УДК 378.1:338.24

АНАЛИЗ НЕПРЕРЫВНОСТИ БИЗНЕС-ПРОЦЕССОВ И ПОДДЕРЖИВАЮЩЕЙ ИНФРАСТРУКТУРЫ ВУЗА В СФЕРЕ ЭЛЕКТРОННОГО ОБРАЗОВАНИЯ

Чусавитина Г.Н.[1], Чусавитин М.О. [2]

[1] ФГБОУ ВПО «Магнитогорский государственный университет», Магнитогорск, Россия (455034, г. Магнитогорск, пр. Ленина, 114), e-mail: inform@masu-inform.ru
[2] ФГАОУ ВПО «Национальный исследовательский университет Высшая школа экономики», Москва, Россия (101000, г. Москва, ул. Мясницкая, д. 20), e-mail: hse@hse.ru

Нарушение непрерывности функционирования бизнес процессов и ИТ-сервисов электронной информационно-образовательной среды вуза ведет к снижению качества предоставляемых образовательных услуг и эффективности информационного обеспечения, потере конкурентных преимуществ образовательного учреждения и др. Проведенное обследование состояния дел в вузах позволило выделить типичные недоработки в области менеджмента непрерывности бизнеса. Построена обобщенная модель управления непрерывностью бизнеса. Согласно требованиям стандарта ГОСТ Р 53647 разработан и реализован проект по анализу непрерывности деятельности вуза в сфере оказания дистанционных образовательных услуг. В результате проекта идентифицированы ключевые продукты и услуги, а также поддерживающие их критических виды деятельности, предложены рекомендации по устранению выявленных недостатков в сфере управления непрерывностью электронного образования.

Ключевые слова: непрерывность деятельности (бизнеса) образовательной организации, модель управления непрерывностью бизнеса, анализ непрерывности, электронное образование, функционирование бизнес-процессов и ИТ-сервисов.

ANALYSIS OF BUSINESS CONTINUITY AND SUPPORTING INFRASTRUCTURE OF UNIVERSITY IN THE FIELD OF ELECTRONIC EDUCATION

Chusavitina G. N.[1] , Bondarenko E.V.[1], Chusavitin M. O.[2]

[1]Federal state educational institution of higher professional education «Magnitogorsk State University», 114 Prospekt Lenina, Magnitogorsk, Chelyabinskaya oblast 455038, Russia e-mail: inform@masu-inform.ru
2National Research University Higher School of Economics, 20 Myasnitskaya Ulitsa, Moscow 101000, Russia, email: hse@hse.ru

Continuity break of business processes and IT services of electronic informational and educational environment of the university leads to a decrease in educational quality, reduction of efficiency in information management and to the loss of competitive advantage, etc. Survey of current situation in universities has entitled the typical lacks of business continuity management. The generalized model of business continuity management was developed. According to the requirements of GOST R 53647, a project designed to analyze a continuity of a university, in case of provision of distance education services was developed and implemented. The project identified key products and services, their critical supporting activities, and provided recommendations of corrective to the identified gaps in the continuity of the e-learning management systems.

Key words: business continuity of educational organization; business continuity management model; continuity analysis; electronic education; continuity of business process and it-services.

В современном информационном обществе образовательные учреждения широко используют преимущества информационных и коммуникационных технологий (ИКТ) при реализации образовательных программ в форме электронного обучения (e-education) или с использованием дистанционных образовательных технологий. В Федеральном законе Российской Федерации «Об образовании» под электронным обучением понимается организация образовательного процесса с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-

телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие участников образовательного процесса. Под дистанционными образовательными технологиями – образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников [4].

Очевидно, что ИКТ являются критической частью инфраструктуры электронного образования, которая подвержена различным инцидентам, приводящим к нарушению непрерывности деятельности организации. Наиболее эффективным подходом к развитию устойчивости деятельности организации является подход, основанный на методологии управления непрерывностью бизнеса (УНБ). Под непрерывностью бизнеса (деятельности) (business continuity) мы будем понимать «стратегическую и тактическую способность организации планировать свою работу в случае инцидентов и нарушения ее деятельности, направленную на обеспечение непрерывности деловых операций на установленном приемлемом уровне» [1, с. 1]. Проблемы, связанные с УНБ организаций, и подходы к их решению сегодня находят отражение в ряде научных трудов зарубежных и отечественных ученых по экономике, менеджменту, информационной безопасности, кибернетике и информатике. Связано это с тем, что в современных условиях возрастает зависимость материальных и нематериальных активов организации, в том числе и репутации, от негативных воздействий природного, техногенного или социального характера. Так, в исследовании «Статистика уязвимостей веб-приложений за 2010-2011 годы» [6], проведенном Positive Technologies, приводятся данные, полученные в результате подробного анализа защищенности 123 веб-приложений. По результатам анализа все исследованные ресурсы содержали уязвимости (в среднем по 15 уязвимостей на каждый из них). При этом 64% ресурсов содержали уязвимости критического уровня риска, 98% – среднего уровня и 37% – низкого, а около 10% сайтов были заражены вредоносным кодом. Десять уязвимостей, выявленных на наибольшем количестве сайтов, представлены на рис. 1.

