия (как правило крупный бизнес принимает такой документ), с учетом стратегических целей, конкурентных преимуществ, угроз экономической безопасности, срока их воздействия и возможности предотвращения и др. особенностей деятельности.

На рис. 1 представлены этапы развития системы обеспечения экономической безопасности предприятия.

Представленные на рисунке этапы позволяют формировать достаточно эффективную систему обеспечения экономической безопасности предприятия, снижающую величину угроз, способствуя достижению предприятием поставленных стратегических целей при успешном функционировании в нестабильных условиях внешней и внутренней среды.

При построении системы безопасности необходимо определить приемлемый уровень риска, как с точки зрения его управляемости и предсказуемости, так и возможных последствий его реализации. [15, с. 313]

В результате цифровой трансформации меняется стиль работы (становится цифровым), повышается адаптивность предприятия к внешним вызовам и угрозам с обеспечением гибкости технологических операций. Конечно руководство предприятия должно осознанной перейти на этот уровень, прогнозируя особенности будущей деятельности с расчетом окупаемости вложений. [16] Возможен переход на цифровую базу (IT-решения), без повышения эффективности, что только

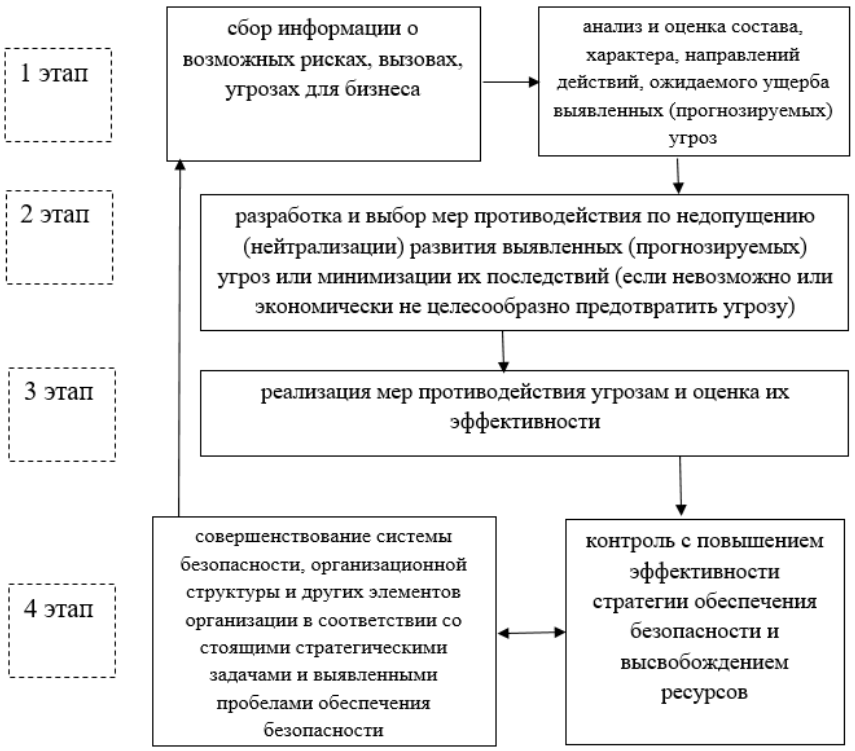

Рис. 1. Этапы развития системы обеспечения экономической безопасности предприятия
Fig. 1. Stages of the enterprise's economic security system

снижает рентабельность (предприятие покупает и внедряет IT-системы, как лидеры отрасли, но при этом не получает ожидаемого результата). [17, 18] При обеспечении безопасности IT-решения могут применяться для борьбы с киберугрозами, для анализа поведения потенциальных преступников, террористов и самоубийц (например, система искусственного интеллекта VaakEye), для разработки центров данных, приложений для эффективной работы, системных решений.

