УДК 338.012

ДВОЙСТВЕННАЯ ПРИРОДА ЦИФРОВОЙ ТРАНСФОРМАЦИИ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ[8]

Самусева Анна Вадимовна, преподаватель-стажёр
Белорусский национальный технический университет
Samuseva Anna Vadimovna, teacher trainee
Belarusian National Technical University, annasamusevaa@gmail.com

Аннотация. В статье обосновывается, что цифровизация одновременно создает новые возможности для защиты экономических интересов и порождает ранее неизвестные угрозы. Предлагаются направления совершенствования диагностики угроз. Определены перспективы использования полученных результатов в деятельности промышленных предприятий и органов государственного управления.

Ключевые слова: экономическая безопасность, цифровая трансформация, промышленное предприятие, риски, угрозы, пороговые значения.

На данный момент традиционные подходы к обеспечению экономической безопасности промышленных предприятий, ориентированы преимущественно на защиту материальных активов и финансовых потоков, что перестает быть достаточным в условиях новых вызовов. Стремительная цифровизация всех сфер экономической деятельности, усиление геополитической нестабильности, а также трансформация глобальных цепочек создания стоимости определяют потребность в переосмыслении самой концепции экономической безопасности. На передний план выходят вопросы способности предприятий к адаптации, прогнозированию рисков и формированию внутренних механизмов устойчивости, интегрированных в стратегическое управление.

Ключевым направлением развития экономической безопасности выступает цифровая трансформация экономики. Развитие киберфизических систем, промышленного интернета вещей, искусственного интеллекта и технологий обработки больших данных создает принципиально новые условия функционирования промышленных предприятий. Как справедливо отмечает М.С. Оборин, «современные цифровые решения на сегодняшний день являются приоритетным направлением повышения эффективности промышленного производства. Но условия цифровизации не только положительно влияют на эффективность промышленной отрасли, но и способствуют появлению новых рисков и угроз для всех участников цепочки производственной деятельности» [1, с. 46]. В этих условиях традиционные угрозы видоизменяются, приобретая новые формы и масштабы, а также возникают новые риски. Цифровизация производственных процессов, с одной стороны, повышает их эффективность, прозрачность и управляемость, но с другой – создает новые угрозы экономической безопасности. Цифровая трансформация пронизывает все этапы производственного цикла – от проектирования до послепродажного обслуживания, что создает возможности для повышения эффективности, но одновременно порождает ранее неизвестные риски: кибератаки, утечки конфиденциальной информации, зависимость от иностранных программных продуктов и цифровых платформ. Из этого следует, что дальнейшие исследования должны быть направлены на поиск баланса между эффективностью цифровизации и надежностью защиты информационных активов предприятия.

Цифровая трансформация экономики кардинально меняет природу и характер угроз экономической безопасности промышленных предприятий. Традиционные методы защиты в цифровой среде зачастую оказываются несостоятельными. Отсюда следует вывод: система экономической безопасности предприятия должна быть не статичным набором защитных мер, а динамичной структурой, способной адаптироваться к появлению принципиально новых видов угроз. Более того, сама скорость появления новых угроз в цифровой среде требует пересмотра подходов к периодичности оценки уязвимостей – переход от ежеквартального или ежегодного к мониторингу в режиме реального времени.

[8] Выполнено при поддержке БРФФИ (договор с БРФФИ № Г24МП-023 от 02.05.2024 г. «Разработка модели экономической безопасности промышленного предприятия в Республике Беларусь»).

Особый интерес представляют результаты экспертных опросов, согласно которым в пятерку наиболее перспективных цифровых инструментов обеспечения экономической безопасности на ближайшие пять лет вошли: «приоритет 1 – цифровые средства защиты данных, приоритет 2 – SIEM-системы, приоритет 3 – автоматизированные системы управления аудитом, приоритет 4 – системы анализа данных и приоритет 5 – DLP-системы» [2, с. 25]. Данные результаты могут служить ориентиром при формировании стратегий цифровизации систем экономической безопасности на промышленных предприятиях, однако требуют обязательной адаптации к специфике конкретных производств, поскольку универсально эффективных решений для предприятий разных отраслей и масштабов не существует. Выбор конкретных инструментов должен определяться прежде всего характером угроз, с которыми сталкивается предприятие, а также его финансовыми возможностями.