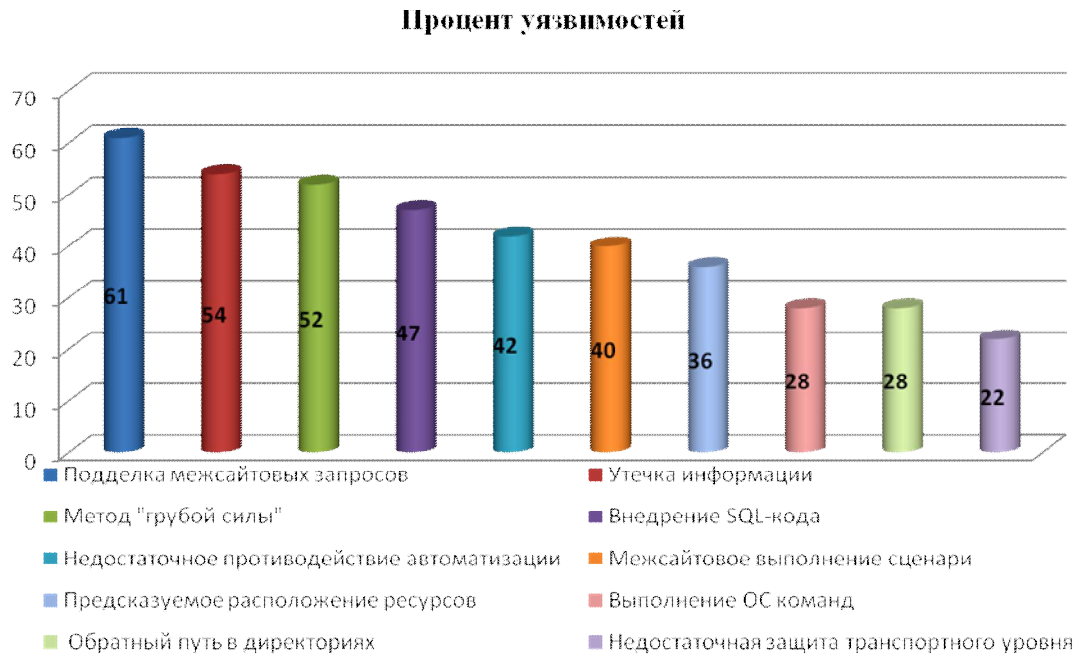


Рис. 1. **Наиболее распространенные уязвимости** (**доля сайтов**, %) [6]**.**

Данные о потерях российских вузов от сбоев в работе информационной инфраструктуры отсутствуют, однако можно предположить, что и для образовательных учреждений, оказывающих дистанционные образовательные услуги в сфере высшего профессионального образования, проблема УНБ актуальна. Среди потенциальных инцидентов и нарушений непрерывности можно назвать: сбои оборудования; некорректную работу программного обеспечения; несанкционированный доступ к информационно-образовательным ресурсам; воздействия вредоносного программного обеспечения; ошибки обслуживающего персонала и пользователей; техногенные воздействия и др. Нарушения непрерывности функционирования бизнес-процессов и ИТ-сервисов электронной информационно-образовательной среды вуза ведут к снижению качества предоставляемых образовательных услуг и эффективности информационного обеспечения, потере конкурентных преимуществ образовательного учреждения и др.

