DOI: 10.24412/1994-3776-2024-4-88-93 УДК: 658

М. К. Измайлов

ПРОБЛЕМЫ ФОРМИРОВАНИЯ ЦИФРОВОЙ СТРАТЕГИИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

M. Izmaylov. Problems of forming a digital strategy for industrial enterprises

Аннотация. Ускоряющаяся цифровая трансформация промышленности предъявляет все более высокие требования к предприятиям в части разработки и реализации эффективных цифровых стратегий. Проведенное исследование выявило ключевые проблемы, препятствующие успешному переходу промышленных компаний к новым технологическим решениям. Для преодоления этих вызовов исследованием предложены комплексные рекомендации, нацеленные на формирование четкой, интегрированной с бизнес-стратегией цифровой стратегии, развитие цифровых компетенций персонала, внедрение системы управления рисками, модернизацию ИТ-архитектуры на основе принципов информационной интеграции, а также обеспечение надежной защиты от киберугроз. Реализация этих мер позволит промышленным предприятиям успешно трансформировать бизнес-модели и упрочить конкурентные позиции в цифровую эпоху.

Ключевые слова: цифровая трансформация, промышленные предприятия, цифровая стратегия, компетенции, риски, кибербезопасность, информационная интеграция, конкурентоспособность.

Контактная информация: 195251, Санкт-Петербург, ул. Политехническая, д. 29; e-mail: izmajlov_mk@spbstu.ru

Abstract. The accelerating digital transformation of industry places increasingly high demands on enterprises to develop and implement effective digital strategies. The research has identified key challenges that hinder the successful transition of industrial companies to new technological solutions. To overcome these challenges, the study offers comprehensive recommendations aimed at forming a clear digital strategy integrated with business strategy, developing digital competencies of personnel, implementing a risk management system, modernizing IT architecture based on the principles of information integration, and ensuring reliable protection against cyber threats. The implementation of these measures will allow industrial enterprises to successfully transform business models and strengthen their competitive position in the digital era.

Keywords: digital transformation, industrial enterprises, digital strategy, competencies, risks, cybersecurity, information integration, competitiveness.

Contact information: 29 Polytechnicheskaya str., St. Petersburg, 195251; e-mail: izmajlov_mk@spbstu.ru

Стремительный переход к цифровым технологиям в промышленности оказывает существенное влияние на все аспекты деятельности современных предприятий. Цифровая трансформация производственных процессов, систем управления и бизнес-моделей создает новые возможности для повышения эффективности и конкурентоспособности, но в то же время порождает целый спектр рисков и угроз экономической безопасности. Обеспечение устойчивого развития промышленных предприятий в условиях нарастающих киберугроз и технологических вызовов становится ключевой задачей менеджмента. Несмотря на осознание важности цифровой трансформации, многие промышленные компании сталкиваются с существенными трудностями при разработке и реализации эффективной стратегии обеспечения экономической безопасности. Отсутствие целостного понимания

Измайлов Максим Кириллович - кандидат экономических наук, доцент Высшей школы производственного менеджмента Санкт-Петербургского политехнического университета Петра Великого

M. Izmaylov – Candidate of Economic Sciences, Associate Professor of Graduate School of Industrial Management of Peter the Great St. Petersburg Polytechnic University

взаимосвязей между цифровизацией, производственной эффективностью и комплексной защитой бизнеса тормозит внедрение необходимых технологических решений и организационных изменений. В работе предлагается комплексный подход к формированию цифровой стратегии промышленных предприятий, ключевым элементом которого является разработка и реализация действенных механизмов обеспечения экономической безопасности на основе передовых технологий. Исследуются взаимосвязи между цифровой трансформацией, повышением производственной эффективности и устойчивым развитием бизнеса в условиях нарастающих киберрисков. Предложенные в работе рекомендации по внедрению интегрированных систем управления информационной безопасностью, защите "умных" производственных систем, шифрованию конфиденциальных данных, развитию аналитических и прогностических возможностей, а также управлению рисками и обеспечению непрерывности бизнеса могут быть использованы руководителями и специалистами промышленных предприятий при разработке и реализации эффективных цифровых стратегий. Результаты исследования также представляют интерес для отраслевых ассоциаций и органов государственного управления в контексте повышения общей киберустойчивости промышленного сектора.

