

УДК 658.51

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ИННОВАЦИОННЫХ ИТ-РЕШЕНИЙ ДЛЯ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ БИЗНЕС-ПРОЦЕССОВ КОММЕРЧЕСКИХ СТРУКТУР

Цыплакова П.Ю.,

МИРЭА – Российский технологический университет, Москва,
email: p_tsyplakova@mail.ru, alexbulinmirea@gmail.com, bur77@mail.ru

Булин А.А.,

МИРЭА – Российский технологический университет, Москва,
email: p_tsyplakova@mail.ru, alexbulinmirea@gmail.com, bur77@mail.ru

Бурлаков В.В.,

МИРЭА – Российский технологический университет, Москва,
email: p_tsyplakova@mail.ru, alexbulinmirea@gmail.com, bur77@mail.ru

***Аннотация.** В настоящее время риск возникновения непредвиденных обстоятельств является неотъемлемой частью бизнеса. Эффективность управления в подобных ситуациях напрямую зависит от готовности организации к внештатным событиям. Обеспечение непрерывности бизнес-процессов становится краеугольным камнем успешной работы компаний в современном мире, особенно в контексте информационной безопасности, анализе рисков, прогнозировании угроз. Сегодняшние условия рынка требуют от компаний сохранения конкурентоспособности и устойчивости, что делает обеспечение непрерывности бизнеса одним из ключевых направлений стратегического и оперативного управления. Ведется активная разработка подходов к управлению непрерывностью бизнеса, включая алгоритмы выявления рисков и разработку мер по их минимизации с использованием как внутренних, так и внешних ресурсов. Планирование непрерывности бизнеса приобретает первостепенное значение, особенно для коммерческих организаций, поскольку нештатные и чрезвычайные ситуации могут возникнуть внезапно независимо от успешности и размера компании. Готовность организации к различным сценариям развития событий, даже самым маловероятным, свидетельствует о заботе руководства о безопасности бизнеса и о заинтересованности сторон, что положительно сказывается на репутации компании. Программное обеспечение для управления непрерывностью бизнеса помогает компаниям выявлять риски, проводить анализ влияния на бизнес, повышать устойчивость организации и внедрять политики и процедуры для минимизации последствий возможных сбоев. Цифровые платформы, такие как управление непрерывностью бизнеса, помогают компаниям продолжать работать в обычном режиме в случае непредвиденных обстоятельств, таких как перебои в подаче электроэнергии, кибератаки и наводнения. В статье рассматриваются текущие тенденции внедрения автоматизированных систем в области непрерывности бизнеса, а также проводится анализ преимуществ и недостатков существующих ИТ-продуктов в этой сфере. В работе приведены примеры как отечественных, так и зарубежных систем.*

Ключевые слова: инновационные ИТ-решения, бизнес-процессы, коммерческие структуры, непрерывность бизнеса.

COMPARATIVE ANALYSIS OF INNOVATIVE IT SOLUTIONS TO ENSURE THE CONTINUITY OF BUSINESS PROCESSES OF COMMERCIAL STRUCTURES**Tsyplakova P.Y.,**MIREA – Russian Technological University, Moscow,
email: p_tsyplakova@mail.ru, alexbulinmirea@gmail.com, bur77@mail.ru**Bulin A.A.,**MIREA – Russian Technological University, Moscow,
email: p_tsyplakova@mail.ru, alexbulinmirea@gmail.com, bur77@mail.ru**Burlakov V.V.,**MIREA – Russian Technological University, Moscow,
email: p_tsyplakova@mail.ru, alexbulinmirea@gmail.com, bur77@mail.ru

