СОЦИАЛЬНЫЕ И ГУМАНИТАРНЫЕ НАУКИ

УДК 338.242

РИСКИ И УГРОЗЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ И СИСТЕМ ПРОИЗВОДСТВА И УПРАВЛЕНИЯ НА БЕЛОРУССКИХ ПРЕДПРИЯТИЯХ

Криштаносов В.Б.
Белорусский государственный технологический университет, Республика Беларусь, 220006, г. Минск, ул. Свердлова, 13а

RISKS AND THREATS OF DIGITAL TECHNOLOGIES AND SYSTEMS PRODUCTION AND MANAGEMENT IN BELARUSIAN ENTERPRISES

V. B. Kryshtanosau
Belarusian State Technological University, Republic of Belarus, Minsk, Sverdlova str. 13a, 220006
DOI: 10.31618/NAS.2413-5291.2024.2.98.859

АННОТАЦИЯ

Исследуется цифровая трансформация белорусских предприятий. Отмечена прямая корреляция между оценкой предприятиями будущих рисков и угроз и имеющимся негативным опытом противодействия цифровым атакам.

Предложен цифровой инструментарий, направленный на нивелирование (минимизацию) цифровых рисков и угроз, с учетом приоритета отечественных программных средств. Обоснована целесообразность разработки цифровых систем, аналогичных российским «Мультисканер», «Антифишинг», «Антифрод», для имплементации их организациями и институтами государственного управления. Обоснована необходимость создания на базе Национального центра кибербезопасности национальной платформы кибербезопасности.

ABSTRACT

The paper reveals the digital transformation of Belarusian enterprises. It has been a direct correlation between enterprises' assessment of future risks and threats and existing negative experience in countering digital attacks noted. A digital toolkit is proposed aimed at leveling (minimizing) digital risks and threats, taking into account the priority of domestic software. The feasibility of developing digital systems similar to the Russian "Multiscanner", "Anti-Phishing", "Antifraud", for their implementation by organizations and public administration institutions. The need to create a national cyber security platform on the basis of the National Cyber Security Center is substantiated.

Ключевые слова: цифровая трансформация, цифровые технологии и системы управления и производства, кибербезопасность.

Keywords: digital transformation, digital technologies and management and production systems, cybersecurity.

Введение. В условиях текущих тенденций цифровой трансформации экономики, Республика Беларусь находится в начальной стадии данного процесса. Осуществляется фрагментарное внедрение цифровых технологий и цифровых систем производства и управления на уровне предприятий и отраслей. При этом представляется важным определить основные направления цифровой трансформации, так как это формирует среду новых цифровых рисков и угроз и требует разработки эффективных механизмов их нивелирования.

Основная часть. Осуществление сбора аналитической информации возможно на основе проведения опроса флагманских предприятий в ключевых отраслях экономики страны. Для проведения опроса была разработана анкета, в которой отражались вопросы о внедренных цифровых технологиях и цифровых системах, используемых в бизнес-процессах предприятий в настоящее время, а также о планируемых к внедрению (в течение ближайших 3-5 лет). Отдельным блоком были отражены вопросы, отражающие подверженность предприятий цифровым рискам и угрозам (взломам системы, краже или потере данных, внешним доступом к цифровым системам, DoS атаками и т.д.) и оценке вероятности возникновения новых рисков и угроз по мере внедрения новых цифровых решений на предприятии.

В результате 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%). С учетом динамики планирования и намерений внедрения цифровых инноваций в среднесрочной перспективе (3–5 лет), наиболее популярными цифровыми метатехнологиями станут роботизированные системы и Cloud

Computing (по 46,6% опрошенных предприятий), платформы (39,7%), Digital Twins и AI (по 37,9%), (34,5%), IoT (29,3%). 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 торговли – 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 (рис. 1). В разрезе наличия у предприятий цифровых технологий и систем, отмечается прямая корреляция опыта противодействия цифровым рискам и угрозам с наличием технологий Digital Twins, Cloud, Blockchain, BDA, роботизированных систем. При этом 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%) и очень высокие лишь 5,3% предприятий. Проведенное исследование полученных данных по методологии Пирсона, выявило прямую корреляцию между оценкой предприятиями будущих рисков и угроз и имеющимся негативным опытом противодействия цифровым атакам (рис. 2).