Цель исследования – разработка комплексного подхода к формированию цифровой стратегии промышленных предприятий, ориентированной на повышение их экономической безопасности и устойчивости в долгосрочной перспективе. В ходе исследования был проведен всесторонний анализ научных публикаций посвященных проблемам цифровизации промышленности и обеспечения ее экономической безопасности. Использовались методы системного анализа и сценарного моделирования для выявления ключевых взаимосвязей и закономерностей. Эмпирическую базу работы составили данные о внедрении передовых цифровых технологий на промышленных предприятиях, а также сведения об инцидентах информационной безопасности и их последствиях.

В последние годы проблемы формирования цифровой стратегии промышленных предприятий, с учетом требований обеспечения их экономической безопасности, активно исследуются отечественными учеными. Так, автор в работе «Цифровизация как фактор устойчивой деятельности промышленных предприятий» провел комплексный анализ рисков и угроз, возникающих в ходе цифровизации производственных процессов. Автором разработаны методические рекомендации по разработке и реализации стратегий информационной безопасности в контексте цифровой трансформации промышленности [3]. Устинова О.Е. в статье «Формирование стратегии цифровой трансформации промышленных предприятий» исследует влияние внедрения «умных» производственных систем, промышленного интернета вещей и других цифровых технологий на комплексную защиту бизнеса. Предложены подходы к формированию системы раннего выявления и предупреждения киберугроз на предприятиях [14]. Особое внимание вопросам разработки цифровых стратегий промышленных предприятий с учетом требований экономической безопасности уделяется в работах О. О. Джиоевой, О. М. Танделовой, С. В. Галачиевой, Д. М. Самекеева «Цифровая трансформация промышленных предприятий в условиях инновационной экономики». Авторами предложены модели интеграции систем управления информационной безопасностью, защиты «умных» производственных систем и обеспечения непрерывности бизнес-процессов [13]. Вопросы формирования цифровых экосистем промышленных предприятий с учетом требований экономической безопасности рассмотрены в публикациях Коротовских А. Е. «Различия в типах стратегии цифровой трансформации промышленного предприятия», Добкина А. С. «Стратегии развития промышленного предприятия в условиях нарастающей неопределенности и активизации цифровой трансформации» и Кухтиной Е. К. «Перспективы формирования стратегии устойчивого развития предприятий промышленности в условиях цифровой трансформации» [4,2,5]. Обобщая результаты проведенного обзора, можно сделать вывод, что в последние

годы отечественные ученые уделяют все больше внимания комплексным аспектам формирования цифровых стратегий промышленных предприятий, ориентированных на повышение их экономической безопасности и устойчивости в условиях нарастающих киберугроз. Предлагаемые подходы и решения имеют высокую практическую значимость для руководителей и специалистов промышленного сектора.

Для исследования проблем формирования цифровой стратегии промышленных предприятий важное значение имеют статистические данные, характеризующие текущий уровень цифровизации и киберустойчивости промышленного сектора. Согласно данным Росстата, доля организаций, использующих технологии «Интернета вещей» в промышленности, выросла с 11,6% в 2022 году до 16,8% в 2023 году [11]. В то же время, доля предприятий, внедривших системы управления производственными процессами на основе технологий «Индустрии 4.0», составила 14,3% в 2023 году. Существенный прогресс наблюдается и в развитии отечественных систем управления информационной безопасностью на промышленных предприятиях. Согласно результатам исследования РОЦИТ, доля организаций, имеющих сертифицированную СМИБ, выросла с 28% в 2019 году до 38% в 2023 году [8]. Вместе с тем, данные Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) свидетельствуют о высоком уровне киберугроз, с которыми сталкивается промышленность. По оценкам экспертов, в 2023 году число инцидентов информационной безопасности в промышленном секторе увеличилось на 27% по сравнению с предыдущим годом [12]. Согласно результатам опроса Учебно-методического центра РСПП, только 56% промышленных предприятий России имеют в своей структуре подразделение, отвечающее за информационную безопасность [7]. При этом лишь 32% компаний проводят регулярный аудит ИБ и управление рисками. Приведенные статистические данные свидетельствуют о значительных проблемах, с которыми сталкиваются промышленные предприятия при формировании эффективных цифровых стратегий, ориентированных на повышение их экономической безопасности и устойчивости. Несмотря на определенный прогресс в развитии "Индустрии 4.0" и систем управления информационной безопасностью, многие организации по-прежнему испытывают серьезные трудности в обеспечении должного уровня киберзащищенности критических производственных активов и бизнес-процессов.