В системе безопасности за каждым должностным лицом закреплены свои функциональные обязанности. Не детализируя их по должностным уровням (регламентам) и учитывая, что трудно (не всегда возможно и экономически целесообразно) все защитить, безопасность ключевых направлений деятельности от реальных угроз осуществляется с помощью следующих направлений деятельности по обеспечению безопасности:

– сбора информации и проверки контрагентов;
– анализа деятельности конкурентов;
– реализации профилактических мероприятий по недопущению возникновения угроз;
– контроля за работой подчиненных сотрудников, включая проведение служебных проверок и внутренних расследований;
– противодействия экономическим преступлениям;
– взаимодействия с правоохранительными органами [19, 20].

Вышеперечисленные направления деятельности системы безопасности позволяют предотвращать угрозы и негативные воздействия, улучшая текущие показатели работы предприятия. Отметим, что для предприятий различных сфер деятельности будут актуальными различные угрозы, отличающиеся степенью сформированности и последствиями воздействия. Общим является то, что на первое место среди угроз безопасности выходят информационные угрозы (кибератаки, по-

хищение конфиденциальной информации, финансовых активов и др.), делающие предприятие уязвимым и вызывающие необходимость в рамках цифровой трансформации создания и внедрения информационных технологий устойчивых к киберугрозам, а также развитие механизмов обнаружения, предупреждения информационных угроз с ликвидацией последствий их проявления.

Проблемы противодействии угрозам на уровне предприятия вызваны:

– пробелами организационного характера, допущенными при планировании и создании целостной системы (комплексной программы) обеспечения безопасности предприятия;

– не верно определенным горизонтом планирования для выбранной бизнес-модели (слабый уровень планирования и прогнозирования при недостаточной компетентности сотрудников);

– ограниченностью располагаемых ресурсов, не позволяющей точно прогнозировать возникновение новых угроз;

– чрезмерными расходами на безопасность в результате отсутствия оценки экономической эффективности мер обеспечения безопасности;

– слабой степенью координации (согласованности) между структурными подразделениями предприятия, сторонними организациями при обеспечении безопасности;

– ошибочно определенными критериями цифровой трансформации с целью достижения «цифровой зрелости».

Для устранения данных проблем авторами на основе проведенных исследований разработаны направления совершенствования системы обеспечения экономической безопасности предприятия:

– учет в системе безопасности специфических технологических, финансовых, организационно-управленческих, кадровых факторов деятельности организации;

– использование предупредительных мер направленных на прогнозирование угроз, адаптацию деятельности предприятия к изменениям во внутренней и внешней среде;

– координации деятельности (объединения усилий) службы безопасности и правоохранительных органов с целью снижения уровня угроз и эффективного противодействия существующим угрозам;

– расчета экономической целесообразности противодействия вызовам и угрозам;

– профессионального аудита безопасности, направленного на ликвидацию просчетов в обеспечении безопасности;

– просчитывание и реализация цифровых проектов в области обеспечения экономической безопасности (при этом отсутствует уверенность в «правильном» подходе и велика вероятность ошибки);

– активизации деятельности «агентов трансформации».

Крупной компании достаточно тяжело перестроить работающий бизнес-процесс, ведь в них работают сотрудники с разным возрастом, опытом, культурой. [21] Как правило, реализация цифровой трансформации осуществляется нелегко. Необходимо вовлечение сотрудников с поиском мотива для принятия цифровых проектов. Одним из мотивов является сравнение с лидерами отрасли, вызывающим у сотрудников соревновательные стремления.

Развитие информационных технологий способствовало за счет новых возможностей появлению на мировом и региональном рынке компаний (например, Oracle, Ebay, PayPal, Badoo, Telegram и др.) с новыми моделями бизнеса (по прошествии некоторого времени становящимися уже «традиционными») [22], постоянно развивающими технологическую составляющую и более конкурентоспособными по сравнению с классическими традиционными предприятиями.

