УДК 334.7:004.415.2.043

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

[1]Чернова Е.В., [1]Гаврилова И.В., [2]Доколин А.С., [1]Романова М.В.

[1]ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», Магнитогорск, e-mail: HellenaChernova@mail.ru, Old_Raven@mail.ru, romanova.mv@mail.ru;

[2]МОУ «Средняя общеобразовательная школа № 28», Магнитогорск, e-mail: a.dokolin@gmail.com

Обеспечение непрерывности деловой активности компаний выступает важным преимуществом в конкурентной борьбе современных компаний. В настоящее время выделились два подхода к управлению непрерывностью бизнеса, в каждом из которых ключевая роль отводится информационным технологиям. Средства обеспечения информационной безопасности снижают риски простоев из-за действий злоумышленников. Системы управления бизнес-процессами позволяют отслеживать выполнение бизнес-процессов, своевременно предупреждают об угрозах, предоставляют возможность совершенствовать работу с клиентами. Облачные технологии, изначально поддерживающие непрерывность сервисов, обеспечивают качественную ИТ-поддержку стартапам и небольшим компаниям. Были определены возможности систем управления бизнес-процессами в обеспечении непрерывности бизнеса. Была изучена практика применения облачных технологий в компаниях и выделили основные и дополнительные модели применения облачных технологий для обеспечения непрерывности бизнеса.

Ключевые слова: управление непрерывностью бизнеса, информационная безопасность, управление бизнес-процессами, iBPMS

INFORMATION TECHNOLOGY IN BUSINESS CONTINUITY MANAGEMENT

[1]Chernova E.M., [1]Gavrilova I.V., [2]Dokolin A.S., [1]Romanova M.V.

[1]Nosov Magnitogorsk State Technical University, Magnitogorsk, e-mail: HellenaChernova@mail.ru, Old_Raven@mail.ru, romanova.mv@mail.ru;

[2]High comprehensive school No. 28, Magnitogorsk, e-mail: a.dokolin@gmail.com

Ensuring the continuity of business activity is an important competitive advantage of modern companies. Currently separated two approaches of business continuity management, each with a key role for information technology. Information security means lower risks of downtime due to the actions of intruders. Business process management systems allow you to trace the execution of business processes, timely warn of threats, provide an opportunity to improve the work with clients. Cloud technologies, initially supporting continuity of services, provide quality IT-support to start-ups and small businesses. We determined Business Process Management Systems functionality for business continuity. We have studied the practice of applying cloud technologies in companies and provide basic and advanced models of cloud technologies for business continuity.

Keywords: business continuity management, information security, business process management, iBPMS

Ведение успешного бизнеса и конкурентоспособность современной организации в условиях информационного общества нуждаются в эффективных подходах к обеспечению непрерывного функционирования ключевых бизнес-процессов [1]. Очевидно, что даже для крупной фирмы кратковременный отказ работы клиентской системы ведет к финансовым убыткам, а для небольшой компании может оказаться фатальным. Первоочередной задачей руководства становится потребность в организации бизнес-процессов компании таким образом, чтобы ее функционирование не прекращалось при возникновении критических или внештатных ситуаций либо было возобновлено в кратчайшие сроки.

Управление непрерывностью бизнеса – «целостный процесс управления, в ходе которого выявляются потенциальные угрозы для организации и определяются возможные последствия для хозяйственных операций в случае осуществления этих угроз, а также создается основа обеспечения способности организации восстанавливаться и эффективно реагировать на инциденты, что гарантирует соблюдение интересов основных заинтересованных сторон, сохранение репутации, брэнда и деятельности по созданию добавленной стоимости» [2]. Согласно стандарту BS 25999-1:2006 «Business continuity management. Part 1: Code of practice», процесс управления непрерывностью включает в себя управление восстановлением и продолжением хозяйственной деятельности в случае нарушения нормального хода бизнеса, а также управление общей программой обеспечения непрерывности бизнеса посредством проведения обучения, учений и анализа с целью поддержания одного или нескольких планов обеспечения непрерывности бизнеса в актуальном состоянии [3, 4].

В данное время существует ряд стандартов в области управления непрерывностью деятельности организации, описывающих лучшие практики процесса управления непрерывностью и аварийного восстановления функционирования компании в чрезвычайных ситуациях. Наибольшее распространение среди них получили стандарты BS 25999-x Business Continuity Management, на базе которых в 2009–2012 гг. была разработана серия российских стандартов ГОСТ Р 53647.X «Менеджмент непрерывности бизнеса». В шести его частях представлены практическое руководство, требования, руководство по внедрению, руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности», требования к системе менеджмента персональной информации для обеспечения защиты данных, а также описаны положения, обуславливающие готовность организации к опасным ситуациям и инцидентам [4].