В вузах в области УНБ существуют следующие типичные недоработки: отсутствуют планы, которые были бы направлены на восстановление после сбоев или прерываний деятельности бизнес-функций; неполная структура и отсутствие задокументированных протоколов нарушения непрерывности и восстановления бизнес-процессов в результате системных сбоев, аварий, катастроф и других непредвиденных негативных обстоятельств; не полный и не регулярный анализ воздействия существующих рисков, угроз и уязвимостей на бизнес-функции образовательного учреждения; недостаточный уровень подготовки

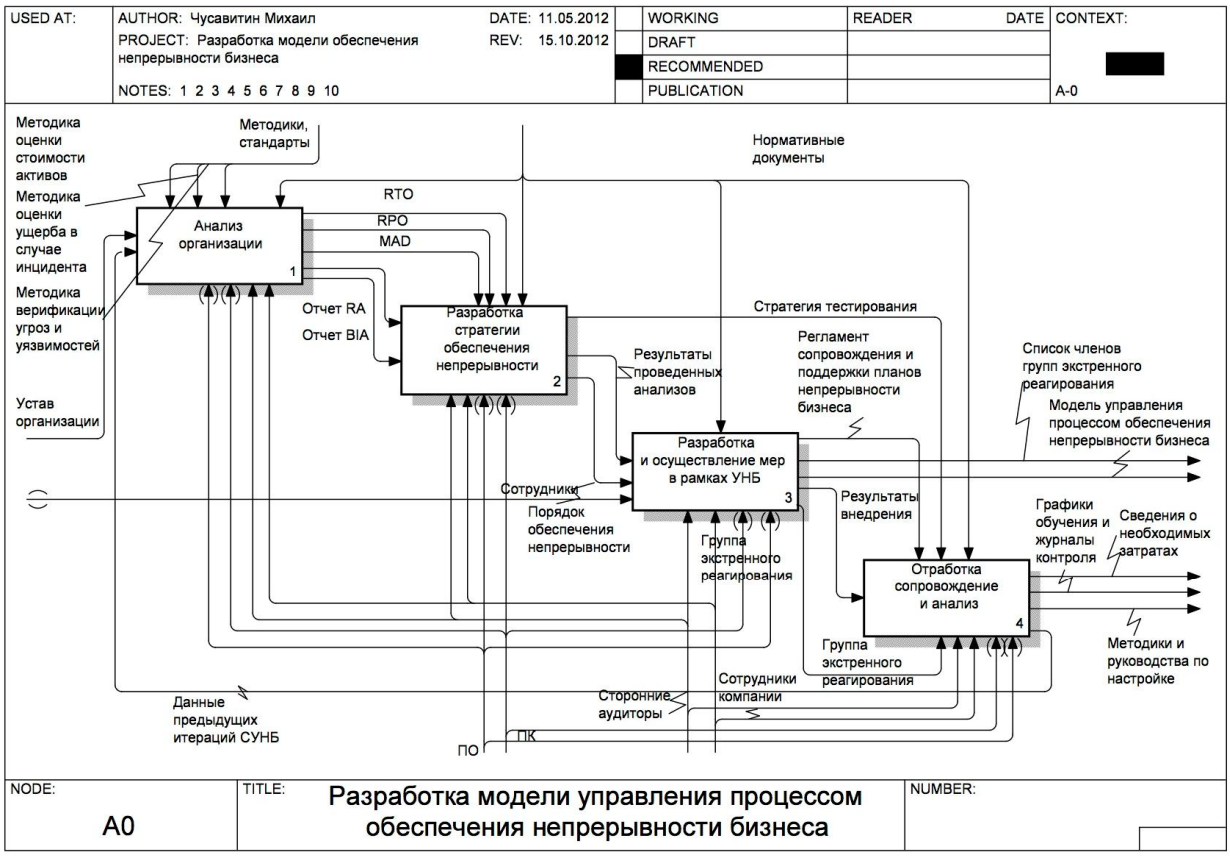
сотрудников по вопросам УНБ и др. Вышеизложенные обстоятельства обуславливают объективную потребность в разработке программы управления непрерывностью деятельности вуза в сфере оказания дистанционных образовательных услуг.

Жизненный цикл процесса УНБ согласно ГОСТ Р 53647 включает шесть элементов: управление программой построения процесса УНБ; анализ организации; определение стратегии обеспечения непрерывности деятельности; разработка и внедрение процедур реагирования; тестирование, поддержка и пересмотр мероприятий процесса УНБ; встраивание процесса управления непрерывностью деятельности в культуру организации. Фрагмент, разработанной в ходе исследования обобщенной модели УНБ, представлен на рис. 2. С учетом низкого уровня зрелости системы УНБ образовательной организации первоочередной задачей является анализ непрерывности деятельности вуза.