Особого внимания заслуживает разработка методических подходов к оценке уровня «цифровой устойчивости» предприятия – способности сохранять параметры безопасного функционирования в условиях цифровой трансформации, противодействовать киберугрозам и адаптироваться к изменениям цифровой среды. Перспективным представляется создание комплексных систем мониторинга, которые включают в себя сбор данных из различных источников и использование технологий искусственного интеллекта для прогнозирования угроз на основе анализа больших данных. Такие системы позволят перейти от традиционной модели, ориентированной на устранение уже реализовавшихся угроз, к новой, основанной на раннем обнаружении и превентивных мерах. Важным элементом методического инструментария выступают пороговые значения индикаторов экономической безопасности. Как отмечается в научной литературе, «для проведения мониторинга экономической безопасности целесообразно использовать инструмент пороговых значений. При этом их следует рассматривать не с позиций обязательного наступления катастрофы (от термина «пороговый эффект»), а с тем, чтобы отделить нормальный уровень экономической безопасности от недостаточного» [3, с. 50]. В условиях цифровой трансформации требуется пересмотр традиционных пороговых значений и введение новых индикаторов, отражающих цифровые риски: уровень защищенности информационных систем, частоту кибератак, степень зависимости от зарубежного программного обеспечения и т.д.

Развитие цифровых технологий неразрывно связано с углублением отраслевой дифференциации подходов к обеспечению экономической безопасности. Очевидно, что механизмы защиты, набор ключевых показателей и пороговые значения будут существенно различаться для предприятий машиностроения, химической промышленности, легкой промышленности и других отраслей. Более того, цифровые решения, эффективные в одной отрасли, могут оказаться бесполезными или вредоносными в другой. Для предприятий машиностроения, характеризующихся длительным производственным циклом и сложной кооперацией, первостепенное значение имеют риски нарушения цепочек поставок и защиты конструкторской документации. Для предприятий химической промышленности на первый план выходят угрозы, связанные с экологической безопасностью и защитой технологических процессов. Предприятия легкой промышленности в большей степени уязвимы с точки зрения контрафактной продукции и несанкционированного копирования дизайнерских решений. Учет этих особенностей позволит повысить практическую значимость научных разработок и обеспечить их более широкое внедрение в реальный сектор экономики. Формирование отраслевых методик обеспечения экономической безопасности, разработанных с учетом отраслевых особенностей, основанных на реальных промышленных предприятиях, представляет собой перспективное направление дальнейших исследований. Такие методики должны включать не только перечень типовых угроз и мер реагирования, но и систему индикаторов, пороговых значений, а также рекомендации по созданию специализированных служб безопасности с учетом отраслевой специфики.

Предложенные рекомендации по созданию и функционированию службы экономической безопасности могут быть использованы предприятиями различных форм собственности при организации систем защиты экономических интересов. Особую ценность они представляют для предприятий, только приступающих к формированию специализированных подразделений безопасности, поскольку позволяют избежать типичных ошибок и использовать уже известные подходы. Разработанные рекомендации должны быть также использованы при подготовке внутрифирменных документов, регламентирующих вопросы экономической безопасности: положений, инструкций,

регламентов и планов антикризисного реагирования. Наличие таких документов, разработанных с учетом современных научных подходов и адаптированных к специфике конкретного предприятия, является необходимым условием эффективного функционирования системы безопасности.

Результаты исследования могут быть востребованы отраслевыми органами управления, министерствами и ведомствами при разработке программ развития промышленности, стратегических документов и методических рекомендаций для подведомственных предприятий. Как отмечает в исследованиях М.С. Оборин, необходимо «создать единую интеграцию взаимосвязи органов власти и представителей промышленности по созданию единой базы противодействия преступлениям в сфере информации; совершенствовать нормативно-правовую базу по защите от информационного мошенничества» [1, с. 52]. Перспективным направлением практического использования результатов является создание отраслевых центров мониторинга угроз на принципах государственно-частного партнерства. В рамках таких проектов может быть отработано взаимодействие между промышленными предприятиями, научными организациями и органами государственного управления, определены наиболее эффективные формы сотрудничества и механизмы финансирования совместных инициатив. Реализация подобных проектов позволит не только повысить уровень защищенности предприятий, но и сформировать устойчивую экосистему, в которой наука, бизнес и государство будут совместно решать задачи обеспечения экономической безопасности.

Список использованных источников

1. Оборин, М. С. Экономическая безопасность промышленных предприятий в цифровой экономике / М. С. Оборин // Вестник Самарского государственного экономического университета. – 2022. – № 1 (207). – С. 44–54.

2. Свистунов, В. М. Цифровизация как инструмент экономической безопасности современной организации / В. М. Свистунов, О. А. Агеева, И. Д. Мацкуляк // Вестник университета. – 2025. – № 5. – С. 15–27.

3. Митяков, Е. С. Оценка рисков в задачах мониторинга угроз экономической безопасности / Е. С. Митяков // Труды НГТУ им. Р. Е. Алексеева. – 2018. – № 1 (120). – С. 44–51.