Проведенный анализ статистических данных и результатов эмпирических исследований позволяет выявить ключевые взаимосвязи между цифровизацией, производственной эффективностью и экономической безопасностью промышленных предприятий. Так, внедрение «умных» производственных систем, оснащенных различными датчиками, контроллерами и исполнительными механизмами, позволяет значительно повысить гибкость и точность производственных процессов, минимизировать простои оборудования, сократить брак и производственные издержки. По оценкам экспертов, использование технологий «Индустрии 4.0» способно повысить производительность труда на 10-30% за счет оптимизации загрузки оборудования, устранения «узких» мест и повышения качества продукции [9]. В то же время, интеграция различных производственных, логистических и управленческих систем, подключение к «Интернету вещей», наряду с очевидными эффектами, создает новые уязвимости и угрозы для экономической безопасности. Согласно данным Ростелекома, около 40% всех кибератак на российские компании в 2023 году были направлены против предприятий обрабатывающей промышленности [10]. При этом среднее время восстановления бизнеса после атаки составляет 4-6 месяцев, а прямые финансовые потери могут достигать сотен миллионов рублей.

Одним из ключевых элементов успешной цифровой стратегии промышленных компаний должно стать создание и внедрение интегрированных систем управления информационной безопасностью. Такие системы позволяют обеспечить комплексную защиту ключевых производственных активов, систем управления и конфиденциальных данных от

разнообразных киберугроз. Важно, чтобы данные системы были полностью интегрированы с «умными» производственными комплексами, технологиями промышленного интернета вещей и другими цифровыми решениями, внедряемыми на предприятиях. Неотъемлемой частью интегрированной системы управления информационной безопасностью должны стать специализированные механизмы защиты «умных» производственных систем и промышленного интернета вещей. Это предполагает использование средств многофакторной аутентификации при удаленном доступе к оборудованию, применение криптографических методов защиты передаваемых данных, а также разработку и регулярное тестирование планов быстрого реагирования на инциденты информационной безопасности в производственной среде [6]. Особое внимание следует уделить развитию аналитических и прогностических возможностей систем управления информационной безопасностью. Интеллектуальные инструменты сбора, анализа и прогнозирования киберугроз позволяют своевременно выявлять аномалии и предотвращать инциденты, способные нанести критический ущерб производственным процессам и финансовому состоянию предприятия. Одновременно с совершенствованием технологических механизмов защиты информации необходимо уделять пристальное внимание формированию культуры информационной безопасности среди сотрудников. Обучение персонала правилам кибергигиены, повышение их мотивации к активному участию в обеспечении информационной безопасности, а также выстраивание доверительных отношений с внешними партнерами - все это способствует повышению киберустойчивости предприятия в целом. Таким образом, разработка и внедрение комплексных механизмов обеспечения экономической безопасности становятся ключевым элементом эффективных цифровых стратегий современных промышленных компаний. Лишь системный подход, сочетающий технологические, организационные и культурные аспекты, способен обеспечить устойчивое развитие бизнеса в условиях нарастающих киберугроз.

На основании проведенного анализа и выявленных ключевых проблем, связанных с формированием цифровой стратегии промышленных предприятий можно предложить следующие рекомендации для нивелирования существенных пробелов.

1. Внедрение интегрированных систем управления информационной безопасностью. Для эффективной защиты информационных активов в условиях цифровизации производства необходимо разработать и внедрить комплексную политику информационной безопасности. Она должна учитывать специфику "умных" производственных систем и промышленного интернета вещей, обеспечивая надежную защиту от киберугроз. Важно создать централизованную систему управления доступом к критичным данным и мониторинга событий информационной безопасности. Ключевым моментом является интеграция систем управления информационной безопасностью с производственными системами, ERP, PLM и другими бизнес-приложениями.

2. Защита «умных» производственных систем и промышленного интернета вещей. Для предотвращения кибератак на критические производственные активы необходимо внедрить специализированные решения, способные выявлять и блокировать угрозы в режиме реального времени. Важно также обеспечить безопасную удаленную подключаемость производственного оборудования, применяя средства многофакторной аутентификации пользователей. Кроме того, следует разработать и регулярно тестировать планы быстрого реагирования на инциденты информационной безопасности в производственной среде.

