Published in the Russian Federation
Sochi Journal of Economy
Has been issued since 2007.
ISSN: 1996-9005
Vol. 41, Is. 3, pp. 167-175, 2016

www.vestnik.sutr.ru

UDC 338.2 + 004.56

The Place of Risk Assessment in the Process of Business Continuity Management

Vladlena S. Oladko

Financial University under the Government of the Russian Federation, Russian Federation
125993 (GSP-3), Moscow, Leningradsky prosp., 49
PhD (Engineering), lecturer
E-mail: oladko.vs@yandex.ru

Abstract

The article considers the actual problem of assessing risks to business continuity due to failures of information infrastructure of the organization. The main causes of discontinuities and methods of assessment of damage from the effects analyzed. The author considers and describes the stages of the life cycle of business continuity management. The importance and place of risk assessment in the process of business continuity management is indicated. A conceptual model of risk management of business continuity was developed.

Keywords: failure, information infrastructure, enterprise network, risk management, information security, threat, damage.

Введение

В настоящее время деятельность любой организации невозможна без использования информационных систем (ИС), которые позволяют обрабатывать, хранить и передавать большие объемы данных, автоматизируют большинство бизнес-процессов и играют значительную роль в жизненном цикле производства продукции или оказании услуг. Эффективность выполнения данных функций определяется влиянием различных угроз и дестабилизирующих факторов на программно-аппаратное обеспечение и три основных свойства информации: конфиденциальность, целостность, доступность. Поскольку от выполнения данных свойств и надежности программно-аппаратного обеспечения будет напрямую зависеть непрерывность функционирования ИС и деятельность всего предприятия в целом. Это подтверждается и данными исследований, проведенных компанией Positive Technologies в 2014–2015 годах [1], которые показали, что нарушение информационной инфраструктуры, на долю которой приходится 31 % случаев, является одним из основных последствий инцидентов информационной безопасности.

При этом необходимо учитывать, что при обеспечении требуемого уровня безопасности информации и непрерывности деятельности предприятия необходимо обеспечить защиту, как от атак злоумышленника, так и от угроз случайного характера. Выбор и проектирование подобной системы защиты осуществляется в процессе управления непрерывностью бизнеса, стратегии и жизненный цикл которого регламентированы нормативно методическими документами и регуляторами. При этом важную роль в процессе управления играет именно оценка риска, позволяющая проанализировать и рассчитать опасность каждой возможной угрозы и отобрать наиболее опасные и актуальные причины нарушения непрерывности деятельности защиту от которых нужно предусмотреть в первую очередь.

Материалы и методы

Для написания данной статьи были использованы материалы научной, учебной литературы, законодательство Российской Федерации, статистические данные, собранные из печатных и электронных источников информации.

В качестве основных методов исследования при выполнении работы были использованы: метод описания, системного анализа, аналогии и обобщения.

Причины нарушения непрерывности бизнеса

Анализ литературных источников [2-4] показывает, что процесс функционирования ИС регламентируется, обеспечивается и управляется на четырех уровнях:

— аппаратный уровень – используемые технические средства и аппаратное обеспечение.

— программный уровень – используемое гетерогенное программное обеспечение;

— правовой уровень – использует нормативно-методические документы, стандарты и руководящие документы регуляторов;

— организационный уровень – планы и политики организации собственника ИС.

При этом, наиболее критичными для непрерывности деятельности являются такие элементы аппаратной части как сервера и сетевое оборудование. Сбои и ошибки в работе на уровне программного обеспечения так же являются критичными, поскольку они могут привести к нарушению целостности и доступности обрабатываемых данных, потери при их передаче и полном уничтожении при хранении. В качестве основных источников угроз и дестабилизирующих факторов, приводящих к нарушению функционирования ИС и прерыванию деятельности предприятия можно выделить:

1) Человеческий фактор (антропогенные угрозы):

–террористические акты;

–биологические инциденты (например, эпидемия, заражение, пандемия);

–социальная нестабильность (например, забастовки персонала);

–атаки внешнего злоумышленника на объекты ИС (например, DDos-атаки);

–атаки внутреннего злоумышленника – инсайдера (например, отключение сервисов, уничтожение информации);

–кража и порча оборудования, вандализм.