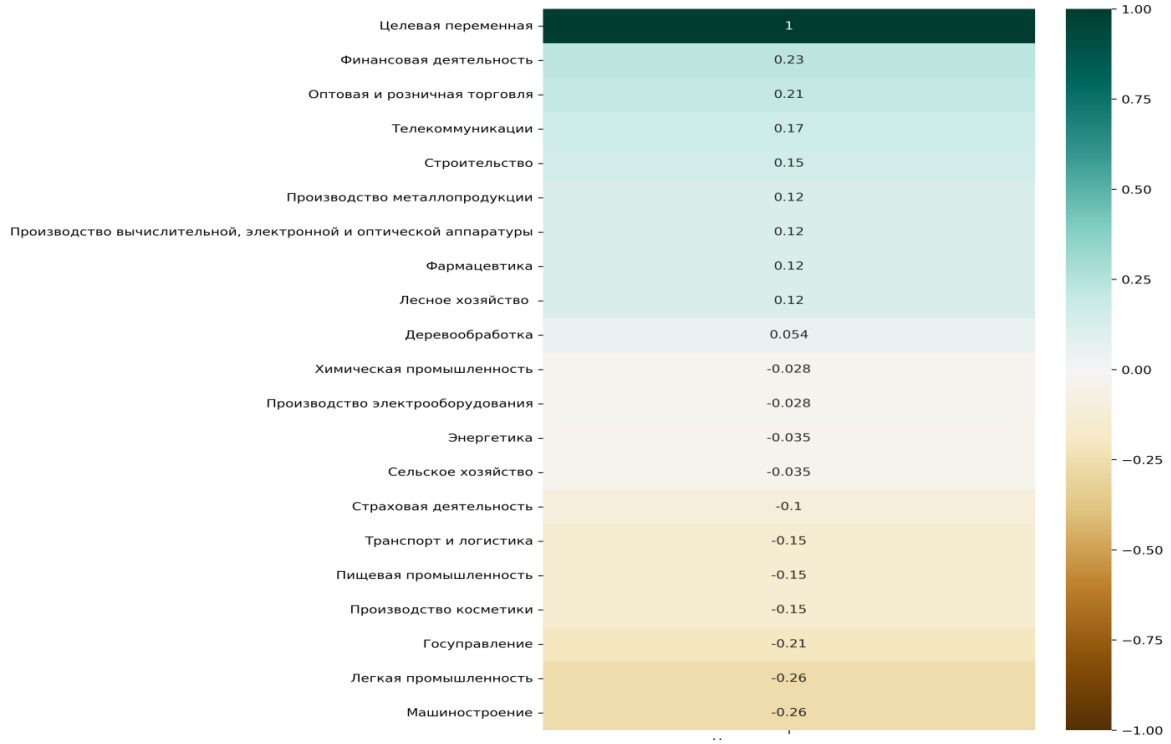
При этом крайне низко оценивают будущие цифровые риски и угрозы руководители предприятий легкой промышленности, производители вычислительной, электронной и оптической аппаратуры, фармацевтики, транспорта и логистики. Анализ данных проведенного опроса показал, что ряд руководителей сохраняют низкие оценки будущих цифровых рисков и угроз несмотря на имеющийся негативный опыт противодействия им. В особенности это характерно для таких сфер деятельности, как легкая промышленность, производство вычислительной, электронной и оптической аппаратуры, фармацевтика, транспорт и логистика (рис. 3). Это может свидетельствовать о недостаточном понимании рисков и угроз цифровой трансформации на уровне высшего менеджмента предприятий. Одним из механизмов решения данной проблемы может стать введение для руководителей предприятий (как государственных, так и частных) обязательных курсов по кибербезопасности в рамках MBA или переподготовки руководящих кадров в Академии управления при Президенте Республики Беларусь или Белорусском государственном университете информатики и радиоэлектроники (БГУИР).

