УДК 338.242

В. Б. Криштаносов, канд. экон. наук,
докторант кафедры менеджмента,
технологий бизнеса и устойчивого развития
(БГТУ, г. Минск)

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПРЕДПРИЯТИЙ РЕСПУБЛИКИ БЕЛАРУСЬ: АКТУАЛЬНОЕ СОСТОЯНИЕ И НАПРАВЛЕНИЯ РАЗВИТИЯ

В условиях текущих тенденций цифровой трансформации экономики, осуществляется фрагментарное внедрение цифровых технологий и цифровых систем производства и управления на уровне предприятий и отраслей Беларуси. На отраслевом уровне цифровая трансформация осуществляется путем внедрения цифровых технологий, цифровых систем производства и управления. В рамках исследования, проведенного компанией Beroc в 2019 году в отношении предприятий малого и среднего бизнеса [1, с. 7-14], представлены сведения о внедрении CRM-систем на 22,2% опрошенных предприятиях. 21,5% предприятий отметили внедрение ERP-систем. Уровень внедрения BPM-систем – 2,3%. По данным Белстата, в 2022 году 18,5% предприятий использовали технологии IoT, 12,3% – BDA, 3,6% – AI, 0,6% – Digital Twin. В результате проведенного опроса 133 крупнейших предприятий ключевых белорусских отраслей, получены анкеты 58 субъектов. Анализ агрегированных данных свидетельствует о текущем использовании цифровых метатехнологий, среди которых выделяются Cloud Computing (внедрены в 32,8% опрошенных предприятиях), роботизированные системы и BDA (по 29,3% предприятий), платформы (20,7%), IoT (19%). В разрезе цифровых производственных и управленческих систем, наибольшее распространение получили к настоящему времени ERP (APS / MRP/MRPII) – 69% опрошенных предприятий, SCADA, CAM – 43,1%, CRM – 41,4%, CAD/CAE – 39,7%, PDM – 15,5%, BPM – 15,5%. В среднесрочной перспективе (3-5 лет), как ожидается, ERP (APS / MRP/MRPII) будут внедрены у подавляющего большинства предприятий, CRM – 60,3%, SCADA, CAM – 56,9%, CAD/CAE – 44,8%, 3D-печать, BPM и SCM (по 27,6%), PDM – 20,7%.

В секторальном разрезе анализ данных, предоставленных флагманскими предприятиями белорусской экономики, показывает активное внедрение цифровых инноваций в: машиностроении – Cloud Computing, роботизированные системы, ERP/APS/ MRP/MRPII; PDM; CAD, CAE; SCADA, CAM; производстве электрооборудования – ERP/APS/MRP/MRPII; PDM; SCADA, CAM; CAD, CAE; PLC, CALS,

PLM; 3D-печать; химической промышленности – Cloud Computing, роботизированные системы, Digital Twins, ERP/APS/MRP/MRPII; SCADA, CAM; легкой промышленности – ERP/APS/ MRP/MRPII; SCADA, CAM; CRM; CAD, CAE; деревообработке – IoT, ERP/APS/ MRP/MRPII; SCADA, CAM; CRM; сельском хозяйстве – Cloud Computing, IoT, ERP/APS/MRP/MRPII; SCADA, CAM; энергетике – BDA, цифровые платформы, ERP/APS/MRP/MRPII; SCADA, CAM; CAD, CAE; строительстве – роботизированные системы, CAD, CAE; BIM; транспорте и логистике – AI, BDA, ERP/ APS/MRP/MRPII; BPM; телекоммуникациях – IoT, AI, BDA, Cloud Computing, ERP/APS/MRP/MRPII, BPM; финансовой деятельности – AI, BDA, Cloud Computing, Blockchain, роботизированные системы, Digital Twins, платформы, ERP/ APS/MRP/MRPII; CRM; BPM; страховой деятельности – Cloud Computing, ERP/APS/MRP/MRPII; CRM; оптовой и розничной торговле – BDA, Cloud Computing, ERP/APS/ MRP/MRPII; CRM; CAD, CAE; фармацевтике – ERP/APS/MRP/MRPII; SCADA, CAM; CAD, CAE. Среди используемых систем производства и управления, большую долю занимают инновации, разработанные иностранными компаниями. Как показал анализ результатов опроса, доля иностранных систем превышает 60%. Иностранные системы превалируют среди систем BIM, CAPP (100% внедренных систем являются иностранными), SCADA, CAM (92%), CAD, CAE (91,3%), 3D-печать (87,5%), MDM (75%), TQM (66,7%). Продолжение использования данных цифровых систем будет в краткосрочном периоде генерировать для белорусских предприятий дополнительные риски по мере отказа иностранных поставщиков от технической поддержки и соответствующего обновления. Перевод данных систем на отечественное ПО потребует дополнительных финансовых ресурсов предприятий, задействования определенного числа ИТ специалистов. Это также формирует потенциал дополнительных рисков внешнего вмешательства по мере отсутствия обновления иностранного ПО и длительного и периода перевода бизнес- и технологических процессов на отечественные аналоги ПО. Как показали результаты опроса, более 54% белорусских флагманских предприятий сталкивались с различными видами цифровых рисков и угроз. В секторальном разрезе следует выделить финансовую деятельность, оптовую и розничную торговлю, телекоммуникации, строительство, производство металлопродукции, вычислительной, электронной и оптической аппаратуры, фармацевтику. 36,8% предприятий оценивают будущие цифровые риски и угрозы как средние (вероятность от 25% до 50%), 29,8% – как низкие (вероятность от 10% до 25%), 15,8% – как высокие (вероятность от 50% до 75%),