Согласно требованиям стандарта ГОСТ Р 53647.1-2009 и с учетом рекомендаций, изложенных в [2–4; 6; 7 и др.], был разработан и реализован проект по анализу системы УНБ вуза в сфере оказания дистанционных образовательных услуг. Данный анализ предназначен для обеспечения понимания организацией непрерывности своей деятельности путем идентификации ключевых продуктов и услуг, а также поддерживающих их критических видов деятельности и ресурсов [2].

В результате проведенного нами анализа воздействия на бизнес (BIA Business Impact Analysis) были определены воздействия инцидентов (нарушений) на образовательную деятельность вуза и идентифицированы критические виды деятельности, определены требования к непрерывности критического вида деятельности, а также – значения допустимых отклонений основных параметров, при которых обеспечивается требуемый уровень эффективности работы ИТ-сервисов. Следующим шагом анализа являлась оценка угроз выявленному наиболее критичному виду деятельности вуза – «оказание дистанционных образовательных услуг». Данный бизнес-процесс исследовался с точки зрения подверженности тем или иным объективным внешним и внутренним угрозам, выявлялись уязвимости каждого ресурса, поддерживающего данный бизнес-процесс, и определялось потенциальное воздействие при превращении угрозы в инцидент, нарушающий деятельность организации. На данном шаге был построен реестр рисков прерывания критического бизнес-процесса. Под рисками мы понимаем возможность возникновения неблагоприятных условий или воздействий на образовательную деятельность вуза (включая миссию, функции, образ, репутацию, активы, ресурсы), обуславливаемых взаимодействием образовательной системы с угрозами и опасностями, индуцируемыми и производимыми в результате функционирования электронной информационно-образовательной среды.

Иерархическая структура рисков, разработанная в ходе проекта, базируется на архитектуре образовательной системы (Learning Technology Systems Architecture – LTSA), введенной в международном стандарте IEEE P1484.1 (IEEE P1484.1/D8, 2001-04-06), используемом для проведения лицензирования информационных систем в области образования и снижения рисков при проектировании и разработке информационных систем в области обучения.