Проведенный анализ цифровых технологий и систем, в разрезе их уязвимостей (внутренних и внешних угроз) и текущей имплементации

белорусскими предприятиями, позволяет сгруппировать их следующим образом:

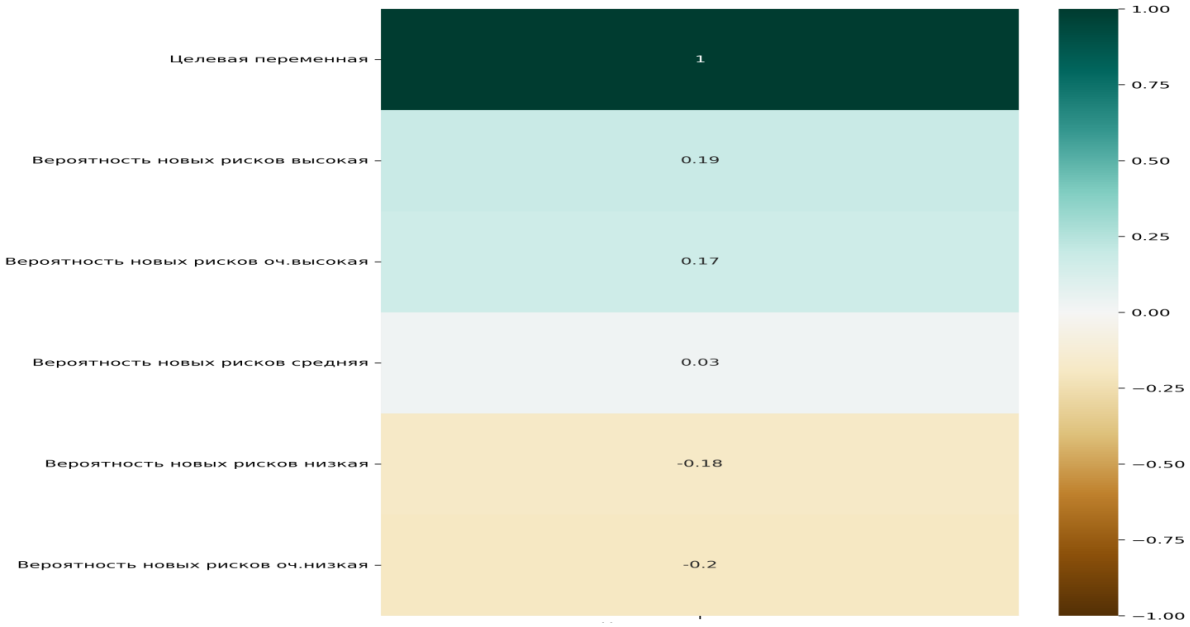
А. Цифровые технологии: а) генерирующие высокие цифровые риски и угрозы: IoT, роботизированные системы (в т.ч. RPA), AI; б) генерирующие средние цифровые риски и угрозы: Cloud Computing, BDA.

Б. Цифровые системы производства и управления: а) генерирующие высокие цифровые риски и угрозы: PDM, SCADA/CAM; б) генерирующие средние цифровые риски и угрозы: ERP (APS / MRP/MRPII), CRM, SCM.



Примечание – Составлено автором по результатам исследования.

Рис. 1 – Корреляция сферы деятельности предприятия с опытом противодействия кибератакам



Примечание – Составлено автором по результатам исследования.

Рис. 2 – Корреляция вероятности новых рисков с опытом противодействия кибератакам

Примечание – Составлено автором по результатам исследования.