Крайне сложно подвергнуть цифровой трансформации (практически невозможно) только систему экономической безопасности предприятия без всего предприятия в целом. В рамках стратегии цифровой трансформации необходима оценка эффективности бизнес-модели и предполагаемые изменения в рамках цифровой трансформации с ожидаемыми результатами (целе-

выми показателями). Расчет бюджета новых бизнес-моделей, цифровых преобразований с учетом окупаемости позволяет принять обоснованное решение о начале цифровой трансформации предприятия (Концепцию цифрового предприятия, стратегию ведения бизнеса (цифровых продуктов) с формированием цифровой структуры, цифровой культуры с управлением процессом трансформации) с разработкой дорожной карты трансформации.

Комплексное решение указанных проблем с учетом предлагаемых рекомендаций позволит повысить экономическую безопасность предприятия, показатели уставной деятельности и, в конечном итоге, его конкурентоспособность.

Заключение

Подводя итоги, отметим, что происходит распространение цифровых технологий во всех сферах деятельности человека, и обеспечение экономической безопасности предприятия не стало исключением. Внедряются модели и средства обеспечения безопасности с элементами искусственного интеллекта, направленные на повышения уровня обеспечения экономической безопасности предприятия, вызывая необходимость анализа и оптимизации этой деятельности.

В рамках исследования получены следующие результаты:

1. При оценке ситуации в области обеспечения экономической безопасности, выявлены проблемы организационного и управленческого характера, возникающие в системе экономической безопасности предприятия. Закреплены практические основы по разработке системы экономической безопасности предприятия, описан комплексный подход по функционированию системы экономической безопасности предприятия в условиях цифровой трансформации.

2. Определены и проанализированы угрозы безопасности, отличающиеся степенью сформированности и последствиями воздействия и вызывающие наибольшие сложности в развитии предприятия в условиях цифровой трансформации: на первое место среди угроз безопасности выходят информационные угрозы (кибератаки, похищение конфиденциальной информации, финансовых активов и др.), приводящие к потере, искажению или разглашению конфиденциальной информации, в итоге делающие предприятие уязвимым. Возникает необходимость в рамках цифровой трансформации создания и внедрения информационных технологий устойчивых к киберугрозам, а также развитие механизмов обнаружения, предупреждения информационных угроз с ликвидацией последствий их проявления.

3. Определены факторы, влияющие на эффективный выбор реализации цифровой трансформации на предприятии. Обоснована необходимость интеграции (включения) направлений деятельности предприятия по обеспечению безопасности между собой, с другими функциональными направлениями деятельности с целью выстраивания интегративной системы собирающей, передающей, анализирующей данные по цифровым каналам (о ситуации на рынке, предпочтениях клиентов и т.д.), что позволяет повысить эффективность и соответственно конкурентоспособность предприятия. Данная деятельность может осуществляется в рамках созданного на предприятии специализированного программного продукта, включающего в себя цифровые сервисы как для сотрудников по обеспечению безопасности в направлении интеграции, включая цифровизацию.

4. Предложены направления совершенствования экономической безопасности предприятия в условиях цифровой трансформации: учет факторов деятельности организации, использование предупредительных мер, координация деятельности службы безопасности и правоохранительных органов; расчет экономической целесообразности (эффективности) противодействия вызовам и угрозам, профессиональный аудит безопасности, экономический анализ реализации цифровых проектов в области обеспечения экономической безопасности, активизация деятельности «агентов трансформации».

Направления дальнейших исследований

В статье рассматривается обеспечение экономической безопасности в условиях цифровой трансформации предприятия с позиции среднего и крупного бизнеса. Для этих предприятий необходимы дальнейшие исследования по изучению типичных ошибок, допускаемых компаниями при обеспечении безопасности в условиях цифровой трансформации с целью минимизации ущерба.

СПИСОК ИСТОЧНИКОВ

1. **Хачатурян М.В.** Особенности управления рисками цифровой трансформации бизнес-процессов организации в условиях пандемии // Креативная экономика. 2021. Т. 15. № 1. С. 45–58.