12,3% – очень низкие (до 10%) предприятий. При этом крайне низко оценивают будущие цифровые риски и угрозы руководители предприятий легкой промышленности, производители вычислительной, электронной и оптической аппаратуры, фармацевтики, транспорта и логистики. Анализ данных проведенного опроса показал, что ряд руководителей сохраняют низкие оценки будущих цифровых рисков и угроз несмотря на имеющийся негативный опыт противодействия им. Это может свидетельствовать о недостаточном понимании рисков и угроз цифровой трансформации на уровне высшего менеджмента предприятий, одним из механизмов решения может стать введение для руководителей предприятий (как государственных, так и частных) обязательных курсов по кибербезопасности в рамках МВА или переподготовки руководящих кадров в Академии управления при Президенте Республики Беларусь, БГУИР.

Проведенное исследование показало, что в настоящее время технологии IoT является как одними из ключевых в рамках цифровой трансформации, так и одной из самых уязвимых для внешнего злонамеренного воздействия. Так, технология глубокого анализа пакетов (DPI) применяется с целью идентификации информации о пользователях и приложениях, генерирующих сетевой трафик, что позволяет осуществлять его контроль [2]. Одним из ИКТ решений для противодействия кибератакам систем IoT является технология программно-определяемых сетей (SDN), которая позволяет программировать сетевой трафик, перенаправлять его и автоматизировать выполнение политики сетевой безопасности. Технология виртуализации сетевых функций (NFV) позволяет агрегировать ресурсы безопасности предприятия, обеспечивая киберзащиту всем пользователям сети [3]. Для решения задачи обеспечения кибербезопасности в том числе роботизированных систем предприятия АО Лаборатория Касперского разработана система Kaspersky Industrial CyberSecurity, которая обеспечивает защиту промышленной инфраструктуры на всех уровнях: от серверов SCADA и рабочих станций операторов до программируемых логических контроллеров и сетевого оборудования. Комплексное решение разработано Positive Technologies – это система глубокого анализа технологического трафика для выявления сложных атак внутри сетей SCADA и проактивного поиска киберугроз (PT ISIM 4) [4]. Технология BDA является одним из основных драйверов цифровой трансформации, генерируя новые источники доходов, повышая качество производства и управления, оптимизируя затраты, обеспечивая в целом высокую конкурентоспособность предприятия на рынке. Российской Федерации в 2022-2023 гг. лидирующие позиции в адаптации

цифровых систем под специфику сред обработки больших данных и разработке защищённых платформ занимают, в том числе Лаборатория Касперского и ООО Киберпротект [5]. Представляется целесообразным воспользоваться опытом Российской Федерации, которая на базе Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак осуществляет работу по развитию государственных систем в области кибербезопасности, включая «Мультисканер», «Антифишинг», «Антифрод». В Республике Беларусь данную функцию в рамках компетенции может на себя взять сформированный в стране в 2023 году Национальный центр кибербезопасности посредством национальной платформы кибербезопасности.

Структурно она должна включать четыре ключевых системы: а) обновляемую в режиме 24/7 базу сигнатур киберугроз; б) систему мониторинга цифровых рисков и угроз со встроенными элементами AI; в) автоматизированную систему нивелирования цифровых рисков и угроз «план аварийного восстановления» (DRP); г) систему управления, включающую приоритезацию нивелирования цифровых угроз в рамках соответствующего регламента.

ЛИТЕРАТУРА

1. Огинская А. Использование информационных технологий белорусским бизнесом / А. Огинская, Р. Морозов : BEROC. – Минск, 2019. – 31 с.

2. Awati R. Definition: deep packet inspection (DPI) [Электронный ресурс] / R. Awati, J. Scarpati. – 2023. – Режим доступа: https://www.techtarget.com/searchnetworking/definition/deep-packet-inspection-DPI. – Дата доступа: 20.01.2024.

3. Широкий Ю. Технологии кибербезопасности в эпоху IoT [Электронный ресурс] / Ю.Широкий. – 2019. – Режим доступа: https://www.cta.ru/articles/cta/oborudovanie/setevoe-oborudovanie/124332/. – Дата доступа: 20.01.2024.

4. Positive Technologies Industrial Security Incident Manager [Электронный ресурс] / Positive Technologies. – 2023. – Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/products/isim/PT-ISIM-DS-05-2022.pdf. – Дата доступа: 14.01.2024.

5. Лыткин С. Обзор защищённых платформ и накладных средств безопасности больших данных [Электронный ресурс] / С. Лыткин. – 2022. – Режим доступа: https://www.anti-malware.ru/ analytics/Market_Analysis/Big-Data-Protection#part3. – Дата доступа: 08.01.2024.