Abstract. *Currently, the potential for unforeseen events forms an integral part of the business landscape. The efficacy of management in such situations directly depends on the organization's preparedness for unexpected events. Ensuring business continuity has become a cornerstone for the successful operations of organizations in today's market, particularly with regard to information security, risk assessment, and threat prediction. Today's business environment requires companies to maintain their competitiveness and long-term sustainability. Ensuring business continuity is a key aspect of strategic and operational management, and approaches to managing this are actively being developed. This includes the development of algorithms to identify risks and implement measures to minimize them, utilizing both internal and external resources. Business continuity planning plays a crucial role, particularly for commercial organizations, as abnormal and emergency situations may arise without warning, regardless of a company's success or size. The preparedness of an organization for various scenarios, even the most unlikely ones, demonstrates management's dedication to business security and all stakeholders' interests, positively impacting the company's reputation. Based on a systematic approach to continuous planning, the fundamental principles and steps for the management of the process have been established. By utilizing this information, numerous companies have developed automated systems to ensure smooth operation within their organizations. These systems assist in automating routine tasks, performing complex computational processes, and creating predictive models and analyses. Business continuity management software allows companies to identify risks, conduct business impact assessments, enhance organizational resilience, and implement policies and procedures that minimize the effects of potential failures. Digital platforms such as business continuity managements allow companies to maintain normal operations in the event of unforeseen circumstances, such as power outages, cyberattacks, and natural disasters. The article explores current trends in the implementation of automated systems for business continuity, and analyses the advantages and disadvantages of existing information technology products in this area. It provides examples of domestic and international systems and discusses their merits and limitations.*

Keywords: innovative IT solutions, business processes, commercial structures, business continuity.

«Поскольку предприятия стремятся оставаться конкурентоспособными и удерживаться на плаву во все более сложном и развивающемся цифровом ландшафте, важность внедрения комплексной системы управления непрерывностью бизнеса (BCMS) приобретает решающее значение. При наличии правильных BCMS орга-

низации могут извлечь выгоду из повышения операционной эффективности» [7]. Управление непрерывностью бизнеса (ВСМ) включает в себя заблаговременное планирование потенциальных сбоев и разработку стратегий по уменьшению воздействия угроз. ВСМС позволяет определить области и виды риска, для принятия превентивных мер с целью снижения вероятности возникновения угроз. Жизненный цикл ВСР (англ. business continuity planning, ВСР) состоит из пяти основных шагов:

- Выявление рисков
- Анализ рисков
- Моделирование/создание стратегии
- Создание планов обеспечения непрерывности деятельности
- Обучение и поддержка

Процесс планирования непрерывности бизнеса циклический. Каждый этап основывается на итогах предыдущего шага, что позволяет построить качественную, масштабируемую систему, которая будет соответствовать стратегическим целям компании. На рисунке 1 представлены этапы жизненного цикла обеспечения непрерывности бизнес-процессов.

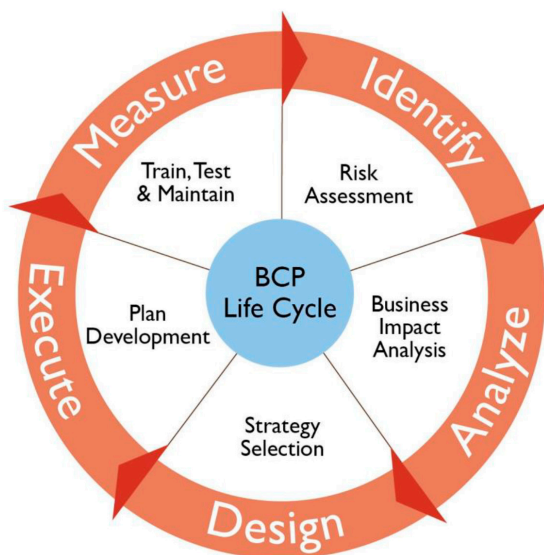


Рис. 1. Этапы жизненного цикла обеспечения непрерывности бизнес-процессов

Использование программного обеспечения в управлении непрерывностью бизнеса помогает компаниям выявлять и устранять возможные сбои в работе организации. Программное обеспечение включает в себя множество модулей, которые должны соответствовать этапам жизненного цикла процесса непрерывности: выявлять риски, количественно оценивать разрушительный потенциал угроз, принимать меры по предотвращению и минимизации рисков, а также соблюдать требования, представленные перед организацией законодательными органами внутренними нормативными документами. Система активно внедряется во все внутренние процессы организации включая комплаенс, управление рисками, а также отделы, ответственные за управление качеством и безопасность. Данного вида автоматизированные системы внедряют как часть стратегии по управлению рисками, кибербе-

зопасностью и комплаенсом. Имея достаточный функционал, такая система может помочь спрогнозировать и минимизировать угрозы, помочь в аварийном восстановлении, произвести оповещение, тестирование и обучение сотрудников, что позволит автоматизировать значительную часть процесса непрерывности в компании.