2. **Коломыцева О.Ю., Плотников В.А.** Специфика обеспечения экономической безопасности предприятия в условиях цифровизации экономики // Известия Санкт-Петербургского государственного экономического университета. 2019. № 5-1 (119). С. 75–83.

3. **Litvinenko A.N., Grachev A.V., Titov V.A., Guzikova L.A.** Shadow economy-threat and factor of economic security // ACM International Conference Proceeding Series. Proceedings Papers – 3rd International Scientific and Practical Conference, DEFIN 2020.

4. **Грачев А.В., Пузыревский Л.С., Бабкин А.В.** Теневая экономика как инструмент обеспечения экономической безопасности хозяйствующих субъектов // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2011. № 3 (125). С. 214–218.

5. **Быковская Ю.В.** Теоретический анализ сущности и содержания категории «экономическая безопасность»: отечественный и зарубежный опыт проведения исследований // Мировая экономика. Проблемы безопасности. 2020. № 2. С. 108–113.

6. **Кузнецова Е.И.** Теория экономической безопасности в эволюционном развитии современной науки // Экономическая безопасность. 2018. № 1. С. 21–27.

7. **Дианов Д.В.** Статистический очерк по экономической безопасности финансово-кредитных организаций // Вестник Московского университета МВД России. 2021. № 4. С. 272–279.

8. **Бобошко В.И.** Анализ рентабельности активов предприятия как инструмента обеспечения экономической безопасности хозяйствующего субъекта // Вестник Московского университета МВД России. 2021. № 3. С. 328–334.

9. **Klychova G., Zakirova A., Klychova A., Zalyalova N., Dyatlova A., Zaugarova E.** Methodological tools to ensure economic security in the personnel management system of enterprises // В сборнике: E3S Web of Conferences. Innovative Technologies in Environmental Science and Education, ITESE 2019. С. 04008.

10. **Vasilev D.V., Kravets E.G., Naumov Yu.G., Bulgakova E.V., Bulgakov V.G.** Analysis of the data used at oppugnancy of crime in the oil and gas industry // Studies in Systems, Decision and Control. 2019. Т. 181. С. 249–258.

11. **Suglobov A., Kuzmina T., Bessonova E., Bank S., Nabiyeva A.** Economic security strategy for managing and supporting businesses in the context of the COVID-19 // Academy of Strategic Management Journal. 2021. Т. 20. № 6. С. 1–8.

12. **Бабкин А.В.** О соотношении понятий «экономическая безопасность» и «экономический потенциал» // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2013. № 4 (175). С. 121–127.

13. **Avdiysky V.I., Bezdenezhnykh V.M., Lebedev I.A.** Risk in activities of organization as economic category // Espacios. 2018. Т. 39. № 34.

14. **Чечин О.П.** Цифровая трансформация в концепции экономической безопасности // Экономические науки. 2019. № 176. С. 92–97.

15. **Свирина М.В., Чернецова Ю.А.** Система экономической безопасности страны в условиях цифровой экономики // Вестник экономической безопасности. 2020. № 3. С. 311–313.

16. **Bolshakova L.V., Litvinenko A.N., Baturina E.V., Sidenko I.K., Ivanov A.N., Dali F.A., Shidlovsky G.L.** Application of the econometric model as a mechanism of management of socio-economic systems IIOAB Journal. 2020. Т. 11. № S3. С. 64–71.

17. **Bezdenezhnykh V.M., Karanina E.V., Yartseva N.M.** The problems of using intellectual property as a tool of growth of national economy's competitiveness // International Journal of Economic Policy in Emerging Economies. 2020. Т. 13. № 5. С. 443–452.

18. **Агапова Т.Н., Борисова Е.В., Бобошко Н.М., Дианов Д.В., Долбилов А.В., Иванов А.В. и др.** Применение информационных технологий в экономическом анализе. – М.: Перо, 2020. – 152 с.