2) Техногенные угрозы:

–аварии в системах электроснабжение и отключение электроэнергии;

–ошибки и сбои в работе информационно-программного обеспечения;

–отказы аппаратного обеспечения ИС и поддерживающей инфраструктуры;

–повреждение каналов связи;

–аварии систем жизнеобеспечения (водоснабжение, газ, канализация);

–нарушение информационной безопасности (вредоносное ПО).

3) Природно-техногенные:

–пожар;

4) Природные:

–наводнение;

–гроза;

–паводок;

–ураган.

В результате реализации данных угроз может наблюдаться:

— блокировка доступа к помещениям и поддерживающей инфраструктуре предприятия;

— прерывание бизнес-процессов;

— недоступность персонала;

— недоступность каналов связи;

— недоступность сетевого оборудования;

— недоступность серверов и хостов;

— недоступность программного обеспечения и приложений;

— недоступность носителей информации;

— недоступность критичной информации и данных;

— недоступность финансовых ресурсов;

— нарушение информационно-вычислительного процесса;

— нарушение целостности и доступности данных в процессе их хранения и обработки;

— нарушение информационно-логического взаимодействия пользователей в ИС;

— нарушение функций мониторинга сети;

— нарушения процесса передачи данных, с последующим искажением, нарушением целостности и/или потерей;

— недоступность поставщиков, клиентов, партнеров.

В соответствии с [5, 6] для оценки тяжести последствий от угроз и возможного ущерба применяются количественные и качественные подходы:

–денежное выражение ущерба от каждой угрозы и расчет суммарного ущерба (например, экспертно или на основании статистики типовых инцидентов);

–оценка тяжести ущерба с помощью лингвистических переменных в качественной шкале от «очень низкого» до «критического» в зависимости от степени принятия предприятием того или иного уровня потерь (например, в зависимости от доли ущерба от уставного капитала предприятия);

–оценка тяжести ущерба в количественной ранговой шкале в зависимости от тяжести последствий (например, от времени простоя).

Полученные значения ущерба используют в дальнейшем при оценке риска от каждой угрозы и ее ранжировании.

Управление непрерывностью бизнеса

В соответствии с ГОСТ Р 53647.1-2009 жизненный цикл процесса управления непрерывностью бизнеса и функционирования ИС состоит из четырех основных этапов анализ которых представлен в таблице 1.

Таблица 1. Этапы жизненного цикла управления непрерывностью деятельности предприятия.

№ этапа	Назначение этапа	Описание шагов
Этап 1. Анализ непрерывности деятельности предприятия	Анализ текущего состояния бизнеса организации и факторов влияющих на устойчивость и надежность функционирования ИС и непрерывность бизнес процессов	А) Определение потребности и актуальности управления непрерывностью деятельности Б) Разработка содержания проекта обеспечения непрерывности деятельности и его пошагового плана. Определение, как будет исполняться проект, проводиться его мониторинг, аудит и закрытие. Определение границы проекта, роли членов проектной команды и цели проекта. В) Изучение и составление ранжированных списков критичных и наиболее ценных ресурсов, бизнес-процессов, сервисов и данных предприятия, установление их взаимозависимости Г) Анализ угроз непрерывности деятельности, позволяет исследовать возможное воздействие инцидентов на ключевые виды деятельности предприятия, данные, ИС и бизнес-процессы. Д) Определение показателей непрерывности MOA, RTO, RPO, SDO. Е) Оценка рисков и составление модели актуальных по уровню риска угроз