Цель исследования

Цель данной работы состоит в изучении и исследовании передовых, инновационных ИТ-технологий в области обеспечения непрерывности бизнеса, а именно внедрения автоматизированных систем с целью устойчивого функционирования бизнес-процессов организации

Материалы и методы исследования

«Стабильность организации является важнейшей динамической возможностью для управления непрерывностью бизнеса, особенно во времена кризиса» [4]. Автоматизация позволяет повысить эффективность внутренних процессов организации, избежать и спрогнозировать риски и угрозы, а также обеспечить гибкость при изменениях внешней среды. В современном мире использование автоматизированных систем по управлению непрерывностью бизнеса становится все более актуально. Причиной этого является растущее число угроз, с которыми сталкивается организация. Такие угрозы могут нарушить бесперебойную работу бизнеса и повлечь огромные финансовые и репутационные потери. Помимо этого, автоматизированные системы дают возможность сократить время на выполнение рутинных задач, уменьшить влияние человеческого фактора, улучшить текущие модели по управлению ресурсами, строить свои модели для внутренних процессов и помогать в принятии стратегических решений. Кроме того, автоматизированные системы помогают обеспечить устойчивую, бесперебойную работу, что является необходимым условием при создании внутреннего процесса обеспечения непрерывности. Таким образом, использование автоматизированных систем при выстраивании процесса непрерывности в организации, является ключевым инструментом для современных компаний, целью которых стоит построение устойчивого, развивающегося и конкурентноспособного бизнеса.

Результаты исследования и их обсуждение

Автоматизированные системы могут помочь организациям эффективно выстроить процесс непрерывности бизнеса и обеспечить грамотное управление этим процессом. Системы могут создавать планы по обеспечению непрерывности, внедрять их во внутреннюю организационную и процессную структуру, а также тестировать и модернизировать их. В случае наступления чрезвычайной ситуации система способна запустить необходимый план, для более оперативного восстановления работоспособности компании. Улучшение координации между различными подразделениями – автоматизированные системы могут помочь организациям улучшить координацию между различными подразделениями, которые участвуют в управлении непрерывностью бизнеса. Это поможет обеспечить согласованное и эффективное реагирование на сбои. Повышение осведомленности о рисках – автоматизированные системы могут помочь организациям повысить осведомленность о рисках, которые могут нарушить их работу. Это поможет быстро принять меры по предот-

вращению сбоев и более быстрому восстановлению работы организации в случае сбоев. Снижение затрат на управление непрерывностью бизнеса — автоматизированные системы могут помочь организациям снизить затраты на управление непрерывностью бизнеса. Это может быть достигнуто за счет более эффективного использования ресурсов и более быстрого восстановления работы организации в случае сбоя. В целом, использование автоматизированных систем в управлении непрерывностью бизнеса может помочь организациям повысить свою устойчивость к сбоям и обеспечить более быстрое восстановление работы в случае сбоя.

Разобрав текущие потребности пользователя, можно вычленил основной функционал систем управления непрерывностью бизнеса. Это не исчерпывающий перечень, внедрение дополнительных элементов системы, возможно при необходимости.

Функционал ПО должен содержать следующие аспекты:

1. Этапы, связанные с жизненным циклом процесса:

- Выявление рисков и угроз, анализ — анализ влияния на бизнес (BIA) По своей сути, анализ воздействия помогает организациям выявлять конкретные риски и угрозы для операций, финансовых показателей, репутации, сотрудников и цепочек поставок. Анализ влияния является базой для построения процесса идентификации, оценки и прогнозирования рисков и угроз

- Моделирование/создание стратегии — планирование определяет стратегию восстановления бизнеса и описывает их. Создается методология использования тех или иных ресурсов и планов

- Создание планов обеспечения непрерывности — план обеспечения непрерывности бизнеса (BCP) — это процесс, который определяет потенциальное воздействие чрезвычайных ситуаций. Система должна давать возможность пользователю разрабатывать политику реагирования на ИС/ЧС и помогать предприятиям быстро восстановиться, чтобы они могли функционировать в обычном режиме. BCP обычно создается до стихийного бедствия и в нем участвуют ключевые заинтересованные стороны компании. «Наличие хорошо разработанного плана обеспечения непрерывности бизнеса гарантирует, что ваши сотрудники и активы смогут безопасно и быстро вернуться к работе после аварии» [10].