3. Шифрование конфиденциальных данных. Для защиты данных, циркулирующих в ключевых бизнес-приложениях, ERP, PLM и других информационных системах, необходимо внедрить средства криптографической защиты. При этом важно создать централизованную систему управления ключами шифрования с гибкими политиками доступа. Регулярное тестирование эффективности применяемых криптографических алгоритмов и средств также является необходимым условием.

4. Развитие аналитических и прогностических возможностей. Для своевременного выявления и предотвращения кибератак следует внедрить решения для сбора, агрегации и анализа данных об информационных угрозах и инцидентах. Создание интеллектуальных систем мониторинга и обнаружения аномалий позволит оперативно реагировать на киберугрозы. Разработка прогностических моделей и сценариев оценки вероятности реализации угроз и их потенциального ущерба также играет ключевую роль.

5. Управление рисками и обеспечение непрерывности бизнеса. Для эффективного управления рисками, связанными с цифровой трансформацией, необходимо сформировать комплексную систему оценки, мониторинга и контроля этих рисков. Кроме того, важно разработать и регулярно тестировать планы обеспечения непрерывности ключевых бизнес-процессов на случай инцидентов информационной безопасности. Создание распределенных отказоустойчивых архитектур для хранения данных и резервных каналов связи также является важной мерой обеспечения киберустойчивости.

Предложенные рекомендации позволят промышленным предприятиям внедрить эффективные механизмы обеспечения экономической безопасности в процессе цифровой трансформации, повысив устойчивость бизнеса к киберугрозам.

Проведенное исследование показало, что формирование эффективной цифровой стратегии является ключевым фактором успеха промышленных предприятий в условиях ускоряющейся цифровой трансформации. Однако, переход к цифровым технологиям сопряжен с рядом серьезных вызовов, которые необходимо комплексно решать для достижения желаемых результатов. Одна из ключевых проблем - отсутствие у многих компаний четкого видения и последовательной стратегии цифровой трансформации. Зачастую предприятия подходят к цифровизации фрагментарно, без должной проработки стратегических целей и этапов реализации [1]. Необходимо разработать всеобъемлющую цифровую стратегию, органично интегрированную с общей бизнес-стратегией организации. Это позволит обеспечить системный и последовательный подход к внедрению цифровых технологий, ориентированный на достижение конкретных результатов. Еще одна серьезная сложность - недостаток компетенций и опыта в области цифровых технологий у сотрудников предприятий. Внедрение инновационных решений часто сдерживается дефицитом квалифицированных кадров, способных эффективно управлять цифровыми проектами. Для решения этой проблемы требуется системная работа по развитию цифровых навыков персонала на всех организационных уровнях - от рядовых сотрудников до топ-менеджмента. Внедрение новых технологий также сопряжено с высокими рисками - организационными, технологическими и финансовыми. Поэтому важно внедрять комплексную систему управления рисками, включающую регулярную оценку, мониторинг и минимизацию негативных последствий. Это позволит обеспечить более плавный и безболезненный переход к цифровым решениям. Еще одна ключевая проблема - недостаточная интеграция информационных систем и данных на предприятиях. Разрозненность ИТ-инфраструктуры и отсутствие единой системы управления данными затрудняют реализацию сквозных цифровых процессов. Для решения этой задачи необходима модернизация ИТ-архитектуры организации на базе принципов информационной интеграции и межсистемного взаимодействия. Наконец, важно уделять серьезное внимание вопросам кибербезопасности. Расширение периметра информационной экосистемы за счет "умных" производственных систем и промышленного интернета вещей значительно повышает киберриски. Поэтому обеспечение информационной безопасности должно быть ключевым элементом цифровой стратегии предприятий. Комплексное решение этих проблем позволит промышленным компаниям успешно реализовать программы цифровой трансформации, кардинально повысить операционную эффективность и конкурентоспособность в условиях стремительно меняющейся цифровой реальности.

Литература

1. Гаранин Д. А. 4.5. Обзор практики и перспективы применения технологии блокчейн в логистике / Д. А. Гаранин, Н. С. Лукашевич, Е. Р. Темиргалиев // Глобальные вызовы цифровой трансформации рынков : Коллективная монография. – Санкт-Петербург : ПОЛИТЕХ-ПРЕСС, 2023. С. 427-450.