Рис. 3 – Корреляция низкой оценки вероятности новых цифровых рисков и угроз с имеющимся опытом противодействия кибератакам

С целью нивелирования выделенных цифровых рисков и угроз в отношении наиболее уязвимых отраслей и секторов белорусской экономики требуется реализация соответствующих мероприятий по обеспечению кибербезопасности. В условиях санкционного воздействия, приоритет следует отдавать отечественным (белорусским и российским) программным средствам. Современные возможности специальных программных средств решают комплексные задачи, что позволяет предприятиям экономить сократить как перечень необходимых инструментов, так и расходы по их имплементации, интеграции с существующими системами, и последующей технической поддержкой. 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 – Deep Packet Inspection) применяется с целью идентификации информации о пользователях и приложениях, генерирующих сетевой трафик, что позволяет осуществлять его контроль [2]. В настоящее время на российском рынке тестируется система анализа трафика Гарда DPI, разработанная компанией Гарда Технологии. Одним из ИКТ решений для противодействия кибератакам систем IoT является технология программно-определяемых сетей (SDN – Software-Defined Networking), которая позволяет программировать сетевой трафик, перенаправлять его и автоматизировать выполнение политики сетевой безопасности. Технология виртуализации сетевых функций (NFV – Network Functions Virtualization) позволяет агрегировать ресурсы безопасности предприятия, обеспечивая киберзащиту всем пользователям сети [3]. ООО Киберпротект (включено в российский реестр отечественного ПО) осуществляет реализацию распределенных отказоустойчивых систем на основе данных технологий. АО Лаборатория Касперского для выполнения данной задачи разработана система Kaspersky IoT Infrastructure Security (включено в российский реестр отечественного ПО), агрегирующая данные, собранные с различных устройств, и передающая их в корпоративную сеть (или облачные платформы). Тем самым обеспечивается кибербезопасность всей IoT-инфраструктуры.

Роботизированные системы (в том числе RPA) представляют собой сложную производственную (коммерческую) систему, подверженную комплексным киберфизическим рискам и угрозам. Для решения задачи обеспечения кибербезопасности в том числе роботизированных систем предприятия АО Лаборатория Касперского разработана система Kaspersky Industrial CyberSecurity (включено в российский реестр отечественного ПО), которая обеспечивает защиту промышленной инфраструктуры на всех уровнях: от серверов SCADA и рабочих станций операторов до программируемых логических контроллеров и сетевого оборудования. ПО позволяет

обнаруживать и предотвращать кибератаки различной степени сложности, в том числе вызванные человеческим фактором, вредоносными программами, атаками APT и действиями хактивистов, обеспечивая непрерывность технологических процессов. При этом система позволяет обеспечить видимость происходящего на всех уровнях технологического процесса и предоставляет расширенные возможности по обнаружению, расследованию и реагированию на киберинциденты в рамках всей промышленной инфраструктуры. Система выявляет аномалии и вторжения в SCADA, CAM на ранних этапах и обеспечивает необходимые контрмеры для предотвращения ущерба технологическим процессам. Комплексное решение для защиты промышленных предприятий разработано компанией Positive Technologies – это система глубокого анализа технологического трафика для выявления сложных атак внутри сетей SCADA и проактивного поиска киберугроз (Industrial Security Incident Manager, PT ISIM 4) [4]. Система позволяет осуществлять контроль изменений конфигураций, настроек безопасности, пользовательских политик доступа, обнаруживать SCADA-специфичные вредоносные программы, инструменты APT, выявлять атак и аномалии, осуществлять проактивный поиск киберугроз.