- Обучение и поддержка — обучение пользователей и поддержка пользователей находящихся на территории чрезвычайной ситуации или участвующих в процессе ликвидации последствий ИС/ЧС

2. Репликация

- Возможность продолжить работу в случае выхода из строя одного центра обработки данных или серверной комнаты. «Облачное аварийное восстановление (DR) стало важнейшей стратегией обеспечения непрерывности бизнеса и защиты данных в условиях непредвиденных сбоев и катастроф» [5].

3. Отчетность

- Автоматизированные отчеты должны содержать полезную информацию и важную документацию, которыми можно поделиться с аудиторами соответствия требованиям, а также соглашения об уровне обслуживания (SLA), гарантирующие восстановление данных в установленные сроки.

Помимо всего жизненного цикла важно осуществлять «Программный подход к обеспечению непрерывности бизнеса и сами планы, используемые для восстановления бизнеса после сбоя, могут работать не совсем так, как ожидали разработчики плана» [1].

При анализе автоматизированных систем рассматривались самые популярные и функциональные российские и зарубежные продукты в области устойчивого функционирования. RiskOptics служит для упрощения и автоматизации инициатив в части обеспечения непрерывности бизнеса, а именно управление рисками GRC. Программное решение позволяет выявлять угрозы, отслеживать риски и управлять ими. Система имеет два модуля.

ROAR и ZenGRC. ZenGRS предназначен для организаций со сложными требованиями к управлению рисками, модуль подстраивается под потребности конкретных заказчиков. Дает возможность управлять рисками на всех этапах от разработки перечня возможных рисков, до выявления и фиксации.

ROAR дает вам возможность видеть, понимать ИТ-риски и кибер-риски и действовать в соответствии с ними, автоматизировать соблюдение требований и сообщать о влиянии на главные приоритеты вашей организации.

Desk Alters – решение для внутренних коммуникаций упрощает немедленную связь с персоналом во время чрезвычайной ситуации, включая ИТ-проблемы. Кроме того, сотрудники могут мгновенно получать важные пошаговые инструкции благодаря возможностям системы обмена сообщениями, гарантируя, что они знают, что делать.

LOGICMANAGER – одно из самых полных решений. Включает в себя управление корпоративными и ИТ – рисками. Оценивает критичность бизнес-процессов. Мониторит НС/ЧС и связывает наступление чрезвычайной ситуации с конкретным планом ОНиВД. Предоставляет настраиваемые отчеты руководству компании. В процессе генерации планов система использует прогнозные модели.

QUANTIVATE – Программное решение для управления рисками и комплаенсом. Производит оценку угроз совместно с анализом влияния на бизнес, дает возможность создавать планы ОНиВД, генерирует тестовые угрозы и планы. Присутствует централизованное хранилище документации

На российском рынке количество таких систем значительно ниже, чем за рубежом. Это касается не только создания систем, но и их внедрения в работу компании. Большинство систем находятся на стадии разработки, а применение зарубежных систем – аналогов в российских компаниях редкость. В России можно встретить автоматизированные системы управления непрерывностью в крупных компаниях (СБЕР, ВТБ, OZON и т.д.). Зачастую такие компании сами разрабатывают ПО под свои потребности, а не покупают готовые пакетные решения за рубежом или у коллег по рынку.

Так как большинство систем компании разрабатывают для внутреннего использования, а соответственно информации в свободном доступе не так много рассмотрим несколько основных ПО для обеспечения непрерывности.