		нарушения непрерывности, защиту от которых необходимо предусмотреть в первую очередь.
Этап 2. Выбор (разработка) стратегии непрерывности деятельности	Анализ стратегий обеспечения непрерывности деятельности и выбор соответствующих превентивных или ответных мер на актуальные угрозы для каждого бизнес-процесса, сервиса, объекта ИС таким образом, чтобы предприятие могло продолжать свою деятельность и оказывать услуги на допустимом уровне.	А) Планирование защиты приоритетных и критических бизнес-процессов, данных, сервисов и объектов ИС. Б) Планирование механизмов смягчения последствий инцидентов, разработка ответных и превентивных мер В) Выбор эффективных средств и решений по обеспечению непрерывности на основе допустимого риска, стоимости восстановления и стоимости простоя.
Этап 3. Разработка и внедрение ответных мер на угрозы нарушения непрерывности	Разработка и внедрение в управление непрерывностью деятельности ответных мер на угрозы для создания структуры управления при возникновении инцидента, планов непрерывности функционирования и планов восстановления функционирования, подробно описывающих ответные меры, которые должны быть предприняты в процессе и после инцидента для поддержки или восстановления деятельности предприятия.	А) Реагирование на угрозы, влекущие нарушение непрерывности функционирования ИС. Определение последовательности действий, которые необходимо осуществить при обнаружении инцидента нарушения непрерывности. Б) Управление инцидентами — определяет методы, необходимые для смягчения или уменьшения размера происшествия. В) Восстановление деятельности — определяет последовательность действий, которые необходимо осуществить для того, чтобы восстановить данные, подсистемы ИС и сервисы на заданном уровне.
Этап 4. Применение поддержка и анализ	Проведение регулярного анализа и аудита планов и средств обеспечения непрерывности, поддержка их в состоянии полноты и актуальности	А) Тестирование и пересмотр планов, целью является получение подтверждения работоспособности планов, проверка достаточности и методического и технического обеспечения, получение персоналом предприятия и группой восстановления необходимых навыков и знаний. Б) Обслуживание и обновление планов, в случаях: изменения инфраструктуры ИС, изменения организационной структуры предприятия, изменений в законодательстве, обнаружения недостатков в планах при их тестировании

По результатам проведённого анализа жизненного цикла можно сделать вывод о том, что управление непрерывностью деятельности предприятия является циклическим процессом, в котором особое место занимают процедуры оценки и управления риском (см. рис. 1). Поскольку именно оценка и анализ риска позволяет определить допустимый для предприятия уровень риска, составить модель актуальных и наиболее опасных с точки зрения ущерба для каждого конкретного предприятия угроз нарушения непрерывности деятельности. А затем, основываясь на принципе поиска оптимального соотношения между стоимостью решений по обеспечению непрерывности, восстановлению и стоимостью простоя подобрать наиболее приемлемые для предприятия решения (см. рис. 2). Применение выбранных на основе оценки риском механизмов обеспечения и восстановления непрерывности функционирования, позволит не допустить риск окончательного прекращения деятельности предприятия, в случае, если предоставление сервисов, данных, бизнес-процессов и/или услуг не будут возобновлены.