2. Добкин А. С. Стратегии развития промышленного предприятия в условиях нарастающей неопределенности и активизации цифровой трансформации / А. С. Добкин, В. А. Мордовец // Теория и практика управления предпринимательскими структурами в современных условиях : Сборник научных трудов II Международной научно-практической конференции, Санкт-Петербург, 16–17 февраля 2023 года / Под общей редакцией В.А. Мордовца. Санкт-Петербург: Санкт-Петербургский университет технологий управления и экономики, 2023. С. 189-193.

3. Измайлов М. К. Цифровизация как фактор устойчивости деятельности промышленных предприятий / М. К. Измайлов // Телескоп: журнал социологических и маркетинговых исследований. 2024. № 1(13). С. 28-35. DOI 10.24412/1994-3776-2024-1-28-35.

4. Коротовских А. Е. Различия в типах стратегии цифровой трансформации промышленного предприятия / А. Е. Коротовских // Актуальные проблемы науки и образования в условиях современных вызовов (шифр - МКАП 7) : Сборник материалов VII международной научно-практической конференции, Москва, 21 января 2022 года. Москва: ООО «Институт развития образования и консалтинга», 2022. С. 179-182. DOI 10.34755/IROK.2022.52.56.011.

5. Кухтина Е. К. Перспективы формирования стратегии устойчивого развития предприятий промышленности в условиях цифровой трансформации / Е. К. Кухтина // Научные дискуссии в эпоху глобализации : материалы XXIII Всероссийской научно-практической конференции, Смоленск, 08 декабря 2022 года. – Смоленск: ООО «Полиграф», 2022. С. 179-181.

6. Ливинцова М. Г. Современные принципы стратегического управления и формирования стратегии предприятия / М. Г. Ливинцова, А. А. Иващенко, Н. С. Сергеев // Фундаментальные и прикладные исследования в области управления, экономики и торговли : Сборник трудов Всероссийской научно-практической и учебно-методической конференции. В 8 ч., Санкт-Петербург, 15–19 мая 2023 года. Том Часть 2. – Санкт-Петербург: ПОЛИТЕХ-ПРЕСС, 2023. С. 145-156.

7. Официальный сайт Российского союза промышленников и предпринимателей. [Электронный ресурс] URL: https://rspp.ru/events/news/ (дата обращения 09.08.2024)

8. Официальный сайт РОЦИТ. [Электронный ресурс] URL: https://rocit.ru/ (дата обращения 09.08.2024)

9. Официальный сайт Сколково. Как цифровизация повышает производительность труда в промышленности. [Электронный ресурс] URL: https://skolkovo-resident.ru/cifrovizaciya-povyshaet-proizvoditelnost-truda-v-promyshlennosti/ (дата обращения 09.08.2024)

10. Официальный сайт ТАСС. В Ростелекоме" сообщили о росте более чем на 60% количества кибератак на структуры РФ. [Электронный ресурс] URL: https://tass.ru/ekonomika/18242635 (дата обращения 09.08.2024)

11. Официальный сайт Федеральной службы государственной статистики. [Электронный ресурс] URL: https://rosstat.gov.ru/storage/document/document_form/form/2022-02/17/0604018(1).doc (дата обращения 09.08.2024)

12. Официальный сайт ЦБ РФ. ФинЦЕРТ. [Электронный ресурс] URL: https://www.cbr.ru/analytics/ib/fincert/ (дата обращения 09.08.2024)

13. Цифровая трансформация промышленных предприятий в условиях инновационной экономики / О. О. Джиоева, О. М. Танделова, С. В. Галачиева, Д. М. Самекеев // Современные тенденции развития информационных технологий в научных исследованиях и прикладных областях : Сборник докладов III Международной научно-практической конференции, Владикавказ, 28–29 апреля 2022 года. – Владикавказ: Северо-Кавказский горно-металлургический институт (государственный технологический университет), 2022. – С. 167-171.

14. Устинова О. Е. Формирование стратегии цифровой трансформации промышленных предприятий / О. Е. Устинова // Вопросы инновационной экономики. 2022. Т. 12, № 3. С. 1427-1442. – DOI 10.18334/vinec.12.3.115129.