Security Vision BCP – первый в России продукт, направленный на обеспечение непрерывности бизнеса. «Продукт разработан с учетом актуальных российских и зарубежных стандартов в области обеспечения непрерывности (ISO 22301, ГОСТ Р ИСО 22301, Положение ЦБ РФ N 787-П, Указание ЦБ РФ N 4148-У, ПП РФ N 730 от 26.08.2013)» [9]. Продукт осуществляет поддержку непрерывности бизнеса и применяется в Business Impact Analysis (BIA) – в процессе оценке критичности бизнес-процессов компании, для последующего создания приоритетов и планов реагирования для каждого критичного процесса при наступлении НС/ЧС. Система позволяет автоматизировать операционное планирование и контроль на каждом этапе цикла (рис. 2).



Рис. 2. Цикл операционного планирования и контроля обеспечения непрерывности SV BCP

«Security Vision BCP – это решение автоматизации процесса обеспечения непрерывности и восстановление деятельности (ОНиВД) после наступления чрезвычайных ситуаций. Продукт находится на стыке технологий: затрагивает как процессы ИБ, оперируя последствиями реализации угроз, связанных с отказом работоспособности информационных систем, оборудования, утраты ключевых поставщиков, персонала или помещений, так и процессы ИТ, анализируя информационную модель предприятия, обслуживающие ресурсы, метрики работоспособности активов и процедуры восстановления» [9]. Помимо этого, система предоставляет модуль мониторинга для отслеживания НС/ЧС и фиксации инцидентов для дальнейшего анализа и построения плана эффективного реагирования. Вся система насчитывает порядка пятнадцати модулей:

- Модуль управления инцидентами
- Модуль управления активами и инвентаризацией
- Модуль управления уязвимостями
- Модуль анализа угроз кибербезопасности (ТИ)
- Модуль взаимодействия с НКЦКИ (ГосСОПКА)
- Модуль взаимодействия с ФинЦЕРТ
- Модуль управления рисками кибербезопасности
- Модуль управления соответствием обработки ПДн
- Модуль управления соответствием КИИ
- Модуль управления соответствием ISO 27001
- Модуль управления соответствием SWIFT
- Модуль управления соответствием PCI-DSS
- Модуль управления операционными рисками (Положение № 716-П Банка России)
- Модуль управления соответствием Положениям Банка России (683-П, 684-П, 672-П, 382-П)
- Модуль управления аудитами и стандартами информационной безопасности (проектный, собственный стандарт).



Рис. 3. Принцип автоматизированной системы управления непрерывностью бизнеса КоордКом