По мнению Сергея Петренко, в зависимости от области профессионального становления выделяются два основных подхода к обеспечению непрерывности бизнеса: обеспечение непрерывности выполнения ИТ-процессов и ИТ-сервисов (ИТ-подход) или поддержка работы систем, обеспечивающих основные бизнес-процессы и сведение данных в единые отчетные формы (бизнес-подход) [5]. Как мы видим, в обоих случаях основным механизмом обеспечения непрерывности бизнеса выступают информационные технологии. Возникает закономерный вопрос: как оптимально выстроить работу организации, опираясь на стандартные современные информационные технологии, с учетом потребностей непрерывного ведения деятельности, а также реагирования на возможные инциденты? По нашему мнению, основой решения этой проблемы выступает анализ бизнес-процессов с позиции их устойчивости к инцидентам, среди которых в первую очередь необходимо выделить наиболее критичные для ведения бизнеса и затем сгруппировать их относительно ИТ-процессов и услуг.

Согласно Business Continuity Management, первым шагом для разработки политики непрерывности бизнеса является «первичный анализ воздействия на бизнес, BIA – Business Impact Analysis, целью которого является ранжирование бизнес-процессов и ИТ-сервисов предприятия по степени критичности и получение первичной, достаточно общей, оценки вероятных потерь для бизнеса в случае нарушения функционирования названных процессов и сервисов» [3]. По мнению экспертов, проведение BIA является наиважнейшим пунктом для разработки функциональной программы BCM, поскольку непосредственно данные BIA дают руководству понимание того, что именно и в какой степени нуждается в защите и особом отношении. Стандарты BCM рекомендуют начинать BIA с разработки схем бизнес-процессов и основных информационных потоков организации. Одновременно с этим необходимо просчитать масштабы потерь от нарушения работы критичных бизнес-процессов и проанализировать основные информационные сервисы и их связи с бизнес-процессами и информационными потоками организации.

Сформулируем основные внутренние угрозы ведения бизнеса:

– утечка или утрата ценной информации (коммерческая тайна, информация о клиентах и поставщиках, экономическая информация);

– нарушение производственного цикла (прекращение или задержка предоставления услуг, остановка или задержка создания/предоставления продукта, задержка документационной поддержки услуг/продуктов);

– проблемы внутреннего управления организацией (задержка актуальной информации, проблемы контроля, оперативное взаимодействие разных структур, скорость принятия решений различными отделами и т.п.).

Опираясь на вышесказанное, можно отметить, что все выделенные угрозы так или иначе связаны с используемыми в компаниях информационными технологиями и, следовательно, организация любого уровня имеет критичную привязку к современным информационным технологиям, системам и сервисам.

Обеспечение информационной безопасности организации

Современные реалии ведения бизнеса таковы, что невозможно отделить процесс управления непрерывностью деятельности организации от процесса обеспечения информационной безопасности организации [6]. Безопасность функционирования любого бизнеса зависит от уровня понимания руководством организации значимости внедрения в деятельность компании ИТ-решений, связанных с защитой информации и информационной безопасностью.

Неоспорим тот факт, что стоимость и масштаб программного обеспечения для поддержки информационной безопасности будет различным для организаций различного уровня и различных областей, однако возможно выделить необходимый и реко-

мендуемый набор программных продуктов, уникальный для любого бизнеса. Основным объектом должны стать системы разграничения доступа, согласно штатным уровням работы с конфиденциальной информацией. Парольная защита должна быть естественной для работников на любой должности, и они должны понимать всю ответственность за нарушения работы с системой доступа. Применение такой системы позволит снизить риски утечки информации и облегчит контроль за действиями пользователя с информацией [7].

Следующими по важности становятся системы резервного копирования и правила их включения в деятельность организации. Резервное копирование – процесс создания копии информационного объекта на независимом носителе информации. Распространенными ошибками являются временные периоды создания резервной копии информации, хранение резервной копии на сервере с исходной информацией и ведение резервного копирования в рабочее время. Третьими по значимости можно выделить системы антивирусной защиты. Современные вредоносные программы могут проникать на рабочие станции даже при отсутствии подключения к интернету или запрете скачивать и загружать файлы из сети, их разнообразие и механизмы воздействия меняются с такой скоростью, что обычный пользователь не может быть подготовлен к самостоятельному противодействию и защите от заражения. Обновление вирусных баз так же является обязательным требованием, в противном случае неактуальный антивирус не сможет обеспечить полную защиту информации на рабочей станции и серверах.

Системы управления бизнес-процессами

Системы управления бизнес-процессами включают в себя методологию (чаще всего workflow-нотации, eEPC, BPMN) моделирования бизнес-процессов и программного обеспечения для их автоматизации.