Cloud Computing является важнейшей цифровой технологий, внедрение которой позволяет оптимизировать расходы предприятий на развитие и поддержание цифровых систем, трансформируя постоянные издержки в переменные. В Республике Беларусь услуги в сфере Cloud Computing оказывает ООО «Белорусские облачные технологии», которое является одним из ведущих поставщиков облачных решений, ИТ-инфраструктуры и хостинга, предоставляя услуги опорной сети для Единой сети передачи данных и Республиканского центра обработки данных. **Республиканская платформа с** применением системы защиты информации позволяет beCloud обеспечивать киберзащищенный облачный сервис. Для пользователей Cloud Computing данный сервис провайдера предоставляет возможность сократить капитальные расходы, увеличить производительность и скорость реагирования на внешние цифровые риски и угрозы, использовать резервное копирование. Кроме того, компания предлагает комплекс программно-аппаратный «Шлюз безопасности Bel VPN Gate 4.5» (ПАК Bel VPN Gate) предназначено для защиты информации (сетевого трафика), поступающей в информационную систему и/или выходящей из нее, а также обеспечивающим защиту информационной системы посредством фильтрации потока информации. При оказании услуги beCloud обеспечивает техническую и криптографическую защиту информации в соответствии с требованиями Оперативно-аналитического центра при Президенте Республики Беларусь (ОАЦ).

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. Обеспечение защиты Big Data предприятия предполагает введение соответствующей политики контроля доступа к конфиденциальным данным, на основе ролей и принципа минимальных привилегий. Важное значение для обеспечения безопасности данных является их шифрование при хранении и передаче. Шифрование данных при передаче предотвращает атаки через посредника (АП). Мониторинг сетей и систем с использованием решения для управления информацией о безопасности и событиями (SIEM) помогает обнаруживать угрозы на ранней стадии благодаря агрегированию данных с сетевых устройств, серверов и приложений для выявления аномалий. Это позволяет предотвратить угрозы нулевого дня, которые не имеют соответствующих сигнатур, и не могут быть обнаружены антивирусным ПО. Инструменты предотвращения потери данных (DLP) помогают предотвратить утечку конфиденциальных данных из защищенных систем. В Российской Федерации в 2022-2023 годах 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]. ПО Kaspersky Security для систем хранения данных является комплексным решением для защиты любых типов данных, которое обеспечивает несколько уровней для проверки объектов, что позволяет снизить нагрузку на серверы и исключить «антивирусный шторм» при проверке значительного количества сущностей. Система позволяет выявлять вредоносные программы и пресекать попытки удаленного шифрования. Разработку систем обеспечения безопасности Big Data и независимый аудит операций с базами данных и бизнес-приложениями осуществляет компания Гарда Технологии (РФ). ПО «Акронис Защита Данных» ООО Киберпротект является российской системой резервного копирования, поддерживающей резервирование в любой инфраструктуре, включая облачную. Для шифрования Big Data компания Аладдин Р.Д. (РФ) разработала систему криптографической защиты информации с возможностью централизованного управления Secret Disk для Linux 2.0. Система позволяет внедрить криптографическую защиту информации и двухфакторную аутентификацию, а также централизованно управлять политиками шифрования на большом количестве рабочих станций. Российская группа компаний «Астра» реализует защищенную операционную систему Astra Linux со встроенными средствами защиты информации. В Республике Беларусь ЗАО Банковско-финансовая телесеть предлагает услуги по организации стационарного узла шифрования.

Среди белорусских компаний услуги по «Предотвращению утечки данных» (DLP) оказывает BeCloud, которая на основе республиканской платформы реализует модель облачных сервисов «Программное обеспечение как услуга» (SaaS). ПО позволяет выявлять случаи нарушения политики безопасности организации в отношении конфиденциальных данных путем анализа всей информации: исходящей, входящей и циркулирующей внутри организации. Кроме того, BeCloud предоставляют услугу «Объектное облачное хранилище» (DSaaS) как инструмент для хранения Big Data. ПО для шифрование Big Data в Республике Беларусь предоставляет Научно-производственное республиканское унитарное предприятие Научно-исследовательский институт технической защиты информации. Отечественные разработки криптографической защиты информации «Сигма» и «NTCrypto» предоставляет возможность пользователям осуществлять безопасное хранение ключевой информации с выполнением соответствующих криптографических преобразований. Использование данного ПО позволяет в целом снизить или нивелировать цифровые риски и угрозы в отношении цифровых систем производства и управления, функционально обеспечивающих хранении коммерчески чувствительной информации, включая PDM, CRM и ERP (APS/MRP/MRPII). ERP системы представляют стержневой элемент управления современных компаний. Взлом данной системы открывает злоумышленникам доступ к личной информацию сотрудников, клиентов и поставщиков, позволяет осуществить кражу, модифицировать либо удалить финансовые записи, нарушить администрирование процессов закупок, выявить критически важные бизнес-операции, повредить данные либо полностью останавливая цифровые бизнес-процессы компании. Безопасность ERP систем базируется обеспечении защиты цифровой инфраструктуры, сетевых и операционных систем, баз данных. Одним из специальных решений, обеспечивающих безопасность функционирования ERP системы предприятия (как и CRM) является использование возможностей облачной инфраструктуры. В Республике Беларусь BeCloud предоставляет услуги хостинга ПО «1С Предприятие 8» и «1С: CRM ПРОФ для Беларуси». Важно отметить, что с учетом специфики ERP систем, обеспечение их бесперебойного и киберзащищенного функционирования позволяет минимизировать цифровые риски и угрозы в отношении SCM систем.