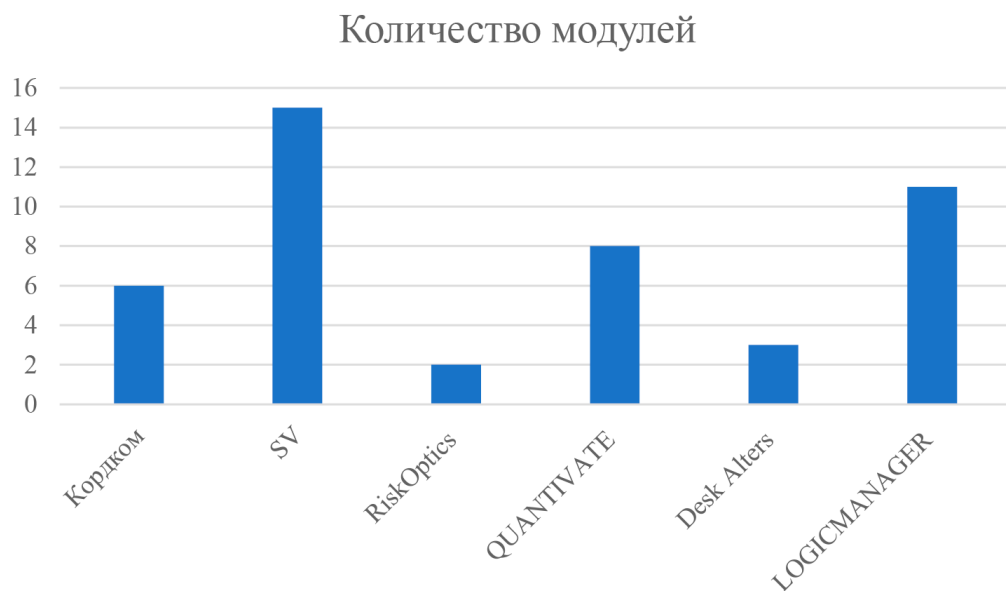


Рис. 4. График количества модулей систем

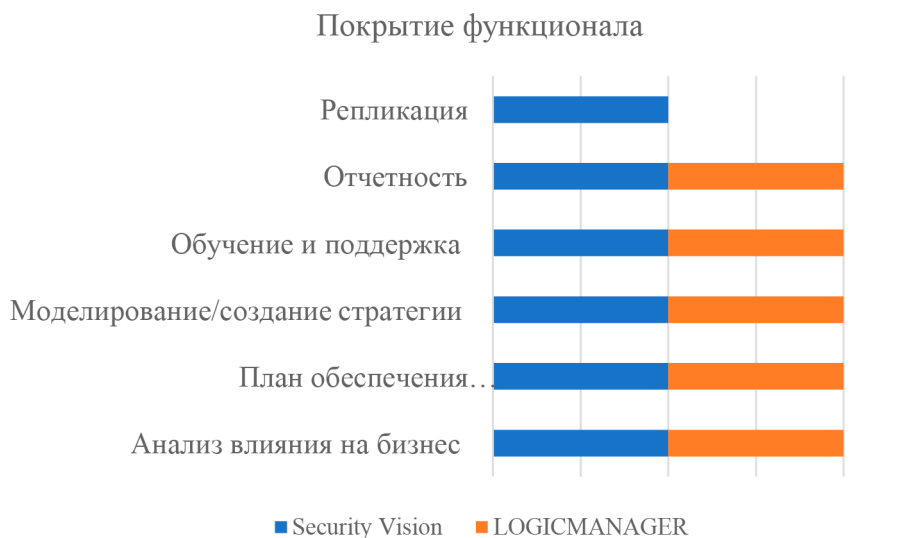


Рис. 5. Покрытие модулями основных этапов цикла непрерывности бизнеса

Отдельно возможно подключить резервное копирование данных.

Помимо Security Vision ВСП свои пакетные решения в области непрерывности в России продают КоордКом – платформа, на основе которой осуществляется построение системы экстренного реагирования и решения задач мониторинга и реагирования и взаимодействия в Системах-112 и АПК «Безопасный город». Продукт позволяет осуществлять более эффективный мониторинг, благодаря интеграции с ГИС системами, которые позволяют передать информацию о местонахождении, видеозаписей с камер видеонаблюдения, датчиков сигнализации и систем оповещения. На рисунке 3 представлен принцип автоматизированной системы управление непрерывностью бизнеса КоордКом.

Также в системе доступен функционал фиксации отклонений мониторинговых показателей и генерации аналитических отчетов на основе полученных отклонений. Система интегрирована со службами экстренного реагирования, что позволяет эффективно решать поставленные задачи.

Отобрав основные системы с самым наполненным функционалом, построим график количества модулей каждой системы (рис. 4). По текущей выборке Security Vision включает в себя наибольшее количество модулей, обеспечивающих непрерывность бизнеса.

Но не всегда раздутый функционал – это хорошо, важно понимать на сколько модули отвечают запросам конечного потребителя. В этом случае необходимо рассмотреть покрытие системы каждого этапа цикла непрерывности бизнеса. Выберем две самые наполненные системы (рис. 5).

Функционал двух систем LOGICMANAGER и Security Vision очень схож. Большая часть бизнес-потребностей пользователя удовлетворяется их функционалом. «Ключом к успешной стратегии обеспечения непрерывности бизнеса является построение хорошо продуманного плана и его тестирование во всей организации» [8]. Обе системы способны генерировать планы ОНиВД, а также активировать тестовые ситуации. Помимо этого, системы способны анализировать влияние

на бизнес, самостоятельно моделировать стратегию и составлять отчетность. Тем не менее Security Vision имеет один существенный плюс, наличие возможностей репликации данных. В данном случае для полной автоматизации всего процесса пользователям системы LOGICMANAGER придется докупать еще один продукт, что увеличит сумму затрат.