Любая система управления бизнес-процессами содержит в себе следующие модули [8]:

– графический инструментарий, который предназначен для описания и анализа процессов;

– сервер выполнения заданий (сервер workflow) – основной сервер, на котором выполняются описанные процессы, при этом сервер контролирует состояние каждого процесса и бизнес-события в рамках этого процесса;

– средства оперативной работы для внесения изменений в ходе выполнения процесса, например при управлении списками заданий и рабочими приоритетами;

– инструменты мониторинга и управления, которые показывают, насколько процесс выполнен или на какой стадии находится, при каких условиях.

Развитие и интеграция интеллектуальных технологий в программные продукты расширили функционал систем управления бизнес-процессами и привели к появлению нового класса систем – iBPMS (intellectual Business Process Systems), которые кроме перечисленных выше компонентов включают в себя:

- дополнительные методы анализа выполнения бизнес-процессов, обеспечивающие непрерывность бизнес-процессов компании: реал-тайм бизнес-анализ, интерактивные панели управления, оповещения в исключительных ситуациях;
- более мощные инструменты бизнес-правил;
- социальные инструменты, позволяющие подключить как можно больше внешних источников, к которым относятся экспертные оценки и отзывы заказчиков;
- инструменты для работы с неструктурированной информацией, включая видео, аудио и социальные потоки;
- средства интеграции с разными аналитическими инструментами;
- поддержку мобильных устройств, позволяющих иметь доступ к бизнес-процессам 24 часа в сутки;
- средства обеспечения доступа на основе ролей, навыков и шаблонов взаимодействия.

Другими словами, управление непрерывностью бизнеса является одной из обязательных функций таких iBPMS.

Ежегодно Gardner Group анализирует рынок IBPM систем, группируя программные решения с помощью «Магического квадрата». Сопоставление и анализ квадратов позволили выявить следующие тенденции на рынке iBPMS [9].

1. На протяжении последних пяти лет лидирующие позиции занимают продукты Pegasystem, Appian и IBM, при этом наметилось отставание последней от своих конкурентов.

2. Несмотря на продолжающуюся консолидацию на рынке BPMS, в квадранте Gartner регулярно появляются новые вендоры. При этом стоит отметить две категории новичков: 1) вендоры, которые сфокусированы на своем BPMS-решении и при этом нейтральны к прочему ИТ-окружению (Bizagi, Auraportal, Axon Ivy); 2) вендоры, которые ориентированы на тесную интеграцию с продуктами Microsoft (K2, AgilePoint),

что позволит с наименьшими затратами организовать управление непрерывностью бизнеса в организациях, информационная инфраструктура которых построена на ИТ-решениях Microsoft.

3. Растущие требования рынка к BPMS-решениям вынуждают разработчиков постоянно совершенствовать свои продукты.

Впрочем, использование iBPMS могут позволить себе только компании, в которых успешно внедрен процессный подход к управлению: выделены и регламентированы бизнес-процессы, определены основные роли, описано окружение бизнес-процессов. Сфера деятельности компании при этом не имеет значения. В том случае, если процессы компании определены нечетко или же процессный подход не применяется вообще, эффекта от внедрения подобных систем не будет – а это значит, что организация непрерывности бизнеса будет осуществляться на основе типовых офисных пакетов, антивирусного программного обеспечения, автоматизированных рабочих мест и интернет-решений [10].

Облачные технологии

По данным журнала CNews около 90% организаций используют в своей деятельности облачные технологии – мощный инструмент управления непрерывностью бизнеса за счет обеспечения защиты данных и приложений на стороне поставщика услуг. Облачные инструменты успешно интегрировались в деятельность компаний за счет разнообразия и доступности сервисов, охватывающих любые потребности бизнеса: начиная от офисных программ, электронной почты, платежных систем и заканчивая разработкой программного обеспечения [11].

Выделяют три основных модели предоставления облачных инструментов:

1) инфраструктура как услуга (Infrastructure as a service), в рамках которой клиентам предоставляется компьютерная инфраструктура (объединенные в сеть виртуальные платформы или компьютеры), которые организация настраивает самостоятельно для решения своих бизнес-задач;

2) платформа как услуга (Platform as a service), при которой клиенту передается платформа с установленным системным и прикладным программным обеспечением;

3) программное обеспечение как услуга (Software as a service), при которой клиент получает доступ к лицензионным версиям необходимого ему программного обеспечения. Очевидно, что все эти модели могут использоваться совместно.