19. **Егорова Е.В.** Внутренний контроль как инструмент обеспечения экономической безопасности хозяйствующего субъекта // Сборник научных трудов: Актуальные проблемы обеспечения экономической безопасности. – М.: Научный консультант, 2016. С. 29–34.

20. **Коноваленко С.А., Трофимов М.Н.** Особенности документального исследования специалистами-ревизорами в рамках реализации ст.160 УК РФ «Присвоение и растрата» // Криминологический журнал. 2021. № 1. С. 121–126.

21. **Лошаков А.С.** Актуальные направления повышения производительности труда в современной России // Вестник Московского финансово-юридического университета. 2020. № 2. С. 75–83.

22. **Скляренко Р.П.** Структура рынка наукоемкой продукции // Вестник Московского гуманитарно-экономического института. 2017. № 3. С. 65–76.

REFERENCES

1. **M.V. Khachaturyan,** Osobennosti upravleniya riskami tsifrovoy transformatsii biznes-protsessov organizatsii v usloviyakh pandemii // Kreativnaya ekonomika. 2021. T. 15. № 1. S. 45–58.

2. **O.Yu. Kolomytseva, V.A. Plotnikov,** Spetsifika obespecheniya ekonomicheskoy bezopasnosti predpriyatiya v usloviyakh tsifrovizatsii ekonomiki // Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta. 2019. № 5-1 (119). S. 75–83.

3. **A.N. Litvinenko, A.V. Grachev, V.A. Titov, L.A. Guzikova,** Shadow economy-threat and factor of economic security // ACM International Conference Proceeding Series. Proceedings Papers – 3rd International Scientific and Practical Conference, DEFIN 2020

4. **A.V. Grachev, L.S. Puzyrevskiy, A.V. Babkin,** Tenevaya ekonomika kak instrument obespecheniya ekonomicheskoy bezopasnosti khozyaystvuyushchikh subyektov // Nauchno-tekhnicheskiye vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Ekonomicheskiye nauki. 2011. № 3 (125). S. 214–218.

5. **Yu.V. Bykovskaya,** Teoreticheskiy analiz sushchnosti i soderzhaniya kategorii «ekonomicheskaya bezopasnost»: otechestvennyy i zarubezhnyy opyt provedeniya issledovaniy // Mirovaya ekonomika. Problemy bezopasnosti. 2020. № 2. S. 108–113.

6. **Ye.I. Kuznetsova,** Teoriya ekonomicheskoy bezopasnosti v evolyutsionnom razvitii sovremennoy nauki // Ekonomicheskaya bezopasnost. 2018. № 1. S. 21–27.

7. **D.V. Dianov,** Statisticheskiy ocherk po ekonomicheskoy bezopasnosti finansovo-kreditnykh organizatsiy // Vestnik Moskovskogo universiteta MVD Rossii. 2021. № 4. S. 272–279.

8. **V.I. Boboshko,** Analiz rentabelnosti aktivov predpriyatiya kak instrumenta obespecheniya ekonomicheskoy bezopasnosti khozyaystvuyushchego subyekta // Vestnik Moskovskogo universiteta MVD Rossii. 2021. № 3. S. 328–334.

9. **G. Klychova, A. Zakirova, A. Klychova, N. Zalyalova, A. Dyatlova, E. Zaugarova,** Methodological tools to ensure economic security in the personnel management system of enterprises // V sbornike: E3S Web of Conferences. Innovative Technologies in Environmental Science and Education, ITESE 2019. S. 04008.

10. **D.V. Vasilev, E.G. Kravets, Yu.G. Naumov, E.V. Bulgakova, V.G. Bulgakov,** Analysis of the data used at oppugnancy of crime in the oil and gas industry // Studies in Systems, Decision and Control. 2019. T. 181. S. 249–258.