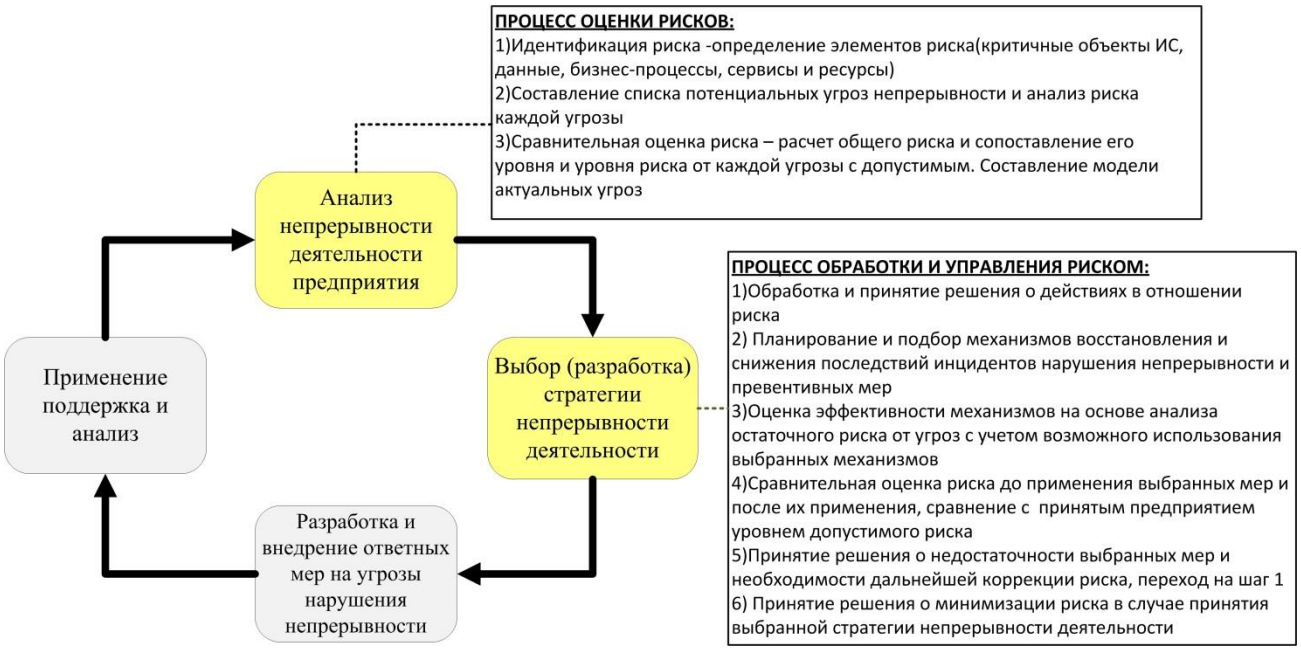

Рис. 1. Место оценки рисков на этапах жизненного цикла управления непрерывностью бизнеса

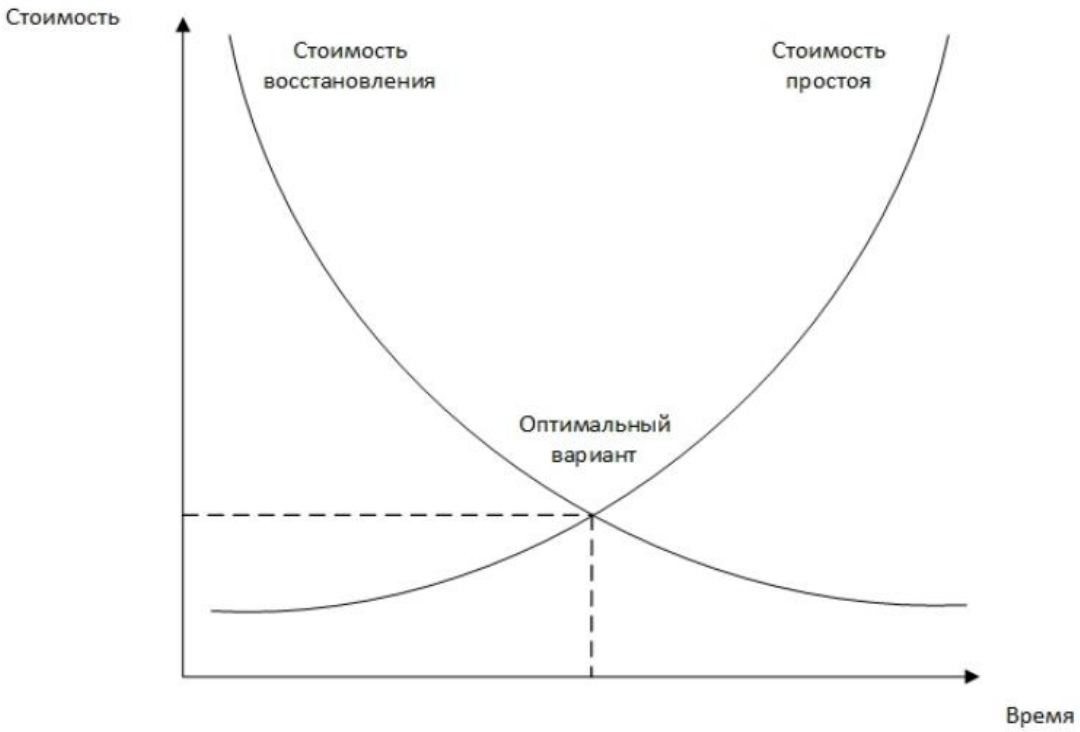

Рис. 2. Выбор оптимального решения по обеспечению непрерывности бизнеса на основе управления риском