Среди отраслей и секторов белорусской экономики, находящихся в зоне наибольшего цифрового риска, находятся, в том числе, финансовая и страховая деятельность, государственное управление, транспорт и логистика, оптовая и розничная торговля, производство электрооборудования, машиностроение, фармацевтика, ИКТ. С учетом проведенного анализа на основе актуальных отечественных цифровых программных средств представляется возможным с учетом функциональной специфики предложить использование ряда решений. Актуальная оценочная стоимость цифровых средств киберзащиты варьируется в зависимости от предлагаемых решений, специфики отрасли и эксплуатируемых цифровых технологий и систем производства и управления. Так, стоимость реализации технических решений для нивелирования основных цифровых рисков и угроз, связанных с системами IoT, составляет около 930 тыс. росс. рублей. Киберзащита роботизированных систем – от 500 тыс. росс. рублей; Cloud Computing – от 320 руб.; BDA – 348 руб. для простых систем и до 150 тыс. руб. для комплексной защиты инфраструктуры; ERP (на базе 1С) – 1460 руб.; CRM – 225 руб. Данные цифровые решения позволяют минимизировать (нивелировать) текущие и потенциальные цифровые риски и угрозы, обеспечивая необходимую устойчивость развития белорусских предприятий и организаций среднесрочной перспективе. Отдельно следует отметить целесообразность использование гибких моделей ценообразования благодаря подходу «кибербезопасность как услуга» (CSaaS). Государственные и частные предприятия имеют возможность использовать формируемую инфраструктуру внутренних центров кибербезопасности для приобретения полноценных сервисов в рамках модели CSaaS, что позволит обеспечить экономию финансовых ресурсов в случае масштабирования услуг кибербезопасности в рамках холдингов или отраслей.

Вместе с тем отдельный блок цифровых рисков и угроз связан с государственным управлением. Привлечение внешних исполнителей для обеспечения кибербезопасности используемых цифровых систем и Big Data с точки зрения национальной безопасности представляется неоптимальным. В этой связи представляется целесообразным воспользоваться опытом Российской Федерации, которая на базе Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) осуществляет работу по развитию государственных систем в области кибербезопасности, включая имплементацию таких цифровых систем как «Мультисканер», «Антифишинг», «Антифрод» и других для защиты государственных информационных систем. В Республике Беларусь данную функцию в рамках компетенции может на себя взять сформированный в стране в 2023 году Национальный центр кибербезопасности. Данный государственный институт цифровой безопасности должен взять на себя компетенции по созданию национальной платформы кибербезопасности. Анализ международного опыта показывает, что структурно она должна включать четыре ключевых системы: а) обновляемую в режиме 24/7 базу

сигнатур киберугроз, формируемую специальными ИТ службами по результатам анализа: имевших место внутренних киберинцидентов, внешнего взаимодействия с дружественными государствами; и в рамках государственно-частного партнерства; б) систему мониторинга цифровых рисков и угроз со встроенными элементами AI, с учетом контекстуализации цифровых следов и отслеживания потенциального развития рисков и угроз; в) автоматизированную систему нивелирования (минимизации) цифровых рисков и угроз, алгоритмы которой базируются на разработанном подходе «план аварийного восстановления» (DRP); г) систему управления DRP, включающую приоритезацию нивелирования цифровых угроз в рамках соответствующего регламента с учетом особенностей атакованного предприятия, отрасли и разновидности атаки.