11. **A. Suglobov, T. Kuzmina, E. Bessonova, S. Bank, A. Nabiyeva,** Economic security strategy for managing and supporting businesses in the context of the COVID-19 // Academy of Strategic Management Journal. 2021. T. 20. № 6. S. 1–8.

12. **A.V. Babkin,** O sootnoshenii ponyatiy «ekonomicheskaya bezopasnost» i «ekonomicheskiy potentsial» // Nauchno-tekhnicheskiye vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Ekonomicheskiye nauki. 2013. № 4 (175). S. 121–127.

13. **V.I. Avdiysky, V.M. Bezdenezhnykh, I.A. Lebedev,** Risk in activities of organization as economic category // Espacios. 2018. T. 39. № 34.

14. **O.P. Chechin,** Tsifrovaya transformatsiya v kontseptsii ekonomicheskoy bezopasnosti // Ekonomicheskiye nauki. 2019. № 176. S. 92–97.

15. **M.V. Svirina, Yu.A. Chernetsova,** Sistema ekonomicheskoy bezopasnosti strany v usloviyakh tsifrovoy ekonomiki // Vestnik ekonomicheskoy bezopasnosti. 2020. № 3. S. 311–313.

16. **L.V. Bolshakova, A.N. Litvinenko, E.V. Baturina, I.K. Sidenko, A.N. Ivanov, F.A. Dali, G.L. Shidlovsky,** Application of the econometric model as a mechanism of management of socio-economic systems IIOAB Journal. 2020. T. 11. № S3. S. 64–71.

17. **V.M. Bezdenezhnykh, E.V. Karanina, N.M. Yartseva,** The problems of using intellectual property as a tool of growth of national economy's competitiveness // International Journal of Economic Policy in Emerging Economies. 2020. T. 13. № 5. S. 443–452.

18. **T.N. Agapova, Ye.V. Borisova, N.M. Boboshko, D.V. Dianov, A.V. Dolbilov, A.V. Ivanov i dr.,** Primeneniye informatsionnykh tekhnologiy v ekonomicheskom analize. – M.: Pero, 2020. – 152 s.

19. **Ye.V. Yegorova,** Vnutrenniy kontrol kak instrument obespecheniya ekonomicheskoy bezopasnosti khozyaystvuyushchego subyekta // Sbornik nauchnykh trudov: Aktualnyye problemy obespecheniya ekonomicheskoy bezopasnosti. – M.: Nauchnyy konsultant, 2016. S. 29–34.

20. **S.A. Konovalenko, M.N. Trofimov,** Osobennosti dokumentalnogo issledovaniya spetsialistami-revizorami v ramkakh realizatsii st.160 UK RF «Prisvoyeniye i rastrata» // Kriminologicheskiy zhurnal. 2021 № 1. S. 121–126.

21. **A.S. Loshakov,** Aktualnyye napravleniya povysheniya proizvoditelnosti truda v sovremennoy Rossii // Vestnik Moskovskogo finansovo-yuridicheskogo universiteta. 2020. № 2. S. 75–83.

22. **R.P. Sklyarenko,** Struktura rynka naukoyemkoy produktsii // Vestnik Moskovskogo gumanitarno-ekonomicheskogo instituta. 2017. № 3. S. 65–76.

СВЕДЕНИЯ ОБ АВТОРАХ / THE AUTHORS

БАБКИН Александр Васильевич
E-mail: al-vas@mail.ru
BABKIN Aleksandr V.
E-mail: al-vas@mail.ru
ORCID: https://orcid.org/0000-0002-0941-6358

ЛОШАКОВ Андрей Сергеевич
E-mail: Loshakov@inbox.ru
LOSHAKOV Andrey S.
E-mail: Loshakov@inbox.ru
ORCID: https://orcid.org/0000-0002-8641-353X

Статья поступила в редакцию 28.10.2021; одобрена после рецензирования 05.12.2021; принята к публикации 14.12.2021.

The article was submitted 28.10.2021; approved after reviewing 05.12.2021; accepted for publication 14.12.2021.