Разнообразие потребностей деловой среды привело к появлению дополнительных моделей [12]:

1) все как услуга (Everything as a Service) – организации при наличии доступа в интернет получают полностью информационную инфраструктуру, включая специализированные корпоративные информационные системы, поддерживающие управление бизнес-процессами;

2) аппаратное обеспечение как услуга (Hardware as a Service) – по сути, аренда компьютерного оборудования без программного обеспечения;

3) рабочее место как услуга (Workplace as a Service): в рамках данной модели компания-клиент на основе облачных технологий формирует для своих сотрудников автоматизированные рабочие места, снабженные всем необходимым программным обеспечением; очень часто такая модель используется для организации работы удаленных офисов;

4) данные как услуга (Data as a Service) – в рамках модели клиенту предоставляется дисковое пространство, которое он может использовать для хранения больших объемов информации; модель очень распространена среди физических лиц – пользователей глобальной сети;

5) безопасность как сервис (Security as a Service) – модель, основной идей которой является обеспечение безопасности используемых в компании информационных технологий и услуг.

Следует отметить, что использование облачных технологий не всегда избавляет организации от необходимости самостоятельного управления непрерывностью бизнеса, так как существует вероятность отказа в обслуживании даже у очень крупного и надежного поставщика облачных технологий. По этой причине необходимо продумать стратегии использования услуг альтернативных поставщиков, а также вопросы обеспечения сохранности конфиденциальных данных, составляющих коммерческую тайну. В то же время для некрупных компаний или стартапов зачастую уровень и объем предоставляемых облачных технологий вполне достаточен и, что важнее, финансово доступен.

Итак, несмотря на то, что проблема управления непрерывностью деятельности организации рассматривается достаточно давно (понятие непрерывного производства появилось ещё в XIX в.) [6], в ИТ-контексте эта проблема рассматривается на протяжении последних двадцати лет. В результате выделились два основных подхода к управлению непрерывностью деятель-

ности компаний: ИТ-подход, направленный на обеспечение работоспособности поддерживающих бизнес информационных технологий, и бизнес-подход, связанный с внедрением систем управления бизнес-процессами. Для реализации каждого подхода создан высокопроизводительный ИТ-инструментарий, который, совершенствуясь, позволяет организациям активно работать и развиваться в условиях отечественной кризисной экономики.

Список литературы

1. Ovchinnikova I.G., Kurzaeva L.V., Solomatina N.B., Chusavitina G.N., et al. Elaboration of a Frame Model for Intensification and Managing Requirements to Learning Outcomes in Regional Systems of Continuing Professional Education International Review of Management and Marketing. – 2016. – vol. 6, no. 2S. – P. 190–197. Available at: http://www.econjournals.com/index.php/irmm/issue/view/71 (accessed 18 October 2017).

2. Мусатов К. Непрерывность бизнеса. Подходы и решения // Jet Info. – 2017. – № 5 [Электронный ресурс]. – URL: http://www.jetinfo.ru/jetinfo_arhiv/nepreryvnost-biznesa-podkhody-i-resheniya/nepreryvnost-biznesa-podkhody-i/2007 (дата обращения: 15.12.2017).

3. Standard BS 25999-1:2006 «Business continuity management. Part 1: Code of practice». – British Standards. – 39 p.

4. Чернова Е.В. Профессиональные компетенции магистров бизнес-информатики в курсе «Управление непрерывностью бизнеса» / Е.В. Чернова // Научные труды SWorld. – Выпуск 3(44). Том 4. – Иваново: Научный мир, 2016. – 100 с.

5. Петренко С.А. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться. Информационные технологии для инженеров / С.А. Петренко, А.В. Беляев. – М.: ДМК Пресс; М.: Компания АйТи, 2011. – 400 с.

6. Chusavitina G.N., Zerkina N.N. Mery profilaktiki kiberekstremizma v podgotovke budushchikh uchitelei [Cyber Extremism Preventive Measures in Training of Future Teachers]. SGEM2015 Conference Proceedings, Book 1, Vol 2. – P. 275–280.

7. Folkers A. Continuity and catastrophe: business continuity management and the security of financial operations // Economy and Society. – 2017. – vol. 46(1). – P. 103–127.

8. Гаврилова И.В. Свободное программное обеспечение для управления бизнес-процессами / И.В. Гаврилова // Теория и практика применения свободного программного обеспечения Сборник трудов участников Всероссийской молодежной конференции с элементами научной школы. – 2011. – С. 144–147.

9. Анализ магических квадрантов Gartner [Электронный ресурс]. – Режим доступа: http://bpm-in-ua.com/article_id/27.html (дата обращения: 15.12.2017).

10. Bajgoric N. (n.d.). Information Architectures for Business Continuity // Continuous Computing Technologies for Enhancing Business Continuity, 2009, pp. 60–78.

11. Saleem M. Cloud Computing and Its Technologies: A Survey. IJARCCE. – 2017. – № 6(6).

12. Dhawan G. Conceptualization of Cloud Computing and its Security Threats, Challenges, Technologies and Application // International Journal for Research in Applied Science and Engineering Technology. – 2017. – V(IV). – P. 629–635.