Выводы

«Автоматизация может стать ключевым рычагом обеспечения непрерывности текущего и будущего бизнеса» [11]. Использование автоматизированных систем в процессе непрерывности является преимуществом в борьбе с нестабильным миром, внезапными рисками и различными нештатными и чрезвычайными ситуациями, которые рано или поздно настигают каждую компанию, независимо от её размеров. «Ключом к разработке эффективной системы снижения непрерывности является знание того, где мы находимся сегодня» [6].

Можно заметить, что большая часть зарубежных систем направлены на управление рисками. «Управление рисками имеет значение. Это важно для организаций, которым нужен систематический, надлежащий контроль» [2], но риск менеджмент не исключает наличие других этапов в создании автоматизированного процесса непрерывности. Системы адаптивны для многих видов бизнеса, но не все забирают на себя поддержку всех этапов непрерывности бизнеса. В России, с учетом более позднего появления данного направления, системы более функциональны, они включают больше компонентов цикла непрерывности бизнеса. В зарубежных компаниях для полной автоматизации процесса непрерывности приходится внедрять несколько систем, затрагивающих разные этапы цикла, что приводит к большим финансовым затратам, связанным не только с внедрением таких систем, но и с поддержанием. Однако в зарубежных системах активно используются прогнозные модели и искусственный интеллект, что делает эти системы более адаптивными под запросы пользователя, смену рынка, различные НС/ЧС. В отечественных системах не часто можно встретить прогнозные модели. Можно предложить, что с большой вероятностью данный тренд накроет системы по обеспечению непрерывности бизнеса в ближайшие годы, что сделает их абсолютными лидерами по сравнению с зарубежными аналогами. Стоит отметить, что отечественные системы адаптированы под российскую законодательную базу, что уменьшает затраты на доработку в области нормативной документации. На текущий момент большинство зарубежных систем не поставляются на российский ИТ-рынок, что дает возможность еще больше развивать отечественные продукты, выходить на рынок небольшим стартапам или продавать внутренние решения больших компаний на внешний рынок.

Литература

1. Джеймс Кракс. Business Continuity Management: A Practical Guide to Organizational Resilience and ISO 22301.1-е изд. Kindle Edition, 2021. 362 p.
2. Дженнифер Гири. How to be a Chief Risk Officer: A handbook for the modern CRO. Нильсен, 2022. 238 с.
3. Саид Эсламян. Disaster Risk Reduction for Resilience: Disaster Risk Management Strategies. Springer, 2022. 811 с.
4. Ana Corrales, Loyda Lily Gomez Santos Universidad de La Sabana Sustainability and Resilience Organizational Capabilities to Enhance Business Continuity Management: A Literature

Review // MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations. 2021. № 4. P. 8196.

5. Hassan Ali Cloud Disaster Recovery: Planning and Implementing Business Continuity // ResearchGate. 2023.

6. Torabi S.A. Developing a Robust Business Continuity Framework for Supply Chain Resilience // International Journal of Production Research. 2022. № 59. P. 1-37.

7. Внедрение систем управления непрерывностью бизнеса // Risk Publishing. [Электронный ресурс]. URL: <https://riskpublishing.com/business-continuity-management-systems-implementation/> (дата обращения: 15.03.2024).

8. Планирование обеспечения непрерывности бизнеса: что делать и чего не делать в процессе // Agility. [Электронный ресурс]. URL: <https://www.agilityrecovery.com/article/business-continuity-planning-dos-and-donts-process> (дата обращения: 15.03.2024).

9. Продукт обеспечения непрерывности бизнеса (Security Vision BCP) как связующее звено между процессами ИТ и ИБ // Security Vision. [Электронный ресурс]. URL: <https://www.securityvision.ru/blog/produkt-obespecheniya-nepreryvnosti-biznesa-security-vision-bcp-kak-svyazuushchee-zveno-mezhdu-protsessami-it-i-ib> (дата обращения: 15.03.2024).

10. Business Continuity Planning // IT Chronicles. [Электронный ресурс]. URL: <https://itchronicles.com/business-continuity-planning-a-guide-to-create-an-effective-bcp/> (дата обращения: 22.03.2024).

11. Leveraging Automation to Achieve Business Continuity in the New Normal // UI Path. [Электронный ресурс]. URL: <https://www.uipath.com/blog/automation/business-continuity-leveraging-automation> (дата обращения: 23.03.2024).