УДК 65.011.8

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В ХОДЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРОИЗВОДСТВЕННО-ЛОГИСТИЧЕСКИХ СИСТЕМ

О. В. Мясникова

кандидат экономических наук, доцент, Институт бизнеса Белорусского государственного университета, кафедра логистики, г. Минск, Республика Беларусь, e-mail: miasnikovaov1@gmail.com

Статья посвящена вопросам обеспечения безопасности при осуществлении цифровой трансформации производственно-логистических систем. Разработана классификация угроз для процессов цифровой трансформации производственно-логистических систем. Предложены меры по меры по устранению угроз для сохранения устойчивости и управляемости системы, снижению потерь.

Ключевые слова: производственно-логистическая система; цифровая трансформация; риски; угрозы; безопасность; управление.

ENSURING ECONOMIC SECURITY DURING THE DIGITAL TRANSFORMATION OF PRODUCTION AND LOGISTICS SYSTEMS

O. V. Miasnikova

PhD in Economics, Associate Professor, School of Business of Belarusian State University, Department of Logistics, Minsk, Republic of Belarus, e-mail: miasnikovaov1@gmail.com

The article is devoted to the issues of ensuring security in the implementation of digital transformation of production and logistics systems. A classification of threats to the processes of digital transformation of production and logistics systems has been developed. Measures to eliminate threats to maintain the stability and manageability of the system, reduce losses are proposed.

Keywords: production and logistics system; digital transformation; risks; threats; security; management.

Введение. Производственно-логистическая система (ПЛС) как сложная, открытая, адаптивная система звеньев цепи создания ценности, объединенных в пределах цикла производства и обеспечивающих сквозное управление материальными, сервисными и сопутствующими потоками. Цифровая трансформация ПЛС (ЦТ ПЛС) – преобразование структур, форм и способов деятельности ПЛС за счет освоения цифровых тех-

нологий, результатом которого является создание цифровой ПЛС, где бизнес-модели, жизненные циклы и бизнес-процессы построены на первичности цифрового представления ее основных продуктов и услуг. В работах [1–3] выделены некоторые риски и угрозы, доказано, что в ходе ЦТ ПЛС возникают угрозы нарушения целостности и снижения эффективности системы. Цель данной статьи – выделить угрозы безопасности и предложить меры по устранению их проявления.

Основная часть. Нами установлено, что угрозы различной природы, масштабов, источников, комплексно проявляются в различных элементах системы, генерируют негативные последствия для ее существования, управления и экономики как показано на рисунке.

Классификация угроз для процессов цифровой трансформации производственно-логистических систем

Собственная разработка.

В качестве мер по снижению рисков и угроз предложено применять для осуществления ЦТ ПЛС «движимый угрозами» (Threat-driven) подход, сформулированный нами в работе [1]. Он основан на выявлении, анализе угроз, устранении причин и недопущении последствий. Например, к глобальным угрозам следует отнести нарушения надежности цепей поставок, из-за кризисных явлений, пандемии, релокации производств, диверсификации цепей поставок в пользу местных производите-

лей, сокращения протяженности цепи за счет посреднических структур и нарастания автоматизации производств.

В ходе ЦТ формируются активы нового типа – цифровые. Наличие кибернетической составляющей угрожает управляемости ПЛС. Управление в виртуальном пространстве бизнес-приложений, облачных вычислений создает угрозой самому существованию бизнеса, т. к. в случае сбоев перейти на «ручной» режим управления гиперсвязанными производствами на мобильных платформах, автоматическими рабочими центрами, роботизированными человеко-независимыми системами очень сложно. Необходимо снизить риск прерывания главных бизнес-процессов при любом изменении унаследованной ИТ-инфраструктуры ПЛС, некорректности алгоритмов искусственного интеллекта, остановки процессов и потери данных из-за сбоев энергоснабжения, Интернет связи, кибер-атак. Данные как цифровой актив являются носителем угроз нарушение устойчивости функционирования системы из-за краж, утечки и недостоверности данных, а также их избыточности (цифровой хординг, Digital Hoarding – «порочная страсть собирать все подряд»).

Заключение. Наличие угроз вызывает ряд действий по их нейтрализации и недопущению перерастания последствий за критический уровень. Необходимо развивать компетенции персонала, выделять соразмерный объем ресурсов для защиты своих активов, создавать киберзащиту, необходимые для сохранения управляемости и устойчивости системы. Основными мерами являются формирование новых компетенций и навыков, развитие новых форм занятости, резервирование данных, интероперабельность, интеграция ИТ-решений, резервное энергоснабжение, управление кибербезопасностью.

Библиографические ссылки

1. *Мясникова О. В.* Трансформация производственно-логистической системы в умную сеть поставок: теоретико-методологические аспекты // Новости науки и технологий. 2021. № 2 (57). С. 53–62.

2. *Мясникова О. В.* Методологические подходы к обеспечению эффективности процесса цифровой трансформации производственно-логистических систем // Бизнес. Инновации. Экономика: сб. науч. ст. / Ин-т бизнеса БГУ. Минск, 2021. Вып. 5. С. 175–183.

3. *Мясникова О. В.* Спиральная модель и сценарии изменения производственно-логистических систем в ходе цифровой трансформации // Бизнес. Инновации. Экономика: сб. науч. ст. / Ин-т бизнеса БГУ. Минск, 2022. Вып. 6. С. 229–238.