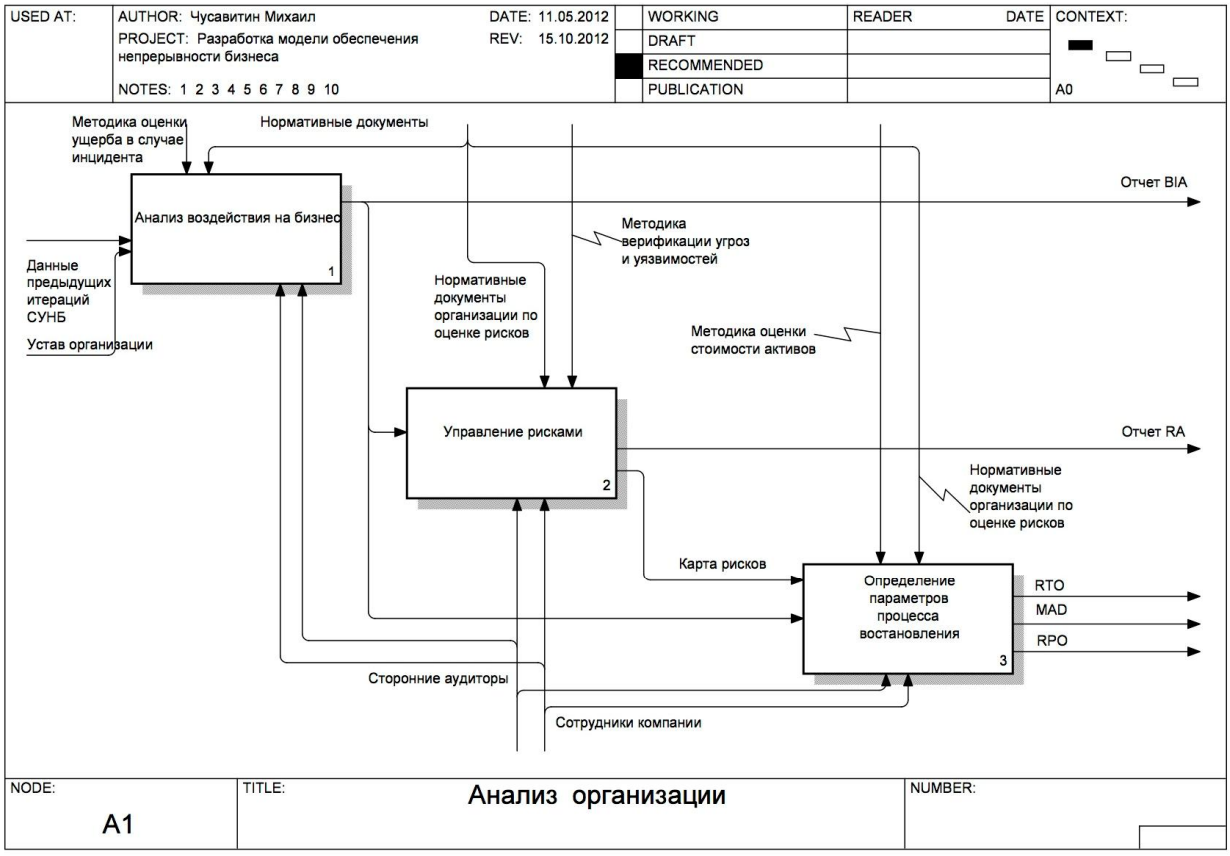


Рис. 2. Модель МНБ.

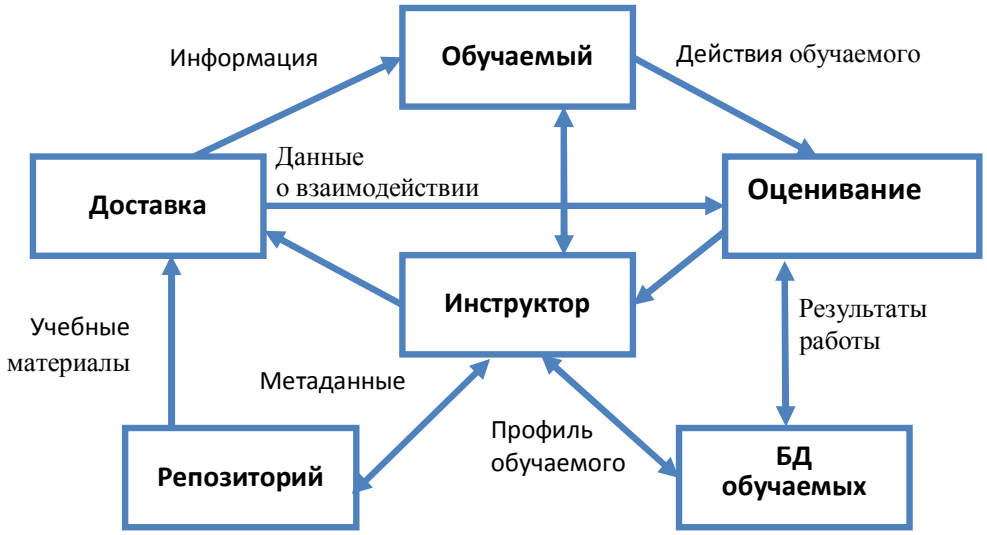


Рис. 3. Архитектура информационно-образовательной среды.

Согласно уровню 3 System (Компоненты системы) данного стандарта архитектура информационно-образовательной среды содержит следующие компоненты: «Обучаемый», «Инструктор», «Репозиторий», «Доставка», «Оценивание», «База данных обучаемых» (рис. 3).

В соответствии с этим в проекте были выявлены риски обучаемого, инструктора, БД обучаемого; риски, связанные с репозитарием, оцениванием и доставкой. На этапе идентификации рисков нами были проанализированы инциденты, связанные с нарушением непрерывности дистанционного образования в МаГУ, использовались материалы из открытых источников, в том числе научные работы, базы данных угроз и уязвимостей информационной инфраструктуры, бенчмаркетинг и др. В ходе проделанной работы был составлен реестр рисков, содержащий описание: условий возникновения риска, возможного воздействия, возможного ущерба, причины риска, типа риска. Ниже представлен фрагмент реестра риска (табл. 1).

На следующем этапе необходимо было определить действия для снижения потерь и обработки риска. Как правило, каждый вид риска допускает несколько вариантов управления, поэтому возникает задача сравнительного анализа их эффективности. Основными способами управления рисками являются предупредительные мероприятия, резервирование, страхование, диверсификация и хеджирование. Выбор способа управления рисками осуществляется путем сравнения расчетных показателей риска для различных управляющих воздействий. Как правило, в модели присутствует набор управляющих параметров, варьируя которые можно задавать стратегию управления. Задание управляющих воздействий может подразумевать также изменение структуры модели, соответствующее

определенным реорганизационным мероприятиям в самой компании. Например, для воздействия на антропогенные риски можно использовать предупредительные мероприятия, состоящие в обучении и регулярной переподготовке кадров.