Таким образом, можно сделать вывод, что управление непрерывностью на всех этапах жизненного цикла обеспечивает объединение всех применяемых на предприятии мер в целостный, адекватный реальным угрозам и управляемый комплекс, позволяющий предприятию непрерывно предоставлять услуги, избежать влияния угроз, дестабилизирующих факторов, чрезвычайных ситуаций и атак злоумышленника, а также минимизировать возможный ущерб. При этом ключевое значение на начальных этапах жизненного цикла управления непрерывностью деятельности имеет управление рисками информационной безопасности, которое по своей сути представляет собой ядро данной системы.

Модель управления рисками нарушения непрерывности бизнеса

В соответствии с поставленными перед управлением непрерывностью бизнеса целями и задачами, была разработана концептуальная схема процесса управления рисками, которая представлена на рисунке 3 и описывается последовательностью из восьми шагов:

1) сбор данных о предприятии, информационной инфраструктуре и требованиях к непрерывности бизнеса и непрерывности функционирования информационной инфраструктуры;

2) идентификация объектов и источников риска;

3) составление модели угроз;

4) оценка ущерба и риска от каждой угрозы;

5) анализ и сравнительная оценка рисков;

6) обработка рисков и выработка управленческих решений относительно риска;

7) реализация управленческих решений, поиск дополнительных средств, и повторная оценка риска;

8) формирование отчета и рекомендаций по управлению рисками и снижению потенциально опасных рисков.

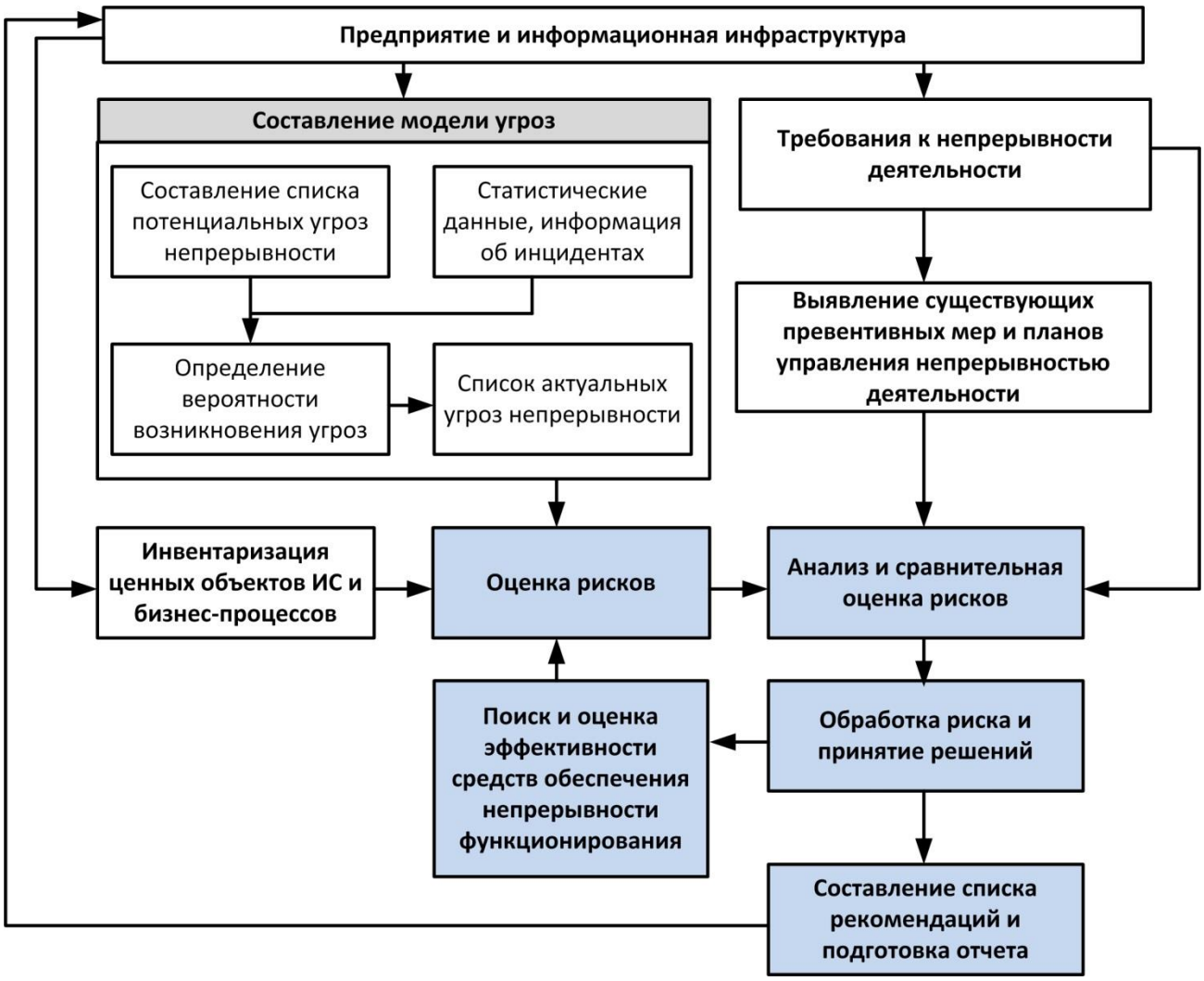

Рис. 3. Концептуальная схема управления риском нарушения непрерывности бизнеса

Шаги с 4 по 7 представляют собой цикл с обратной связью, выход из которого осуществляется при условии эффективности управляющих воздействий. В том случае если решения признаны недостаточно эффективными, рекомендуется повторить цикл управления и выработать новые решения.

Заключение

В настоящее время одним из наиболее частых последствий инцидентов информационной безопасности является нарушение информационной инфраструктуры предприятия, влекущее за собой потери данных, остановки бизнес-процессов и нарушение непрерывности бизнеса. Для снижения тяжести подобных последствий применяют различные стратегии обеспечения непрерывности бизнеса, целью которых является как проактивная защита от угроз, так и быстрое восстановление функционирования системы и доступности данных и сервисов. Для выбора наиболее эффективной и сбалансированной стратегии, позволяющей обеспечить приемлемый для предприятия уровень непрерывности бизнеса, необходимо в рамках жизненного цикла управления непрерывностью бизнеса регулярно применять процедуры управления рисками. Предложенная концептуальная модель управления рисками может применяться на таких стадиях жизненного цикла как проектирование и сопровождение информационной инфраструктуры предприятия, выработка и принятие стратегий непрерывности бизнеса, а также периодический аудит состояния экономической и информационной безопасности предприятия. В дальнейшем планируется автоматизация модели управления рисками нарушения непрерывности деятельности и создания системы поддержки принятия решений, которая сможет

применяться при управлении непрерывностью бизнеса предприятия и в процессе периодического внутреннего аудита.

Примечания:

1. Positive Research 2015. Сборник исследований по практике безопасности [Электронный ресурс]. PTSecurity. URL: http://www.ptsecurity.ru/download/PT_Positive_Research_2015_RU_web.pdf (дата обращения 12.09.2016).

2. Максимов Д.Н. Формирование модели управления бизнес-процессами предприятия легкой промышленности на основе информационных технологий [Электронный ресурс] // Экономика и социум. 2015. №2(15). URL: http://www.iupr.ru/domains_data/files/zurnal_15/Maksimov%20D.N.%20%28informacionnye%20i%20kommunikativnye%20tehnologii%29.pdf (дата обращения 20.09.2016).

3. Тысячникова Н.А. Обеспечение непрерывности бизнеса является приоритетной задачей кредитной организации и важнейшим фактором финансовой устойчивости банковской системы в целом. [Электронный ресурс]. Внутренний контроль в кредитной организации. 2009. №3 URL: http://gaap.ru/articles/obespechenie_nepreryvnosti_deyatelnosti_bankov_planirovanie_i_kontrol/ (дата обращения 20.09.2016).

4. Оладько В.С. Программный комплекс для активного мониторинга и аудита безопасности корпоративной сети организации // Моделирование, оптимизация и информационные технологии. 2015. № 3 (10). С. 17.

5. Дорофеев А.В., Марков А.С. Планирование обеспечения непрерывности бизнеса и восстановления // Вопросы кибербезопасности.2015. №3(11). С. 68-73.

6. Аткина В.С. Результаты исследования уровней катастрофустойчивости корпоративных информационных систем // Актуальные проблемы гуманитарных и естественных наук. 2012. № 9. С. 22-27.

References

1. Positive Research 2015. Sbornik issledovanii po praktike bezopasnosti [Elektronnyi resurs]. PTSecurity. URL: http://www.ptsecurity.ru/download/PT_Positive_Research_2015_RU_web.pdf (data obrashcheniya 12.09.2016).

2. Maksimov D.N. Formirovanie modeli upravleniya biznes-protsessami predpriyatiya legkoi promyshlennosti na osnove informatsionnykh tekhnologii [Elektronnyi resurs] // Ekonomika i sotsium. 2015. №2(15). URL: http://www.iupr.ru/domains_data/files/zurnal_15/Maksimov%20D.N.%20%28informacionnye%20i%20kommunikativnye%20tehnologii%29.pdf (data obrashcheniya 20.09.2016).

3. Tysyachnikova N.A. Obespechenie nepreryvnosti biznesa yavlyaetsya prioritetnoi zadachei kreditnoi organizatsii i vazhneishim faktorom finansovoi ustoichivosti bankovskoi sistemy v tselom. [Elektronnyi resurs]. Bnutrennii kontrol' v kreditnoi organizatsii. 2009. №3 URL: http://gaap.ru/articles/obespechenie_nepreryvnosti_deyatelnosti_bankov_planirovanie_i_kontrol/ (data obrashcheniya 20.09.2016).

4. Olad'ko V.S. Programmnyi kompleks dlya aktivnogo monitoringa i audita bezopasnosti korporativnoi seti organizatsii // Modelirovanie, optimizatsiya i informatsionnye tekhnologii. 2015. № 3 (10). S. 17.

5. Dorofeev A.V., Markov A.S. Planirovanie obespecheniya nepreryvnosti biznesa i vosstanovleniya // Voprosy kiberbezopasnosti.2015. №3(11). S. 68-73.

6. Atkina V.S. Rezul'taty issledovaniya urovnei katastrofustoichivosti korporativnykh informatsionnykh sistem // Aktual'nye problemy gumanitarnykh i estestvennykh nauk. 2012. № 9. S. 22-27.

УДК 338.2 + 004.56

Место оценки риска в процессе управления непрерывностью бизнеса

Владлена Сергеевна Оладько

Финансовый университет при Правительстве Российской Федерации, Российская Федерация
125993 (ГСП-3), г. Москва, Ленинградский просп., 49
Кандидат технических наук, преподаватель
E-mail: oladko.vs@yandex.ru

Аннотация. В статье рассмотрена актуальная проблема оценке рисков нарушения непрерывности бизнеса вследствие отказов и сбоев информационной инфраструктуры организации. Проанализированы основные причины нарушения непрерывности бизнеса и способы оценки ущерба от возможных последствий. Рассмотрены и описаны этапы жизненного цикла процесса управления непрерывностью бизнеса и показана значимость процедуры оценки риска в данном процессе. Представлена разработанная концептуальная модель управления рисками непрерывности бизнеса.

Ключевые слова: отказ, информационная инфраструктура, корпоративная сеть, управление рисками, информационная безопасность, угроза, ущерб.