Заключение. Таким образом, на основе данных проведенного опроса выявлены актуальные цифровых технологии и системы производства и управления, используемые белорусскими предприятиями в рамках производственно-экономической деятельности, среди которых выделяются Cloud Computing, роботизированные системы, BDA, IoT. В разрезе цифровых производственных и управленческих систем, наибольшее распространение получили ERP (APS/MRP/MRPII), SCADA, CAM, CRM CAD/CAE, PDM, BPM. Анализ результатов опроса показал, что на долю иностранных систем приходится более 60% всех цифровых систем предприятий: они превалируют среди систем BIM, CAPP, SCADA, CAM, CAD, CAE, 3D-печати, MDM, TQM. Выделены риски, связанные с продолжением использования данных систем в условиях санкционного давления.

Список литературы

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

2. Awati R. Scarpati J. Definition: deep packet inspection (DPI) [Электронный ресурс]. URL: https://www.techtarget.com/searchnetworking/ definition/deep-packet-inspection-DPI (дата обращения: 20.01.2024).

3. Широкий Ю. Технологии кибербезопасности в эпоху IoT [Электронный ресурс]. URL: https://www.cta.ru/articles/cta/oborudovanie/ setevoe-oborudovanie/124332/ (дата обращения: 20.01.2024).

4. Positive Technologies Industrial Security Incident Manager [Электронный ресурс]. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/products/isim/ PT-ISIM-DS-05-2022.pdf (дата обращения: 14.01.2024).

5. Лыткин С. Обзор защищённых платформ и накладных средств безопасности больших данных [Электронный ресурс]. URL: https://www.anti-malware.ru/analytics/Market_Analysis/Big-Data-Protection#part3 (дата обращения: 08.01.2024).

УДК 378.4: 811.111
МРНТИ 16.41.21

ИЗУЧЕНИЕ ИНОСТРАННОГО ЯЗЫКА В ИНКЛЮЗИВНОЙ СРЕДЕ ВУЗА

Мусина Саулеш Кайсаровна
НАО ЕНУ имени Л.Н. Гумилева, Астана, Казахстан
Муканова Салтанат Канатхалиевна
ЕНУ имени Л.Н. Гумилева, Астана
Нургалиева Улжан Сайновна
НАО ЕНУ имени Л.Н. Гумилева, Астана, Казахстан

LEARNING A FOREIGN LANGUAGE IN AN INCLUSIVE UNIVERSITY FIELD

Mussina Saulesh Kaissarovna
NJSC ENU named after L.N. Gumilyov
Mukanova Saltanat Kanatkhalievna,
NJSC ENU named after L.N. Gumilyov
Nurgaliyeva Ulzhan Sainkyzy
NJSC ENU named after L.N. Gumilyov
DOI: 10.31618/NAS.2413-5291.2024.2.98.860

АННОТАЦИЯ

В данной статье представлен опыт работы в условиях инклюзивного образования в различных высших учебных заведениях. Обзор источников показывает, что проблемы инклюзивного высшего образования реализуются в Казахстане частично. Проведен опрос и анализ преподавателей ВУЗов по вопросам работы в инклюзивной среде. Рассматриваются основные принципы и подходы к созданию вузовской среды, способствующей инклюзивности и участию студентов с различными специальными потребностями. Авторы также обсуждают важность организационной поддержки и предлагают практические рекомендации для создания более доступной и равноправной образовательной среды в вузах. При исследовании инклюзивного образования в вузе при обучении иностранного языка предложены методы и формы обучения. Внедрение принципов инклюзии в обучении иностранного языка в вузе имеет