Таблица 1 – Фрагмент реестра рисков

Категория: Репозиторий (Образовательные информационные ресурсы)
Класс: Контрольно-измерительные материалы
Подкласс: Тестовые материалы

Описание риска (угрозы)	**Уязвимости**	**Возможный источник угрозы**	**Вероятные последствия – результаты реализации угрозы (сценарии)**
Перегрузка приложения тестирования	Отсутствие механизма защиты от перегрузки канала связи. Архитектура приложения, неоптимизированная для высоких нагрузок	Студент	Невозможность проведения тестирования; изменение базы тестирования преподавателем; оценки результатов тестирования. Вред репутации организации
Несанкционированный доступ к ответам и результатам тестирований	Информация частично, или полностью не зашифрована. Действие вредоносного ПО	Студент	Фальсификация результатов тестирования. Компрометация тестового набора. Невозможность проведения тестирования
Отсутствие доступа к материалам тестирования	Сетевые кабели не продублированы и не защищены. Выход из строя оборудования сервера. Архитектура приложения не поддерживает технологии обеспечения должной отказоустойчивости. Отсутствие системы своевременного распознавания вторжения на сервере. Неверная настройка ПК	Студент. Администратор	Невозможность проведения тестирования; оценки результатов
Умышленное изменение содержания	Использование слабых паролей владельцами информации. Информация частично или полностью не зашифрована. Не используется блокировка ПК. Действие вредоносного ПО	Студент. Преподаватель	Фальсификация, изменение рейтингов успеваемости

Низкая производи-тельность тестирования	Непродуманная архитектура решения. Незапланированная большая нагрузка на сервер. Недостаток вычислительных ресурсов. Неверная приоритетность задач на сервере	Препода-ватель. Студент. Админи-стратор сервера	Невозможность проведения тестирования частично или полностью. Компрометация результатов при повторном проведении тестирования

На следующем этапе исследования предполагается определить стратегию МНБ, разработать и внедрить ответные меры, осуществлять поддержку и анализ МНБ, внедрять МНБ в культуру организации. В результате проделанной работы ожидается обеспечить:

— возрастание эффективности и качества электронного образования за счет повышения непрерывности и устойчивости ИТ-сервисов и поддерживающей инфраструктуры, снижения возможного ущерба при сбоях и катастрофах;

— оптимальное распределение имеющихся ресурсов вуза по критерию «эффективность – стоимость» при применении специальных средств и методов обеспечения непрерывности;

— повышение обоснованности стратегии, плана и программы развития информационных технологий, информационных систем образовательного учреждения и средств их обеспечения;

— повышение эффективности использования бюджетных ресурсов, выделяемых ИТ подразделениям, и др.

Список литературы

1. ГОСТ Р 53647.1-2009. Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 998-ст.

2. ГОСТ Р 53647.2-2009. Менеджмент непрерывности бизнеса. Часть 2. Требования. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 998-ст.

3. ГОСТ Р 53647.3-2010. Менеджмент непрерывности бизнеса. Часть 3. Руководство по внедрению. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 735-ст.

4. Об образовании : Закон Российской Федерации от 10 июля 1992 года № 3266-1.

5. Петренко С.А., Беляев А.В. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться. Информационные технологии для инженеров. – М. : ДМК Пресс ; Компания АйТи, 2011. – 400 с.
6. Статистика уязвимостей веб-приложений за 2010-2011 годы [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/files/Statistika2012.pdf (дата обращения: 17.10.08).
7. Чусавитин М.О. Применение методов имитационного моделирования при управлении непрерывностью бизнеса // Труды Вольного экономического общества России. Том сто шестьдесят четвертый. Москва : Российский экономический университет имени Г.В. Плеханова, 2011. - С. 192–200.
8. ISO/IEC 27031:2011 «Информационные технологии. Методы обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий для обеспечения непрерывности бизнеса».

Рецензенты

Баранкова Инна Ильинична, д.т.н., профессор, зав. кафедрой информатики и информационных технологий ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск.

Девятов Диляур Хасанович, д.т.н., профессор, зав. кафедрой вычислительной техники и прикладной информатики ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск.